UNIVERSIDADE FEDERAL DO PARANÁ

DIOGO DE ANDRADE

# O USO DE CADEIAS DE ASSINATURAS PARA DISTRIBUIÇÃO E GERENCIAMENTO DE CHAVES EM REDES TOLERANTES A ATRASOS E DESCONEXÕES

CURITIBA

2013

DIOGO DE ANDRADE

# O USO DE CADEIAS DE ASSINATURAS PARA DISTRIBUIÇÃO E GERENCIAMENTO DE CHAVES EM REDES TOLERANTES A ATRASOS E DESCONEXÕES

Dissertação apresentada ao Programa de Pós-Graduação em Informática, Departamento de Informática, Setor de Ciências Exatas, Universidade Federal do Paraná, como parte das exigências para a obtenção do título de Mestre.

Orientador:Prof. Dr. Luiz Carlos Pessoa Albini

CURITIBA

2013

A553u Andrade, Diogo de
O uso de cadeias de assinaturas para distribuição e gerenciamento de chaves em redes tolerantes a atrasos e desconexões. / Diogo de Andrade. – Curitiba, 2013.
403f. : il.; 30 cm.

Dissertação (mestrado) - Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-graduação em Informática, 2013.
Orientador: Luiz Carlos Pessoa Albini.
Bibliografia: p. 132-136.

1.Computadores - Medidas de segurança. 2. Internet (Redes de computação) - Sistemas de segurança. 3. Criptografia. I. Universidade Federal do Paraná. II. Albini, Luiz Carlos Pessoa. III. Título.

CDD: 005.82

Ministério da Educação
Universidade Federal do Paraná
Programa de Pós-Graduação em Informática

# PARECER

Nós, abaixo assinados, membros da Banca Examinadora da defesa de Dissertação de Mestrado em Informática, do aluno Diogo de Andrade, avaliamos o trabalho intitulado, *"O Uso de Cadeias de Assinaturas para Distribuição e Gerenciamento de Chaves em Redes Tolerantes a Atrasos e Desconexões"*, cuja defesa foi realizada no dia 28 de fevereiro de 2013, às 15:00 horas, no Departamento de Informática do Setor de Ciências Exatas da Universidade Federal do Paraná. Após a avaliação, decidimos pela aprovação do candidato.

Curitiba, 28 de fevereiro de 2013.

Prof. Dr. Luiz Carlos Pessoa Albini
**DINF/UFPR** – Orientador

Prof. Dr. Luiz Augusto de Paula Lima Jr
**PUC/PR**– Membro Externo

Prof. Dr. André Luiz Pires Guedes
**DINF/UFPR** – Membro Interno

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ
Setor de Ciências Exatas
Coordenação de Pós-Graduação em Informática

À Ana Paula, minha esposa amada.
Aos meus pais Altino e Lourdes.
Por todo amor, por quem sou e
por tudo que alcancei.

# AGRADECIMENTOS

Considero a folha de agradecimento deste trabalho a prova de que ele é fruto do trabalho não só de uma pessoa, mas sim de todos que o cercam.

Desta forma, agradeço a Deus, por todas as oportunidades que surgiram pelos caminhos percorridos e que ainda virão.

À minha esposa, Ana Paula de Carvalho, que compreendeu como ninguém as dificuldades enfrentadas para que esse trabalho chegasse ao fim.

Agradeço, também, aos meus pais pelo apoio e incentivo durante essa caminhada de estudos que começou em uma escolinha primária municipal do subúrbio de Curitiba.

Aos meus queridos(as) amigos(as) e familiares que estiveram próximos nesse momento, principalmente ao pessoal do grupo de pesquisa NR2 da UFPR que me auxiliou e colaborou em muitos momentos do desenvolvimento deste trabalho. Aos colegas de trabalho da GVT e da LACTEC que me concediam tempo para comparecer à reuniões e aulas durante o horário de trabalho. Aos amigos da graduação de Ciência da Computação, que mesmo sem eu dar sinais de vida ainda convidavam para as festinhas que eram organizadas.

Agradeço imensamente ao meu orientador, Luiz Carlos P. Albini, por toda disposição, subsídio e, principalmente, pela confiança na minha capacidade de desenvolver esse estudo.

Ao PPGInf/ UFPR pela oportunidade.

# RESUMO

As Redes Tolerantes a Atrasos e Desconexões (DTNs) são parte das redes *Ad-Hoc* e, desta forma, herdam seus problemas, dentre eles, o problema de prover segurança. Por serem redes que usam sinais de rádio para estabelecer comunicação entre seus participantes, elas podem ser alvo de ataques passivos, nos quais os atacantes não interferem diretamente na rede, e ataques ativos, nos quais eles interferem diretamente na rede. O uso de criptografia para cifrar as mensagens é uma das principais técnicas de defesa usada contra ataques. Há duas formas de criptografia: simétrica e assimétrica. Nos sistemas simétricos, as mensagens são cifradas e decifradas com a mesma chave. Já nos sistemas assimétricos, há duas chaves, uma para cifrar e outra para decifrar. Com o uso de alguns algoritmos específicos, pode-se usar o par de chaves do sistema assimétrico para garantir confiabilidade na origem da mensagem através do uso de assinaturas digitais. Para isso, o nodo cifra uma mensagem com sua chave privada a fim de garantir que todos os nodos que possuam sua chave pública possam abrir a mensagem e confiar em sua origem. A tarefa de administrar as chaves nos sistemas assimétricos é denominada de Gerenciamento de Chaves. Esse sistema consiste em gerar, distribuir, armazenar, validar e revogar as chaves bem como garantir a real relação entre chave e nodo. Existem poucos esquemas de gerenciamento de chaves para as DTNs, sendo que os existentes são baseados em estruturas que podem dificultar a comunicação entre os nodos, ou então, são facilmente afetados pela presença de nodos atacantes. Desta forma, este trabalho propõe um esquema de gerenciamento de chaves para DTNs baseado no encadeamento de assinaturas digitais e que siga as premissas de segurança: autenticidade, confidencialidade e integridade. No esquema proposto, os nodos repassam chaves públicas dentro de mensagens assinadas digitalmente, criando uma cadeia rastreável. Os nodos que recebem as cadeias só acessam a chave pública se possuírem todas as outras chaves para verificar cada assinatura. O esquema proposto converge para o ponto em que todos os nodos obtém as chaves públicas dos demais nodos da rede em cenários livres de atacantes. Foram realizadas também simulações em cenários com nodos atacantes do tipo *blackhole* e *greyhole*, *sybil* e falsificação. Na presença desses ataques, o esquema teve um acréscimo no tempo de convergência e, na grande maioria das simulações, atingindo um mínimo de 90% de chaves públicas obtidas.
**Palavras-chave:** DTN. Gerenciamento de chaves. Encadeamento. Assinatura digital.

# ABSTRACT

Delay Tolerant Networks (DTN) are part of Ad-Hoc networks, and thus inherit their problems, including the problem of providing security. Due to the fact that they are networks which radio signals to communicate among their participants, they may be subject to passive attacks, in which attacker nodes do not interfere directly in the network, and active attacks, in which nodes interfere directly in the network. The use of cryptography to encrypt messages is one of the main defense techniques against attacks. There are two forms of cryptography: symmetric and asymmetric. In symmetric systems, messages are encrypted and decrypted with the same key. In asymmetric systems, there are two keys, one to encrypt and another one to decrypt. With the use of some specific algorithms, the asymmetric pair of key system to ensure reliability in the message source through the use of digital signatures. In order to do this, the node encrypts a message with his private key in order to ensure that all nodes that have its public key can open the message and trust the source. The task of managing keys in asymmetric systems is called Key Management. This system consists in generating, distributing, storing, validating, and revoking the keys and ensuring the real relationship between the key and the node. There are few key management schemes for DTNs, among them, Hierarchical Identity-Based Cryptography (HIBC), Opportunistic Batch Bundle Authentication (OBBA-FAT) and a scheme based on asymmetric key exchange. This work proposes a key management scheme for DTNs based on the chain of digital signatures which follows the security tenets: authenticity, confidentiality and integrity. In the proposed scheme, nodes retransmit public keys inside the digitally signed messages, creating a trackable chain. The nodes that receive chains only access the public key if they have all other key signature to verify the signature. The proposed scheme converges to the point at which all nodes obtain public keys of other nodes in the network in scenarios which are free of attackers. Simulations in scenarios with attacker nodes of type blackholes and greyholes, sybil and falsification. We're performed as well this work presents the results of the scheme under these scenarios and shows its efficiency even under attacks.


**Keywords:** DTN. Key management. Chaining. Digital Signature.

# LISTA DE FIGURAS

# LISTA DE SIGLAS

BAB Bundle Authentication Block - Bloco de Autenticação Agregado

DoS Denial-of-Services - Rejeição de Serviços

DTN Delay Tolerant Network - Redes Tolerantes a Atrasos e Desconexões

DTNRG Delay Tolerant Networking Research Group

FAT Fragment Authentication Tree - Árvore de Autenticação Fragmentada

FDTN Ferry-Based Delay-Tolerant Networks - Redes Tolerantes a Atrasos e Desconexões com Balsas

GDH Group Diffie Hellman - Groupo Diffie Hellman

HIBC Hierarchical Identity-Based Cryptography - Criptografia Baseada em Hierarquia de Identidades

IRTF Internet Research Task Force

OBBA Opportunistic Batch Bundle Authentication - Autenticação de Rajada Oportunística

OSM Offline Security Manager - Gerente de Segurança Externo

PCB Payload Confidentiality Block - Bloco de Confidencialidade da Carga Útil

PGP Pretty Good Privacy - Privacidade Bastante Boa

PGP-Like Self-Organized Public Key Management System - Sistema de Gerenciamento de Chaves Públicas Auto-Organizado

PIB Payload Integrity Block - Bloco de Integridade da Carga Útil

PKG Private Key Genarator - Provedor de Chaves

PROPHET Probabilistic Routing Protocol using History of Encounters and Transitivity

SHA Secure Hash Algorithm - Algoritmo de Hash Seguro

The ONE The Opportunistic Network Environment simulator - Simulador de Ambientes para Redes Oportunística

# SUMÁRIO

# CAPÍTULO 1

# INTRODUÇÃO

As redes *Ad-Hoc* [1] [2] [3] são redes móveis sem infraestrutura, o que obriga todos os nodos a funcionarem como roteadores. As pesquisas em redes *Ad-Hoc* ainda estão concentradas em resolver problemas tais como roteamento [4] [5], consumo de energia [6], segurança [7] [8], dentre outros, limitando ainda seu uso.

A transmissão de dados nas redes ad-hoc é feita por meio de sinais de rádio. Para que haja a transmissão, os participantes da rede precisam estar em contato. Desta forma, define-se que estão em contato dois nodos quaisquer, *x* e *y*, se a posição ocupada por *x* estiver dentro de alcance da área de transmissão de *y*, e a posição ocupada por *y* estiver dentro de alcance da área de transmissão de *x*, assim como pode ser observado na Figura 1.1.

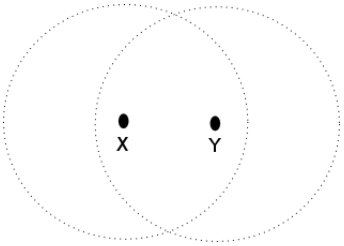



Figura 1.1: Exemplo de contato

Uma parte das redes *Ad-Hoc* são chamadas Redes Tolerantes a Atrasos e Desconexões *Delay Tolerant Network - DTN* [9] [10], cujo principal objetivo é permitir que os nodos transmitam, mesmo que o destino das mensagens possa estar ou ficar inalcançável durante um período de tempo. Isso ocasiona o armazenamento dos dados em *buffers* nos outros participantes até que possam ser entregues quando o destino for encontrado, independente do tempo que leve. Isso representa uma das principais características das DTNs. Apresentam, também, atrasos longos que podem variar de poucos milissegundos a dias ou até mesmo anos. Por fim, as frequentes desconexões podem gerar uma comunicação intermitente entre os nodos [11].

Para conseguir realizar o armazenamento persistente das mensagens há uma nova camada abaixo da camada de aplicação denominada *camada de agregação* (*Bundle Layer*) [12]. As camadas de uma DTN podem ser observadas na Figura 1.2.

As características da camada de agregação são: armazenamento persistente, decisões de roteamento, compartilhamento de dados agregados entre as aplicações e adaptação da camada de convergência a diferentes protocolos [13].


Figura 1.2: Camadas de uma DTN

Embora as DTNs apresentem essa diferença nas camadas de rede, elas herdaram os problemas das redes Ad-Hoc, dentre eles, a dificuldade em prover segurança. Devido a existência de um agravante, a dificuldade de diferenciar se um nodo ainda faz parte da rede ou se já a deixou.

A falta de informações confiáveis sobre o estado de um nodo na rede, permite que nodos maliciosos usem isso para se passar por outros nodos ou mesmo criarem nodos fictícios. Assim eles podem manipular o tráfego de dados, obter informações sigilosas sobre outros nodos, alcançar vantagens em votações ou na divisão de recursos distribuídos.

As redes Ad-Hoc e as DTNs têm sérios problemas com ataques, tanto ativos quanto passivos [14]. A saber, os ataques ativos são aqueles nos quais os nodos atacantes participam ou intervêm na rede de forma direta, como, por exemplo, alterando mensagens de dados, interferindo na criação de rotas ou gerando sobrecarga sobre algum nodo específico. Já os ataques passivos, são aqueles nos quais os nodos atacantes não interferem diretamente na rede, eles ficam “escutando” as transmissões e apenas estão interessados em obter informações que percorrem a rede [15].

Entre os ataques ativos pode-se destacar: *blackholes* e *greyholes* [16][17], *sybil* [18], falsificação e falta de cooperação [19]:

- Ataques *greyholes* e *blackholes* são aqueles nos quais os nodos maliciosos deixam de repassar parte das mensagens de alguns nodos da rede. Se essa parte representar todas as mensagens, o nodo recebe o nome de *blackhole*. Caso ele deixe de repassar apenas algumas mensagens, ele rebebe o nome de *greyhole*.
- Já o ataque *sybil* acontece quando um nodo cria identidades falsas para participar da rede, desta forma ele pode obter vantagem em uma votação por exemplo.
- O ataque de falsificação acontece quando um nodo tenta se passar por outro ou então, altera alguma informação para que nodos confundam um ao outro.

- O ataque de falta de cooperação é aquele no qual um nodo recusa-se a colaborar na rede com o armazenamento temporário de mensagens, por exemplo. Desta forma, o nodo usa os recursos da rede, mas não aceita compartilhar os seus recursos com os demais nodos.

A principal técnica de defesa contra ataques, ativos ou passivos, é a criptografia [20]. Nessa técnica, cada nodo tem atrelado uma chave que é usada para cifrar as mensagens. Há duas formas de criptografia: simétrica e assimétrica. Nos sistemas simétricos, cada par de nodos usa a mesma chave para cifrar e para decifrar as mensagens. Nos sistemas assimétricos, cada nodo possui duas chaves, uma usada para cifrar as mensagens e outra para decifrá-las [21]. Uma chave recebe o nome de chave pública e a outra de chave privada.

No sistema assimétrico, se o nodo origem de uma mensagem cifrá-la usando a chave pública do nodo destino, somente o nodo que possuir a chave privada correlacionada poderá abrí-la. Isso garante a confidencialidade da mensagem.

Embora a criptografia seja usada para impedir ou minimizar o efeito de diversos ataques, existem ainda ataques que não são afetados pelo uso de criptografia na troca de mensagens, como por exemplo ataques de falta de cooperação ou ataques da camada de rede (blackhole ou greyhole, por exemplo).

Ao usar determinados algoritmos, como por exemplo o RSA, para cifrar as mensagens, as mesmas chaves podem ser usadas para gerar o que é denominado de assinatura digital [22]. Na qual o nodo através de uma mensagem cifrada com sua chave privada garante a todos que possuem sua chave pública a vericidade da mensagem.

A administração segura das chaves é denominada gerenciamento de chaves [23]. O gerenciamento de chaves, nos sistemas assimétricos, consiste em gerar, distribuir, armazenar, validar, revogar e garantir a real relação entre chave e nodo.

Os sistemas simétricos possuem a vantagem do rápido processamento, entretanto, têm como desvantagem a necessidade do compartilhamento da chave entre os nodos, que comumente é feita por um meio seguro e pré estabelecido ou anterior a formação da rede, por exemplo, um canal de infravermelho de curto alcance ou via cabo. Devido a isso, esse sistema tornou-se inviável para uso nas redes Ad-Hoc devido a sua mobilidade. Os sistemas assimétricos têm um processamento mais lento e precisam de uma entidade que realize o gerenciamento das chaves. Em virtude da necessidade dessa entidade centralizadora gerencial de chaves, o modelo tradicional do sistema assimétrico também tornou-se inviável para uso em redes Ad-Hoc [8] [19].

Assim, para que o gerenciamento de chaves seja eficiente quando usado em redes Ad-Hoc, ele precisa levar em consideração a alta mobilidade dos nodos (topologia dinâmica e descentralidade) e ser auto-organizado [24]. Há vários esquemas de ge-

renciamento de chaves para redes Ad-Hoc na literatura:

- baseado em identidade [25];
- baseado em cadeias de certificados [26][27][28][29];
- baseado em *clusters* ou grupos [30][31][19];
- baseado em pré distribuição [32] e
- baseado em mobilidade [33]

Dentre os esquemas baseados em cadeias de certificados destaca-se o esquema *"Self-Organized Public Key Management System"* [26][27], chamado de *PGP-Like*. Esse esquema é totalmente distribuído e auto-organizável, baseado no conceito apresentado pelo *Pretty Good Privacy* (PGP) [34], no qual, os próprios nodos criam o par de chaves pública e privada e emitem certificados para os nodos de sua confiança. Cada nodo mantem um repositório de certificados que é trocado periodicamente com seus vizinhos. As chaves são autenticadas por meio da existência de cadeias de certificados, construídas com o repositório local de cada nodo. O *PGP-Like* não considera ataque de má conduta, possuindo apenas uma forma de detecção de certificados conflitantes.

A proposta inicial deste trabalho era verificar a eficácia do *PGP-Like* sobre uma DTN. Desta forma, foram feitas simulações, mas os resultados encontrados inviabilizaram a continuação da proposta.

Na figura 1.3 estão os resultados encontrados ao se aplicar o *PGP-Like* em uma rede DTN. Nota-se que em um período de 6 mil segundos poucos certificados conseguiram ser trocados entre os nodos. O principal problema encontrado é o próprio algoritmo do *PGP-Like*, pois um dos passos é a troca de repositórios de certificados entre origem e destino. Quando isso é necessário em uma DTN, poucas vezes obtém-se sucesso devido ao elevado tempo sem comunicação entre os nodos.

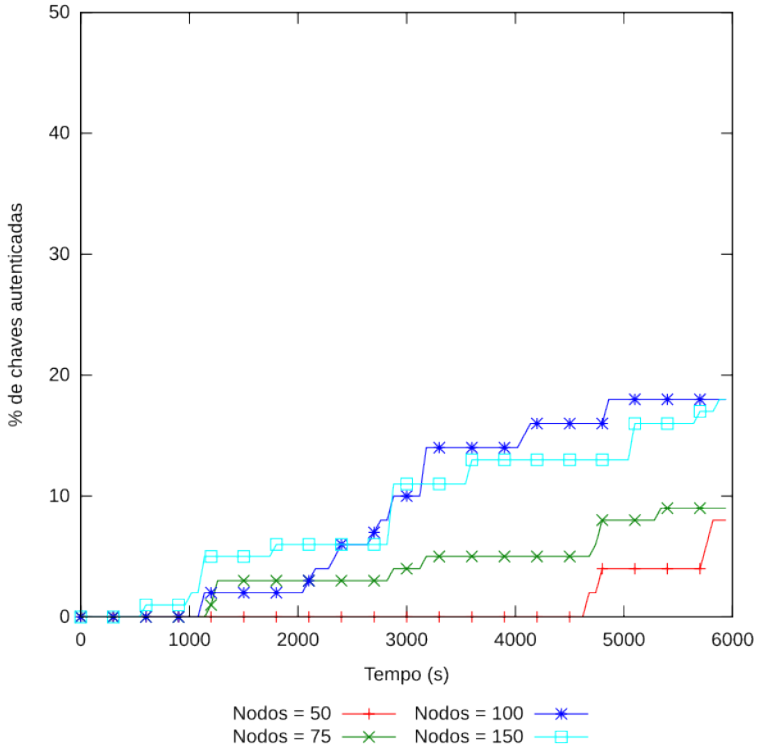



Figura 1.3: Resultado do uso do *PGP-Like* sobre DTN

## 1.1 Contextualização do Problema

Os esquemas de gerenciamento de chaves de redes Ad-Hoc não atingem a mesma eficiência quando utilizadas em DTNs ou até mesmo não funcionam. Isso se deve principalmente à possibilidade dos nodos perderem contato por tempo indeterminado com todos os nodos presentes na rede, ocasionando a seguinte situação: um nodo perde contato com a rede, mas retorna algum tempo depois e não há mais nenhum nodo de sua confiança. Fazendo com que ele não se comunique com mais ninguém por tempo indeterminado.

Para tentar solucionar os problemas de gerenciamento de chaves em redes DTNs foram propostos vários esquemas. Abaixo alguns exemplos:

- baseado em hierarquia de identidade: *Hierarchical Identity-Based Cryptography* (HIBC)[35][36];
- baseado em trocas de chaves assimétricas [13] e
- baseado em múltipla autenticação: *Opportunistic Batch Bundle Authentication* (OBBA-FAT) [37].

Esses esquemas serão detalhados no Capítulo 2. Há também alguns esquemas que são aplicados em ambientes específicos:

- voltados para *Ferry-Based Delay-Tolerant Networks* (FDTN)[38];
- voltado para DTNs semi estruturadas [39];
- voltado para comunicação veicular [40][41] e
- voltado para comunicação entre satélites [42].

Em geral, os esquemas de gerenciamento de chaves para DTN podem funcionar em redes Ad-Hoc, pois levam em consideração as características desse tipo de rede com o acréscimo da principal característica das DTNs, a tolerância a atrasos e desconexões. Ponto esse não contemplado nos esquemas voltados para redes Ad-Hoc.

Um dos principais protocolos para DTN, o *Bundle Protocol* [43][44][45][46] desenvolvido por um grupo de pesquisa do *Internet Research Task Force* (IRTF) [47], chamado *Delay Tolerant Networking Research Group* (DTNRG) [48], não tem como objetivo solucionar o problema de gerenciamento de chaves em DTNs, entretando possui segmentos de segurança em sua especificação que podem colaborar para uma rede mais segura. Desta forma, aponta-se que o esquema proposto neste trabalho pode ser usados em complemento ao *Bundle Protocol* para prover uma rede DTN mais segura. Seu detalhamento está presente no Apêndice A.

## 1.2 Objetivos e Contribuições

Esse trabalho apresenta um novo esquema de gerenciamento de chaves para DTNs baseado em cadeias de assinaturas digitais. Para a construção de uma cadeia, um nodo *x* precisa certificar outro nodo *y*, então ele emite uma mensagem cifrada com sua chave privada (assinatura digital), contendo as informações criptográficas de *y*, como identificação e chave pública. Assim que outro nodo, que possua a chave pública de *x*, receber essa mensagem, ele pode abrí-la e obter a informação que *x* garante que a chave pública presente é de *y*. Cada nodo que recebe a mensagem, a repassa cifrando-a com sua chave privada, criando assim cadeias de assinaturas. Estas cadeias não são necessariamente as rotas encontradas na camada de roteamento. Entretanto, elas podem representar possíveis rotas entre os nodos.

Este esquema deve ser capaz de se adequar aos vários cenários de utilização desse tipo de rede. E seguirá as premissas de segurança: autenticidade, confidencialidade e integridade.

Objetiva-se, também, mostrar:

- o impacto do uso desse esquema sobre o tráfego da rede;
- o tempo de convergência do esquema e as formas de minimizá-lo;

- o tamanho médio das cadeias de assinaturas digitais, e
- qual a resistência do esquema a alguns tipos ataques.

Esse trabalho apresenta as seguintes contribuições:

- proposta de um novo esquema de gerenciamento de chaves baseada no encadeamento de assinaturas digitais;
- avaliação do impacto desse esquema em um ambiente de simulação voltado para DTNs;
- uso de diversas métricas para uma melhor avaliação, e
- investigação sobre a vulnerabilidade do esquema frente a ataques.

## 1.3 Organização do Texto

Esse trabalho esta organizado em 5 capítulos. No capítulo 2 são detalhados alguns esquemas de gerenciamento de chaves para DTNs, suas principais características, vantagens e desvantagens.

No capítulo 3 é apresentado o esquema proposto de gerenciamento de chaves para DTNs baseado em cadeias de assinaturas. É apresentado o funcionamento do esquema detalhando o modelo de troca dos certificados digitais assinados por meio de cadeias, como é feito o processamento de cada cadeia e as ações tomadas para cada situação.

No capítulo 4 são apresentados os resultados das simulações em em cenários livres de atacantes e em cenário sob ataques do tipo *blackholes* e *greyholes*, *sybil* e falsificação. O ataque de falsificação em duas modalidades, ataque independente e ataque em grupo.

Em seguida, no capítulo 5, serão apresentadas as considerações finais sobre o trabalho com relação às contribuições e resultados obtidos.

Por fim, há três apêndices. O apêndice A contém uma análise do protocolo *Bundle Protocol*. No apêndices B, C e D estão os gráficos omitidos durante o capítulo 4. No apêndice B estão os gráficos para a distribuição homogênea de certificados iniciais. Os gráficos para a distribuição heterogênea são apresentados no apêndice C e no apêndice D estão os gráficos da distribuição centralizada em 10% dos nodos

# CAPÍTULO 2

# GERENCIAMENTO DE CHAVES EM REDES DTN

Esquemas de gerenciamento de chaves são conjuntos de técnicas desenvolvidas para uma administração segura das chaves criptográficas dos nodos da rede. Para que os esquemas voltados para DTNs sejam eficientes, devem levar em consideração alguns pontos, entre eles, a topologia dinâmica da rede. Desta forma, o esquema precisa ser, preferencialmente, descentralizado e auto-organizado [24] e ainda, deve levar em consideração todos os pontos já apresentados em conjunto com as principais características dessa forma de comunicação. A seguir serão detalhados os principais esquemas de gerenciamento chaves para DTNs, apresentando suas principais características, problemas e utilizações.

## 2.1 *Hierarchical Identity-Based Cryptography*

Um dos esquemas de gerenciamento de chaves para DTNs é o baseado em hierarquia de identidades/*Hierarchical Identity-Based Cryptography* (HIBC)[35][36]. Essa solução pode ser vista como uma árvore, na qual o nodo raiz é responsável por gerar a chave privada dos nodos filhos ou a chave pública de qualquer outro nodo abaixo dele. Esse nodo é chamado de provedor de chaves/*Private Key Genarator* (PKG). Afim de evitar a sobrecarga sobre um único ponto, cada nodo, que não seja folha, pode ser a raiz de uma sub-árvore, e, então, ser o provedor de chaves dos seus nodos filhos. Os nodos folha da árvore são os usuários que necessitam das chaves para cifrar suas mensagens.

Dado um nodo raiz *a*, diz-se que ele é provedor de chaves da região *A*. Dado um outro nodo *a1*, filho de *a*, diz-se que ele é provedor de chaves da sub-região *A1*, e essa é uma sub-árvore de *A*. A Figura 2.1 ilustra essa arquitetura para uma melhor compreensão.

Para que um nodo folha *x* se comunique com outro nodo qualquer *y* que esteja em uma região oposta à raiz da árvore principal, ele precisa que todos os nodos provedores estejam funcionando. Isso porque o nodo *x* cifra uma mensagem usando a chave pública do provedor de chaves da sua região, que, por sua vez, decifra a mensagem e cifra com a chave pública do próximo provedor, ocorrendo isso até o nodo raiz da árvore principal. Que recebe a mensagem, decifra e cifra com a chave do seu outro nodo filho e a entrega para ele. Seguindo esse fluxo até o destino. Na Figura 2.2 esse fluxo é exemplificado.

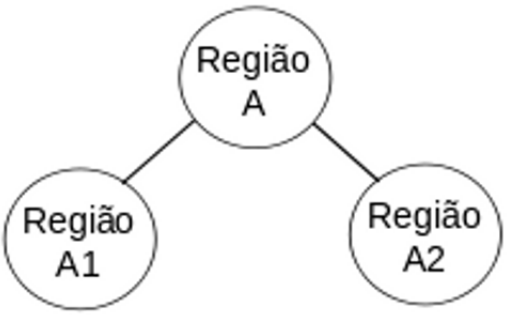



Figura 2.1: Exemplo da Estrutura do HIBC

O maior problema que o HIBC apresenta é a sua principal característica, a necessidade de os nodos comunicarem-se com seus antecessores. Outro problema evidente nesse esquema, é a necessidade do provedor de chaves precisar decifrar a mensagem para então repassá-la. Esse nodo pode ter se tornado malicioso e alterar a mensagem, fragilizando toda a estrutura de comunicação. Os nodos provedores de chaves têm acesso a toda informação que passa por eles, sendo assim, esses nodos podem efetuar um ataque simples, no qual, apenas mensagens selecionadas são repassadas a diante.

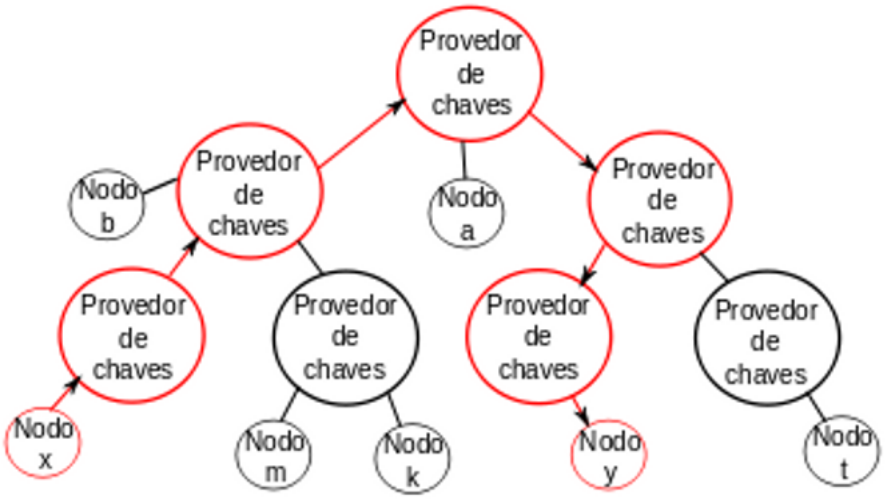



Figura 2.2: Exemplo do fluxo de uma mensagem no HIBC

## 2.2 *Opportunistic Batch Bundle Authentication*

Esse esquema representa a junção de duas funcionalidades, o OBBA responsável direto pelo gerenciamento da chaves e do FAT que minimiza a carga imposta à rede com o uso do OBBA.

### 2.2.1 OBBA

O *Opportunistic Batch Bundle Authentication* (OBBA)[37] é baseado em autenticação múltipla, ou seja, a mensagem é autenticada usando múltiplos caminhos. Ele foi estruturado sobre o protocolo *Bundle*, logo, considera os modelos de autenticação, integridade e confidencialidade presentes no protocolo.

Antes de continuar, salienta-se que o OBBA não define uma forma de distribuição e revogação de chaves, assim, ele considera a existência de um gerente de segurança externo à rede/*Offline Security Manager* (OSM). O OBBA faz da DTN um grafo direcionado, no qual as direções decidem o fluxo das mensagens. O foco da solução é impedir os seguintes ataques:

- Injetar mensagens falsas na rede;
- Tentativa de enganar outros nodos;
- Obter acesso não autorizado a recursos;
- *Denial-of-Services*/Rejeição de Serviços (DoS).

O autor enumera algumas falhas encontradas no decorrer do desenvolvimento do esquema, como por exemplo, a necessidade de minimizar custo de processamento e identificar mensagens falsas afim de rejeitá-las e filtrá-las. Indica também, que o principal custo computacional da autenticação por rajadas está em verificar e certificar todas as assinaturas de remetentes diferentes [37].

Com o objetivo de solucionar esse último problema, foi usado o algoritmo *ID-based batch signature* [49], no qual *n* assinaturas, de *n* mensagens e de *n* usuários são combinadas, gerando uma única chave, permitindo assim que o receptor verifique um conjunto de assinaturas de diferentes nodos de uma só vez. Entretanto, esse passo da combinação das assinaturas é feito antes da criação da rede.

A princípio, a metodologia adotada para o repasse de mensagens foi a inundação, ou seja, o repasse é feito para todos os vizinhos. Contudo, isso gera um alto custo de processamento para os nodos, possibilitando, também, que nodos maliciosos enviem mensagens falsas, ocasionando o uso desnecessário de espaço de armazenamento por toda a rede.

Uma alternativa é apresentada, nela cada nodo mantém duas listas, uma com as mensagens autenticadas e outra com as não autenticadas. Além da inclusão de uma função que calcula a probabilidade de uma assinatura ser falsa ou não, levando em consideração o histórico de contatos oportunísticos. Assim sendo, a detecção de nodos maliciosos não é determinística, sendo probabilística. Essa função recebe como argumento uma rajada de assinaturas, a divide e estrutura-a como uma árvore, para então realizar uma espécie de busca binária.

### 2.2.2 FAT

Para reduzir o número de requisições de assinaturas, adota-se uma abordagem de árvore de autenticação fragmentada/*Fragment Authentication Tree* (FAT)[50]. A FAT configura-se como uma árvore binária na qual as folhas são fragmentos de assinaturas e os nodos intermediários são o *hash* da composição das assinaturas dos nodos filhos. Desta forma, para se obter alguma assinatura não é necessário ter acesso a toda informação, mas, somente a parte dela presente em alguns nodos da árvore. Esse esquema é exemplificado na Figura 2.3.

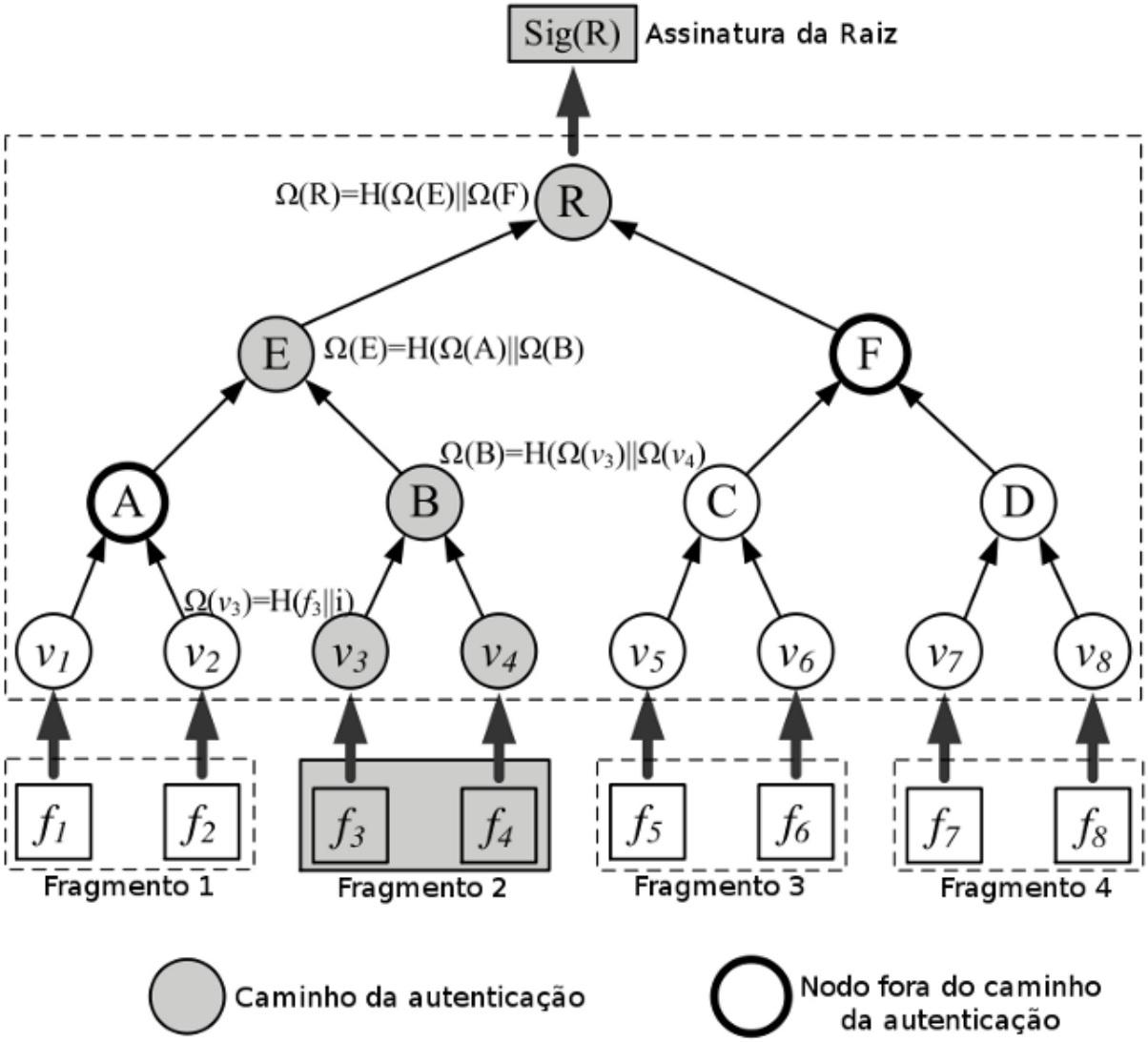



Figura 2.3: Exemplo de FAT. FONTE: [37]

Dados *n* fragmentos base $\{f_i | 1 \leq i \leq n\}$ distribuídos por *m* nodos folha $\{v_i = H(f_i \parallel i) | i = 1, ..., m\}$, o nodo origem constrói a árvore completa usando esses nodos folhas. O valor de cada árvore interna dos nodos é definida por $\Omega(V) = H(\Omega(V_{left}) \parallel$

$\Omega(V_{right})$), onde *V* denota a árvore interna do nodo e $V_{left}$ e $V_{right}$ os nodos filhos do nodo *V*.

### 2.2.3 OBBA-FAT

Apresentadas as características do esquema OBBA e FAT, o autor reuniu as duas ideias anteriores em uma só abordagem, dando origem ao OBBA-FAT. Esquema esse que visa a redução do custo de processamento e da sobrecarga da rede. Para tanto, todo nodo recebe fragmentos da árvore e reconstrói a assinatura da raiz. Se a assinatura da raiz for igual a recebida, todo o bloco recebido é autenticado. Essa junção é mostrada na Figura 2.4.

O OBBA-FAT foi simulado pelo autor usando o *The ONE*. Os resultados mostram uma superioridade desse sobre um esquema de autenticação individual baseado no ECDSA (ECDSA-IBA)[51], com relação as métricas estabelecidas: tamanho do *bundle* distribuído, custo computacional, sobrecarga da rede e consumo de energia. Note que o esquema apresentado em [51] não é voltado para redes do tipo DTN, e sim para redes ad-hoc veiculares. Considera-se esse ponto como um dos principais motivos da diferença entre os valores apontados pelo autor.

Por fim, é incorporada uma estratégia de banco de créditos chamada de SMART para estimular os nodos a repassarem mensagens quando forem intermediários. O SMART é baseado em paridade bilinear possuindo três características principais: bilinearidade, não degenerativo e computável, ou seja, há ao menos um algoritmo eficiente que compute a paridade.

O SMART é construído de forma semelhante ao FAT, baseado em árvores binárias equipadas com uma função *hash*. Assim cada fragmento pode ser validado com apenas parte da árvore.

Embora o OBBA-FAT tenha sido arquitetado para ser um esquema de gerenciamento de chaves, não há consideração alguma sobre a sua vulnerabilidade ou eficiência a ataques. Já o SMART, foi testado e é resistente a três situações: nodo insere créditos falsos, nodo remove créditos a mais e nodo recusa-se a retransmitir mensagens. Os resultados apresentados mostraram que o SMART consegue estimular a cooperação entre os nodos sem gerar sobrecarga excessiva na rede.

Aparentemente os possíveis problemas para os dois esquemas apresentados em [37] estão relacionados a sua principal característica, a estrutura de árvore binária. Pois, para que os nodos possam validar e garantir transmissões seguras, é necessário que todos os nodos da rede tenham uma árvore já construída antes da formação da rede. Em redes do tipo DTN é normal, e até mesmo esperado, que os nodos mantenham uma topologia esparsa com contatos pouco frequentes, mas esse fato parece não ter sido levado em consideração, nem o caso em que nodos entram depois

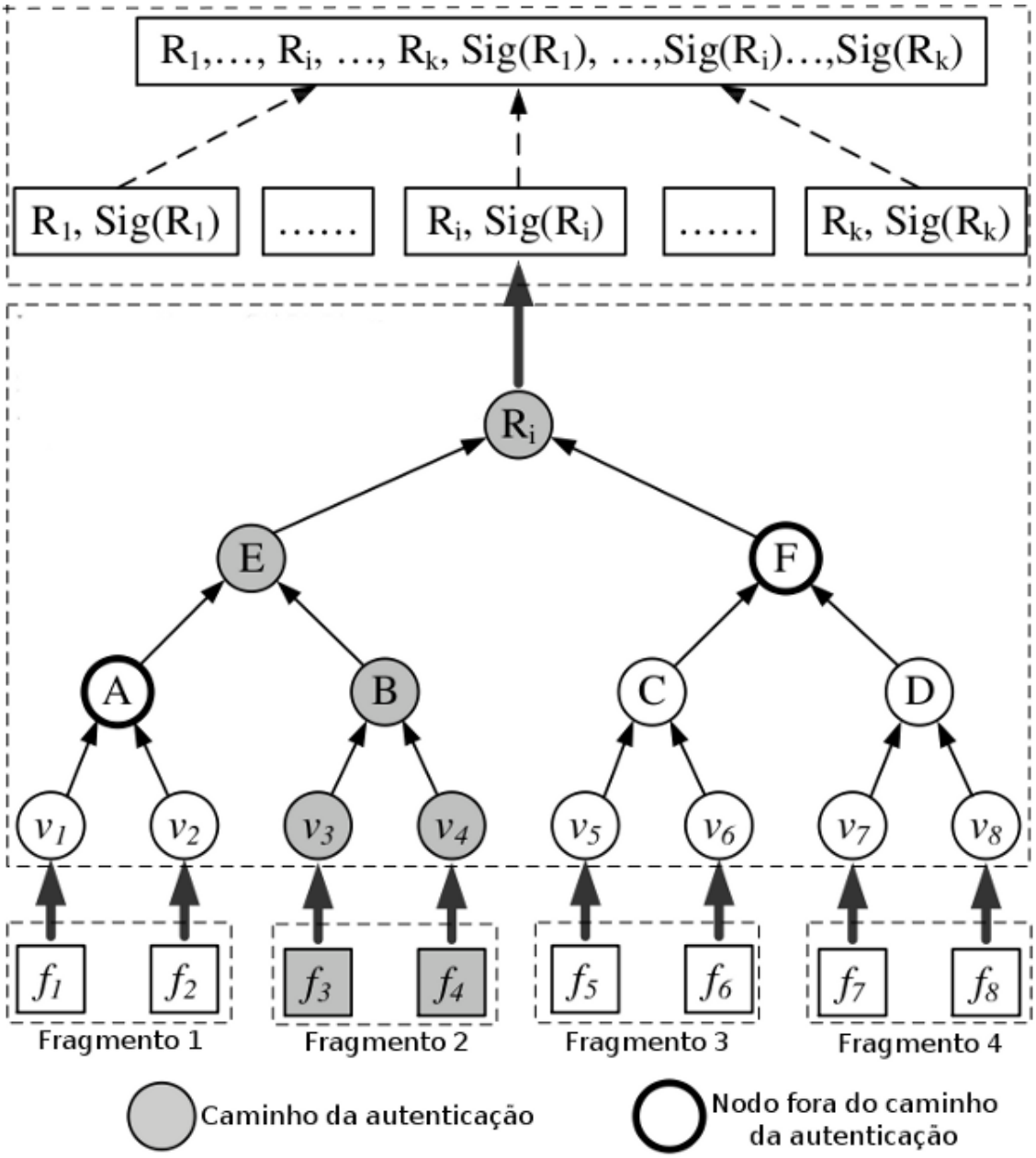



Figura 2.4: Exemplo da abordagem OBBA-FAT. FONTE: [37]

na rede ou que retornam depois de muito tempo à rede. Não fica claro também a eficiência dos esquemas no caso em que algum nodo malicioso altera a estrutura da árvore ou se há detecção de ataques como *greyholes*, *blackholes*, personificação ou virtualização.

## 2.3 Trocas de chaves Assimétricas

Dentre as soluções encontradas para o problema de gerenciamento de chaves nas DTNs, há a formulada em [13]. Nessa proposta, cada nodo tem listas para armazena-

mento de mensagens, chaves e nodos. Quando há um contato entre os nodos, essas listas são trocadas, para que assim, depois de decorrido algum tempo, todos os nodos da rede saibam quem são os participantes da rede e quais suas respectivas chaves. Uma otimização desse esquema foi proposta no mesmo trabalho, no qual os nodos só trocam listas de chaves se houver diferença entre suas listas de nodos.

Dados dois nodos quaisquer da rede, *i* e *j*, as trocas de listas acontecem da seguinte forma:

1. os nodos *i* e *j* estabelecem contato;
2. *i* envia uma mensagem para *j* contendo a sua lista de nodos conhecidos;
3. *j* verifica a lista de nodos conhecidos por *i* em busca de nodos não conhecidos por ele;
4. *j* envia uma mensagem contendo duas listas, a lista de nodos dele e uma lista de chaves públicas dos nodos conhecidos por ele, mas não por *i*;
5. *i* ao receber essa mensagem, atualiza sua lista de chaves com a lista recebida de *j*;
6. *i* verifica quais nodos estão em sua lista, mas não estão na lista de *j*;
7. *i* envia uma lista de chaves dos nodos que *j* não possui;
8. assim que *j* receber a lista de chaves de *i*, ele atualiza sua lista. Assim, ao final do processo, os dois nodos terão o mesmo conjunto de chaves.

Quando um nodo precisa enviar uma mensagem para outro, ele verifica se possui a chave pública do destino. Caso a tenha, ele então cifra a carga útil com a chave do destino, calcula o *hash* desse segmento e o cifra com sua chave privada. Por fim, adiciona a mensagem gerada em sua lista para ser enviada posteriormente. Se não possuir a chave do destino, essa mensagem é adicionada a sua lista. Ela fica nessa lista até que o nodo consiga essa chave ou acabe o tempo de espera. O algoritmo usado para a criptografia e o RSA e para calcular o *hash* é o SHA256.

Como as mensagens são armazenadas de forma persistente pelos nodos, todas as mensagens recebidas por eles chegam até, pelo menos, à camada de agregação. Elas podem ser classificadas em três tipos: lista de nodos, lista de chaves e dados. Ao receber uma mensagem, o nodo verifica qual a tipificação, caso seja alguma das listas, procede como mencionado anteriormente. Se a mensagem for de dados, o nodo valida a autenticidade e a integridade dela, apenas se possuir a chave da origem. Visto que a mensagem está correta, sendo ele o destino, tenta decifrá-la, e obtendo sucesso usa os dados, caso contrário, a descarta. Uma vez que a autenticidade ou a

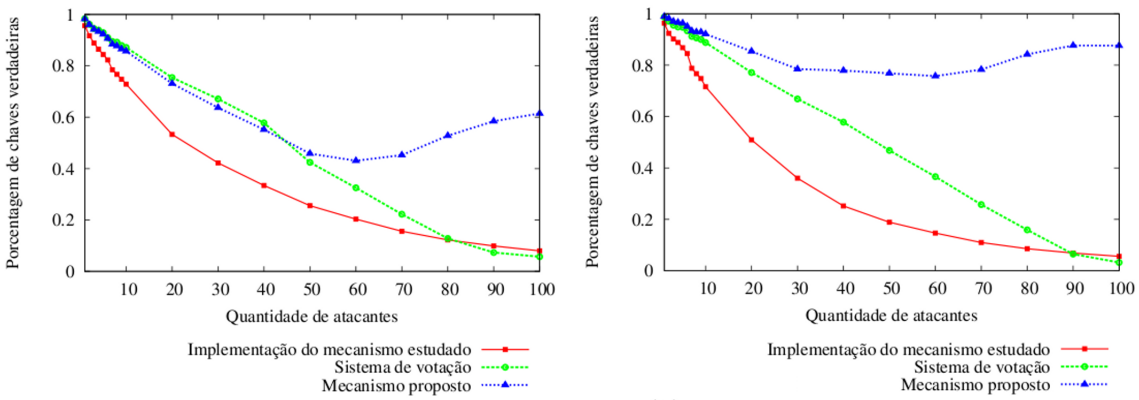
integridade não estiverem corretas, a mensagem também é descartada. Se por acaso o nodo não for o destino, a mensagem é armazenada na lista para repasse futuro.

O esquema foi implementado e foram feitas simulações no *The Opportunistic Network Environment Simulator* (The ONE)[52]. Mais detalhes sobre esse simulador serão apresentados no Capítulo 4. Nos cenários propostos e nas métricas verificas pelo autor (probabilidade de entrega, atraso médio, sobrecarga da rede, sobrecarga de segurança e porcentagem de mensagens não repassadas devido a falta de chave no nodo de origem), esse esquema de segurança não causou uma grande sobrecarga no desempenho da rede, quando comparado com a rede sem o esquema de segurança.

Todavia, esse esquema possui falhas de segurança. Como os nodos trocam suas chaves públicas, nodos maliciosos podem alterar as chaves de alguns, interferindo de forma direta na correspondência nodo-chave. Isso pode acarretar vários problemas, como: o aumento no tempo de convergência do esquema, impedimento que nodos se comuniquem, criação de falsos indicativos de nodos maliciosos, entre outros.

Esse problema foi minimizado em [53], no qual foi proposto um sistema de votação ponderado, baseado em comunicações diretas e no histórico de contatos aplicado sobre [13]. As simulações foram feitas usando o *The ONE* assim como no modelo original.

Abaixo alguns resultados obtidos com essa melhoria, nos quais pode-se notar uma melhoria relevante nos resultados obtidos. Em um cenário nos quais metade dos nodos é atacante o percentual de chaves verdadeiras é 20% maior que no esquema original, Figura 2.5(a). Já em cenários de alta conectividade Figura 2.5(b) o ganho é de mais de 80%.




(a) Raio de transmissão 50 metros (b) Raio de transmissão 100 metros

Figura 2.5: Resultados obtidos pelo Sistema de Votação Ponderado. FONTE: [53]

Os resultados demonstraram a fragilidade do esquema de trocas de chaves ao ataque no qual nodos maliciosos espalham chaves falsas pela rede. Destaca-se que o

trabalho não levou em consideração ataques cooperativos, nos quais nodos falsificam as chaves de forma conjunta e do mesmo modo e, ataques de personificação ou virtualização, nos quais os nodos maliciosos se identificam como outros nodos ou criam nodos virtuais, respectivamente, afim de interferir em rotas ou acessar dados de forma ilícita.

Mostrou-se nesse capítulo alguns esquemas de gerenciamento de chaves para DTNs encontrados. Foram apresentadas as características mais marcantes de cada um, apontando as possíveis falhas. A seguir, será detalhado o esquema proposto neste trabalho. Esquema esse que usará criptografia assimétrica para cifrar cadeias de assinaturas digitais, não usando qualquer estrutura hierarquica na criação das cadeias. Dessa forma o esquema diferencia-se dos apresentados, pois entende-se que o uso de árvores pode limitar ou prejudicar diretamente a DTN, devido a sua estrutura que tende a ser estática, e que a troca direta de chaves pode facilitar a ação de nodos maliciosos.

# CAPÍTULO 3

# ESQUEMA DE GERENCIAMENTO DE CHAVES USANDO CADEIAS DE ASSINATURAS EM REDES TOLERANTES A ATRASOS E DESCONEXÕES

Esse capítulo apresenta um novo esquema de gerenciamento de chaves voltado para DTNs baseado no encadeamento de assinaturas digitais. As próximas seções mostram as características e o funcionamento desse esquema.

## 3.1 Visão Geral

No início da rede, cada nodo possui um identificador único e gera seu próprio par de chaves pública/privada. Para que o esquema funcione corretamente, considera-se que os algoritmos de criptografia e de assinatura digital sejam o mesmo. Assim segundo [22], recomenda-se o uso dos algoritmos RSA, ElGamal ou Rabin, pois eles trabalham bem em ambas as situações, embora sejam lentos. A confiabilidade nas chaves e assinaturas é diretamente ligada ao algoritmo usado para criá-las e na forma como cada nodo mantém suas chaves.

Considera-se ainda, que os nodos possuem de forma segura a chave pública de alguns outros nodos. Essas chaves podem ser obtidas através de escolhas aleatórias, usando Group Diffie Hellman (GDH) [54], troca anterior à construção da rede, entre outros. Para repassar essa informação, ela é cifrada com sua chave privada, assim, certificando-a. Quando outro nodo recebe essa mensagem cifrada, ele armazena-a e repassa cifrando-a. Os outros nodos seguem esse mesmo passo, criando assim uma cadeia de assinaturas. O esquema é ilustrado na Figura 3.1.

Para aumentar a segurança, pode-se acrescentar um módulo de confiança que auxilie na decisão de repasse das mensagens. Desta forma, os nodos repassariam apenas as mensagens dos nodos em que eles confiassem. Entretanto, esse módulo não foi implementado nesse trabalho e é apontado como um trabalho futuro.

Cada nodo possui um lista para cadeias de assinaturas digitais, cujas posições são indexadas pelo identificador dos outros nodos da rede, aqui chamada de “Lista de Cadeias”. Cada posição pode possuir uma única entrada ou uma lista de cadeias de assinaturas. As chaves públicas que cada nodo possui no princípio da rede, compõe também o início lista de cadeias e representam uma cadeia de um salto entre origem e destino.

Depois de decorrido um determinado intervalo de tempo, os nodos enviam para

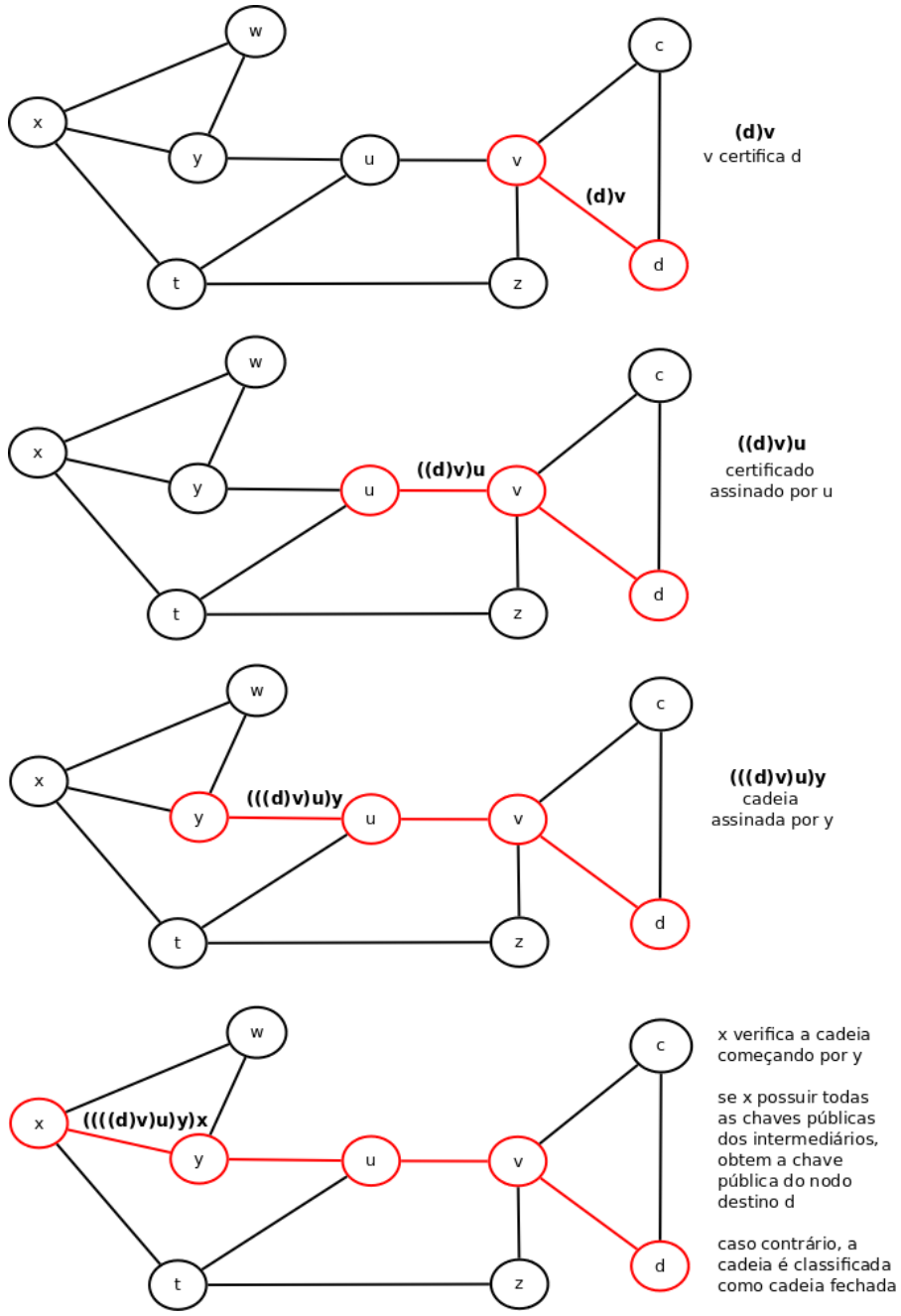



Figura 3.1: Exemplo de encadeamento de assinaturas

seus vizinhos físicos uma mensagem contendo sua Lista de Cadeias juntamente com a identificação do destino de cada cadeia. Cada cadeia presente nessa mensagem é cifrada individualmente a cada salto. Desta forma, os nodos que recebem a mensagem sabem quem foi o último a assinar a cadeia e quem é o destino da cadeia, entretanto não há a informação de quantos saltos formam-na. Essas mensagens são enviadas periodicamente e não há a necessidade de resposta.

As cadeias podem ser classificadas em dois tipos: cadeias abertas e cadeias fechadas. Cadeias abertas são aquelas que o nodo conseguiu verificar todas as assina-

turas e obter a chave pública do nodo destino. As cadeias fechadas são aquelas nas quais o nodo não conseguiu validar alguma assinatura por falta da chave pública de um nodo qualquer da cadeia. Explicita-se que o estado de cadeia aberta ou fechada é relativo a cada nodo, ou seja, uma cadeia aberta para um nodo não necessariamente é aberta para outro nodo.

A seguir, um exemplo da diferença entre cadeias abertas e fechadas para nodos diferentes: o nodo *x* possui a cadeia aberta $(((d)_v)_u)_y$ até o nodo *d*, ou seja, *x* possui as chaves públicas dos nodos *y, u, v* e, conseguentemente, de *d*. Ao repassar essa cadeia para *z*, ele a envia cifrada com sua chave privada. O nodo *z* recebe a cadeia $((((d)_v)_u)_y)_x$ como uma cadeia fechada, dando início ao processo de validação das assinaturas. Essa cadeia será classificada como cadeia aberta apenas se o nodo *z* tiver as chaves públicas dos nodos *x, y, u* e *v*. Caso contrário, ela permanecerá como uma cadeia fechada até o recebimento das chaves públicas necessárias para finalizar esse processo de validação. Somente ao final do processo, o nodo *z* terá acesso à chave pública do nodo *d*.

O espaço ocupado em memória e a quantidade de cadeias em cada posição desta lista são limitados para que um mesmo destino não ocupe todo o espaço disponível. Ao atingir o máximo de espaço ou o limite de cadeias em uma posição, as novas cadeias que são verificadas como fechadas são descartadas, mantendo-se apenas as presentes anteriormente.

## 3.2 Distribuição e armazenamento das chaves

Um nodo *x* ao receber uma mensagem contendo a Lista de Cadeias de outro nodo qualquer *y*, seleciona a primeira cadeia e tenta decifrá-la nível a nível, começando por *y* até conseguir obter a chave pública do nodo destino. Isso esta ilustrado na Figura 3.2.

Se *x* fracassar em qualquer que seja o ponto da cadeia, ele a classifica como cadeia fechada, e em seguida, verifica a existência de alguma entrada em sua lista de cadeias para o nodo destino da cadeia recebida. Havendo essa entrada, se a cadeia for fechada, ele insere a nova cadeia na lista, mantendo assim as duas cadeias fechadas. Caso contrário, a cadeia recebida é descartada, pois já há uma cadeia aberta para esse destino. Contudo, se *x* conseguir abrir a cadeia e já existir uma aberta em sua lista, é necessário decidir qual cadeia será mantida. A regra aplicada nesse ponto refere-se apenas ao tamanho da cadeia, ou seja, por quantos saltos ela passou até chegar à *x*. Assim, a menor cadeia aberta é mantida e a maior descartada. Essa decisão pode ser considerada frágil e passível de fraude, indicando um ponto de análise futuro. Se *x* conseguir abrir a cadeia e já existirem cadeias fechadas para o destino,

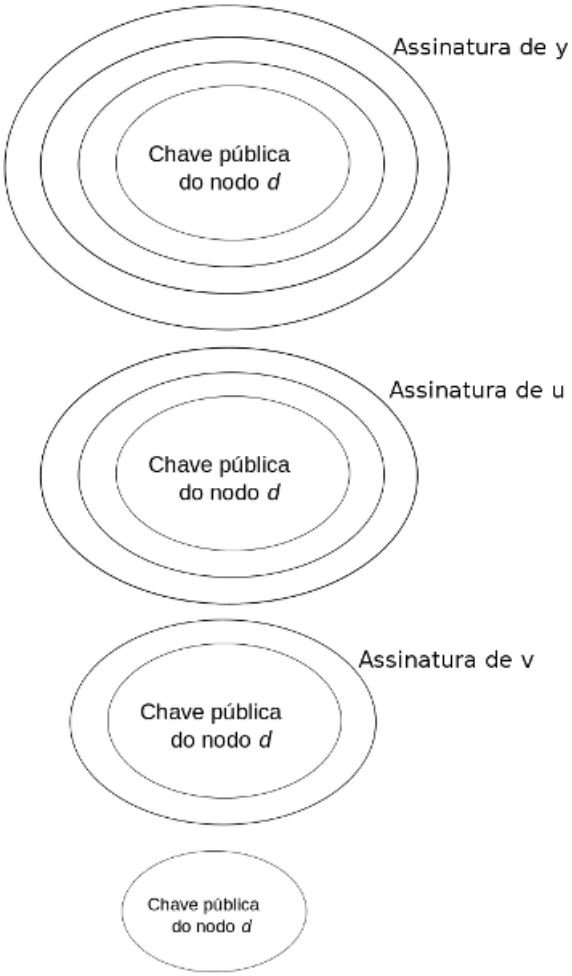



Figura 3.2: Exemplo de abertura de cadeia

todas as fechadas são descartadas e somente a cadeia aberta é adicionada na lista. Logo, todo nodo mantém em cada posição da lista de cadeias diversas cadeias fechadas ou somente uma cadeia aberta para aquele destino. O fluxograma da Figura 3.3 apresenta os passos acima descritos.

Cadeias fechadas podem possuir circularidade de assinaturas, pois se o um nodo não conseguiu abrir a cadeia completamente por falta de uma chave qualquer, o restante da cadeia e o seu tamanho continuam desconhecidos para ele. Desta forma, uma cadeia pode ser assinada inúmeras vezes pelo mesmo nodo sem que ele saiba. Isso acarreta um problema quando o número de certificados iniciais na rede toda é muito pequeno. Nesses casos, a circularidade pode gerar cadeias imensas elevando o número de cadeias fechadas armazendas de forma exponencial.

Essa situação pode ser ilustrada em um cenário em que haja 10 nodos vizinhos que não possuam certificados iniciais entre eles. No primeiro repasse, cada nodo obtem o certificado inicial dos outros 9 vizinhos e classifica todos como cadeias fechadas. No segundo repasse, cada nodo envia sua lista, que possui 10 cadeias. Cada nodo

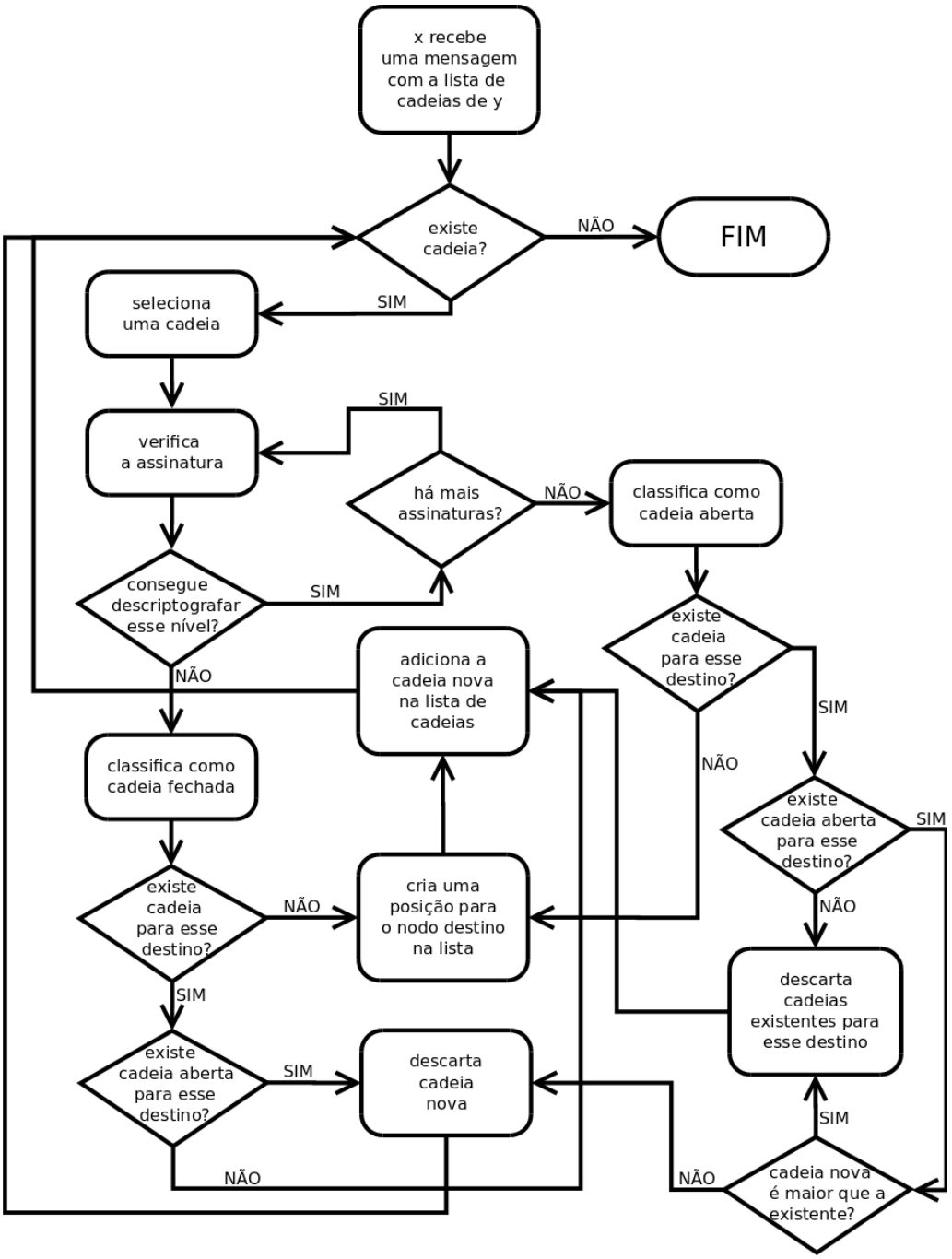



Figura 3.3: Fluxograma da recepção de mensagens

recebe esses 10 certificados dos 9 vizinhos, totalizando em sua lista 100 certificados, pois são 90 novos mais 10 anteriores. No terceiro repasse, cada um desses nodos recebe uma lista de 100 certificados de cada vizinho, totalizando 1000 cadeias em apenas 3 rodadas de repasse.

Outra situação possível é o armazenamento de cadeias equivalentes. Pois, se o nodo não consegue abrir a cadeia, ela pode ser identica a uma outra fechada já existente em sua lista. Isso pode se repetir inúmeras vezes.

Sobre o tamanho das cadeias, que mostra-se um dos limites do esquema, é possível analisar a quantidade de espaço ocupado para o armazenamento delas. Considerando-se por exemplo, o algoritmo RSA com chaves públicas de 512 bits e identificador de nodo com 32 bits, pode-se inferir que cada certificado emitido possui cerca de 566 bits (chave pública + id da origem + id do nodo certificante) e cada cadeia assinada digitalmente no decorrer da rede acrescenta apenas o id do emitente.

Desta forma, no início da rede, o espaço ocupado (s) será expresso pela expressão $s = 566 * C_i$, onde $C_i$ representa o número de certificados iniciais. No caso em que cada nodo possui 20 certificados iniciais, o espaço ocupado no início da rede será de 11320 bits, ou seja, pouco mais, de 1 KByte. No decorrer do funcionamento do algoritmo, cada nodo pode possuir um número variável de cadeias de diversos tamanhos, desta forma, o espaço ocupado por elas é representado pela expressão $s = \sum_{i=1}^{T} Ca_i$, onde $T$ é o total de cadeias do nodo e $Ca_i$ o tamanho de cada cadeia.

## 3.3 Revogação e atualização das chaves

Durante a vida da rede, nenhum nodo tem autonomia para revogar ou atualizar a chave de outro nodo. Desta forma, se o par de chaves do nodo *x* irá expirar, ele apenas envia pela rede uma mensagem contendo sua nova chave pública, mas cifrada com sua chave privada atual. Assim os nodos que possuiam a chave pública do nodo *x* podem atualizar suas listas com a nova chave de *x*.

Essa metodologia pode não ser eficaz caso os nodos não repassem essa informação, mas mostra-se a seguir, que o impacto de ataques como *grey hole* e *black hole* dependendo de sua escala não causam grandes efeitos sobre o esquema.

Ataques como falsificação e personificação só são possíveis se o nodo malicioso possuir a chave privada do nodo que atualiza sua chave, pois a mensagem é cifrada com a chave privada, e essa deveria ser restrita a cada nodo. Caso seja um ataque múltiplo usando essas duas técnicas, ou seja, um nodo se passa por outro e repassa mensagens usando uma outra chave em sua posse, a decisão de repasse está no nodo que possuir as duas chaves diferentes para o mesmo nodo. Decidiu-se por fazer com que os nodos deixem de repassar as duas ou mais chaves diferentes que apontem para um mesmo nodo, até que ele encontre com o nodo origem da chave, assim ele decidirá qual a chave é a verdadeira e então voltará a repassar cadeias para esse destino.

## 3.4 Otimização do modelo de validação de cadeias fechadas

A fim de reduzir o tempo que uma cadeia permance fechada para um nodo, foi feita uma mudança no passo seguinte ao recebimento das cadeias. Ao receber uma cadeia, o nodo verifica se possui todas as chaves públicas necessárias para poder torna-la uma cadeia aberta. Se obtiver sucesso, ele obtém a chave pública presente na cadeia que pode ser um nodo ainda desconhecido. Se isso se confirmar, o nodo percorre sua lista de cadeias em busca de cadeias fechadas que dependam da chave descoberta. Assim que encontra uma cadeia fechada que pode ser aberta com essa chave, o nodo valida o restante das chaves necessárias para torná-la uma cadeia aberta, reiniciando os passos descritos. Essa alteração pode ser melhor compreendida por meio do fluxograma da Figura 3.4.

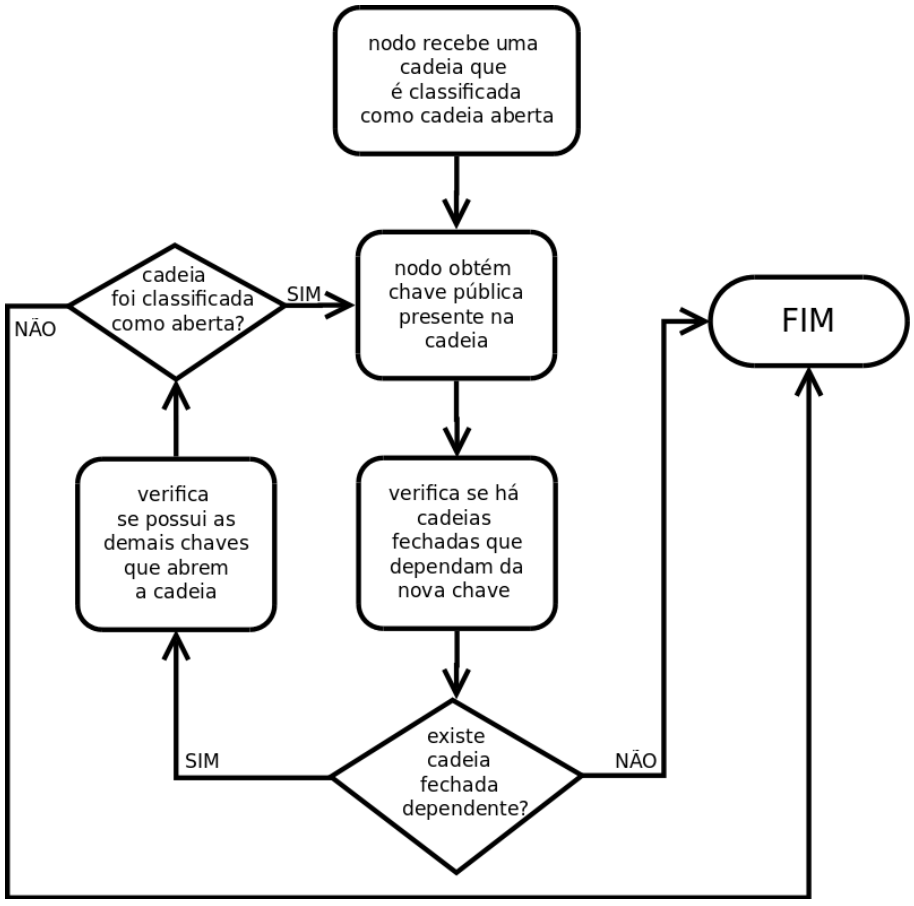



Figura 3.4: Fluxograma do modelo otimizado de validação de cadeias fechadas

Com essa mudança, é possível que uma cadeia recebida seja a responsável pela abertura de todas, ou grande parte, das cadeias fechadas armazenadas. Desta forma, o espaço usado é reduzido drasticamente, pois o nodo mantém apenas as cadeias fechadas que não possui condições de abrir até aquele momento.

# CAPÍTULO 4

# SIMULAÇÕES E RESULTADOS

Esse capítulo apresenta as simulações realizadas e seus resultados. As simulações desse trabalho foram feitas usando o *The ONE*[52]. Esse simulador foi desenvolvido pelo *Networking Laboratory da Helsinki University of Technology*, para estudo de mobilidade em DTNs. A versão utilizada foi a 1.4.1. A escolha por esse simulador foi feita em virtude do crescente número de trabalhos publicados que o utilizam.

O *The ONE* é desenvolvido na linguagem JAVA e é estruturado de forma modular. Possui implementação pronta de alguns protocolos de roteamento para DTNs, mapas de cidades como Nova Iorque e de Helsinki para o deslocamento dos nodos e permite de forma fácil a implementação de novos módulos e aplicações.

Para a criação do esquema foram alterados os módulos que definem os nodos e as mensagens. O módulo de nodos foi alterado para a inclusão do tratamento das filas e para a criação das chaves. O módulo das mensagens foi alterado para permitir que as mensagens sejam cifradas no momento de sua criação. Foram adicionados alguns módulos novos responsáveis pela definição da fila de cadeias e da estruturação de cadeias.

Nas simulações feitas foi validado se o esquema consegue convergir para o ponto em que todos os nodos possuem todas as chaves da rede, o tamanho médio das cadeias abertas e a média do número de cadeias armazenadas durante a simulação.

## 4.1 Parâmetros de Simulação

As simulações foram feitas usando o mapa da cidade de Helsinki presente no simulador que possui dimensões de 4500 metros de largura por 3400 metros de altura. Os nodos podem apenas se movimentar pelas vias definidas pelo mapa, não podendo atravessar um campo aberto, por exemplo. A movimentação empregada é igual para todos os nodos e funciona da seguinte maneira: o nodo define um ponto de interesse diferente do atual de forma aleatória; traça o menor caminho até ele usando o algoritmo de Dijkstra; segue até o ponto; chegando lá, repete os passos anteriores. A velocidade de deslocamento é aleatoriamente variada em um intervalo de 5 m/s a 20 m/s.

No cenário podem haver 50, 75, 100 ou 150 nodos distribuídos de forma aleatória. O raio e a velocidade de transmissão são 100 metros e 2 Mbps, respectivamente. Cada nodo pode armazenar no máximo 5M em seu *buffer* de mensagens. O proto-

colo de roteamento utilizado foi o Epidêmico[55], no qual o roteamento é definido pela movimentação dos nodos. Isso acontece porque sempre que há contato entre os nodos, eles trocam copias das mensagens presentes em suas listas. Desta forma cada mensagem segue por diversos nodos até seu destino, aumentando a possibilidade de sucesso na entrega. Nas simulações iniciais foram aplicados os protocolos *Spray and Wait*[56] e PROPHET (*Probabilistic Routing Protocol using History of Encounters and Transitivity*)[57], mas os resultados foram praticamente idênticos, com uma diferença média no tempo de distribuição das cadeias inferior a 1%. Desta forma optou-se por simular o restante apenas o protocolo epidêmico.

Foram utlizados três formas de distribuição dos certificados iniciais. No primeiro método, todo nodo possui a mesma quantidade inicial de chaves públicas de outros nodos da rede. Para obter essa quantidade, utilizou-se o sorteio de $x$ vezes o número de nodos presentes no início da rede, sendo que os valores para $x$ usados foram 3, 5, 7, 10 e 20. No segundo método a distribuição dos certificados foi heterogênea, ou seja, cada nodo poderia ter uma quantidade aleatória de certificados iniciais, entretanto a quantidade total de certificados ainda totaliza $x$ vezes o número de nodos presentes no início da rede, para os mesmo valores de $x$. No terceiro e último método utilizado, os certificados ficam mais centralizados em 10% dos nodos da rede. Por exemplo, em uma rede com 150 nodos e 10 certificados iniciais por nodo como parâmetro, 135 nodos iniciam a rede com o 3 certificados (mínimo de certificados analisados nas simulações) e os demais 15 nodos com o restante (73 certificados por nodo).

Cada simulação possui 6000 segundos e a cada 10 segundos os nodos enviam para seus vizinhos físicos suas listas de cadeias. Cada rodada de simulações é repetida 30 vezes para então se retirar a média. A Tabela 4.1 contém os parâmetros usados nas simulações.

Explicita-se que o objetivo deste trabalho nao é validar ou analisar o envio de mensagens de dados ocorridos entre os nodos, mas somente a troca de chaves públicas através do envio de cadeias.

| **Parâmetro** | **Valor** |
|---|---|
| Cenário | Mapa de Helsinki |
| Tamanho do cenário | 4500x3400 m |
| Tempo de simulação | 6000 s |
| Quantidade de nodos | 50, 75, 100,150 |
| Raio de transmissão | 100 m |
| Protocolo de roteamento | Epidêmico |
| Modelo de movimentação | Menor caminho usando Dijkstra |
| Velocidade mínima dos nodos | 5 m/s |
| Velocidade máxima dos nodos | 20 m/s |
| Velocidade de transmissão | 2 Mbps |
| Repetição de uma rodada de simulação | 30 |
| Intervalo entre envio da fila de cadeias | 10 s |
| Quantidade de certificados iniciais total | 3, 5, 7, 10 e 20 vezes o número de nodos |
| Tamanho do *buffer* dos nodos | 5 MB. |

Tabela 4.1: Parâmetros de simulação.

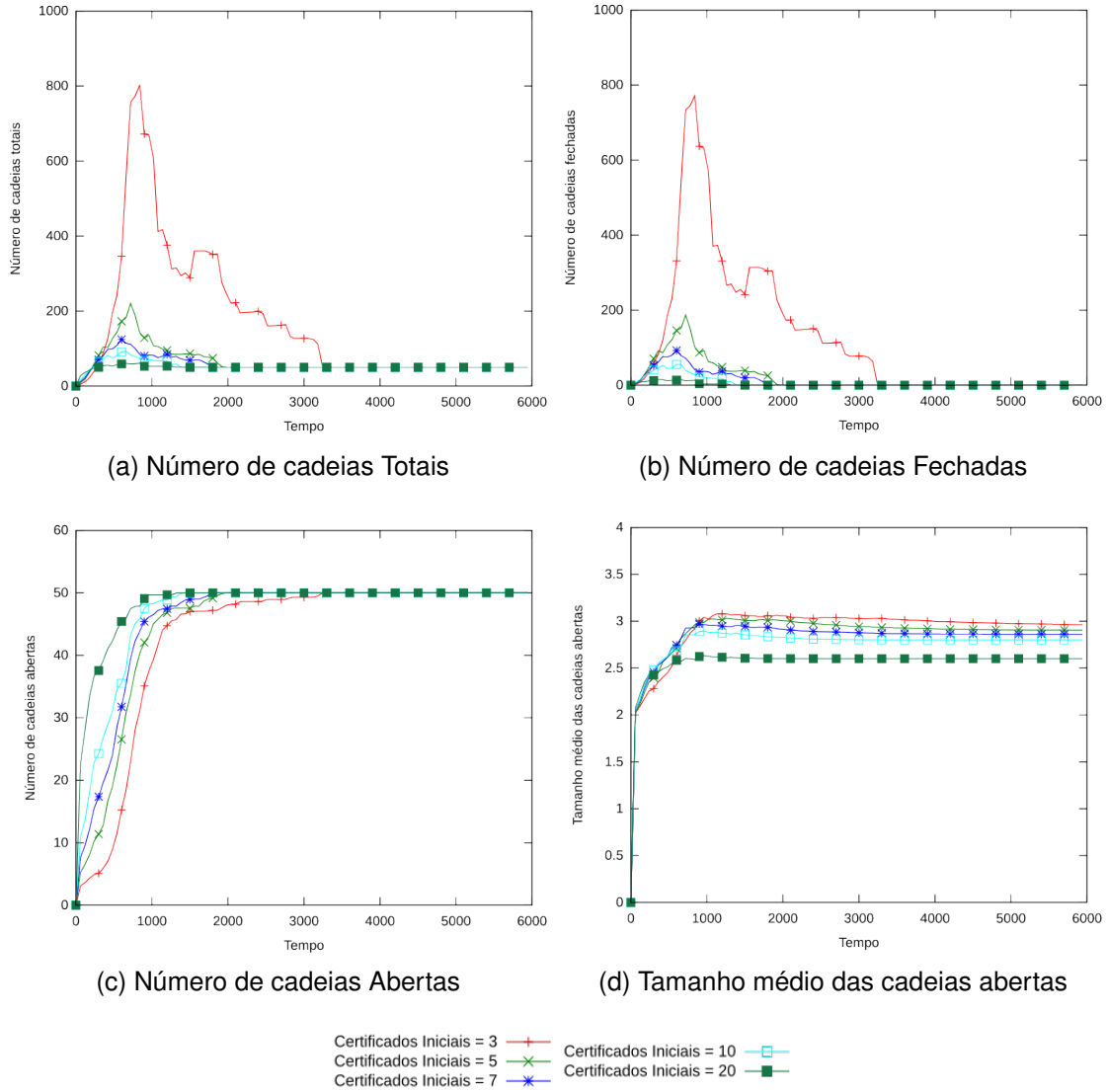
## 4.2 Resultados - Distribuição homogênea de certificados iniciais

A seguir são apresentados os resultados obtidos para distribuição homogênea de certificados iniciais. Os gráficos apresentados são apenas para 50 e 150 nodos, os demais estão presentes no Apêndice B.

### 4.2.1 Simulações Iniciais

Na Figura 4.1 podem ser observados os resultados obtidos nas simulações para os parâmetros mencionados utilizando o esquema para 50 nodos. Na Figura 4.1(a) são apresentados os valores médios para o número total de cadeias armazenadas pelos nodos no decorrer das simulações. Na Figura 4.1(b) e 4.1(c) estão a quantidade de cadeias fechadas e abertas, respectivamente, durante o tempo de simulação. Nota-se ao comparar essas duas figuras, que a grande maioria das cadeias armazenadas é fechada, isso acontece devido a regra de manter apenas uma cadeia aberta ou todas as fechadas que são recebidas.

Pode-se notar também que o esquema proposto consegue convergir para o ponto em que todos os nodos possuem cadeias abertas para todos os outros nodos da rede. Ele levou cerca de 2000 segundos para atingir o ponto de convergência total nas simulações com mais de 3 certificados iniciais e quase 3000 segundos quando a quantidade era 3. Nota-se assim que o número de certificados iniciais impacta o resultado quando seu número é baixo. Essa situação é esperada, pois quanto menos informação inicial, mais mensagens ou um tempo mais longo para que todos




(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias abertas

Figura 4.1: Resultados iniciais para 50 nodos

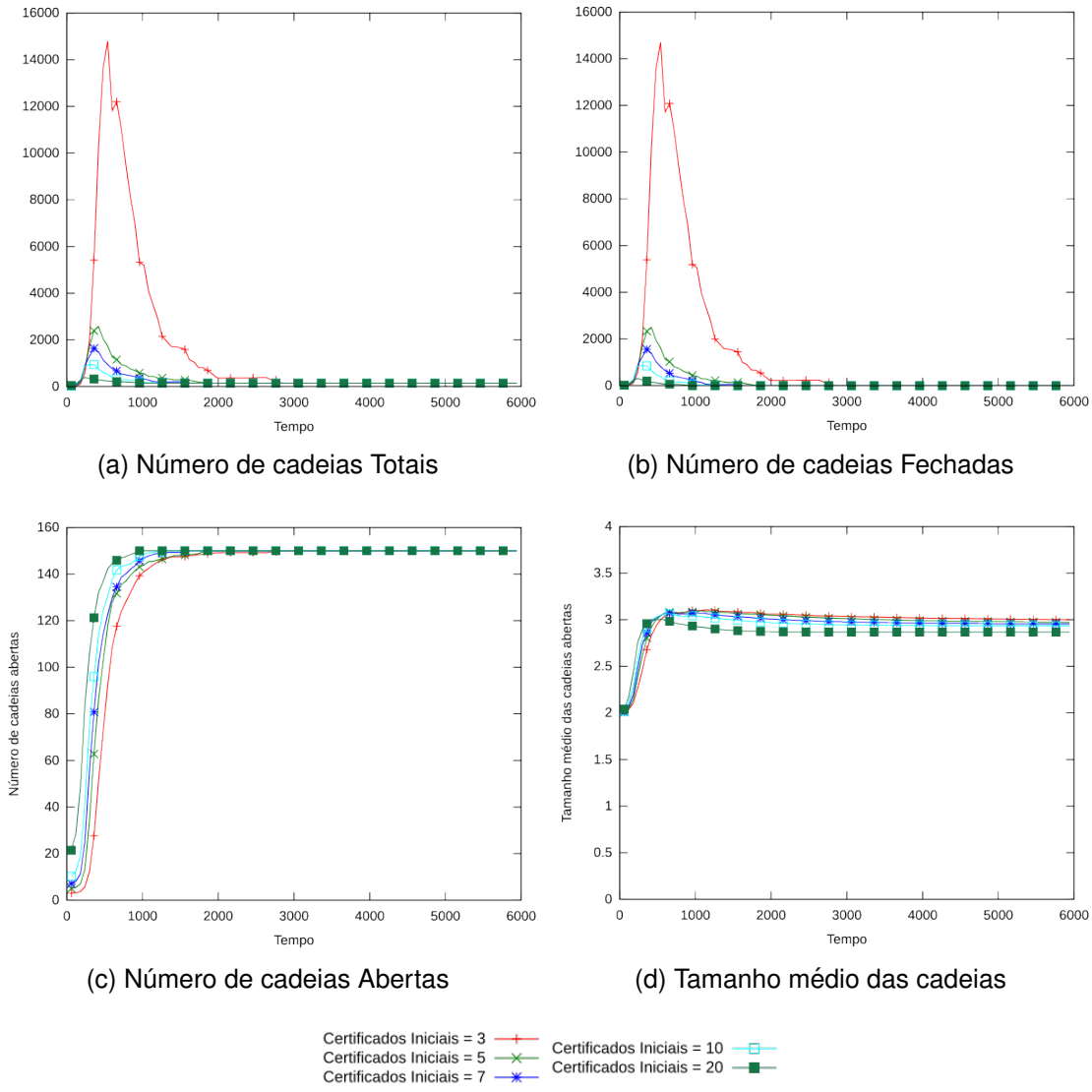
obtenham-nas são necessários.

A Figura 4.1(d) apresenta o tamanho médio das cadeias abertas armazenadas. No início das simulações o tamanho médio é zero, mas depois que cada nodo recebe suas chaves iniciais o tamanho médio salta para 2. Esse valor sofre mudanças durante o período no qual os nodos ainda não possuem todas as chaves da rede mas estabiliza-se próximo de 3. Isso indica que em média, os nodos são alcançaveis com apenas um intermediário.

Na Figura 4.2 podem ser observados os resultados para as simulações com 150 nodos. Evidencia-se que o tempo de convergência sofre pouca alteração e que o maior impacto está na quantidade de cadeias fechadas, Figura 4.2(b), armazenadas durante esse período, e consequentemente, aumentando a quantidade de cadeias totais, Figura 4.2(a). A quantidade de cadeias abertas, Figura 4.2(c), obteve uma

curva similar a encontrada com menos nodos. Já na Figura 4.2(d), nota-se que o tamanho médio das cadeias não sofreu uma grande mudança mesmo o número de nodos sendo triplicados, mostrando uma independência desse valor com relação ao número de nodos e de certificados iniciais.

Com relação aos limites de armazenamento e processamento dos nodos, no pico de armazenamento de cadeias com 150 nodos, cada nodo utilizou no máximo 60% do espaço disponível para guardar as cadeias. Já o processamento foi pouco afetado, pois os nodos liberam a memória ocupada pelas cadeias fechadas por um período de cerca de 500 segundos, assim, não gerou-se sobrecarga para o processador.




(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

(c) Número de cadeias Abertas

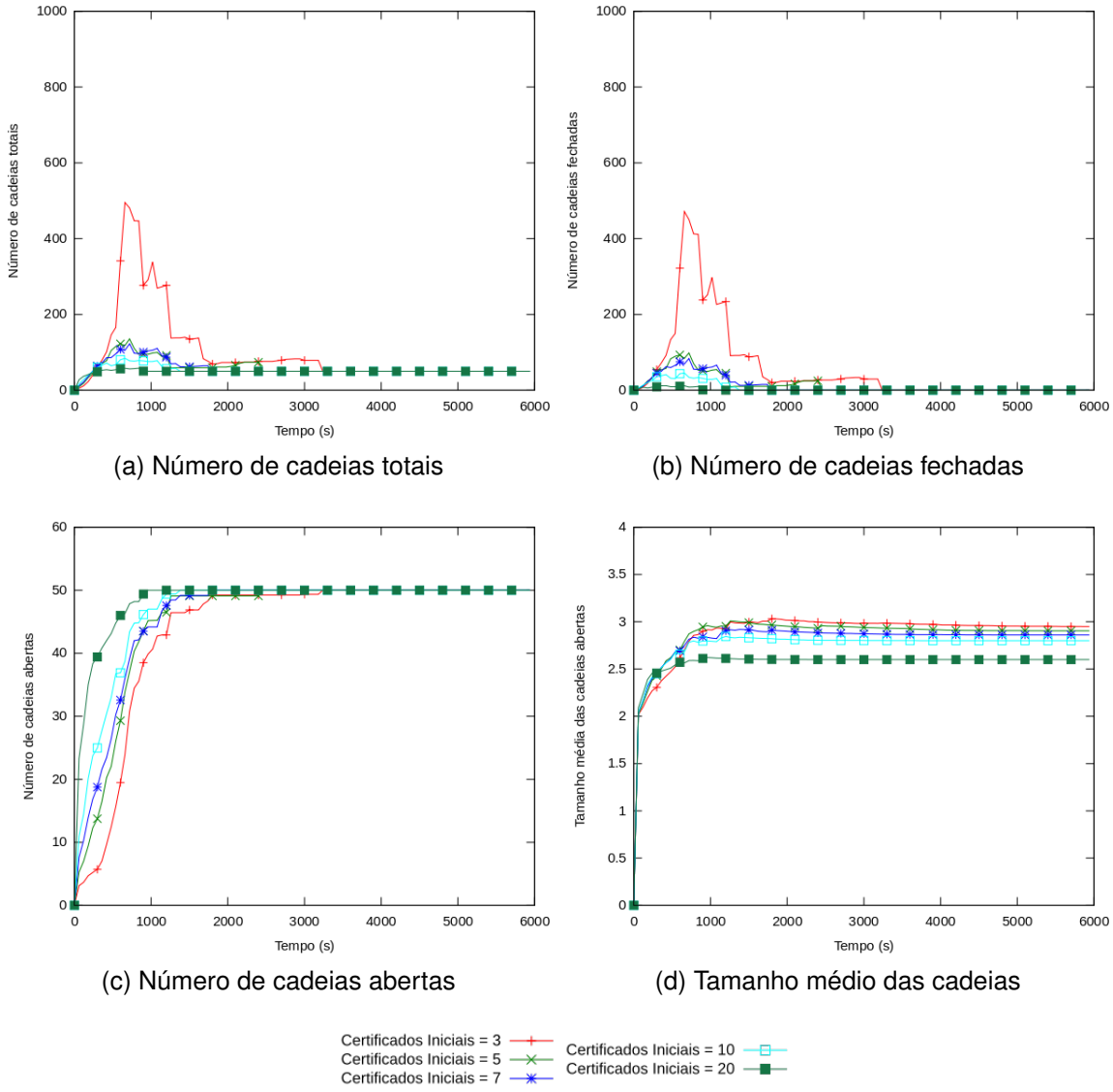
(d) Tamanho médio das cadeias

Figura 4.2: Resultados iniciais para 150 nodos

Um ponto problemático que deve ser salientado é a quantidade de cadeias totais. Tendencialmente, com mais nodos na rede, mais cadeias fechadas são trocadas e consequentemente armazenadas. No cenário com 150 nodos, esse valor chegou

próximo a 15000 cadeias para a quantidade certificados iniciais ($C_i$) igual a 3. Tendo em vista esse problema, buscou-se otimizar a transferência de informação entre os nodos, alterando o modelo de validação de cadeias fechadas. Essa alteração foi explicitada no capítulo 3.

Para essas alterações foram feitas novas simulações considerando os mesmos parâmetros já citados e obteve-se os resultados apresentados nas Figuras 4.3 e 4.4, para 50 e 150 nodos, respectivamente.




(a) Número de cadeias totais

(b) Número de cadeias fechadas

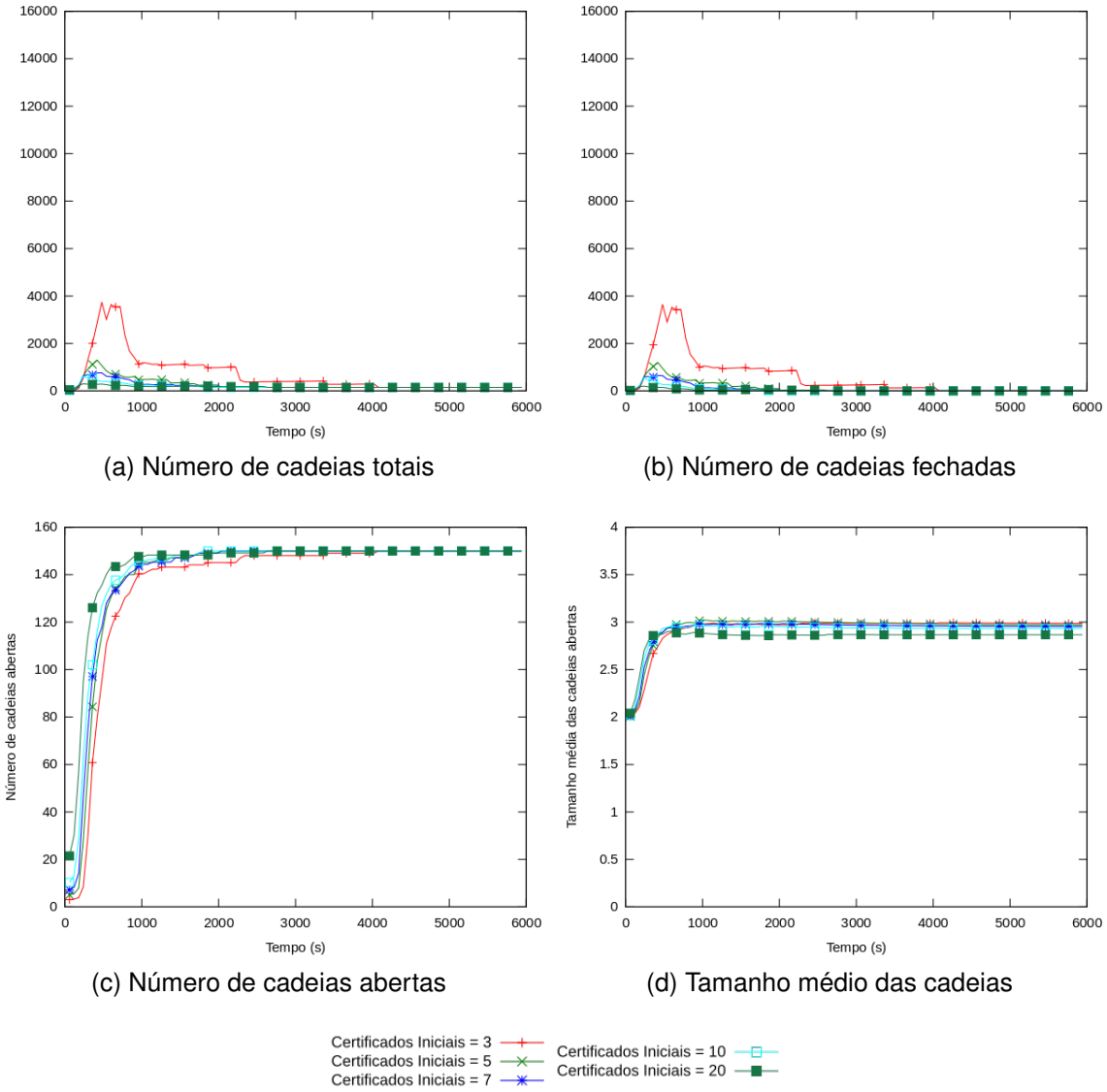
(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

Figura 4.3: Resultados com algoritmo otimizado para 50 nodos

Comparando os resultados das Figuras 4.1(a) e 4.3(a), nota-se que para valores menores de $C_i$, a mudança é mais evidente, sendo que no momento de pico de armazenamento de cadeias, a queda foi de pouco mais de 38% para $C_i$ igual a 3 e 5. As mudanças não afetaram de forma significativa o tempo de convergência das cadeias abertas, como pode ser visto nas Figuras 4.1(c) e 4.3(c).

A queda mais drástica fica explícita ao comparar-se a quantidade de cadeias totais para 150 nodos, conforme as Figuras 4.2(a) e 4.4(a). A queda para 5 certificados iniciais foi de aproximadamente 50% e para 3 foi de mais de 75%.




(a) Número de cadeias totais

(b) Número de cadeias fechadas

(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

Figura 4.4: Resultados com algoritmo otimizado para 150 nodos

Nas Figuras 4.1(d) e 4.3(d), é possível notar que o tamanho médio das cadeias manteve-se próximo a 3, mas que na versão otimizada, a regularidade foi atingida antes.

Como visto anteriormente, ao final da simulação, o espaço ocupado é representado pela expressão $s = \sum_{i=1}^{T} Ca_i$. Considerando esse cenário, no qual o esquema converge de forma satisfatória, pode-se substituir $T$ por $n-1$ e $Ca_i$ por $32 \times 1 + 566$, pois cada nodo manteve apenas uma cadeia aberta de tamanho aproximado igual a 3, ou seja, origem e destino com um intermediário. Desta forma, tem-se:

$$s = \sum_{i=1}^{T} Ca_i \approx \sum_{i=1}^{n-1}(32 \times 1 + 566) \approx 598n - 598bits$$

O espaço ocupado é diretamente proporcional a quantidade de nodos na rede. Ao considerar-se o pior caso simulado, 150 nodos, obtém-se que $s \approx 89102$, ou seja, pouco menos que 11 kBytes ao fim da simulação. Mas o problema visto não são os momentos finais, e sim os momentos de pico de armazenamento. Nesse caso, pode-se estimar $s$ da mesma forma para verificar o pior caso simulado:

$$s = \sum_{i=1}^{T} Ca_i \approx \sum_{i=1}^{4000} (32 \times 1 + 566) bits$$

Desta forma, tem-se que $s \approx 2392000$ bits, equivalente a 291 kBytes. É importante que o espaço ocupado pelas cadeias não seja superior a 10% do buffer de memória dos nodos em condições normais, para que o esquema não sobrecarregue o nodo em condições desfavoráveis.

### 4.2.2 Ataques

Tendo em vista o que esquema convergiu de forma satisfatória em condições normais, agora o esquema será testado em um meio com parte dos nodos maliciosos, ou seja, realizando algum tipo de ação com o objetivo de afetar negativamente a rede ou obter dados não endereçados a ele.

#### 4.2.2.1 Ataque *GreyHole*

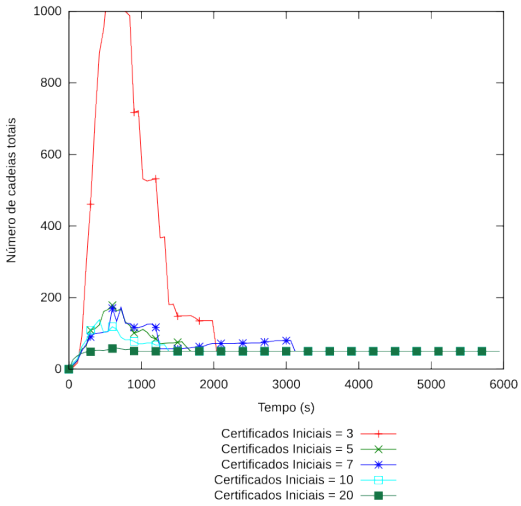
A primeira situação simulada foi a presença de nodos executando o ataque chamado de *greyhole*, no qual, parte das mensagens que chegam até eles é descartada.

Foram feitas simulações usando os mesmos parâmetros utilizados anteriormente, adicionando diferentes porcentagens de nodos maliciosos ($m$), 10, 20 e 50% e diferentes taxas de descarte de mensagens ($t$), 10, 25 e 50% . A escolha de quais nodos eram maliciosos foi aleatória no início de cada simulação e todos eles descartando de forma aleatória, com a mesma taxa, as mensagens que chegavam. Desta forma, não havia um nodo alvo para o ataque ou ataque conjunto sobre um único nodo, mas sim um grupo de nodos maliciosos descartando mensagens de forma a interferir no tempo de convergência do esquema.

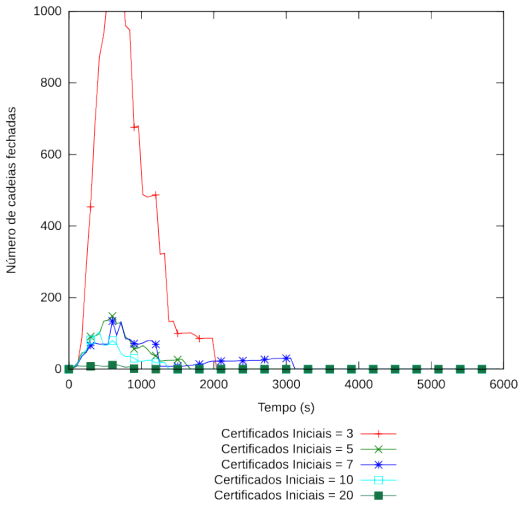
Explicita-se que mesmo o nodo sendo malicioso, algum outro nodo poderia certificá-lo no início da rede, mantendo a identidade de nodos maliciosos oculta ao menos no princípio da simulação. Isto acontece devido à forma adotada de distribuição dos certificados iniciais e da escolha dos nodos maliciosos. Os dois processos são independentes entre si e acontecem no início da rede.

Nas Figuras 4.5 e 4.6 estão os resultados de $m = 10\%$ e $t = 10\%$ para 50 e 150 nodos, respectivamente. Os valores de $C_i = 3$ não estão compatíveis aos valores

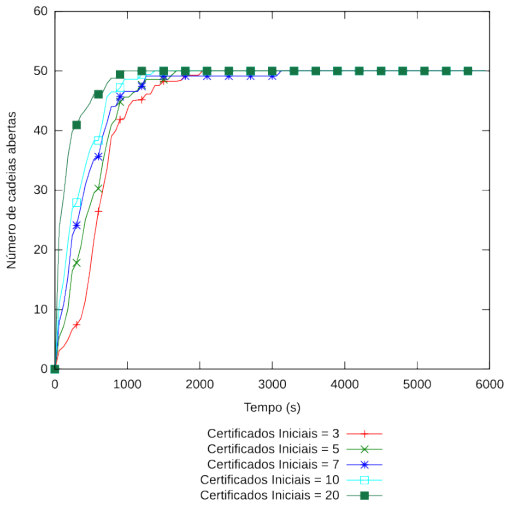
máximos dos gráficos, mas isso é proposital para que a escala dos gráficos permaneça idêntica a presente nos demais gráficos.



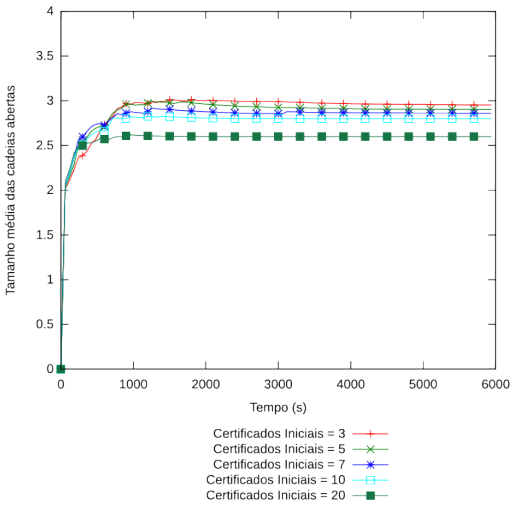

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



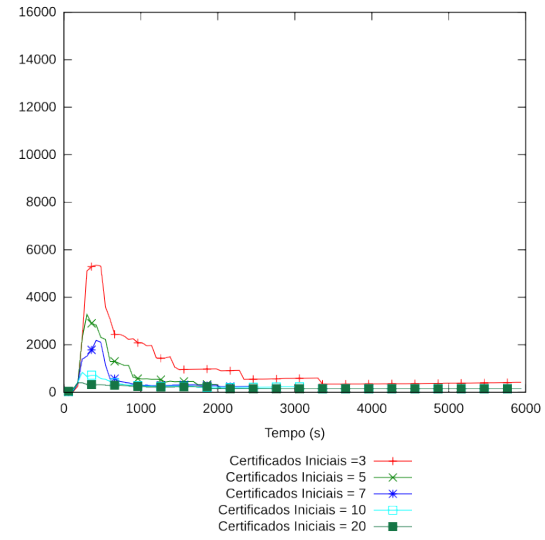

(c) Número de cadeias Abertas



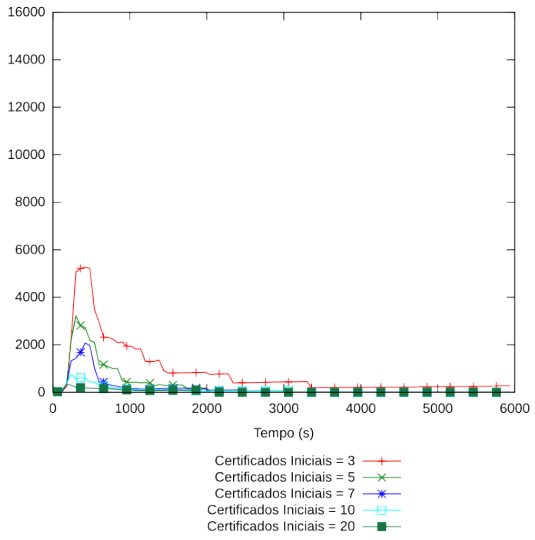

(d) Tamanho médio das cadeias

Figura 4.5: Resultados para 50 nodos, $m = 10\%$ e $t = 10\%$

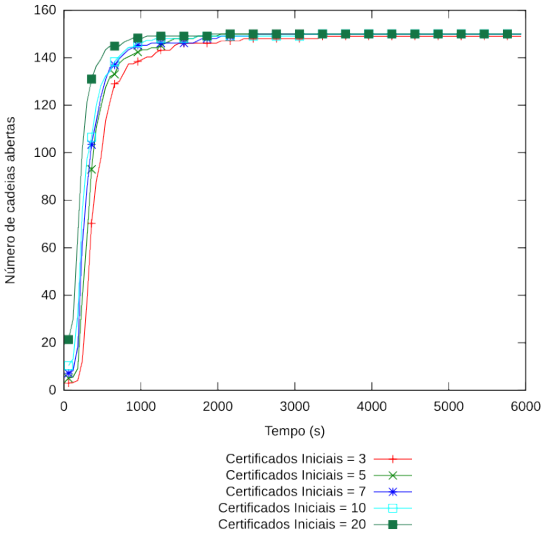
Os resultados apresentados demonstram que o esquema não sofre interferência com uma pequena parte dos nodos descartando poucas mensagens, independente da quantidade de nodos total da rede, mantendo os valores muito próximos aos encontrados anteriormente, com exceção da quantidade total de cadeias para certificados iniciais = 3.



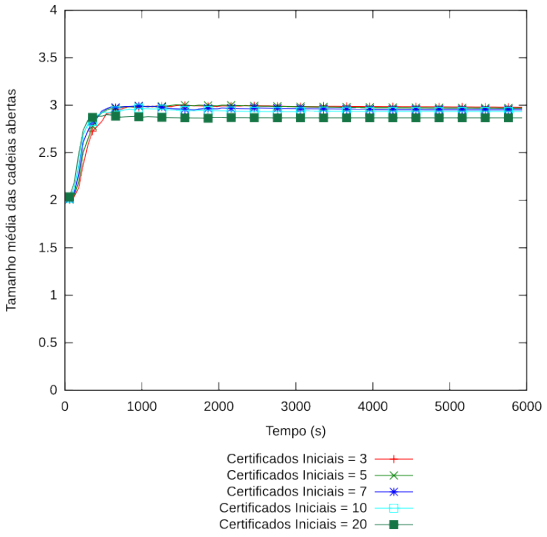

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

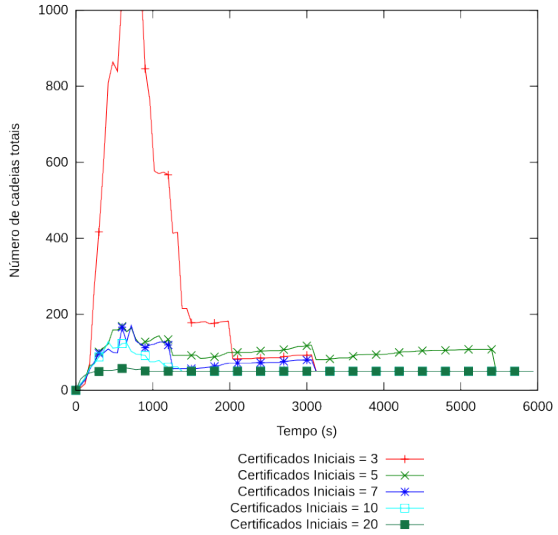



(d) Tamanho médio das cadeias

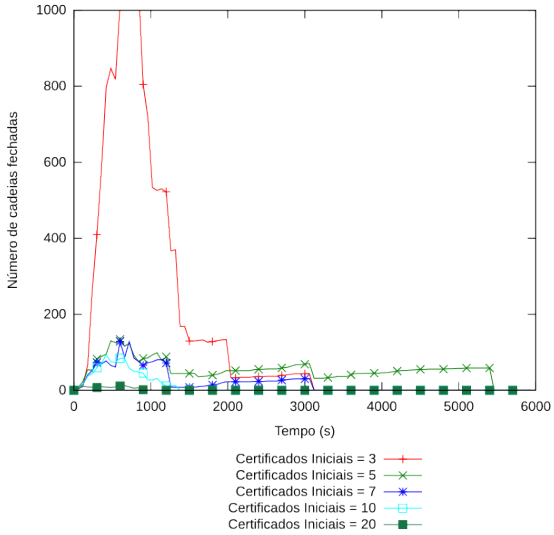
Figura 4.6: Resultados para 150 nodos, $m = 10\%$ e $t = 10\%$

Para 50 nodos o aumento na quantidade de cadeias totais armazenadas foi cerca de 58% e para 150 nodos de 30%. Isso deve-se ao fato de que com menos informação inicial, mensagens perdidas afetam o tempo de convergência do esquema. Entretanto, logo após o instente de maior armazenamento, há uma queda abrupta, demonstrando que o pico foi ocasionado pela falta da chave de poucos nodos, e assim que elas foram obtidas, os nodos descartaram uma grande quantidade de cadeias fechadas.

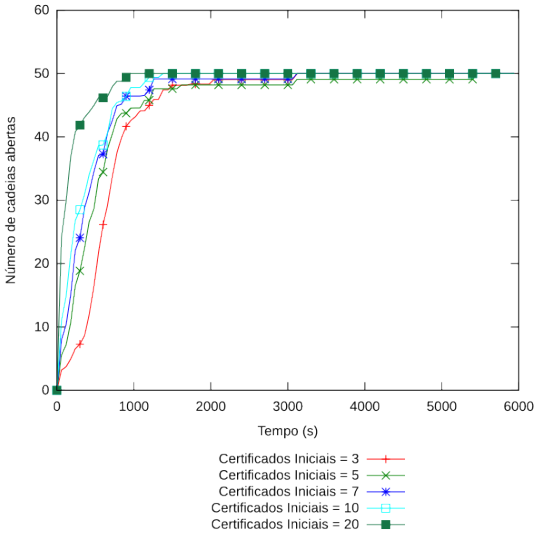
Os gráficos para $m = 20\%$ estão presentes no Apêndice B juntamente com os resultados para 75 e 100 nodos das demais quantidades de maliciosos.



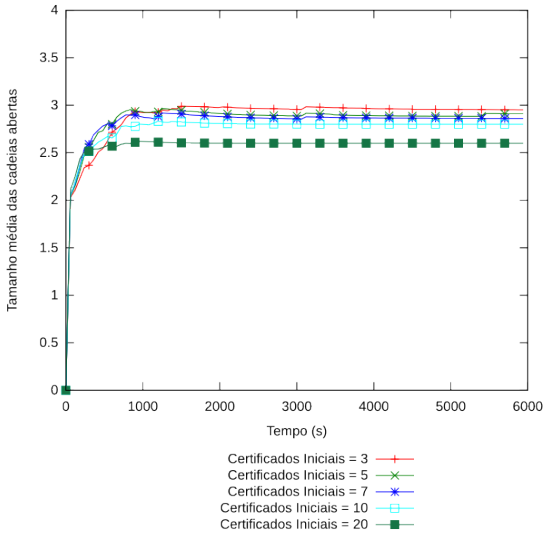

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



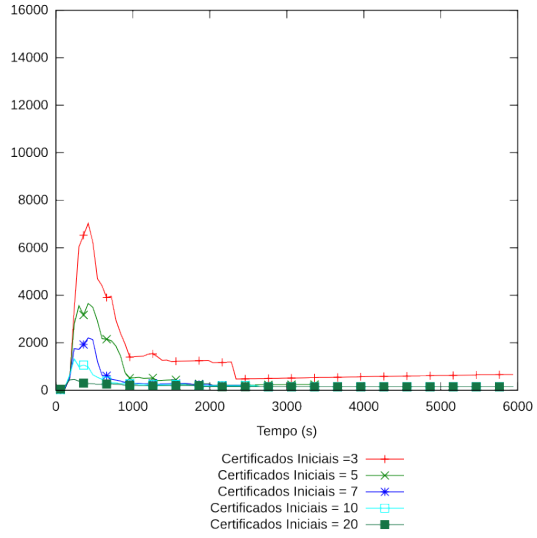

(c) Número de cadeias Abertas



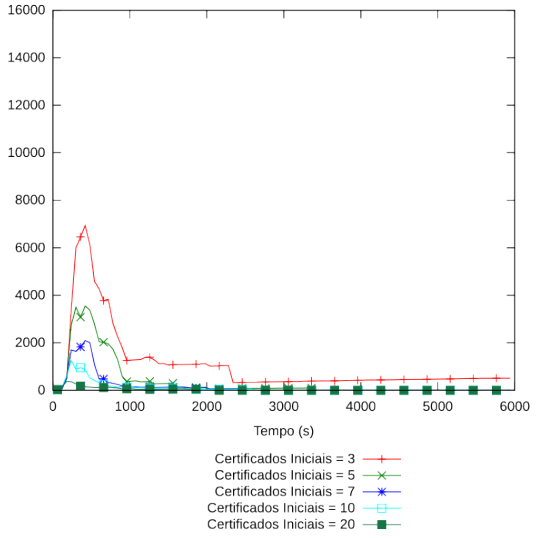

(d) Tamanho médio das cadeias

Figura 4.7: Resultados para 50 nodos, $m = 10\%$ e $t = 50\%$

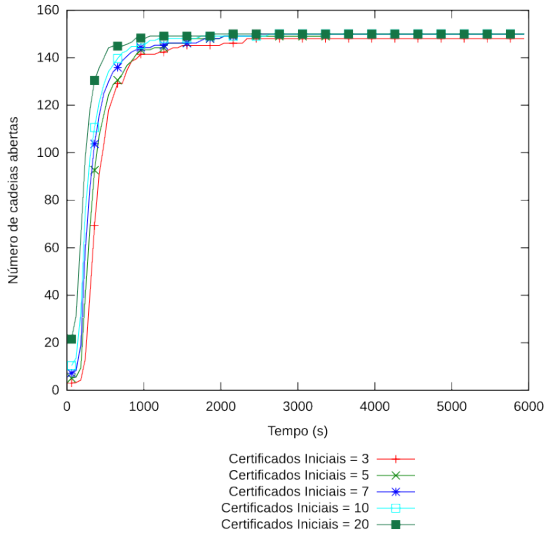
Ao mudar apenas a taxa de descarte dos nodos maliciosos para 50%, pode-se notar nas Figuras 4.7 e 4.8 que os resultados encontrados não mudaram significativamente em comparação com a taxa de 10%. Desta forma, pode-se inferir que para uma pequena quantidade de nodos maliciosos, a taxa de 50% de descarte de mensagens afeta o esquema da mesma maneira que taxas menores.



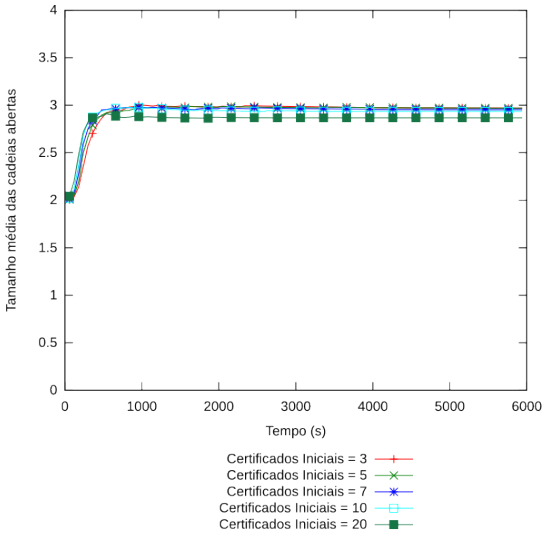

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

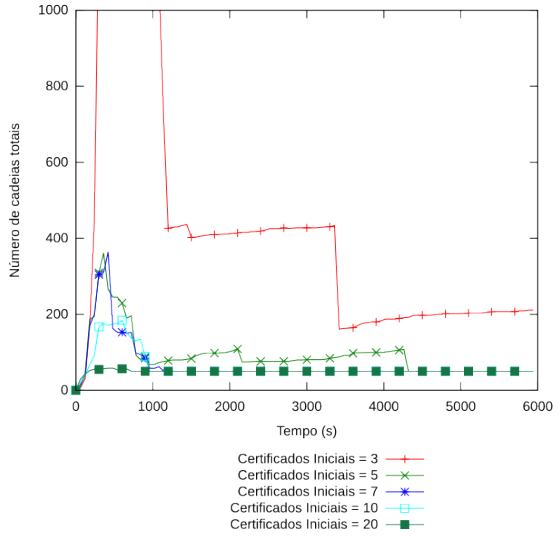



(d) Tamanho médio das cadeias

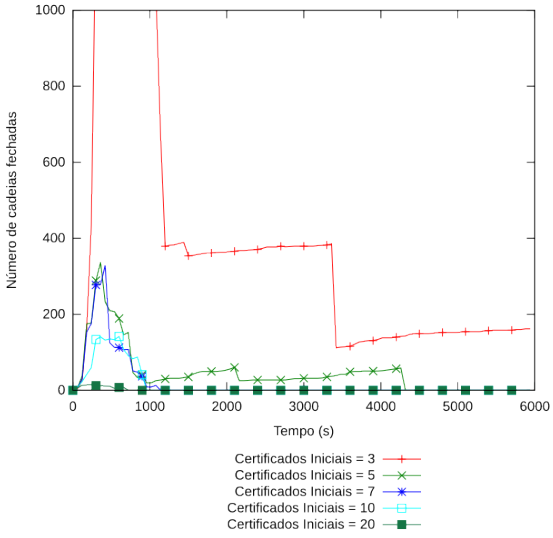
Figura 4.8: Resultados para 150 nodos, $m = 10\%$ e $t = 50\%$

Já nas Figuras 4.9 e 4.10, mudou-se a quantidade de nodos maliciosos na rede para 50% para $t = 10\%$. Nas simulações com 50 nodos o esquema foi mais afetado para quantidade de certificados iniciais menores, 3 e 5, sendo que ao final alguns nodos ainda não obtiveram as chaves de alguns nodos da rede.

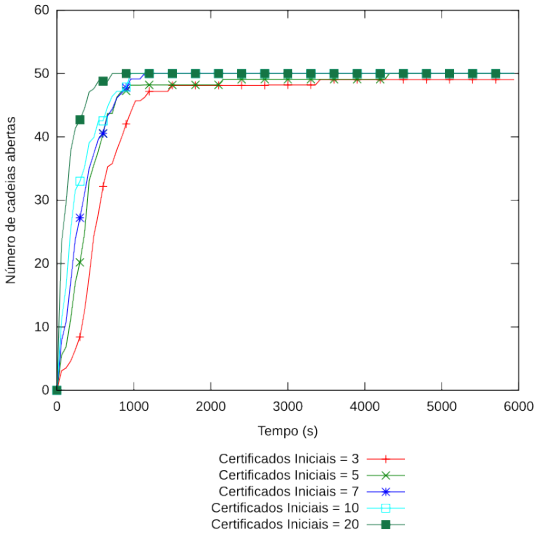
A grande porcentagem de nodos maliciosos, gera uma segmentação da rede e, consequentemente, alguns nodos podem tornar-se inalcançaveis para outros ou sobrecarregar nodos que servem de ligação entre grupos.



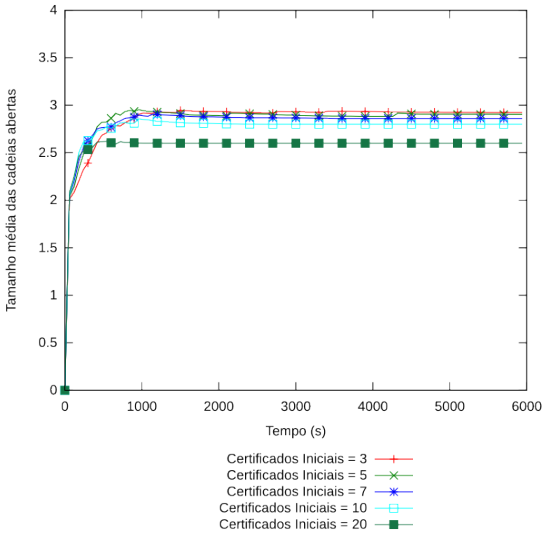

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



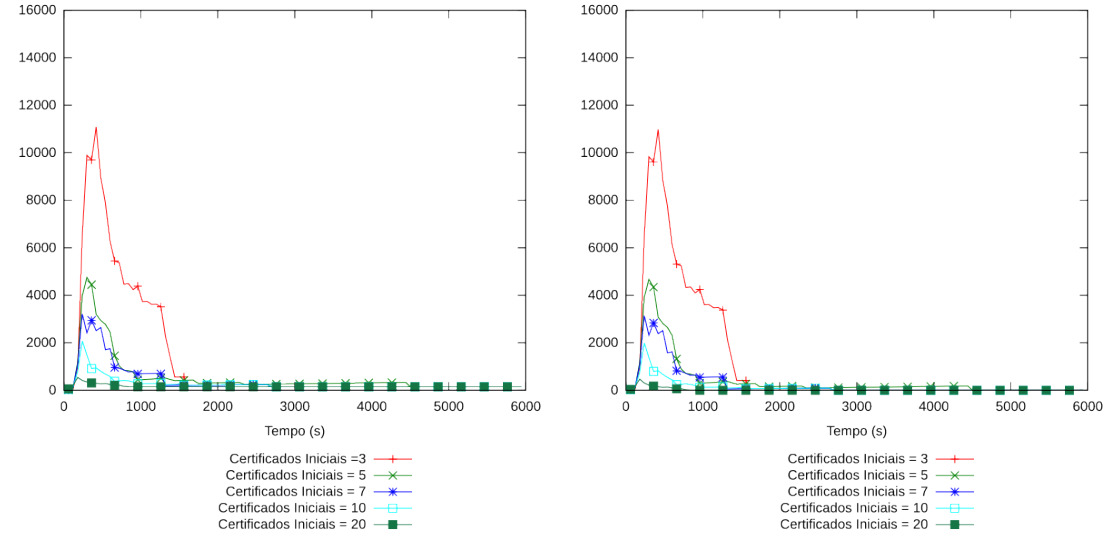

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura 4.9: Resultados para 50 nodos, $m = 50\%$ e $t = 10\%$

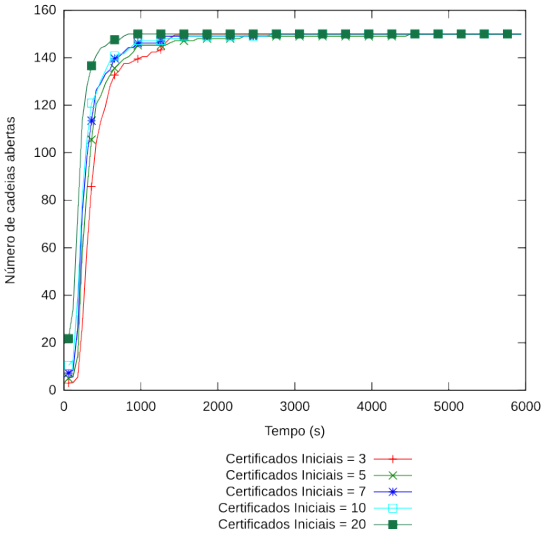
No caso das simulações com mais nodos, que é o caso apresentado na Figura 4.10, embora o número total de cadeias aumente cerca de 40% no pior caso simulado ($C_i = 3$), os nodos podem obter as chaves por diversos caminhos, não elevando tão drasticamente a quantidade de cadeias fechadas e totais armazenadas durante o período de convergência.



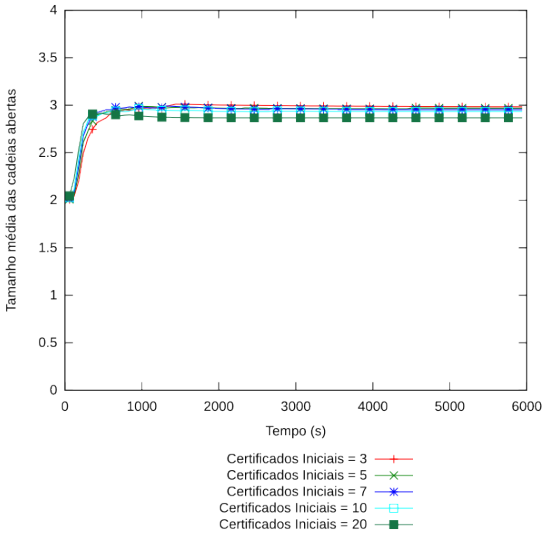

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

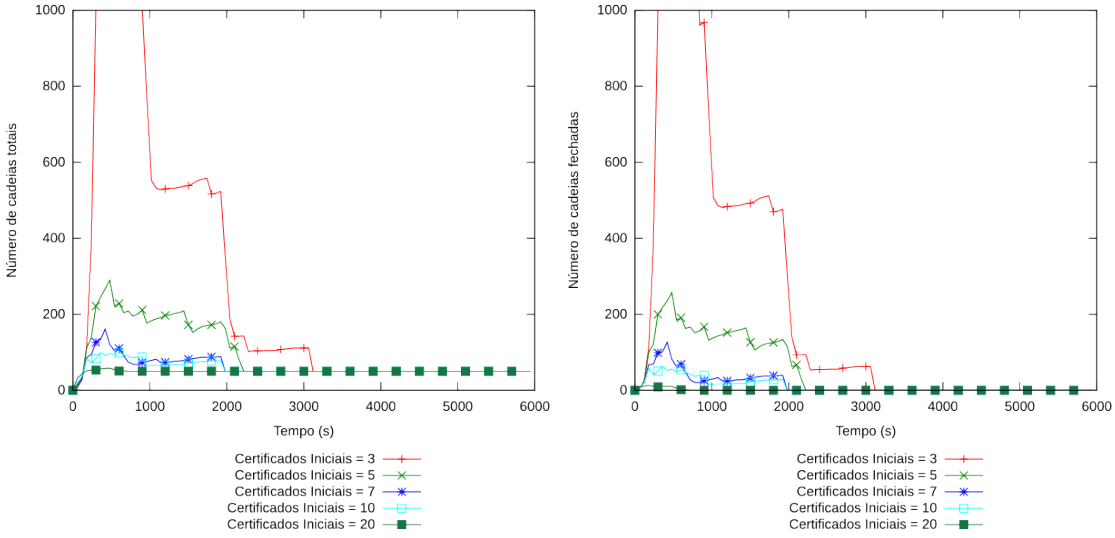



(d) Tamanho médio das cadeias

Figura 4.10: Resultados para 150 nodos, $m = 50\%$ e $t = 10\%$

Simulou-se também com $m = 50\%$ e $t = 50\%$ como pior cenário para um ataque *greyhole*. Os resultados estão expressos nas Figuras 4.11 e 4.12.

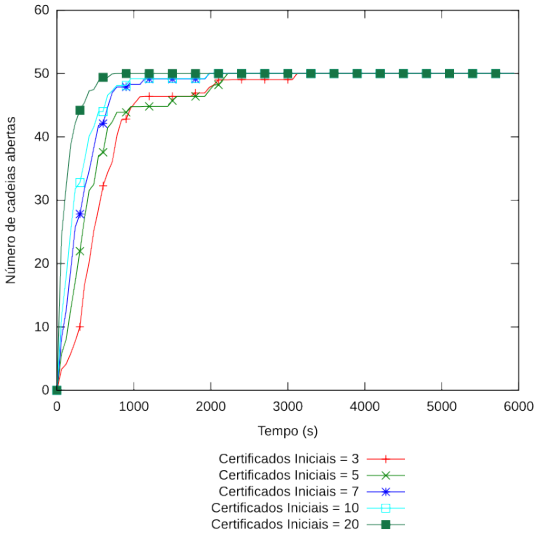
Na Figura 4.11, a quantidade de cadeias fechadas e totais elevou-se mais 300% em comparação ao cenário sem ataques e na Figura 4.12 de pouco mais 250%. Ainda observa-se que o esquema convergiu em um tempo aproximado ao encontrado anteriormente para $C_i > 5$, cerca de 2000s. No entanto, para os cenários com $C_i <= 5$ houve um aumento no tempo, elevando-o para 3000s.



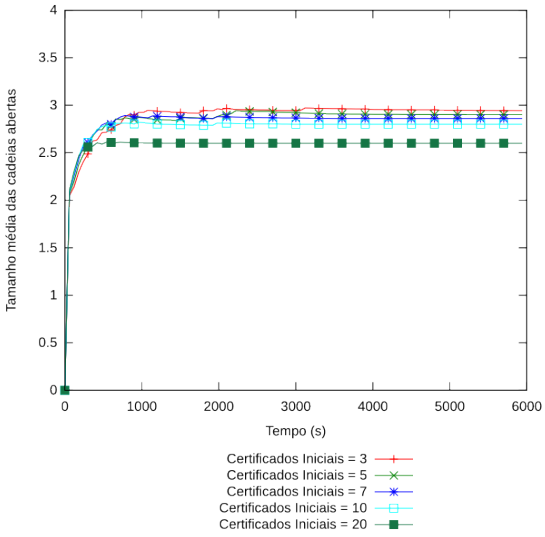

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



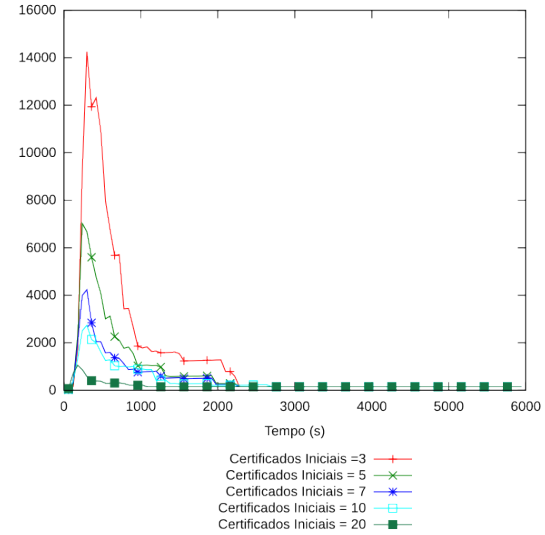

(c) Número de cadeias Abertas



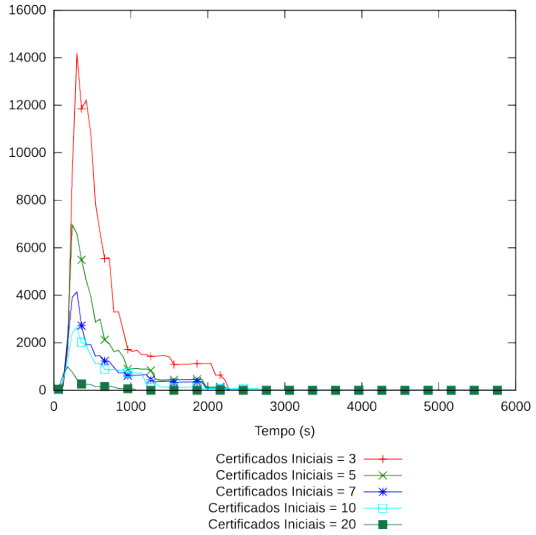

(d) Tamanho médio das cadeias

Figura 4.11: Resultados para 50 nodos, $m = 50\%$ e $t = 50\%$

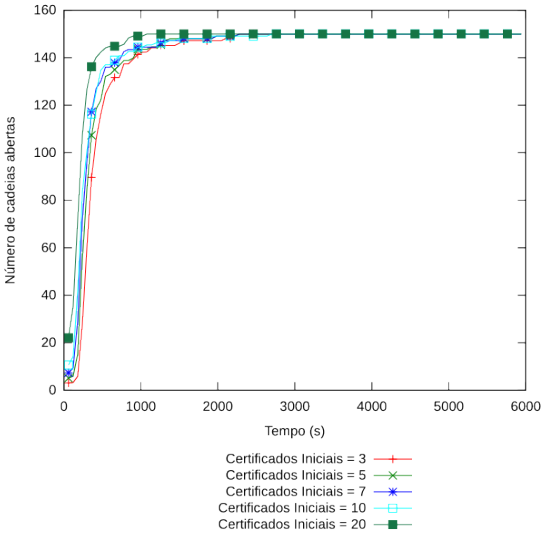
Nota-se que independente da quantidade de nodos maliciosos e das taxas de descarte atribuídas a eles, o tamanho médio das cadeias manteve-se muito próximo do encontrado anteriormente, tendo variação inferior a 10%.



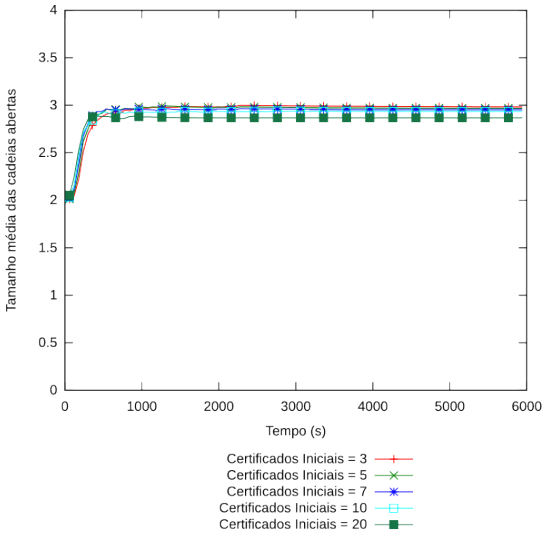

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

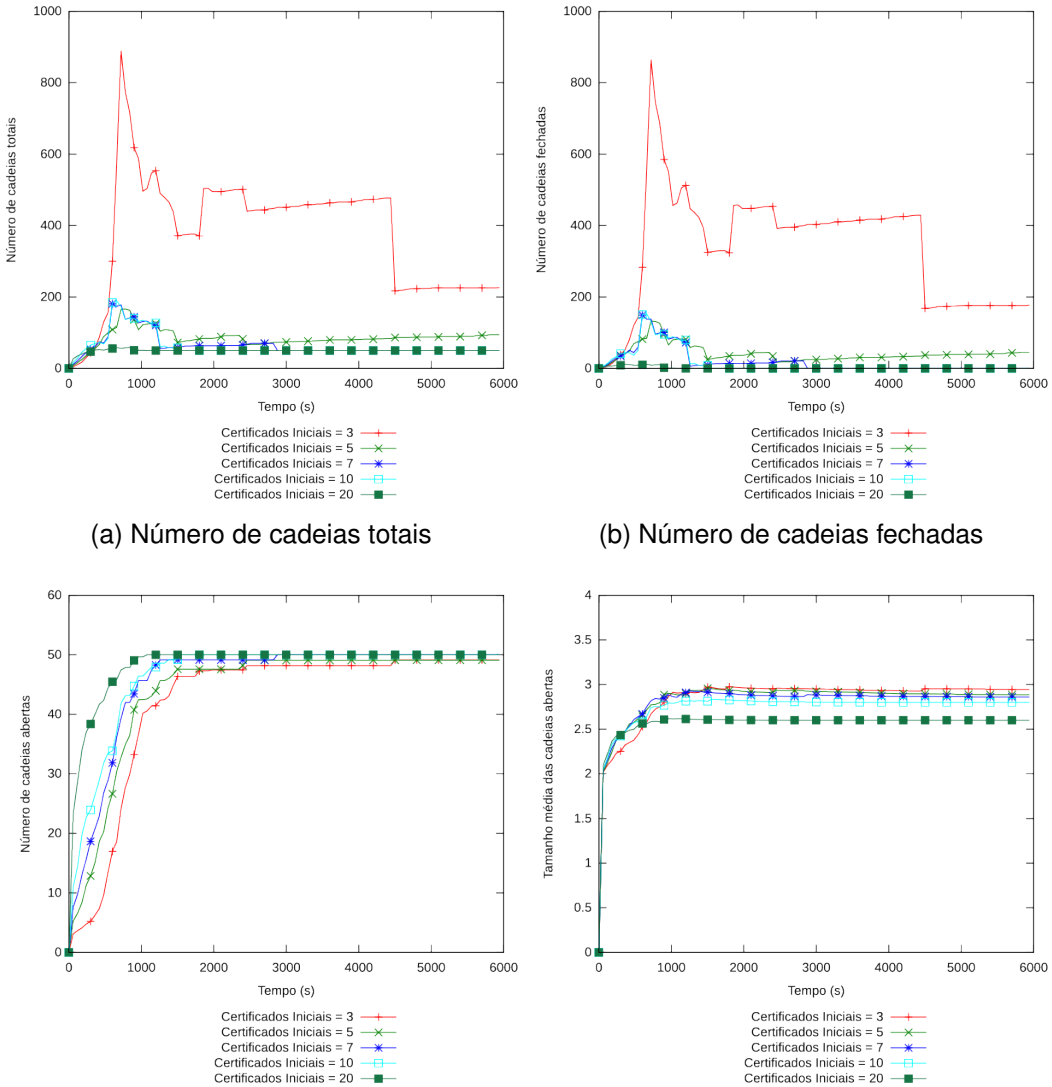
Figura 4.12: Resultados para 150 nodos, $m = 50\%$ e $t = 50\%$

Assim, pode-se notar que mesmo em cenários com altas quantidades de nodos maliciosos e taxas de descarte, o esquema conseguiu convergir sem sofrer alterações no valor de cadeias abertas, mas tendo como principal custo o aumento na quantidade de cadeias armazenadas.

#### 4.2.2.2 Ataque *BlackHole*

Outro tipo de ataque ao qual o esquema foi submetido é o denominado *blackhole*. Esse ataque pode ser visto como um *greyhole* em que a taxa de descarte é de 100%, ou seja, toda mensagem que chega até o nodo malicioso é descartada, independente de origem ou destino.

Foram realizadas simulações para $m$ = 10, 20 e 50% e utilizando os mesmos parâmetros das simulações anteriormente apresentadas. Os resultados nas Figuras 4.13 e 4.14 demonstram os resultados para $m$ = 10% com 50 e 150 nodos da rede.




(a) Número de cadeias totais

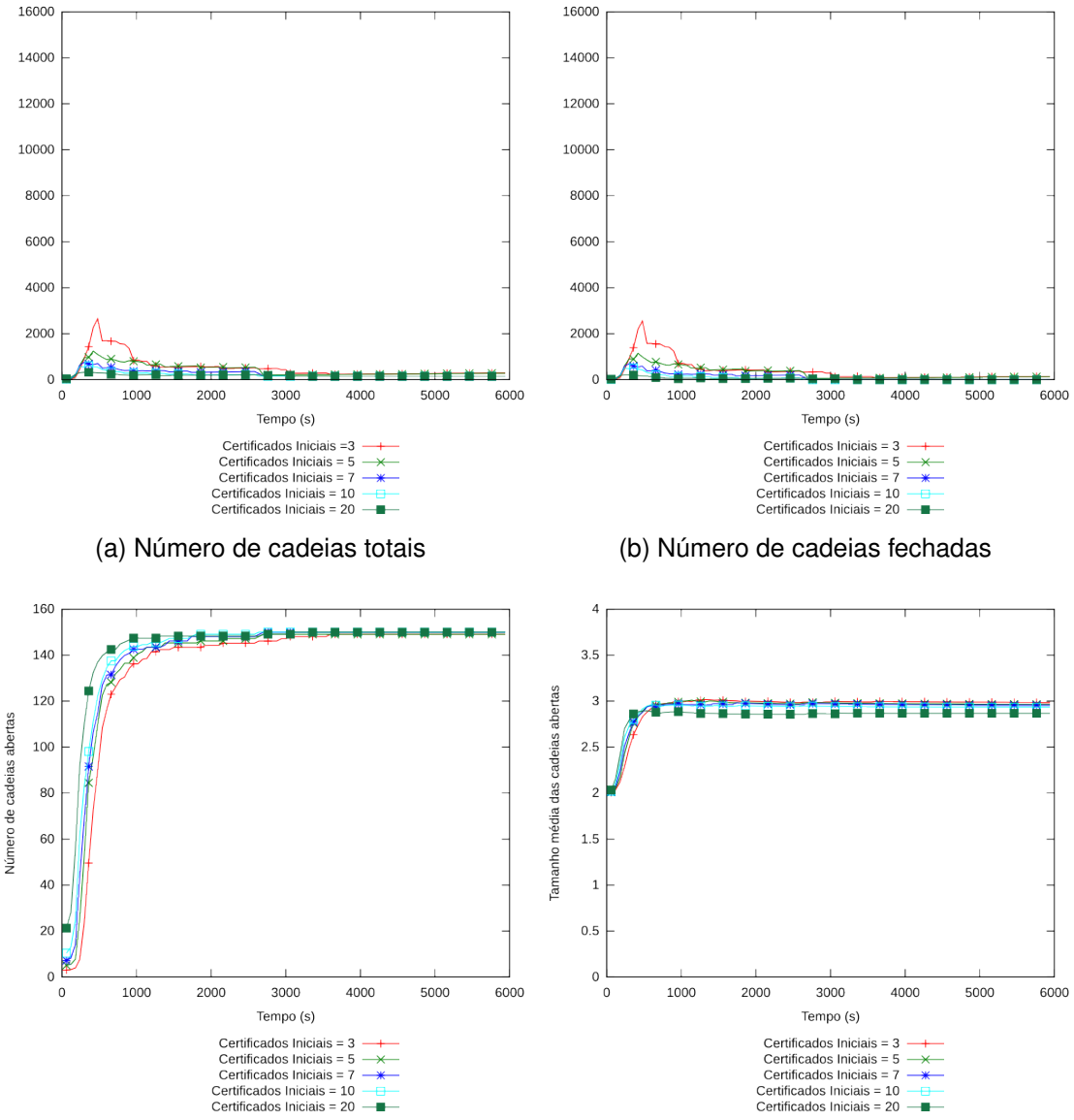
(b) Número de cadeias fechadas

(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

Figura 4.13: Resultados para 50 nodos e $m = 10\%$

Nota-se que em comparação às Figuras 4.3 e 4.4 a quantidade de cadeias fechadas e abertas não sofreram alterações significativas, evidenciando que o esquema é funcional e não sofre com uma pequena porcentagem de nodos efetuando esse tipo de ataque. O tamanho médio das cadeias permaneceu em valores próximos a 3.




(a) Número de cadeias totais

(b) Número de cadeias fechadas

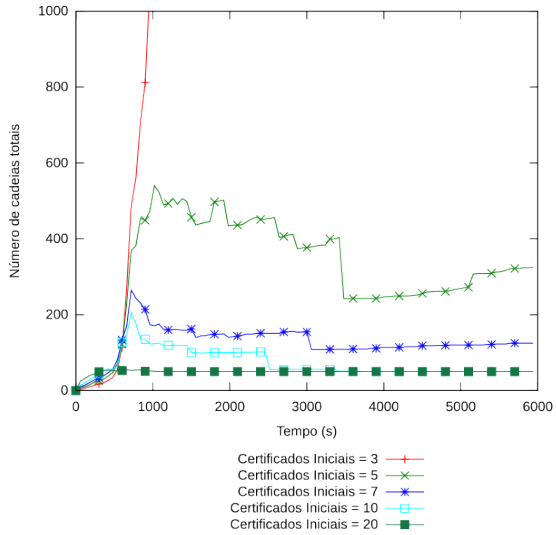
(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

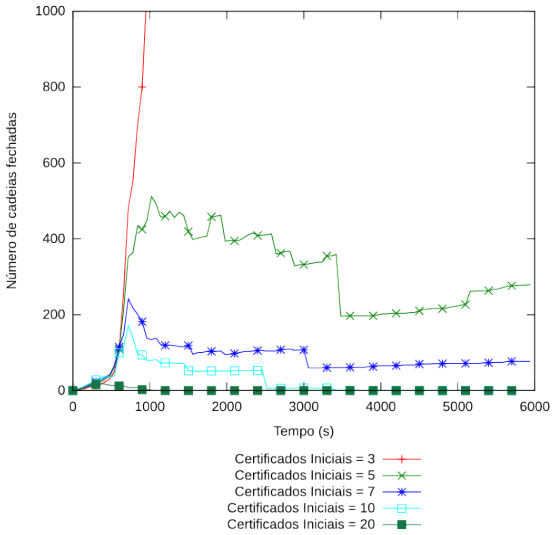
Figura 4.14: Resultados para 150 nodos e $m = 10\%$

Assim como no ataque anterior, mesmo o nodo sendo malicioso, algum outro nodo poderia certificá-lo no início da rede, mantendo a identidade de nodos maliciosos oculta ao menos no princípio da simulação.

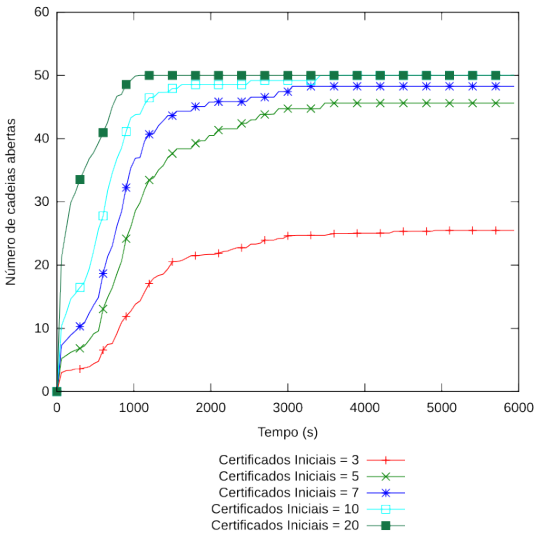
Nas Figuras 4.15 e 4.16 os resultados apresentados são para *m* = 50% dos nodos da rede. Esse cenário é o primeiro em que o esquema não convergiu totalmente durante os 6 mil segundos de simulação. Mantendo uma certa estabilidade na quantidade de cadeias abertas, mas inferior a quantidade total de nodos. Isso acontece devido a alta quantidade de nodos maliciosos que gerou uma divisão da rede em pequenos grupos menores.



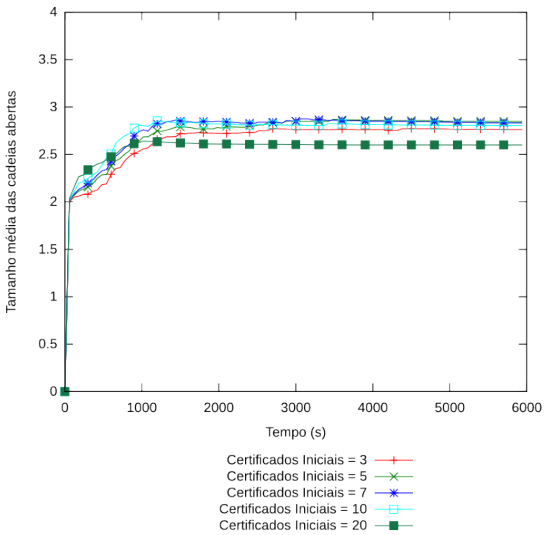

(a) Número de cadeias totais




(b) Número de cadeias fechadas



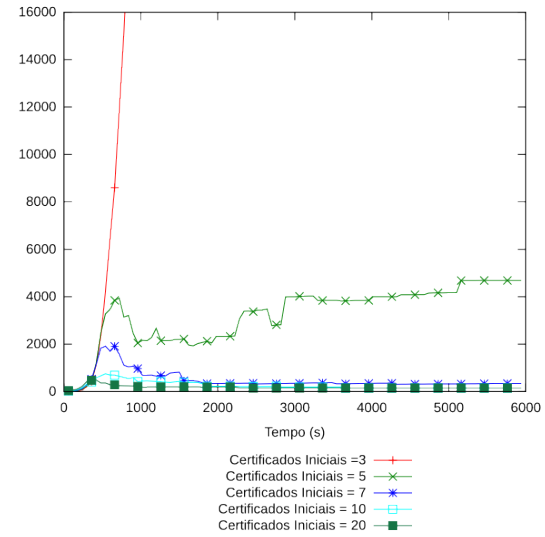

(c) Número de cadeias abertas



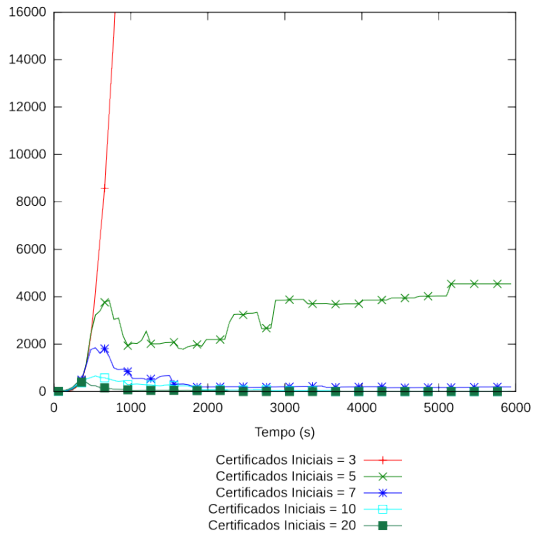

(d) Tamanho médio das cadeias

Figura 4.15: Resultados para 50 nodos e $m = 50\%$

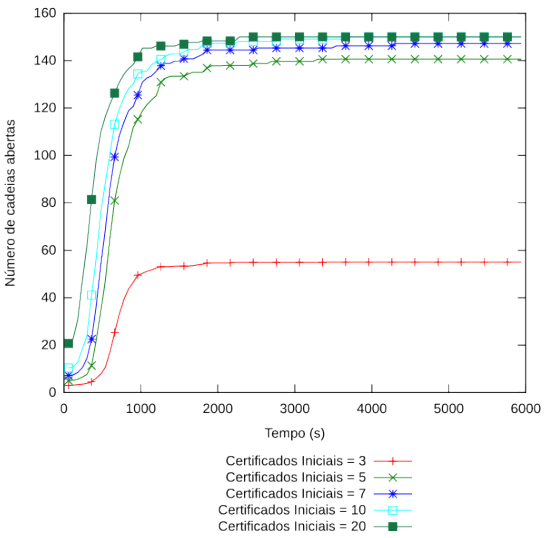
Nota-se que, para $n = 50$, a quantidade mínima de cadeias abertas foi encontrada com $C_i = 3$, e manteve-se estável em 50% dos nodos da metade do tempo em diante. Não se pode inferir que todos os nodos mantiveram os mesmos 50% e nem que os nodos que faltaram eram os nodos atacantes. Analisando as simulações uma a uma, pode-se observar que na maioria dos casos, a rede foi dividida em dois grande grupos isolados e dentro desses, haviam grupos menores com nodos chave se movimentado entre eles. No restante, a quantidade aproximou-se do total, mas atingiu somente para $C_i$ =10 e 20.



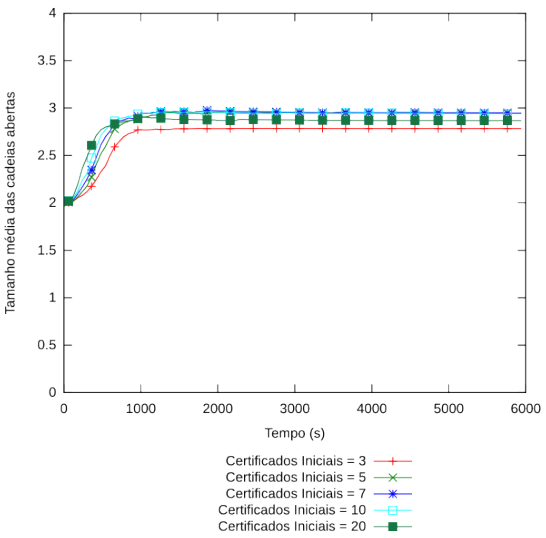

(a) Número de cadeias totais




(b) Número de cadeias fechadas




(c) Número de cadeias abertas




(d) Tamanho médio das cadeias

Figura 4.16: Resultados para 150 nodos e $m = 50\%$

A quantidade de cadeias fechadas extrapolou todos os limites obtidos anteriormente e foi definido um limite de cadeias fechadas para cada destino afim de impedir o uso exagerado de espaço de armazenamento e também, porque as simulações começaram a usar mais 32 GB de memória RAM na máquina usada para realizá-las. Assim, cada destino pode possuir cadeias que totalizem no máximo 10 vezes o número de nodos da rede. Ao atingir esse limite, as cadeias que chegam são descartadas.

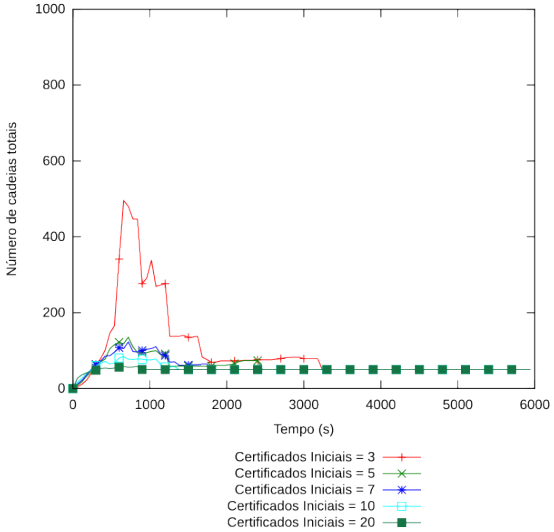
Na Figura 4.16 estão os resultados para 150 nodos e apresentam características semelhantes as encontradas para menos nodos. Todavia, com a presença de mais nodos na rede, os resultados para $C_i > 5$ voltaram a aproximar-se do ideal. Para $C_i = 3$ os resultados foram inferiores, não obtendo cadeias para nem metade dos nodos da rede.

Os resultados encontrados demonstram que o esquema é funcional em um ambiente com nodos realizando esse tipo de ataque, contanto que a quantidade de certificados iniciais seja maior ou igual a 10 para uma quantidade de nodos maliciosos inferior a 50%. Para $C_i = 7$, os resultados são próximos do ideal, faltando, no pior caso testado, cerca de 4% dos nodos. Já para $C_i < 7$, os valores atingidos não são bons e demonstram uma fragilidade do esquema nessas situações.

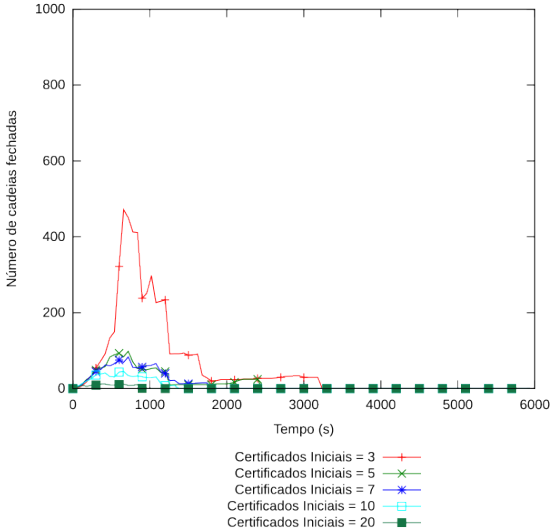
#### 4.2.2.3 Ataque *Sybil*

Foram feitas simulações com a presença de nodos realizando o ataque chamado de *Sybil*. Considerou-se um nodo *sybil* como aquele que desde no início da rede cria nodos falsos e emite certificados para eles. As simulações consideraram três quantidades de nodos falsos na rede ($f$), 10, 20 e 50% dos nodos, ou seja, para $n = 50$ e $f = 50\%$, a rede era formada por 25 nodos reais e 25 nodos falsos. Seguindo o exemplo, no início da rede eram sorteados 25 nodos que eram considerados reais, e escolhido aleatoriamente um nodo para ser o nodo mestre de um nodo falso, desta forma, pode-se obter situações em que cada nodo real possuía um nodo falso ou um único nodo real possui todos os nodos falsos.

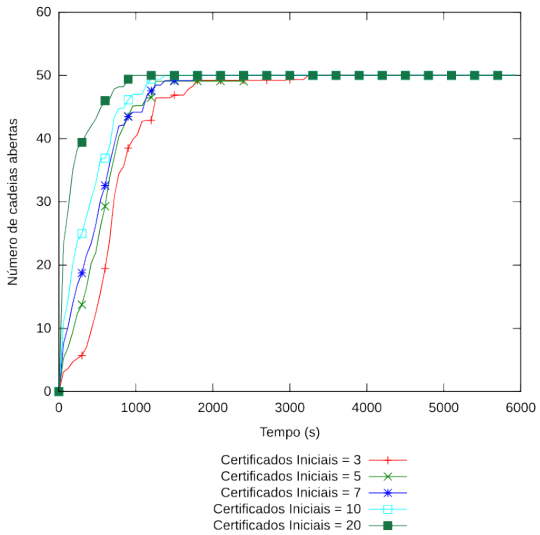
As simulações seguiram os mesmos parâmetros das simulações sem ataques com a inclusão de $f$, e, assim como anteriormente, serão apresentados somente os resultados de 50 e 150 nodos para $f = 10\%$ e $f = 50\%$ nesta seção, mantendo os demais no Apêndice B.




(a) Número de cadeias Totais



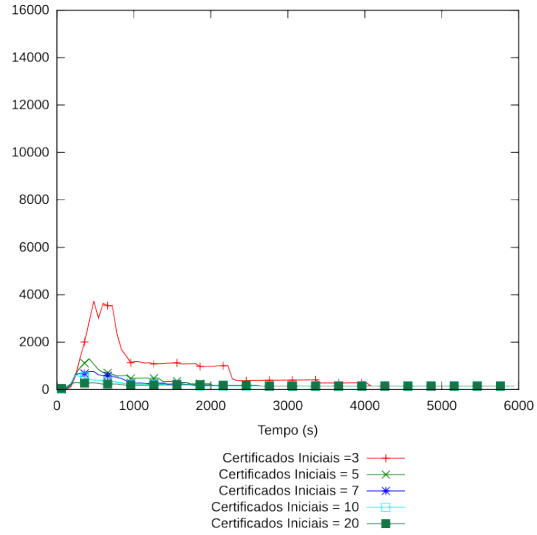

(b) Número de cadeias Fechadas



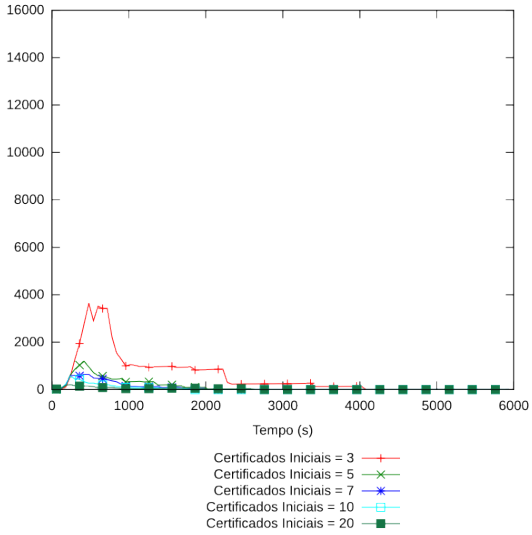

(c) Número de cadeias Abertas

Figura 4.17: Resultados para 50 nodos e $f = 10\%$

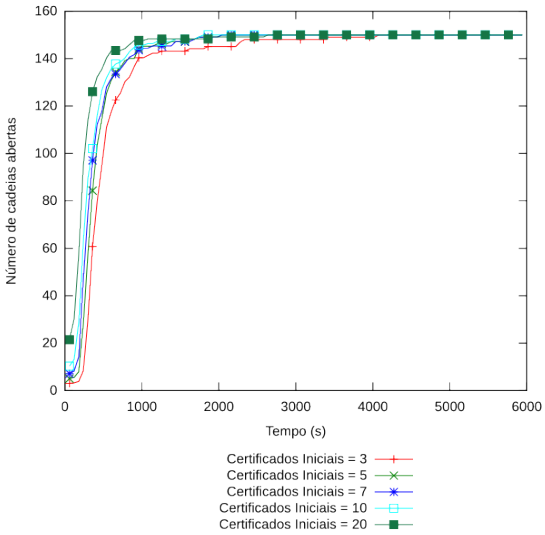
Nas Figuras 4.17 e 4.18 estão os resultados de 50 e 150 nodos para $f = 10\%$.




(a) Número de cadeias Totais



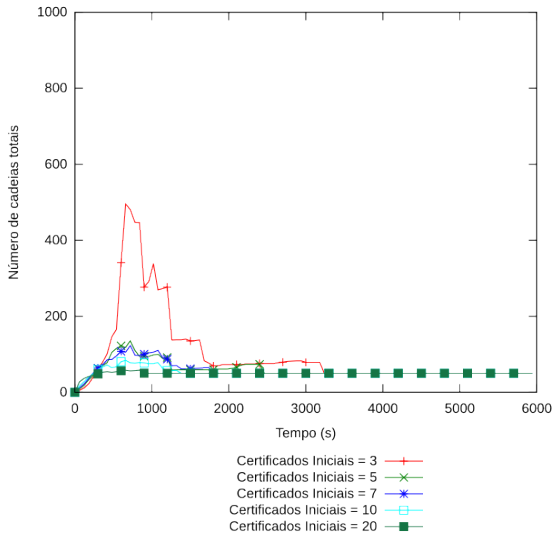

(b) Número de cadeias Fechadas



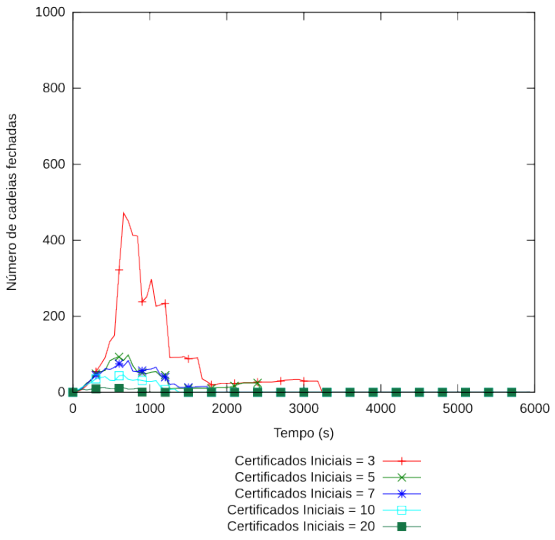

(c) Número de cadeias Abertas

Figura 4.18: Resultados para 150 nodos e $f = 10\%$

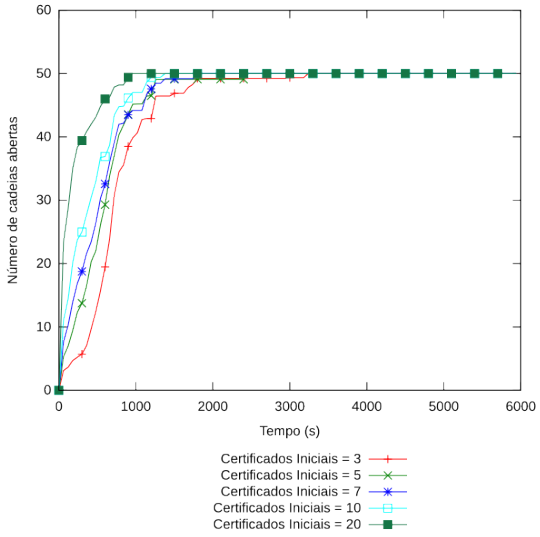
Nas Figuras 4.19 e 4.20 estão os resultados de 50 e 150 nodos para $f = 50\%$.




(a) Número de cadeias Totais



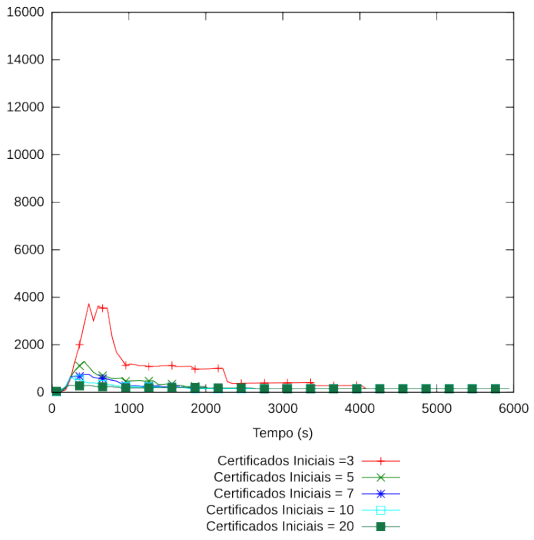

(b) Número de cadeias Fechadas



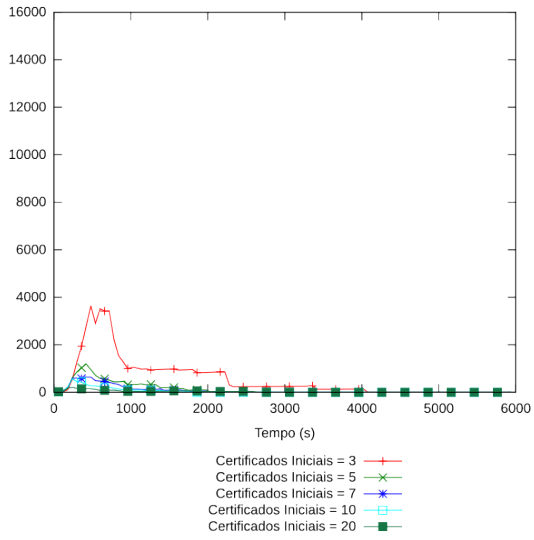

(c) Número de cadeias Abertas

Figura 4.19: Resultados para 50 nodos e $f = 50\%$

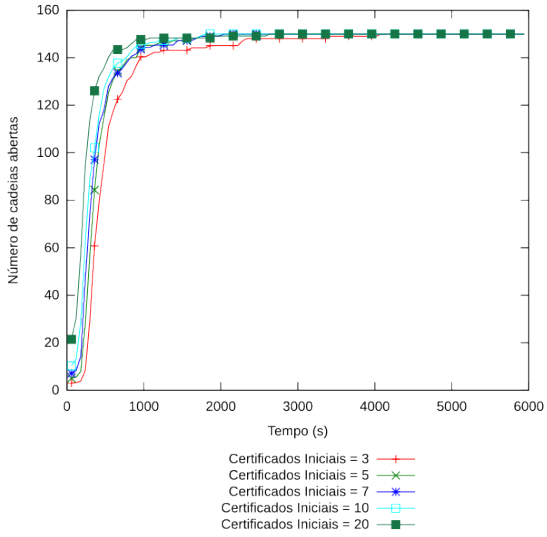
Considera-se que não cabe a esse esquema decidir que o nodo $x$ ou $y$ sejam reais, mas que se eles fazem parte da rede, que os outros nodos saibam suas chaves. A característica de confiável cabe à aplicação que usa as informações de chaves decidir se comunica-se ou não com cada nodo. O esquema apenas precisa garantir que dada uma chave, ela pertença a um único nodo até que expire.




(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



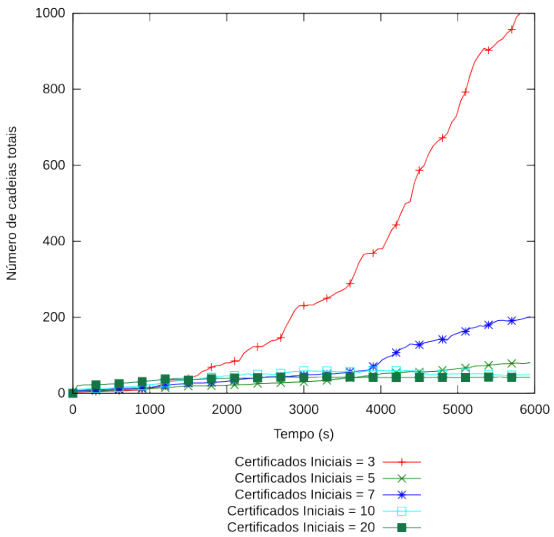

(c) Número de cadeias Abertas

Figura 4.20: Resultados para 150 nodos e $f = 50\%$

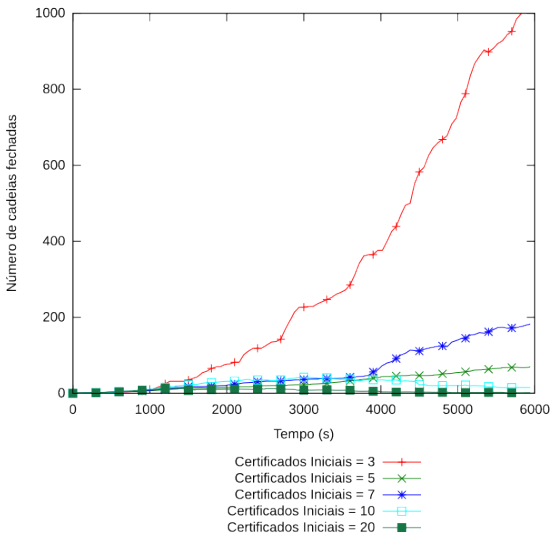
Explicita-se que os resultados encontrados foram quase que idênticos aos encontrados sem ataques, pois para o esquema um nodo falso não afeta nada, contanto que ele não faça mais nada além disso. A pouca diferença encontrada nos resultados deve-se basicamente ao modelo de movimentação utilizado.

### 4.2.3 Ataque de Falsificação

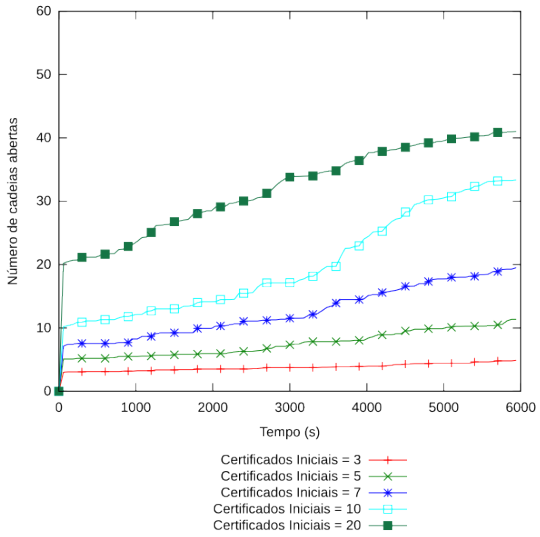
Por fim, o ataque de falsificação, no qual o nodo malicioso diz ser outro nodo da rede. Como um nodo não pode falsificar um certificado de outro nodo sem possuir a chave desse nodo e nem mesmo alterar uma cadeia, pois elas são assinadas, considerou-se a seguinte situação como sendo o ataque de falsificação: o nodo malicioso $x$ recebe uma cadeia qualquer para o nodo $y$. Ele descarta essa cadeia e repassa uma criada por ele, na qual a chave pública de $y$ é trocada por outra chave que faça par com uma chave que ele possua. Desta forma, as mensagem que posteriormente sejam endereçadas a $y$ podem ser abertas por $x$.



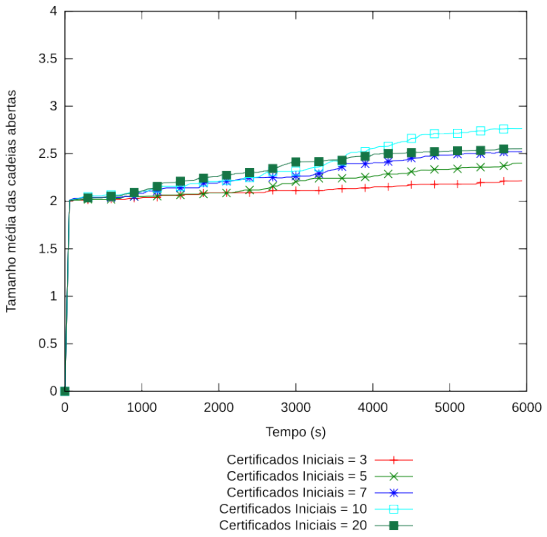

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



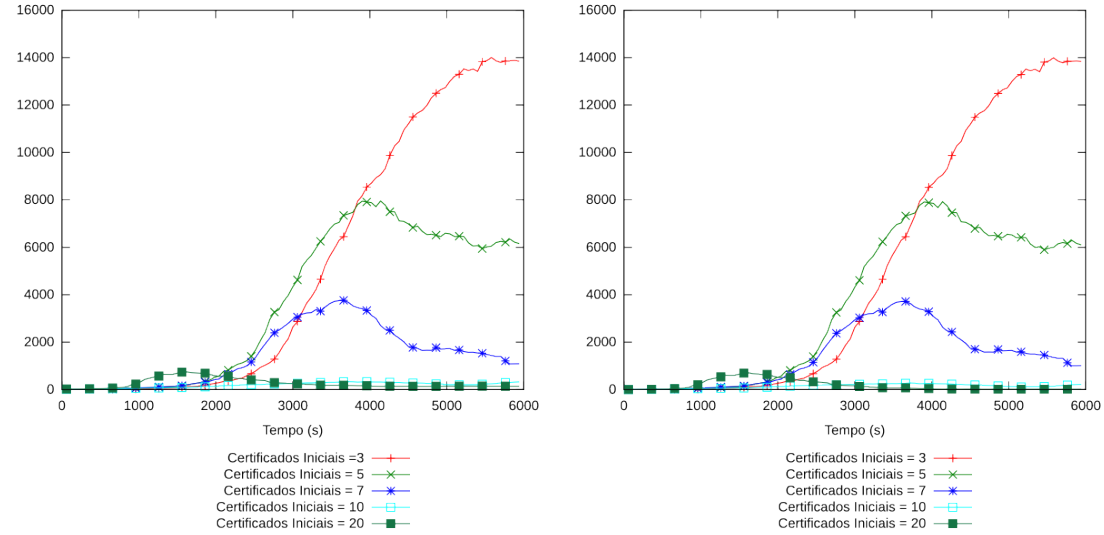

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

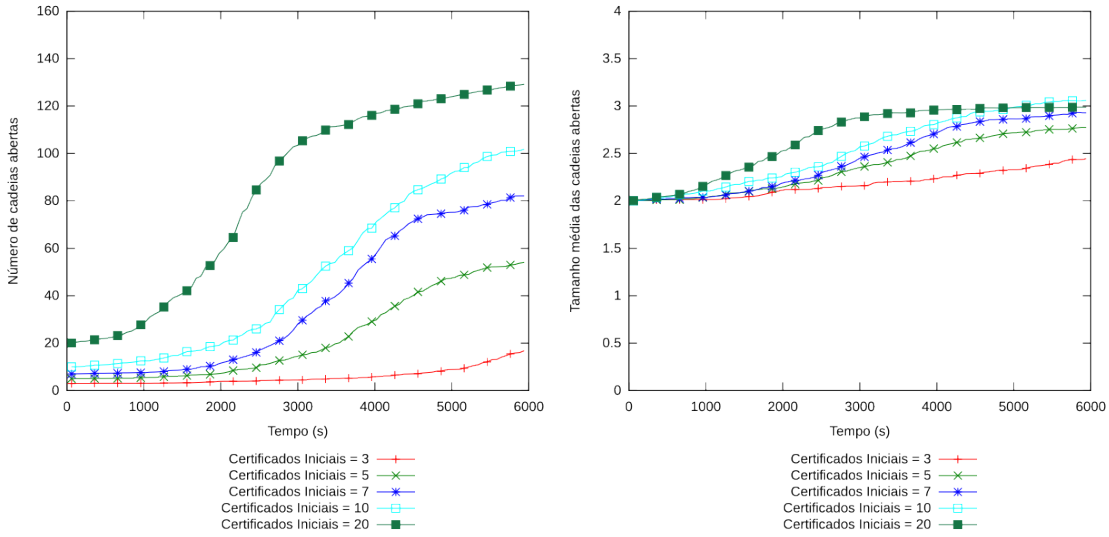
Figura 4.21: Resultados para 50 nodos, $m = 10\%$ e $N_a = 10\%$

Foram realizadas simulações com $m = 10$, 20 e 50% dos nodos e tendo como nodos alvo ($N_a$) 10, 25 e 50% dos nodos. Os nodos maliciosos podem realizar de duas maneiras o ataque, a primeira cada nodo age individualmente, trocando as chaves por qualquer outra que lhe convenha. Na outra todos agem coletivamente, trocando uma chave sempre pela mesma.




(a) Número de cadeias Totais

(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

Figura 4.22: Resultados para 150 nodos, $m = 10\%$ e $N_a = 10\%$

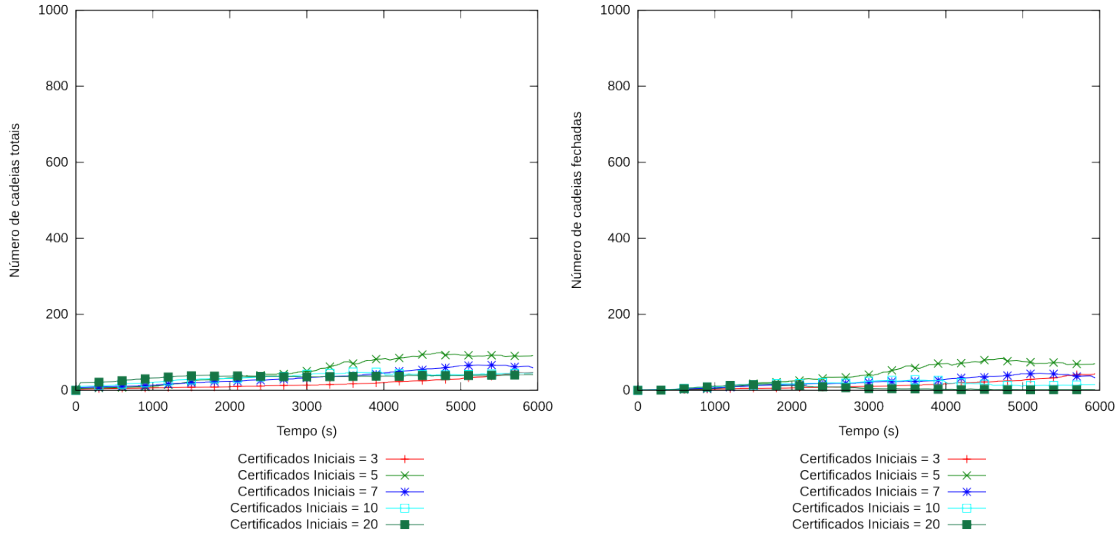
Nas Figuras 4.21 e 4.22 estão os resultados para $m = 10\%$ e $N_a = 10\%$. Nota-se que em nenhum dos casos a quantidade de cadeias abertas chegou ao número de nodos presentes nas simulações. Isso dá-se devido à forma como os nodos tratam os reconhecidos como maliciosos.

Ao receber uma cadeia para um nodo que ainda seja desconhecido, o nodo aceita a chave presente nela como verdadeira e acredita que os nodos que a compõe não são maliciosos. Entretanto, ao receber outra cadeia que possua uma chave diferente para a mesma origem, os primeiros nodos que certificaram as chaves em ambas as cadeias recebidas são considarados prováveis maliciosos.

Deste momento em diante, todas as cadeias que chegam ao nodo e que tem início com um certificado emitido por esses prováveis maliciosos deixam de ser repassadas para os outros nodos. Essa situação é mantida até que o nodo origem seja encontrado e ele confirme alguma das chaves. Se nenhuma chave for validada pela origem, ambos os nodos são marcados como maliciosos. Caso um deles tenha a chave validada, ele volta a ter as cadeias repassadas e deixa de ser um provável maliciso, para que o outro nodo torne-se um malicioso reconhecido. Uma vez identificado como malicioso, um nodo não volta a ser considerado confiável.

Desta forma, o número esperado de cadeias abertas deixa de ser representado por $n$, mas por $n - (n * m)$. Por exemplo, nos cenários com 50 nodos e 10% de nodos maliciosos, o número esperado de cadeias abertas passa a ser de 45 nodos. Mas como pode ser observado, para 50 nodos, o maior valor para cadeias abertas foi para 20 certificados iniciais, que obteve uma quantidade pouco acima de 40. Já para $C_i = 10$, a quantidade chegou a 34 nodos ao fim dos seis mil segundos de simulação. Para 150 nodos, os resultados foram semelhantes. Com $C_i = 20$ os nodos chegaram ao fim do tempo com 135 nodos conhecidos, totalizando o número esperado de nodos.

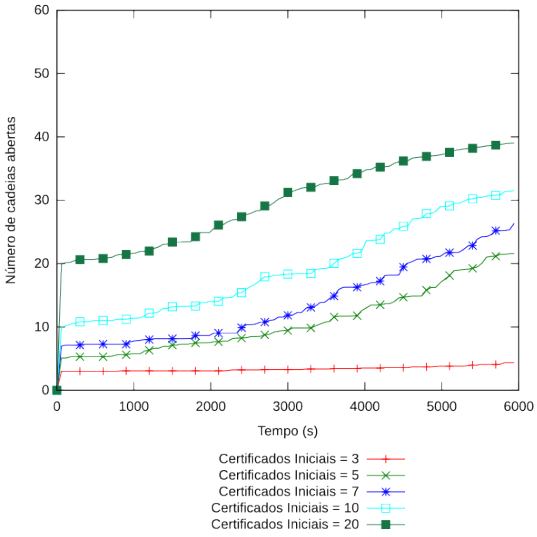
A quantidade de cadeias fechadas chegou a valores acima do padrão encontrado sem nodos atacantes. Isso deve-se ao fato de que embora as chaves de alguns nodos estejam corretas, elas foram certificadas apenas pelos nodos atacantes. Essas chaves deixam de ser repassadas até o momento que a origem da chave seja encontrada e possa validar a chave. Caso contrário, as cadeias são guardadas até atingir o limite de cadeias por nodo determinado. Mesmo sobre a situação de nodos falsificadores na rede, o tamanho médio das cadeias permanceu próximo de 3, indicando o uso de apenas um intermediário para a criação de cadeias.



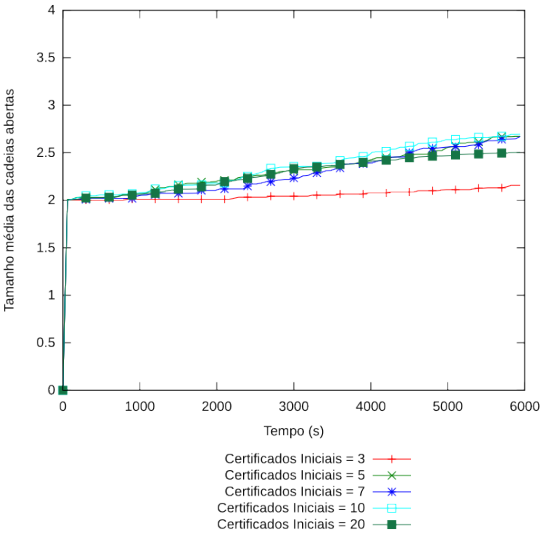

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



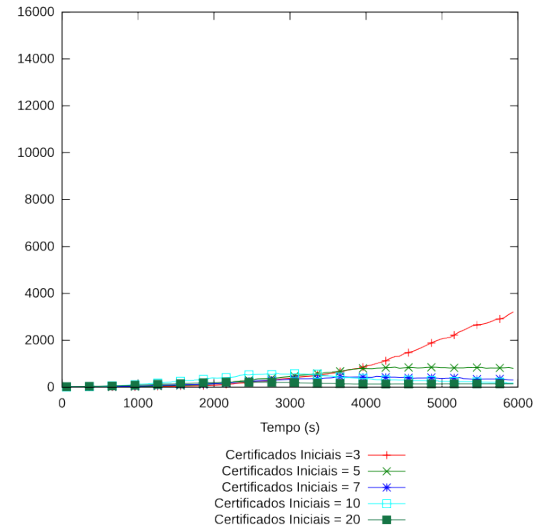

(c) Número de cadeias Abertas



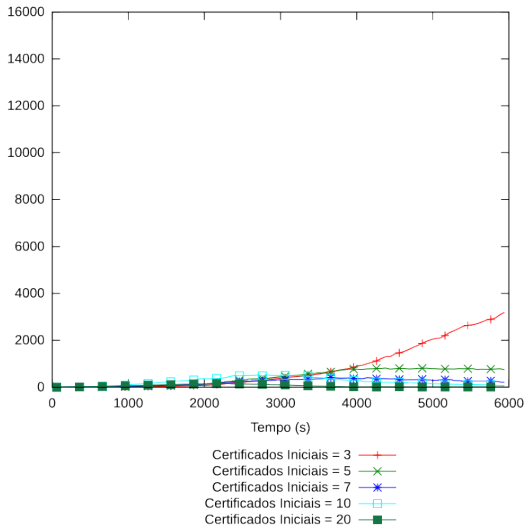

(d) Tamanho médio das cadeias

Figura 4.23: Resultados para 50 nodos, $m = 10\%$ e $N_a = 50\%$

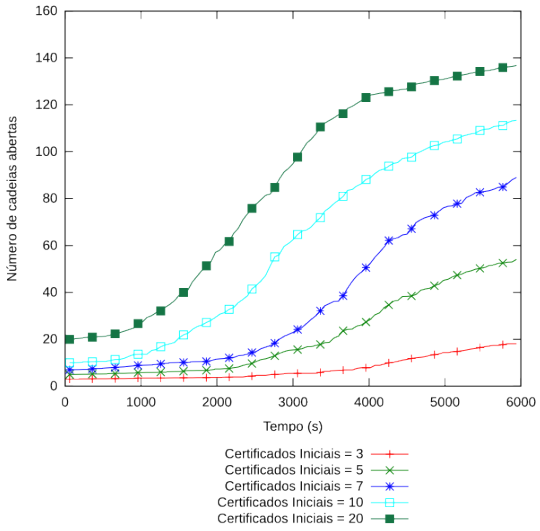
As Figuras 4.23 e 4.24 mostram os resultados de $m = 10\%$ e $N_a = 50\%$ para 50 e 150 nodos respectivamente. Para esse cenário, a quantidade de cadeias fechadas foi bem pequena, com relação aos demais, sendo menor que no cenário sem atacantes, inclusive. Essa situação inesperada aconteceu tanto para 50 quanto para 150 nodos. As cadeias abertas ficaram um pouco acima do esperado, para 150 nodos e $C_i = 20$, demonstrando que alguns nodos atacantes não foram descobertos por todos os nodos da rede. Com 50 nodos, o resultado das cadeias abertas foi semelhante ao encontrado anteriormente.



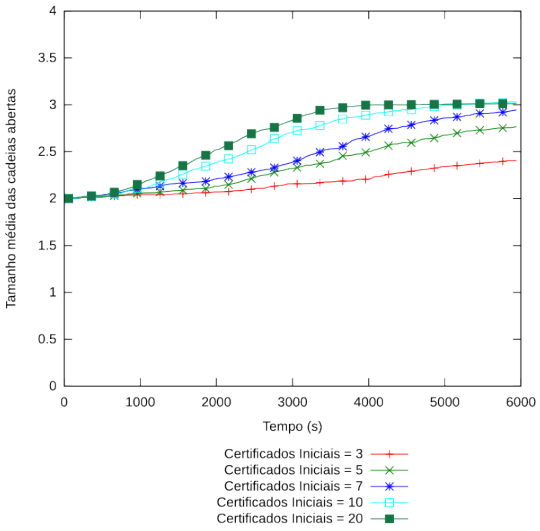

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



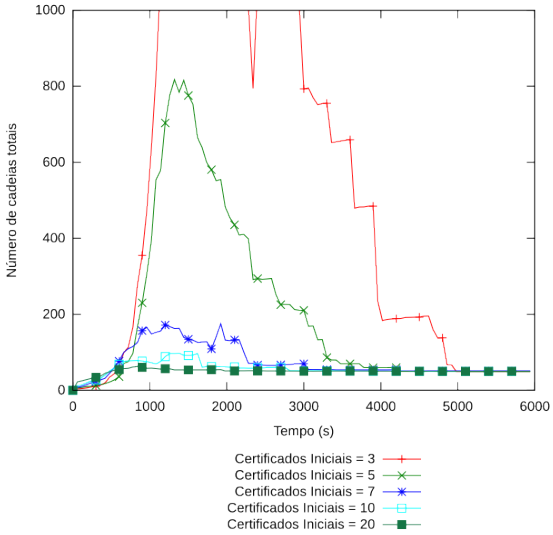

(c) Número de cadeias Abertas



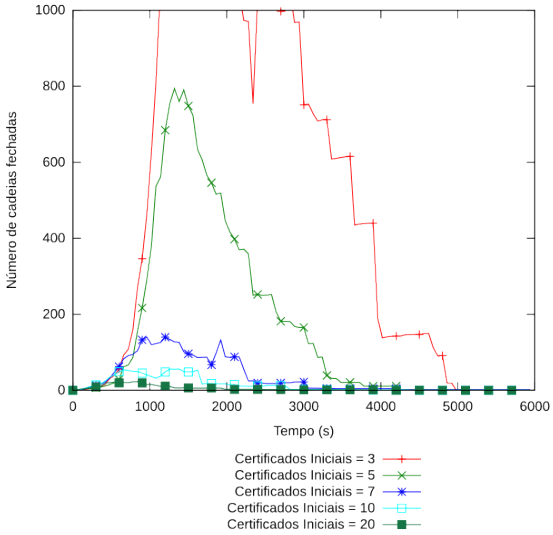

(d) Tamanho médio das cadeias

Figura 4.24: Resultados para 150 nodos, $m = 10\%$ e $N_a = 50\%$

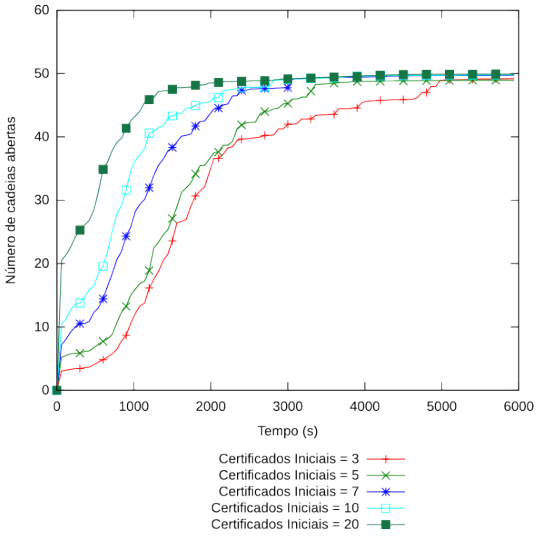
Já nas Figuras 4.25 e 4.26 estão os resultados de $m = 50\%$ e $N_a = 10\%$ para 50 e 150 nodos e pode-se ver que a quantidade de cadeias abertas atingiu o número de nodos da rede em ambos os casos. Isso demonstra que nodos atacantes em alta quantidade são confundidos mais facilmente com nodos não atacantes.



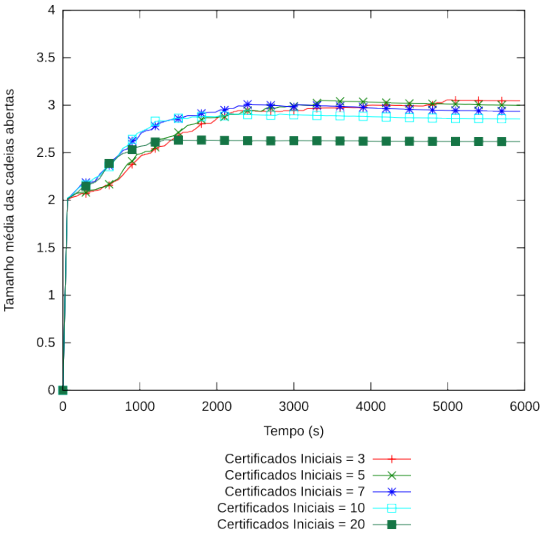

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



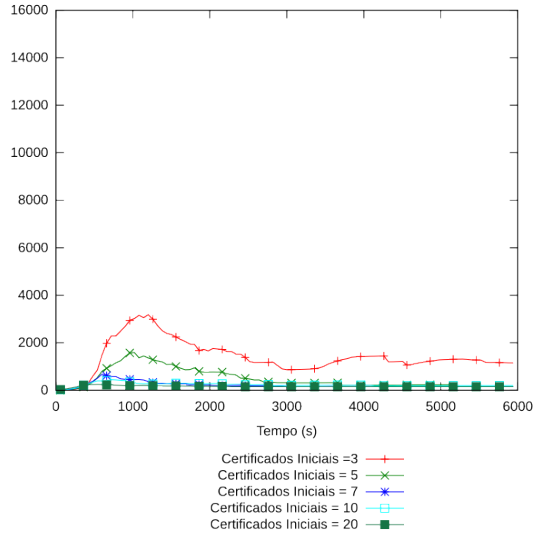

(c) Número de cadeias Abertas



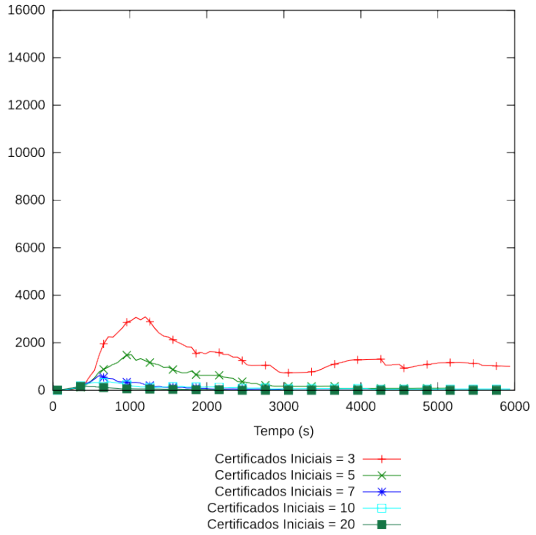

(d) Tamanho médio das cadeias

Figura 4.25: Resultados para 50 nodos, $m = 50\%$ e $N_a = 10\%$

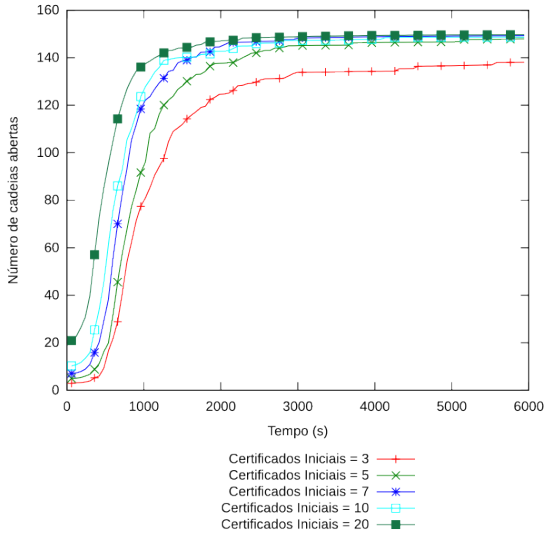
As cadeias fechadas tiveram um padrão semelhante a um cenário sem ataque, com exceção do cenário de 50 nodos e $C_i = 3$, que obteve uma quantidade de cadeias fechadas elevada por grande parte do tempo de vida da rede. Mais próximo do final da simulação, essa quantidade teve quedas acentuadas e atingiu a estabilidade em zero ou, próximo dele.



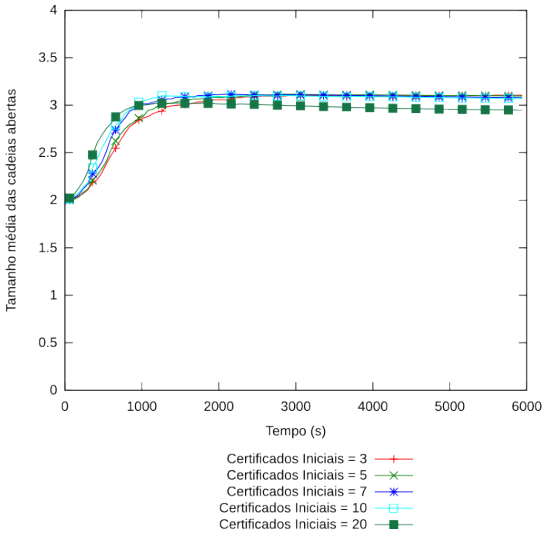

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



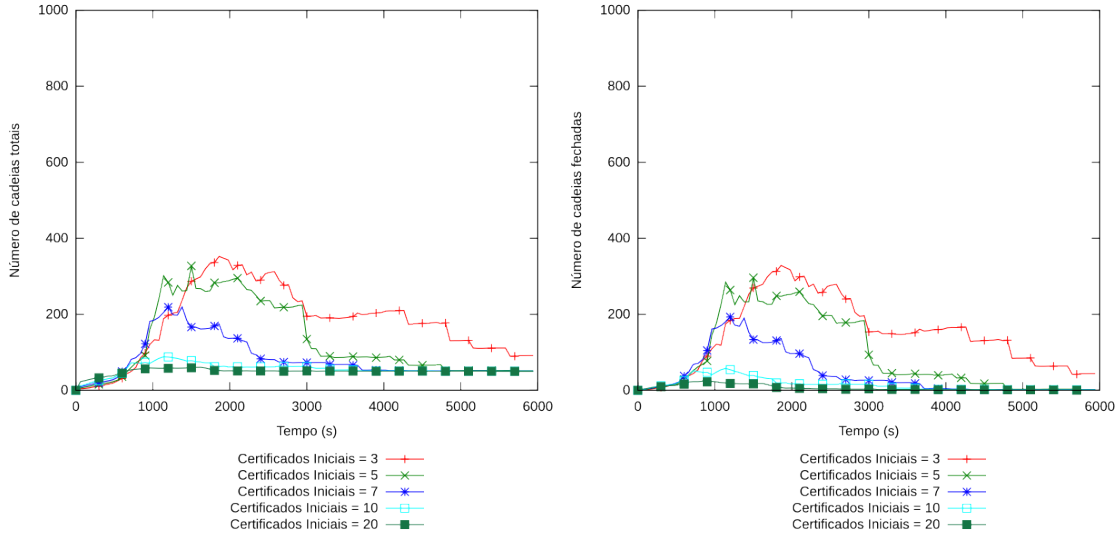

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura 4.26: Resultados para 150 nodos, $m = 50\%$ e $N_a = 10\%$

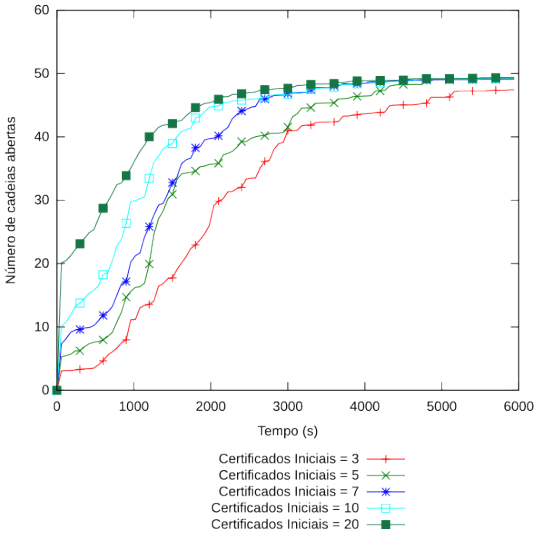
Os resultados para 50 e 150 nodos com $m = 50\%$ e $N_a = 50\%$ estão nas Figuras 4.27 e 4.28. Nos dois resultados de cadeias abertas pode-se ver que o número de nodos foi atingido ou, atingiu valores muito próximos deste. A quantidade de cadeias fechadas foi similar ao cenários sem atacantes.



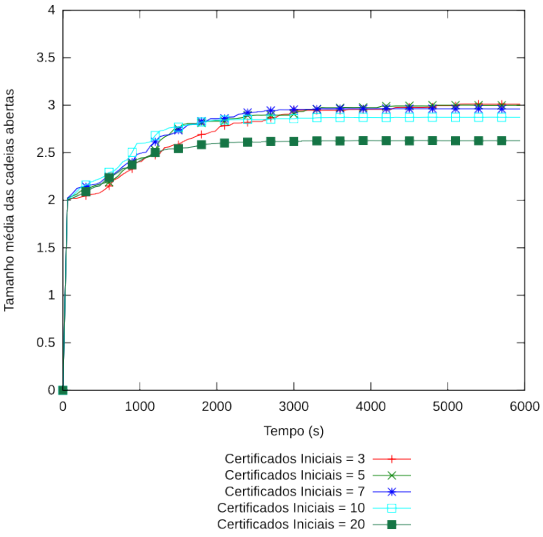

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



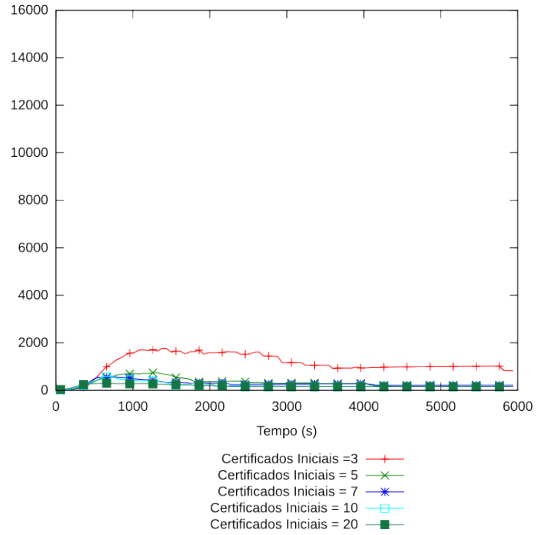

(c) Número de cadeias Abertas



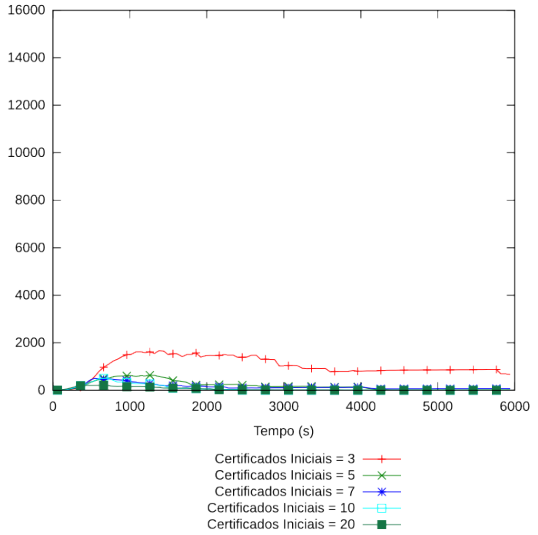

(d) Tamanho médio das cadeias

Figura 4.27: Resultados para 50 nodos, $m = 50\%$ e $N_a = 50\%$

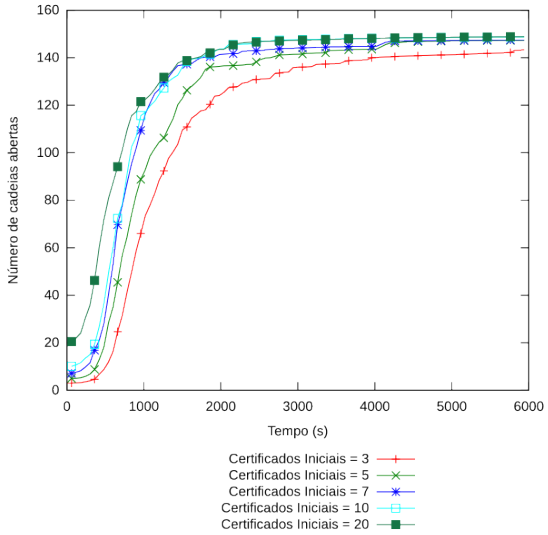
Isso demonstra que os nodos maliciosos, quando estão presentes em grandes quantidades na rede e durante o tempo simulado, permanecem entre os nodos não maliciosos sem serem descobertos. Essa situação não é conveniente para a rede e esse ponto destaca-se como uma possibilidade de melhoria futura do esquema.



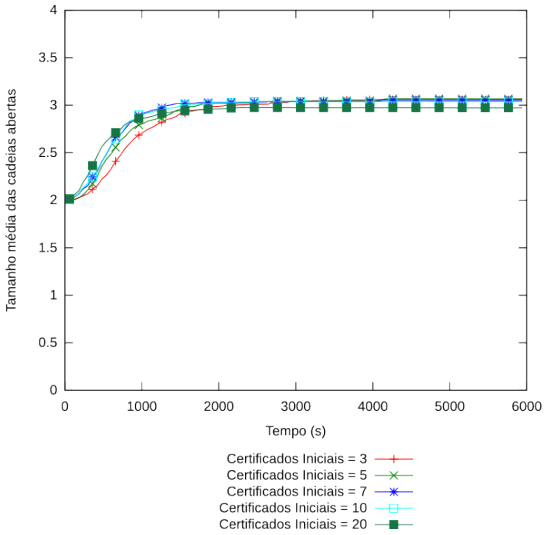

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

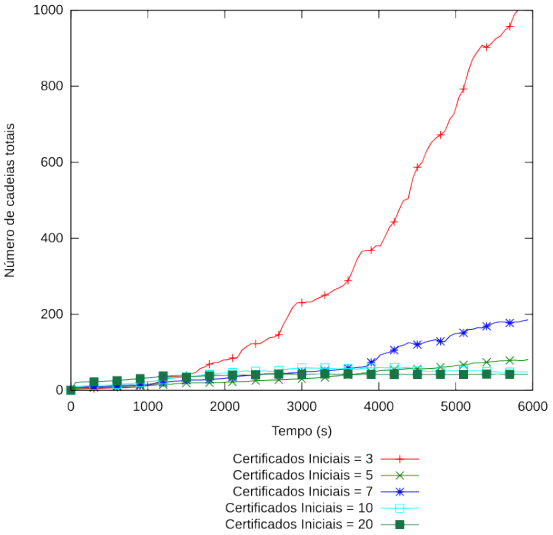



(d) Tamanho médio das cadeias

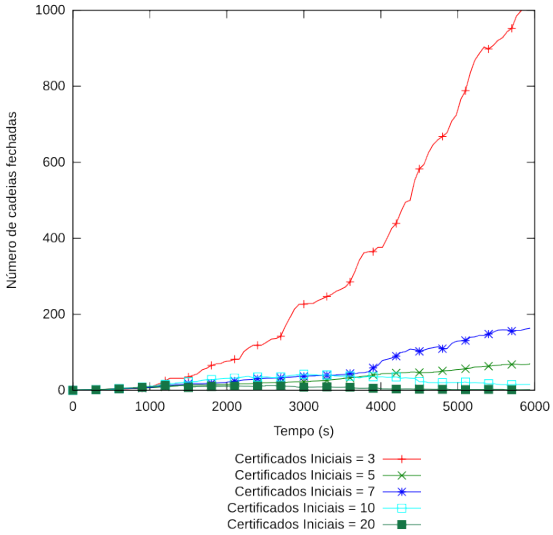
Figura 4.28: Resultados para 150 nodos, $m = 50\%$ e $N_a = 50\%$

Os resultados de parâmetros não apresentados nesta sessão, estão no Apêndice C.

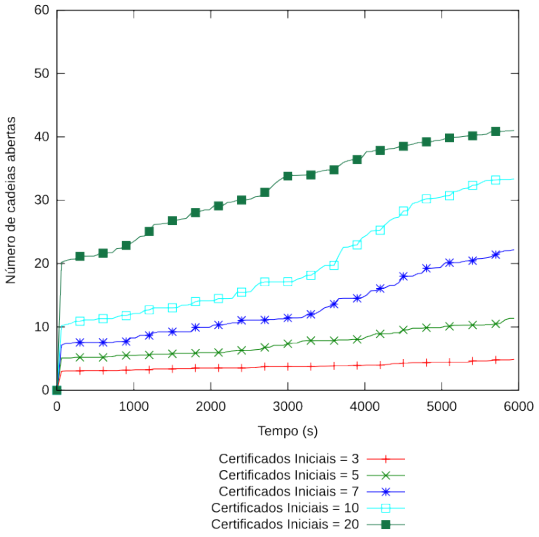
Todos os nodos maliciosos nos resultados apresentados eram independentes, ou seja, se dois nodos atacassem o mesmo nodo, eles usariam chaves falsas diferentes. Assim, pensou-se na possibilidade de os nodos maliciosos usarem a mesma chave falsa para um mesmo alvo, em uma tentativa mais planejada de afetar a rede.



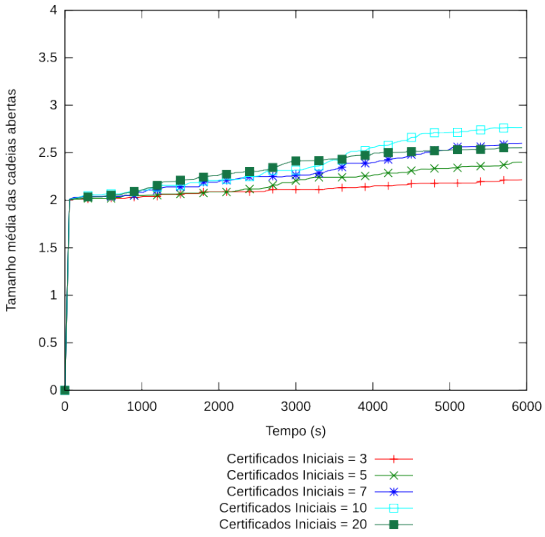

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



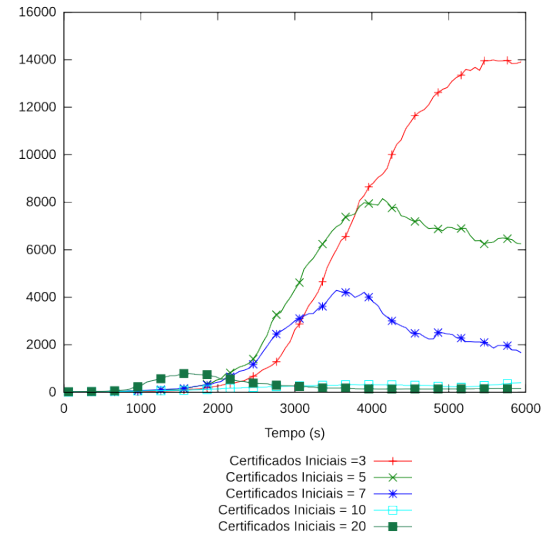

(c) Número de cadeias Abertas



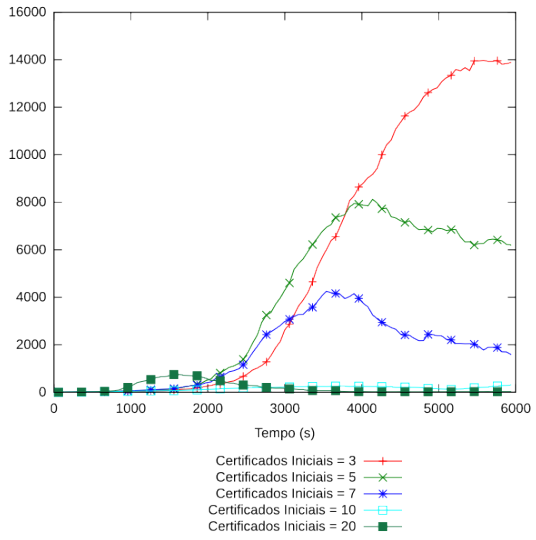

(d) Tamanho médio das cadeias

Figura 4.29: Resultados para 50 nodos, $m = 10\%$ e $N_a = 10\%$ com ataque em grupo

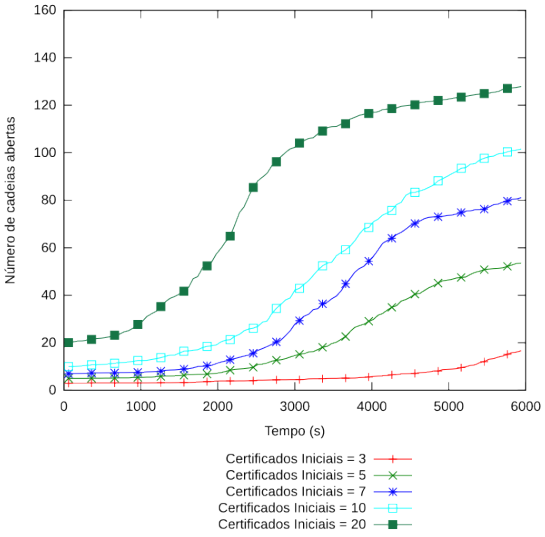
As Figuras 4.29 e 4.30 mostram os resultados obtidos para essa nova situação quando $m = 10\%$ e $N_a = 10\%$. Observa-se que todos os gráficos são bastante semelhantes aos encontrados anteriormente nos ataques independentes.



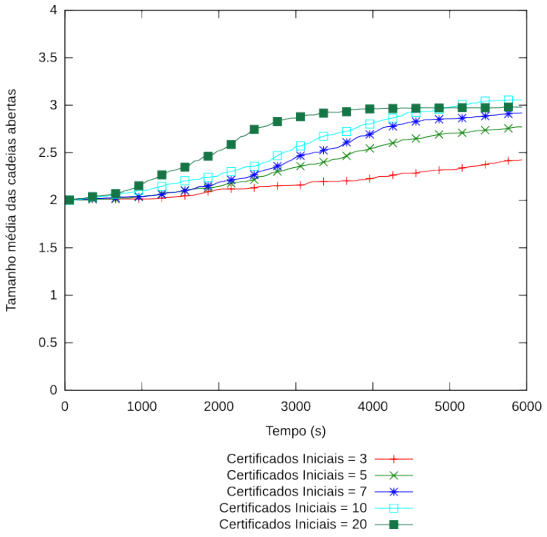

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



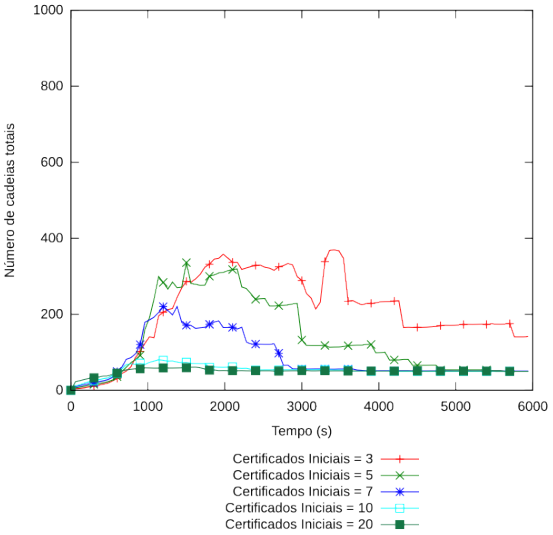

(c) Número de cadeias Abertas



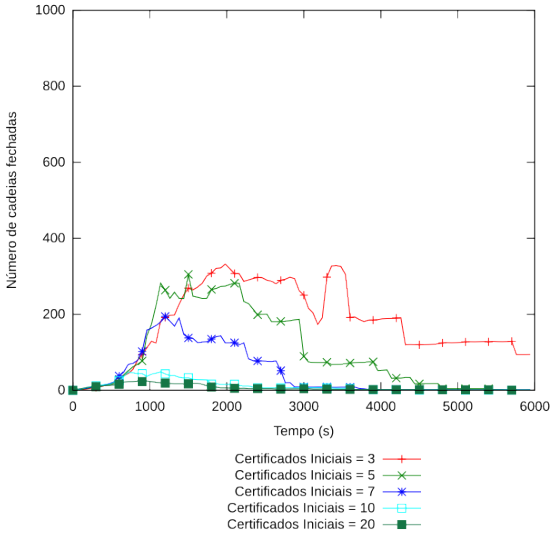

(d) Tamanho médio das cadeias

Figura 4.30: Resultados para 150 nodos, $m = 10\%$ e $N_a = 10\%$ com ataque em grupo

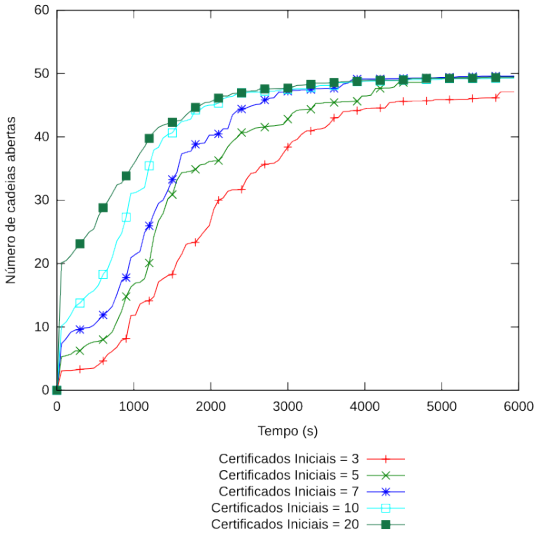
As Figuras 4.31 e 4.32 contêm os resultados para $m = 50\%$ e $N_a = 50\%$ e pode-se observar, assim como nas figuras anteriores, que os valores encontrados foram similares aos já apresentados.



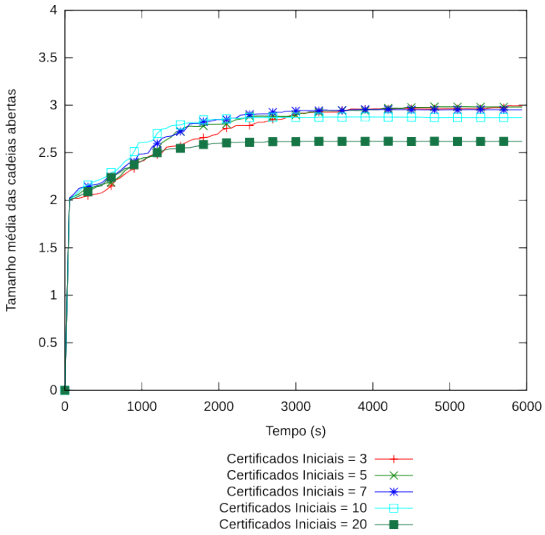

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



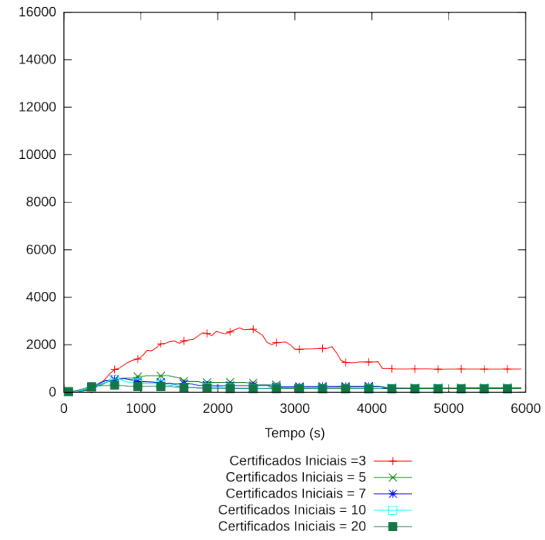

(c) Número de cadeias Abertas



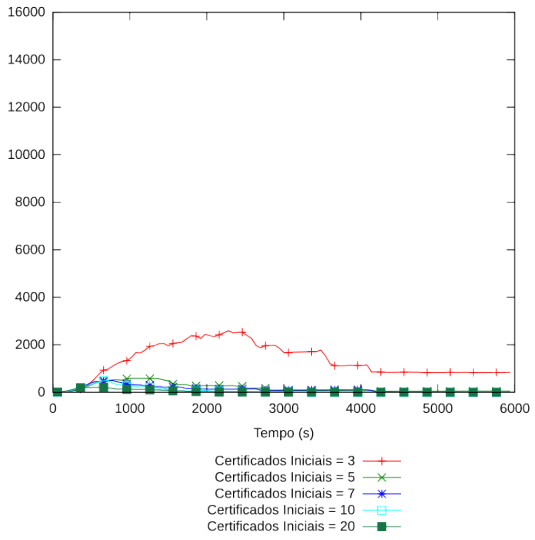

(d) Tamanho médio das cadeias

Figura 4.31: Resultados para 50 nodos, $m = 50\%$ e $N_a = 50\%$ com ataque em grupo

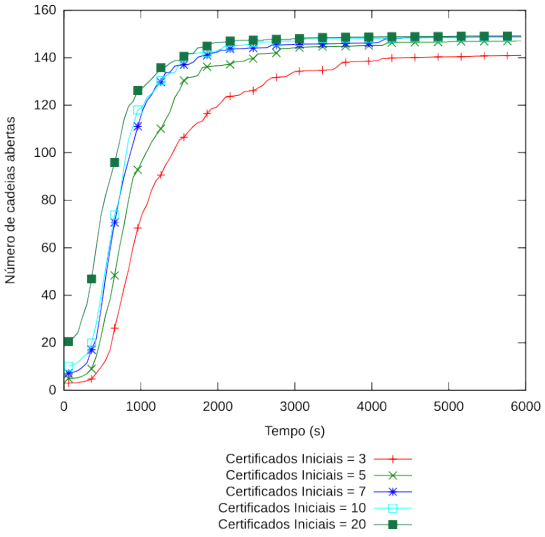
Como visto, seja o ataque de falsificação com os nodos maliciosos usando chaves diferentes, ou seja, usando a mesma chave falsa para o mesmo nodo alvo, ele apresenta resultados muito similares. Sendo assim, os demais resultados para esse tipo de ataque serão omitidos dessa sessão e são apresentados no Apêndice C.



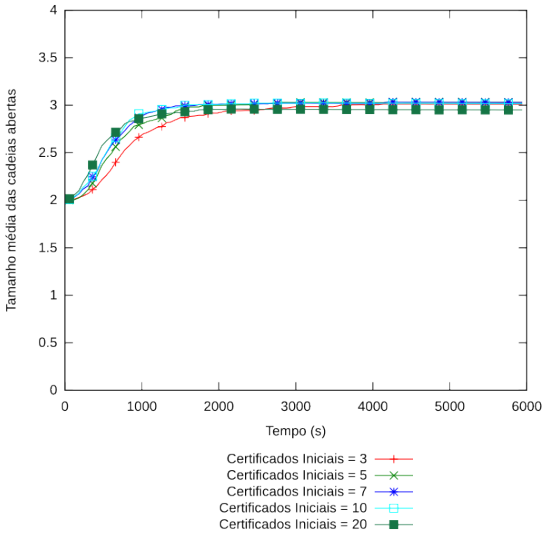

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

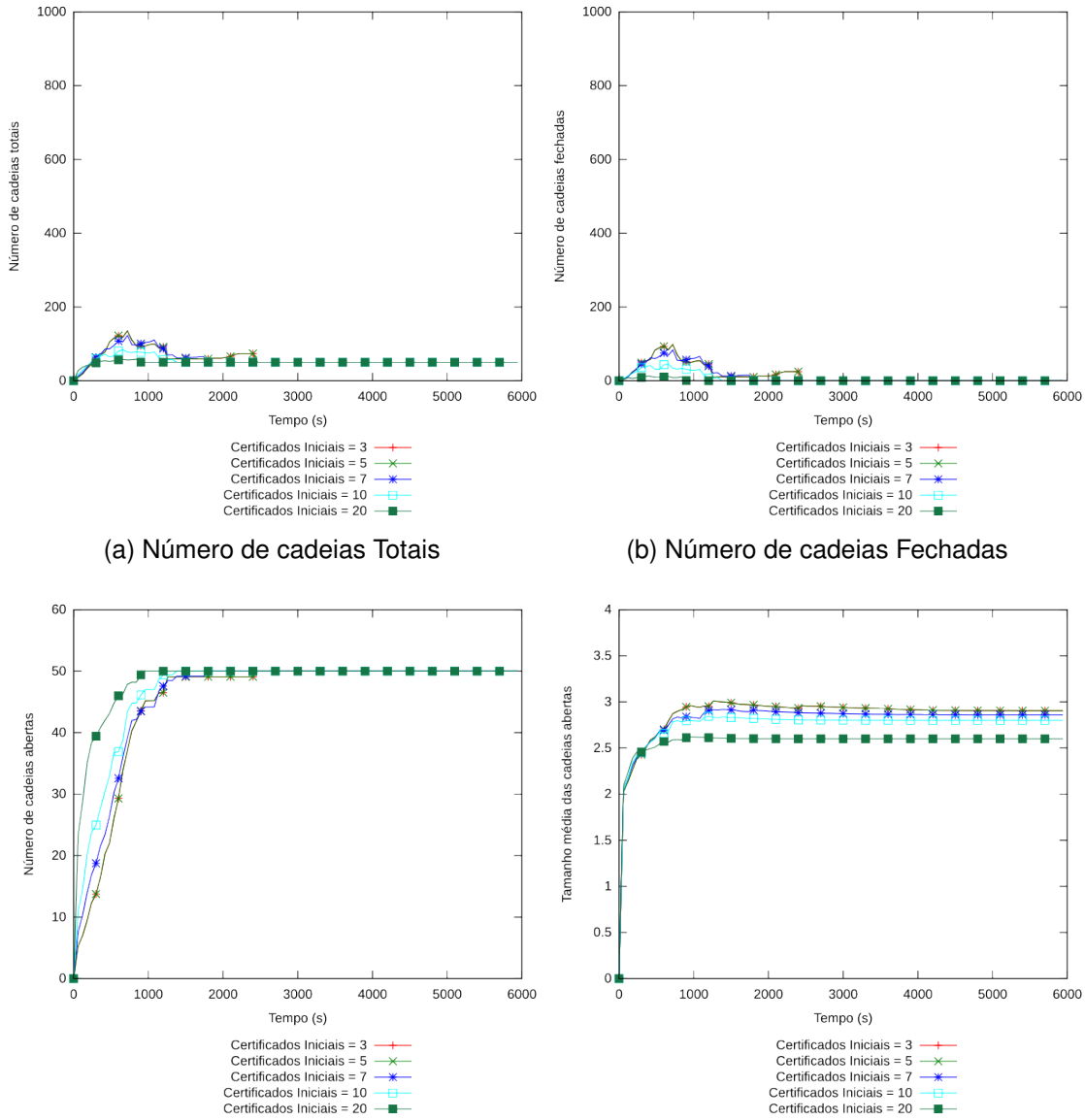
Figura 4.32: Resultados para 150 nodos, $m = 50\%$ e $N_a = 50\%$ com ataque em grupo

## 4.3 Resultados - Distribuição heterogênea de certificados iniciais

A seguir serão apresentados os resultados para a distribuição heterogênea de certificados iniciais. Os gráficos apresentados serão apenas para 50 e 150 nodos, os demais estão presentes no Apêndice C.

Nessa forma de distribuição de certificados iniciais, o valor de $C_i$ é usado como fator multiplicativo para estipular o máximo de certificados iniciais que haverão na rede. Desta forma, para $C_i = 10$ e 100 nodos, haverão 1000 certificados iniciais distribuídos de forma aleatória entre os nodos.

### 4.3.1 Simulações Iniciais




(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

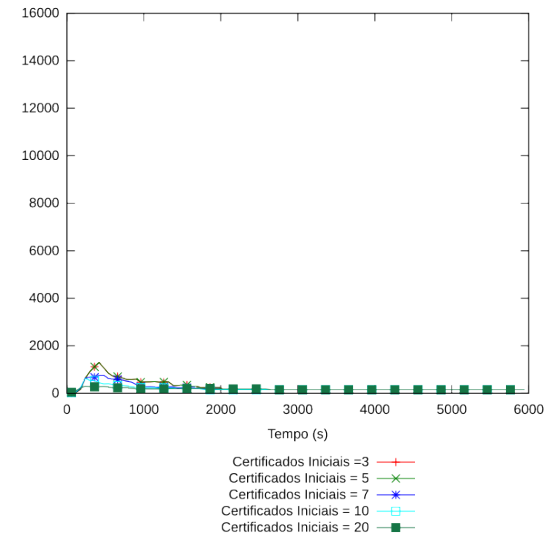
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

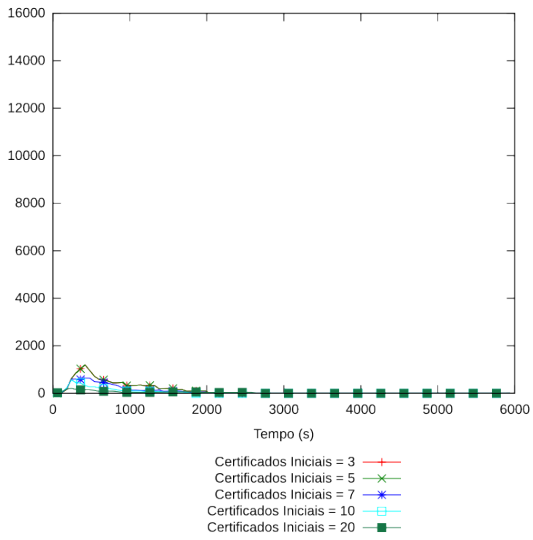
Figura 4.33: Resultados para 50 nodos

Nas Figuras 4.33 e 4.34 estão os resultados do esquema proposto em um ambiente livre de atacantes e com distribuição heterogênea dos certificados iniciais.

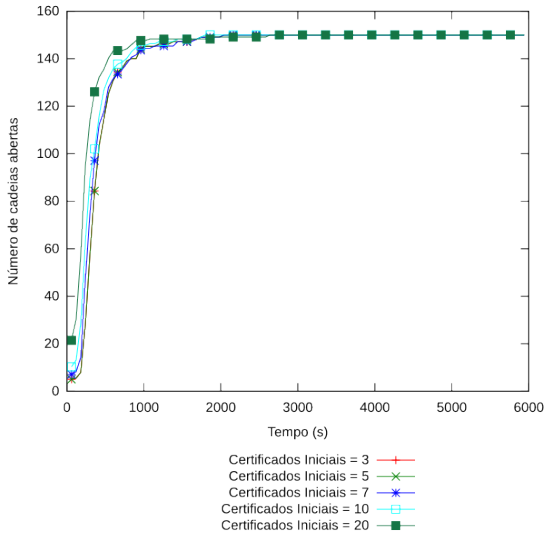
Pode-se ver que a mudança na forma de distribuição dos certificados iniciais não afetou negativamente o esquema. O tempo para convergência sofreu pouca alteração, tendo ele reduzido, em média, pouco mais de 2%. A diferença mais evidente entre os resultados dos dois modelos de distribuição foi a reduçao de cerca de 66% na quantidade de cadeias fechadas durante o instante de pico das simulações, para o fator multiplicativo igual a 3.



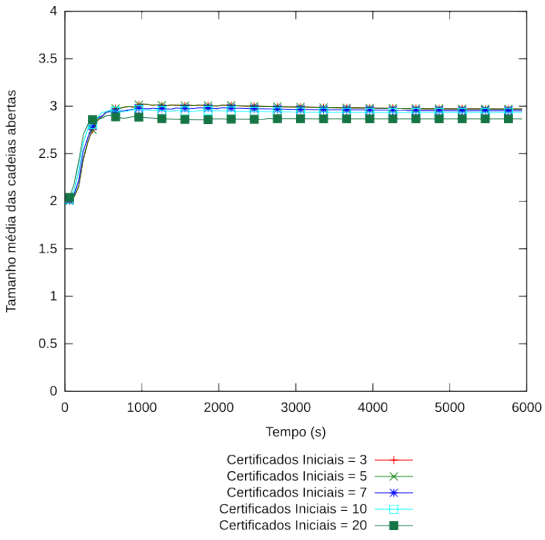

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura 4.34: Resultados para 150 nodos

Pode-se notar que mesmo com a mudança na forma de distribuição, o esquema conseguiu convergir ao ponto no qual todos os nodos possuem cadeias abertas para

os outros nodos da rede. A quantidade de cadeias armazenadas durante as simulações manteve-se muito similar aos resultados encontrados anteriormente, com exceção do valor para $C_i = 3$, que obteve uma queda significativa. O tamanho médio das cadeias abertas manteve-se próximo a 3, indicando ainda o uso de um intermediário.

### 4.3.2 Ataques

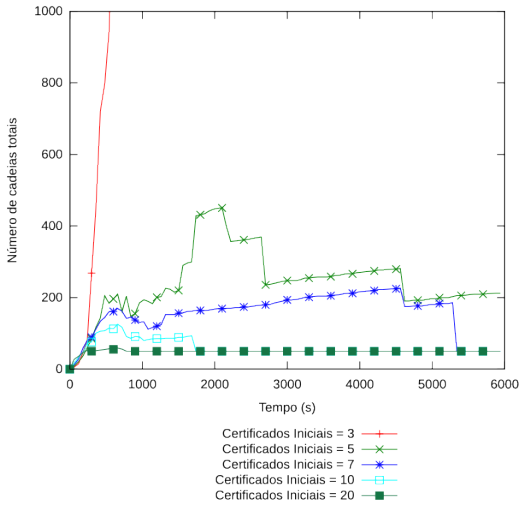
Assim como na forma de distribuição homogênea de certificados iniciais, foram feitas simulações em ambientes com nodos maliciosos executando ataques diversos.

#### 4.3.2.1 Ataque *GreyHole*

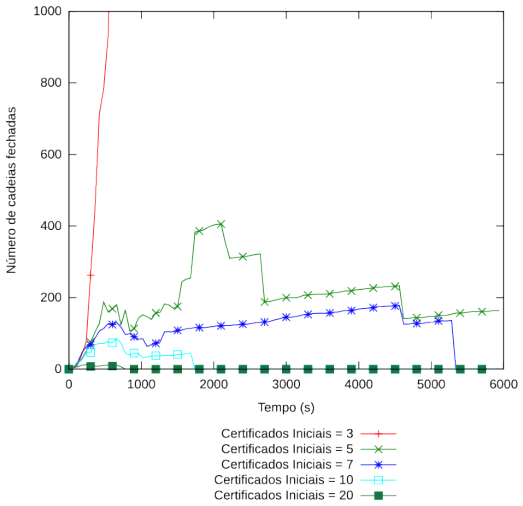
A forma do ataque não foi alterada do usado na distribuição homogênea de certificados iniciais. Os nodos maliciosos ($m$) descartam mensagens seguindo todos a mesma taxa ($t$).

Nas Figuras 4.35 e 4.36 estão os resultados obtidos para 50 e 150 nodos, respectivamente, com $m = 10\%$ e $t = 10\%$.

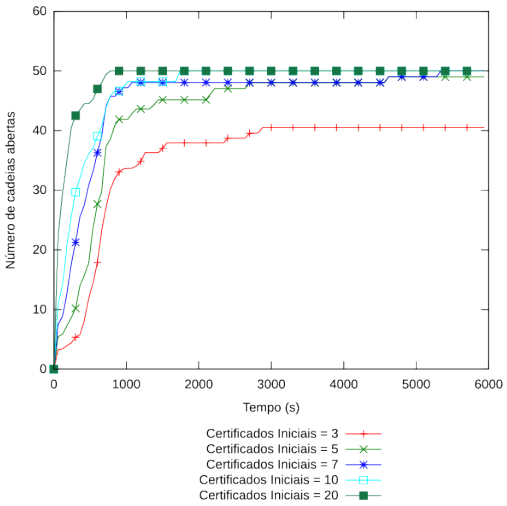
Na Figura 4.35 pode ver que nesse tipo de ataque e distribuição de certificados iniciais, o esquema conseguiu convergir totalmente, no tempo de simulação, para $C_i > 5$, e de forma satisfatória para $C_i = 5$. Entretanto, não obteve o mesmo resultado para $C_i = 3$, na qual a quantidade de cadeias abertas atingiu pouco mais de 80%. A quantidade de cadeias totais ficou limitada pelo tamanho do *buffer* de cada nodo.



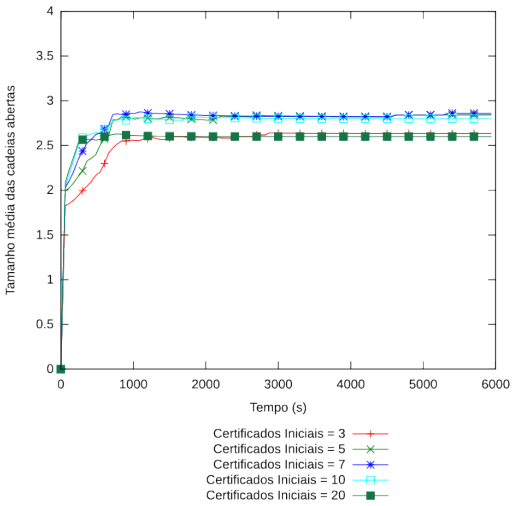

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



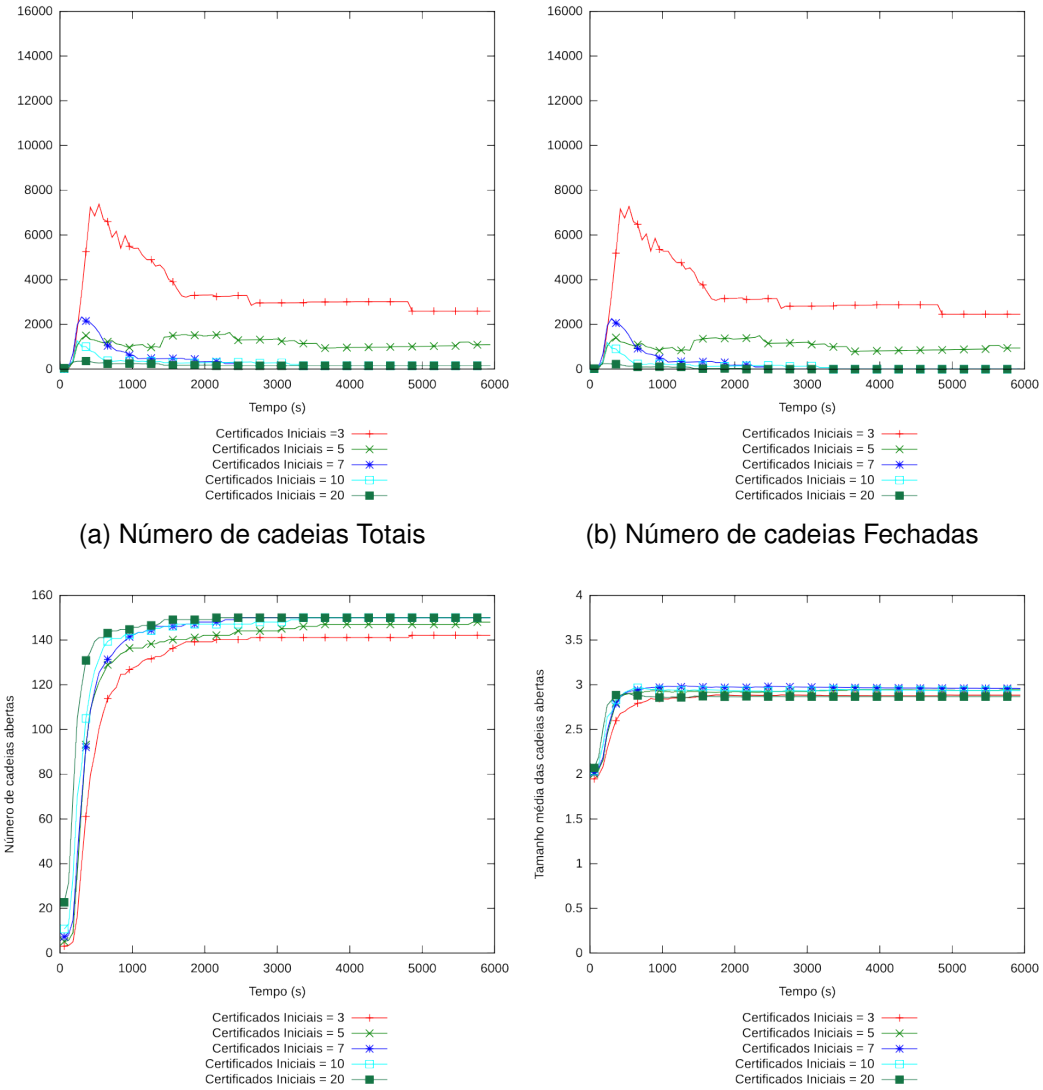

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura 4.35: Resultados para 50 nodos, $m = 10\%$ e $t = 10\%$

O mesmo problema não aconteceu para 150 nodos, como pode ser visto na Figura 4.36. Embora o esquema não tenha convergido totalmente para $C_i <= 5$, a quantidade total de cadeias não atingiu valores altos como os encontrados com 50 nodos. A quantidade de cadeias abertas ao final das simulações ficou acima dos 90%.




(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

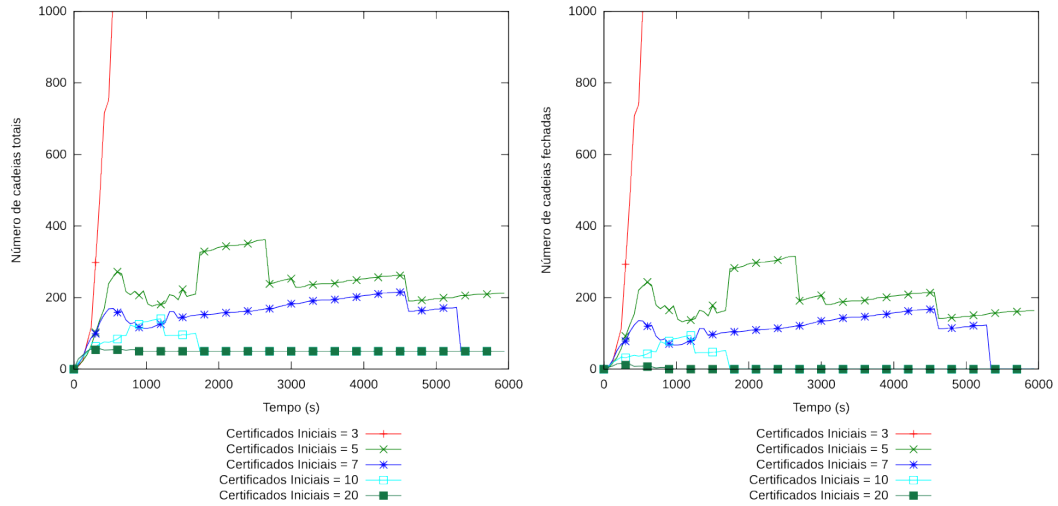
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

Figura 4.36: Resultados para 150 nodos, $m = 10\%$ e $t = 10\%$

Nas Figuras 4.37 e 4.38 estão os resultados obtidos de com $m = 10\%$ e $t = 50\%$ para 50 e 150 nodos.

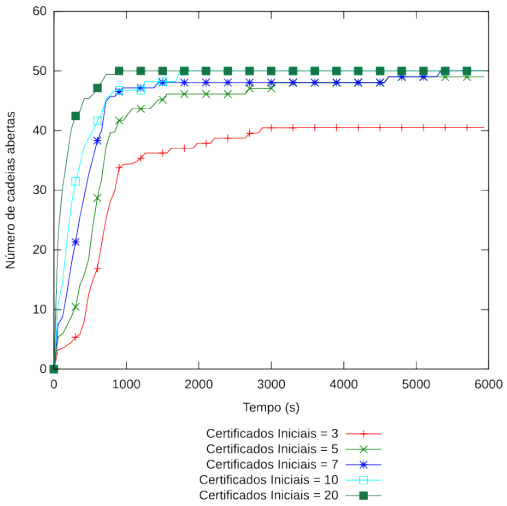
Os resultados foram muito similares entre os dois valores de $t$. A quantidade de cadeias abertas manteve-se pouco acima dos 80% para $C_i = 3$ e 50 nodos e a quantidade de cadeias totais novamente ficou limitada pelo tamanho de *buffer* dos nodos.



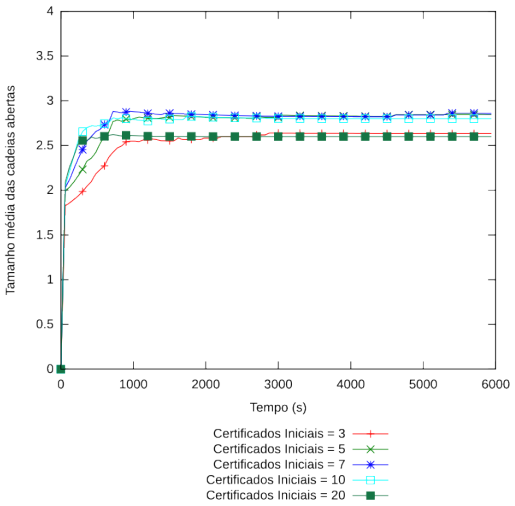

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

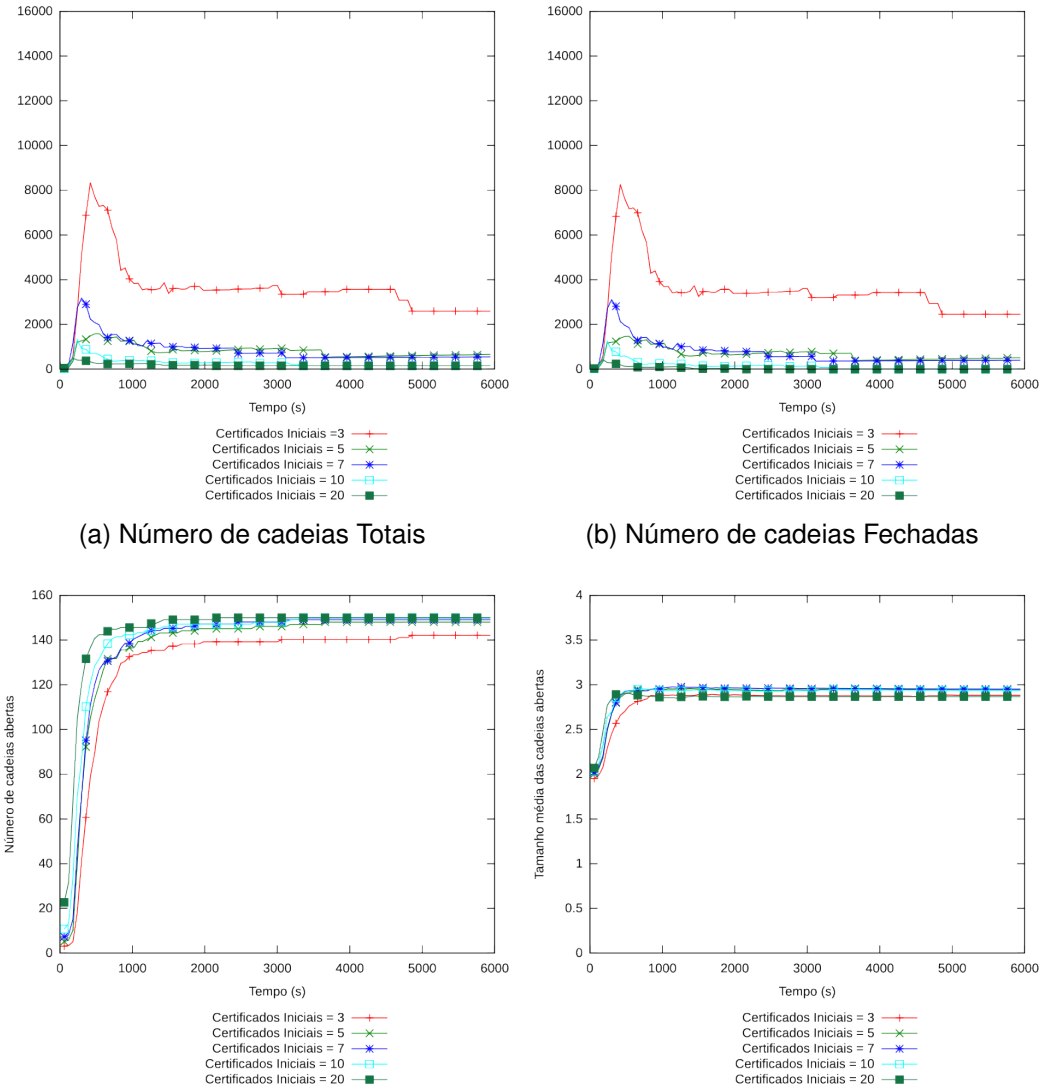



(d) Tamanho médio das cadeias

Figura 4.37: Resultados para 50 nodos, $m = 10\%$ e $t = 50\%$

A similaridade dos resultados com os encontrados para $t = 10\%$ mantiveram-se para 150 nodos, como pode ser observado na Figura 4.38.

Nas Figuras 4.39 e 4.40 estão os resultados para 50 e 150 nodos com $m = 50\%$ e $t = 10\%$.




(a) Número de cadeias Totais

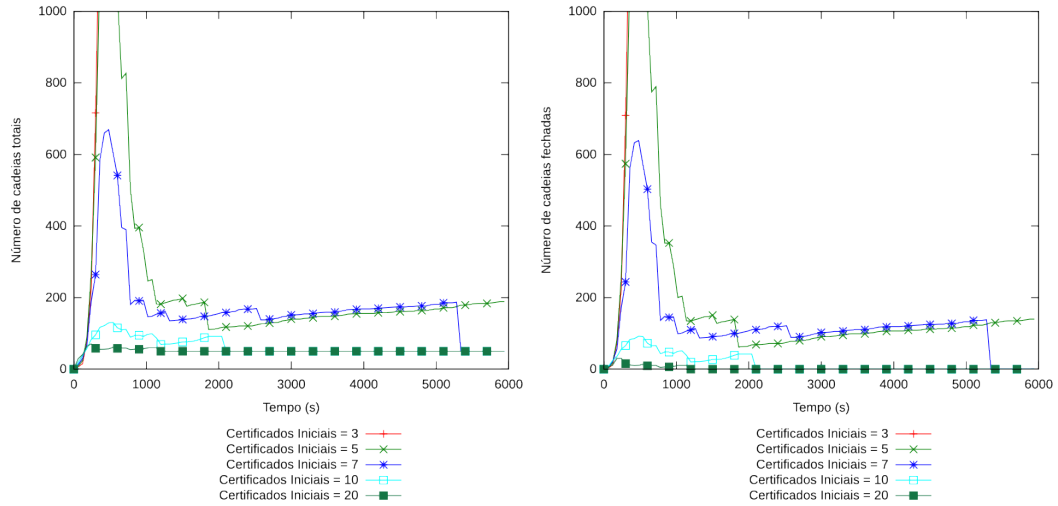
(b) Número de cadeias Fechadas

(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

Figura 4.38: Resultados para 150 nodos, $m = 10\%$ e $t = 50\%$

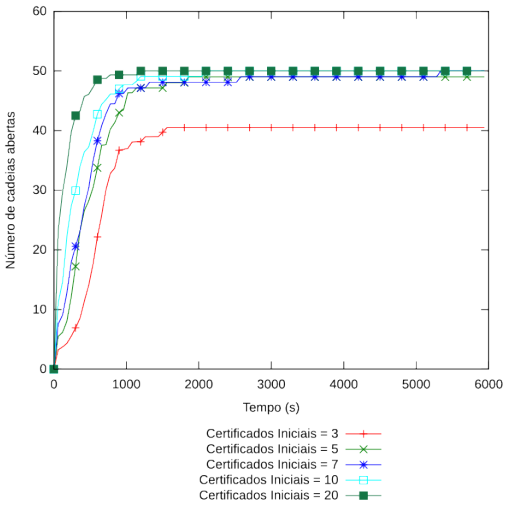
O problema com a quantidade de cadeias totais encontrado anteriormente para $C_i = 3$, foi extendido para $C_i = 5$ e $C_i = 7$, como pode ser visto na Figura 4.39. Entretanto, mesmo atingindo valores mais altos do que demonstrados antes, o esquema conseguiu convergir nesses dois casos.



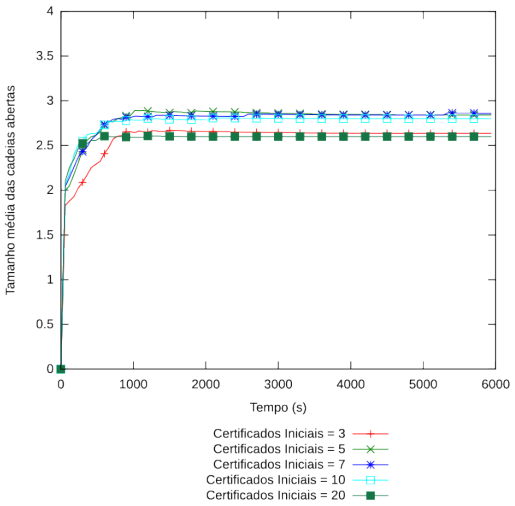

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

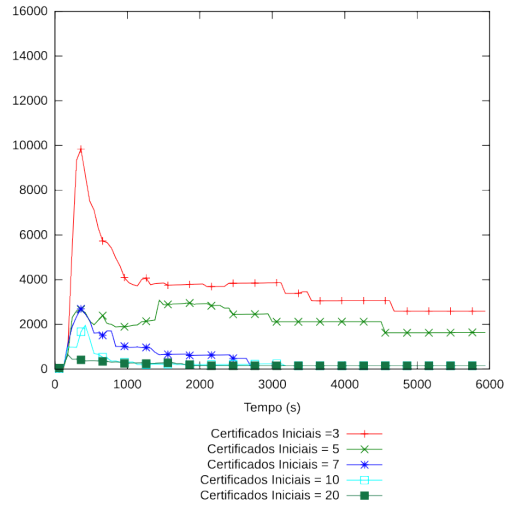



(d) Tamanho médio das cadeias

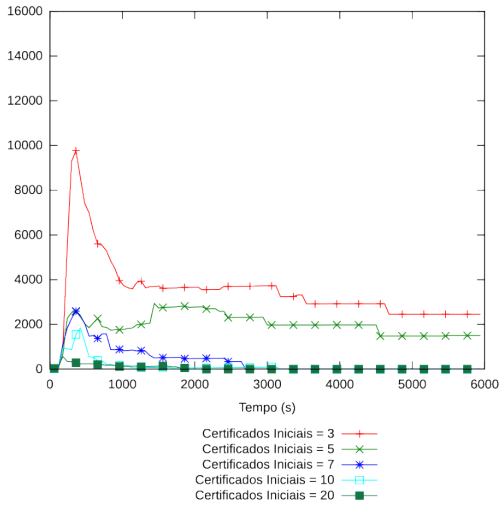
Figura 4.39: Resultados para 50 nodos, $m = 50\%$ e $t = 10\%$

Na Figura 4.40 pode-se notar que o esquema obteve resultados satisfatórios para todos os valores experimentados de certificados iniciais, mantedo ao final das simulações um percentual superior à 90% de cadeias abertas.

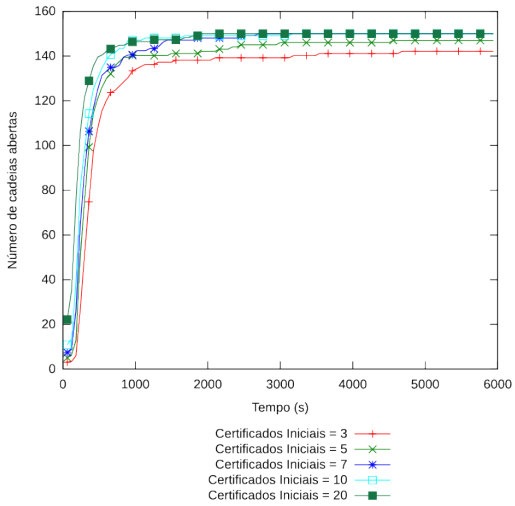
Na Figura 4.41 e na Figura 4.42 estão os resultados para o pior caso simulado nesse tipo de ataque, $m = 50\%$ e $t = 50\%$.



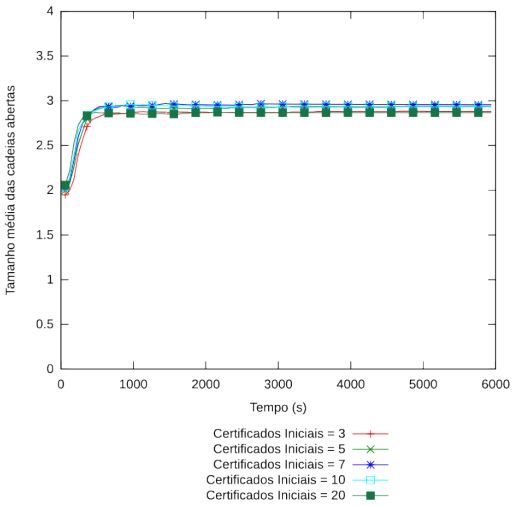

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

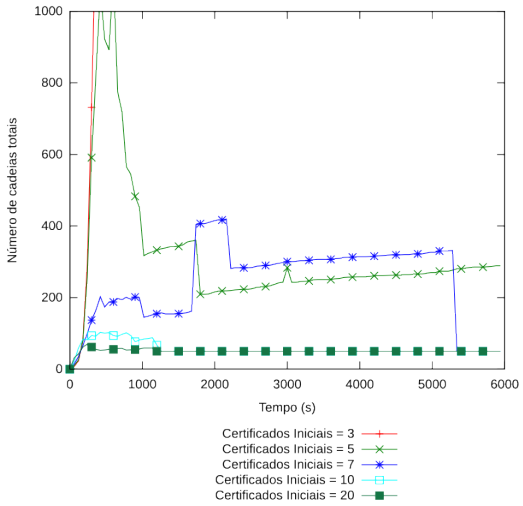



(d) Tamanho médio das cadeias

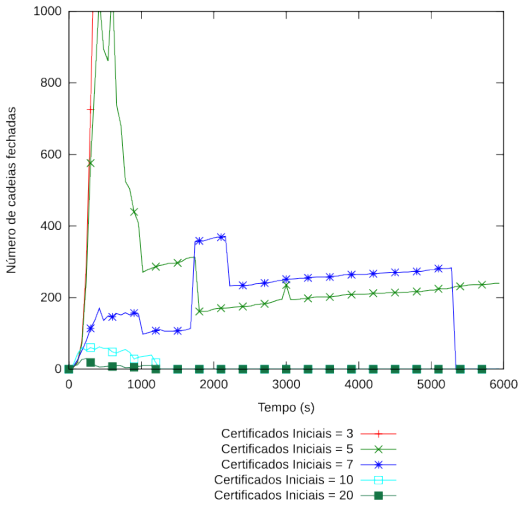
Figura 4.40: Resultados para 150 nodos, $m = 50\%$ e $t = 10\%$

A quantidade de cadeias totais continuou a atingir valores elevados aos encontrados anteriormente para $C_i <= 7$, mas novamente o esquema convergiu para um resultado no mínimo satisfatório, com exceção das simulações no qual $C_i = 3$.

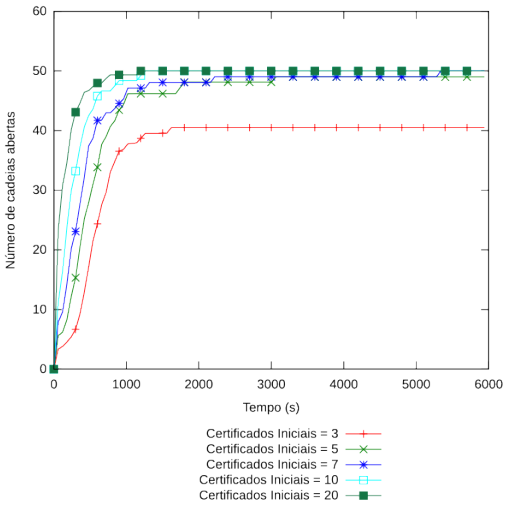
Na Figura 4.42 pode-se observar que para mais nodos, o esquema obtém melhores resultados, assim como nas diferentes quantidades de nodos maliciosos e taxas de descarte de mensagens simulados.



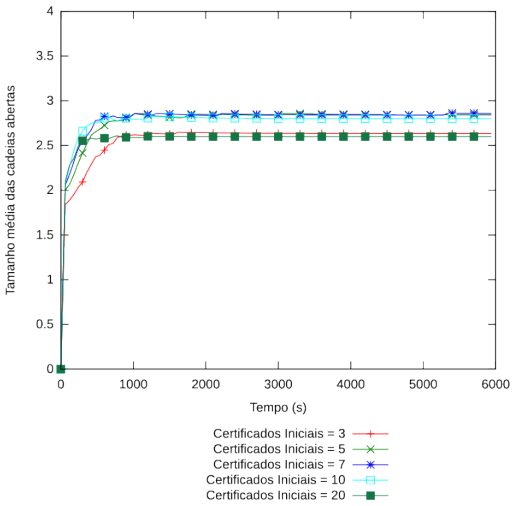

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

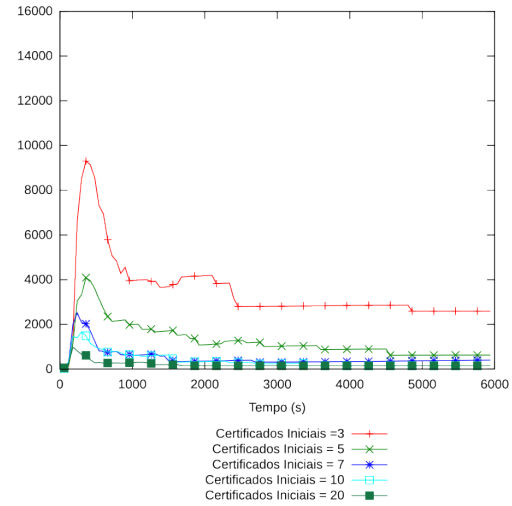



(d) Tamanho médio das cadeias

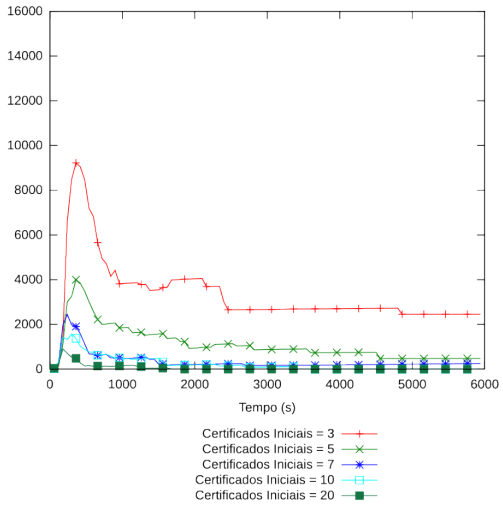
Figura 4.41: Resultados para 50 nodos, $m = 50\%$ e $t = 50\%$

Pode-se concluir que a mudança na distribuição dos certificados iniciais interferiu de forma significativa em comparação aos resultados encontrados na distribuição homogênea.

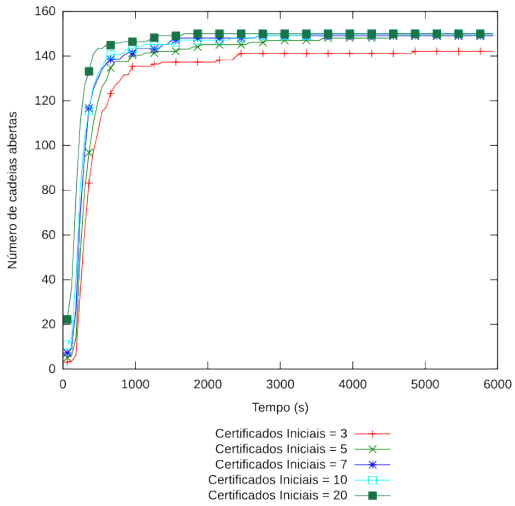
O esquema usou um pouco mais de recursos para armazenar cadeias e demorou um pouco mais para convergir e estabilizar, e quando o fez, foi de forma satisfatória, mas não completa.



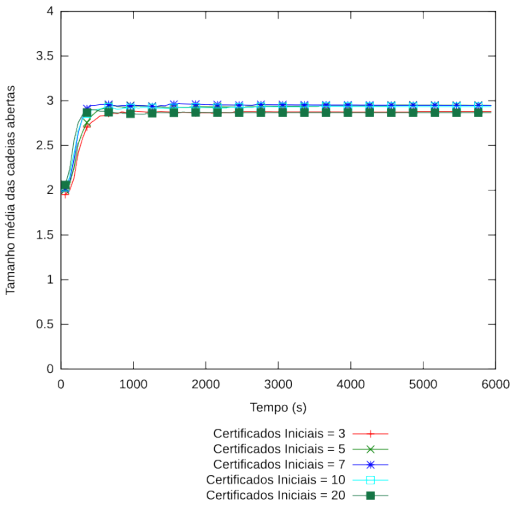

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

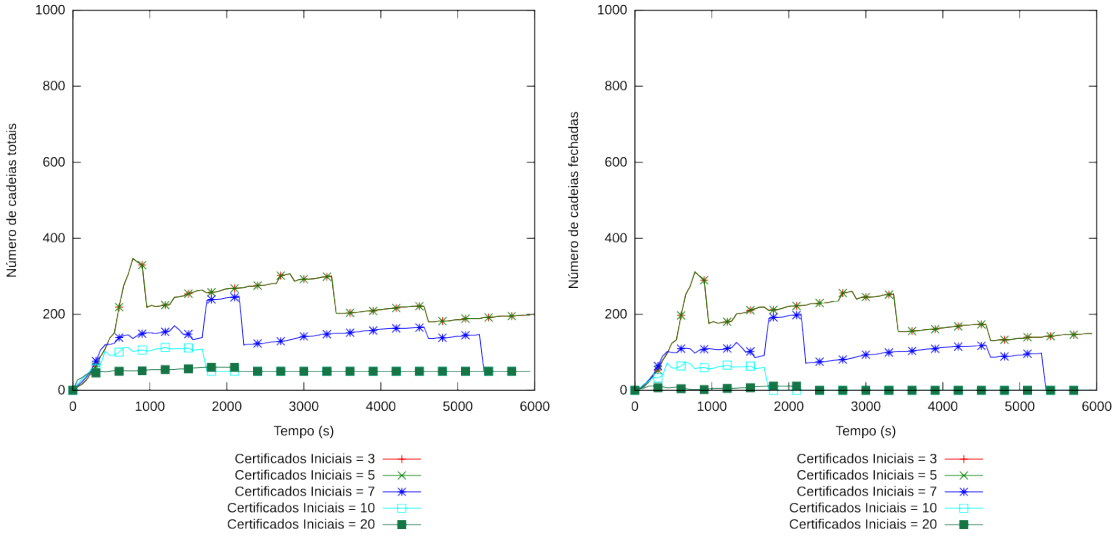



(d) Tamanho médio das cadeias

Figura 4.42: Resultados para 150 nodos, $m = 50\%$ e $t = 50\%$

#### 4.3.2.2 Ataque *BlackHole*

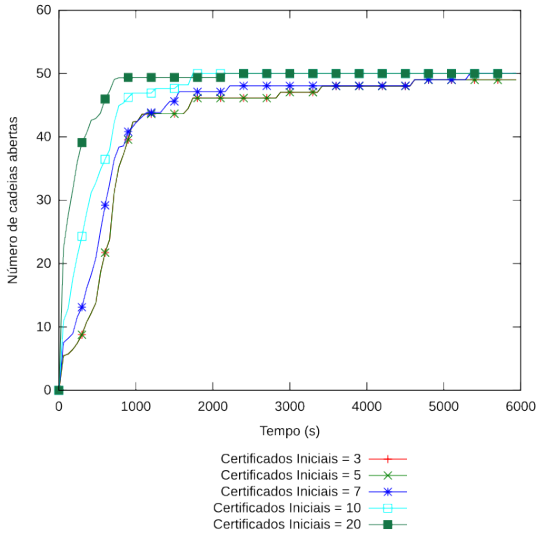
A forma como os nodos maliciosos realizam o ataque *BlackHole* não foi alterado. Cada simulação contava com uma quantidade $m$ de nodos maliciosos realizando o ataque, no qual todas as mensagens que chegavam até ele eram descartadas.



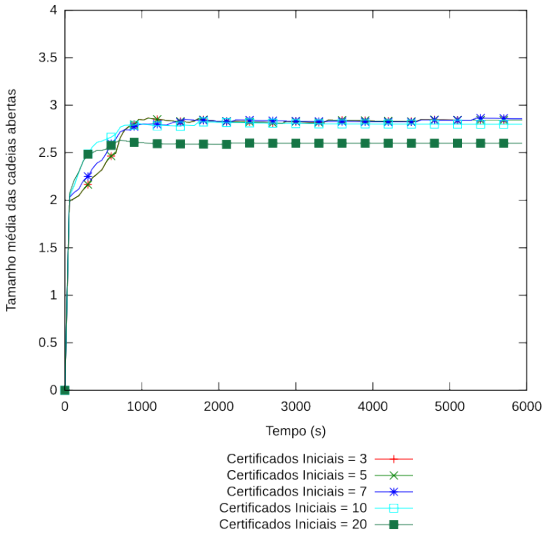

(a) Número de cadeias totais




(b) Número de cadeias fechadas




(c) Número de cadeias abertas

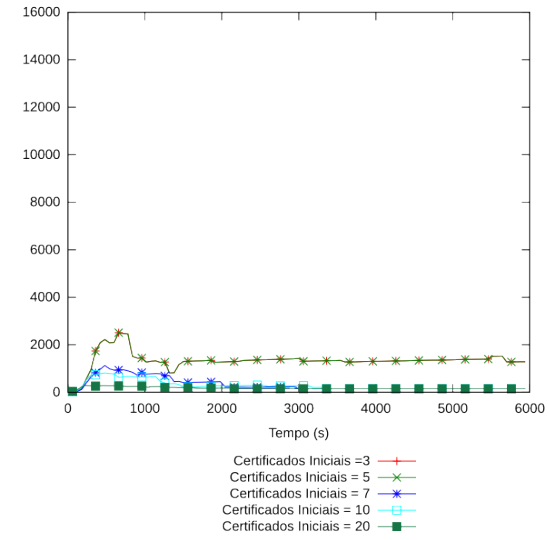



(d) Tamanho médio das cadeias

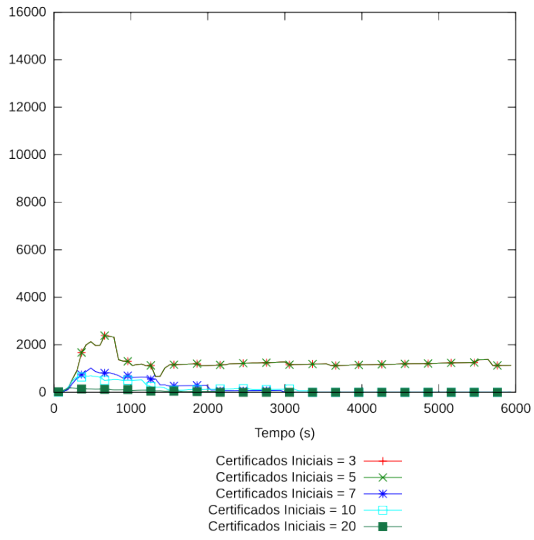
Figura 4.43: Resultados para 50 nodos e $m = 10\%$

Na Figura 4.43 e na Figura 4.44 estão os resultados para $m = 10\%$ em cenários com 50 e 150 nodos.

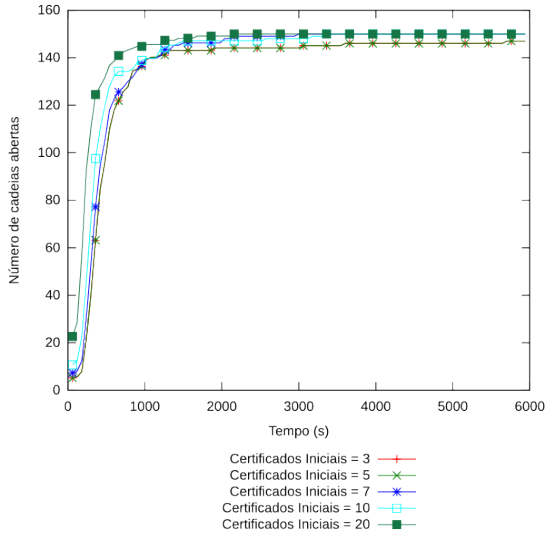
O esquema convergiu totalmente em ambos os casos para $C_i > 5$ e, obteve resultados acima de 90% de cadeias abertas para $C_i <= 5$. Não foi necessário o uso excessivo de espaço de armazenamento, pois a quantidade de cadeias totais manteve-se dentro dos limites e muito próximos dos resultados encontrados na ausência de atacantes.



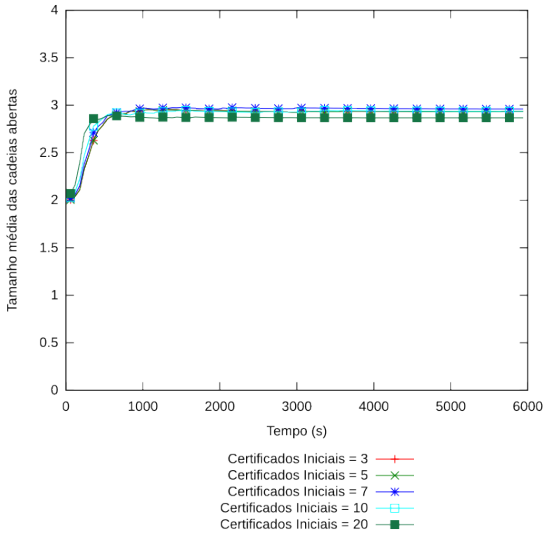

(a) Número de cadeias totais




(b) Número de cadeias fechadas



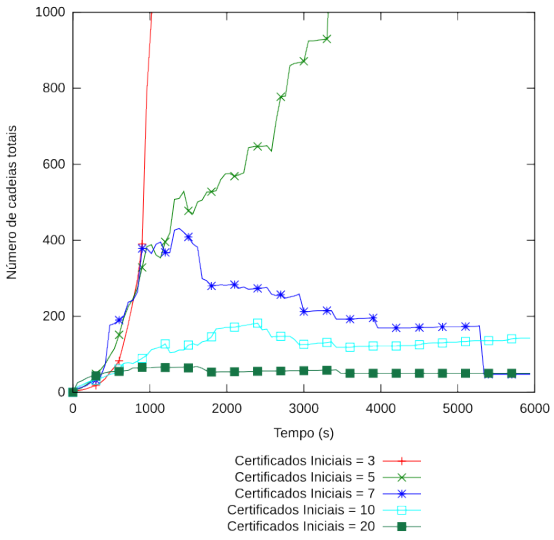

(c) Número de cadeias abertas



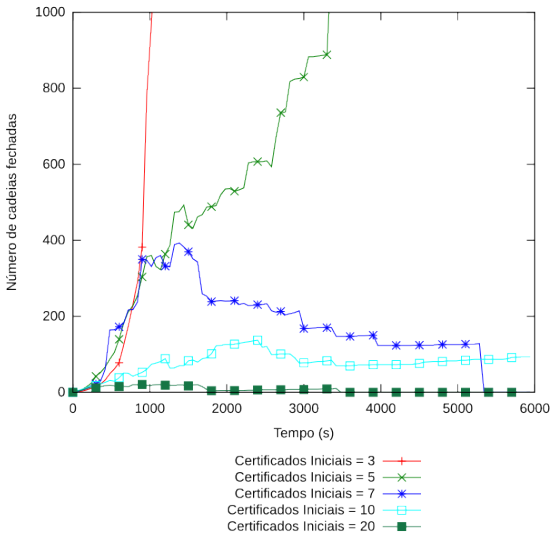

(d) Tamanho médio das cadeias

Figura 4.44: Resultados para 150 nodos e $m = 10\%$

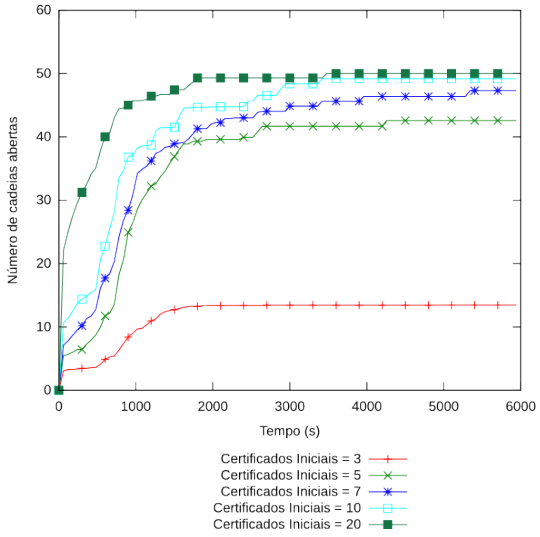
Na Figura 4.45 pode-se observar que ao elevar a proporsão de nodos atacantes para 50%, o esquema encontrou problemas para convergir para quase todas as quantidades de $C_i$ simuladas, com exceção de $C_i = 20$. Para $C_i = 3$ o esquema chegou ao fim das simulações com apenas pouco mais de 20% de cadeias abertas. Para $C_i = 5$ o resultado encontrado foi superior a 80% e para $C_i >= 7$ os valores passaram dos 90%.



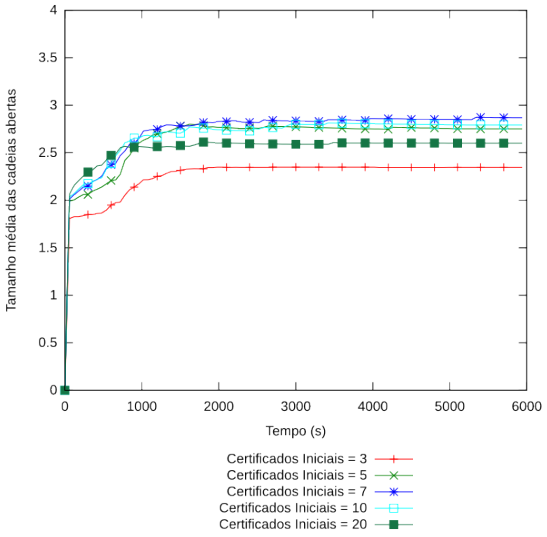

(a) Número de cadeias totais




(b) Número de cadeias fechadas




(c) Número de cadeias abertas



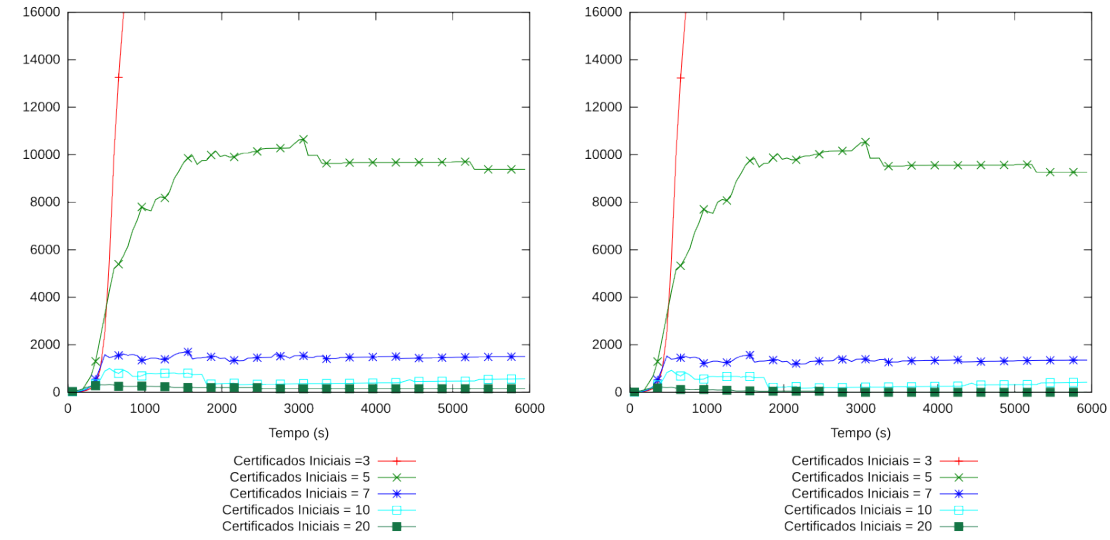

(d) Tamanho médio das cadeias

Figura 4.45: Resultados para 50 nodos e $m = 50\%$

Já a quantidade de cadeias totais foi limitada pelo tamanho do buffer quando a quantidade de certificados iniciais foi inferior à 7.

Na Figura 4.46 os resultados de 150 nodos foram similares aos encontrados nos cenários com 50 nodos.

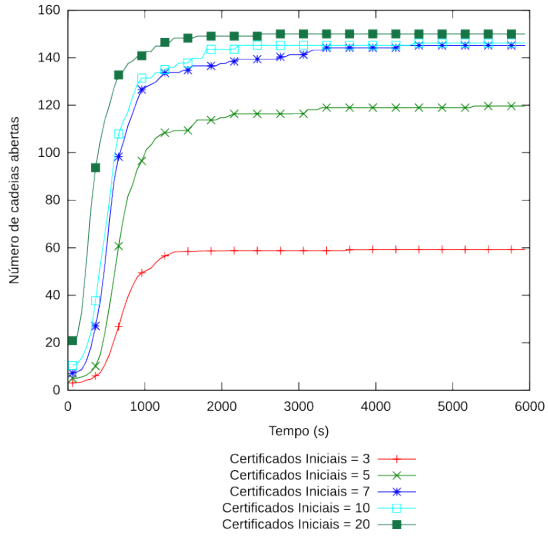
Ao comparar os resultados encontrados aos observados na distribuição homogênea de certificados iniciais, pode-se concluir que eles foram pouco afetados pela mudança.



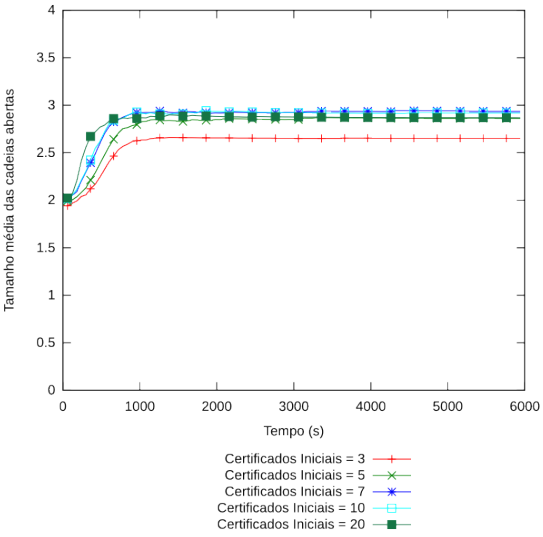

(a) Número de cadeias totais




(b) Número de cadeias fechadas




(c) Número de cadeias abertas




(d) Tamanho médio das cadeias

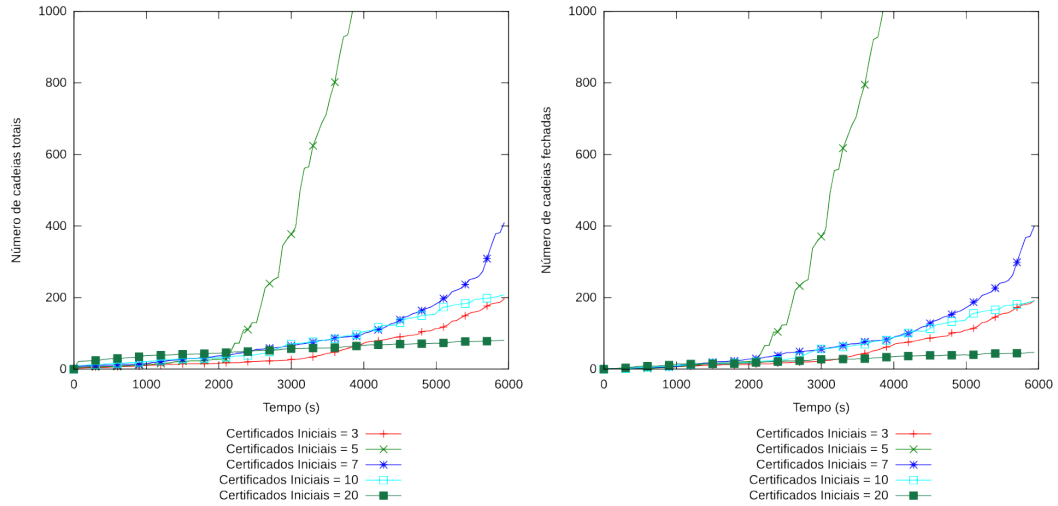
Figura 4.46: Resultados para 150 nodos e $m = 50\%$

#### 4.3.2.3 Ataque *Sybil*

Os resultados encontrados no ataque *Sybil* foram idênticos aos encontrados em um ambiente sem nodos atacantes, da mesma forma como foi demonstrado na distribuição homogênea de certificados iniciais. Desta forma, os gráficos estão todos presentes no Apêndice C.

#### 4.3.2.4 Ataque *Falsificação*

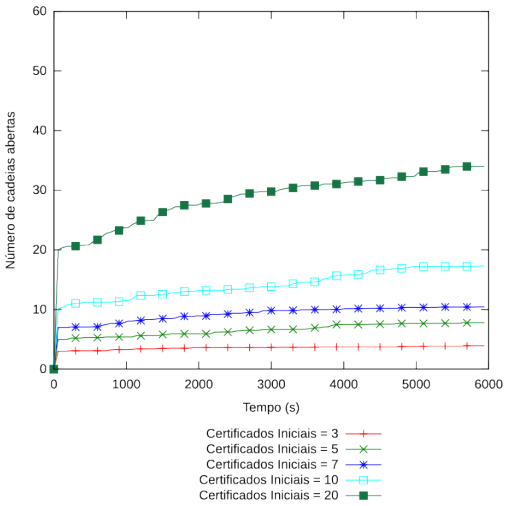
O formato do ataque de falsificação também foi mantido conforme o modelo de distribuição homogêneo de certificados iniciais.



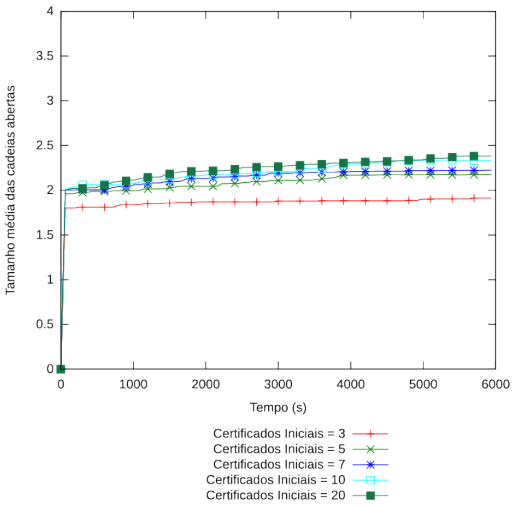

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



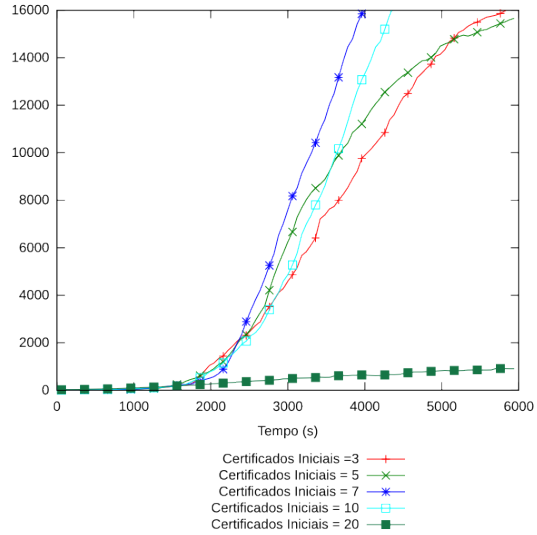

(c) Número de cadeias Abertas



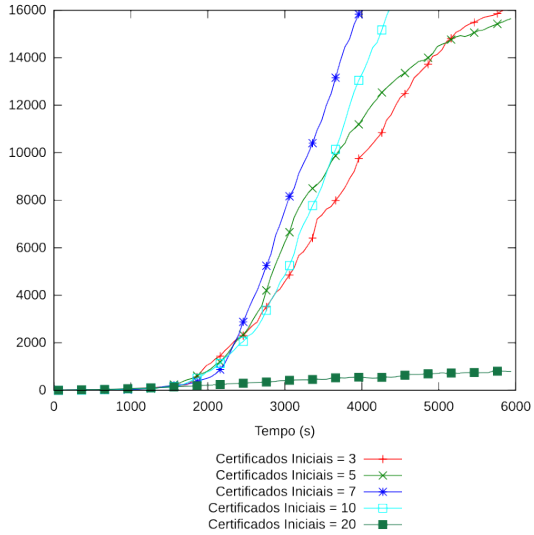

(d) Tamanho médio das cadeias

Figura 4.47: Resultados para 50 nodos, $m = 10\%$ e $N_a = 10\%$

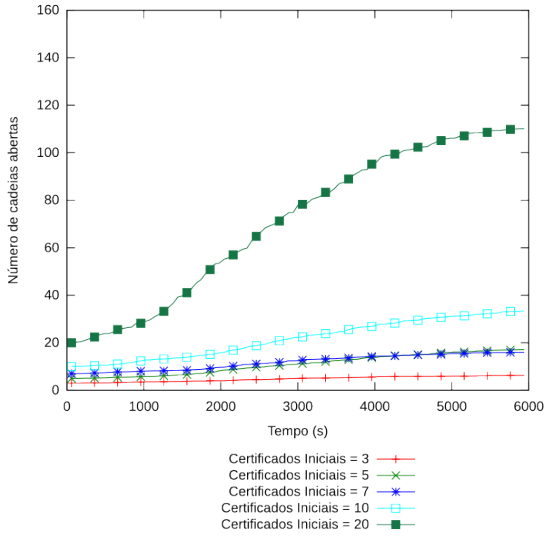
Na Figura 4.47 estão os resultados para $m = 10\%$ e $N_a = 10\%$ com 50 nodos e na Figura 4.48 para 150 nodos.



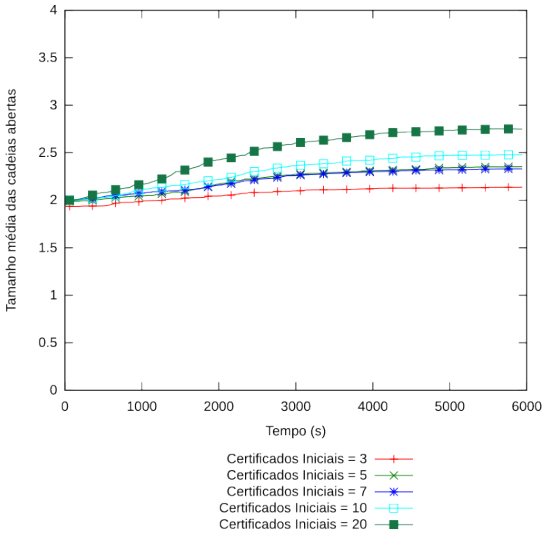

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



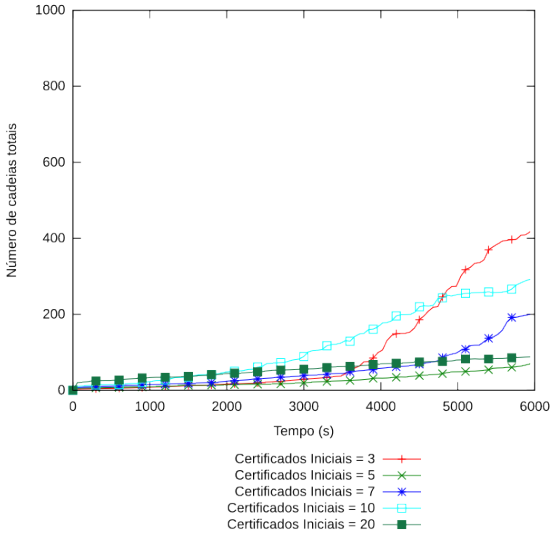

(c) Número de cadeias Abertas



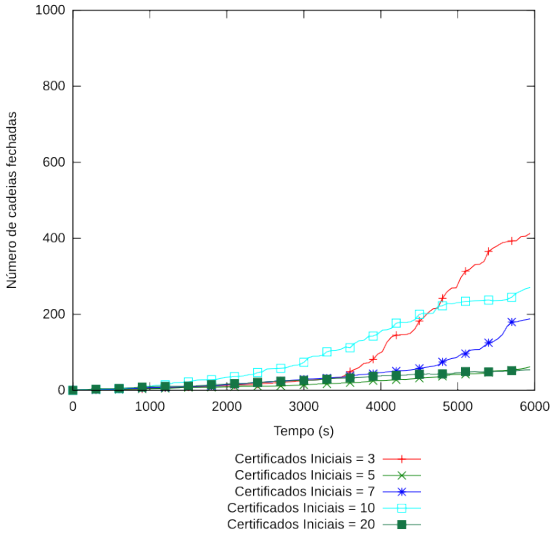

(d) Tamanho médio das cadeias

Figura 4.48: Resultados para 150 nodos, $m = 10\%$ e $N_a = 10\%$

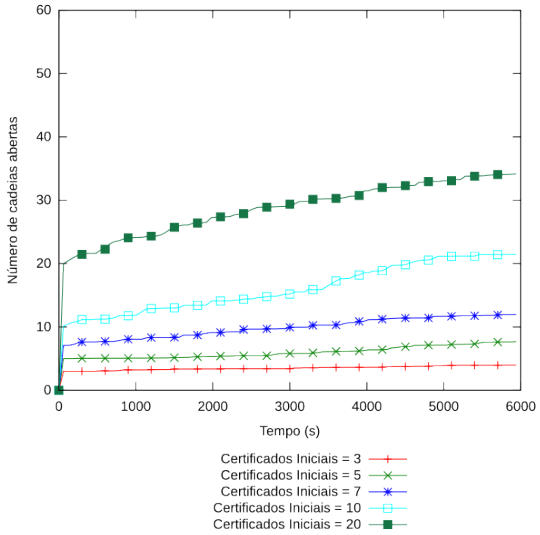
Em ambos os resultados, o esquema não convergiu no tempo de simulação. Para 150 nodos e $C_i = 20$ o esquema atingiu pouco mais de 70% de cadeias abertas ao fim do tempo de simulação, entretanto, no restante dos valores os resultados não chegaram a 20%.



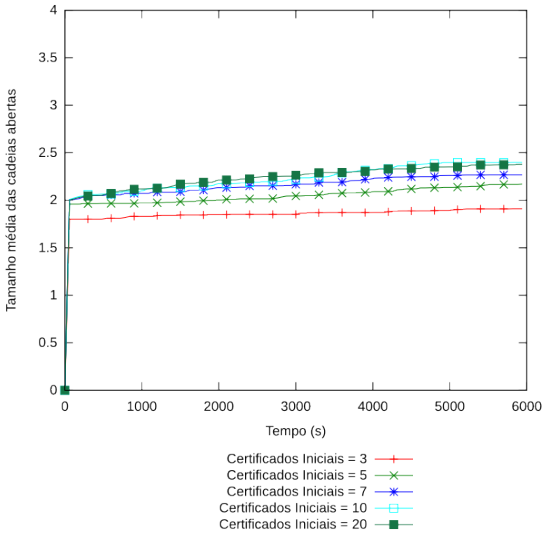

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

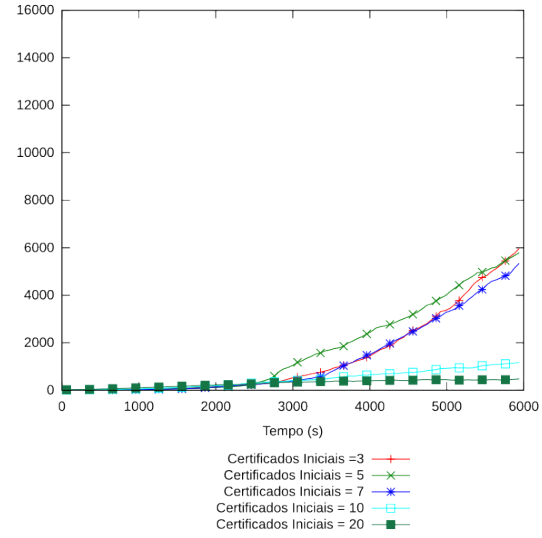



(d) Tamanho médio das cadeias

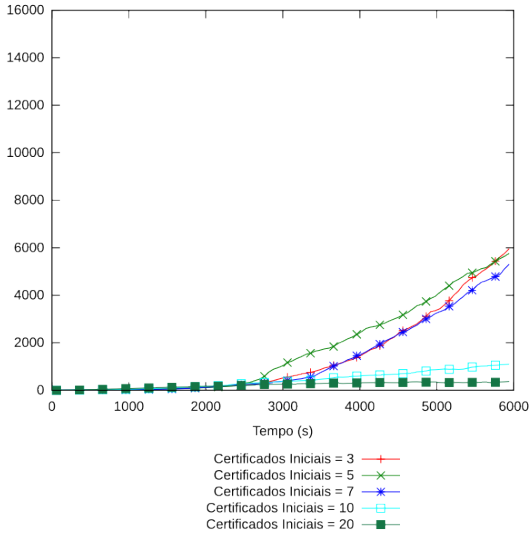
Figura 4.49: Resultados para 50 nodos, $m = 10\%$ e $N_a = 50\%$

Nas Figuras 4.49 e 4.50 estão os resultados para $m = 10\%$ e $N_a = 50\%$, com 50 e 150 nodos, respectivamente.

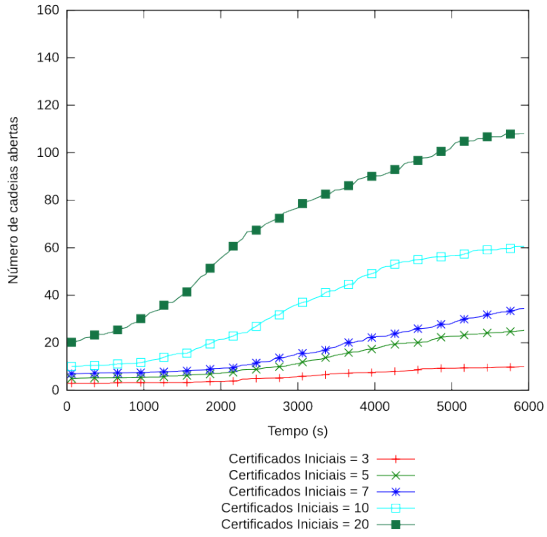
Novamente o esquema não convergiu nos tempo de simulação, atingindo valores muito inferiores aos encontrados na distribuição homogênea de certificados iniciais. O melhor resultado foi encontrado para $C_i = 20$, assim como no conjunto de parâmetros anteriores.



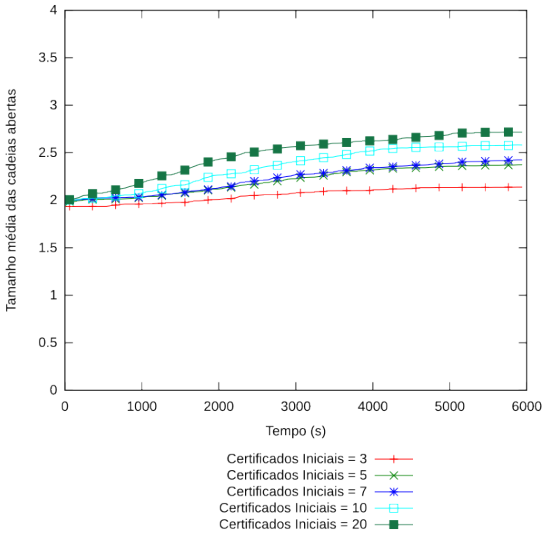

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



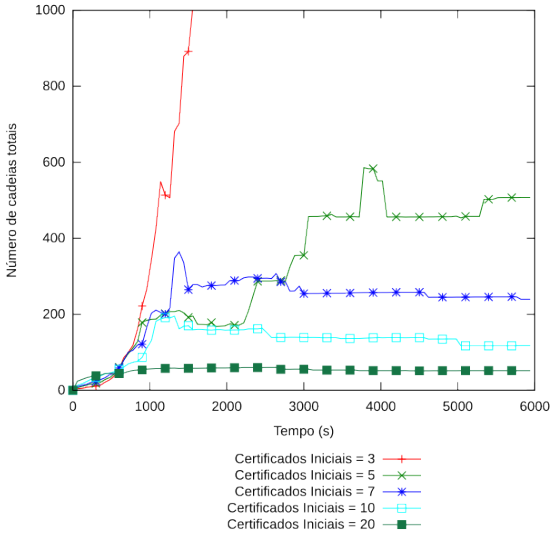

(c) Número de cadeias Abertas



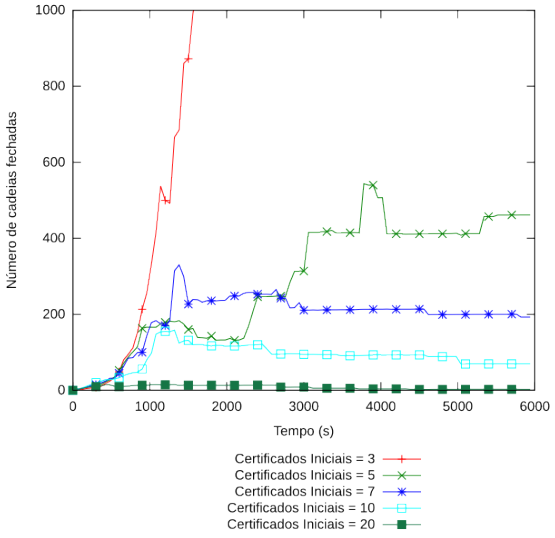

(d) Tamanho médio das cadeias

Figura 4.50: Resultados para 150 nodos, $m = 10\%$ e $N_a = 50\%$

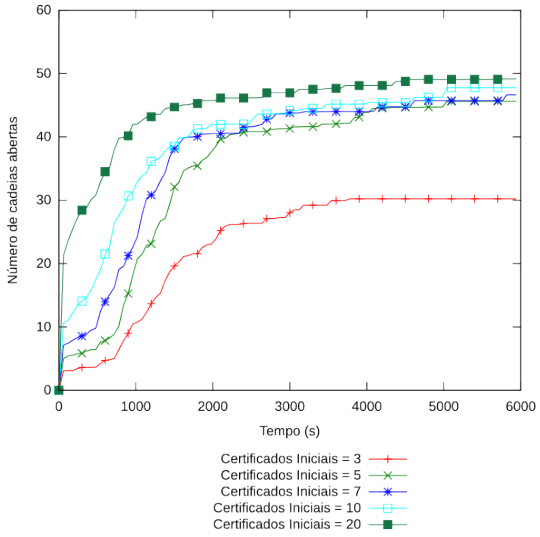
Na Figura 4.51 são apresentados os resultados para $m = 50\%$ e $N_a = 10\%$ com 50 nodos. Já na Figura 4.52 estão os resultados para 150 nodos.



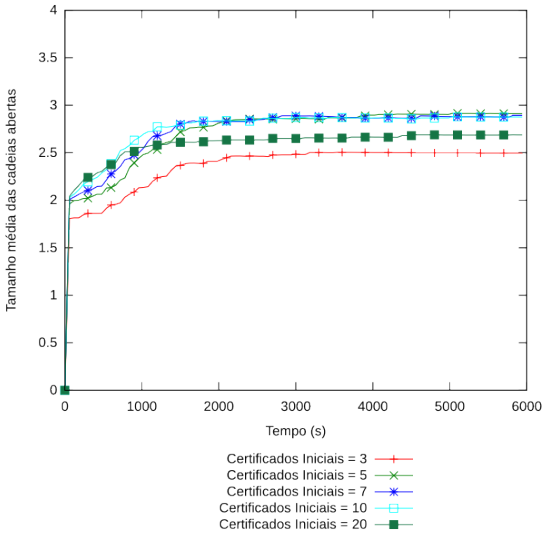

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



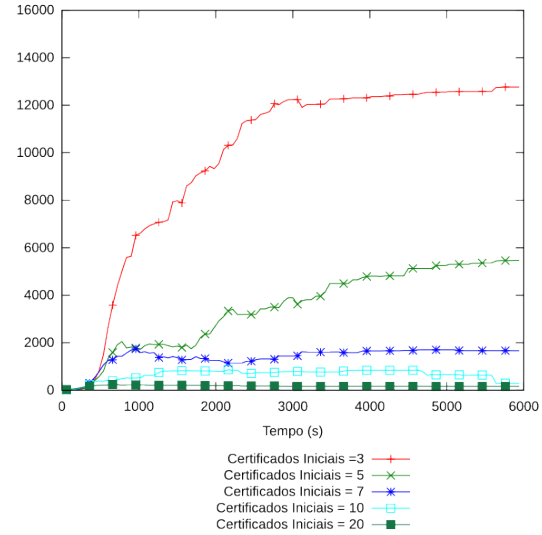

(c) Número de cadeias Abertas



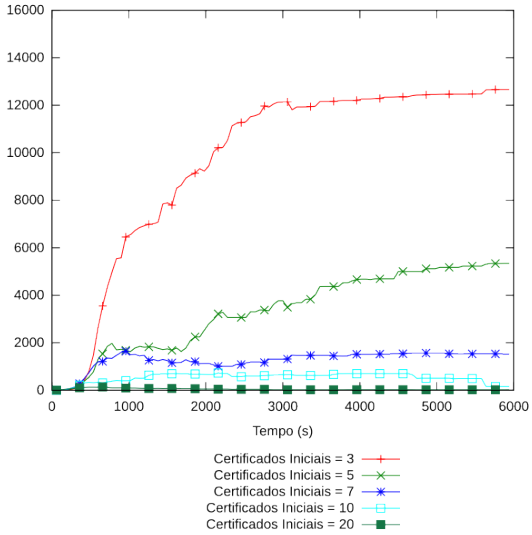

(d) Tamanho médio das cadeias

Figura 4.51: Resultados para 50 nodos, $m = 50\%$ e $N_a = 10\%$

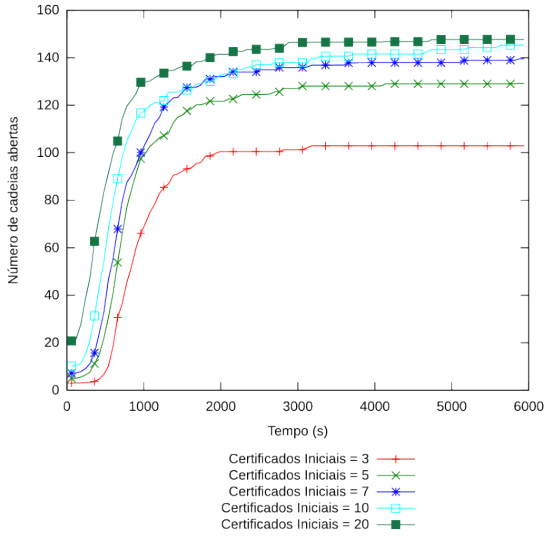
Em ambos os cenários, o esquema convergiu e conseguiu atingir valores superiores a 90% de cadeias abertas ao fim do tempo de simulação para $C_i > 3$. Para 50 nodos, a quantidade total de cadeias para $C_i = 3$ foi limitada pelo tamanho do *buffer* dos nodos. Já com 150 nodos, o esquema estabilizou-se em 66% de cadeias abertas e permaneceu assim por metade do tempo experimentado.



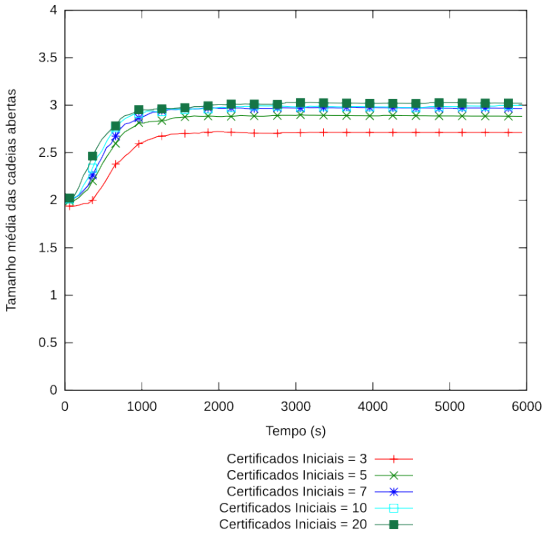

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

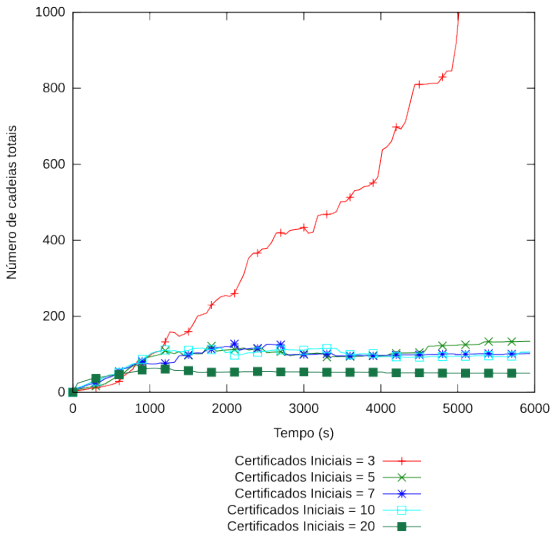



(d) Tamanho médio das cadeias

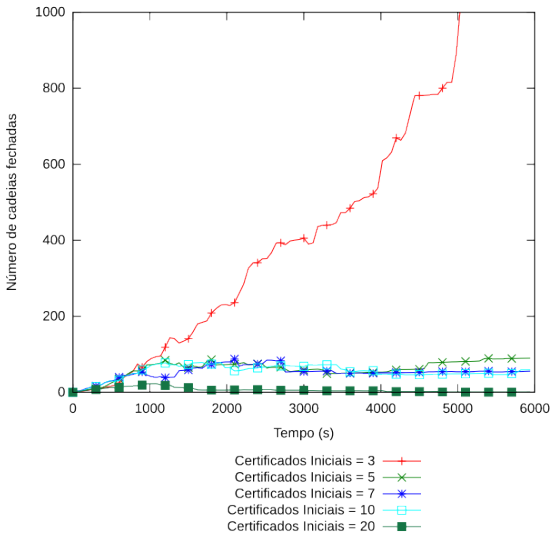
Figura 4.52: Resultados para 150 nodos, $m = 50\%$ e $N_a = 10\%$

As Figuras 4.53 e 4.54 representam os resultados encontrados no pior caso simulado para o ataque de falsificação, $m = 50\%$ e $N_a = 50\%$.

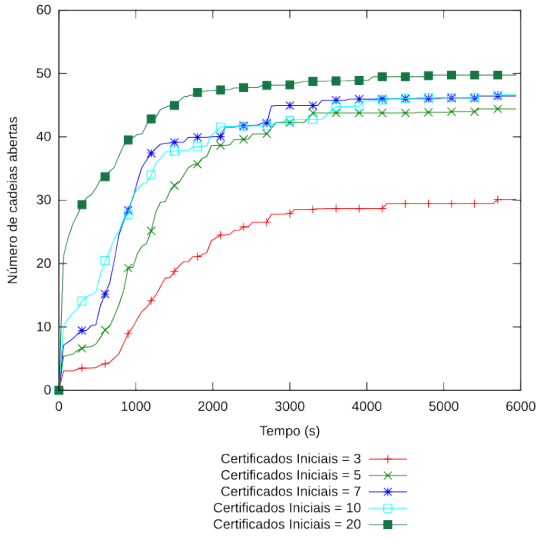
Os resultados atingiram valores satisfatórios (superiores à 90%) para $C_i > 5$. Para $C_i <= 5$, o esquema atingiu pouco mais 60% de cadeias abertas.



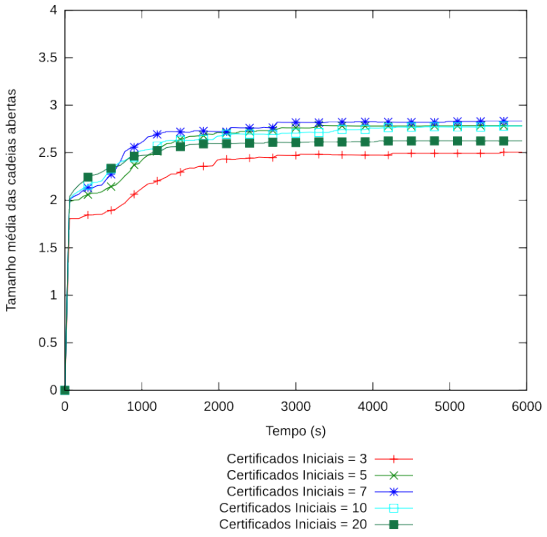

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



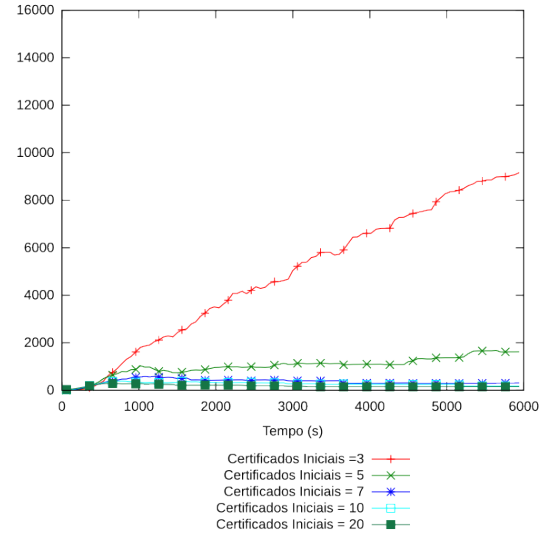

(c) Número de cadeias Abertas



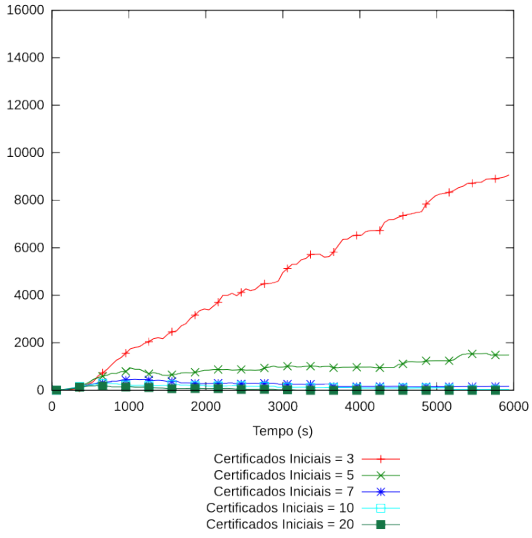

(d) Tamanho médio das cadeias

Figura 4.53: Resultados para 50 nodos, $m = 50\%$ e $N_a = 50\%$

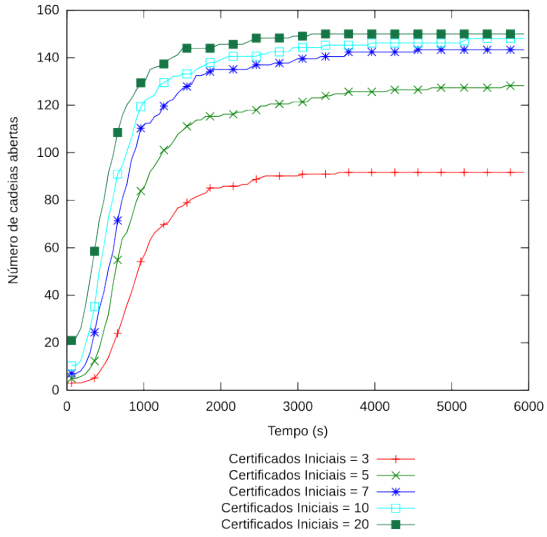
Pode-se concluir que a mudança na forma de distribuição dos certificados iniciais de homogênea para heterogênea interferiu nos resultados de forma significativa nos casos em que há atacantes realizando a falsificação de chaves. Os atacantes conseguiram aumentar ou impedir que o esquema convergisse para um ponto no mínimo satisfatório.



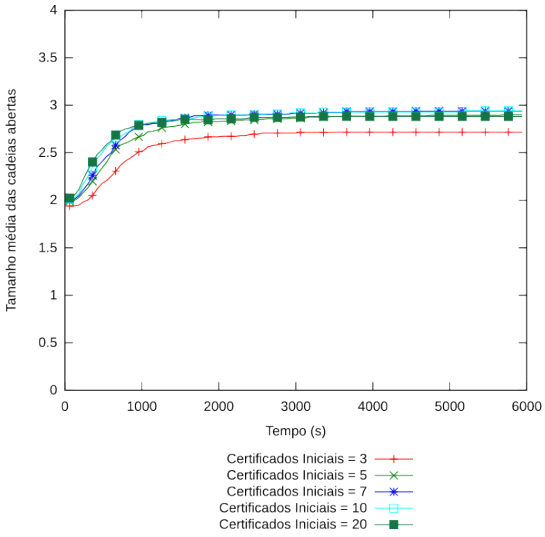

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas



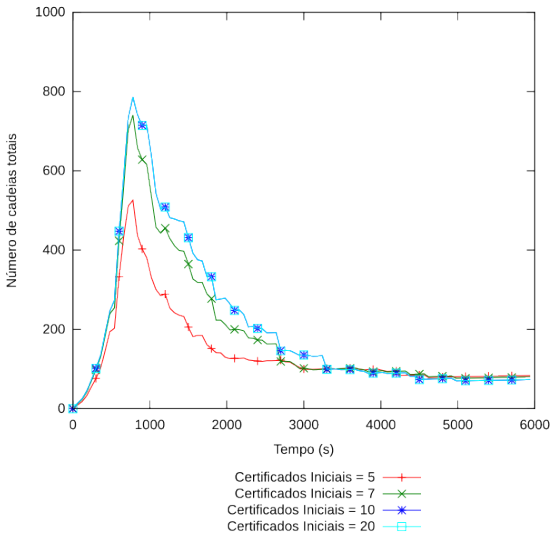

(d) Tamanho médio das cadeias

Figura 4.54: Resultados para 150 nodos, $m = 50\%$ e $N_a = 50\%$

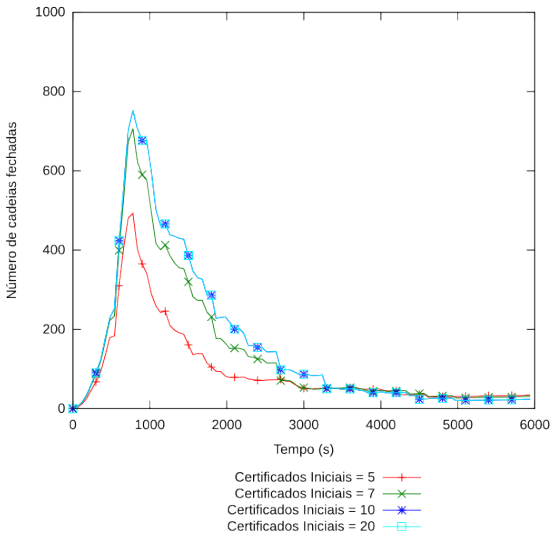
## 4.4 Resultados - Distribuição Centralizada de Certificados Iniciais em 10% dos Nodos

A seguir serão apresentados os resultados para a distribuição mais centralizada de certificados iniciais em 10% dos nodos. Os gráficos apresentados serão apenas para 50 e 150 nodos, os demais estão presentes no Apêndice D.

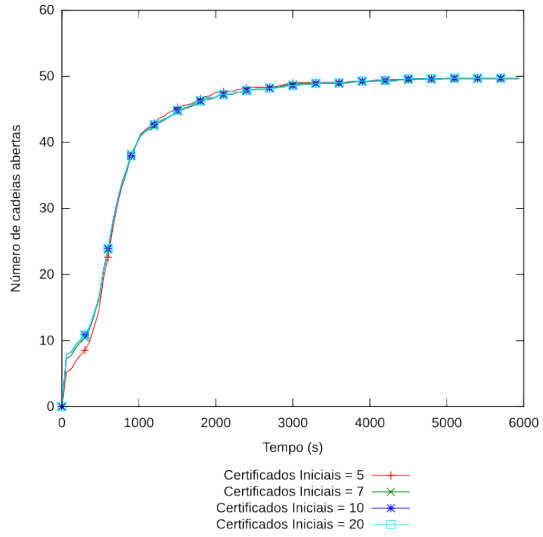
### 4.4.1 Simulações Iniciais



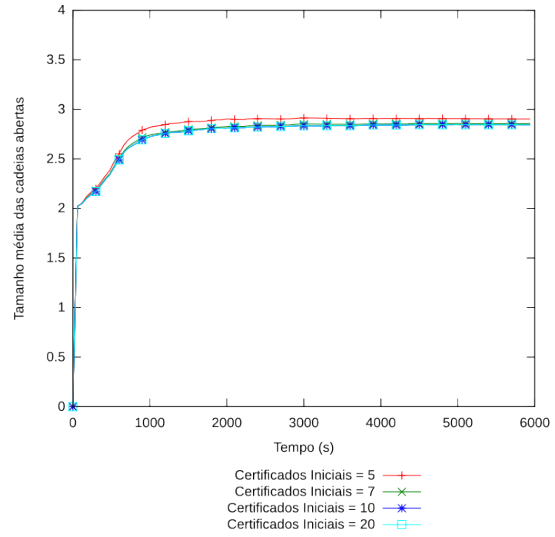

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



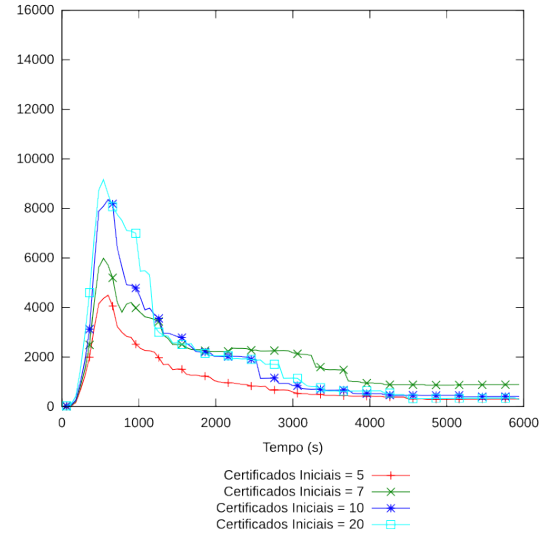

(c) Número de cadeias Abertas



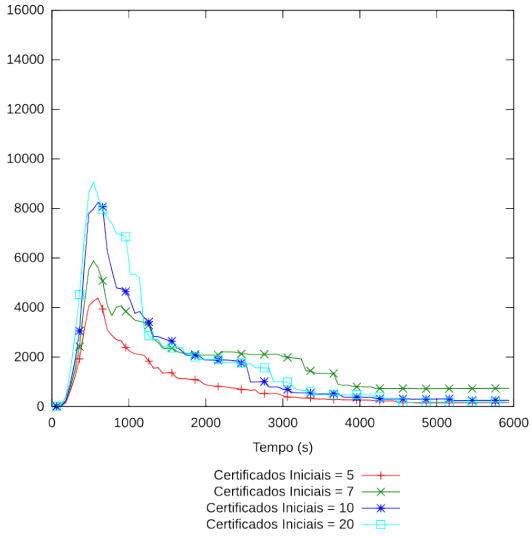

(d) Tamanho médio das cadeias

Figura 4.55: Resultados para 50 nodos

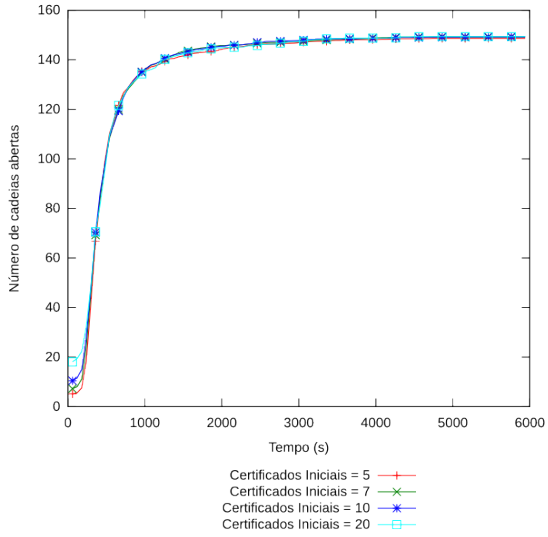
Nessa forma de distribuição poucos nodos iniciam a rede com muitos certificados e muitos nodos com o mínimo simulado (3 certificados).



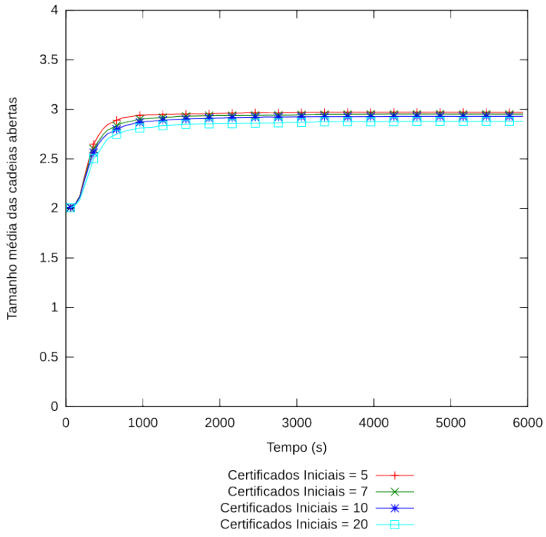

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura 4.56: Resultados para 150 nodos

Explita-se que assim como na distribuição heterogênea, o valor de $C_i$ agora é usado como fator multiplicativo para definir quantos certificados iniciais são distruibuídos pela rede. Desta forma ao indicar-se $C_i = 5$, diz-se que a rede foi iniciada com cinco vezes a quantidade de nodos na rede.

Com essa forma de distribuição, 10% dos nodos recebem uma grande quantidade de certificados e o restante dos nodos apenas 3. Nota-se assim que os valores para $C_i = 3$ não constarão nos gráficos apresentados.

A mudança na forma de distribuição afetou o tempo de convergência e a quantidade de cadeias durante o pico de armazenamento. Na Figura 4.55 pode-se observar que o esquema converge pouco antes dos 5 mil segundos de simulação. Há um au-

mento substancial ao se comparar com os resultados apresentados anteriormente, nos quais o esquema convergia em pouco mais de 2 mil segundos. Na Figura 4.56 o tempo de convergência foi um pouco menor, mas ainda próximo dos 5 mil segundos.

Salienta-se a inversão dos valores obtidos aos encontrados em outras formas de distribuição de certificados iniciais. Nesse modelo, a quantidade de cadeias mantidas é mais alta para $C_i$ mais altos. Isso pode ser observado tanto para 50 quanto para 150 nodos. Tal situação acontece devido a poucos nodos possuirem grande parte dos certificados iniciais. Assim, quanto mais certificados iniciais, maior a diferença entre a quantidade de certificados armazenadas entre os 10% dos nodos e o restante dos participantes da rede.

### 4.4.2 Ataques

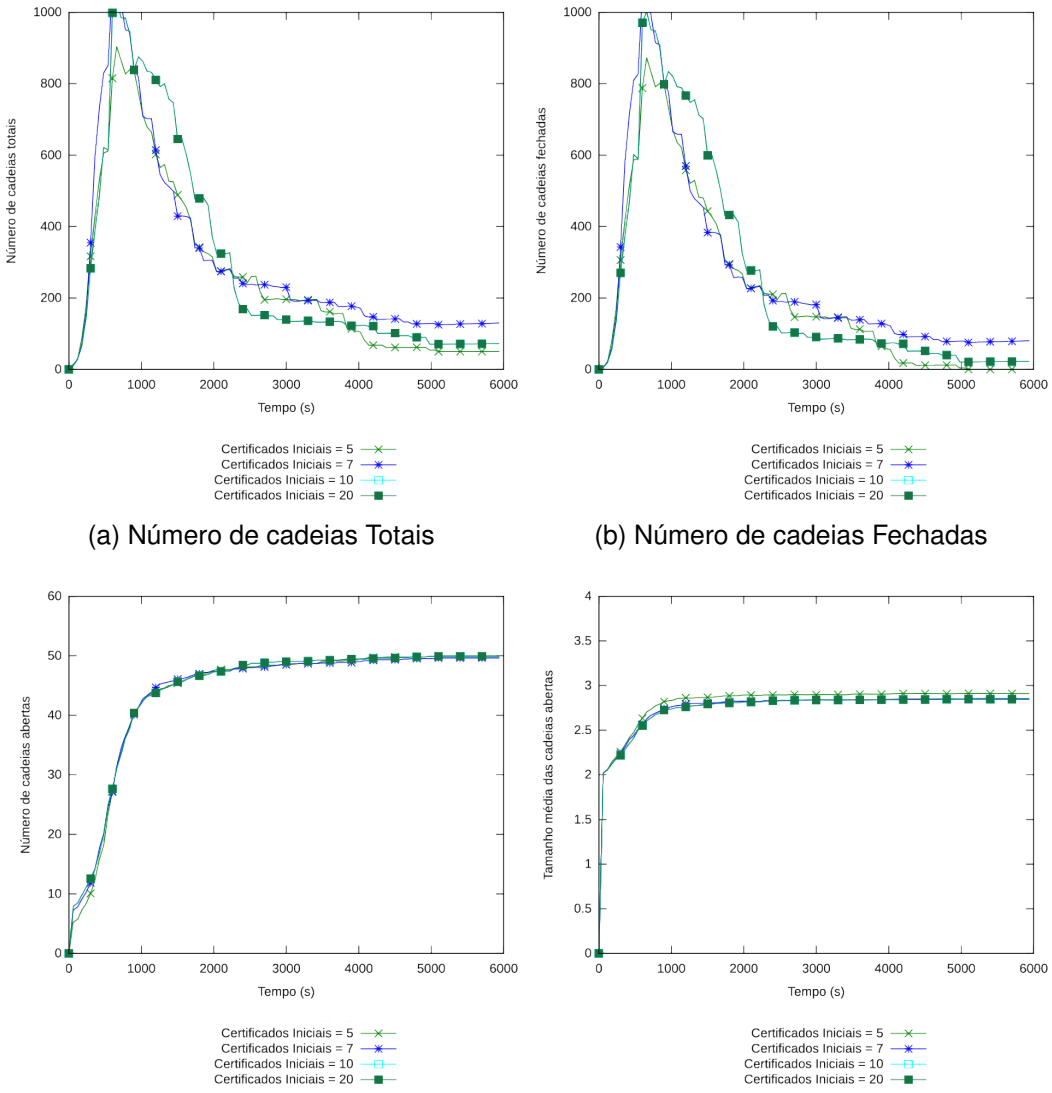
Aplicou-se os mesmo ataques apresentados anteriormente nessa forma de distribuição de certificados iniciais.

#### 4.4.2.1 Ataque *GreyHole*

A escolha dos nodos continuou a ser aleatória. Desta forma um nodo poderia fazer parte do grupo com muitos certificados e ainda ser um nodo malicioso.

Nas Figura 4.57 e 4.58 são apresentados os valores de 50 e 150 nodos para $m = 10\%$ e $t = 10\%$.

A inversão na quantidade de cadeias totais permanceu no ambiente com nodos maliciosos e os resultados encontrados para todos os valores de $C_i$ foi muito próximo do dobro em relação ao ambiente livre de atacantes.




(a) Número de cadeias Totais

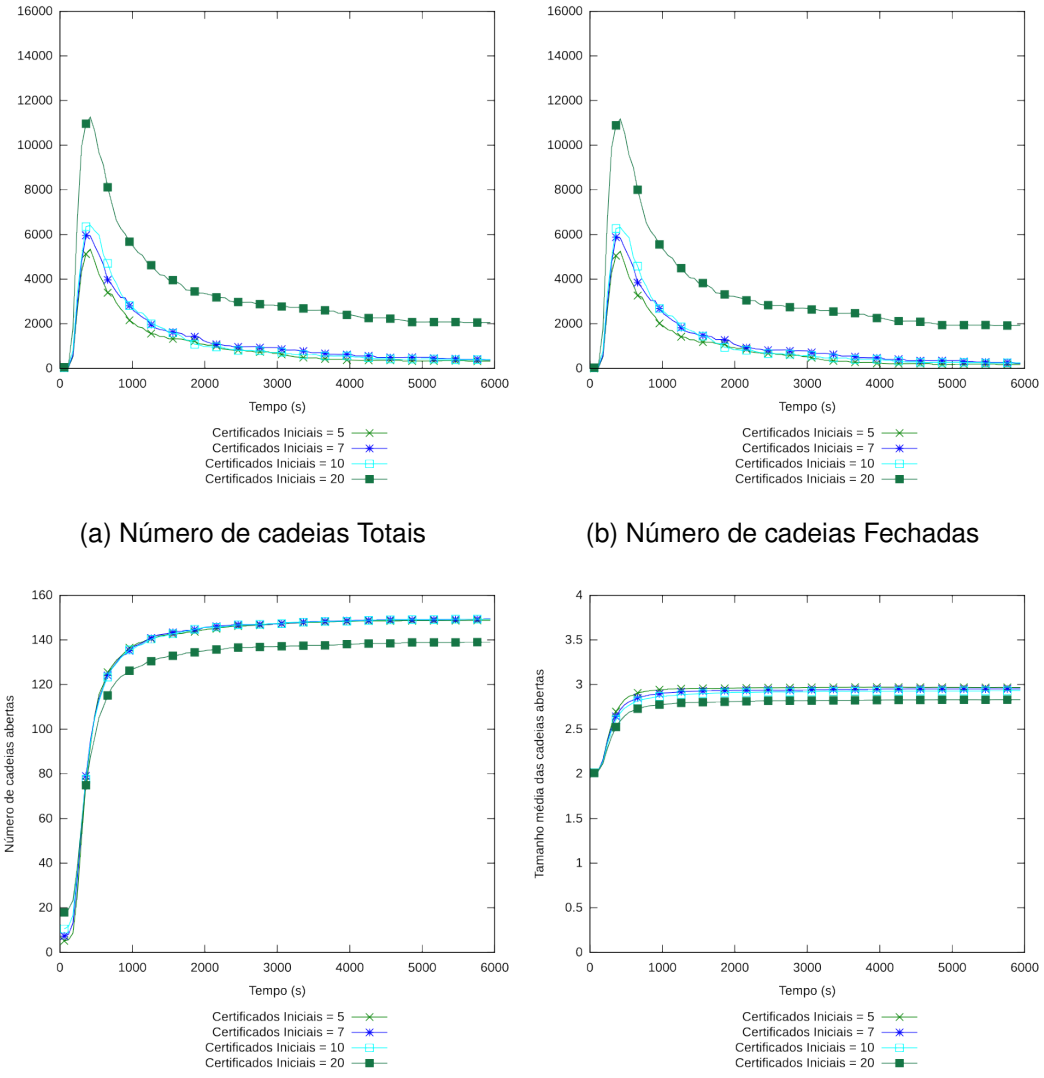
(b) Número de cadeias Fechadas

(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

Figura 4.57: Resultados para 50 nodos, $m = 10\%$ e $t = 10\%$

Para 150 nodos, o aumento na quantidade de cadeias não foi tão elevado como o encontrado para 50 nodos. Mesmo elevando o uso de espaço de armazenamento, o esquema convergiu em um tempo semelhante ao apontado nas simulações sem atacantes.



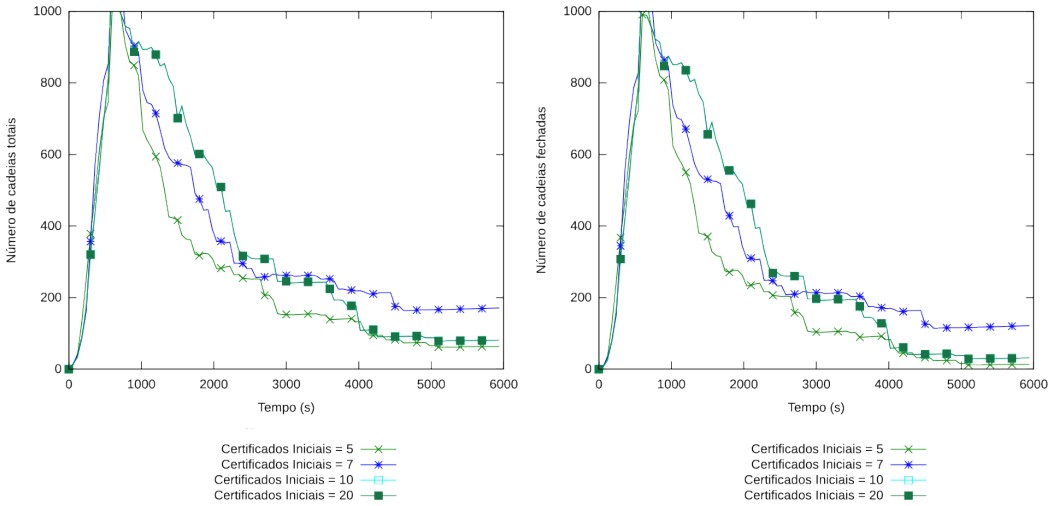

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

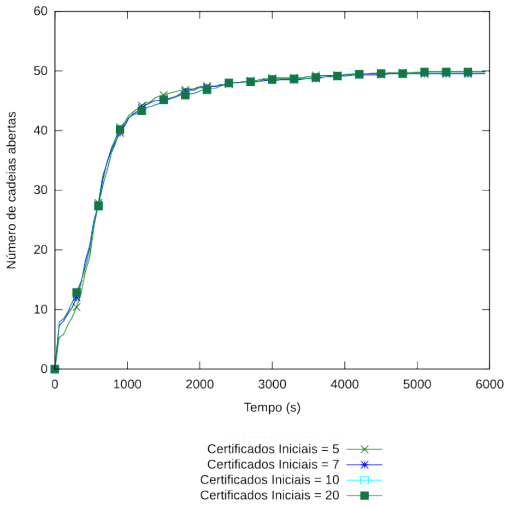
Figura 4.58: Resultados para 150 nodos, $m = 10\%$ e $t = 10\%$



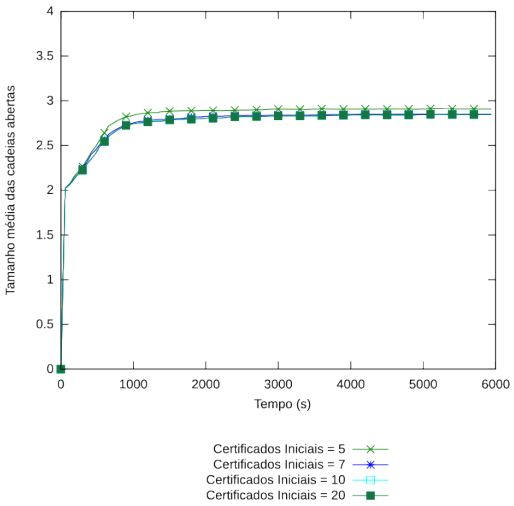

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas



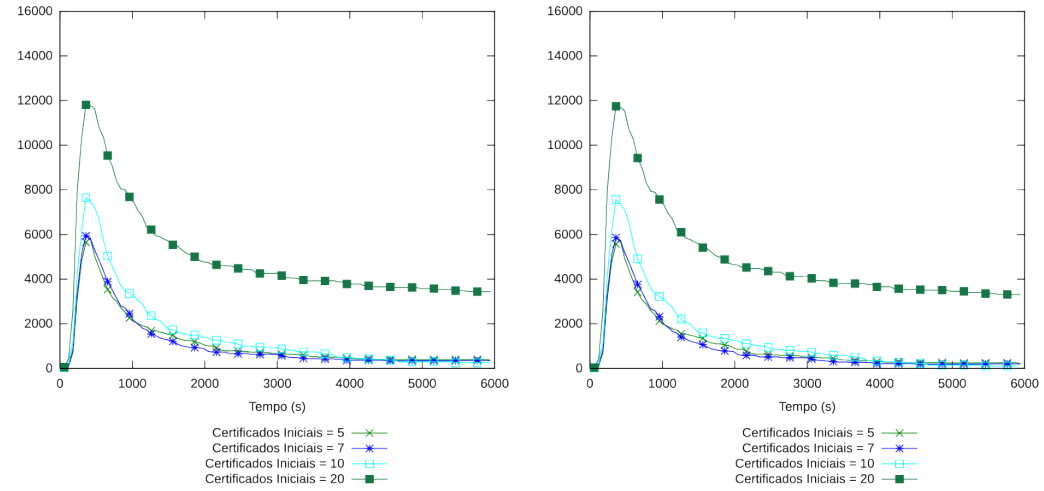

(d) Tamanho médio das cadeias

Figura 4.59: Resultados para 50 nodos, $m = 10\%$ e $t = 50\%$

Na Figura 4.59 estão os resultados de 50 nodos com $m = 10\%$ e $t = 50\%$. Os resultados foram muito semelhantes aos apresentados para $t = 10\%$.

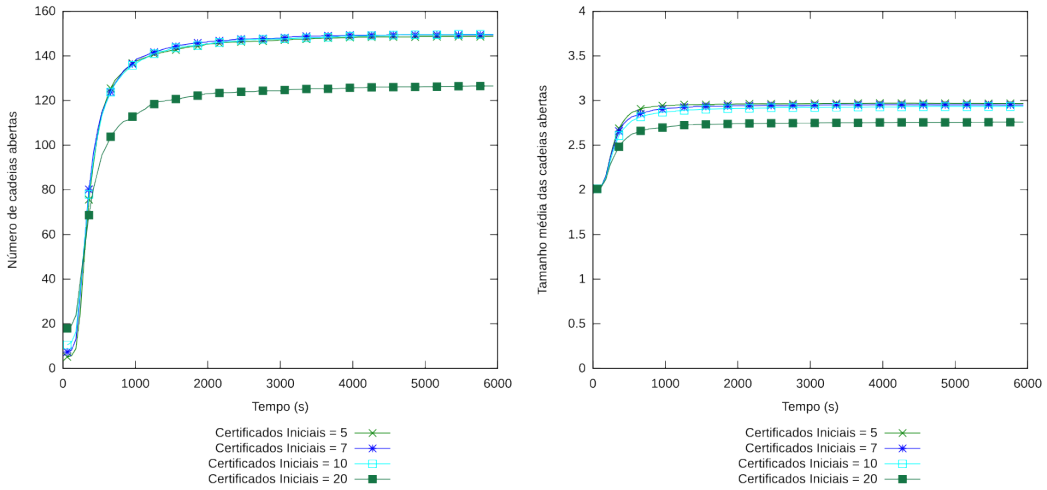
Novamente a quantidade de cadeias totais foi inversa a encontrada em outras formas de distribuição de $C_i$. O esquema manteve o tempo de convergência de cerca de 5 mil segundos.

Os resultados para 150 nodos e $m = 10\%$ e $t = 50\%$ estão na Figura 4.60. Essa é a primeira situação em que o esquema não converge para todos os valores de $C_i$ simulados.




(a) Número de cadeias Totais

(b) Número de cadeias Fechadas



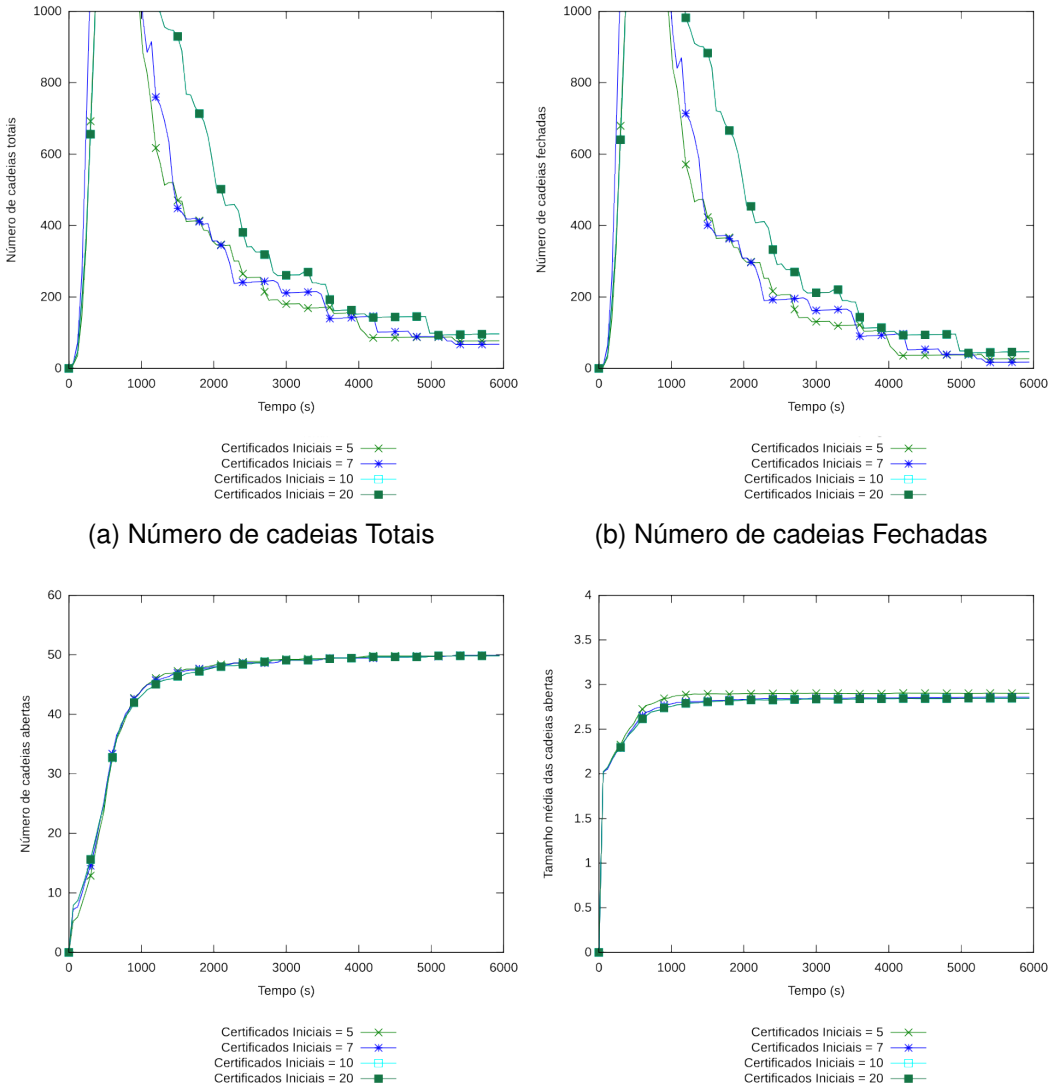

(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

Figura 4.60: Resultados para 150 nodos, $m = 10\%$ e $t = 50\%$

Assim como observado anteriormente, o esquema tem apresentado piores resultados para $C_i$ mais altos. Explicita-se que para $C_i = 20$ o esquema convergiu até possuir 83% de cadeias abertas.

Na Figura 4.61 pode-se notar que com o aumento da quantidade de nodos maliciosos para 50%, a quantidade de cadeias totais elevou-se para cerca de 3 vezes ao encontrado no ambiente sem atacantes. Entretanto, a quantidade não ocupou todo o *buffer* dos nodos.




(a) Número de cadeias Totais

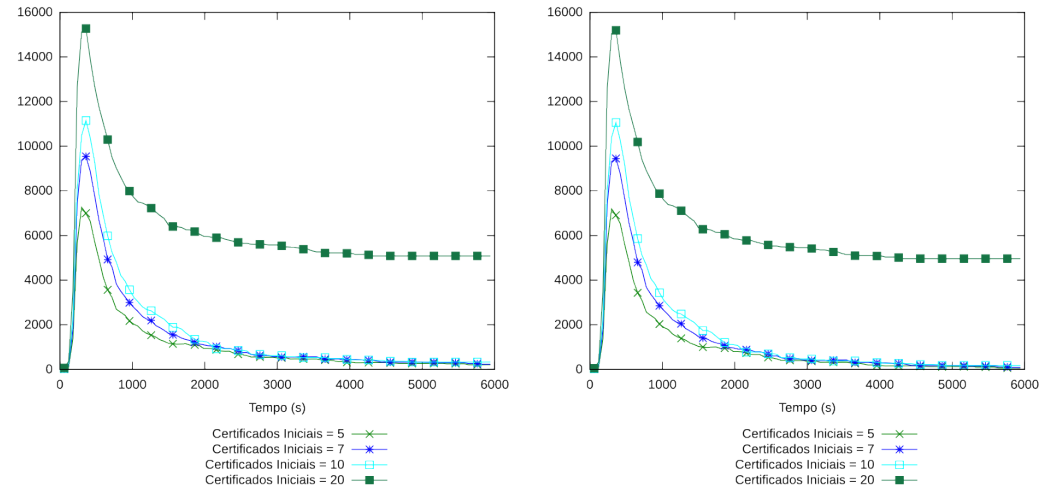
(b) Número de cadeias Fechadas

(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

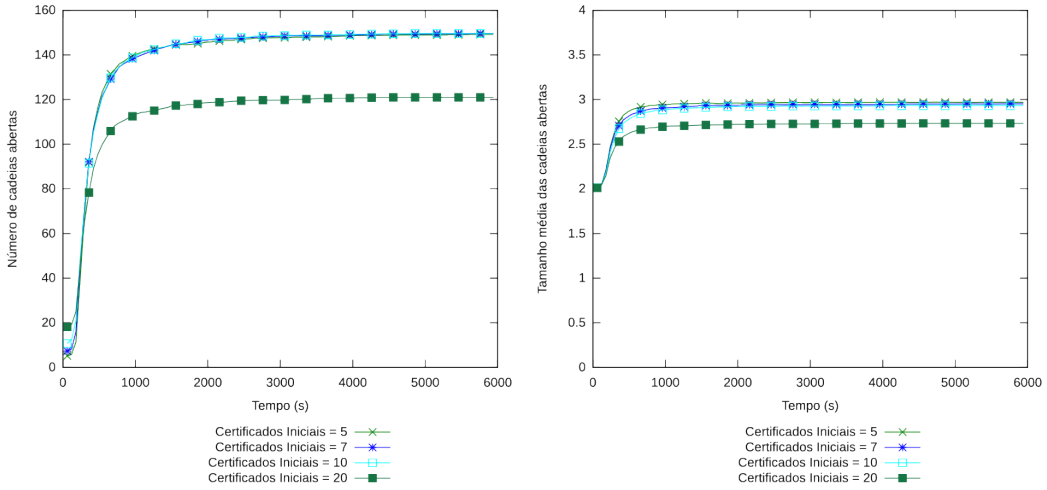
Figura 4.61: Resultados para 50 nodos, $m = 50\%$ e $t = 10\%$

Na Figura 4.62 nota-se que o esquema não convergiu novamente no tempo simulado para $C_i = 20$ e que a quantidade de cadeias totais elevou-se cerca de 2 vezes para todos os valores de certificados iniciais.




(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

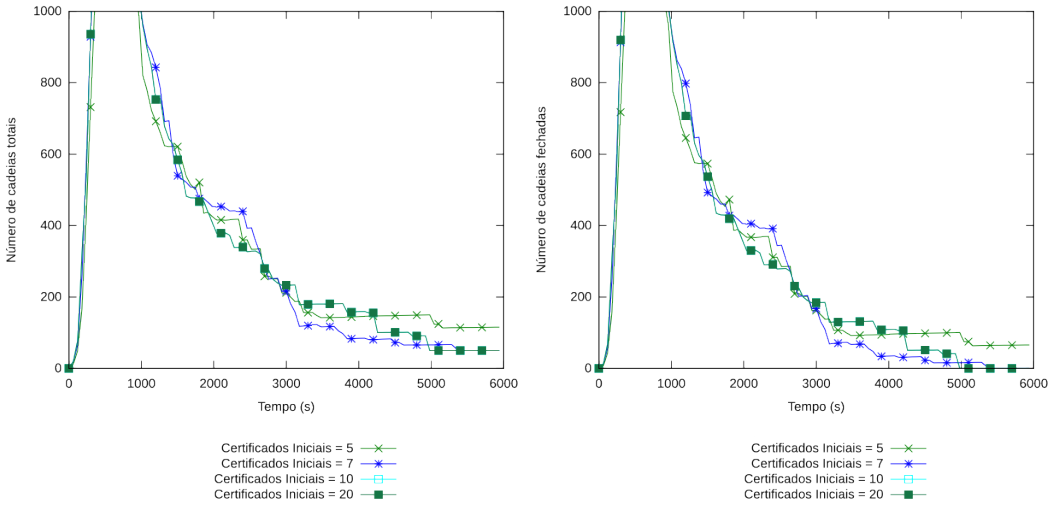



(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

Figura 4.62: Resultados para 150 nodos, $m = 50\%$ e $t = 10\%$

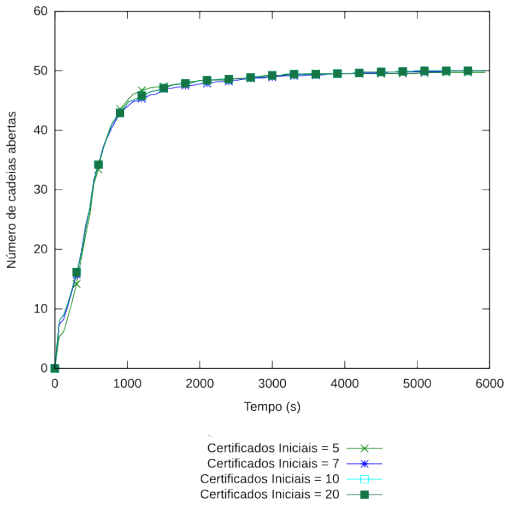
Pode ser observado na Figura 4.63 que, sob o pior cenário simulado nesse tipo de ataque, embora o espaço de armazenamento de cadeias seja elevado, o esquema converge em pouco menos de 6 mil segundos. No entanto, os valores alcançados com 2 mil segundos já são satisfatórios, pois atingem mais de 90% de cadeias abertas.



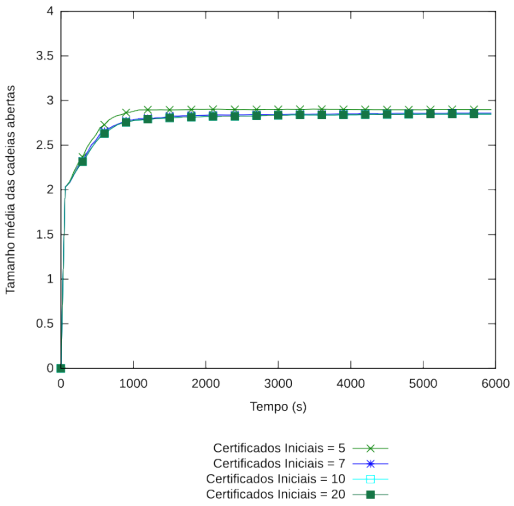

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



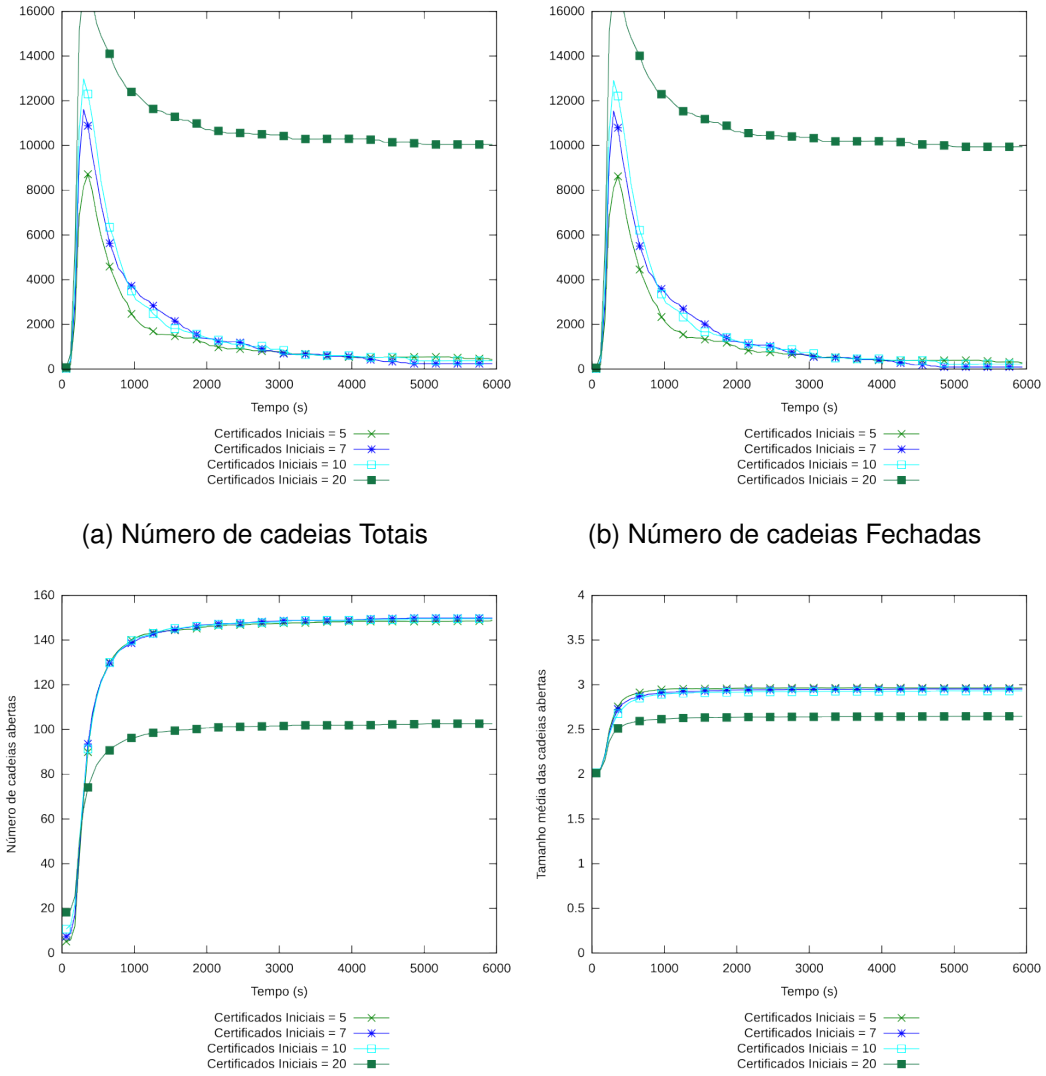

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura 4.63: Resultados para 50 nodos, $m = 50\%$ e $t = 50\%$

Na Figura 4.64 pode-se notar que o esquema não convergiu novamente para $C_i = 20$, atingindo cerca de 70% de cadeias abertas.




(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

(c) Número de cadeias Abertas

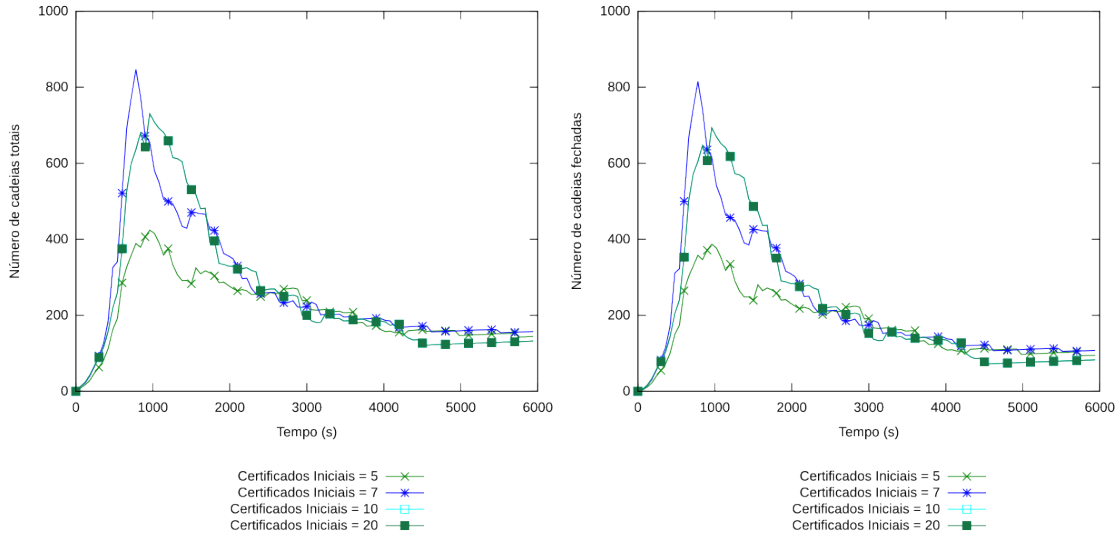
(d) Tamanho médio das cadeias

Figura 4.64: Resultados para 150 nodos, $m = 50\%$ e $t = 50\%$

Apresentados os resultados, conclui-se que a forma mais centralizada é a pior forma de distribuição de certificados para o esquema proposto, pois eleva o tempo de convergência para o dobro encontrado em outras formas de distribuição. O espaço necessário para armazenar as cadeias também eleva-se para valores muito mais elevados que observados anteriormente.

#### 4.4.2.2 Ataque *BlackHole*

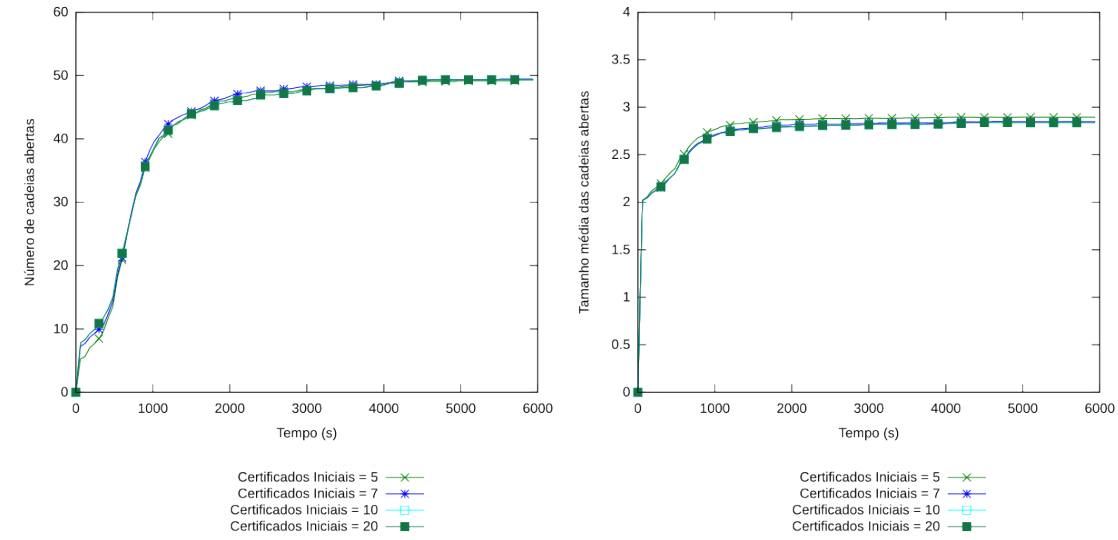
A seguir estão os resultados para o ataque do tipo *blackHole*, no qual os nodos atacantes descartam todas as mensagens que chegam até eles.




(a) Número de cadeias totais




(b) Número de cadeias fechadas




(c) Número de cadeias abertas



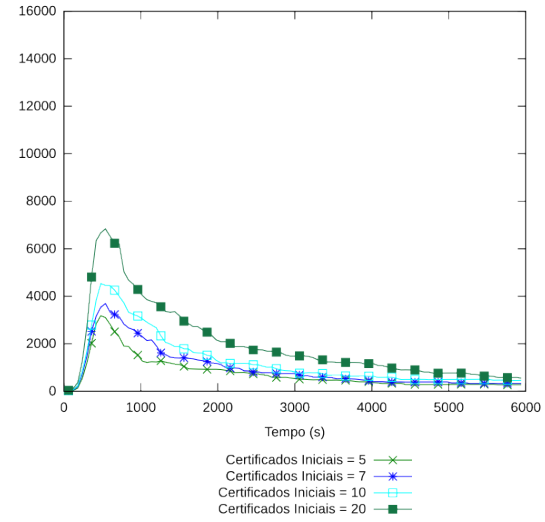

(d) Tamanho médio das cadeias

Figura 4.65: Resultados para 50 nodos e $m = 10\%$

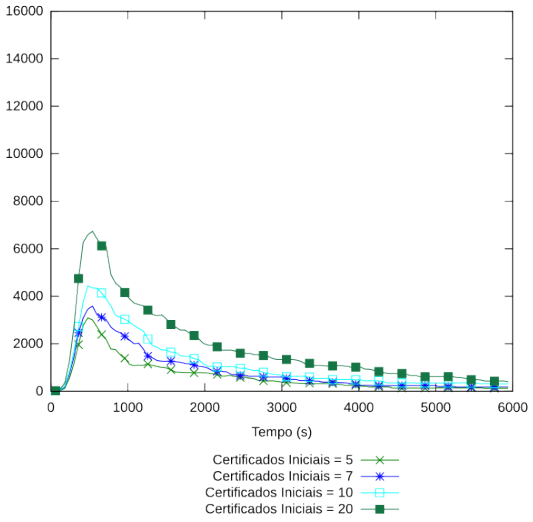
Na Figura 4.65 pode-se ver os resultados para 50 nodos e $m = 10\%$. Nota-se que o esquema não convergiu na sua totalidade, faltando um nodo para todos os valores de $C_i$ simulados, entretanto, esse nodo representa apenas 2% da quantidade total.

O tempo de convergência foi semelhante ao encontrado nas demais simulações dessa forma de distribuição de certificados iniciais. A quantidade de cadeias totais teve uma taxa de crescimento de quase duas vezes ao valor encontrado no ambiente sem atacantes.

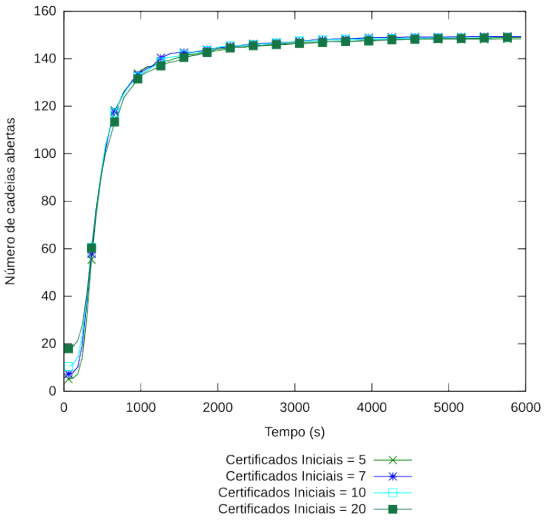
Na Figura 4.66 observa-se que para mais nodos, o esquema convergiu de maneira um pouco mais rápida. Ainda aponta-se o mesmo comportamento de inversão na quantidade de cadeias armazenadas com relação ao número de certificados iniciais.



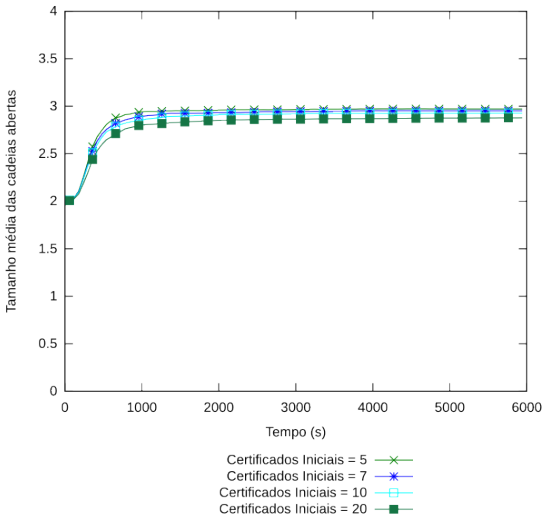

(a) Número de cadeias totais




(b) Número de cadeias fechadas



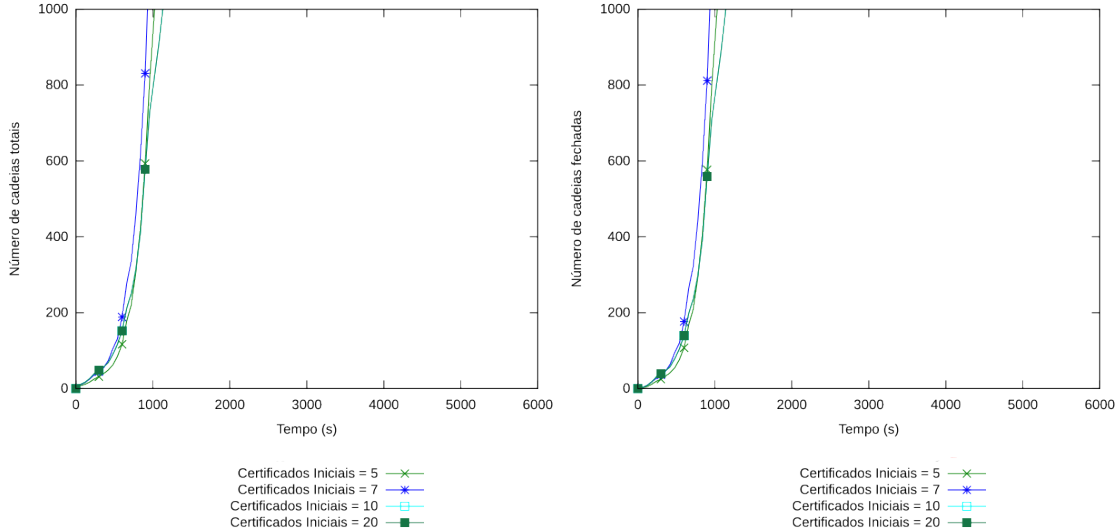

(c) Número de cadeias abertas




(d) Tamanho médio das cadeias

Figura 4.66: Resultados para 150 nodos e $m = 10\%$

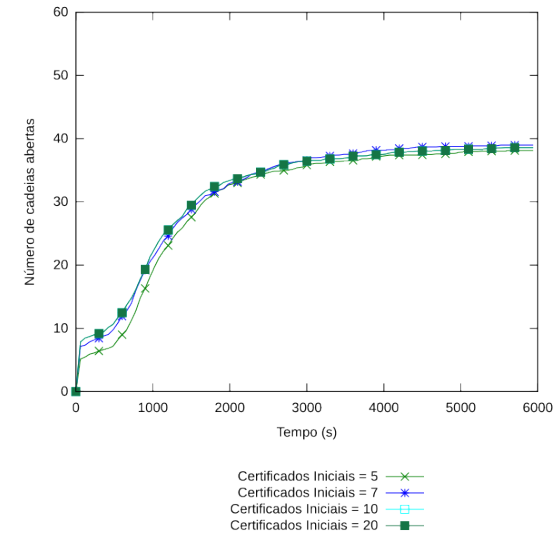
Ao elevar a taxa de atacantes para 50%, pode-se observar por meio da Figura 4.67 que o esquema não converge no tempo simulado para nenhum valor de $C_i$ utilizado. A quantidade de cadeias totais foi limitada pelo tamanho do *buffer* de cada nodo e ao final das simulações, cada nodo possuía pouco menos de 80% de cadeias abertas.



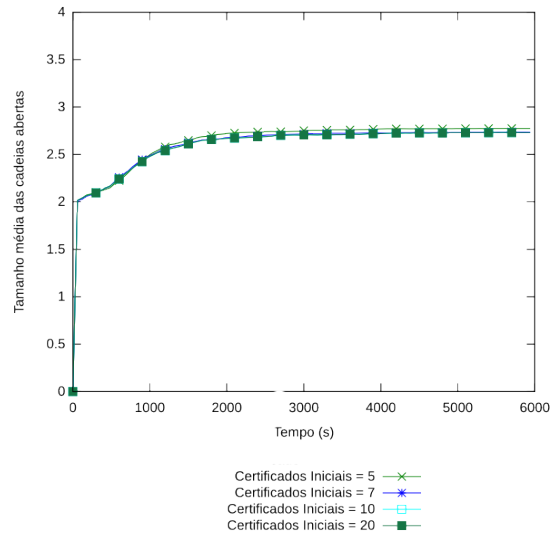

(a) Número de cadeias totais




(b) Número de cadeias fechadas



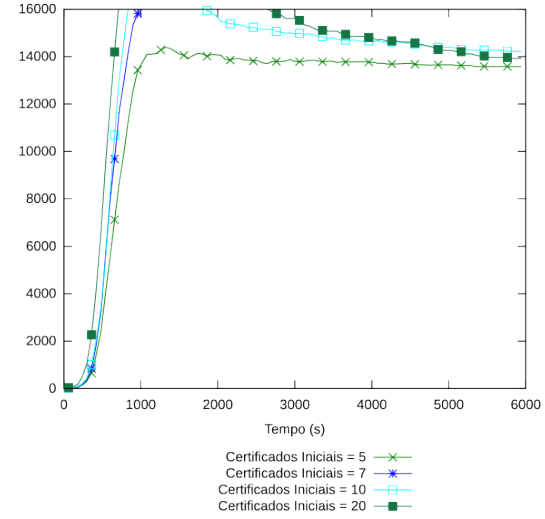

(c) Número de cadeias abertas



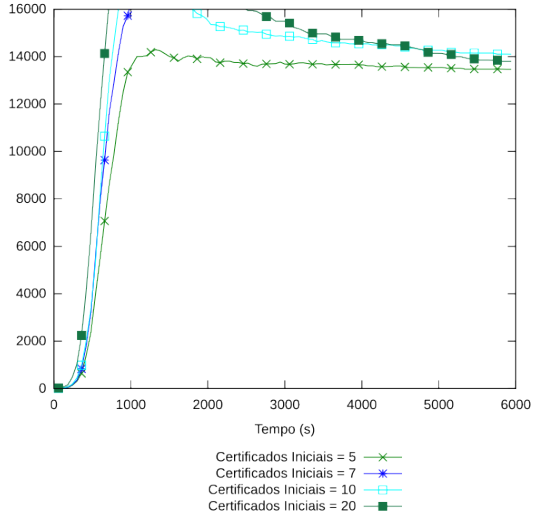

(d) Tamanho médio das cadeias

Figura 4.67: Resultados para 50 nodos e $m = 50\%$

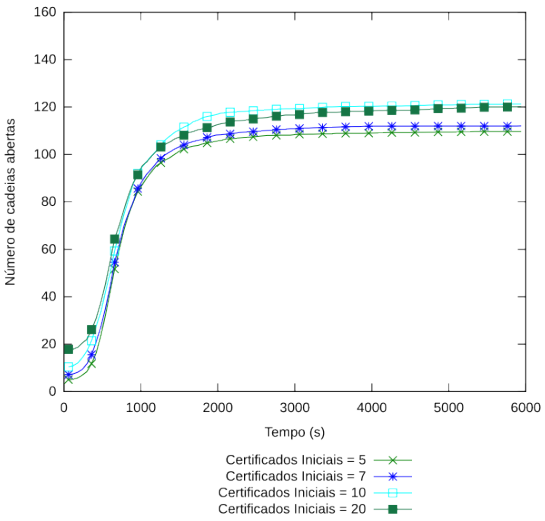
Para 150 nodos, Figura 4.68, o esquema apresenta taxas de cadeias abertas semelhantes às encontradas para 50 nodos, permanecendo entre 70 e 80%. A quantidade total de cadeias foi elevada no momento de pico, entretanto não representou 70% do espaço disponível.



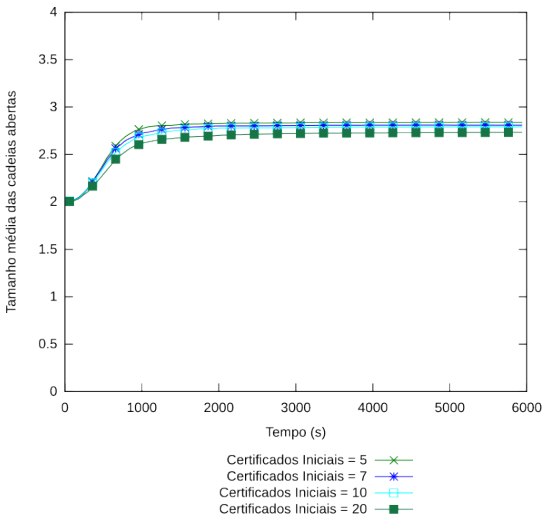

(a) Número de cadeias totais




(b) Número de cadeias fechadas




(c) Número de cadeias abertas




(d) Tamanho médio das cadeias

Figura 4.68: Resultados para 150 nodos e $m = 50\%$

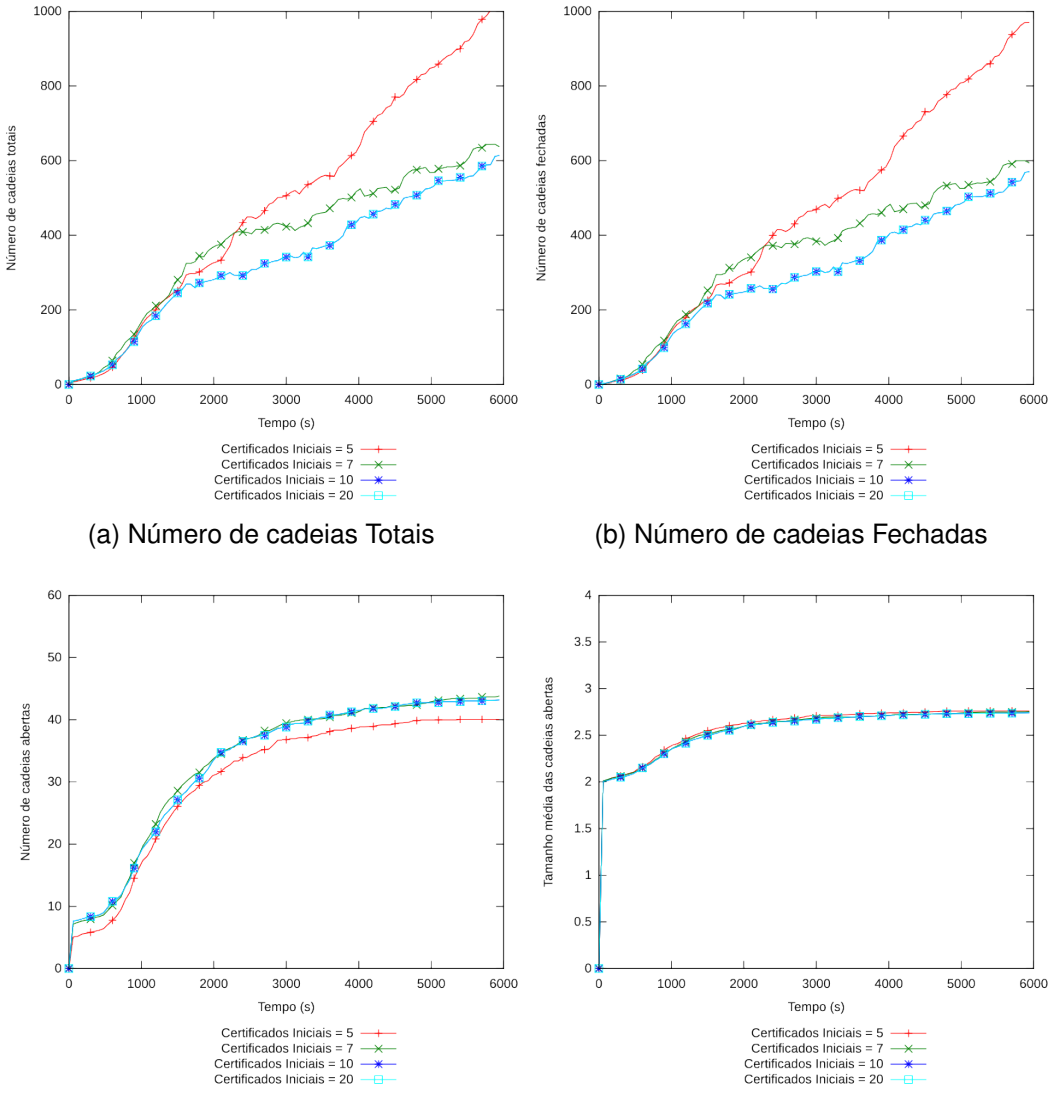
Pode-se concluir que esse tipo de ataque é mais efetivo sobre o esquema quando o modelo centralizado de distribuição de certificados iniciais é usado. Nas simulações com 50 nodos e $m = 50\%$ explicita-se que foram as simulações em que o espaço de armazenamento esvaiu-se mais rapidamente entre todas as combinações realizadas de parâmetros e ataques realizadas.

#### 4.4.2.3 Ataque *Sybil*

Os resultados encontrados no ataque *Sybil* foram idênticos aos encontrados em um ambiente sem nodos atacantes, da mesma forma como foi demonstrado nas distribuições homogênea e heterogênea de certificados iniciais. Desta forma, os gráficos estão todos presentes no Apêndice D.

#### 4.4.2.4 Ataque *Falsificação*

O último tipo de ataque apresentado novamente é o de falsificação.




(a) Número de cadeias Totais

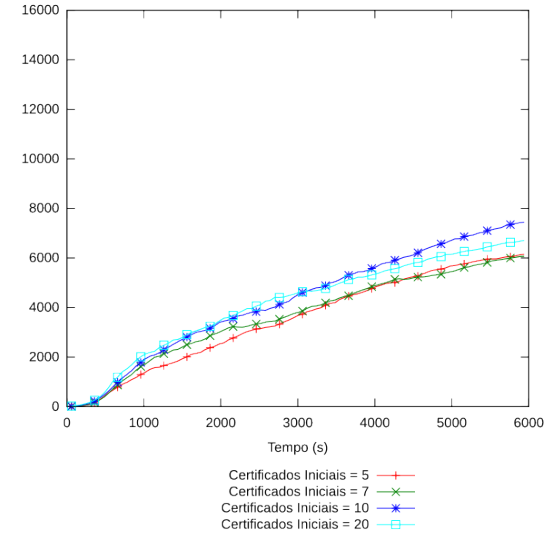
(b) Número de cadeias Fechadas

(c) Número de cadeias Abertas

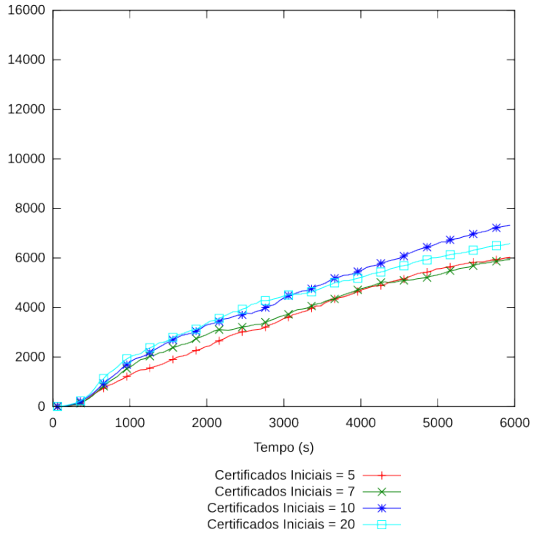
(d) Tamanho médio das cadeias

Figura 4.69: Resultados para 50 nodos, $m = 10\%$ e $N_a = 10\%$

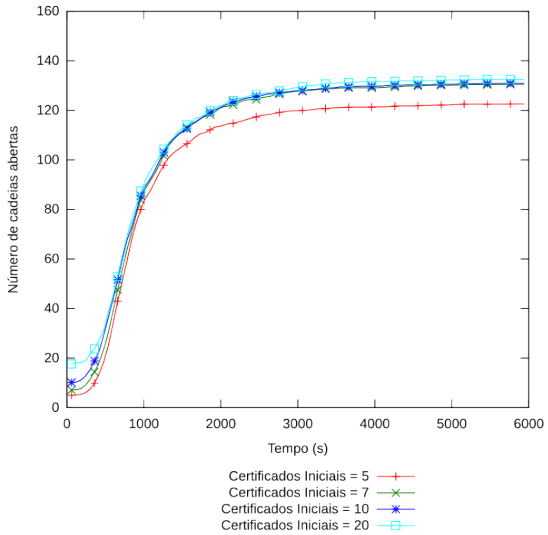
Na Figura 4.69 estão os resultado para $m = 10\%$ e $N_a = 10\%$ com 50 nodos. A quantidade de cadeias abertas ao fim do tempo de simulação ficou entre 80 e 90%. Contudo a quantidade de cadeias totais não apresentou sinais de queda, o que pode indicar que o tempo simulado foi insuficiente para esse conjunto de parâmetros. Ainda pode-se explicitar que dentre os resultados obtidos para esse tipo de distribuição, é o primeiro conjunto que não apresenta a inversão de valores de $C_i$.



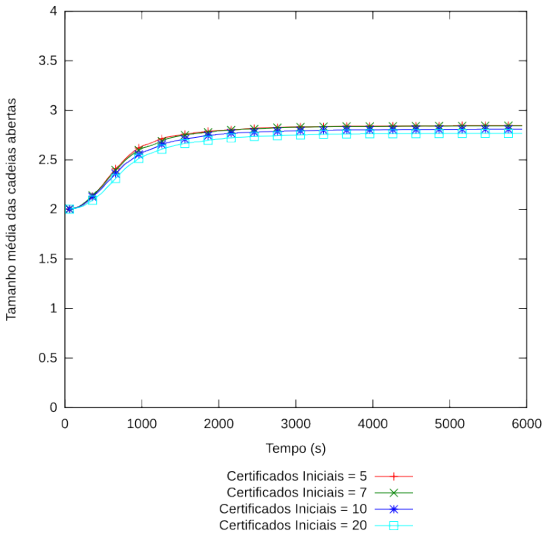

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



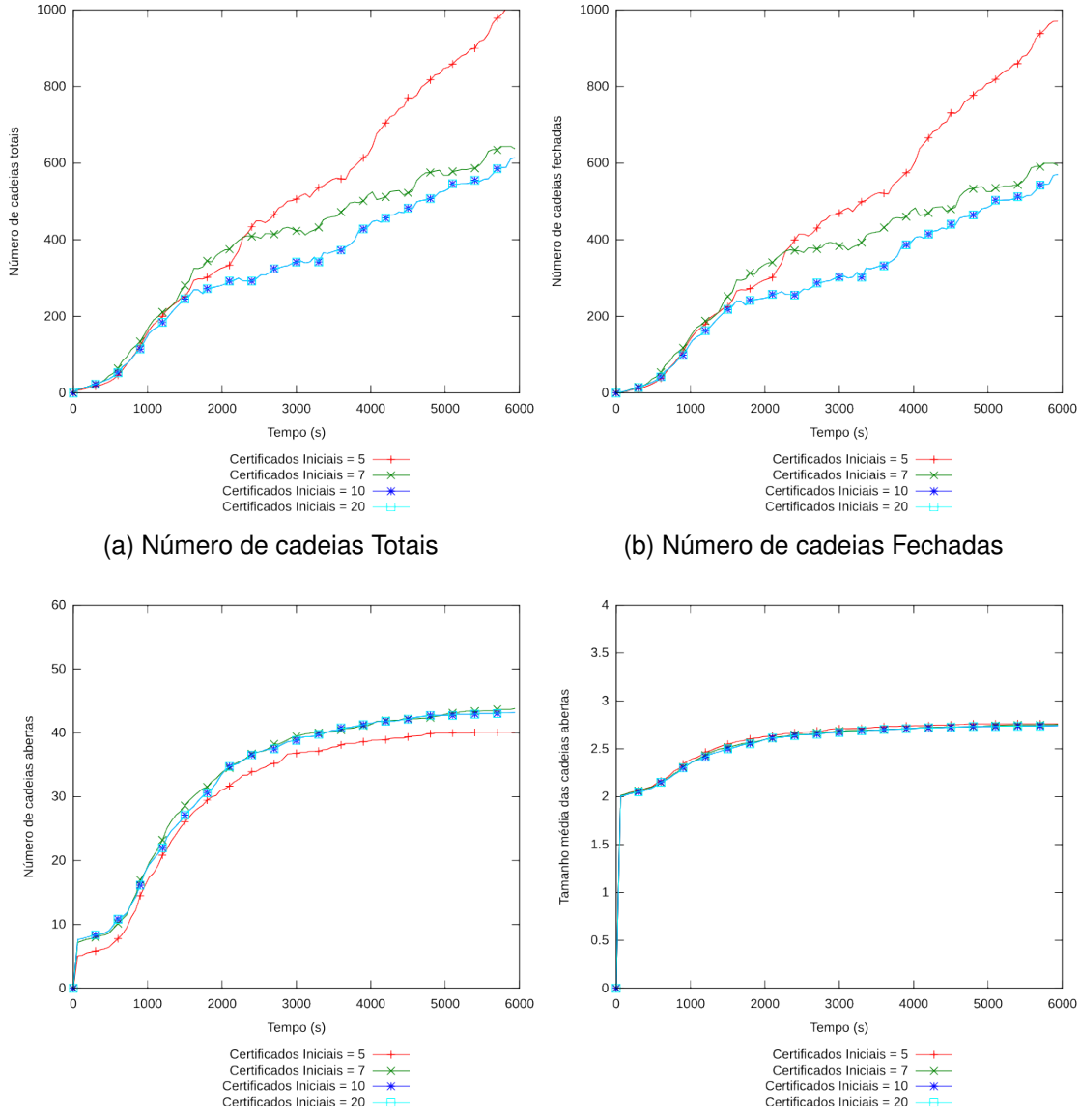

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura 4.70: Resultados para 150 nodos, $m = 10\%$ e $N_a = 10\%$

Ao alterar a quantidade de nodos para 150, pode ver na Figura 4.70 que os resultados foram similares entre si. A quantidade de cadeias totais não apresentou esboços de uma uma queda e não ocupou um elevado espaço de armazenamento. A quantidade de cadeias abertas ao final do tempo de simulação também permaneceu entre 80 e 90%.




(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

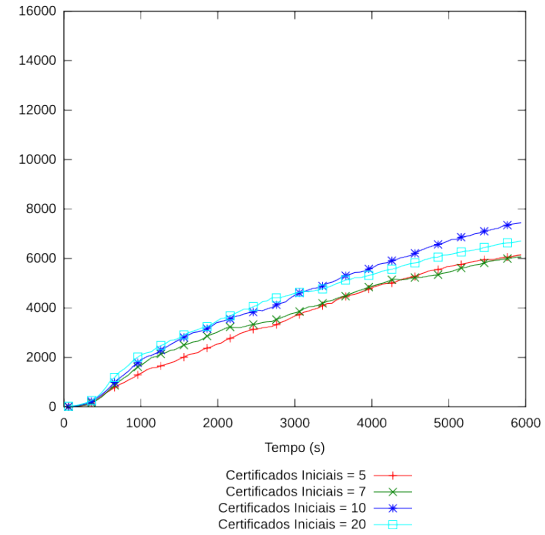
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

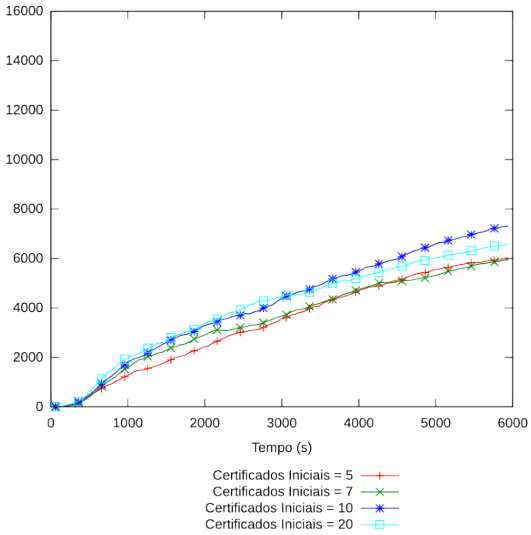
Figura 4.71: Resultados para 50 nodos, $m = 10\%$ e $N_a = 50\%$

As Figuras 4.71 e 4.72 apresentam os resultados para $m = 10\%$ e $N_a = 50\%$ com 50 e 150 nodos.

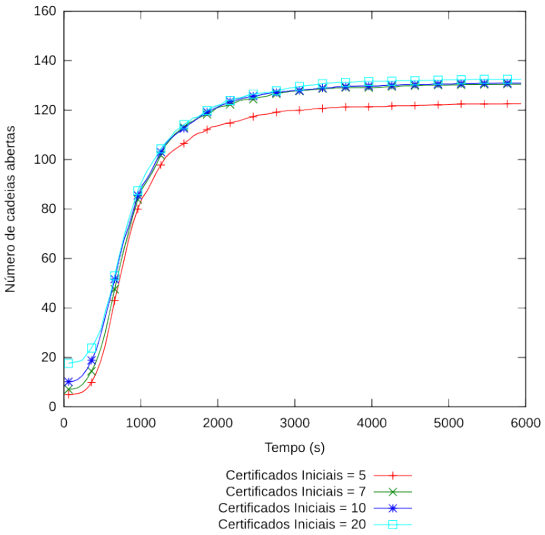
Em ambas as situações, o comportamento apresentado com relação a quantidade total de cadeias foi semalhante, pois os valores são apenas crescentes, não demonstrando qualquer sinal de uma possível queda, mesmo a quantidade de cadeias abertas estando em um mínimo de 80%.



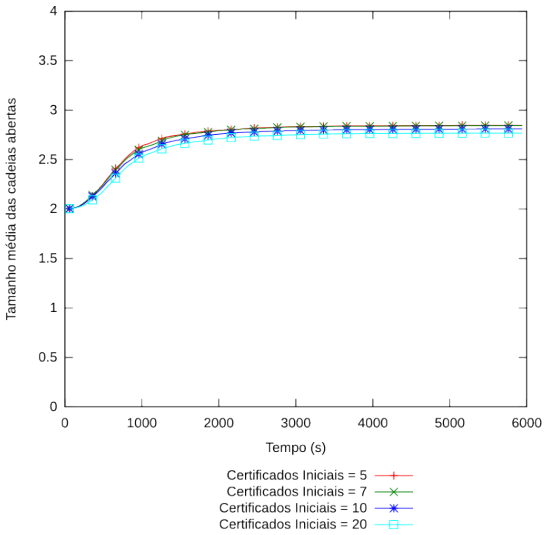

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

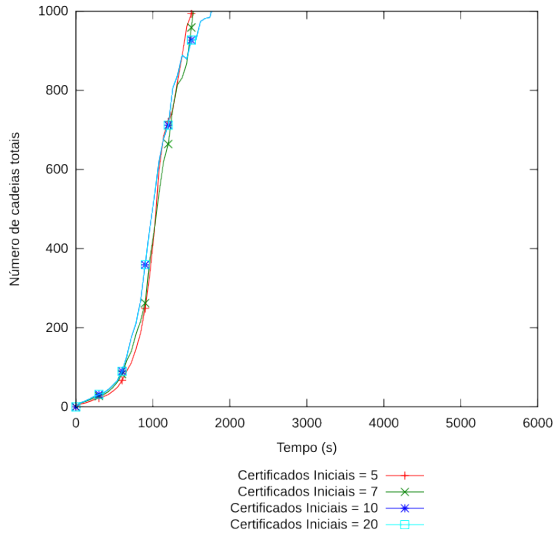



(d) Tamanho médio das cadeias

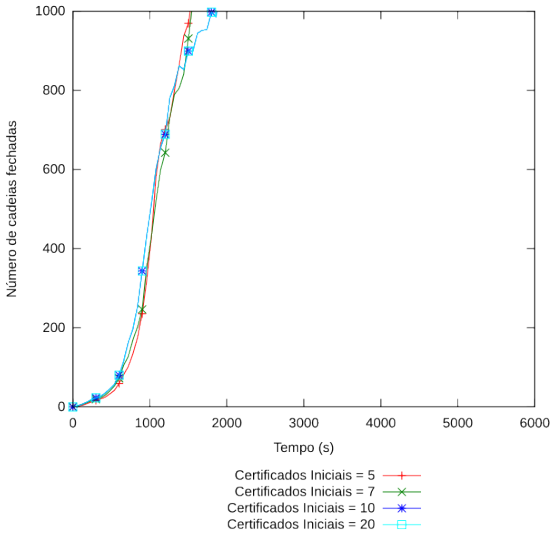
Figura 4.72: Resultados para 150 nodos, $m = 10\%$ e $N_a = 50\%$

Nas Figuras 4.73 e 4.74 observa-se os resultados para 50 e 150 nodos em um ambiente com $m = 50\%$ e $N_a = 10\%$.

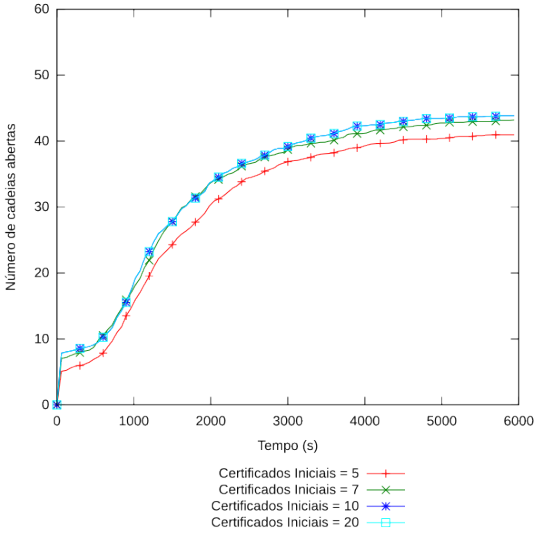
Para 50 nodos, o esquema não convergiu da maneira adequada devido a alta quantidade de cadeias armazenadas durante o tempo e simulação. Embora a quantidade de cadeias abertas tenha sido superior à 80 e pouco abaixo de 90%, a quantidade de cadeias totais ocupou todo o espaço de armazenamento disponível.



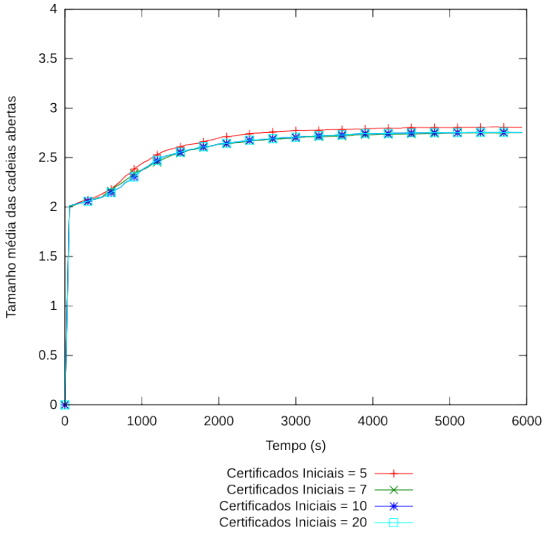

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



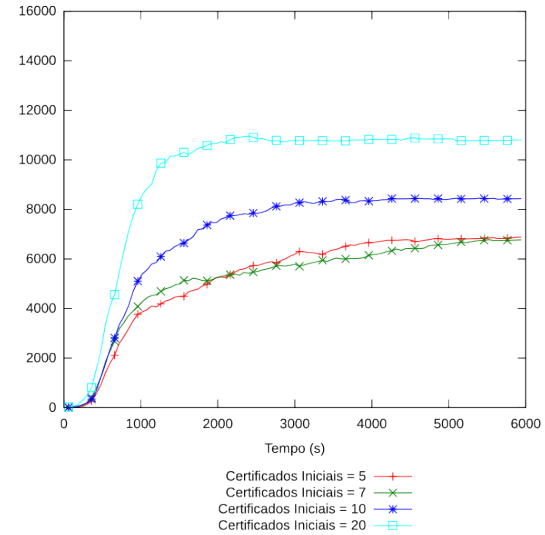

(c) Número de cadeias Abertas



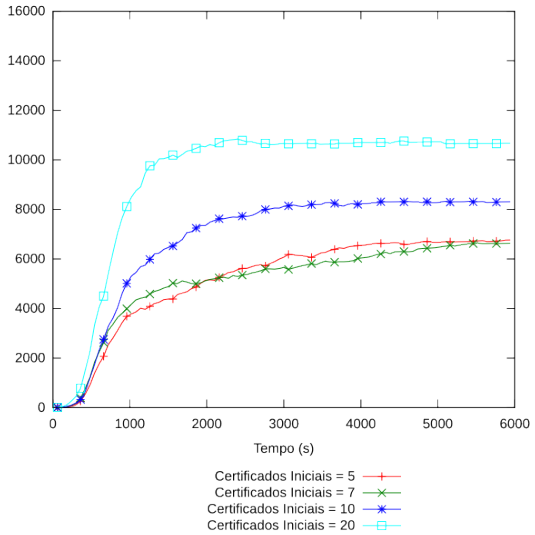

(d) Tamanho médio das cadeias

Figura 4.73: Resultados para 50 nodos, $m = 50\%$ e $N_a = 10\%$

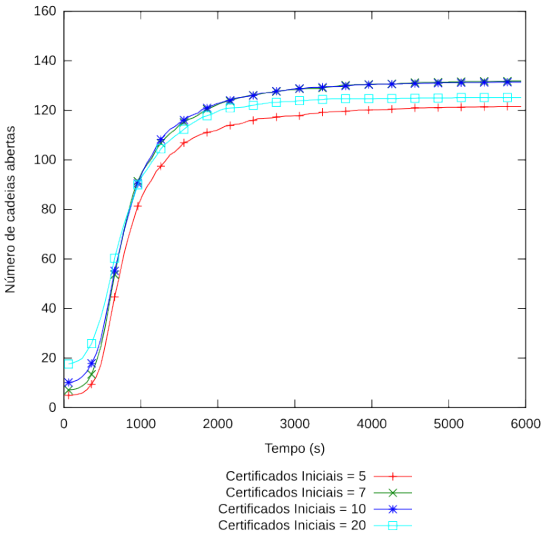
Por meio da Figura 4.74, notas-se que a quantidade de cadeias totais elevou-se até um ponto e estabilizou, diferentemente dos resultados apresentado para esse ataque e forma de distribuição de certificados.



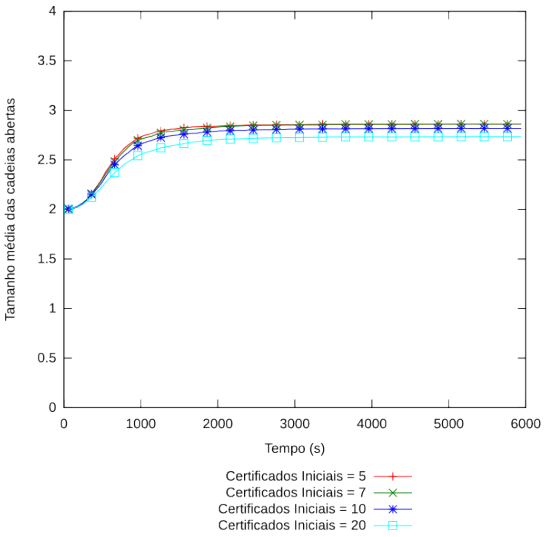

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



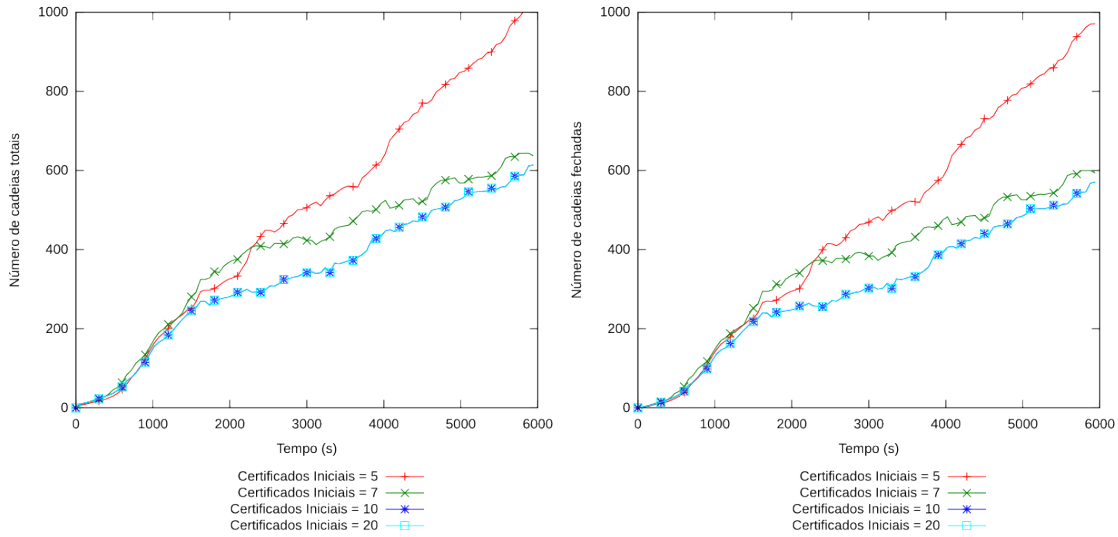

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura 4.74: Resultados para 150 nodos, $m = 50\%$ e $N_a = 10\%$

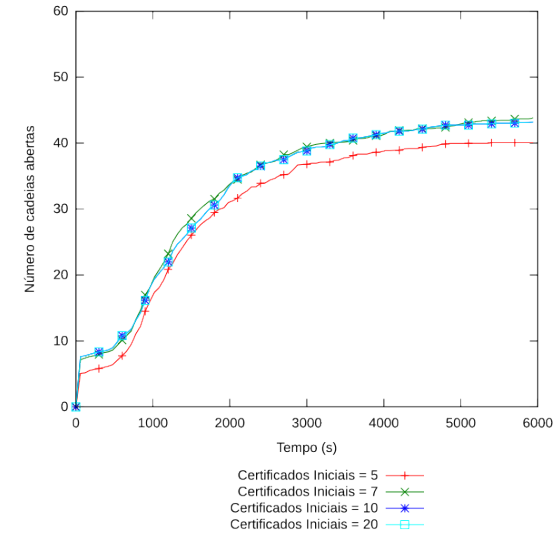
Nas Figuras 4.75 e 4.76 são apresentados os resultados para a combinação mais pessada deste ataque, na qual, $m = 50\%$ e $N_a = 50\%$ para 50 e 150 nodos.



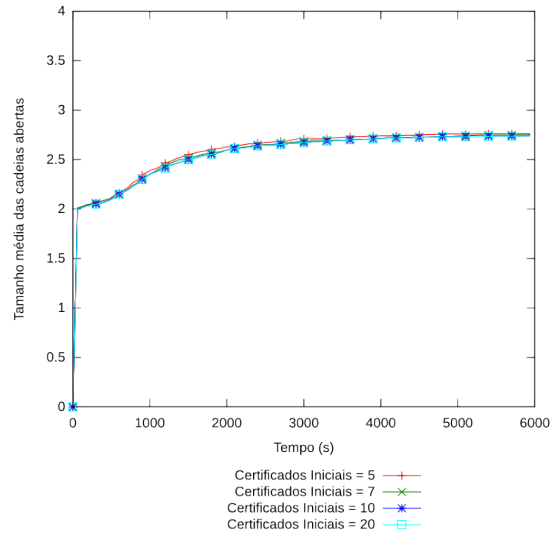

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



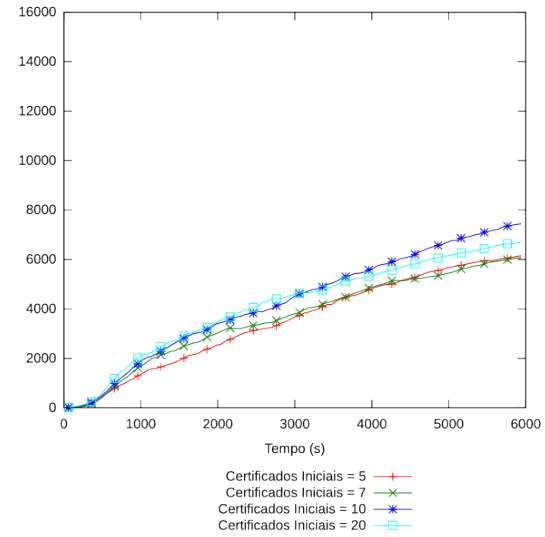

(c) Número de cadeias Abertas



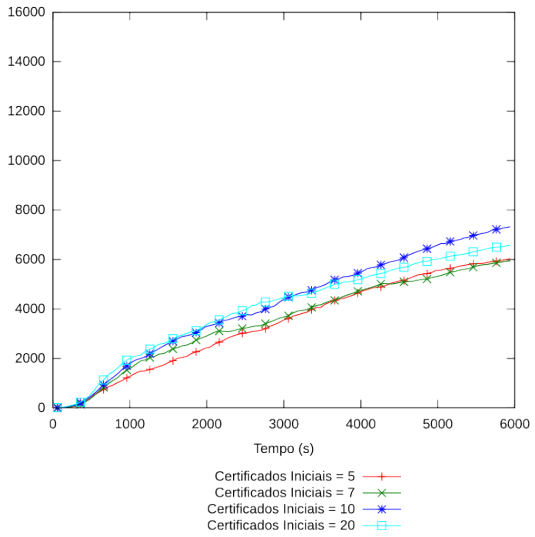

(d) Tamanho médio das cadeias

Figura 4.75: Resultados para 50 nodos, $m = 50\%$ e $N_a = 50\%$

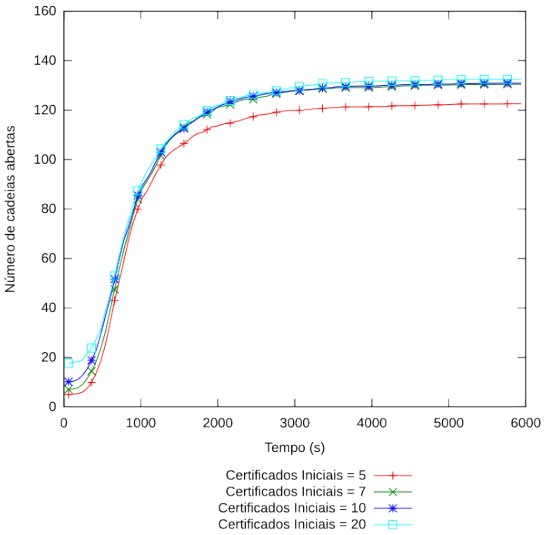
Para as duas quantidade de nodos apresentadas aqui, o comportamento novamente foi semelhante ao encontrado anteriormente. A quantidade de cadeias total apenas cresceu durante o tempo simulado e a quantidade de cadeias abertas atingiu valores entre 80 e 90%.



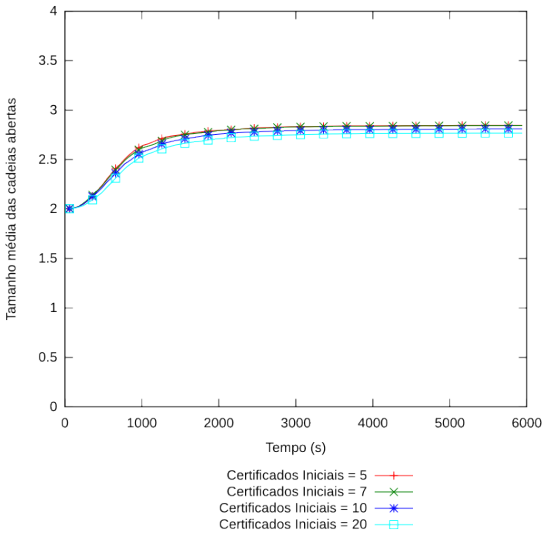

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura 4.76: Resultados para 150 nodos, $m = 50\%$ e $N_a = 50\%$

Com a apresentação desses resultados, pode-se inferir que essa forma de distribuição interfere negativamente no esquema, seja não convergindo ou elevando o tempo tempo necessário para isso e ainda elevando o uso do espaço de armazenamento de cadeias.

## 4.5 Conclusões

Mostrou-se nesse capítulo os resultados do esquema proposto demonstrando que em algum momento todos os nodos possuem todas as chaves da rede. Mostrou-se também que mesmo utilizando o mapa de uma cidade como cenário, os nodos podem ser alcançados com, em média, apenas 1 intermediário. Observou-se ainda que, sob ataques diversos, o esquema consegui atingir o objetivo principal que é convergir para que todos os nodos possíveis possuam as chaves dos demais nodos.

As simulações foram realizadas com diversos valores de $C_i$, mas de maneira geral, para valores inferiores a 7 o esquema tem certa dificuldade ou até mesmo não funciona corretamente. Para valores maiores ou igual a 10, o esquema funcionou de maneira satisfatória na maioria das situações, desta forma, conclui-se que não é necessário mais de 10 certificados iniciais para que o esquema consiga convergir independente da quantidade de nós na rede.

Conclui-se que a forma de distribuição de certificados iniciais interfere no esquema, tanto no tempo de convergência, quanto na quantidade de cadeias totais mantidas durante o processo. Explicita-se que a distribuição homogênea e a heterogênea obtém resultados similares, no entanto, uma distribuição centralizada em pouco nodos prejudica o esquema em ambientes livres de nodos atacantes e em ambientes com nodos maliciosos.

# CAPÍTULO 5

# CONCLUSÃO E TRABALHOS FUTUROS

As DTNs, assim como as redes *Ad-Hoc*, têm muitos problemas com segurança devido à forma como acontece a comunicação entre os participantes da rede, via sinais de rádio. Como os sinais percorrem o ar, pessoas má intencionadas podem realizar ataques diretos ao funcionamento da rede, como *blackholes* e de falsificação, ou mesmo realizar ataques voltados a obter os dados que transitam na rede.

Uma maneira de evitar alguns desses ataques é o uso de criptografia, na qual os nodos cifram suas mensagens com chaves criptográficas para que apenas quem possua essa chave (sistema simétrico) ou outra que faça par com essa chave (sistema assimétrico - par de chaves pública e privada) possa ter acesso aos dados. Com o uso de determinados algoritmos é possível ainda usar essas chaves para criação de assinaturas digitais, para que assim, os outros nodos possam ter uma maior confiança na origem da mensagem.

O acréscimo de chaves para os nodos da rede, criou uma tarefa de administração, que é chamada de gerenciamento de chaves, na qual alguma entidade é responsável por distribuir, armazenar, validar, revogar e garantir a real relação entre chave e nodo. Essa tarefa pode ser desempenha por uma entidade interna, externa, centralizada ou mesmo ser distribuída pelos nodos que fazem parte da rede. Nas DTNs, para que se tenha sucesso na administração das chaves o esquema de gerenciamento precisa ser distribuído e auto-organizado, além de tudo, considerar a sua principal característica, falta de contato por intervalos de tempo indeterminados.

Foram encontrados alguns esquemas de gerenciamento de chaves para DTNs, como por exemplo sistemas baseados em árvores (HIBC e OBBA-FAT) ou em trocas de chaves assimétricas. Observou-se vários problemas nesses gerenciadores de chaves, como a necessidade da existência de nodos chave na rede (PKGs) responsáveis por realizar as tarefas de validação e de repasse na estrutura de árvore utilizada. Há também a possiblidade de falsificação das chaves enviadas quando feita de forma simples e direta.

No esquema proposto, ao iniciar a rede, cada nodo certifica alguns outros nodos. Ao repassar esse certificados, essa mensagem vai cifrada com a chave privada do nodo, criando assim uma mensagem assinada digitalmente. Apenas os nodos que possuam a chave pública desse nodo poderão abrí-la. Os nodos que recebem mensagens contendo os certificados assinados os repassam com sua própria assinatura digital, gerando assim uma cadeia de assinaturas.

Cada nodo que recebe essa mensagem a repassa a outros nodos assinando com sua própria chave privada, criando assim uma cadeia de assinaturas digitais.

Os nodos seguem armazenando essas cadeias ao longo da rede e classificando-as em dois grupos, cadeias abertas e cadeias fechadas. As cadeias fechadas são aquelas que devido a falta de alguma chave pública, o nodo não pode verificar a assinatura digital e consequentemente, abrir o restante da cadeia. Cadeias abertas são todas as cadeias que o nodo conseguiu validar todas as assinaturas e obteve a chave pública da origem. Ao obter mais chaves públicas, o nodo aumenta a possibilidade de abrir novas cadeias.

Cada nodo pode manter diversas cadeias fechadas para um mesmo nodo alvo, entretanto, mantém apenas a menor cadeia aberta para um mesmo nodo. Desta forma, com o decorrer do tempo, a quantidade de dados transmitida pelos nodos vai reduzindo-se gradativamente.

Foram feitas simulações para validar o esquema proposto em um simulador desenvolvido em Java chamado de *The One*. Os resultados obtidos mostraram que na versão inicial desenvolvida, os nodos obtinham cadeias para todos os nodos de forma rápida, entretanto ao custo de um um uso indiscriminado de memória. Assim, foram feitas mudanças na maneira como as cadeias eram abertas e repassadas, afim de otimizar o armazenamento das cadeias. Ao observar os resultados desta versão, pode-se notar que o tempo manteve próximo do obtido anteriormente, com um certo ganho, mas com um uso mais eficiente da memória dos nodos.

Observou-se também que o tamanho médio das cadeias manteve-se próximo de 3, indicando o uso de apenas um intermediário para a troca de mensagens. Esse valor manteve-se por todas as simulações realizadas.

Afim de validar o esquema em situações de risco, foram feitas simulações de ataques de *blackholes* e *greyholes*, *sybil* e falsificação, este com ataques independentes e com ataque em grupo.

Todas as situações foram analisadas com três formas distintas de distribuição de certificados iniciais. Uma distribuição homogênea, na qual todos os nodos começavam com a mesma quantidade de certificados. Uma distribuição heterogênea, na qual a quantidade de certificados iniciais variava de nodo para nodo. E por fim, uma distribuição mais centralizada dos certificados, na qual 10% dos nodos possuem muitos certificados e o restante três.

Na maioria das situações o esquema conseguiu convergir ao ponto em que todos os nodos conheciam todos os outros nodos, ou ao menos, 90% deles. Entretanto, isso aconteceu somente quando a quantidade de certificados iniciais na rede foi igual ou maior que 10 vezes o número de nodos na rede.

Assim, pode-se concluir que o esquema proposto para o gerenciamento e distribuição de chaves em DTNs atingiu o objetivo esperado de distribuir as chaves pela

rede em ambiente sem interferência de nodos atacantes ou mesmo naqueles com a presença desse tipo de nodo.

Propõem-se como trabalhos futuros verificar o impacto do uso do esquema proposto sobre o tráfico de dados da rede; acrescentar um sistema de confiabilidade entre os nodos para então alterar o modo de seleção de cadeias abertas; simular o esquema proposto em conjunto com o *Bundle Protocol*; expor o esquema a novo ataques como por exemplo, o de inundação.

# REFERÊNCIAS


[1] MEHRAN ABOLHASAN, T. W.; DUTKIEWICZ, E. A review of routing protocols for mobile ad-hoc networks. **Ad-Hoc Networks**, v. 2, n. 1, p. 1–22, May 2004.

[2] BROCH, J.; MALTZ, D. A.; JOHNSON, D. B.; HU, Y.-C.; JETCHEVA, J. A performance comparison of multi-hop wireless ad-hoc network routing protocols. In: Annual International Conference on Mobile Computing and Networking, 4. New York, NY, USA, ACM. p. 85–97, 2001.

[3] LI, J.; BLAKE, C.; DE COUTO, D. S.; LEE, H. I.; MORRIS, R. Capacity of ad-hoc wireless networks. In: Annual international Conference on Mobile Computing and Networking, 7. New York, NY, USA, ACM. p. 61–69, 2001.

[4] L.C.P. ALBINI, A. CARUSO, S. C.; MAESTRINI, P. Reliable routing in wireless ad-hoc networks: The virtual routing protocol. **Network and Systems Management**, v. 14, n. 3, p. 335–358, 2006.

[5] BOPPANA, R. V.; KONDURU, S. P. An adaptive distance vector routing algorithm for mobile ad-hoc networks. **INFOCOM**, v. 3, p. 1753–1762, Apr. 2001.

[6] BANNACK, A. **Aplicando gestão de energia ao protocolo de roteamento para redes ad-hoc móveis vrp**. 2008. Dissertação (Mestrado em Informática) - Universidade Federal do Paraná, Programa de Pós-Graduação em Informática, Curitiba, Paraná, Brasil, 2008.

[7] ARGYROUDIS, P.; O'MAHONY, D. Secure routing for mobile ad-hoc networks. **IEEE Communications Surveys and Tutorials**, v. 7, n. 3, p. 2–21, 2005.

[8] BANNACK, A.; DA SILVA, E.; LIMA, M. N.; DOS SANTOS, A. L.; ALBINI, L. C. P. Segurança em redes ad-hoc. In: Simpósio Brasileiro de Telecomunicações, 26. 2008.

[9] C. T. DE OLIVEIRA, M. D. D. MOREIRA, M. G. R. L. H. M. K. C.; DUARTE., O. C. M. B. Redes tolerantes a atrasos e desconexões. In: Simpósio Brasieliro de Redes de Computadores e Sistemas Distribuídos. 2007.

[10] GROUP, N. W. Delay-tolerant networking architecture, request for comments: 4838. http://www.ietf.org/rfc/rfc4838.txt. Jan. 2013.

[11] E. P. C. JONES, L. L.; WARD, P. A. S. Practical routing in delay-tolerant networks. In: Conference of the Special Interest Group on Data Communication. New York, NY, USA, ACM. p. 237–243, 2005.

[12] S. BURLEIGH, A. HOOKE, L. T. K. F. V. C. B. D. K. S.; WEISS, H. Delay-tolerant networking: An approach to interplanetary internet. **IEEE Communications Magazine**, v. 41, n. 6, p. 128–136, 2003.

[13] AES DE MORAES, L. F. M. **Proposta de um mecanismo de segurança baseado em troca de chaves assimétricas para redes tolerantes a atrasos e**

**desconexões**. 2009. Dissertação (Mestrado em Engenharia de Sistemas e Computação) - Universidade Federal do Rio de Janeiro, Instituto Alberto Luiz Coimbra, Curso de Pós-Graduação Engenharia de Sistemas e Computação, Rio de Janeiro, 2009.

[14] DJAMEL DJENOURI, L. K.; BADACHE, N. A survey of security issues in mobile ad-hoc and sensor networks. **IEEE Surveys and Tutorials**, v. 7, n. 4, p. 2–38, 2005.

[15] LUNDBERG, J. **Routing security in ad-hoc networks**. Technical report, Helsinki University of Technology, 2000.

[16] AGRAWAL, P., G. R. K.; DAS, S. K. Cooperative black and gray hole attacks in mobile ad hoc networks. In: International Conference on Ubiquitous Information Management and Communication, 2. 2008.

[17] AL-SHURMAN, M., Y. S.-M.; PARK, S. Black hole attack in mobile ad hoc networks. In: Southeast regional conference, 42. 2004.

[18] DOUCEUR, J. R. The sybil attack. In: International Workshop on Peer-to-Peer Systems, 1. 2001.

[19] DA SILVA, E. **Gerenciamento de chaves públicas sobrevivente baseado em grupos para manets**. 2009. Tese (Doutorado em Informática) - Universidade Federal do Paraná, Programa de Pós-Graduação em Informática, Curitiba, Paraná, Brasil, 2009.

[20] STALLINGS, W. **Data and computer communications**. 8. ed. Prentice Hall, 2006.

[21] DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. **IEEE Transactions on Information Theory**, v. 22, n. 6, p. 644–654, 1976.

[22] SCHENEIER, B. **Applied cryptography**: an introduction to perturbative methods in gauge theories. 2. ed. USA, Wiley, 1996.

[23] A. J. MENEZES, P. C. V. O.; VANSTONE, S. A. **Handbook of applied cryptography**. Danvers, MA, USA, CRC Press, 1996.

[24] JOHANN VAN DER MERWE, D. D.; MCDONALD, S. A survey on peer-to-peer key management for mobile ad-hoc networks. **ACM Computing Survey**, v. 1, n. 39, 2007.

[25] ARAM KHALILI, J. K.; ARBAUGH, W. A. Toward secure key distributionin truly ad-hoc networks. In: Symposium on Applications and the Internet Workshops. Washington, DC, USA, IEEE. p. 342, 2003.

[26] SRDJAN CAPKUN, L. B.; HUBAUX, J.-P. Self-organized public-key management for mobile ad-hoc networks. **IEEE Transactions on Mobile Computing**, v. 2, n. 1, p. 52–64, 2003.

[27] SRDJAN CAPKUN, L. B.; HUBAUX, J.-P. The quest for security in mobile ad-hoc networks. In: International Symposium on Mobile Ad Hoc Networking and Computing, 2. ACM. p. 146–155, 2001.

[28] SRDJAN CAPKUN, L. B.; HUBAUX, J.-P. Mobility helps peer-to-peer. **IEEE Transactions on Mobile Computing**, v. 5, n. 1, p. 43–51, 2006.

[29] SILVA, R. F. E. **Sistema de gerenciamento de chaves públicas baseado em virtualização para redes ad-hoc móveis**. 2010. Dissertação (Mestrado em Informática) - Universidade Federal do Paraná, Programa de Pós-Graduação em Informática, Curitiba, Paraná, Brasil, 2010.

[30] NGAI, E. C. H.; LYU, M. R. Trust and clustering based authentication services in mobile ad-hoc networks. In: International Conference on Distributed Computing Systems Workshops, 24. Washington, DC, USA, IEEE. p. 582–587, 2004.

[31] EDITH C. H. NGAI, M. R. L.; CHIN, R. T. An authentication service against dishonest users in mobile ad-hoc networks. In: Aerospace Conference. IEEE. p. 1275–1285, 2004.

[32] ESCHENAUER, L.; GLIGOR, V. D. A key-management scheme for distributed sensor networks. In: Conference on Computer and Communications Security, 9. New York, NY, USA, ACM. p. 41–47, 2002.

[33] SRDJAN CAPKUN, L. B.; HUBAUX, J.-P. Mobility helps security in ad-hoc networks. In: International Symposium on Mobile Ad Hoc Networking and Computing, 4. New York, NY, USA, ACM. p. 46–56, 2003.

[34] ZIMMERMANN, P. R. **The official pgp user's guide**. Cambridge, MA, USA, MIT Press, 1995.

[35] SETH, A.; KESHAV, S. Practical security for disconnected nodes. In: ICNP Workshop, 1. IEEE. 2005.

[36] KATE, G. Z. A.; HENGARTNER, U. Anonymity and security in delay tolerant networks. In: International Conference on Security and Privacy in Communication Networks, 3. EAI. 2007.

[37] ZHU, H. **Security in delay tolerant networks**. 2009. Tese (Doutorado em Engenharia Elétrica e da Computação) - University of Waterloo, Waterloo, Ontario, Canada, 2009.

[38] ZIMING SONG, C. W.; TANG, Z. An efficient group signature scheme in ferry-based delay-tolerant networks. In: International Conference on Computer and Information Technology, 10. Changsha, Hunan, China, IEEE. 2010.

[39] ANIKET KATE, G. M. Z.; CHERITON, U. H. D. R. Anonymity and security in delay tolerant networks. In: International Conference on Security and Privacy in Communications Networks and the Workshops, 3. IEEE. p. 504–513, 2007.

[40] FRANCK, L.; GIL-CASTINEIRA, F. International symposium on industrial electronics. In: Security and Privacy in Communications Networks and the Workshops. IEEE. p. 2573–2578, 2007.

[41] RONGXING LU, X. L.; SHEN, X. S. Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks. **INFOCOM**, 2010.

[42] N.BHUTTA, G.ANSA, E. J. N. A. M. A.; H.CRUICKSHANK. Security analysis for delay/disruption tolerant satellite and sensor networks. In: International Workshop on Satellite and Space Communications. IEEE. p. 385–389, 2009.

[43] H. W. S. SYMINGTON, S. F.; LOVELL, P. Bundle security protocol specification. 2009.

[44] FARRELL, S.; CAHILL, V. Security considerations in space and delay tolerant networks. In: International Conference on Space Mission Challenges for Information Technology, 2. Washington, DC, USA, IEEE. p. 29–38, 2006.

[45] GROUP, N. W. Bundle security protocol specification, request for comments: 6257. http://www.rfc-editor.org/rfc/rfc6257.txt. Jan. 2013.

[46] GROUP, N. W. Bundle protocol specification, request for comments: 5050. http://tools.ietf.org/rfc/rfc5050.txt. Jan. 2013.

[47] Internet research task force. http://www.irtf.org/.

[48] Delay-tolerant networking research group. http://irtf.org/dtnrg.

[49] CHA, J. C.; CHEON, J. H. An identity-based signature from gap diffie-hellman groups. p. 18–30, 2003.

[50] MERKLE, R. Protocols for public key cryptosystems. In: S and P. IEEE. 1980.

[51] K. REN, W. L.; ZHANG, Y. Multi-user broadcast authentication in wireless sensor networks. In: SECON. IEEE. 2007.

[52] A. KERÄNEN, J. O.; KÄRKKÄINEN, T. The one simulator for dtn protocol evaluation. In: International Conference on Simulation Tools and Techniques, 2. New York, NY, USA, ACM. 2009.

[53] FERNANDEZ, H. M. R.; ECKEL, W. D. **Gerenciamento de chaves assimétricas baseado em votação ara redes tolerantes a atrasos e desconexões**. 2011, Curitiba, Paraná, Brasil, 2011.

[54] DIFFIE, W.; HELLMAN, M. New directions in cryptography. **IEEE Transactions on information Theory**, v. IT-22, n. 6, p. 644–654, Nov. 1976.

[55] VAHDAT, A.; BECKER, D. **Epidemic routing for partially connected ad-hoc networks**. Technical report, Duke University, 2000.

[56] THRASYVOULOS SPYROPOULOS, KONSTANTINOS PSOUNIS, C. S. R. In: .

[57] LINDGREN, A.; DORIA, A.; SCHELEN, O. Probabilistic routing in intermittently connected networks. In: SIGMOBILE Mobile Computing and Communication Review. ACM. 2004.

[58] COUTINHO, S. C. **Números inteiros e criptografia rsa**. IMPA, 2000.

[59] OF STANDARDS, N. I.; TECHNOLOGY. **Fips 180-2, secure hash standard, federal information processing standard (fips)**. Technical report, Department of Commerce, 2002.

[60] N. FERGUSON, B. S. **Practical cryptography**. Wiley, 2003.

[61] LLOYD WOOD, WES EDDY, P. H. A bundle of problems. In: Aerospace conference. Big Sky, Montana, USA, IEEE. 2009.

# APÊNDICE A

## *BUNDLE PROTOCOL*

Um dos principais protocolos para DTN encontrado é o *Bundle Protocol* [43] desenvolvido por um grupo de pesquisa do *Internet Research Task Force*[47], chamado *Delay Tolerant Networking Research Group*[48]. Nesse esquema a segurança é aplicada sobre a camada de agregação, dividindo-a em três blocos: o Bloco de Autenticação Agregado/*Bundle Authentication Block* (BAB), o Bloco de Integridade da Carga Útil/*Payload Integrity Block* (PIB) e o Bloco de Confidencialidade da Carga Útil/*Payload Confidentiality Block* (PCB).

O Bloco de Autenticação Agregado tem como objetivo prover autenticação. Para tanto, provê autenticidade e integridade em comunicações salto a salto. Devido a isso, as informações desse bloco são computadas a cada envio de mensagem.

Na especificação do BAB há apenas definidos os códigos de tipificaçao que devem ser usados para identificar o bloco. Permitindo ao utilizador fazer a escollha do sistema de codificação utilizado para cifrar e decifrar as mensagens. Todavia, são apontadas algumas opções, como a possibilidade de ser usado qualquer tipo de codificação de mensagens para assinaturas digitais, como, por exemplo, o RSA. Uma segunda alternativa é o uso de chaves simétricas baseadas em funções *hash*. Neste caso, o nodo intermediário ou mesmo o nodo destino, ao receber uma mensagem faz o cálculo do *hash* da mensagem, caso não coincida com o informado pelo nodo que enviou a mensagem, ela é descartada. O fluxo desse bloco é exemplificado na Figura A.1:

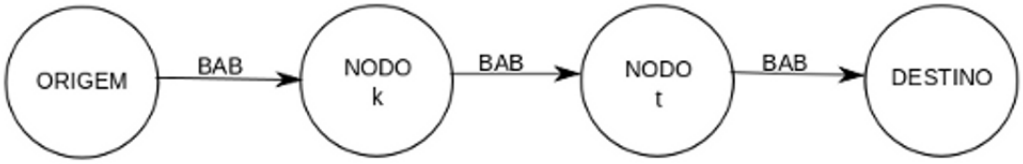



Figura A.1: Autenticação e Integridade Salto a Salto do BAB

O Bloco de Integridade da Carga Útil tem como objetivo prover autenticidade e integridade entre origem e destino, mas pode ser checado salto a salto. Para que seja validado salto a salto, existe a premissa de que a forma de codificação de mensagens empregada seja a de assinaturas digitais (criptografia assimétrica) ou chave de grupo (criptografia simétrica). Assim os nodos presentes na rota, caso tenham a chave pública da origem, podem abrir a mensagem. Diferente da especificação do BAB, o DTNRG deixou mais restrita a forma de implementação do PIB. Caso sejam usadas

assinaturas digitais, deve-se utilizar o algoritmo de criptografia RSA com SHA256 (Secure Hash Algorithm/Algoritmo de Hash Seguro (SHA)), para que as características do bloco sejam mantidas. Para maiores detalhes sobre o RSA ou o SHA, o leitor deve seguir estas referências [58][59][60].

Para que o PIB seja adicionado na mensagem, é necessário que o BAB já tenha sido calculado e adicionado a ela. Desta forma, o PIB encapsula a mensagem já com o BAB. No fluxo de comunicação entre origem e destino, apenas os nodos em posse da chave adequada conseguem verificar a integridade da mensagem e validar a origem desta. Esse fluxo pode ser observado na Figura A.2:

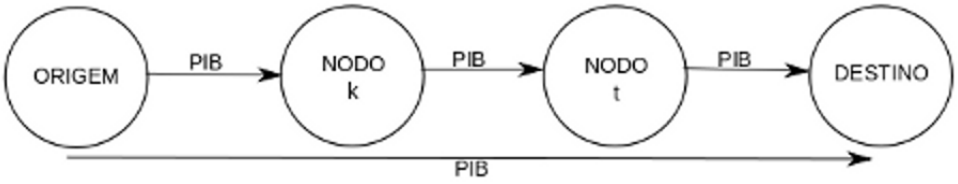



Figura A.2: Integridade Salto a Salto ou Origem/Destino do PIB

O Bloco de Confidencialidade da Carga Útil objetiva assegurar a confidencialidade, ou seja, que somente o destino conseguirá obter as informações enviadas pela origem. Deste modo, o PCB é o bloco com especificação mais restrita dentre os três, na qual há a diretiva de usar o RSA para a criação de chaves de transporte e do AES de 128 bits para a criptografia do corpo da mensagem. A seguir, a Figura A.3 mostra um exemplo de fluxo do PCB.

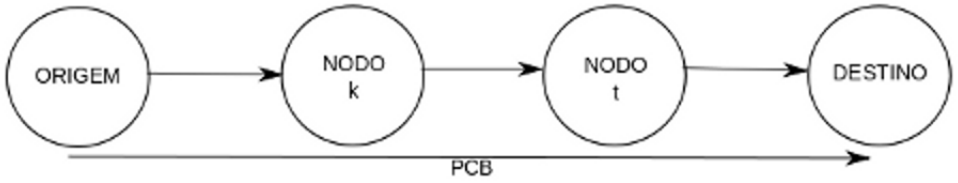



Figura A.3: Confidencialidade entre Origem e Destino - PCB

Um dos problemas desse sistema, dá-se quando o BAB é usado com assinaturas digitais. É a necessidade do pré-compartilhamento das chaves para uso a longo prazo, ou seja, os nodos precisam trocar suas chaves antes da criação da rede. Depois de iniciada a rede, a administração dessas chaves é lenta com relação a revogação de chaves. Essa falta de um mecanismo de distribuição de chaves é apresentada em [44].

Outro problema é relacionado ao PIB, pois para que haja validação da integridade do *bundle* pelos nodos intermediários, eles precisam possuir a chave da origem. Con-

siderando a situação em que há problema em um dos intermediários, como por exemplo, uma falha no sistema de armazenamento, o *bundle* pode ser corrompido sem mesmo que o nodo saiba e repassado para seguir até o destino. Isso pode ocasionar inúmeras retransmissões desnecessárias.

Em [61] foram feitos teste práticos com esse protocolo e são apontados mais problemas:

- há erros de localidade temporal, isso se deve a cada nodo criar seus *bundles* usando sua hora local.
- necessidade de sincronismo, porque alguns *bundles* são descartados como expirados;
- falta de confiabilidade, pois não há um sistema de detecção de erros ou de reutilização de blocos de segurança.
- queda de desempenho diante de erros na comunicação entre intermediários;
- *bundles* com tamanhos muito grande causam fragmentação e geram complicações na segurança.

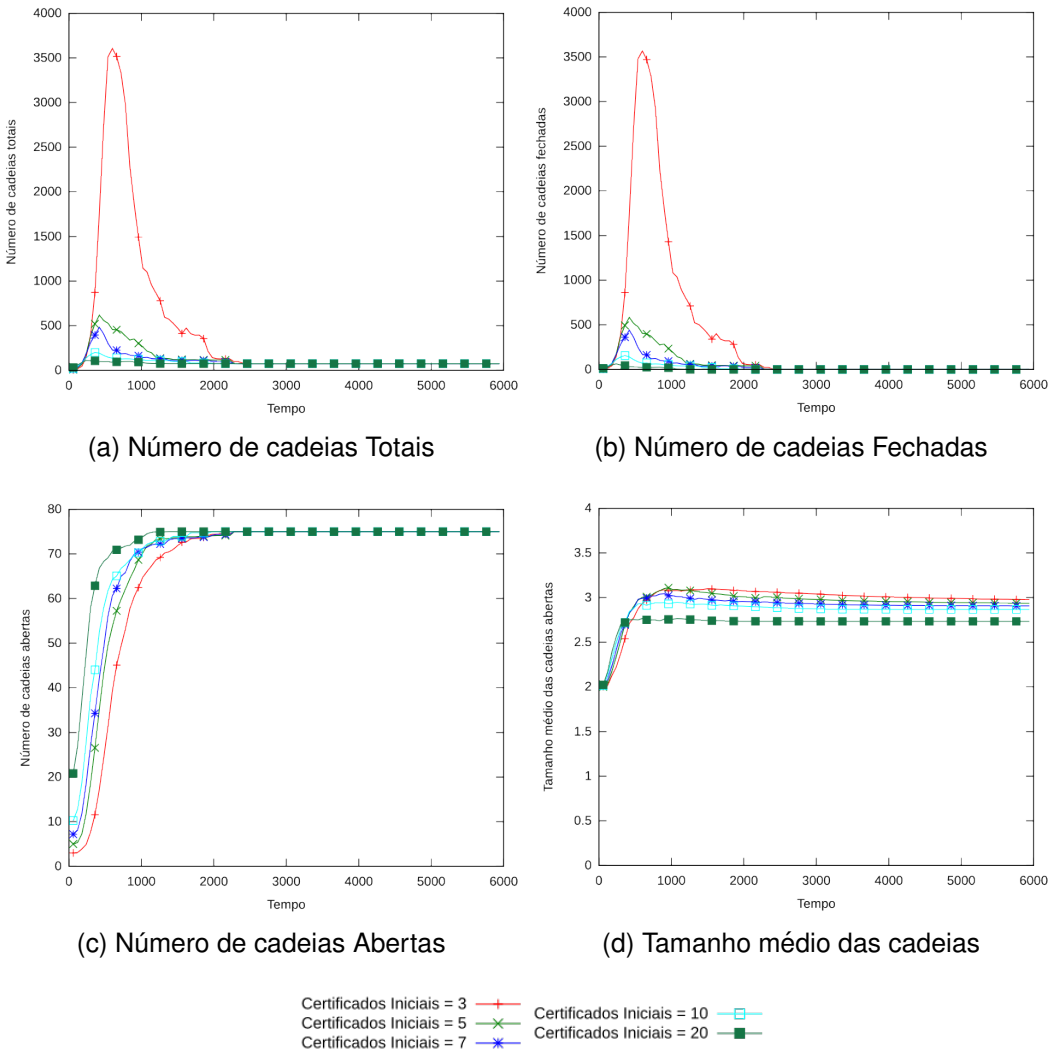
Ainda em [61] é apontado que o *Bundle Protocol* se mais amadurecido, pode um dia torna-se operacional.

# APÊNDICE B

# RESULTADOS - DISTRIBUIÇÃO HOMOGÊNEA DE CERTIFICADOS INICIAIS

Neste apêndice são apresentaddos os gráficos da distribuição homogênea de certificados iniciais que foram omitidos no Capítulo 4. Os gráficos estão organizados da seguinte forma: Versão Inicial, Versão Otimizada seguida dos ataques *GreyHole*, *BlackHole*, *Sybil* e de Falsificação.

## B.1 Versão Inicial



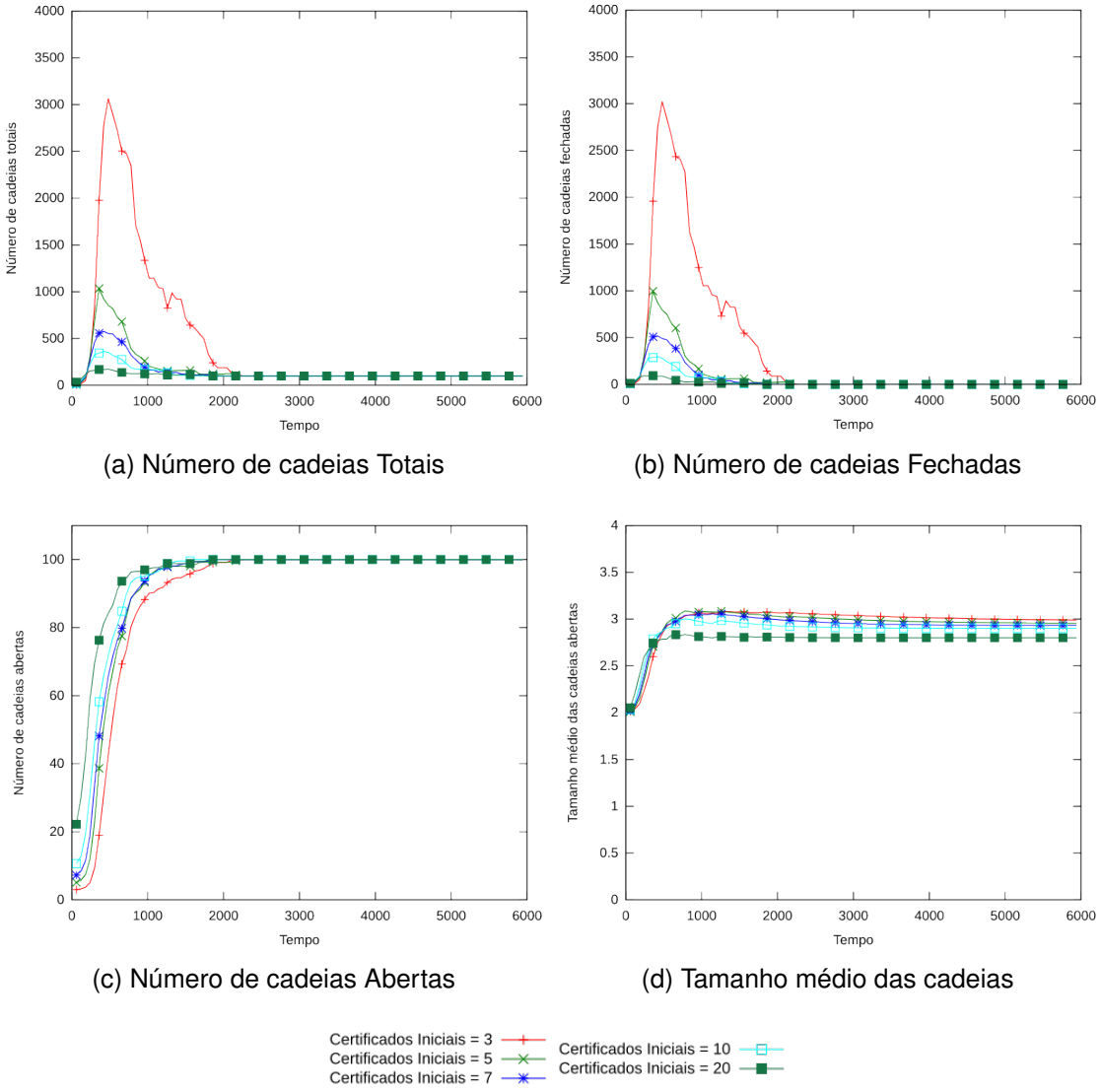

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

Figura B.1: Resultados iniciais para 75 nodos




(a) Número de cadeias Totais

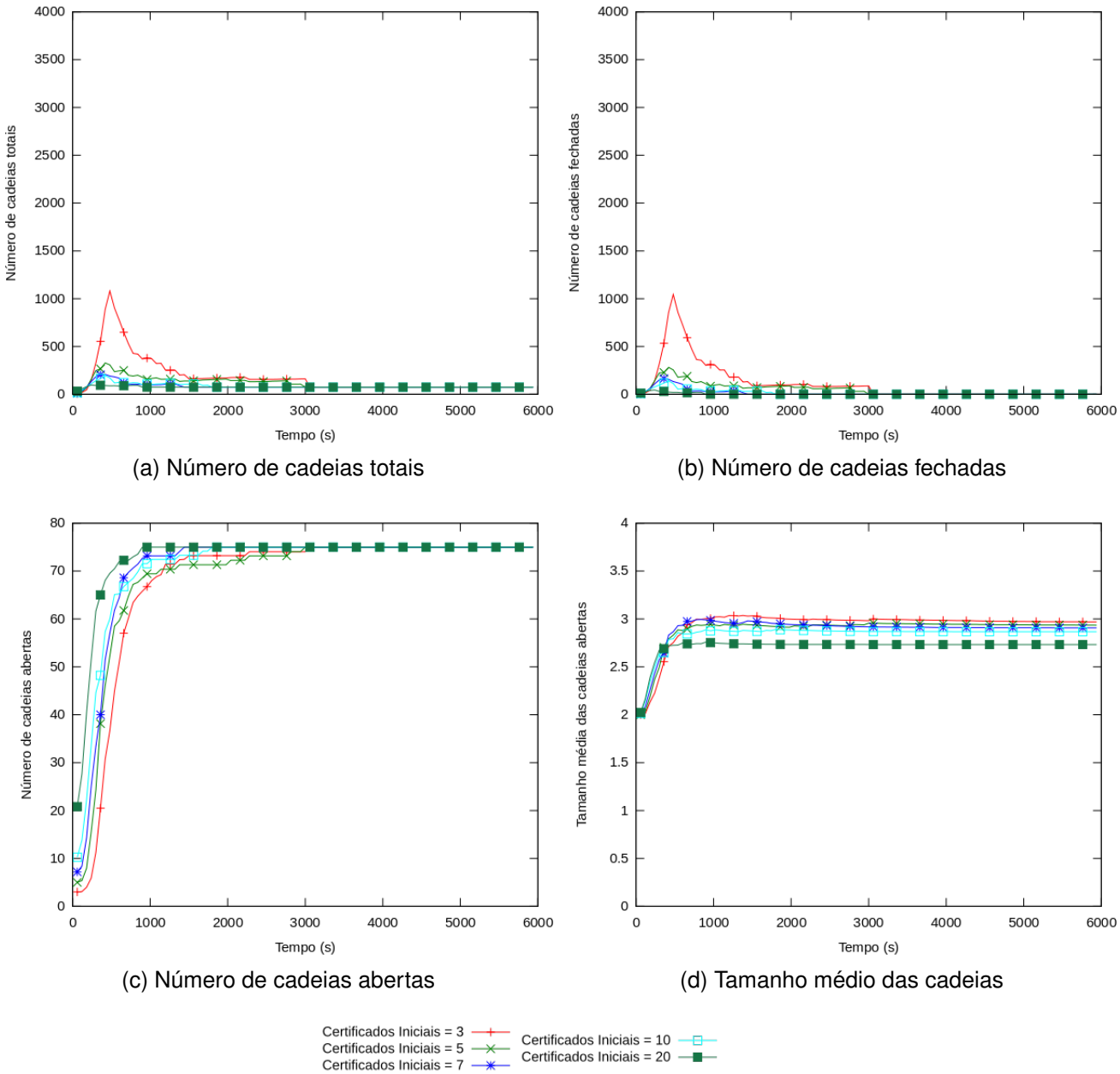
(b) Número de cadeias Fechadas

(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

Figura B.2: Resultados iniciais para 100 nodos

## B.2 Versão Otimizada



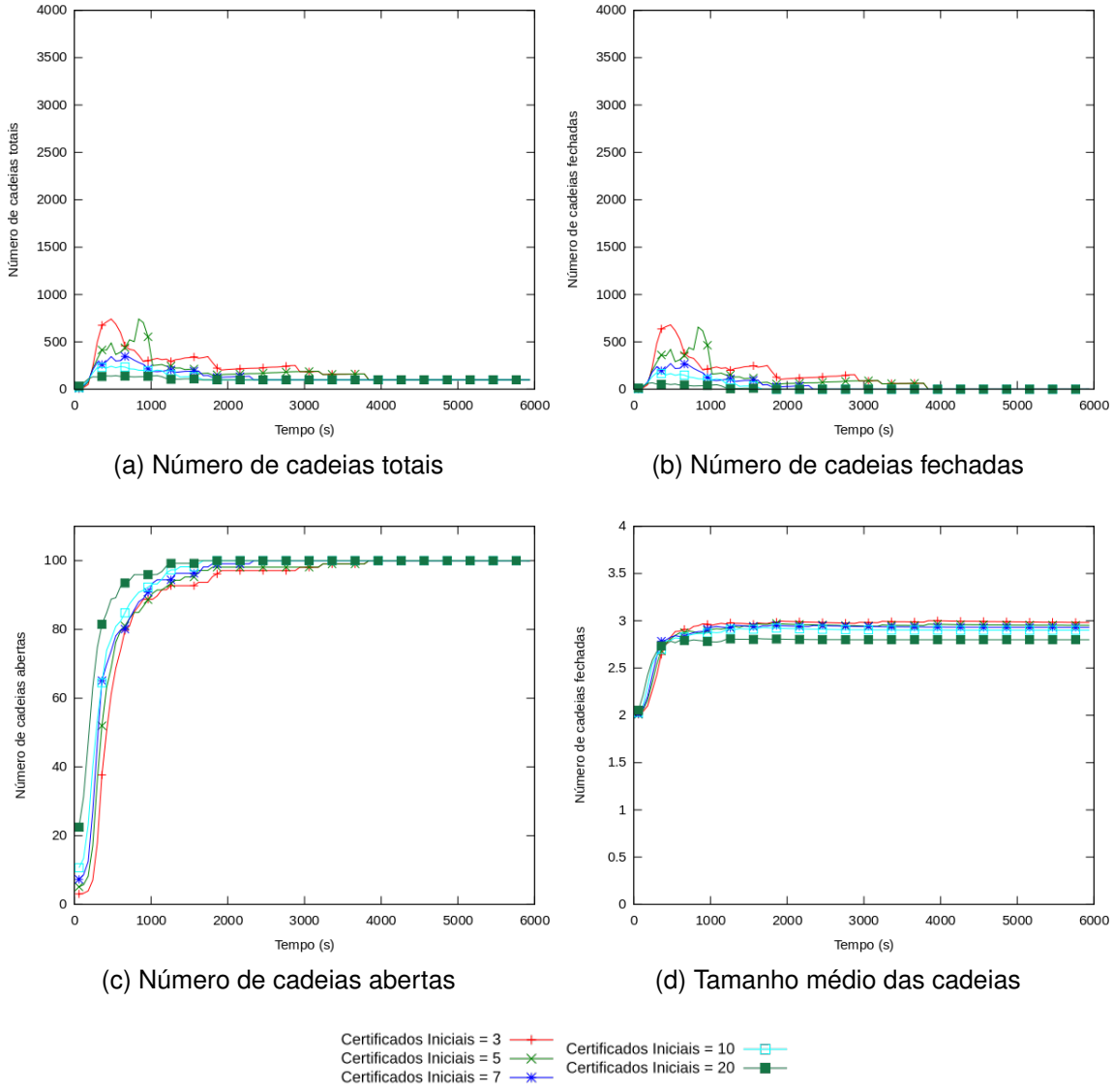

(a) Número de cadeias totais

(b) Número de cadeias fechadas

(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

Figura B.3: Resultados com algoritmo otimizado para 75 nodos




(a) Número de cadeias totais

(b) Número de cadeias fechadas

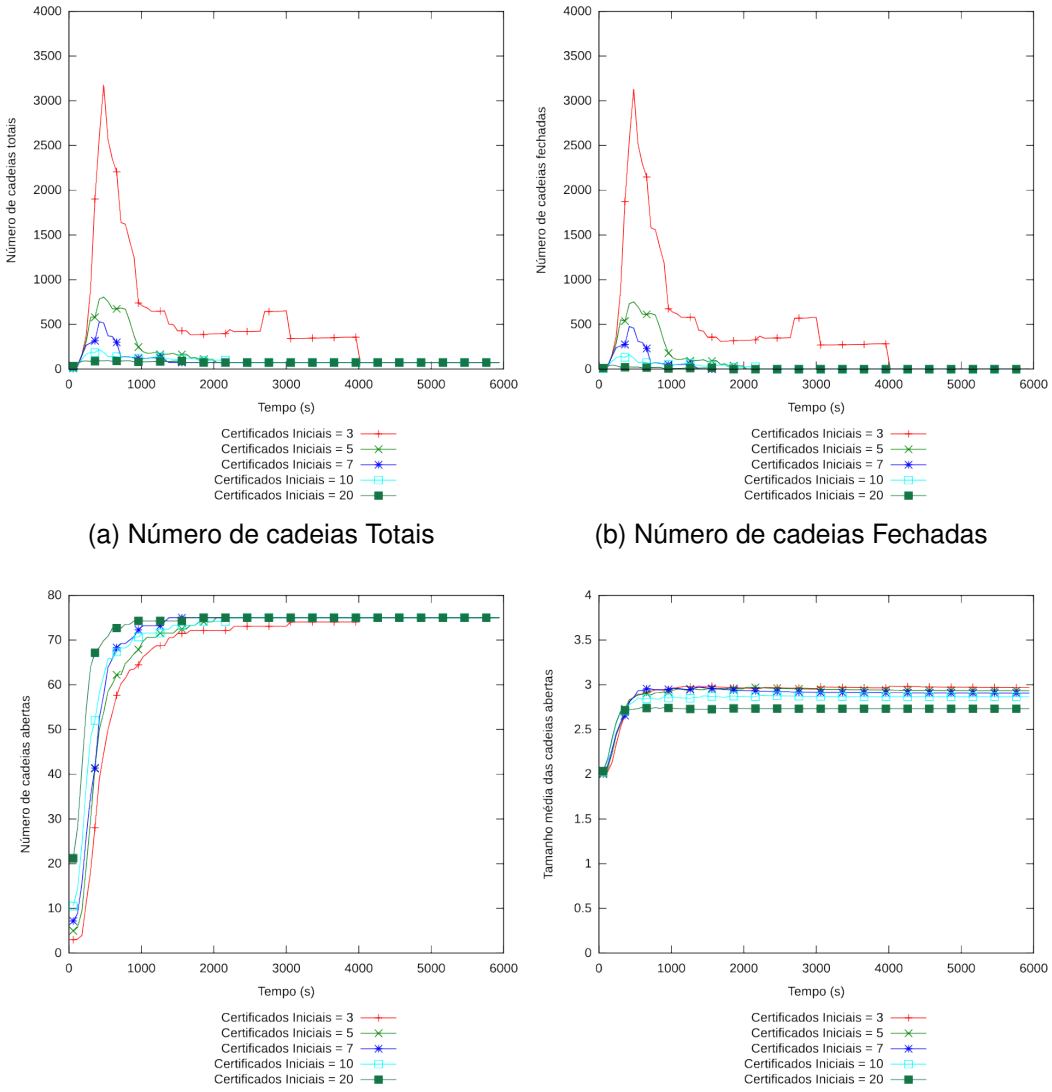
(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

Figura B.4: Resultados com algoritmo otimizado para 100 nodos

## B.3 Ataque *GreyHole*

### B.3.1 Ataque *GreyHole* com $m = 10\%$ e $t = 10\%$



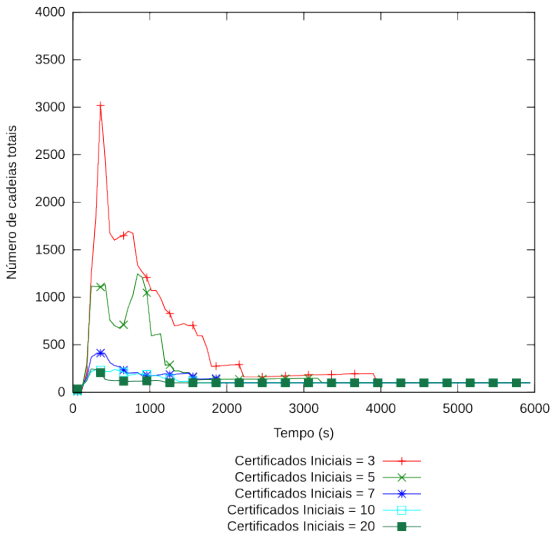

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

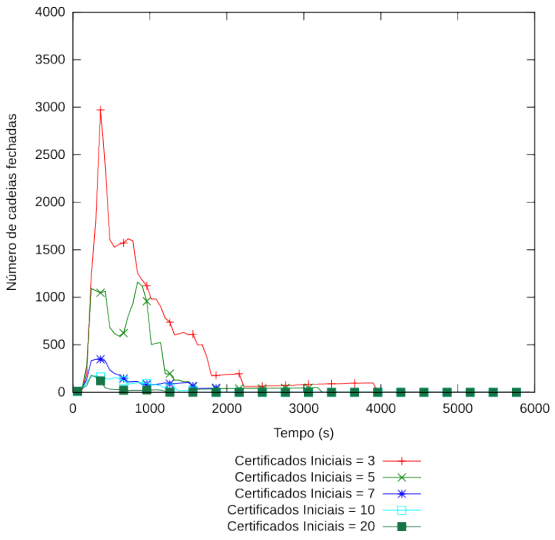
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

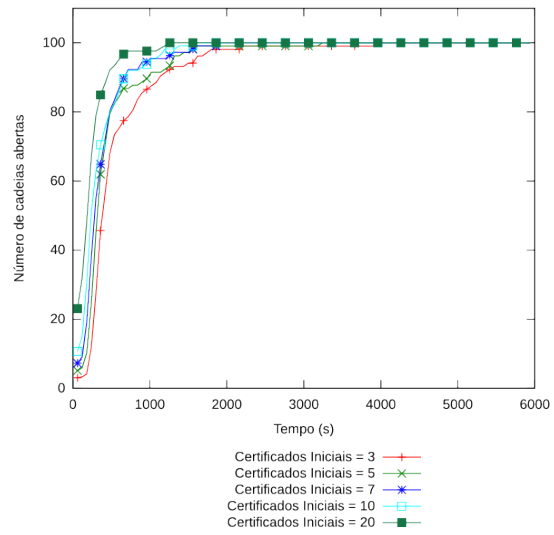
Figura B.5: Resultados para 75 nodos, $m = 10\%$ e $t = 10\%$



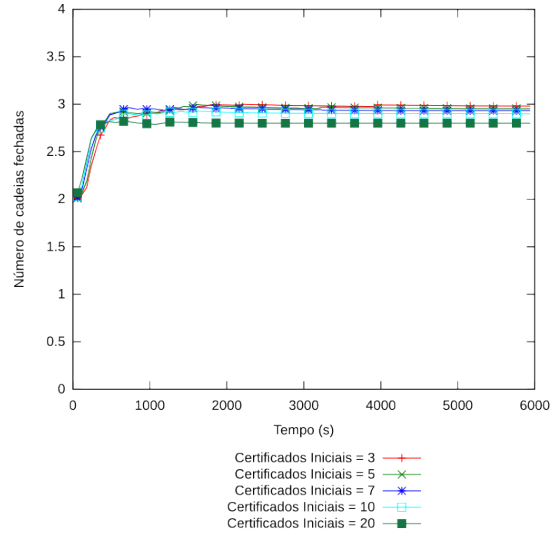

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



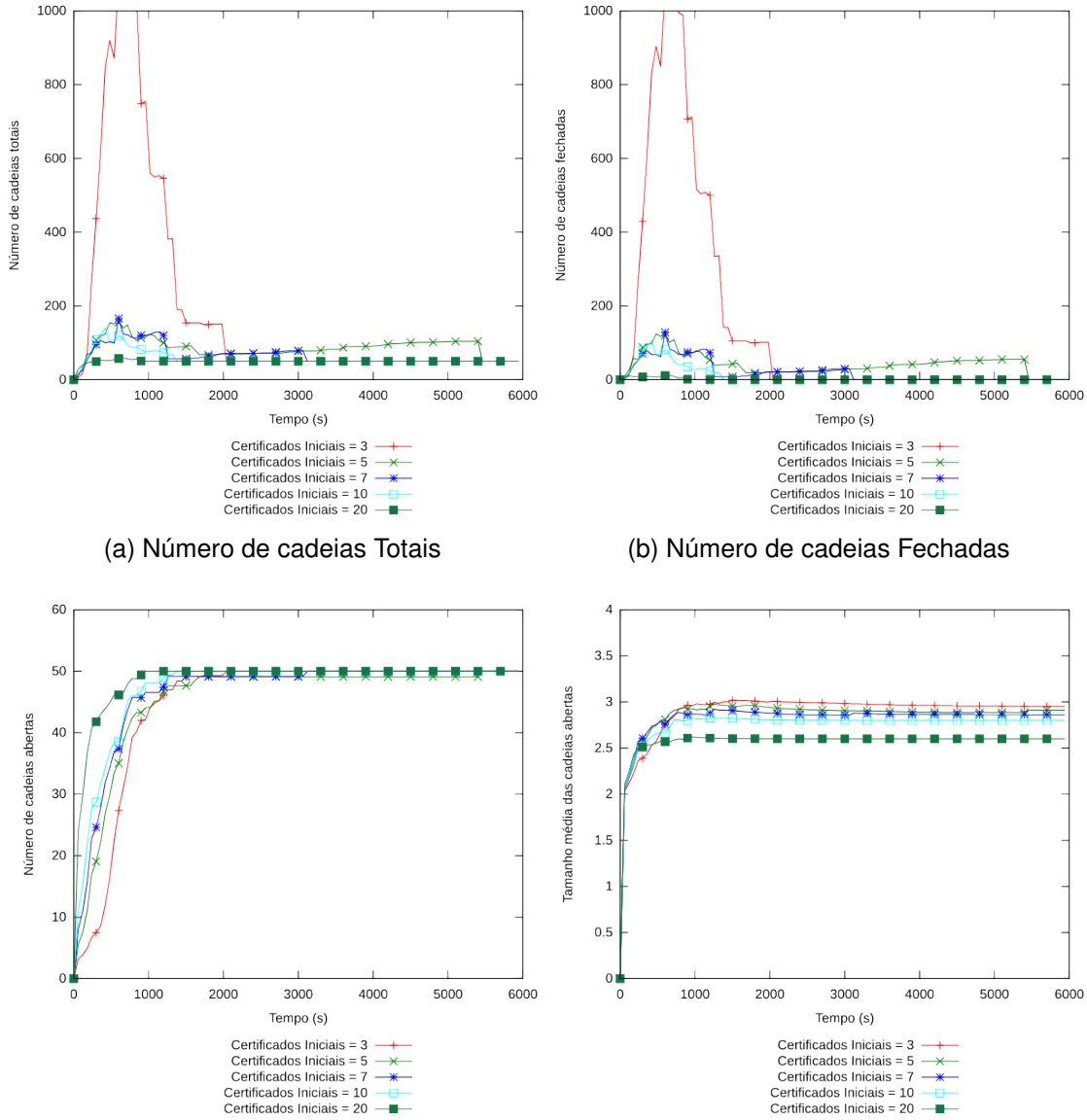

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.6: Resultados para 100 nodos, $m = 10\%$ e $t = 10\%$

### B.3.2 Ataque *GreyHole* com $m = 10\%$ e $t = 25\%$



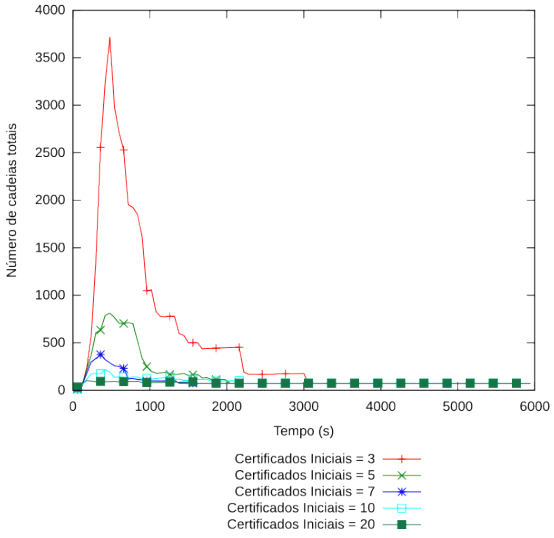

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

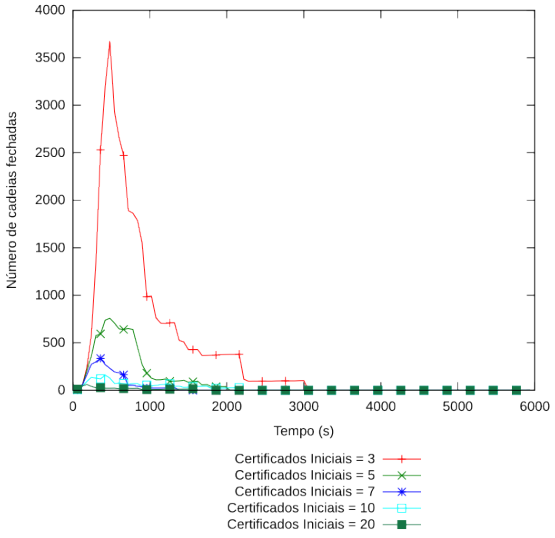
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

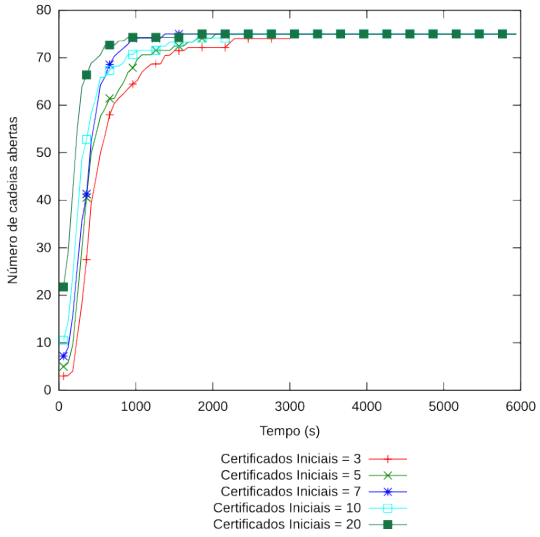
Figura B.7: Resultados para 50 nodos, $m = 10\%$ e $t = 25\%$



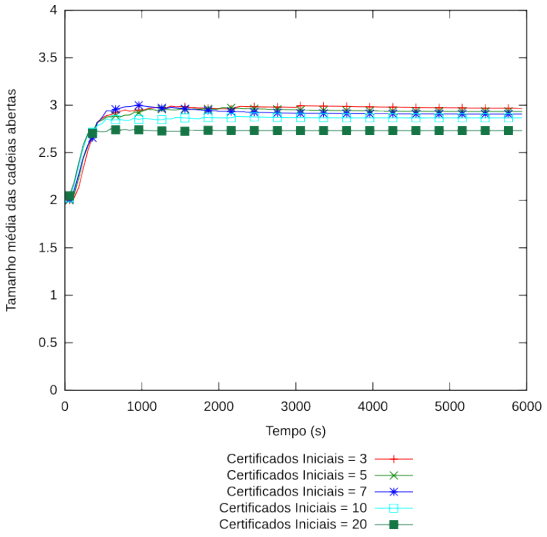

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

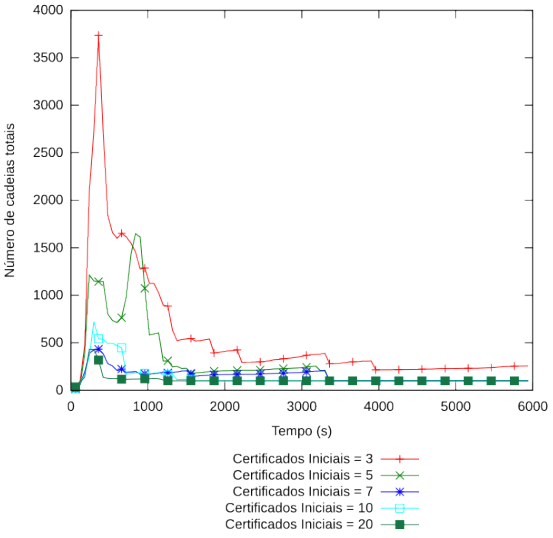



(c) Número de cadeias Abertas

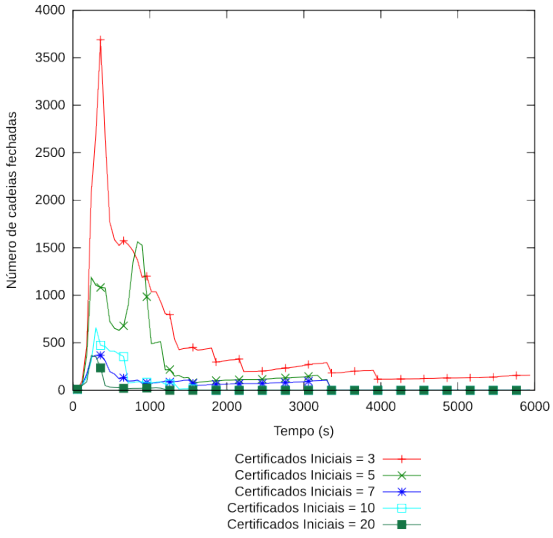



(d) Tamanho médio das cadeias

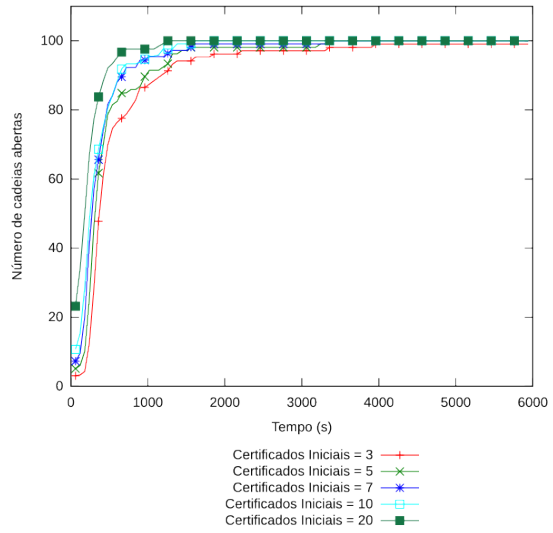
Figura B.8: Resultados para 75 nodos, $m = 10\%$ e $t = 25\%$



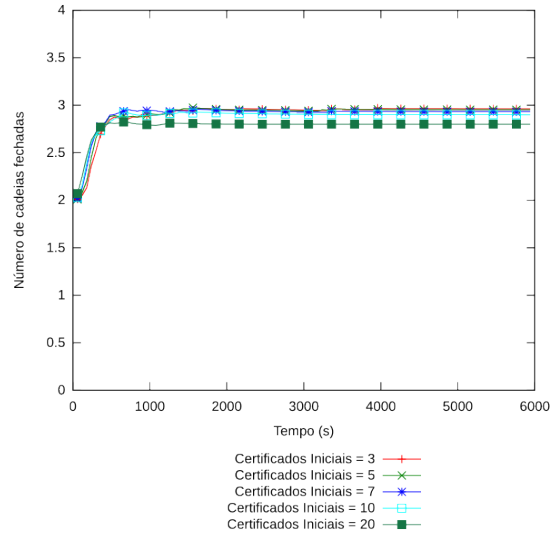

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

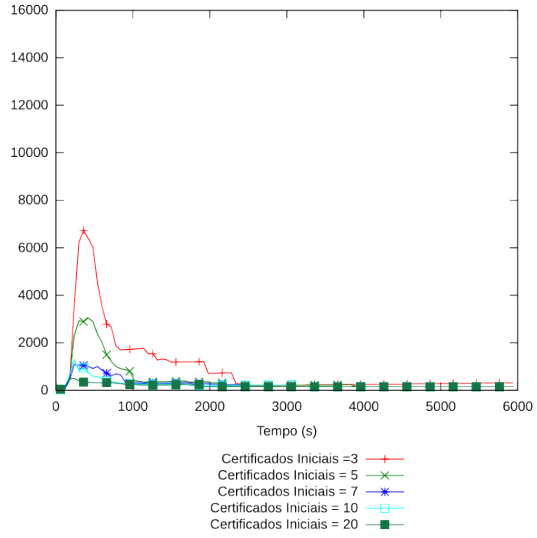



(c) Número de cadeias Abertas

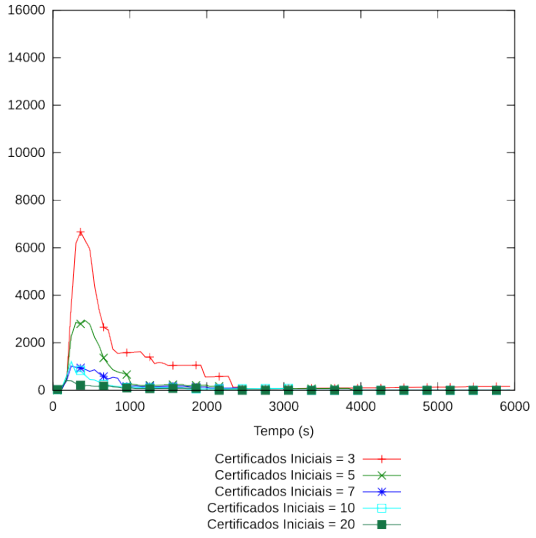



(d) Tamanho médio das cadeias

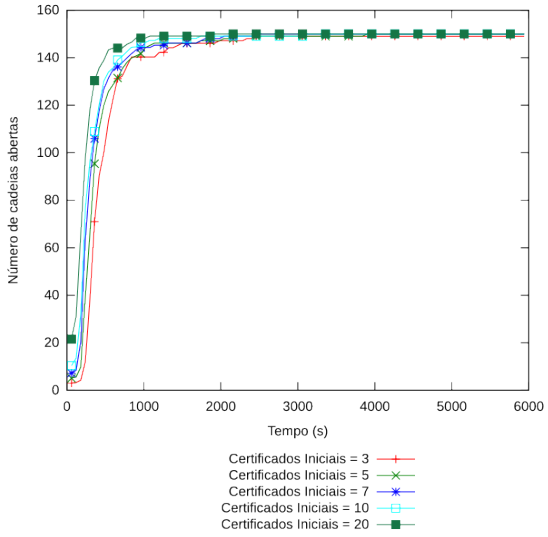
Figura B.9: Resultados para 100 nodos, $m = 10\%$ e $t = 25\%$



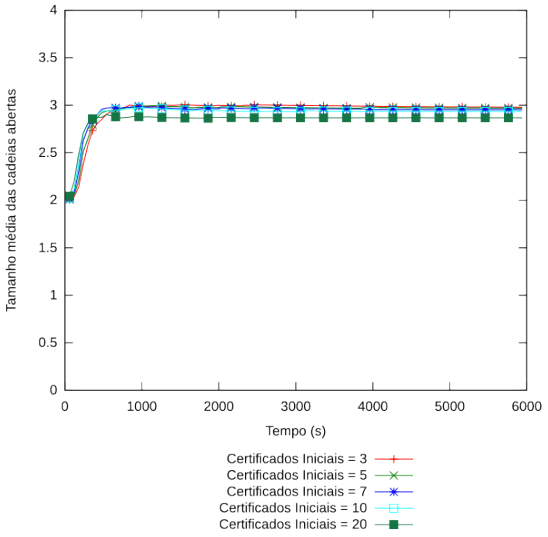

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



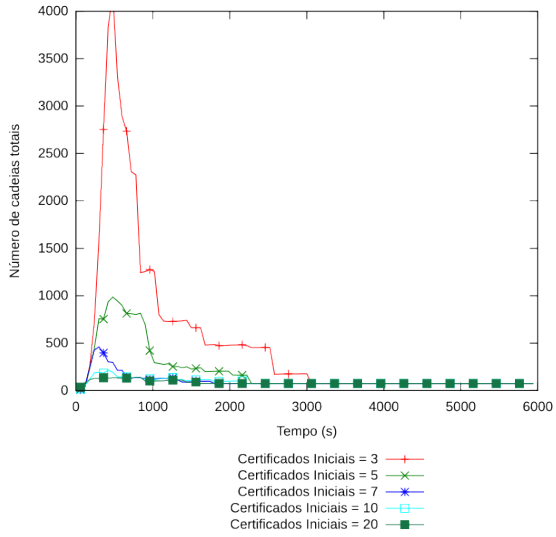

(c) Número de cadeias Abertas



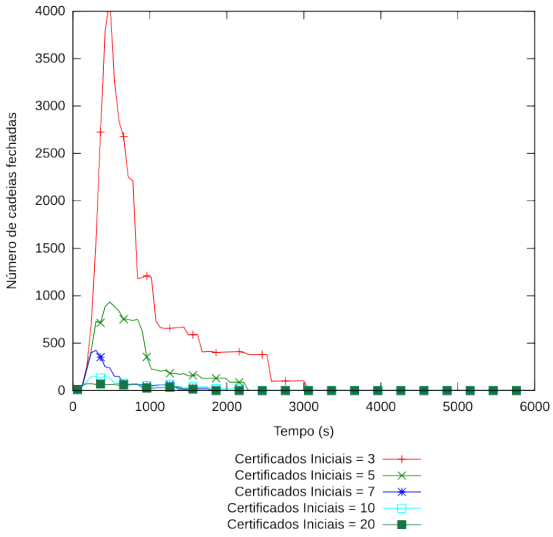

(d) Tamanho médio das cadeias

Figura B.10: Resultados para 150 nodos, $m = 10\%$ e $t = 25\%$

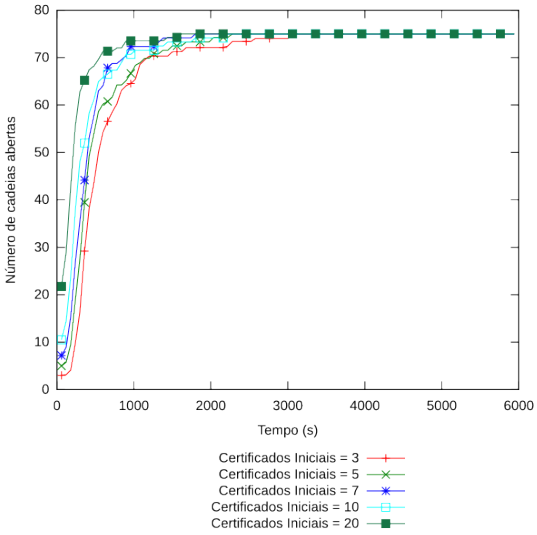
### B.3.3 Ataque *GreyHole* com $m = 10\%$ e $t = 50\%$



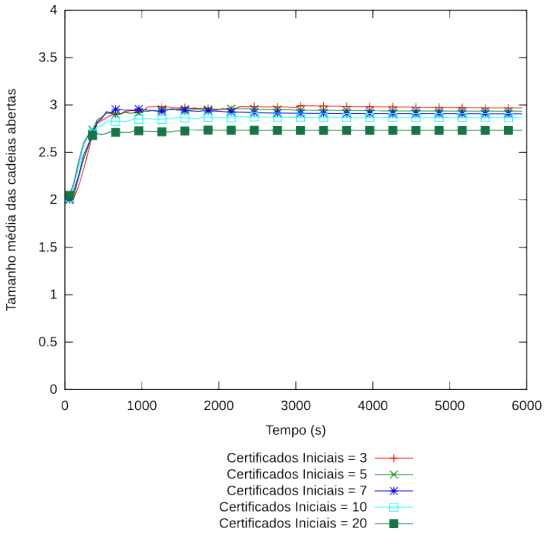

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

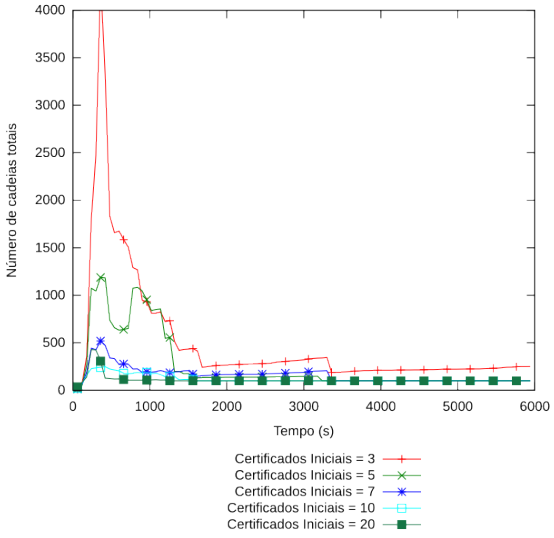



(c) Número de cadeias Abertas

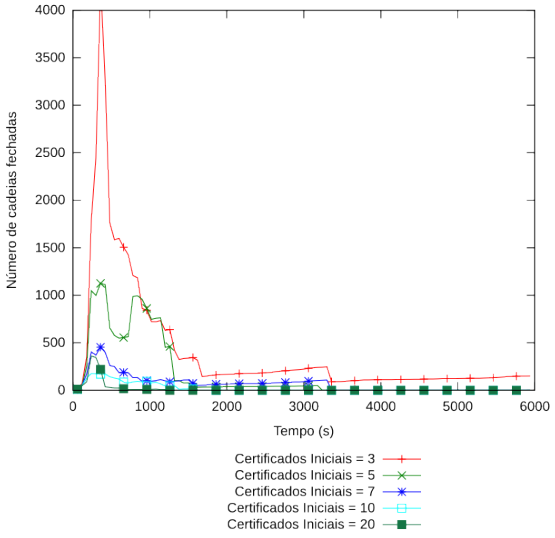



(d) Tamanho médio das cadeias

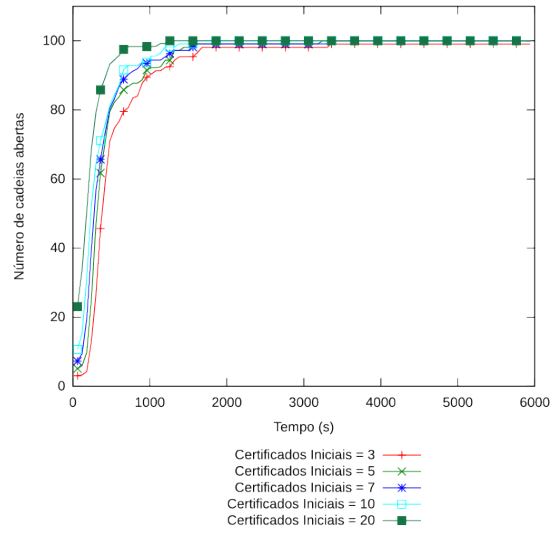
Figura B.11: Resultados para 75 nodos, $m = 10\%$ e $t = 50\%$



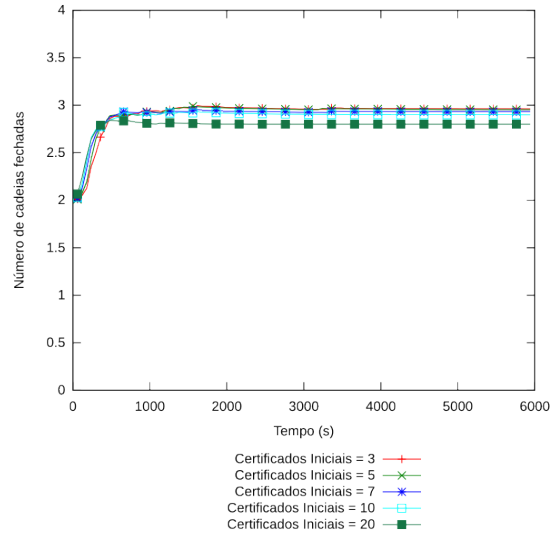

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



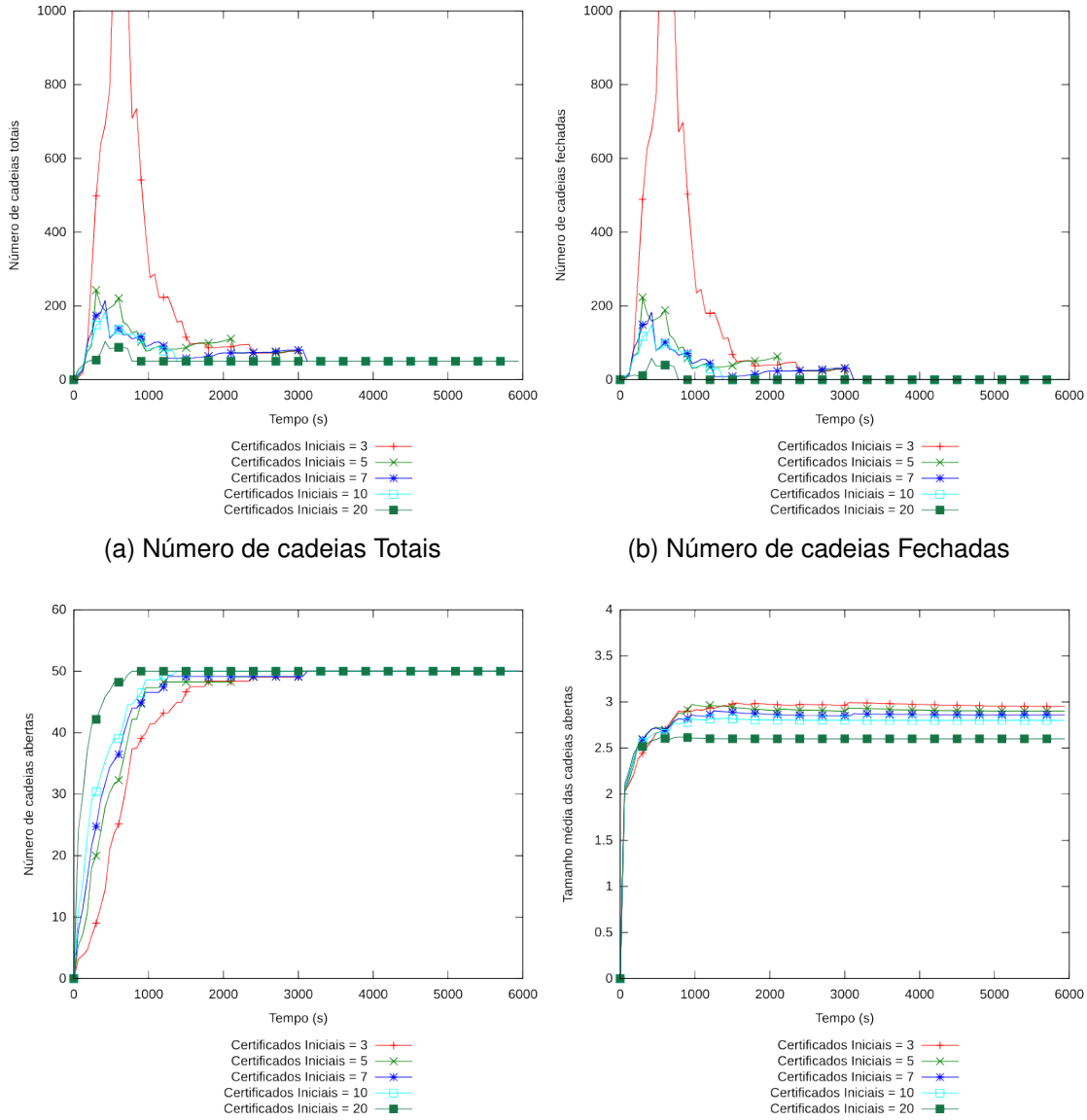

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.12: Resultados para 100 nodos, $m = 10\%$ e $t = 50\%$

### B.3.4 Ataque *GreyHole* com $m = 20\%$ e $t = 10\%$



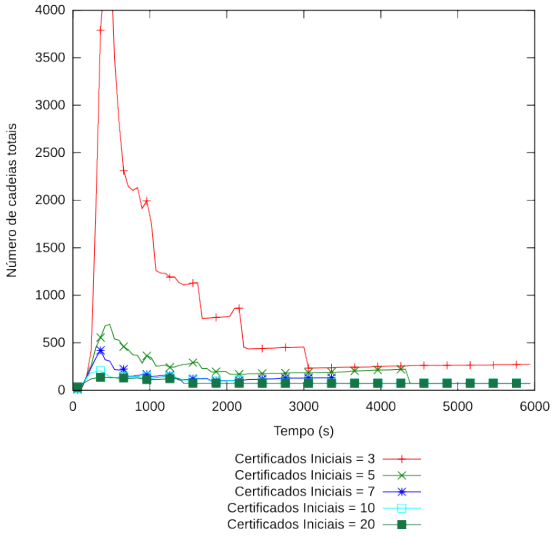

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

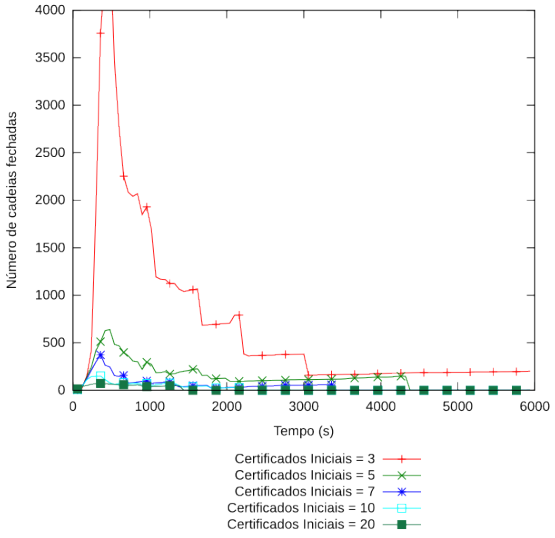
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

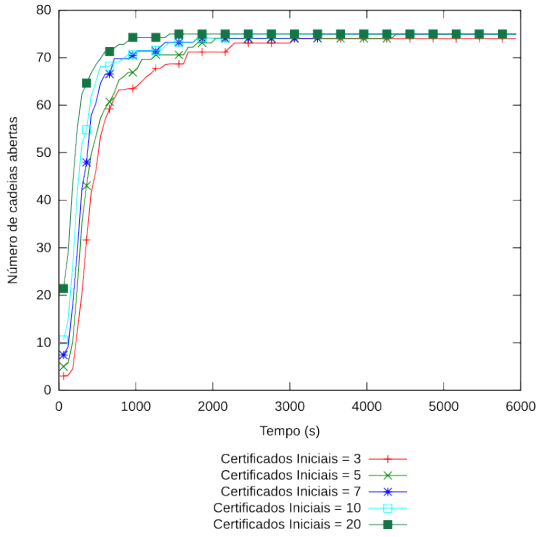
Figura B.13: Resultados para 50 nodos, $m = 20\%$ e $t = 10\%$



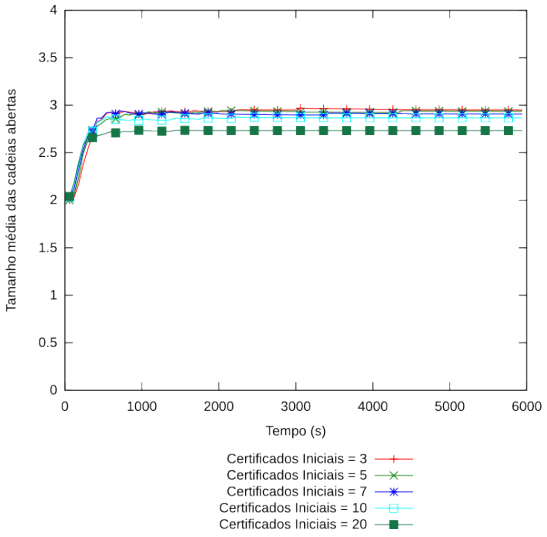

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

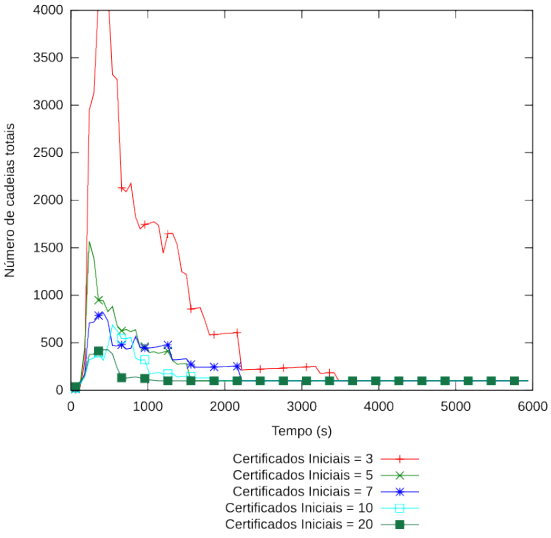



(c) Número de cadeias Abertas

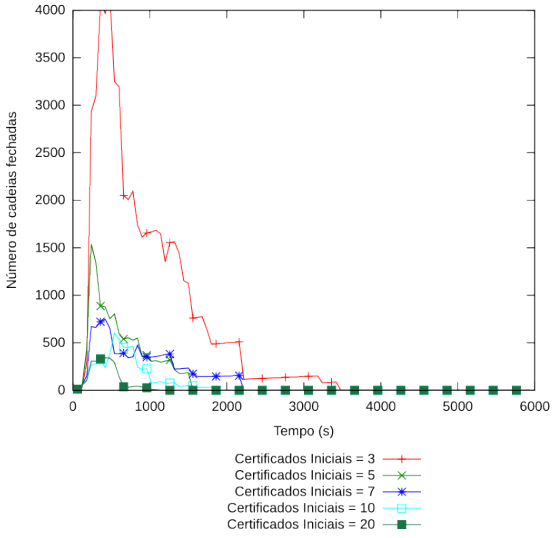



(d) Tamanho médio das cadeias

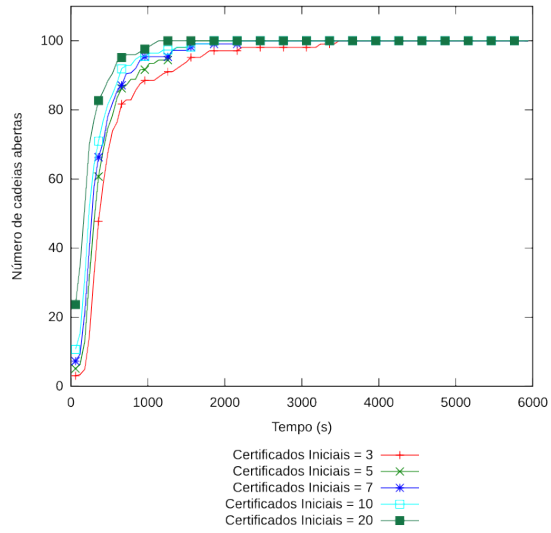
Figura B.14: Resultados para 75 nodos, $m = 20\%$ e $t = 10\%$



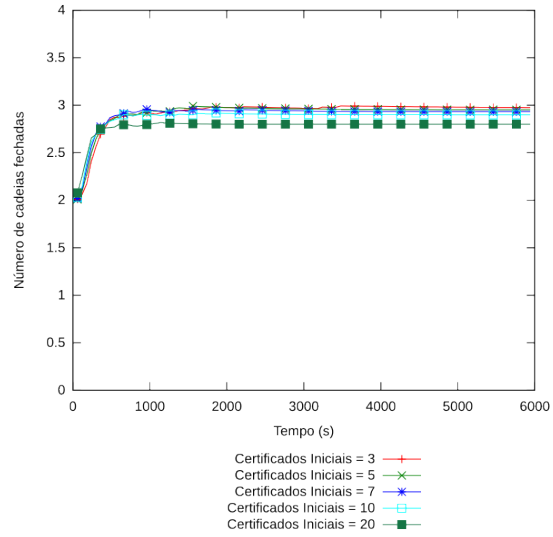

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

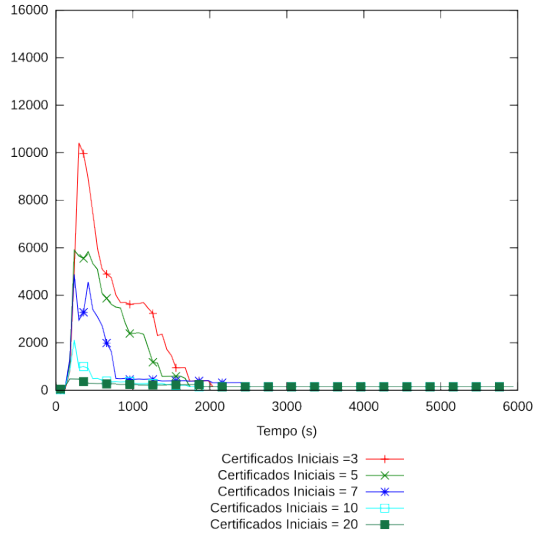



(c) Número de cadeias Abertas

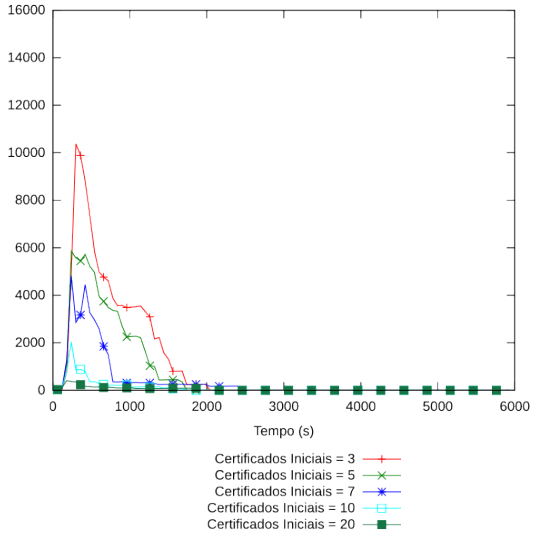



(d) Tamanho médio das cadeias

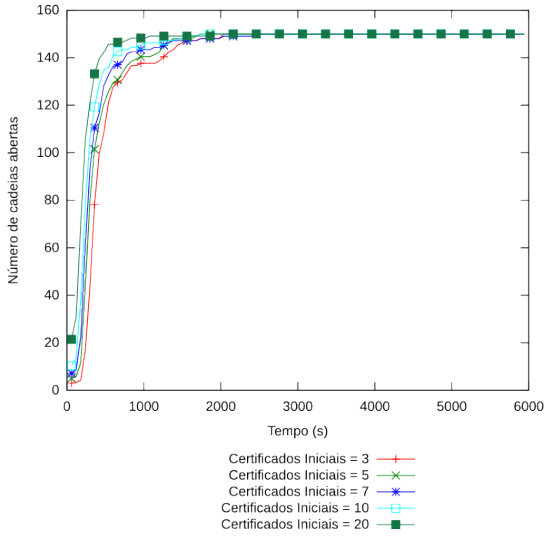
Figura B.15: Resultados para 100 nodos, $m = 20\%$ e $t = 10\%$



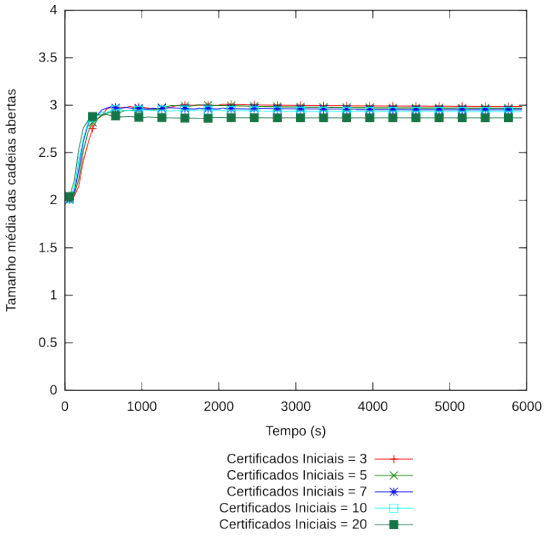

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



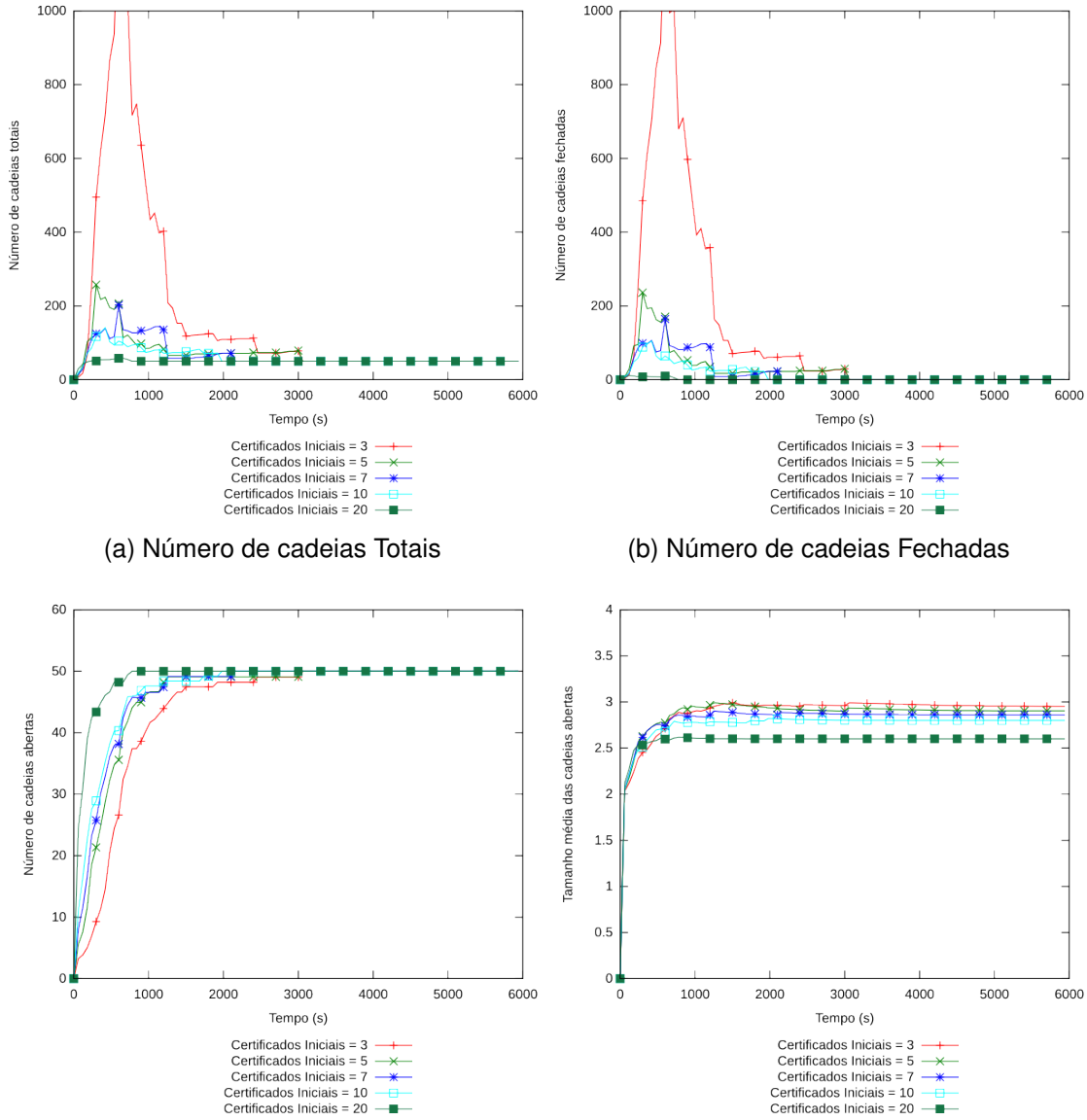

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.16: Resultados para 150 nodos, $m = 20\%$ e $t = 10\%$

### B.3.5 Ataque *GreyHole* com $m = 20\%$ e $t = 25\%$



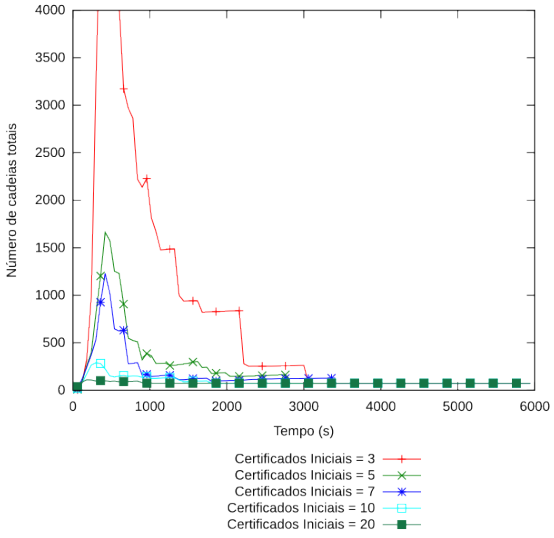

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

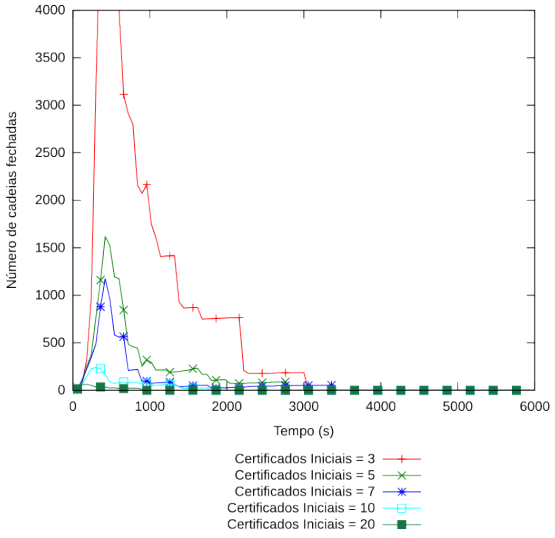
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

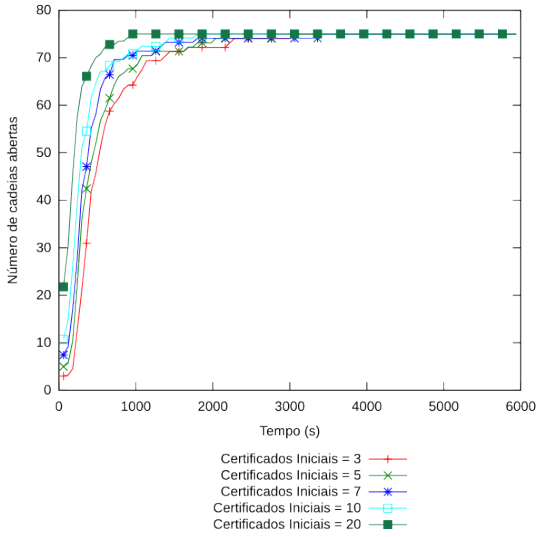
Figura B.17: Resultados para 50 nodos, $m = 20\%$ e $t = 25\%$



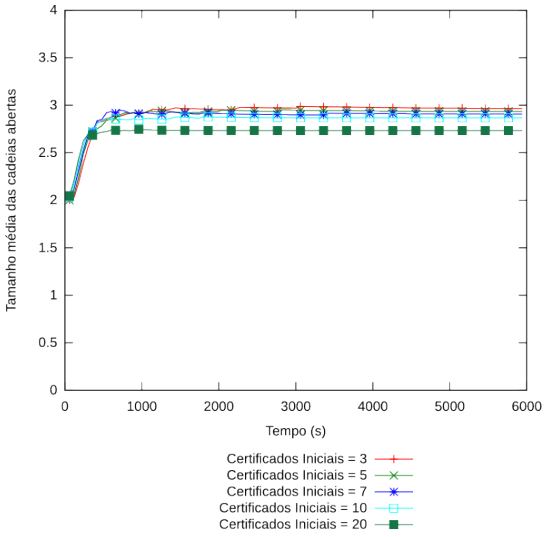

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

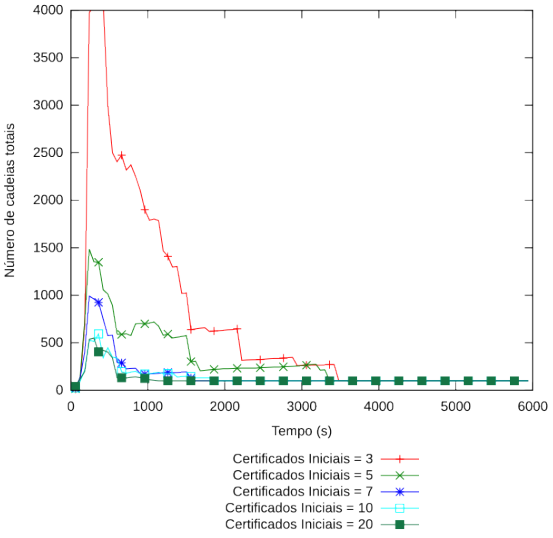



(c) Número de cadeias Abertas

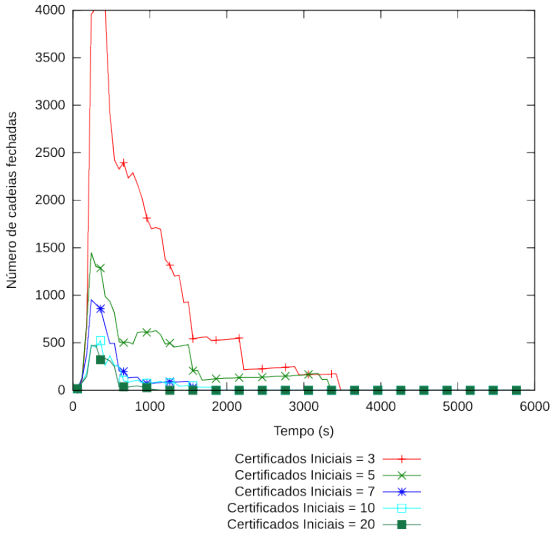



(d) Tamanho médio das cadeias

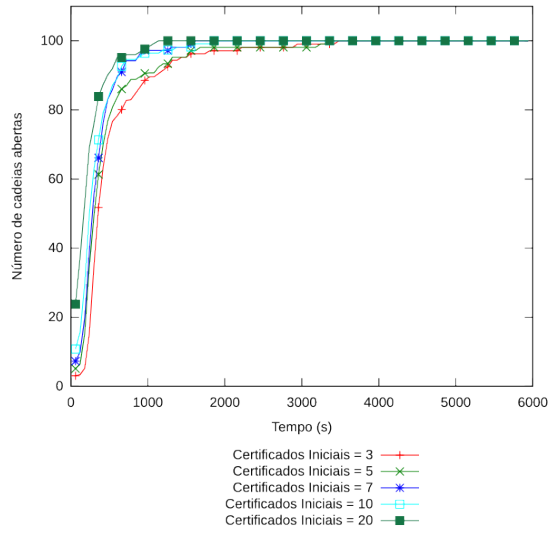
Figura B.18: Resultados para 75 nodos, $m = 20\%$ e $t = 25\%$



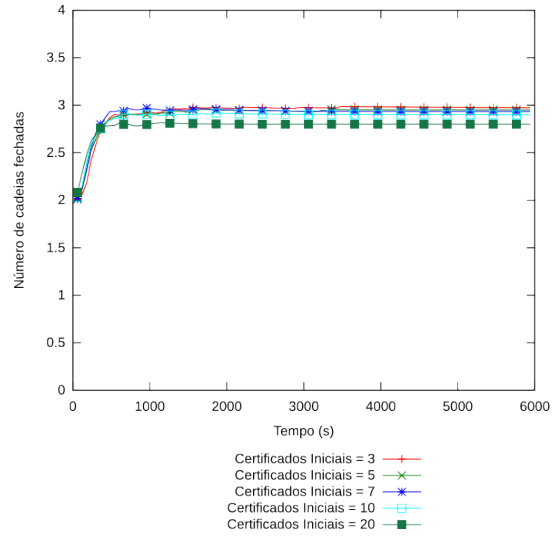

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

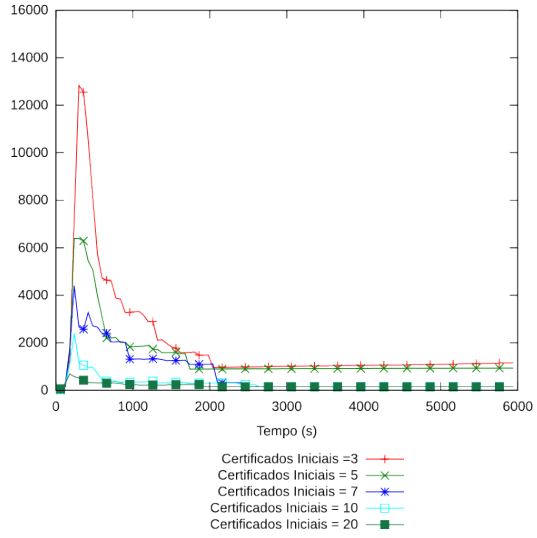



(c) Número de cadeias Abertas

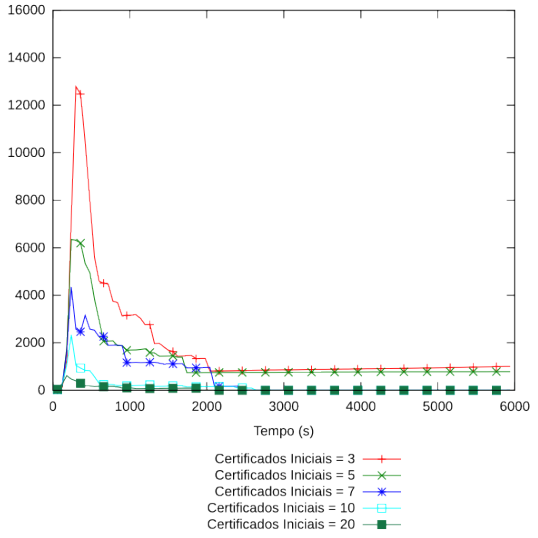



(d) Tamanho médio das cadeias

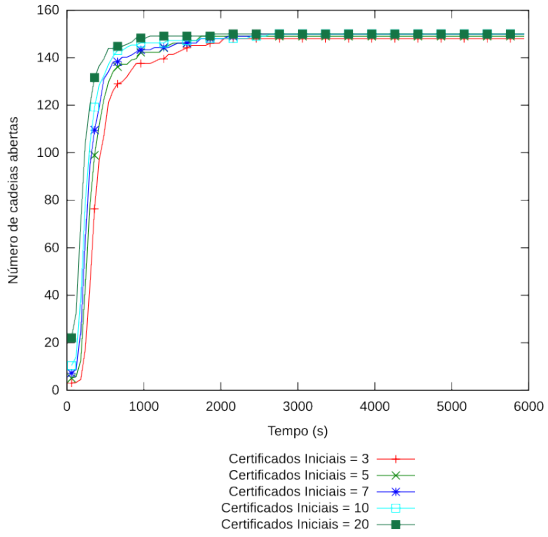
Figura B.19: Resultados para 100 nodos, $m = 20\%$ e $t = 25\%$



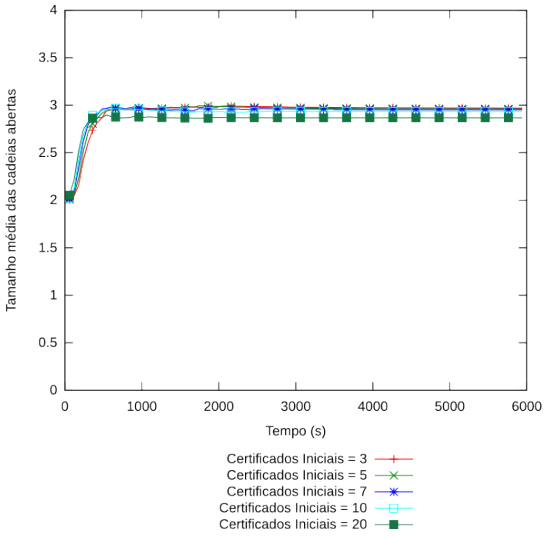

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



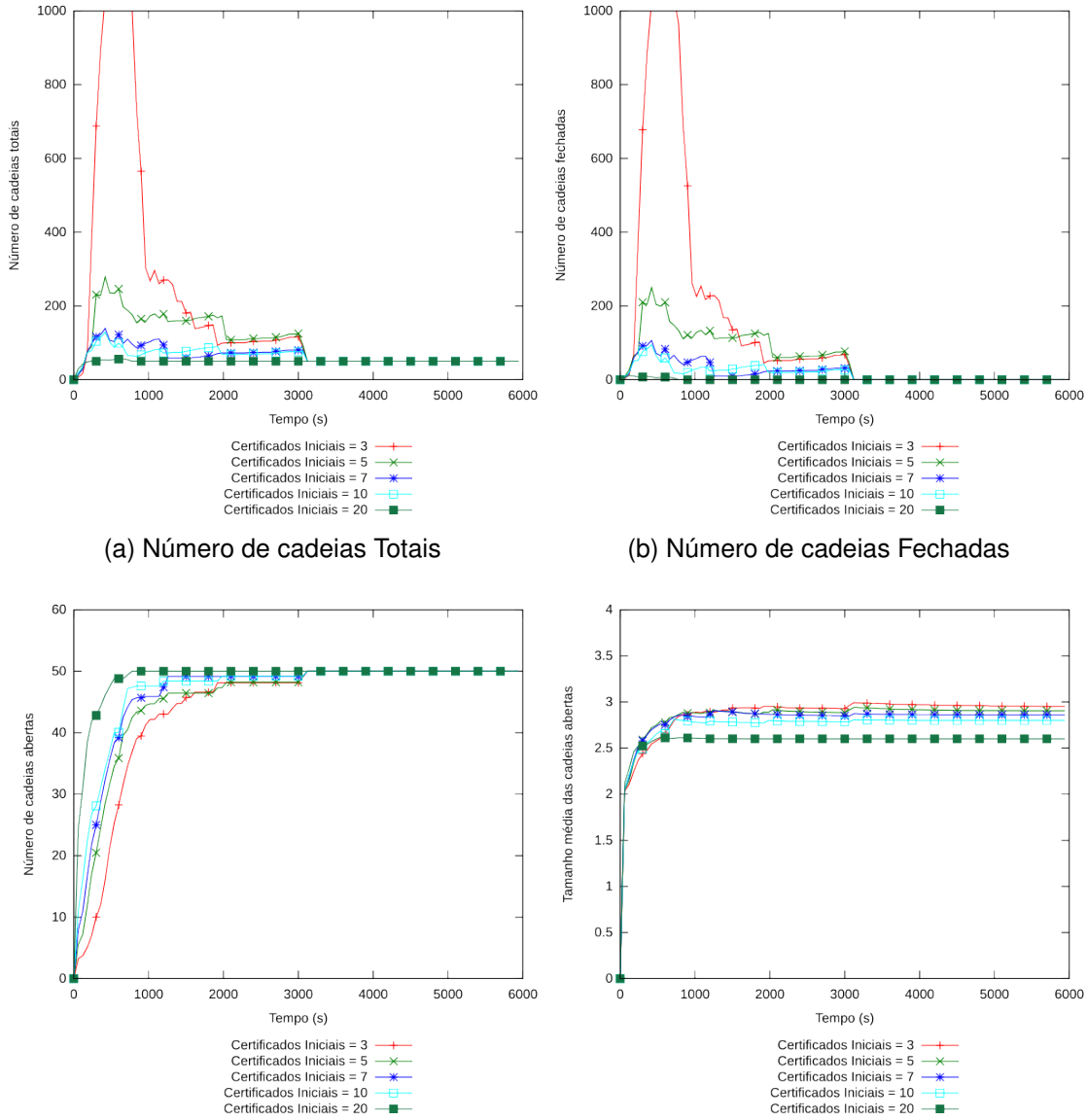

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.20: Resultados para 150 nodos, $m = 20\%$ e $t = 25\%$

### B.3.6 Ataque *GreyHole* com $m = 20\%$ e $t = 50\%$



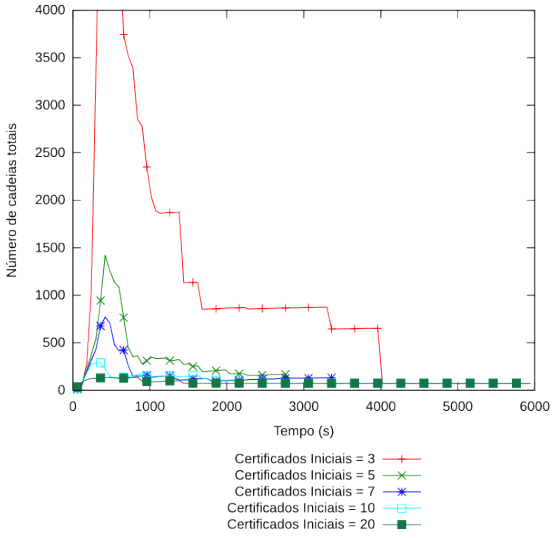

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

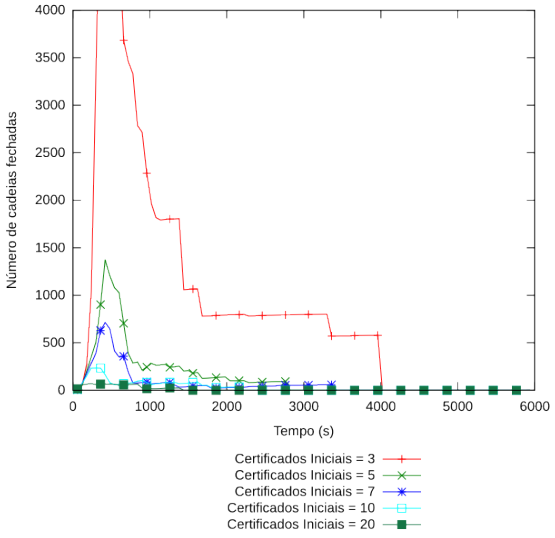
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

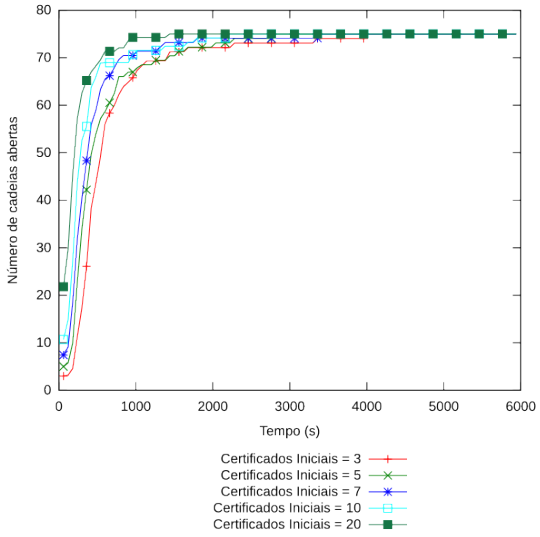
Figura B.21: Resultados para 50 nodos, $m = 20\%$ e $t = 50\%$



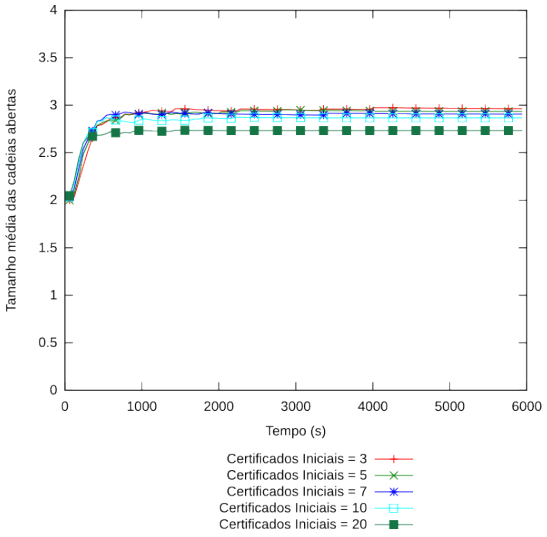

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

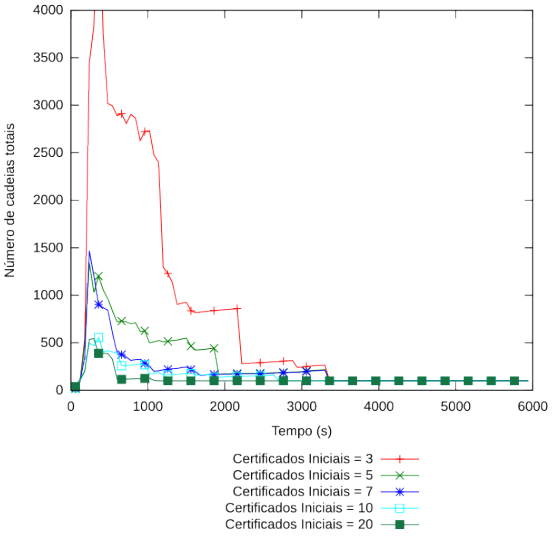



(c) Número de cadeias Abertas

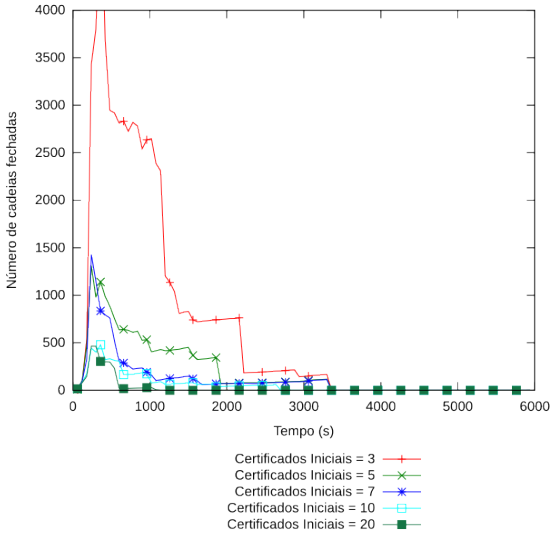



(d) Tamanho médio das cadeias

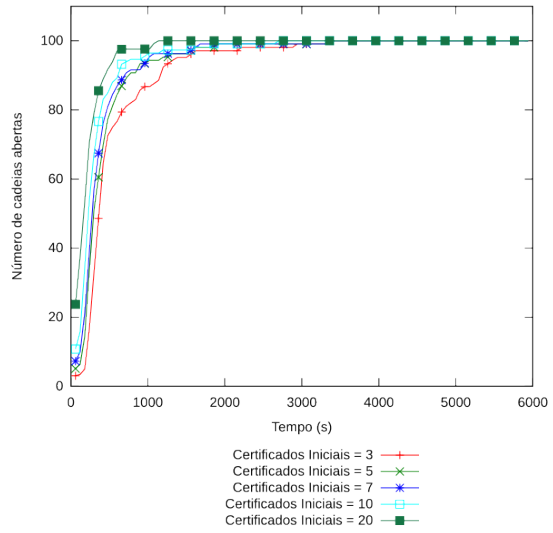
Figura B.22: Resultados para 75 nodos, $m = 20\%$ e $t = 50\%$



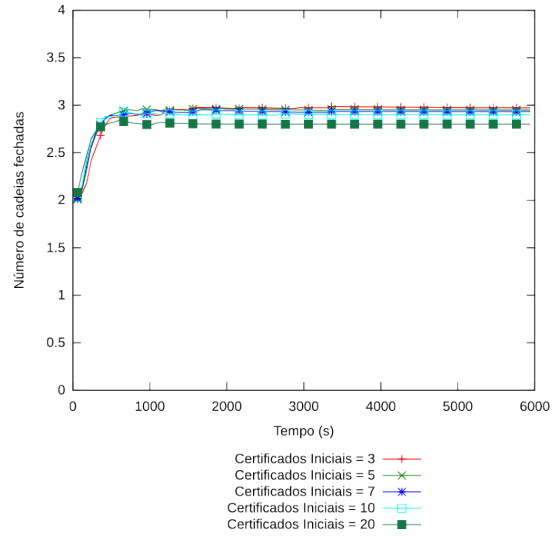

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

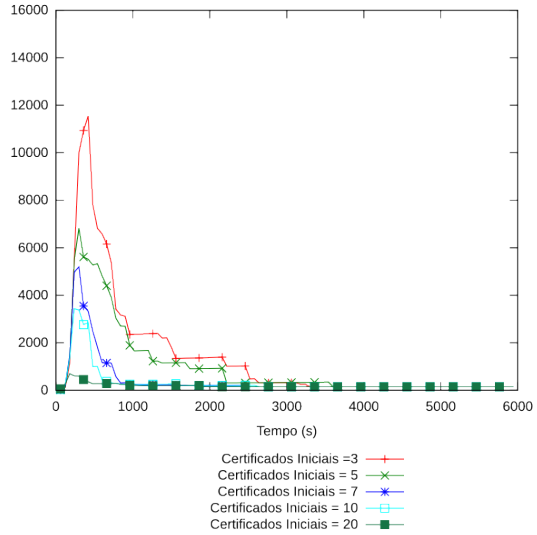



(c) Número de cadeias Abertas

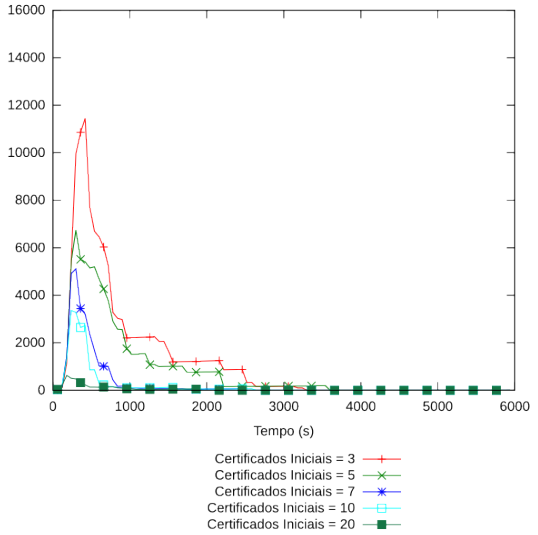



(d) Tamanho médio das cadeias

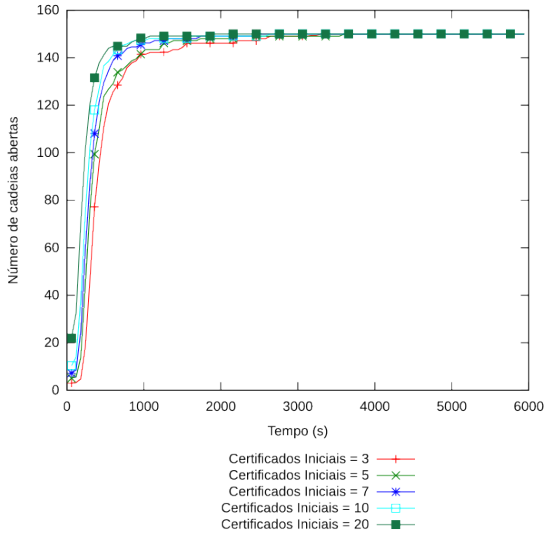
Figura B.23: Resultados para 50 nodos, $m = 20\%$ e $t = 50\%$



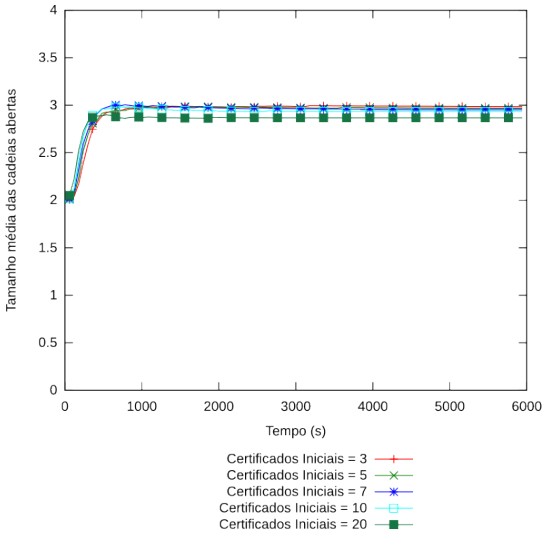

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



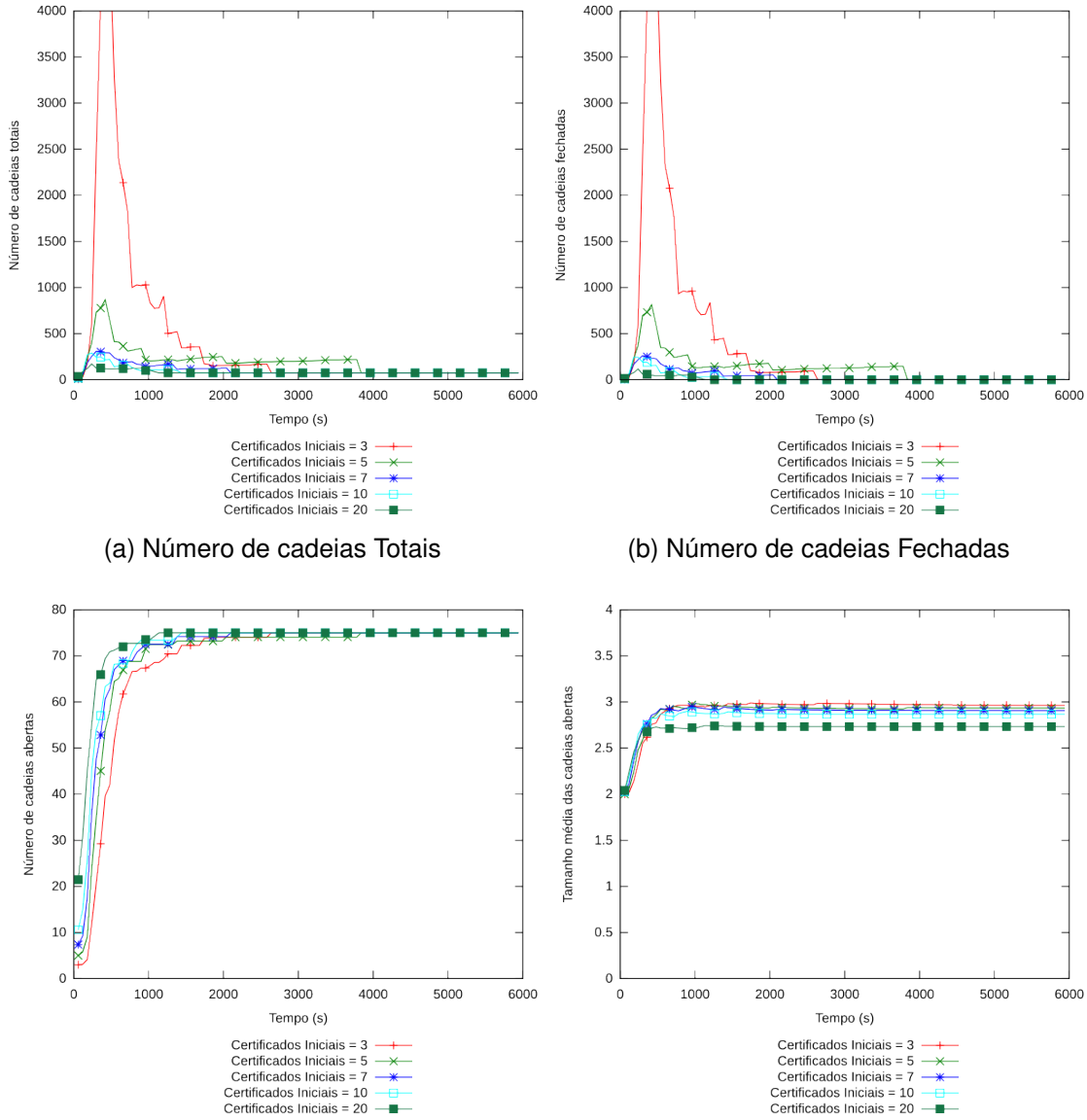

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.24: Resultados para 150 nodos, $m = 20\%$ e $t = 50\%$

### B.3.7 Ataque *GreyHole* com $m = 50\%$ e $t = 10\%$



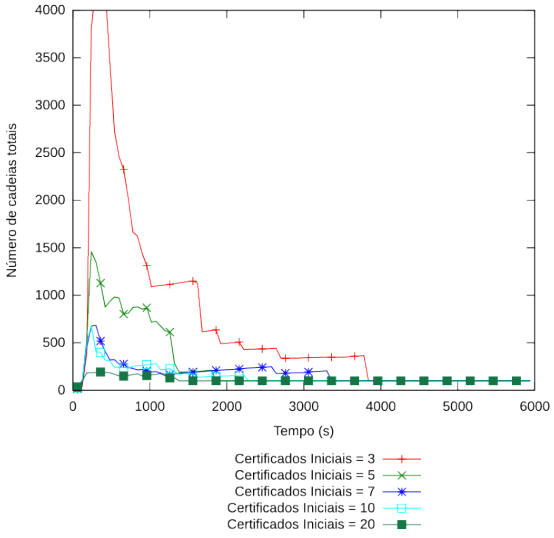

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

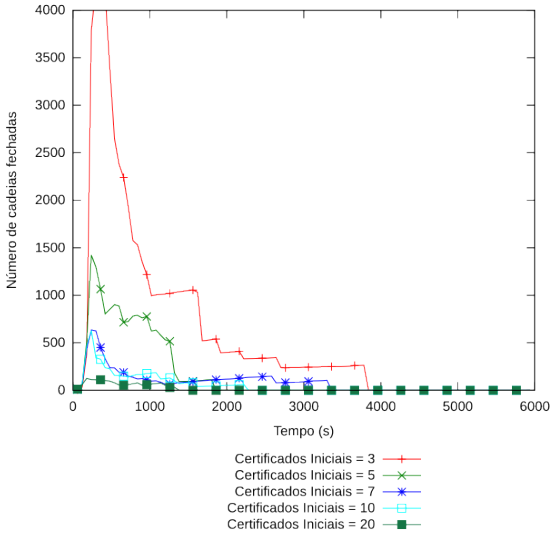
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

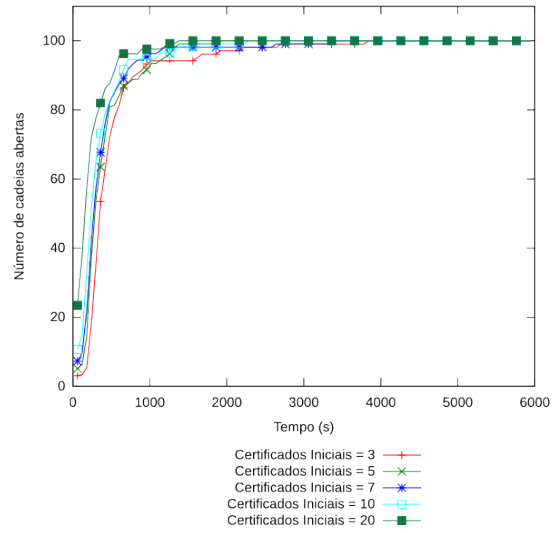
Figura B.25: Resultados para 75 nodos, $m = 50\%$ e $t = 10\%$



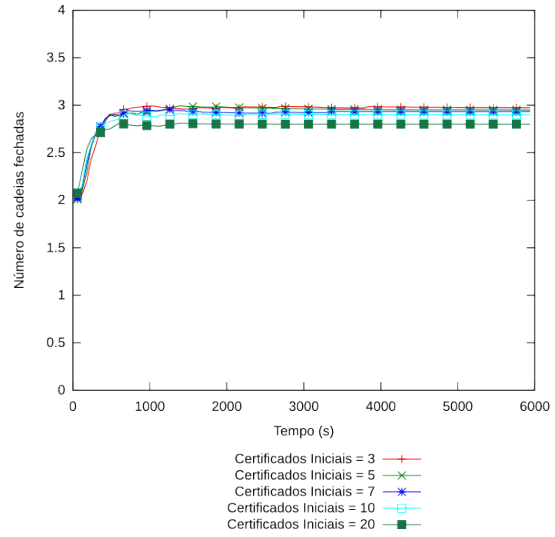

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



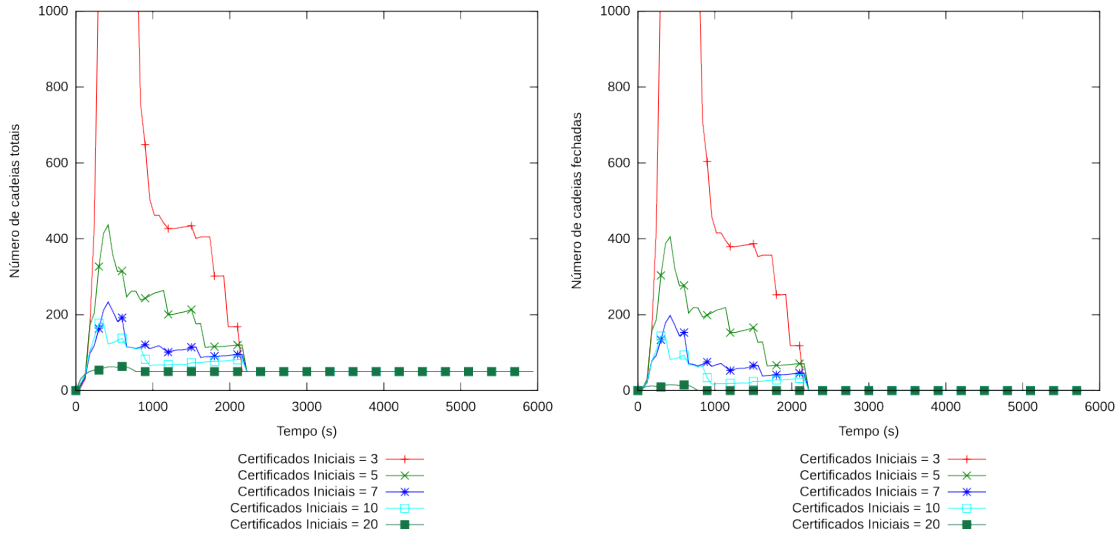

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.26: Resultados para 100 nodos, $m = 50\%$ e $t = 10\%$

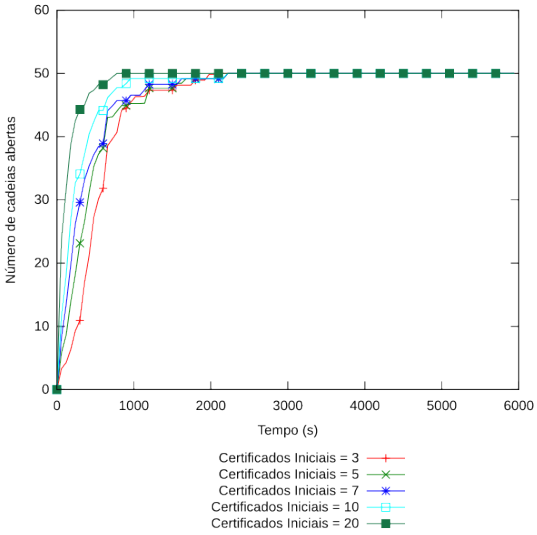
### B.3.8 Ataque *GreyHole* com $m = 50\%$ e $t = 25\%$



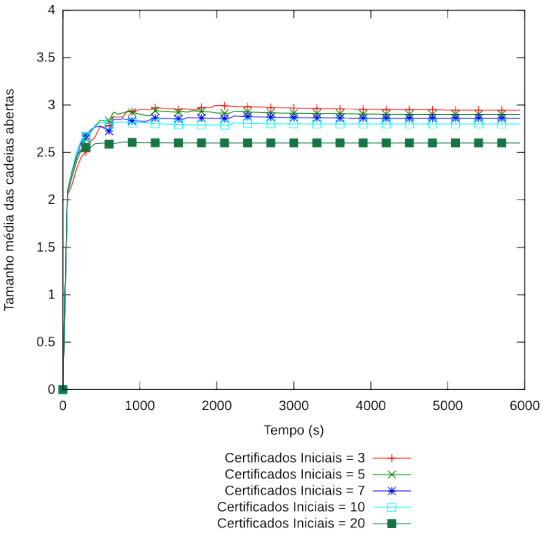

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

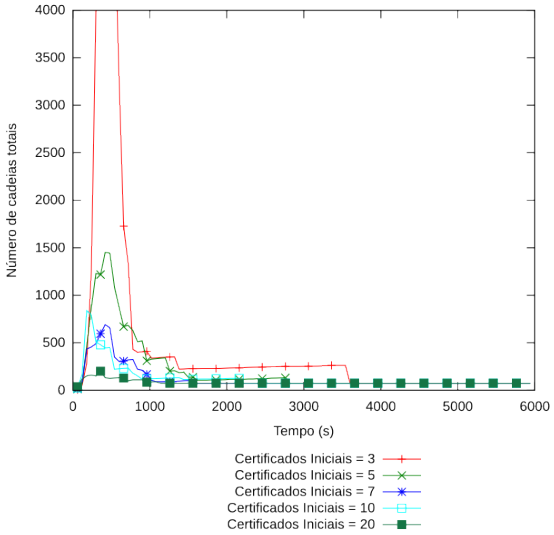



(c) Número de cadeias Abertas

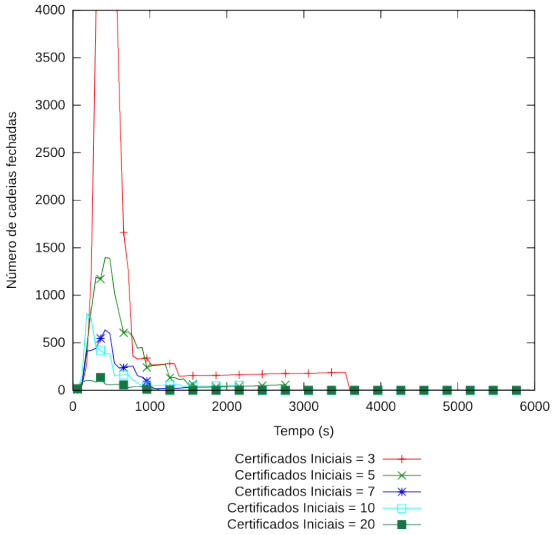



(d) Tamanho médio das cadeias

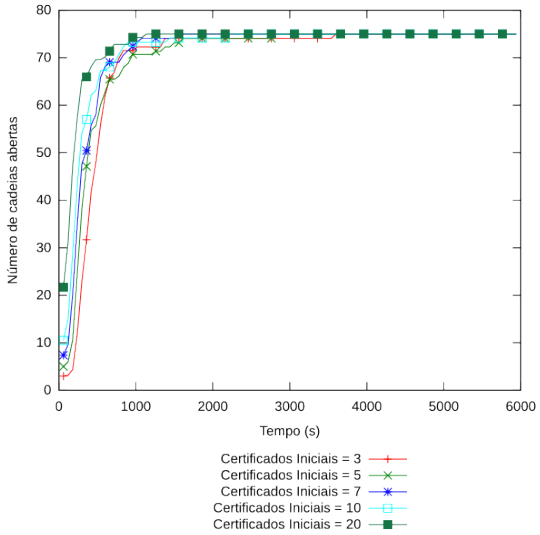
Figura B.27: Resultados para 50 nodos, $m = 50\%$ e $t = 25\%$



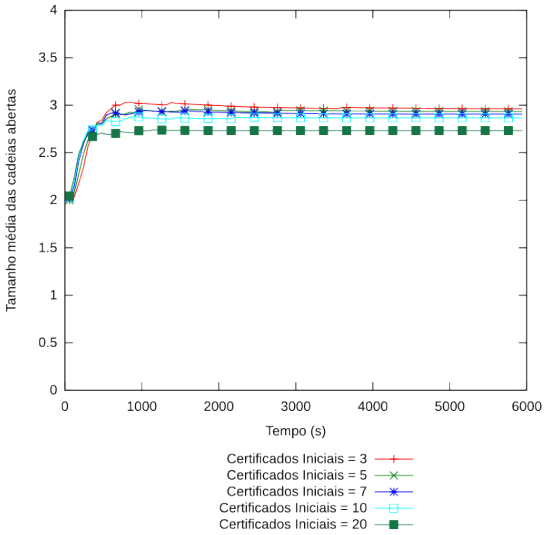

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

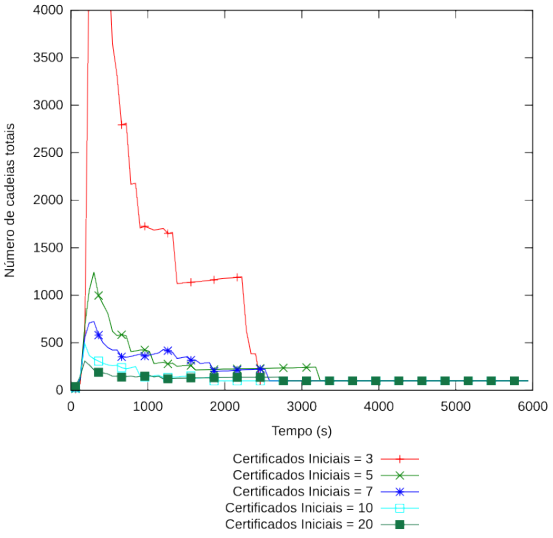



(c) Número de cadeias Abertas

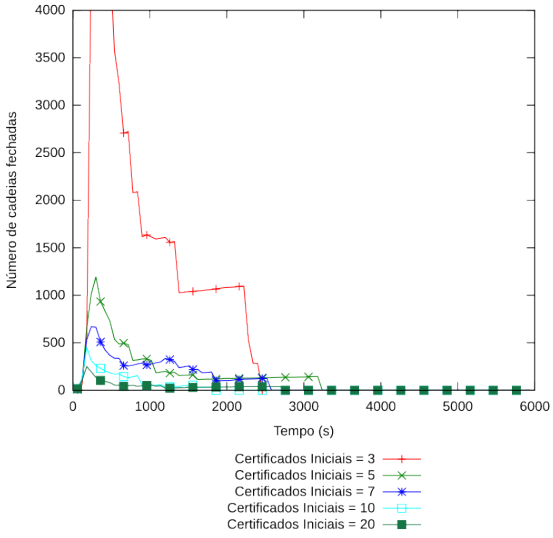



(d) Tamanho médio das cadeias

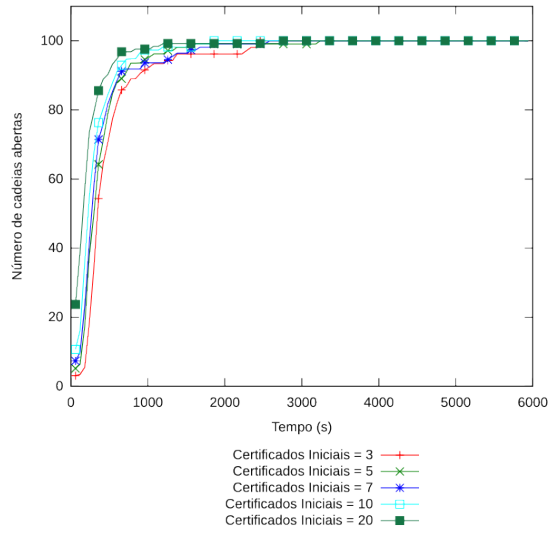
Figura B.28: Resultados para 75 nodos, $m = 50\%$ e $t = 25\%$



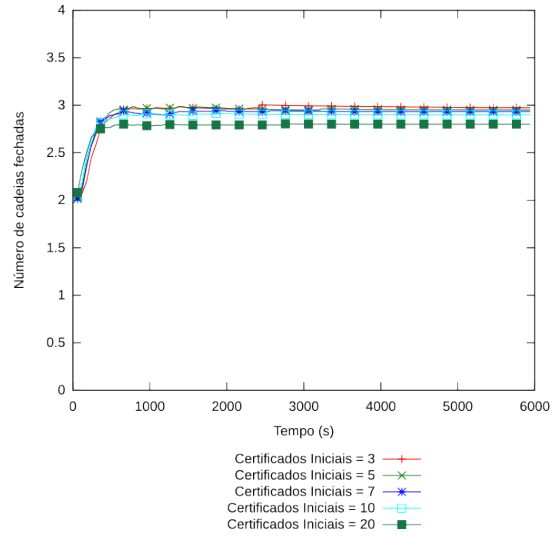

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

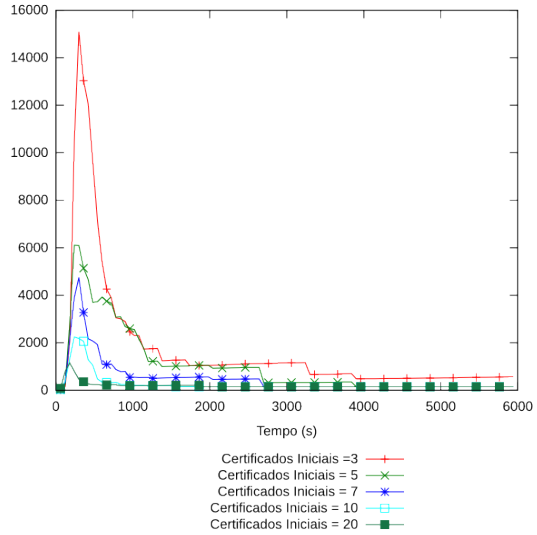



(c) Número de cadeias Abertas

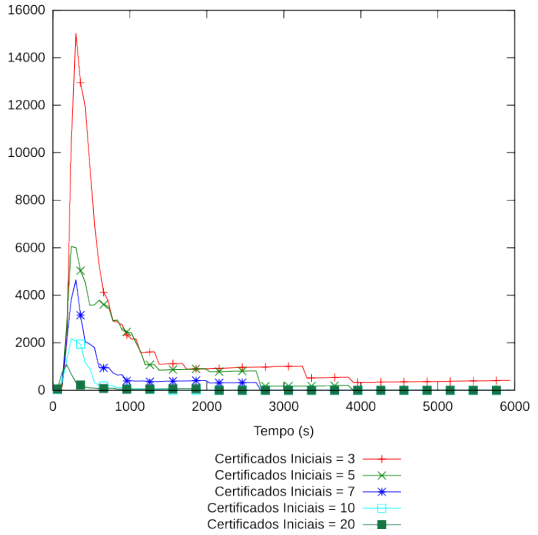



(d) Tamanho médio das cadeias

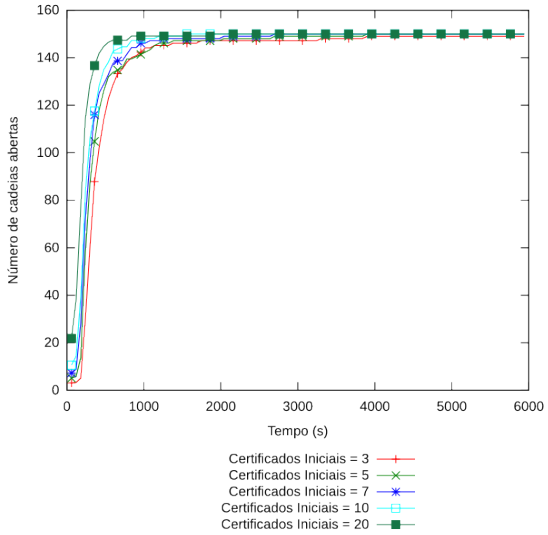
Figura B.29: Resultados para 100 nodos, $m = 50\%$ e $t = 25\%$



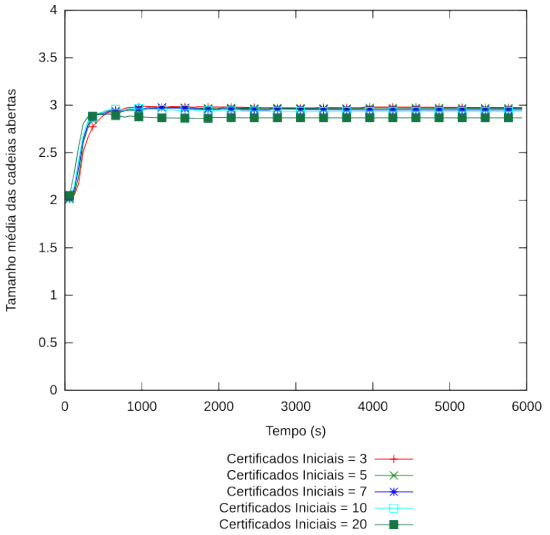

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



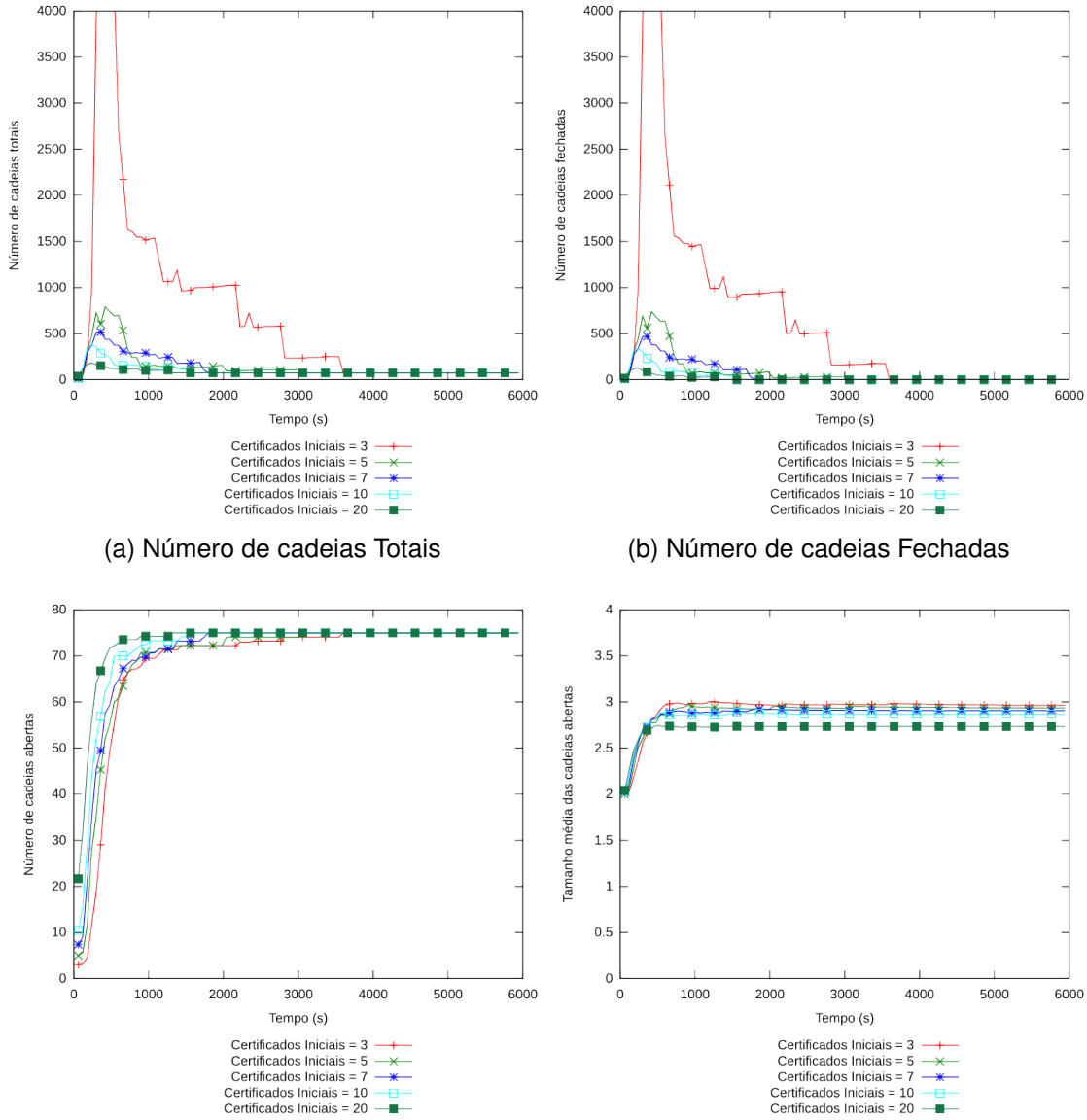

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.30: Resultados para 150 nodos, $m = 50\%$ e $t = 25\%$

### B.3.9 Ataque *GreyHole* com $m = 50\%$ e $t = 50\%$



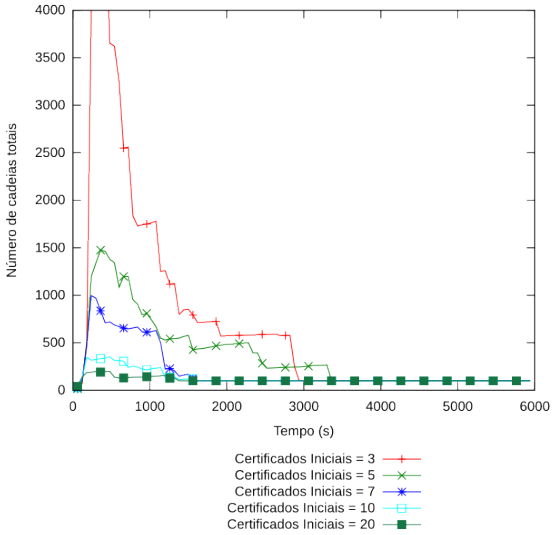

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

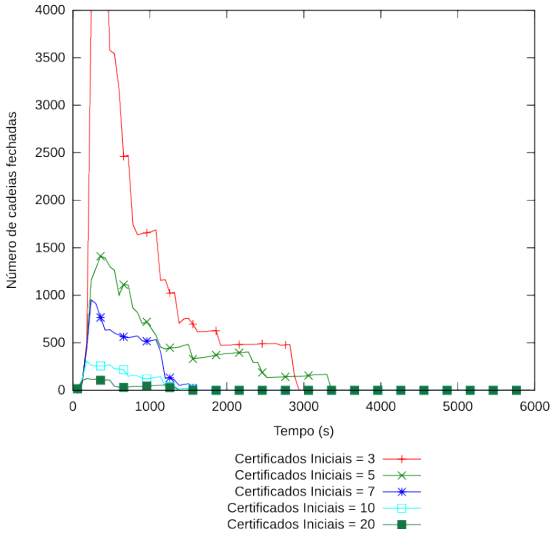
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

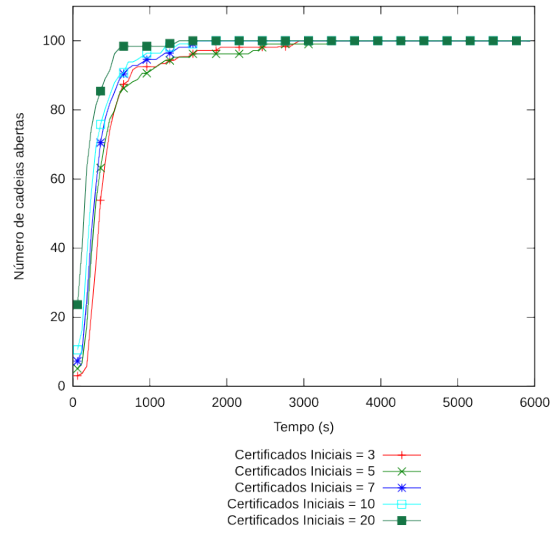
Figura B.31: Resultados para 75 nodos, $m = 50\%$ e $t = 50\%$



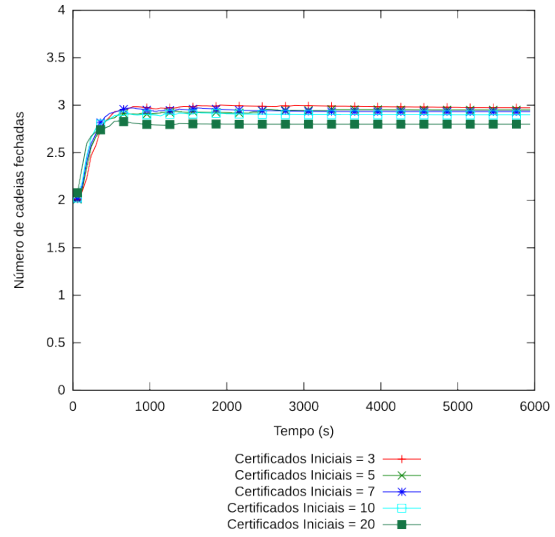

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

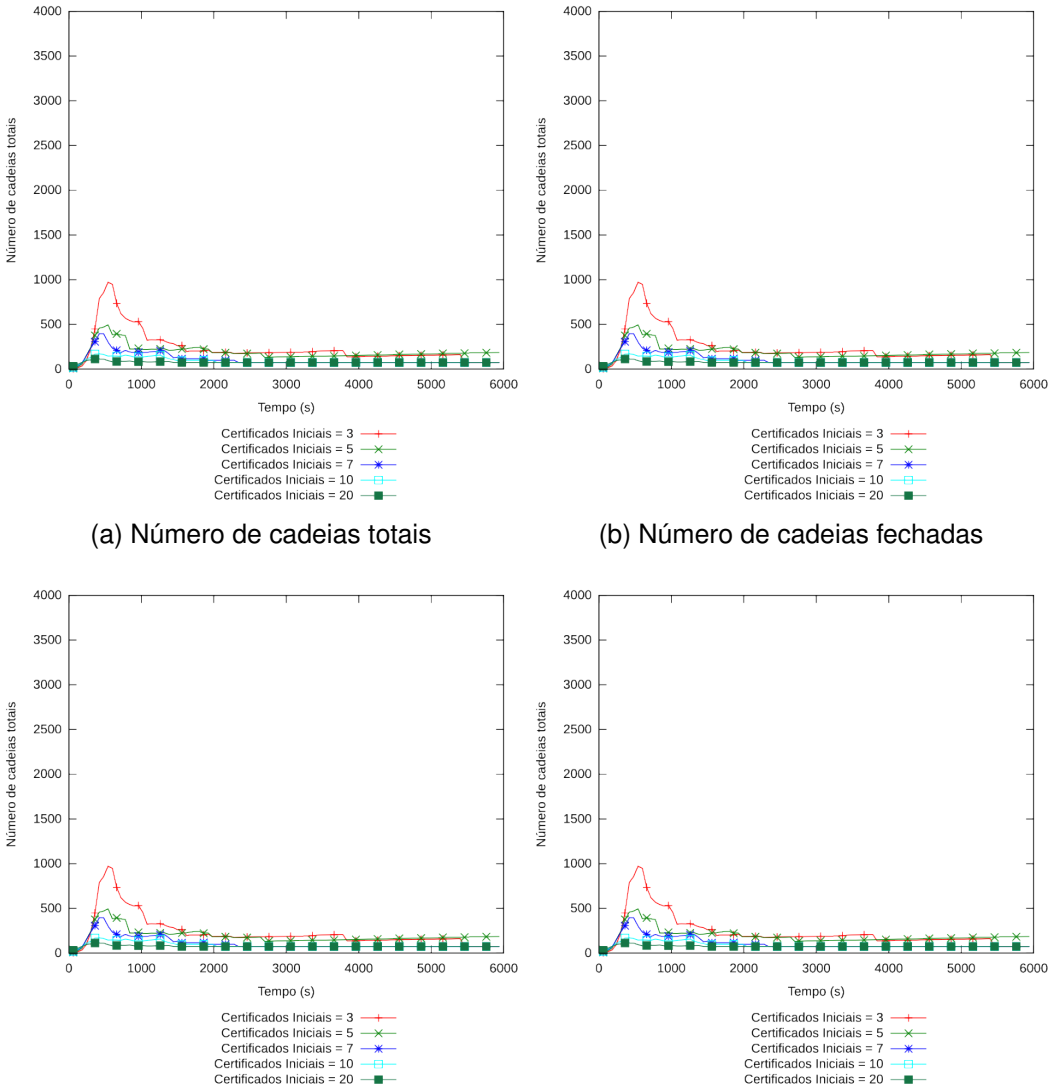



(d) Tamanho médio das cadeias

Figura B.32: Resultados para 100 nodos, $m = 50\%$ e $t = 50\%$

## B.4 Ataque *BlackHole*

### B.4.1 Ataque *BlackHole* com $m = 10\%$



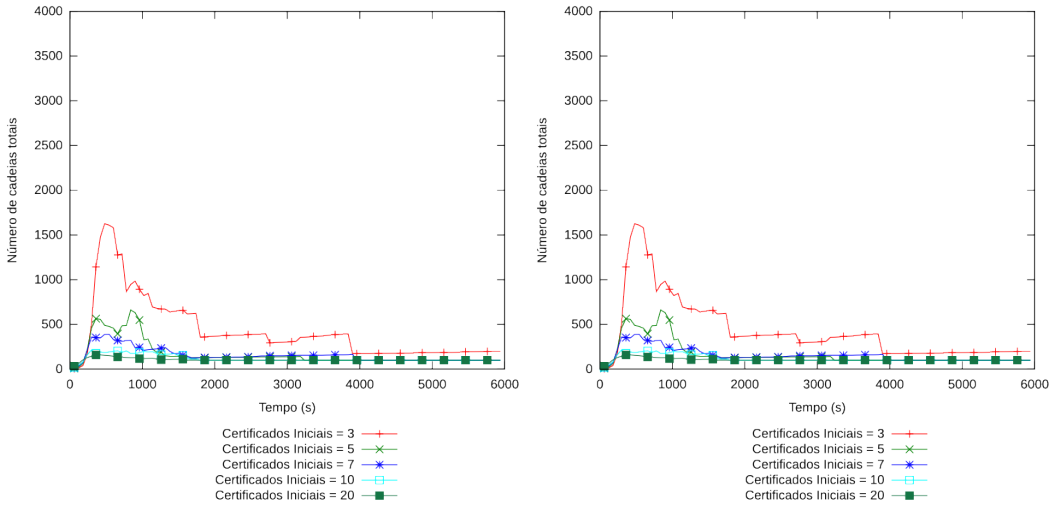

(a) Número de cadeias totais

(b) Número de cadeias fechadas

(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

Figura B.33: Resultados para 75 nodos e $m = 10\%$




(a) Número de cadeias totais

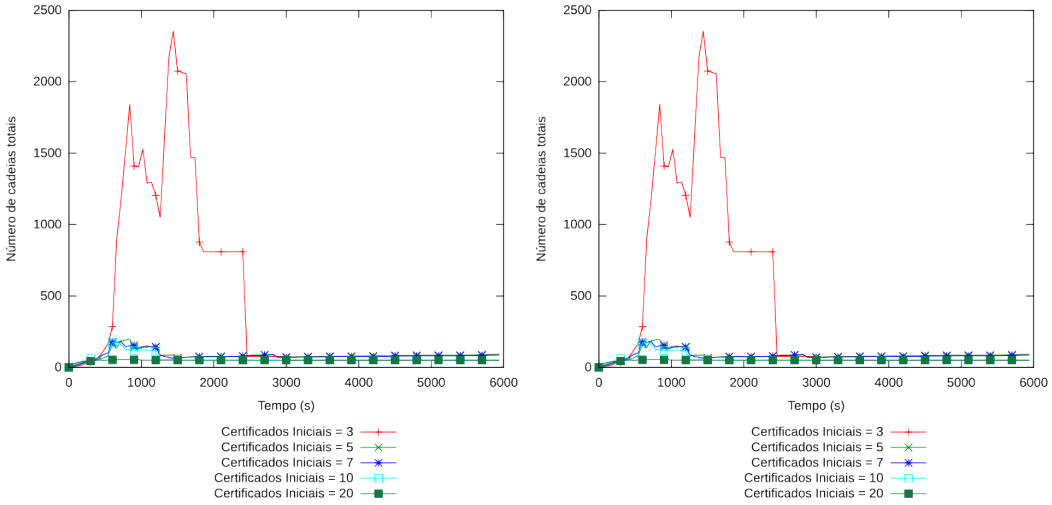
(b) Número de cadeias fechadas

(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

Figura B.34: Resultados para 100 nodos e $m = 10\%$

### B.4.2 Ataque *BlackHole* com $m = 20\%$



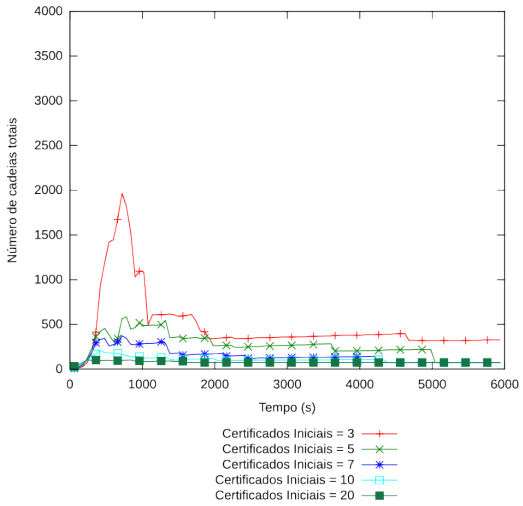

(a) Número de cadeias totais

(b) Número de cadeias fechadas

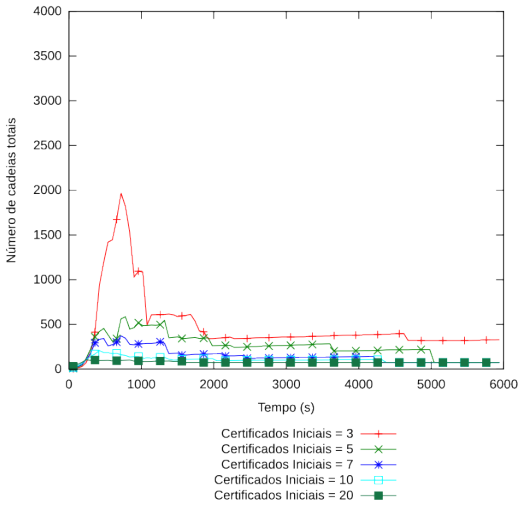
(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

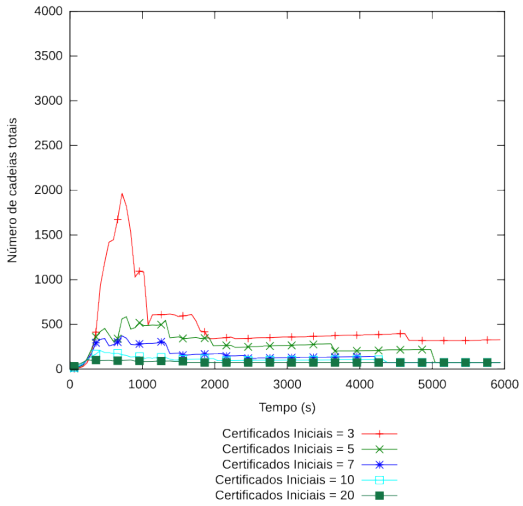
Figura B.35: Resultados para 50 nodos e $m = 20\%$



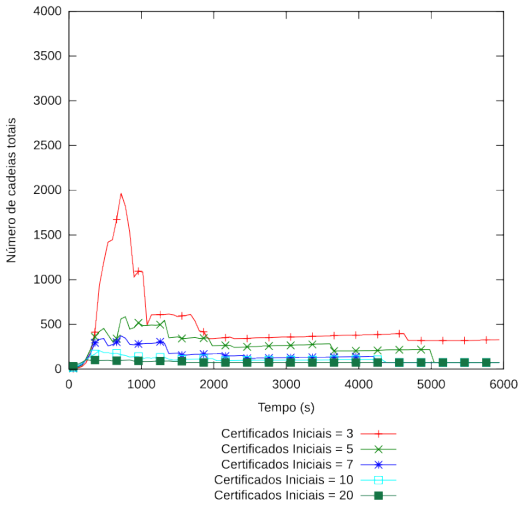

(a) Número de cadeias totais




(b) Número de cadeias fechadas

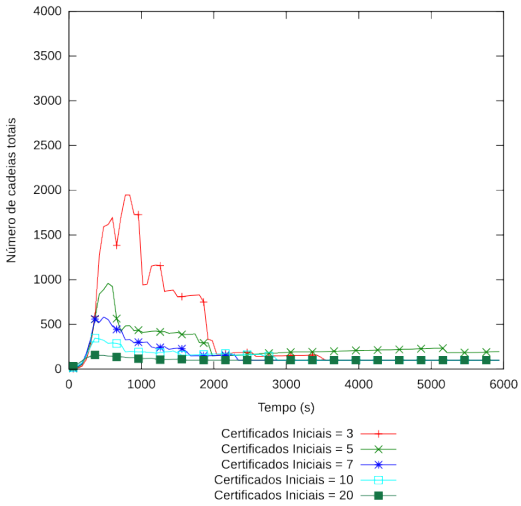



(c) Número de cadeias abertas

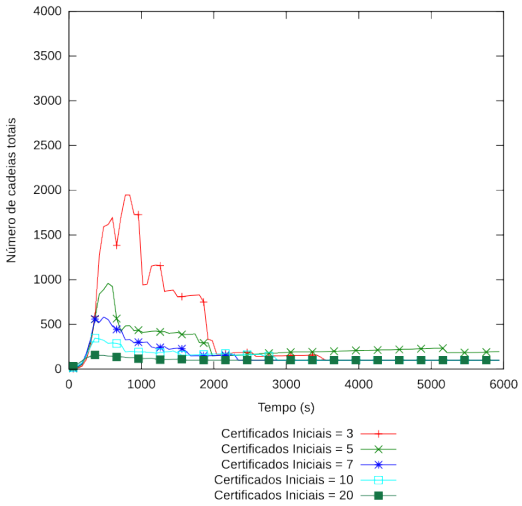



(d) Tamanho médio das cadeias

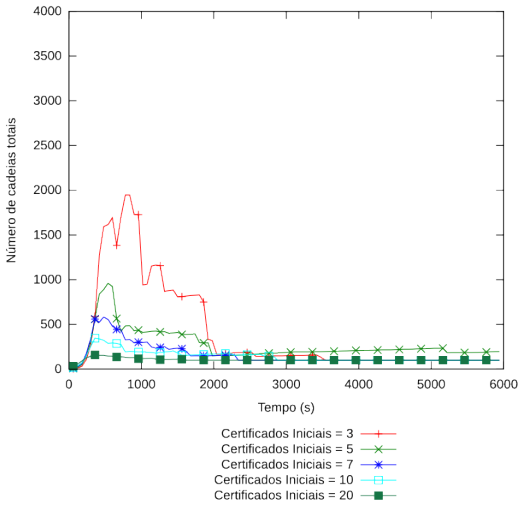
Figura B.36: Resultados para 75 nodos e $m = 20\%$



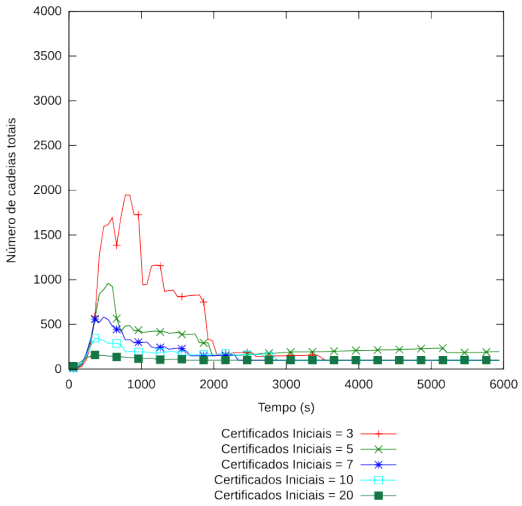

(a) Número de cadeias totais




(b) Número de cadeias fechadas

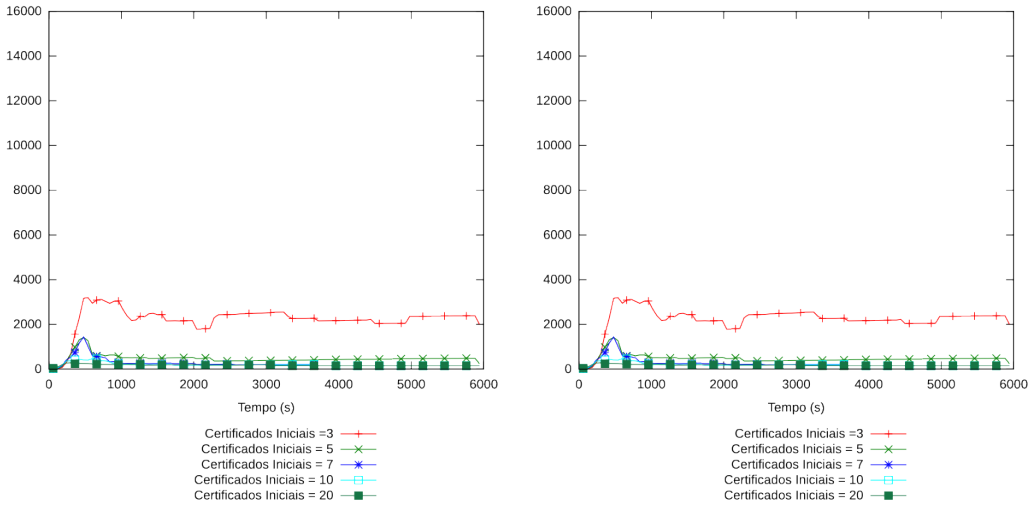



(c) Número de cadeias abertas




(d) Tamanho médio das cadeias

Figura B.37: Resultados para 100 nodos e $m = 20\%$




(a) Número de cadeias totais

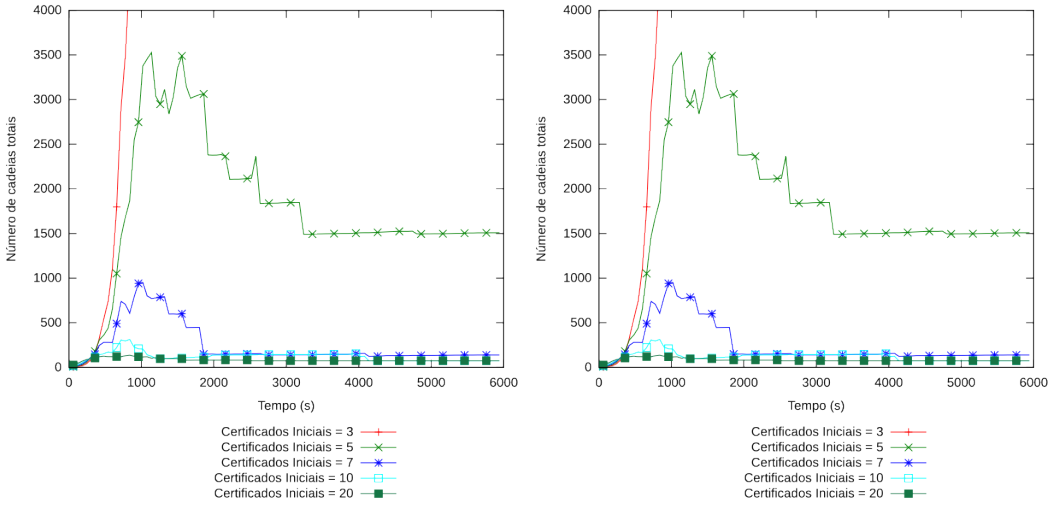
(b) Número de cadeias fechadas

(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

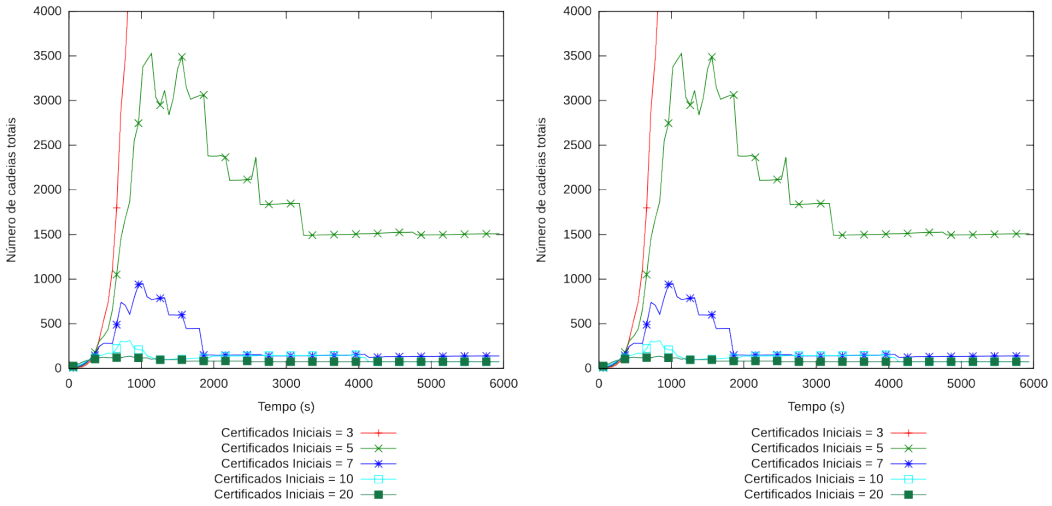
Figura B.38: Resultados para 150 nodos e $m = 20\%$

### B.4.3 Ataque *BlackHole* com $m = 50\%$




(a) Número de cadeias totais

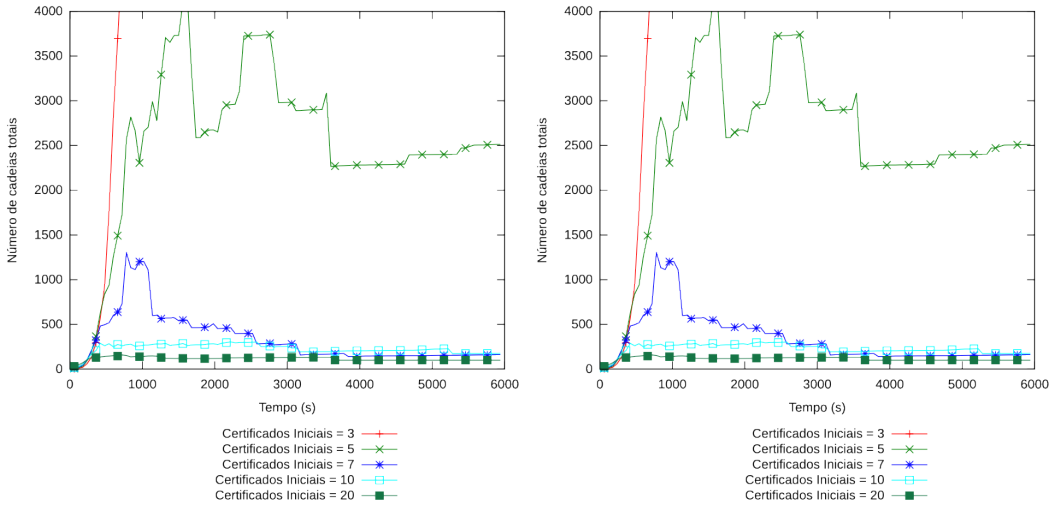
(b) Número de cadeias fechadas




(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

Figura B.39: Resultados para 75 nodos e $m = 50\%$




(a) Número de cadeias totais

(b) Número de cadeias fechadas

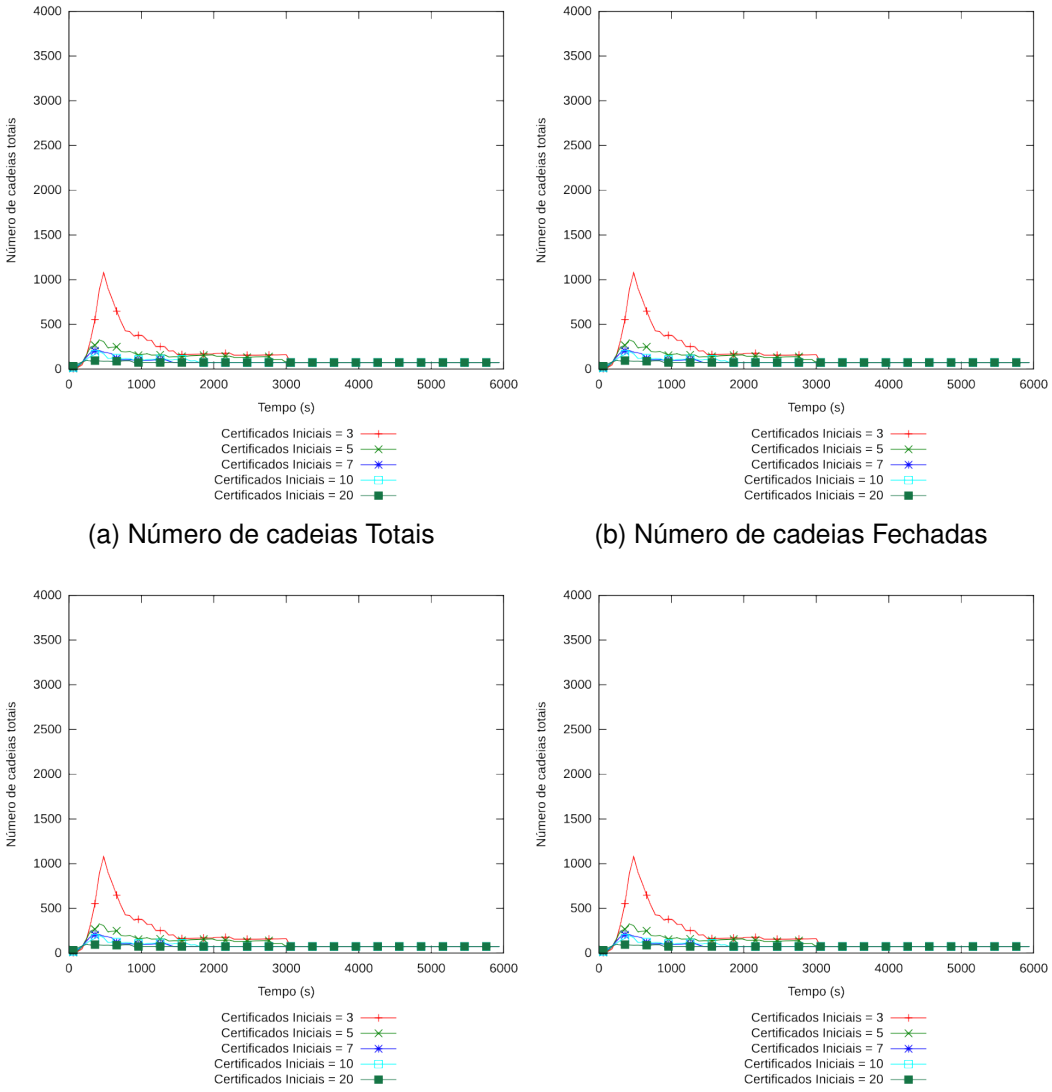
(c) Número de cadeias abertas

(d) Tamanho médio das cadeias

Figura B.40: Resultados para 100 nodos e $m = 50\%$

## B.5 Ataque *Sybil*

### B.5.1 Ataque *Sybil* com $f = 10\%$



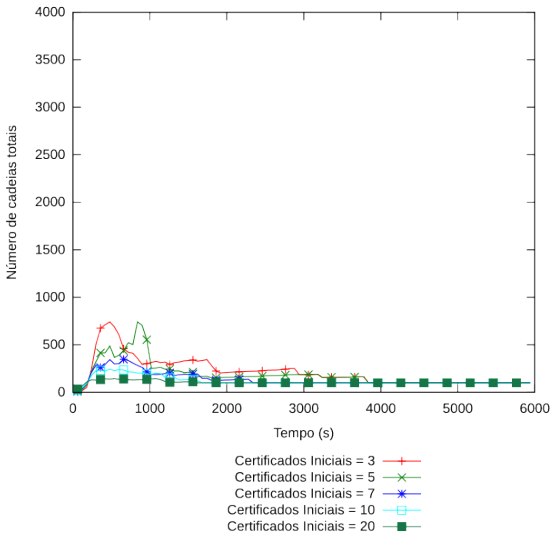

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

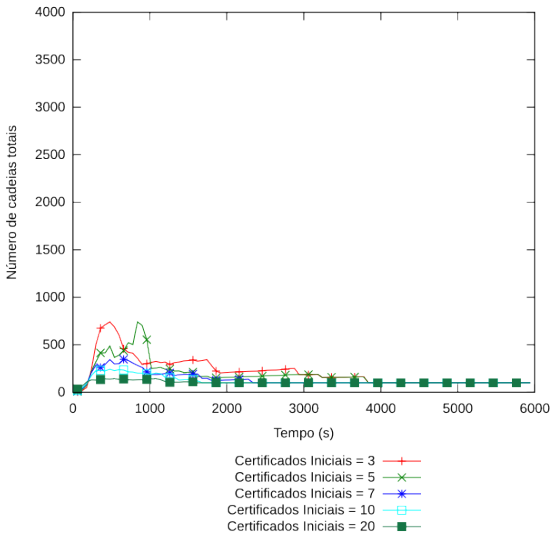
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

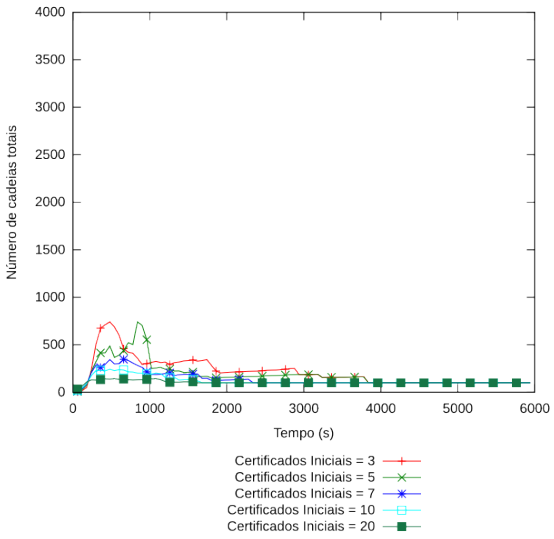
Figura B.41: Resultados para 75 nodos e $f = 10\%$



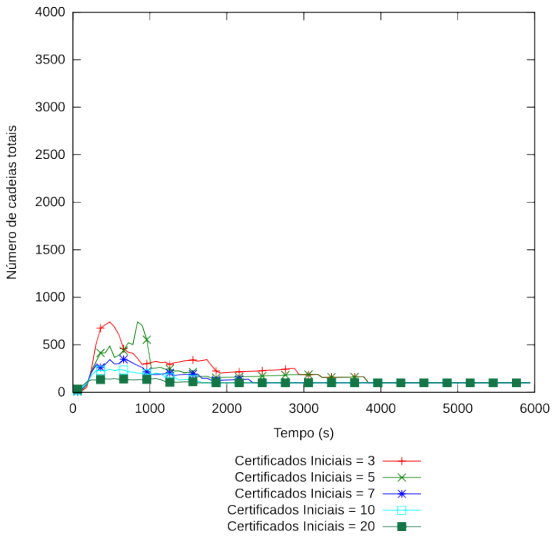

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



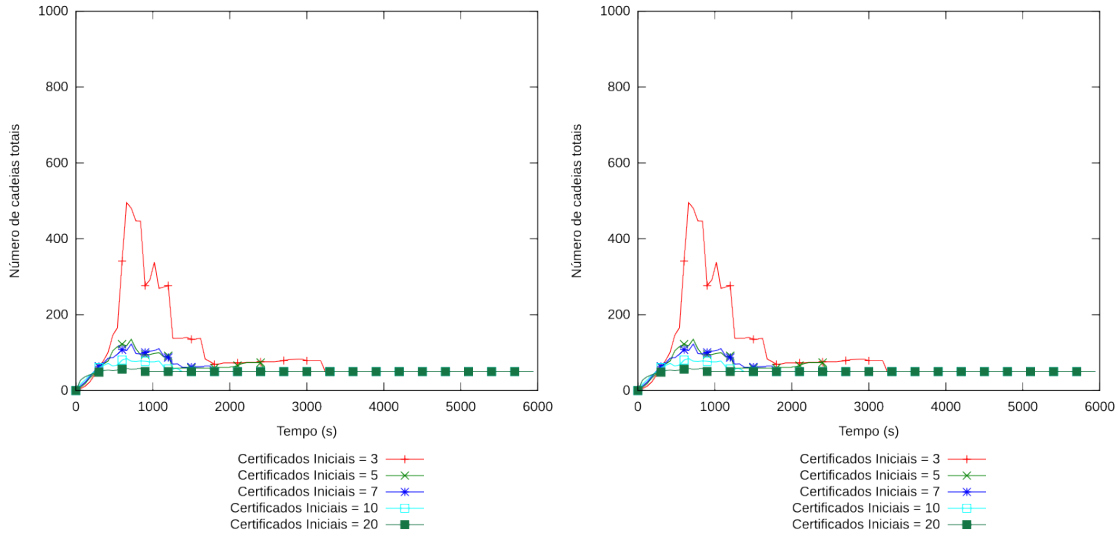

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.42: Resultados para 100 nodos e $f = 10\%$

### B.5.2 Ataque *Sybil* com $f = 20\%$



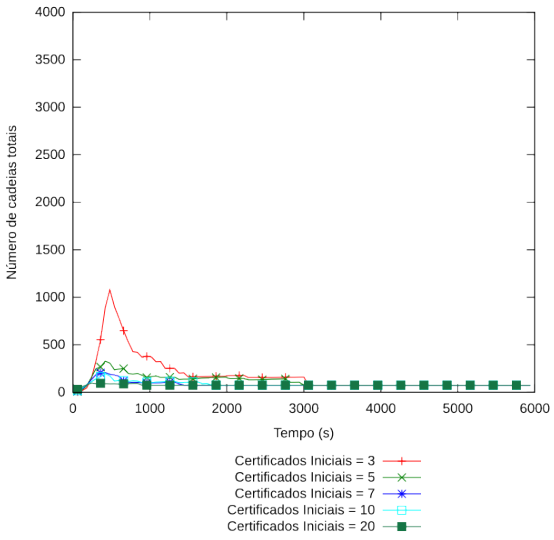

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

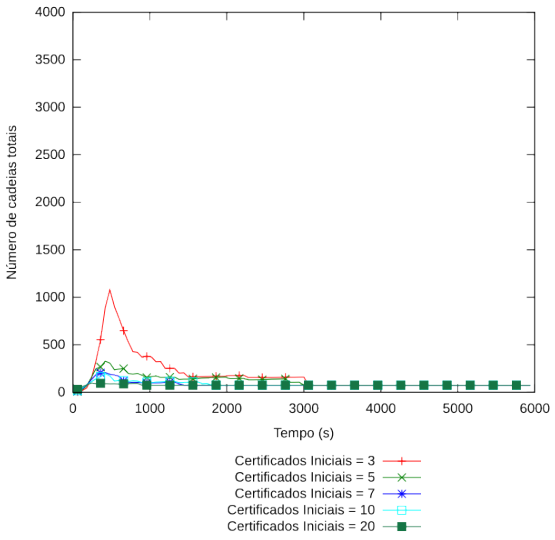
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

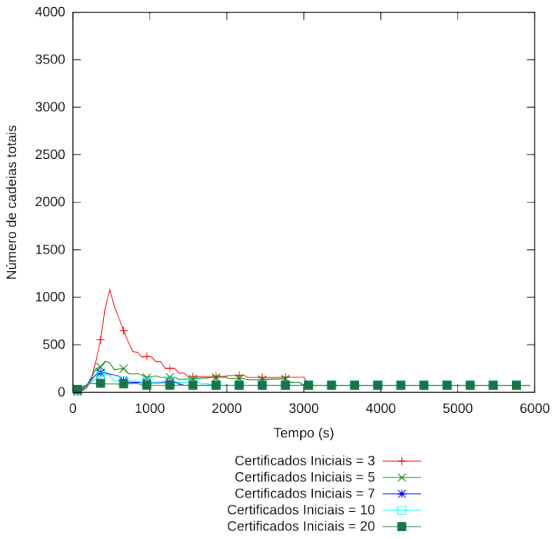
Figura B.43: Resultados para 50 nodos e $f = 20\%$



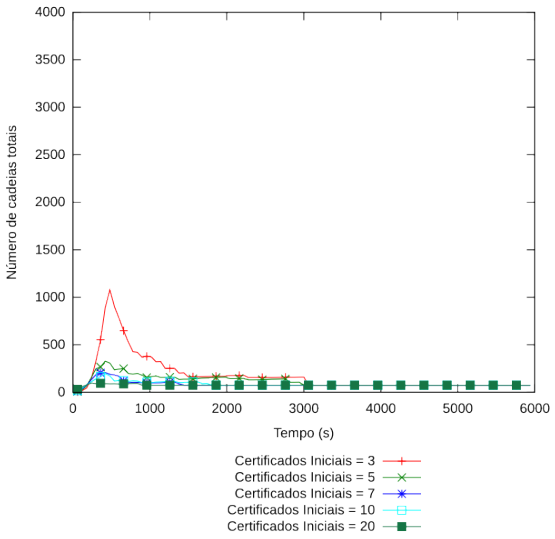

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

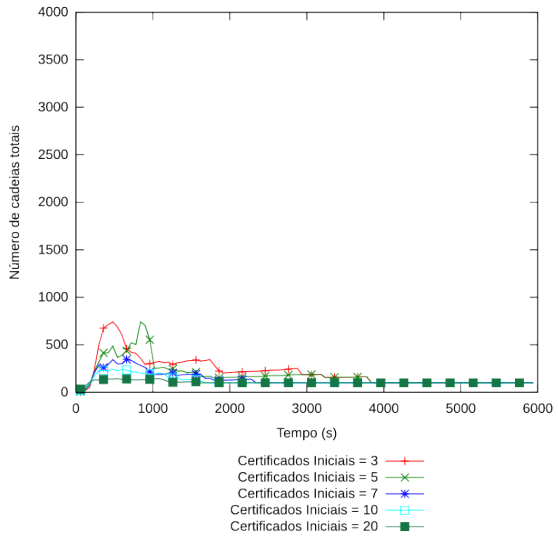



(c) Número de cadeias Abertas

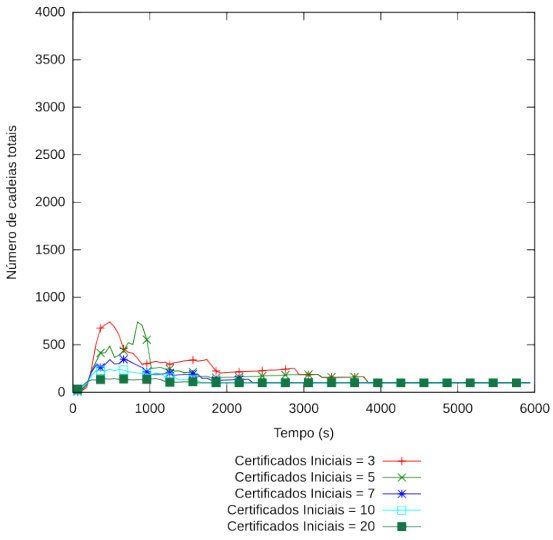



(d) Tamanho médio das cadeias

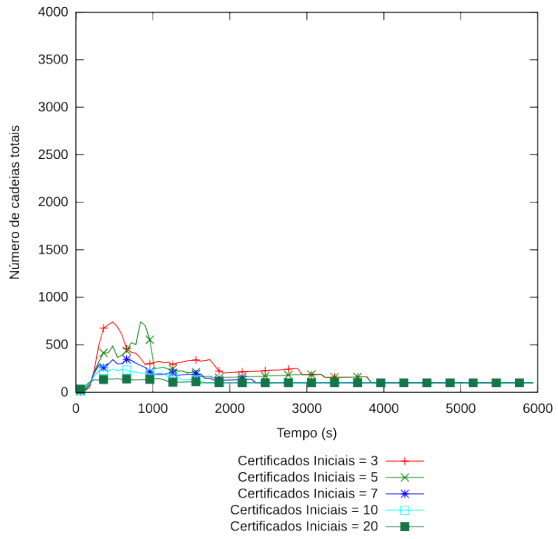
Figura B.44: Resultados para 75 nodos e $f = 20\%$



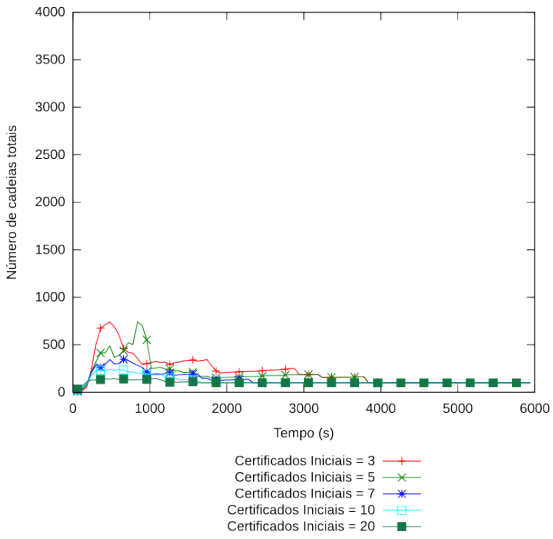

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

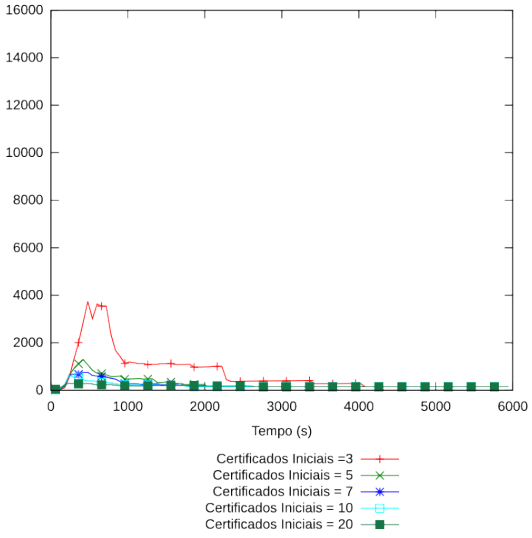



(c) Número de cadeias Abertas

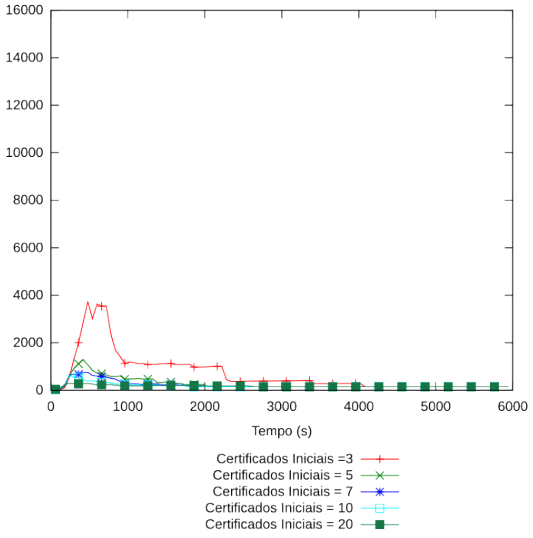



(d) Tamanho médio das cadeias

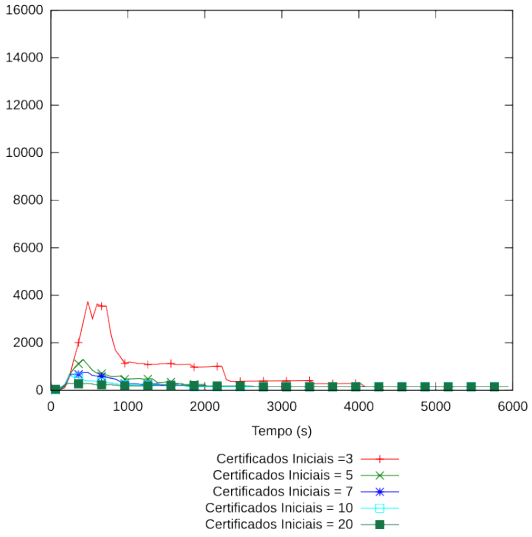
Figura B.45: Resultados para 100 nodos e $f = 20\%$



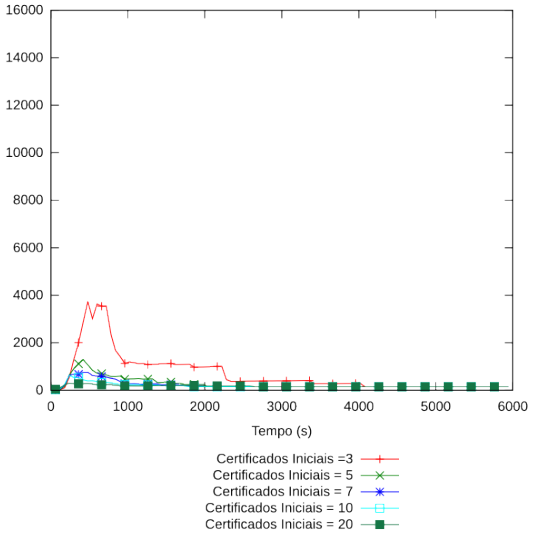

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



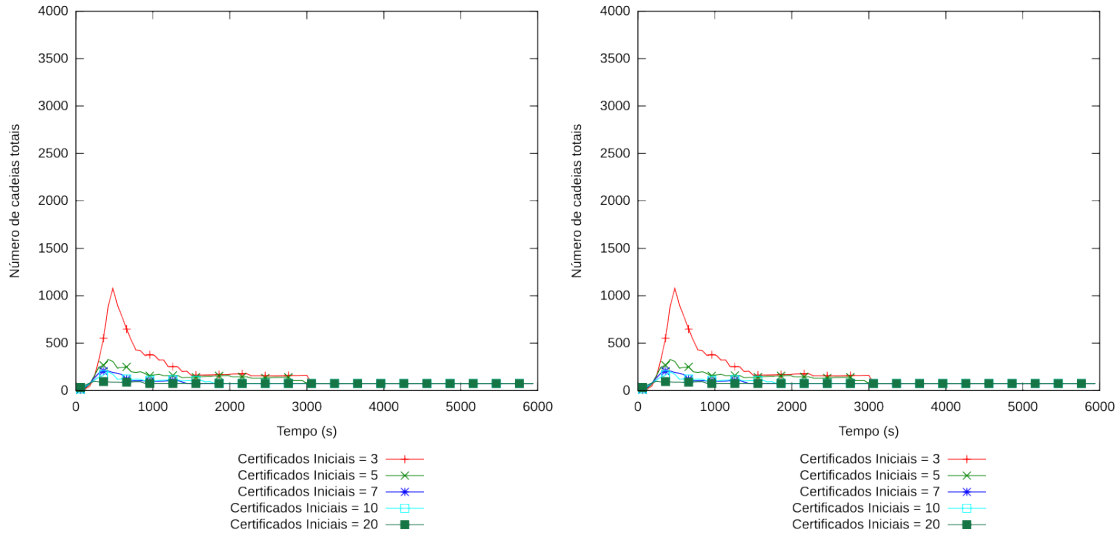

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.46: Resultados para 150 nodos e $f = 20\%$

### B.5.3 Ataque *Sybil* com $f = 50\%$



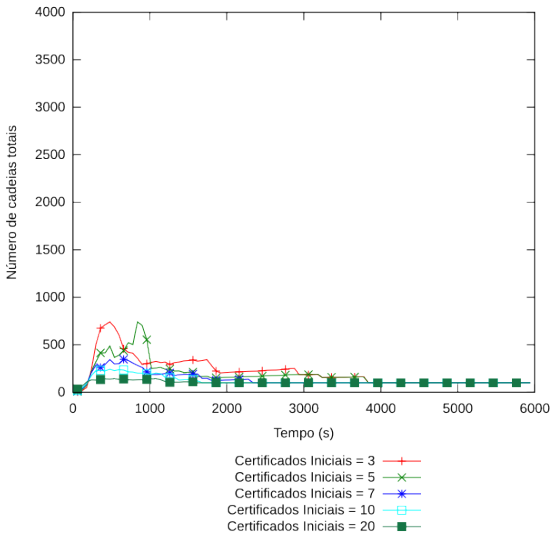

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

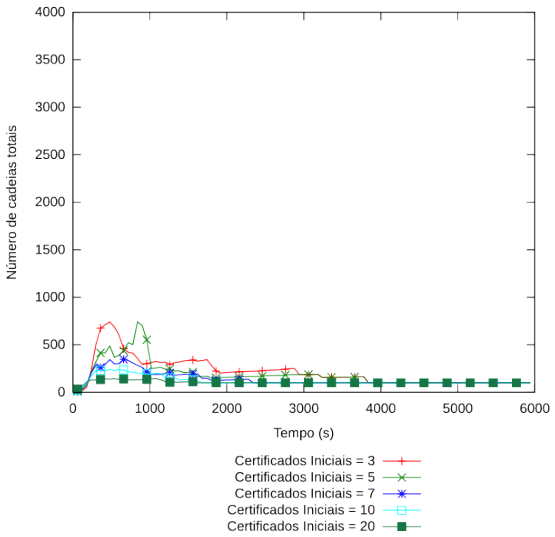
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

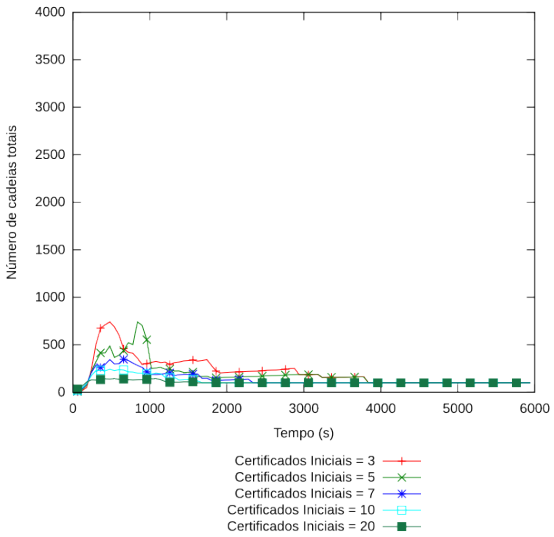
Figura B.47: Resultados para 75 nodos e $f = 50\%$



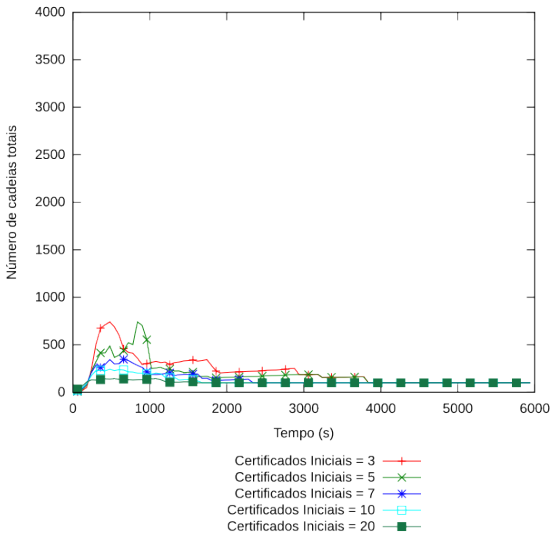

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

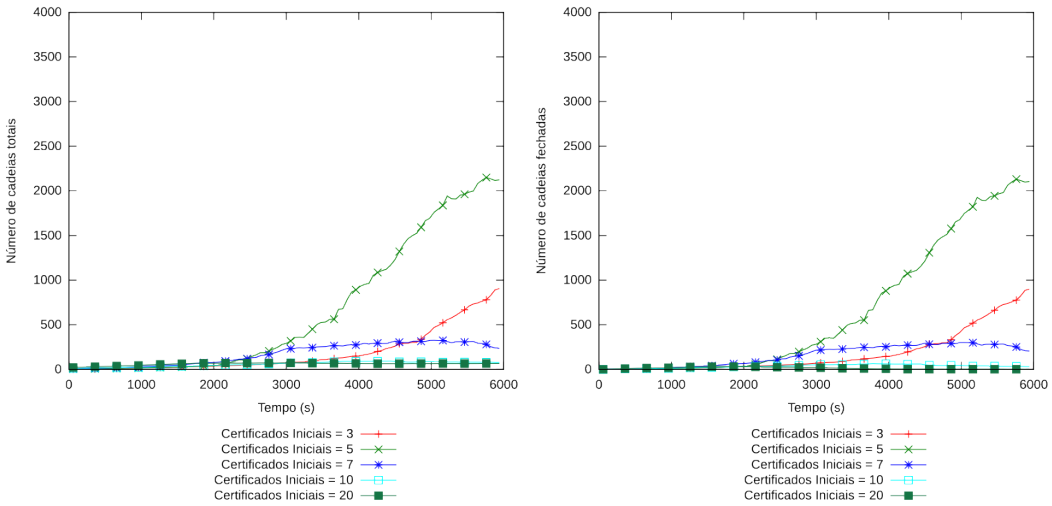



(d) Tamanho médio das cadeias

Figura B.48: Resultados para 100 nodos e $f = 50\%$

## B.6 Ataque de Falsificaçao - Ataque independente

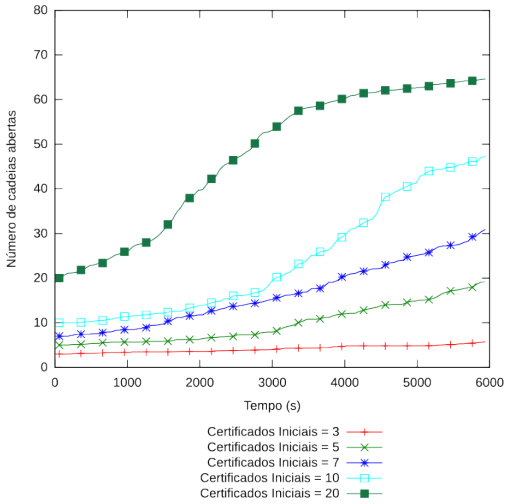
### B.6.1 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 10\%$



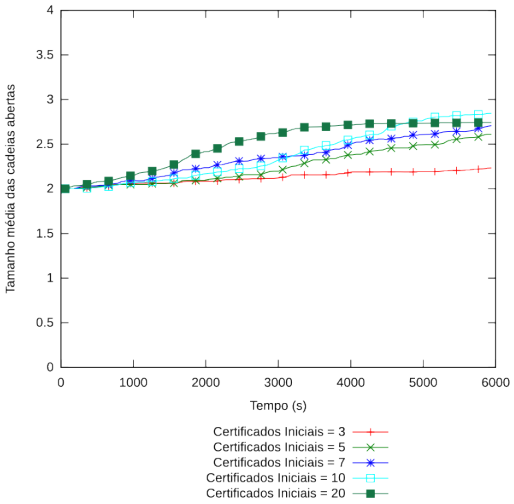

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

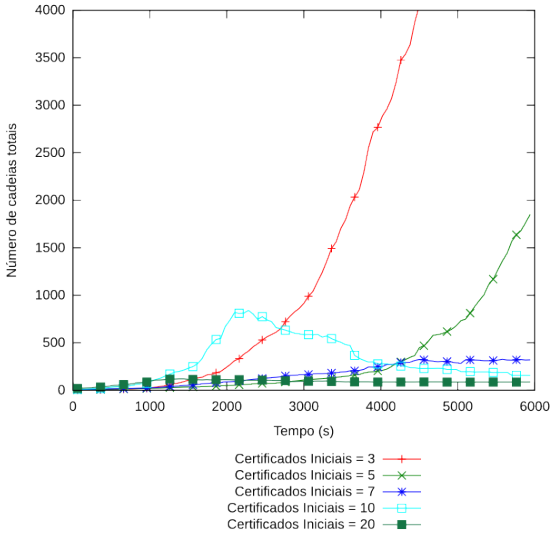



(c) Número de cadeias Abertas

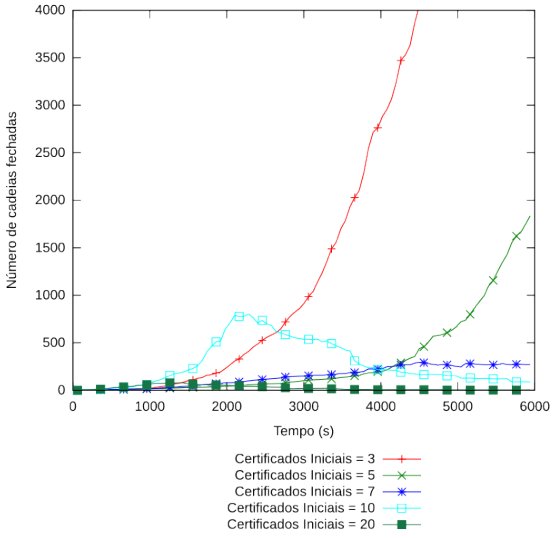



(d) Tamanho médio das cadeias

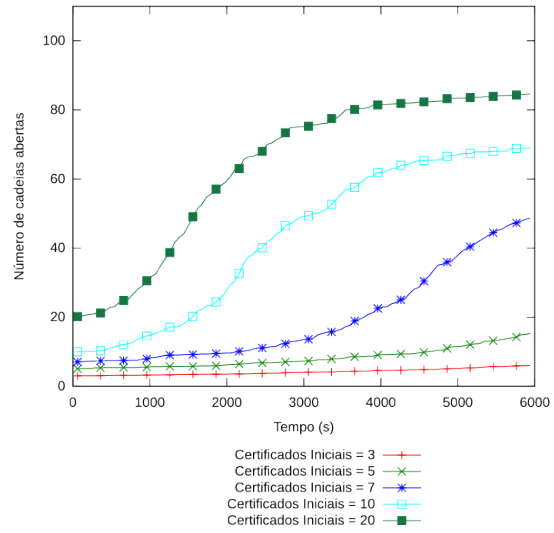
Figura B.49: Resultados para 75 nodos, $m = 10\%$ e $N_a = 10\%$



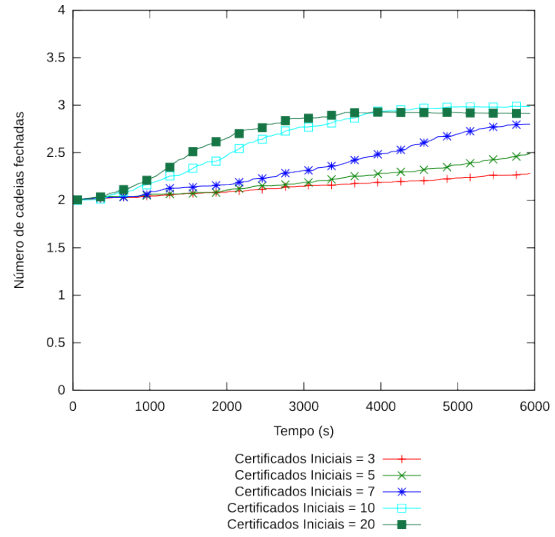

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



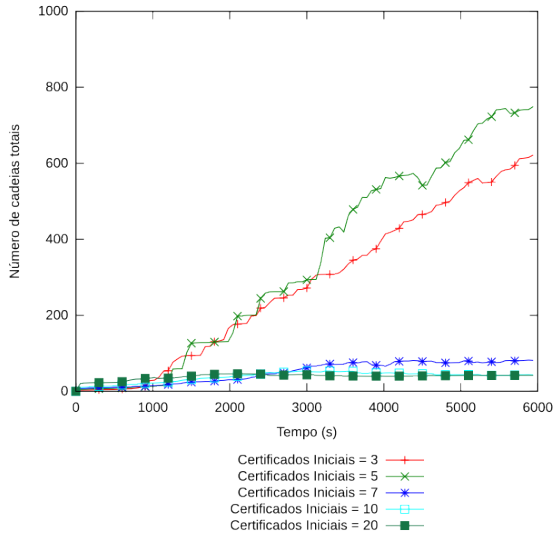

(c) Número de cadeias Abertas



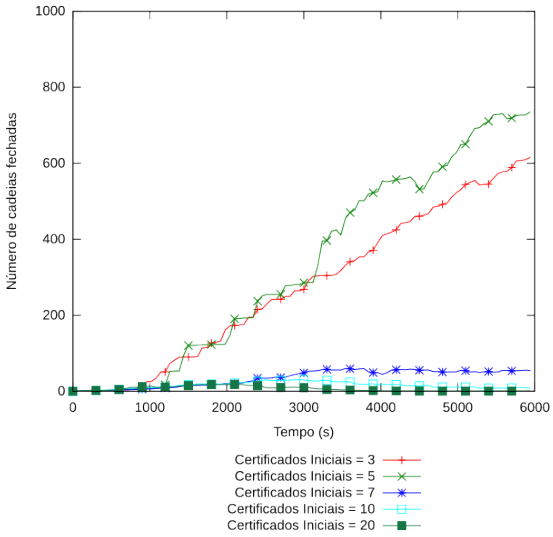

(d) Tamanho médio das cadeias

Figura B.50: Resultados para 100 nodos, $m = 10\%$ e $N_a = 10\%$

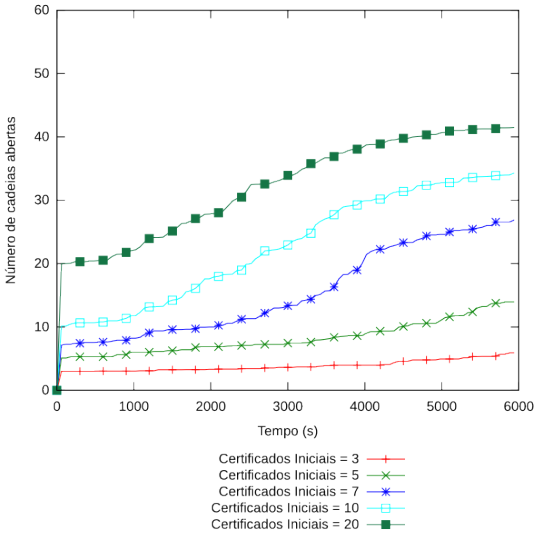
### B.6.2 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 25\%$



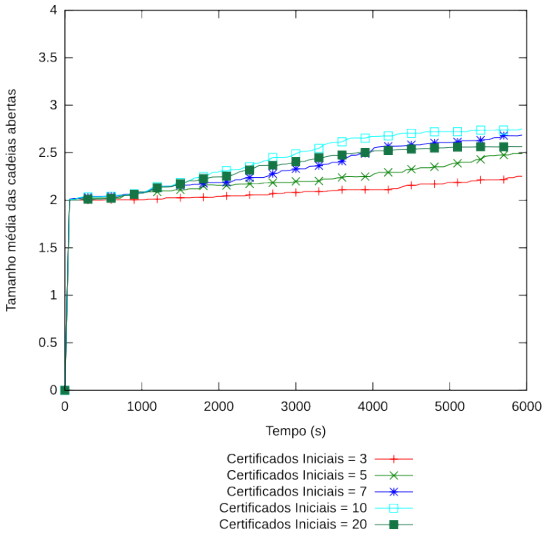

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

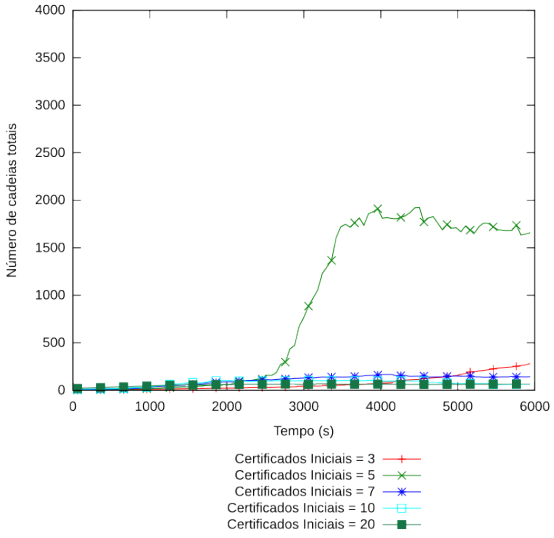



(c) Número de cadeias Abertas

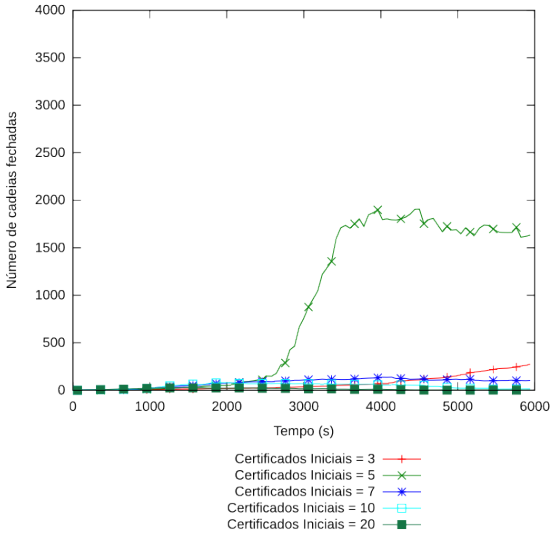



(d) Tamanho médio das cadeias

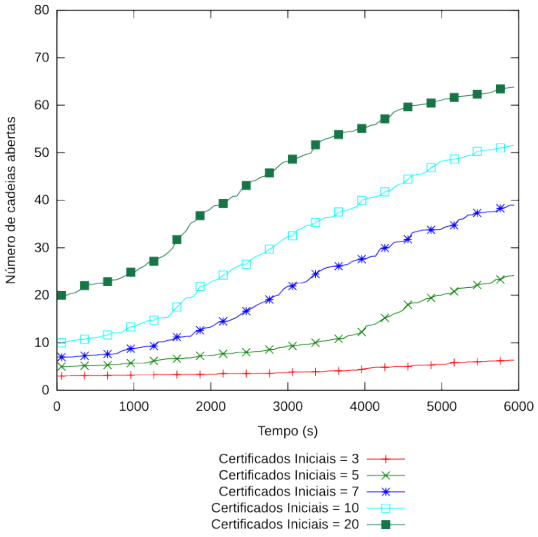
Figura B.51: Resultados para 50 nodos, $m = 10\%$ e $N_a = 25\%$



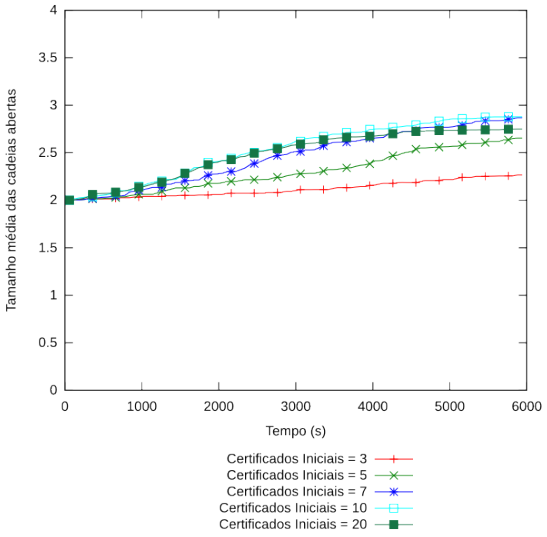

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

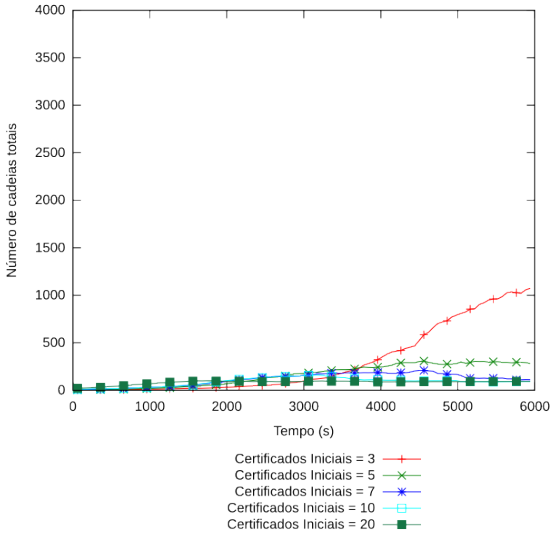



(c) Número de cadeias Abertas

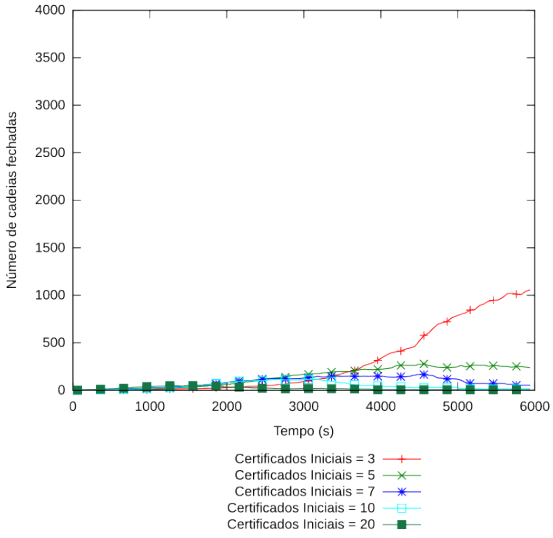



(d) Tamanho médio das cadeias

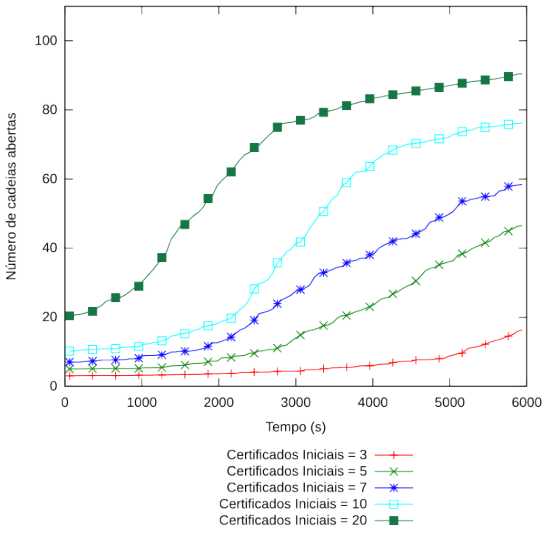
Figura B.52: Resultados para 75 nodos, $m = 10\%$ e $N_a = 25\%$



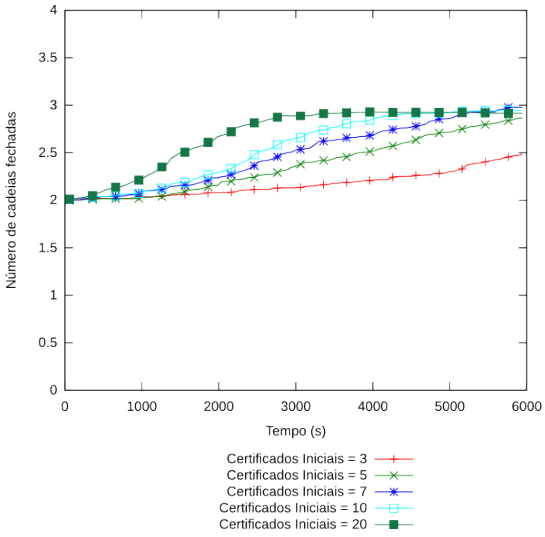

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

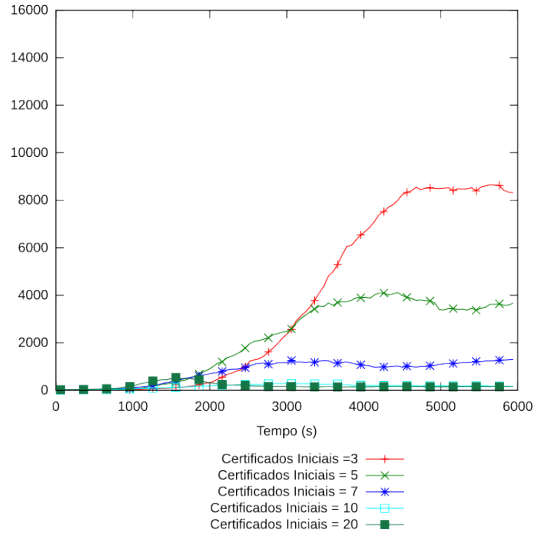



(c) Número de cadeias Abertas

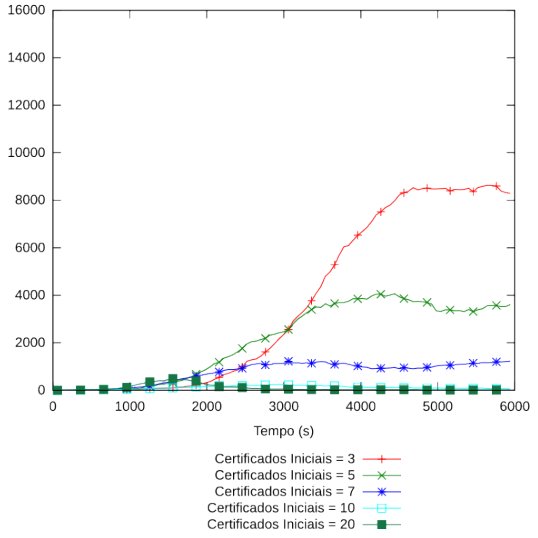



(d) Tamanho médio das cadeias

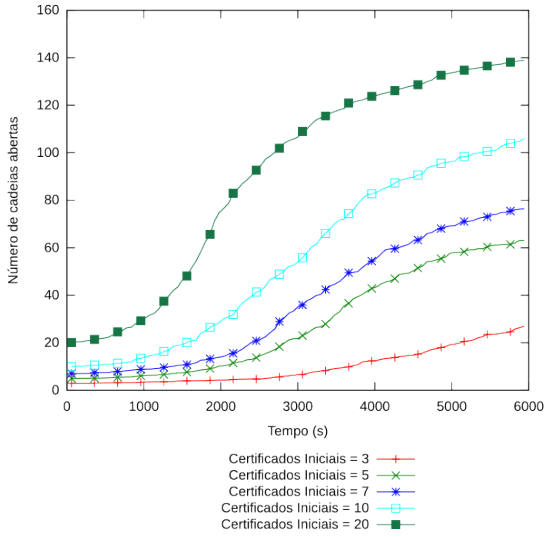
Figura B.53: Resultados para 100 nodos, $m = 10\%$ e $N_a = 25\%$



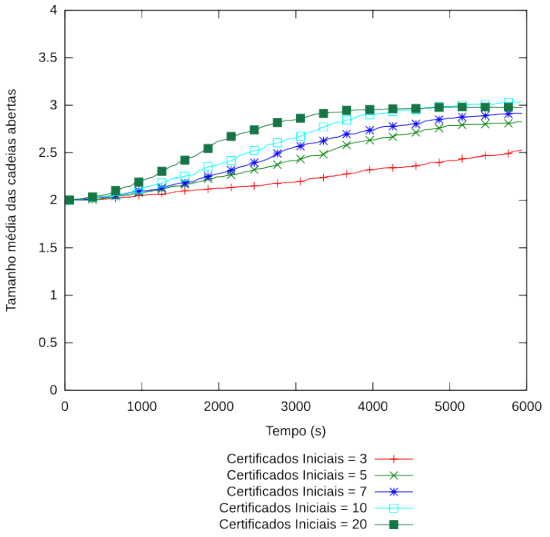

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



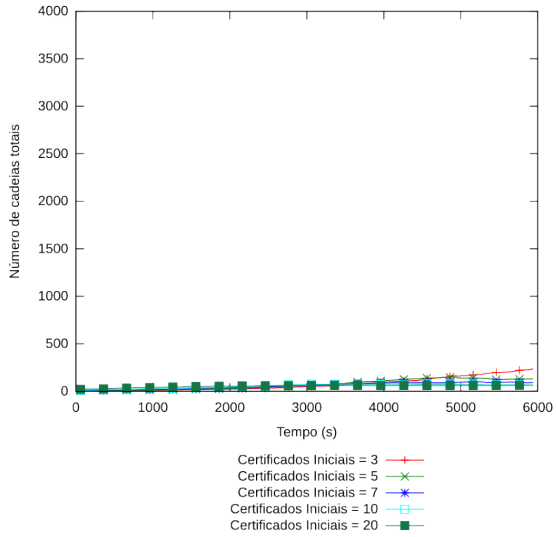

(c) Número de cadeias Abertas



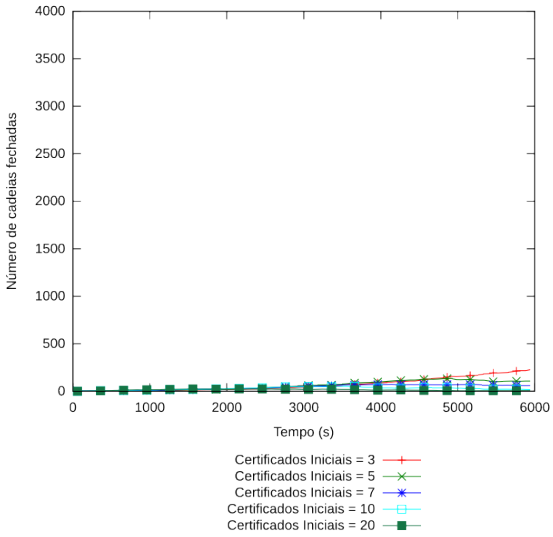

(d) Tamanho médio das cadeias

Figura B.54: Resultados para 150 nodos, $m = 10\%$ e $N_a = 25\%$

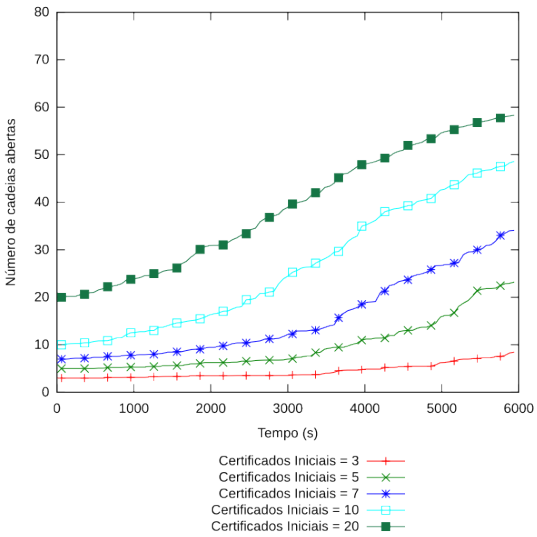
### B.6.3 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 50\%$



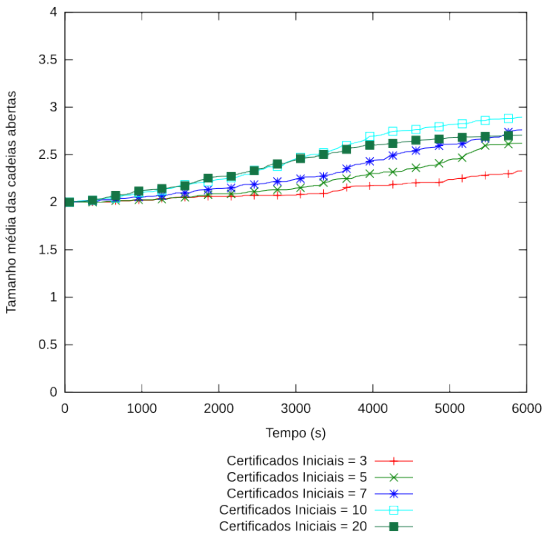

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

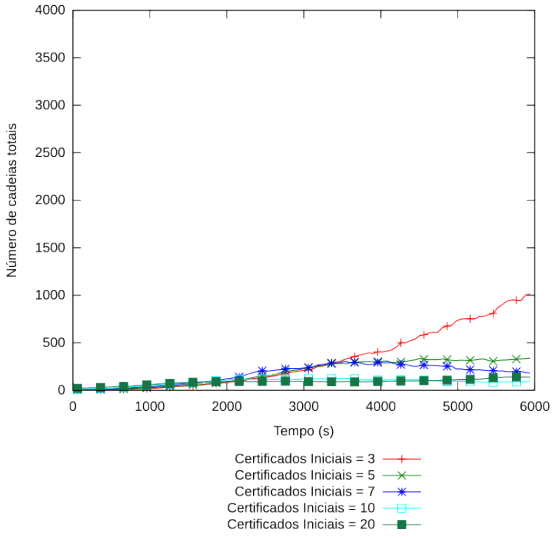



(c) Número de cadeias Abertas

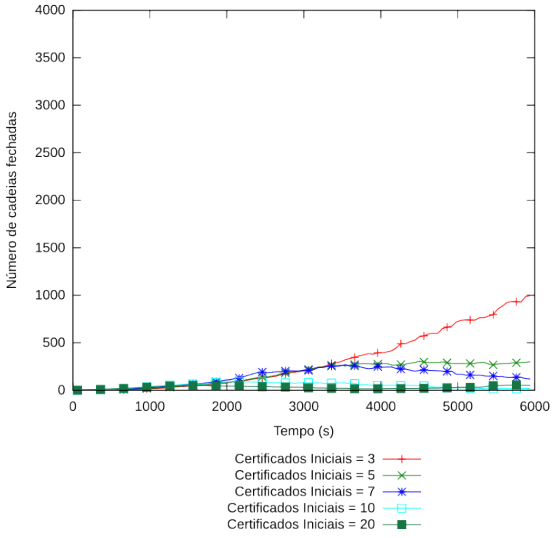



(d) Tamanho médio das cadeias

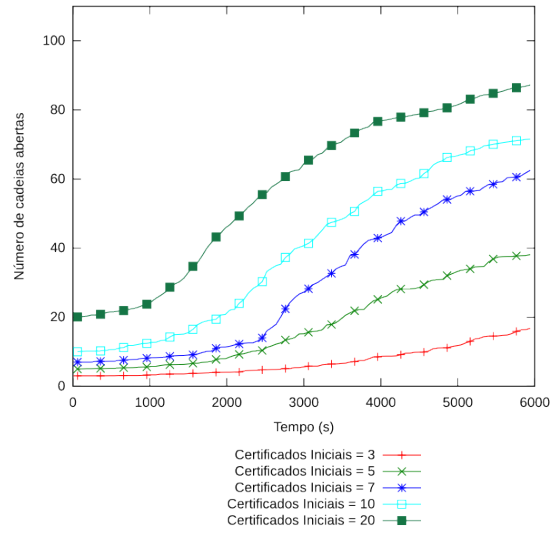
Figura B.55: Resultados para 75 nodos, $m = 10\%$ e $N_a = 50\%$



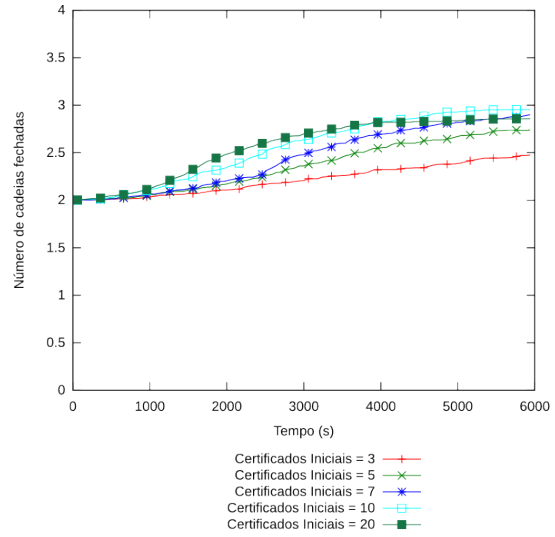

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



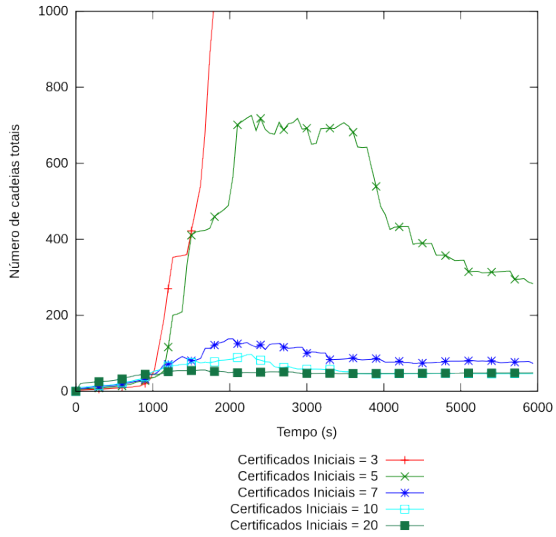

(c) Número de cadeias Abertas



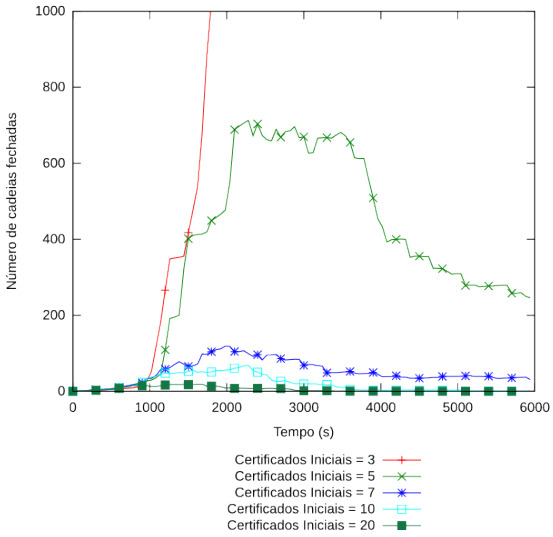

(d) Tamanho médio das cadeias

Figura B.56: Resultados para 100 nodos, $m = 10\%$ e $N_a = 50\%$

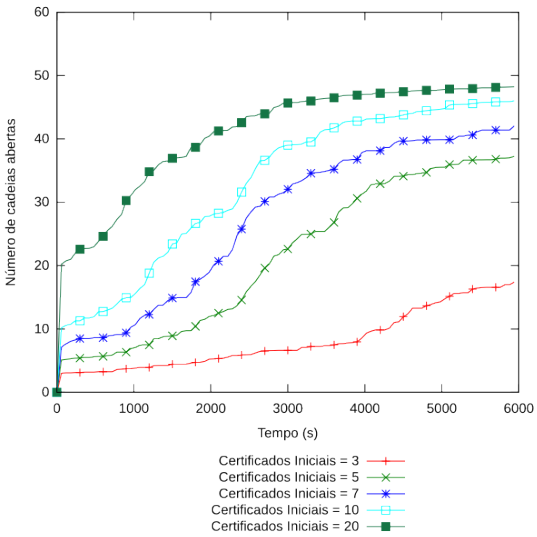
### B.6.4 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 10\%$



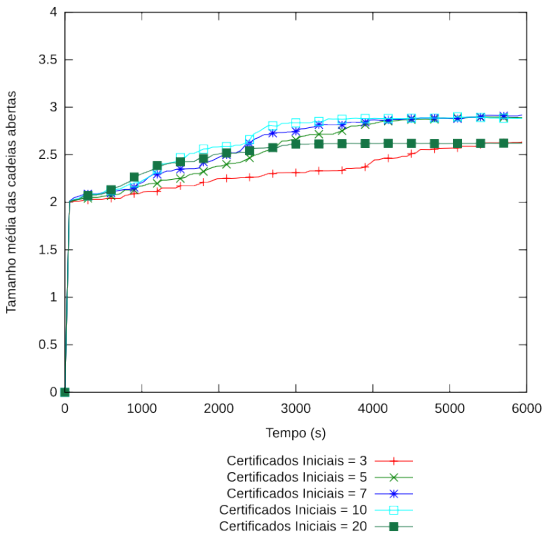

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

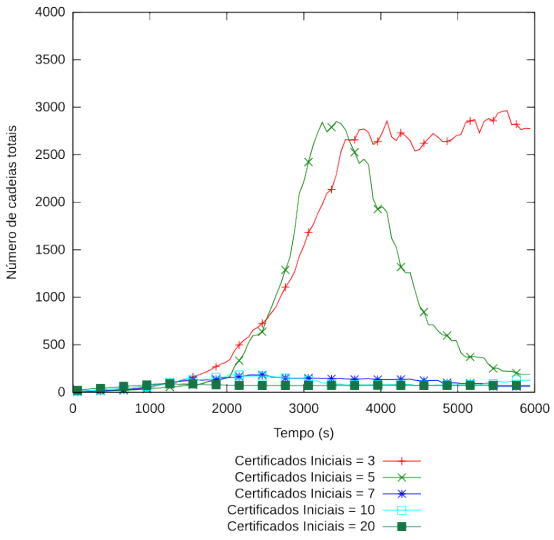



(c) Número de cadeias Abertas

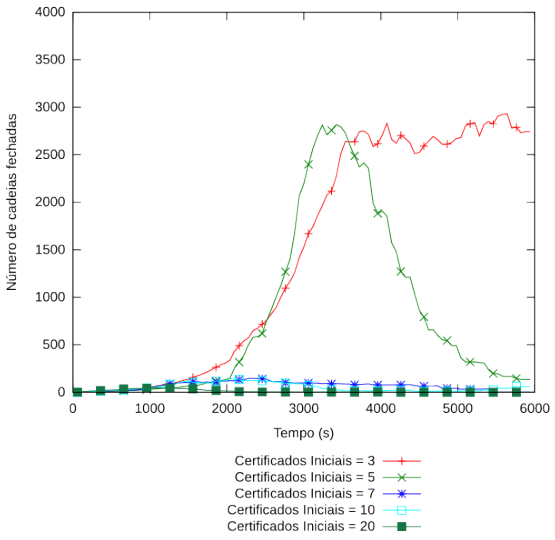



(d) Tamanho médio das cadeias

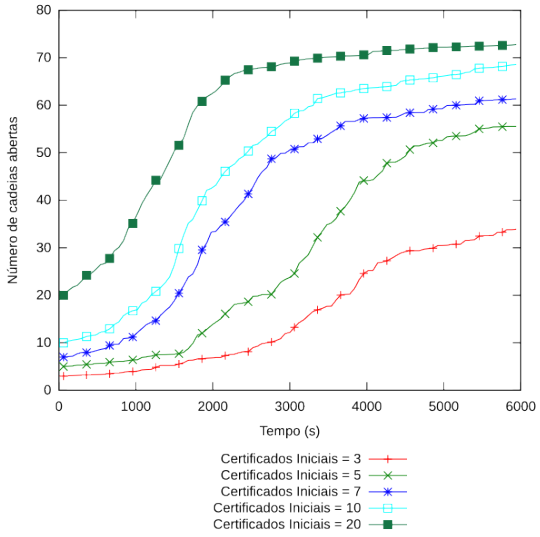
Figura B.57: Resultados para 50 nodos, $m = 20\%$ e $N_a = 10\%$



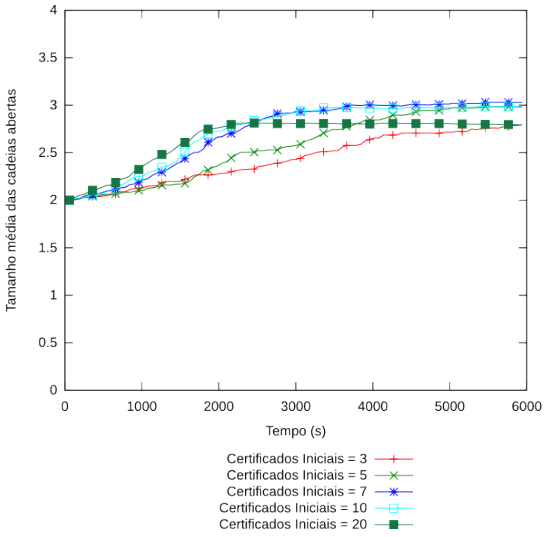

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

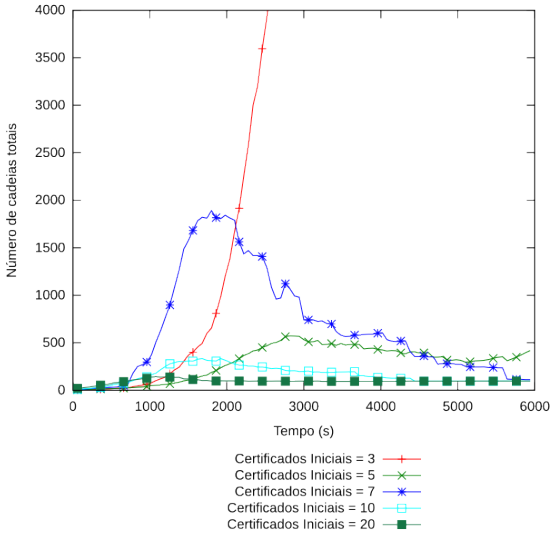



(c) Número de cadeias Abertas

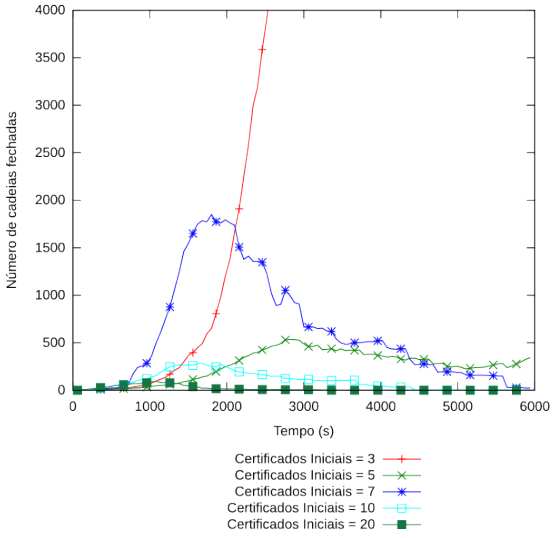



(d) Tamanho médio das cadeias

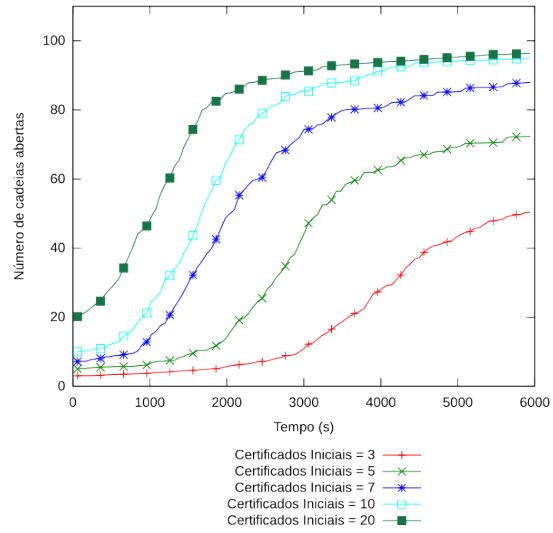
Figura B.58: Resultados para 75 nodos, $m = 20\%$ e $N_a = 10\%$



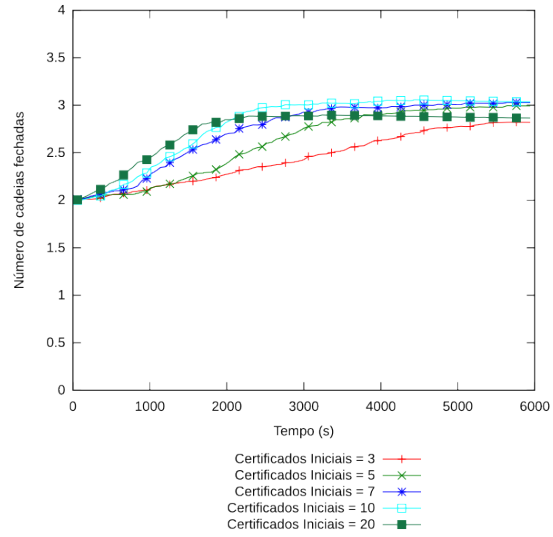

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

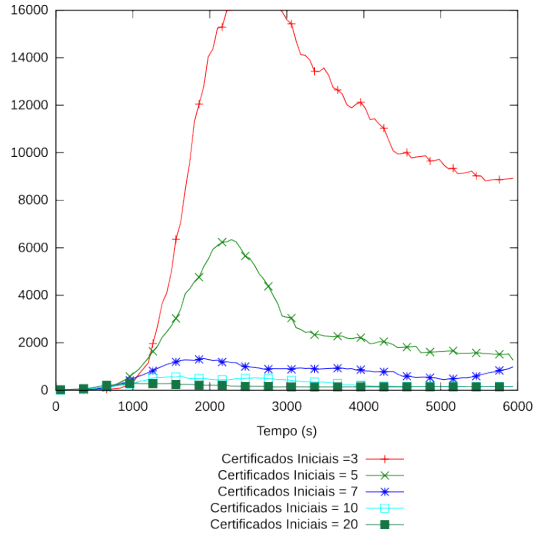



(c) Número de cadeias Abertas

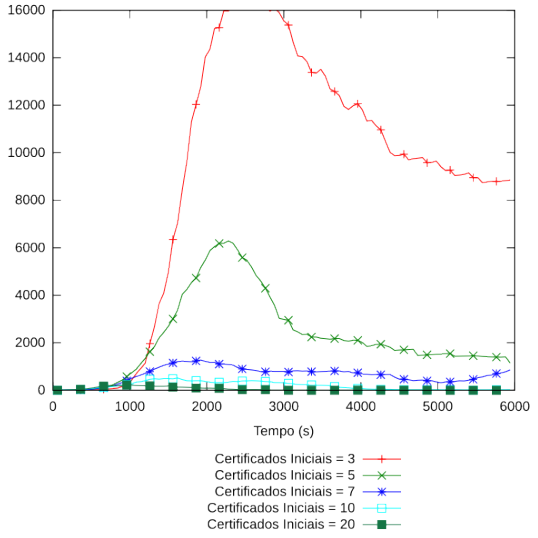



(d) Tamanho médio das cadeias

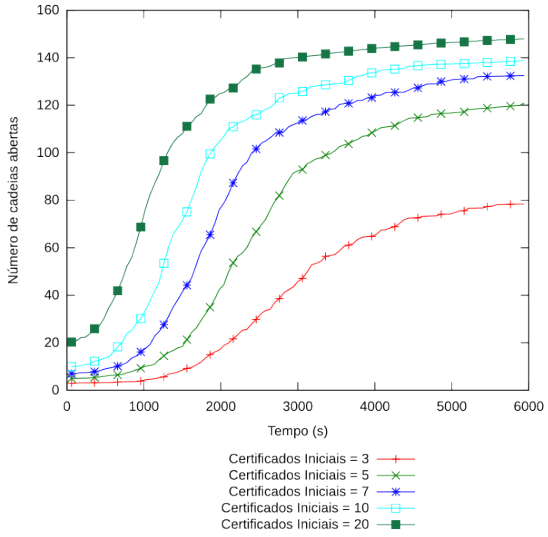
Figura B.59: Resultados para 100 nodos, $m = 20\%$ e $N_a = 10\%$



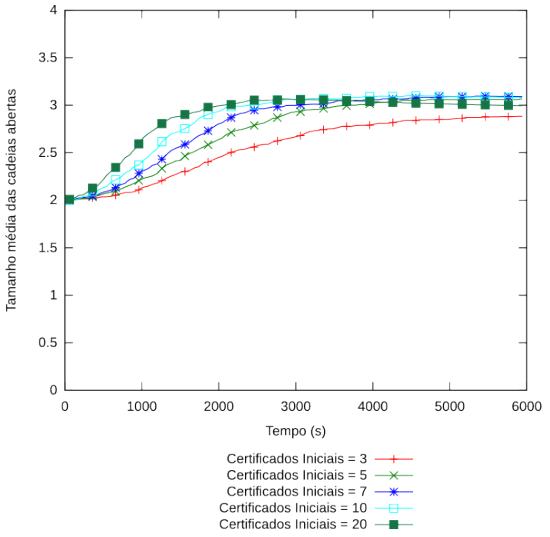

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



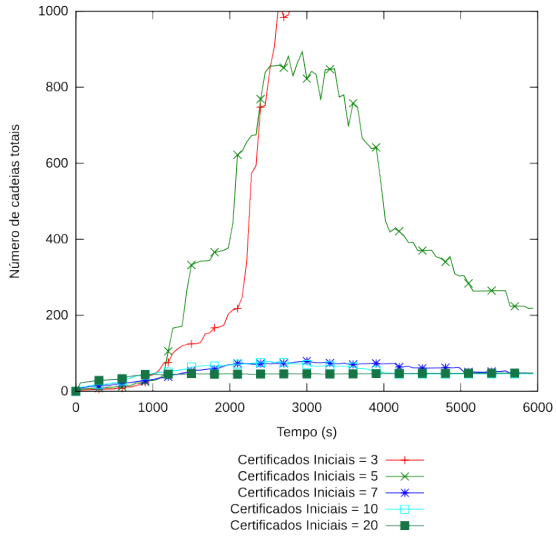

(c) Número de cadeias Abertas



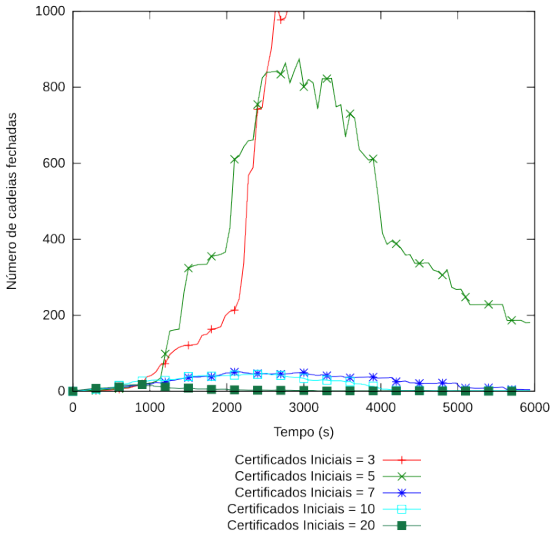

(d) Tamanho médio das cadeias

Figura B.60: Resultados para 150 nodos, $m = 20\%$ e $N_a = 10\%$

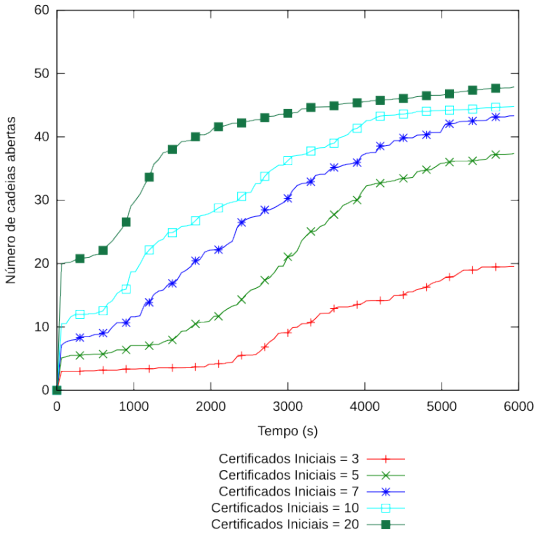
### B.6.5 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 25\%$



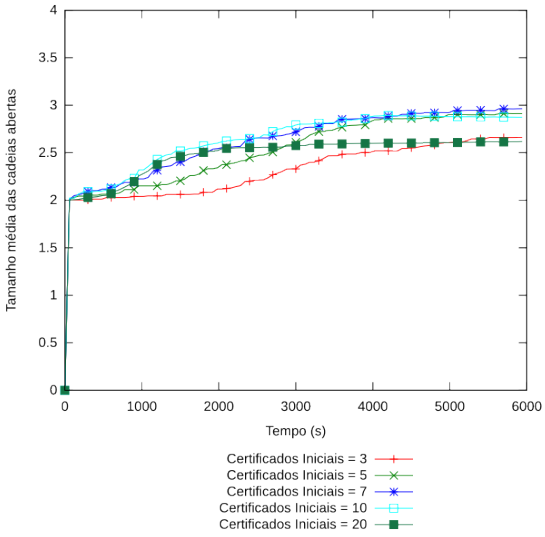

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

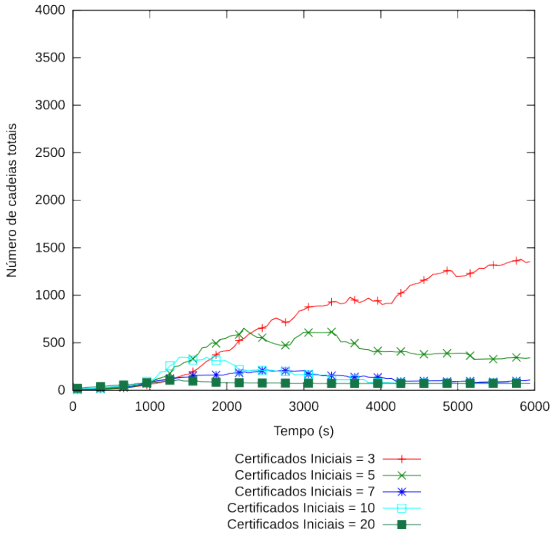



(c) Número de cadeias Abertas

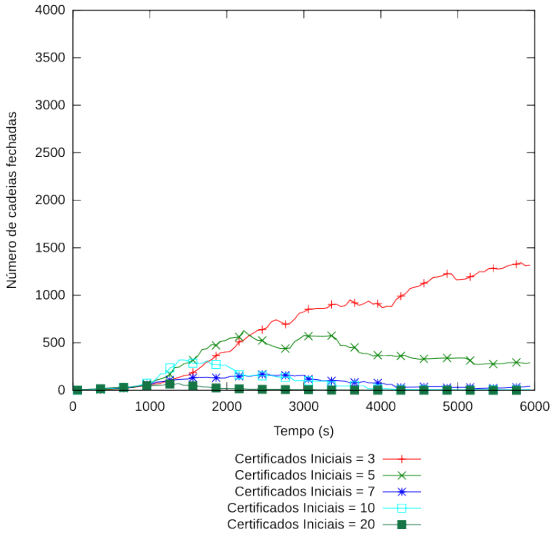



(d) Tamanho médio das cadeias

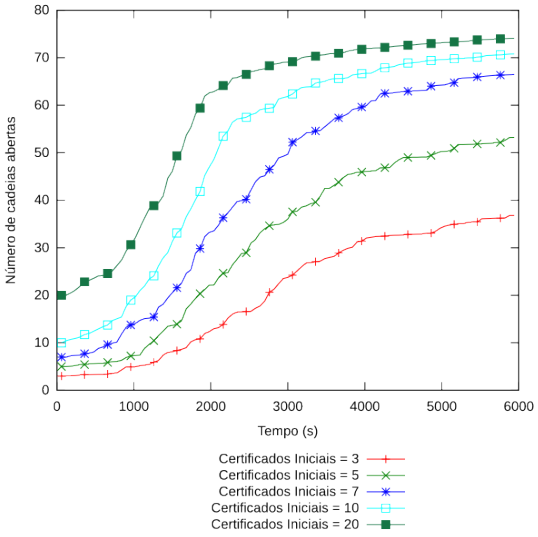
Figura B.61: Resultados para 50 nodos, $m = 20\%$ e $N_a = 25\%$



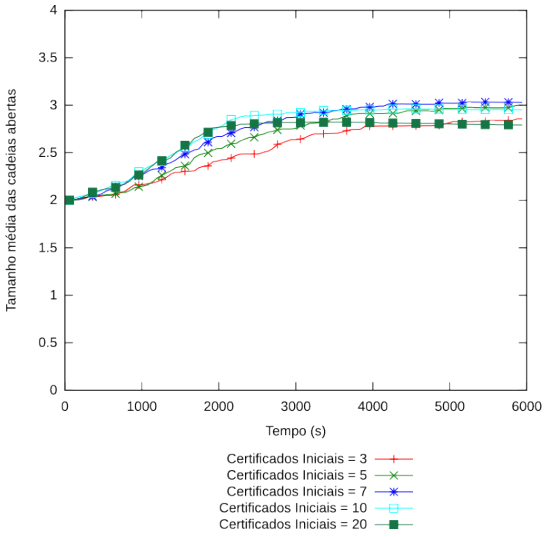

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

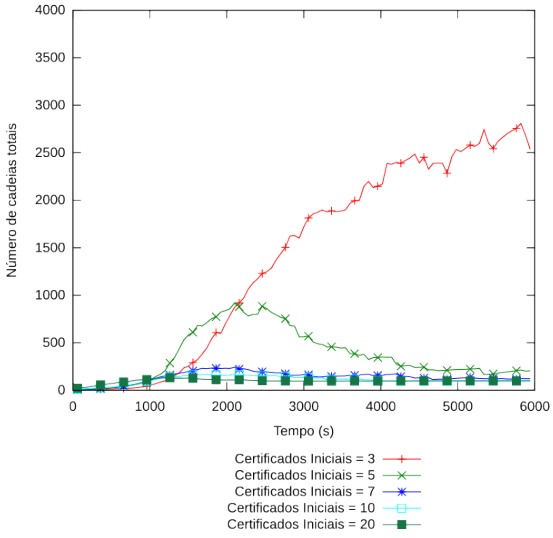



(c) Número de cadeias Abertas

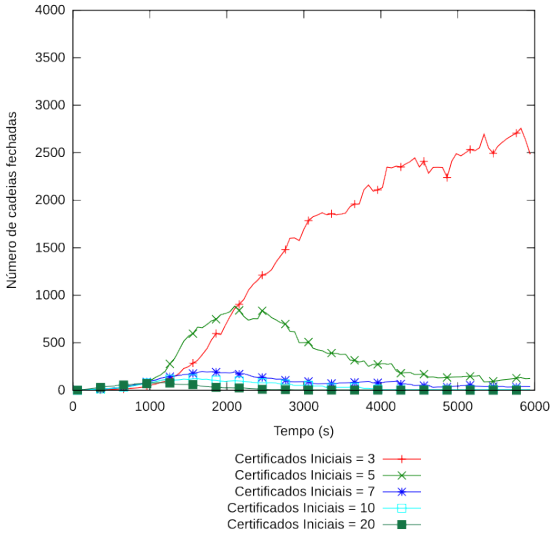



(d) Tamanho médio das cadeias

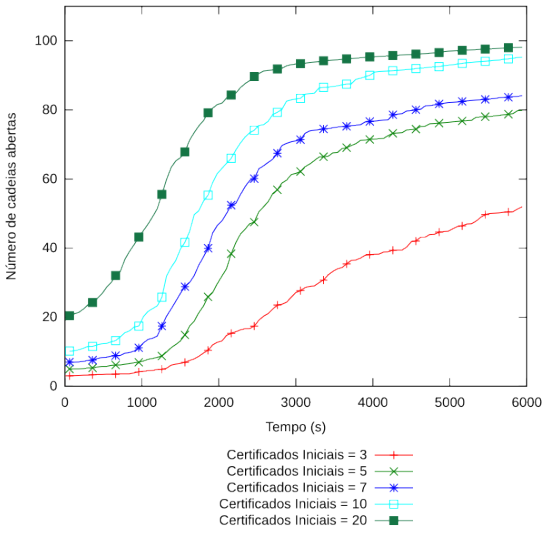
Figura B.62: Resultados para 75 nodos, $m = 20\%$ e $N_a = 25\%$



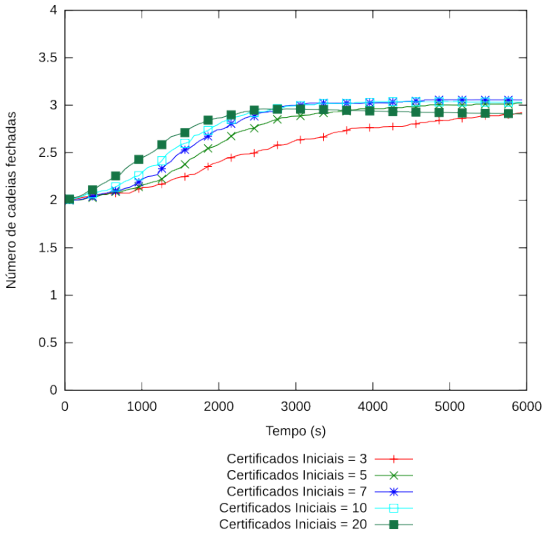

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

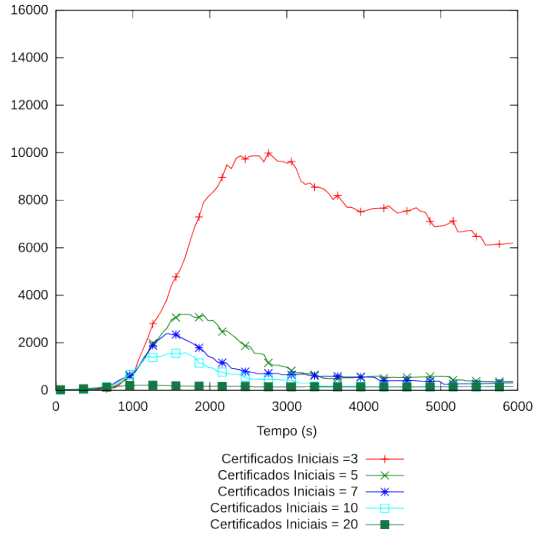



(c) Número de cadeias Abertas

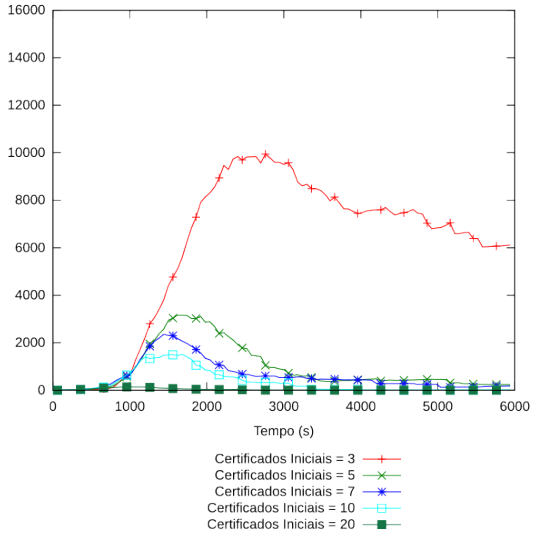



(d) Tamanho médio das cadeias

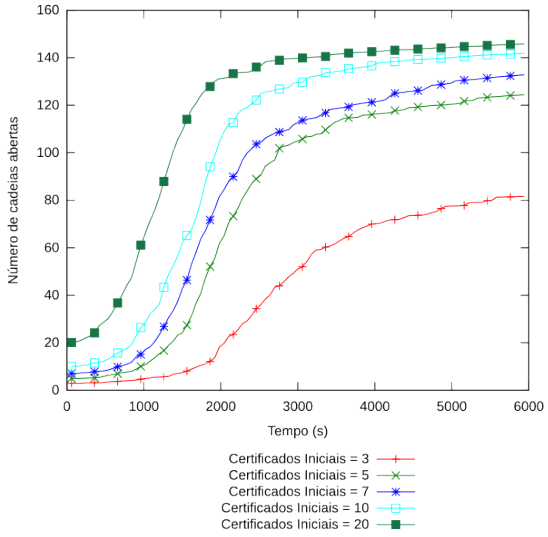
Figura B.63: Resultados para 100 nodos, $m = 20\%$ e $N_a = 25\%$



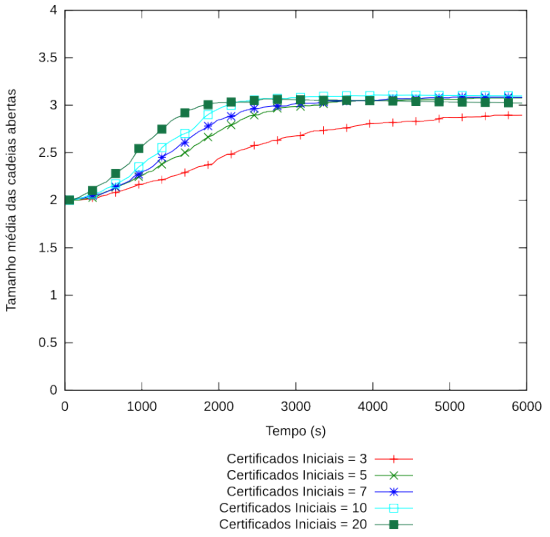

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



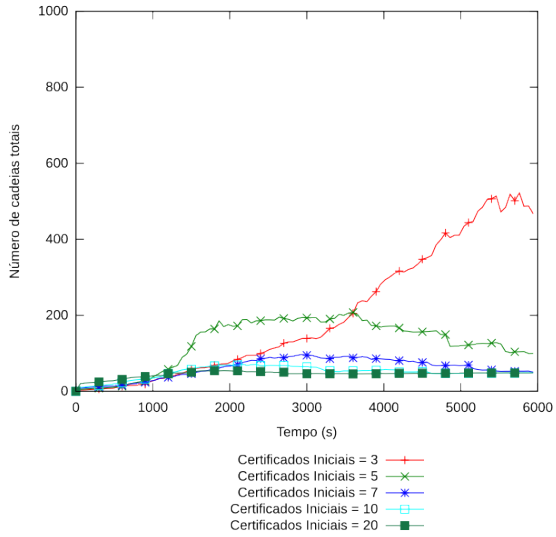

(c) Número de cadeias Abertas



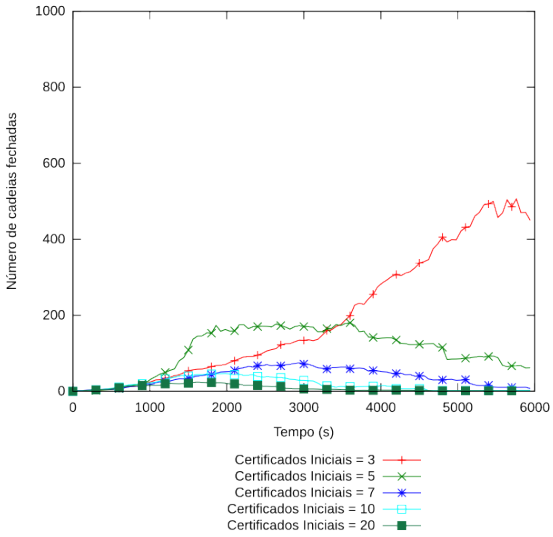

(d) Tamanho médio das cadeias

Figura B.64: Resultados para 150 nodos, $m = 20\%$ e $N_a = 25\%$

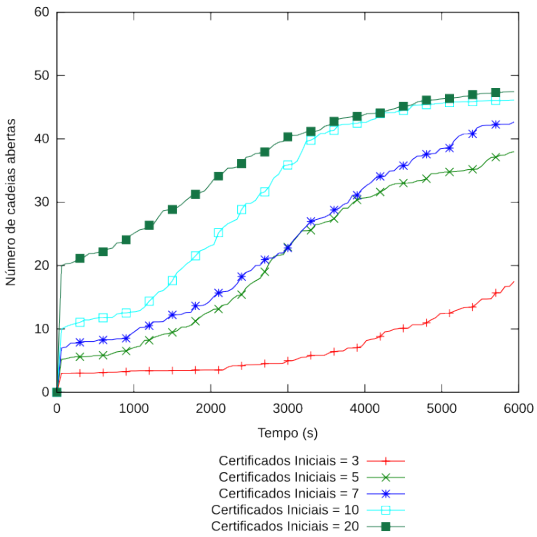
### B.6.6 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 50\%$



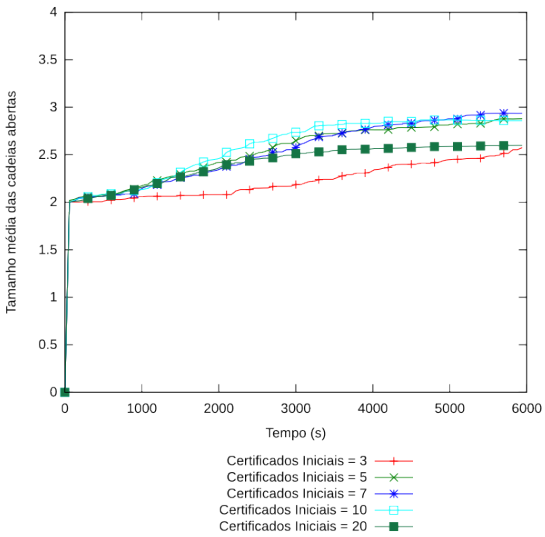

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

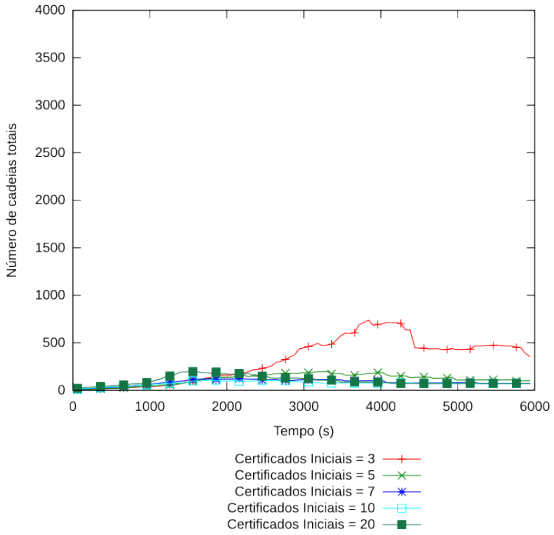



(c) Número de cadeias Abertas

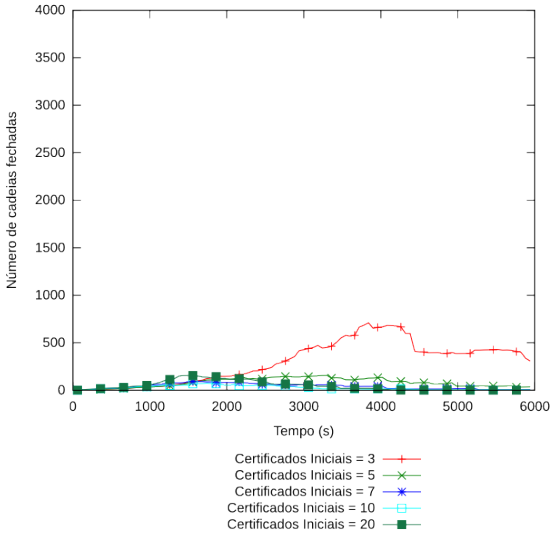



(d) Tamanho médio das cadeias

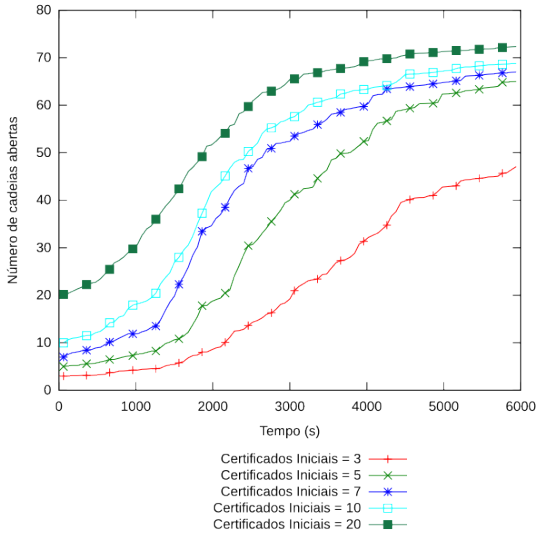
Figura B.65: Resultados para 50 nodos, $m = 20\%$ e $N_a = 50\%$



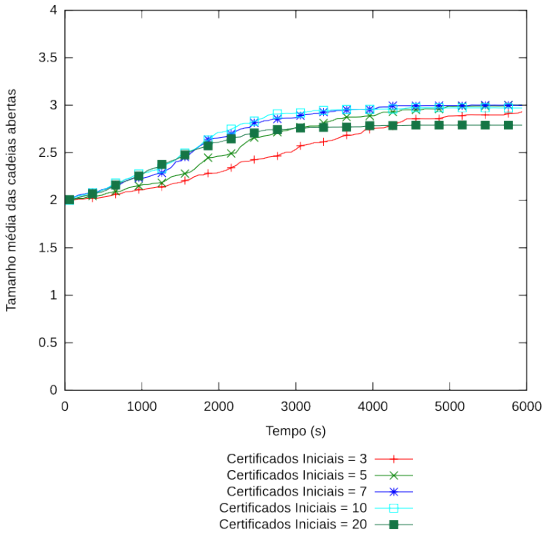

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

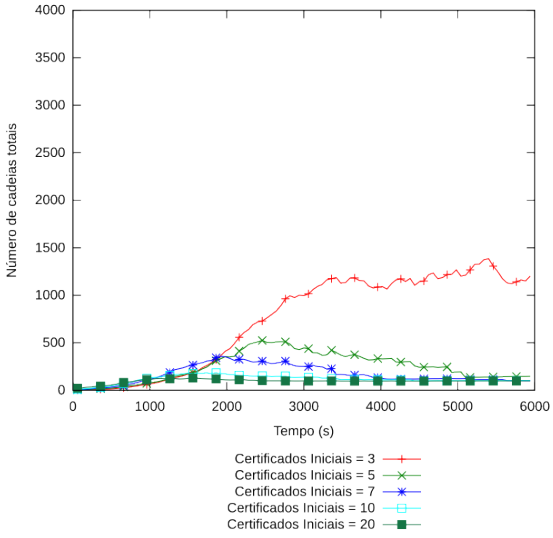



(c) Número de cadeias Abertas

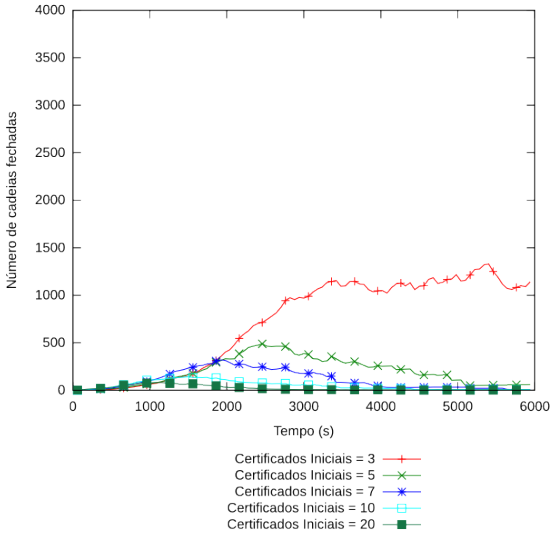



(d) Tamanho médio das cadeias

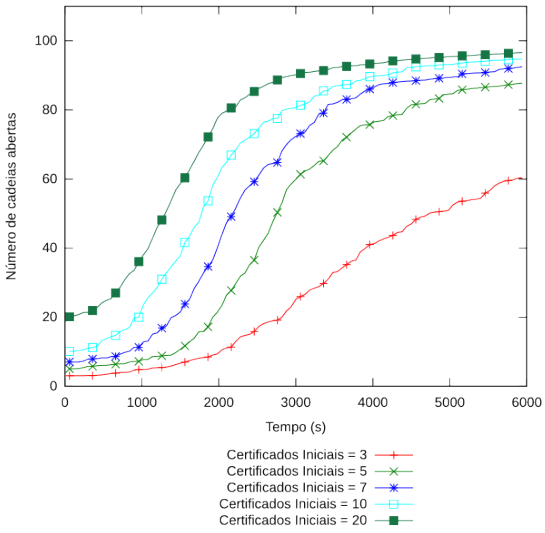
Figura B.66: Resultados para 75 nodos, $m = 20\%$ e $N_a = 50\%$



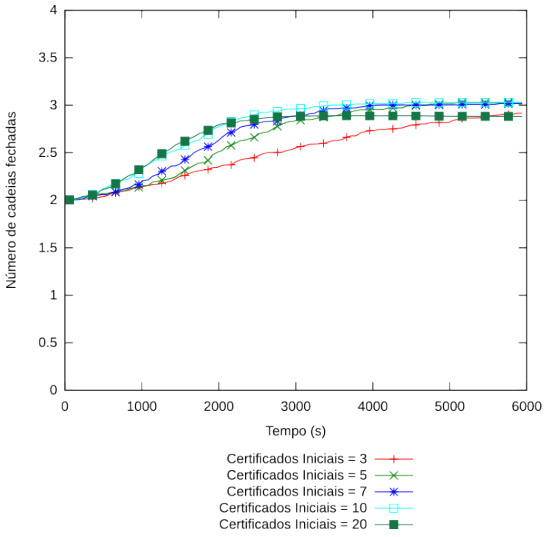

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

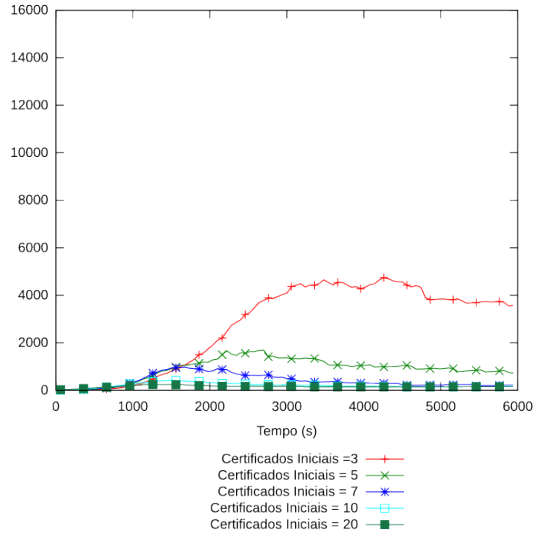



(c) Número de cadeias Abertas

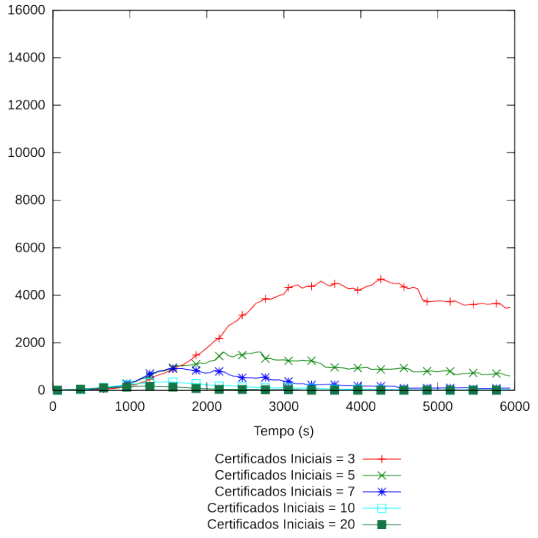



(d) Tamanho médio das cadeias

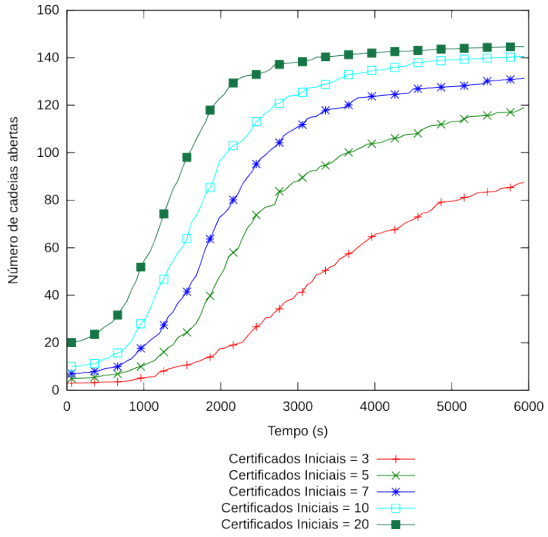
Figura B.67: Resultados para 100 nodos, $m = 20\%$ e $N_a = 50\%$



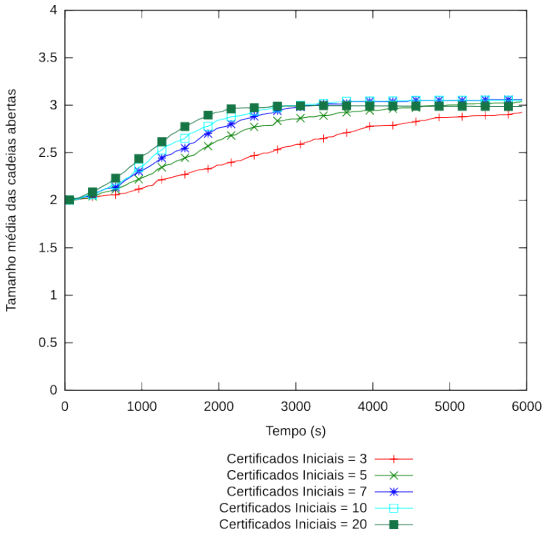

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



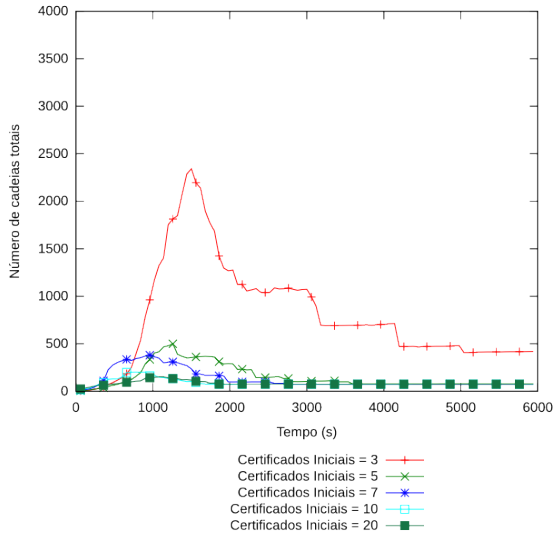

(c) Número de cadeias Abertas



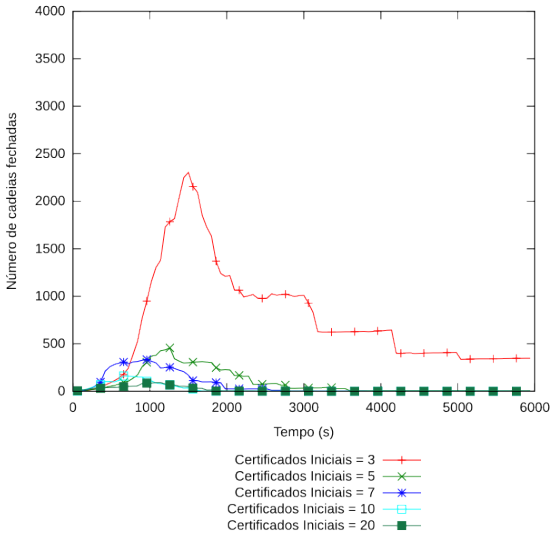

(d) Tamanho médio das cadeias

Figura B.68: Resultados para 150 nodos, $m = 20\%$ e $N_a = 50\%$

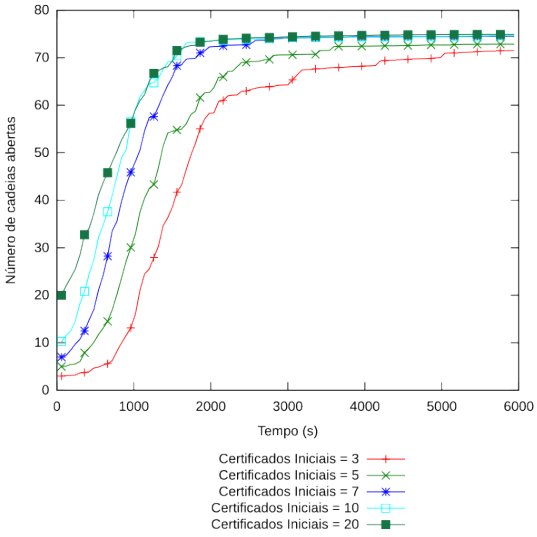
### B.6.7 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 10\%$



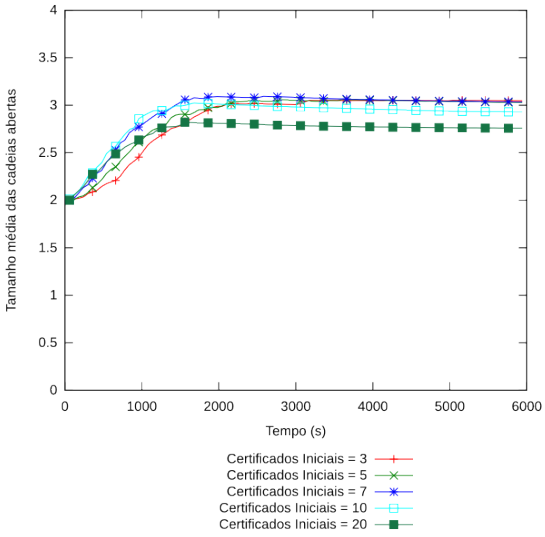

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

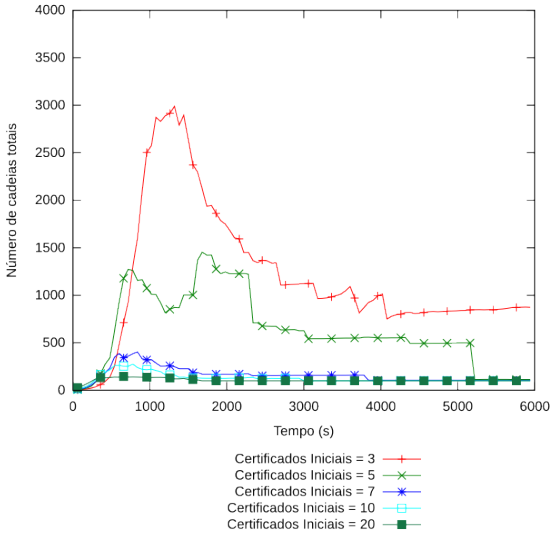



(c) Número de cadeias Abertas

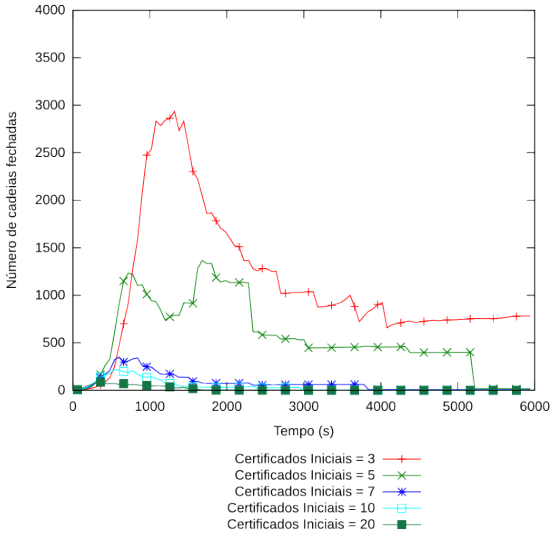



(d) Tamanho médio das cadeias

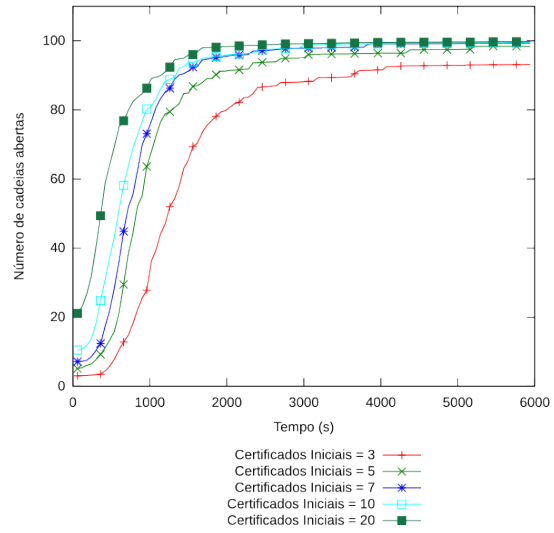
Figura B.69: Resultados para 75 nodos, $m = 50\%$ e $N_a = 10\%$



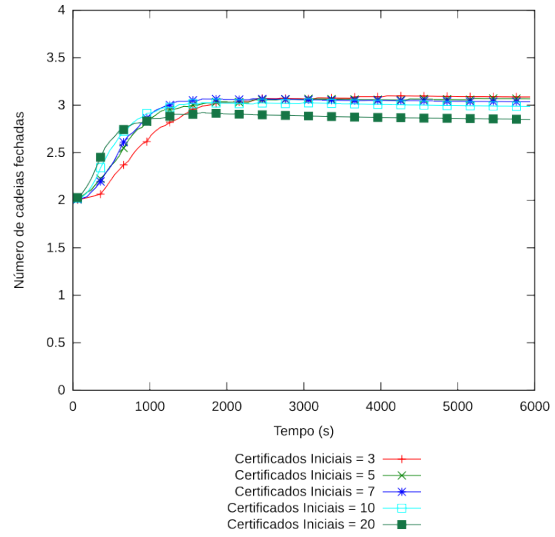

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



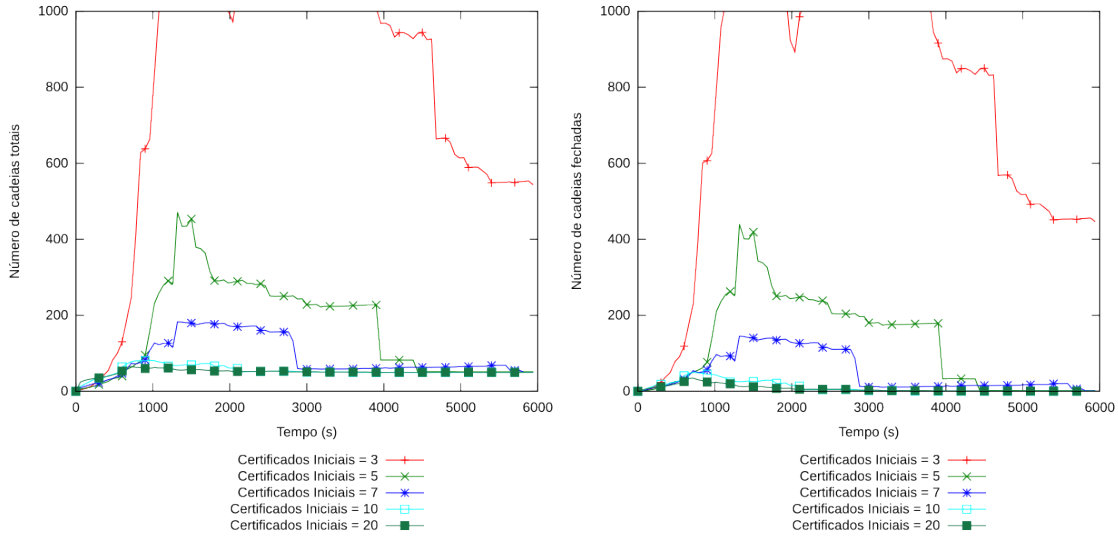

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.70: Resultados para 100 nodos, $m = 50\%$ e $N_a = 10\%$

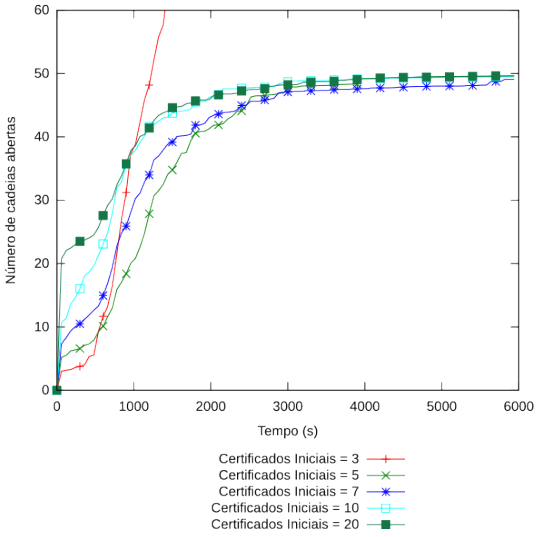
### B.6.8 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 25\%$



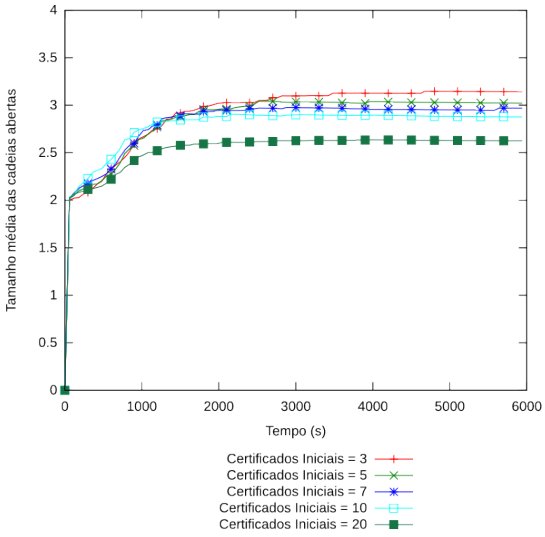

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

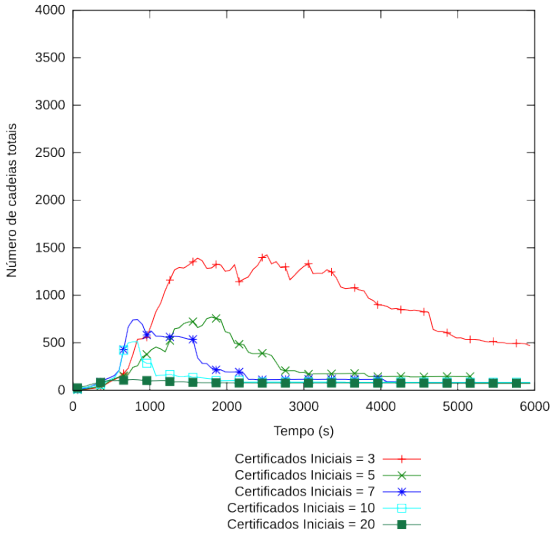



(c) Número de cadeias Abertas

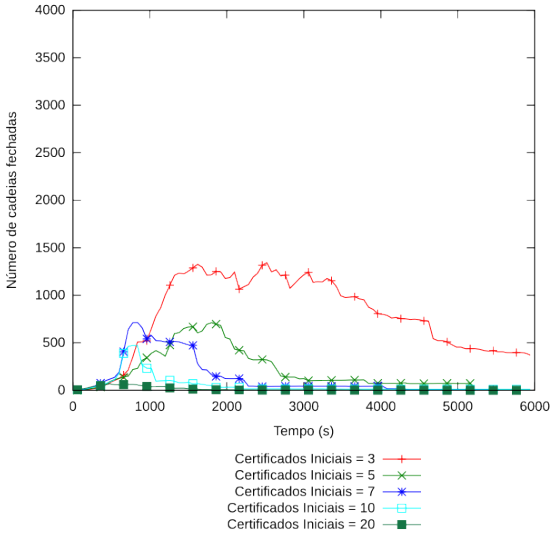



(d) Tamanho médio das cadeias

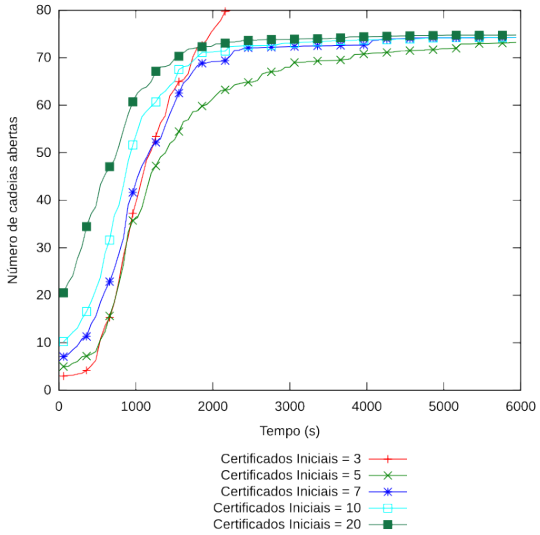
Figura B.71: Resultados para 50 nodos, $m = 50\%$ e $N_a = 25\%$



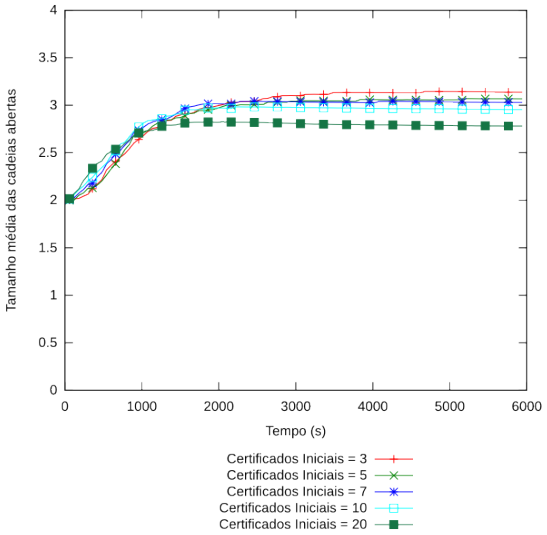

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

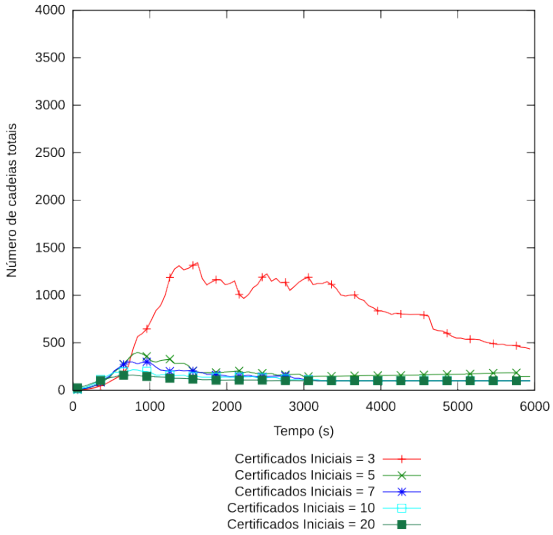



(c) Número de cadeias Abertas

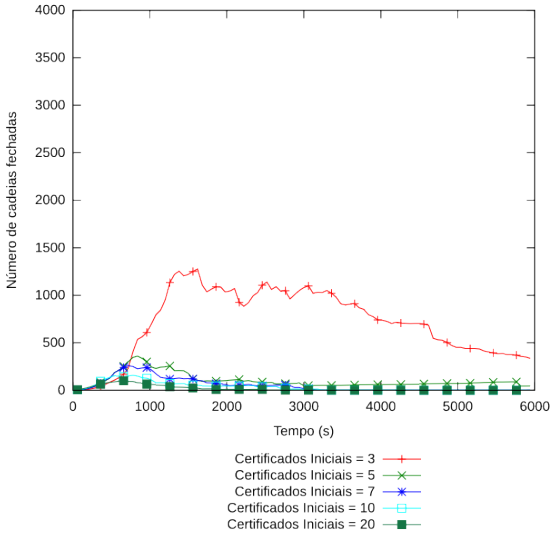



(d) Tamanho médio das cadeias

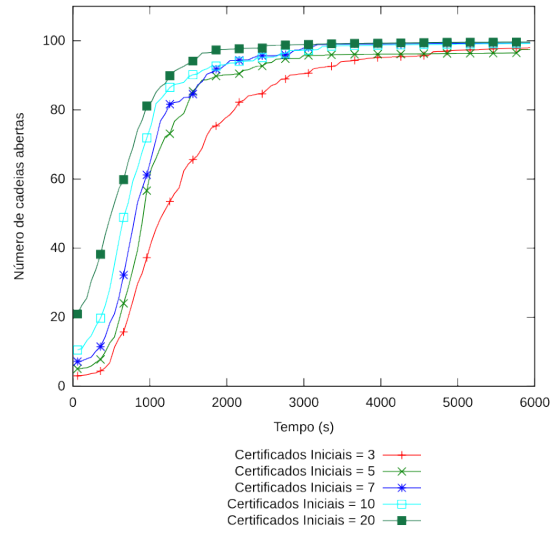
Figura B.72: Resultados para 75 nodos, $m = 50\%$ e $N_a = 25\%$



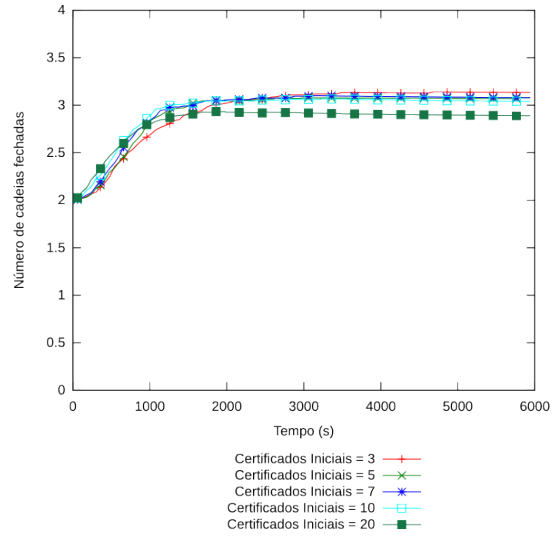

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

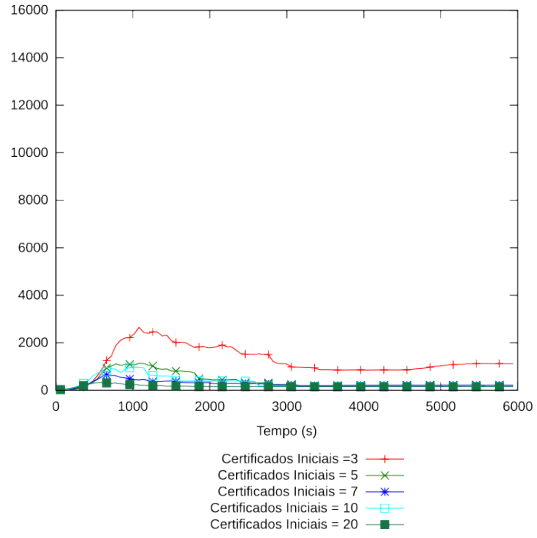



(c) Número de cadeias Abertas

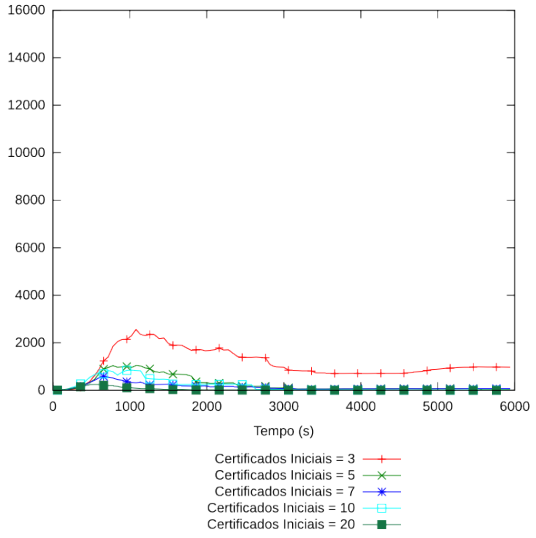



(d) Tamanho médio das cadeias

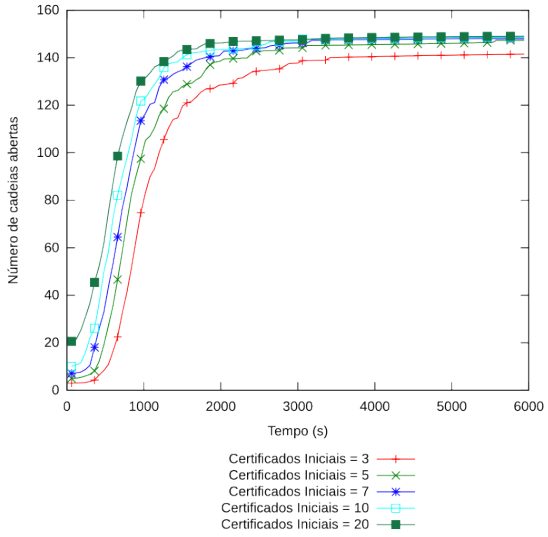
Figura B.73: Resultados para 100 nodos, $m = 50\%$ e $N_a = 25\%$



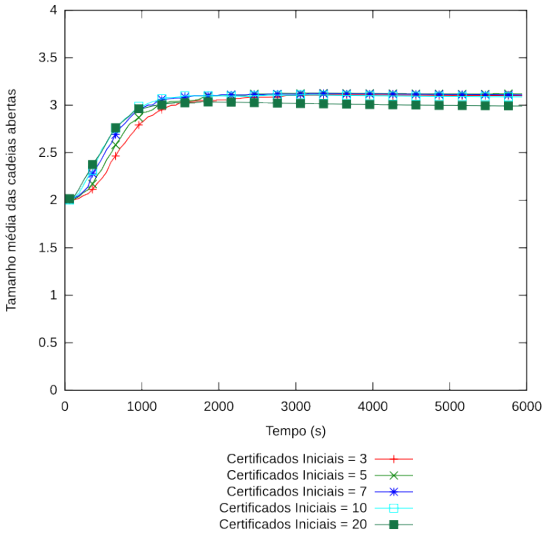

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



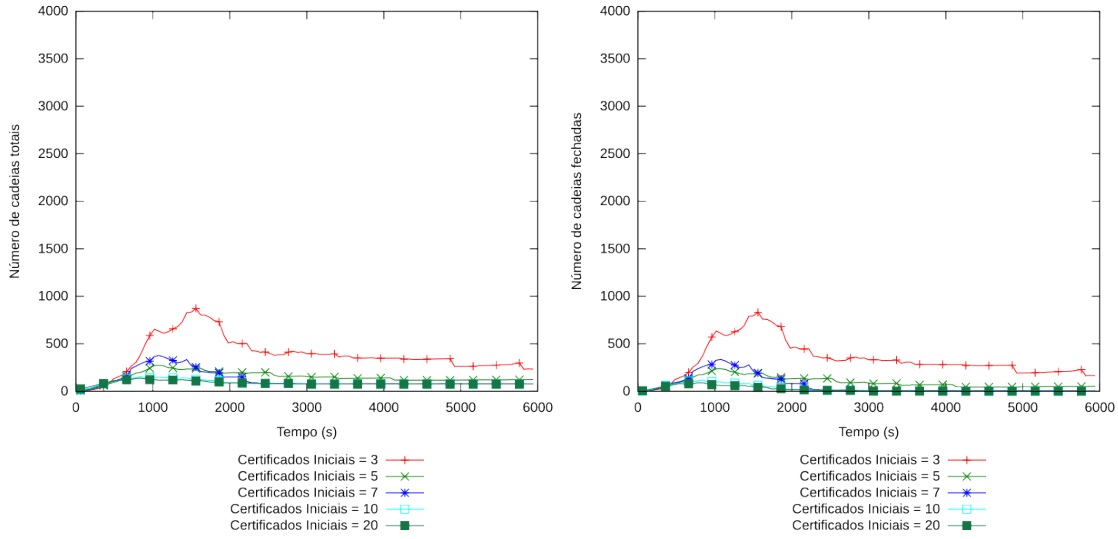

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.74: Resultados para 150 nodos, $m = 50\%$ e $N_a = 25\%$

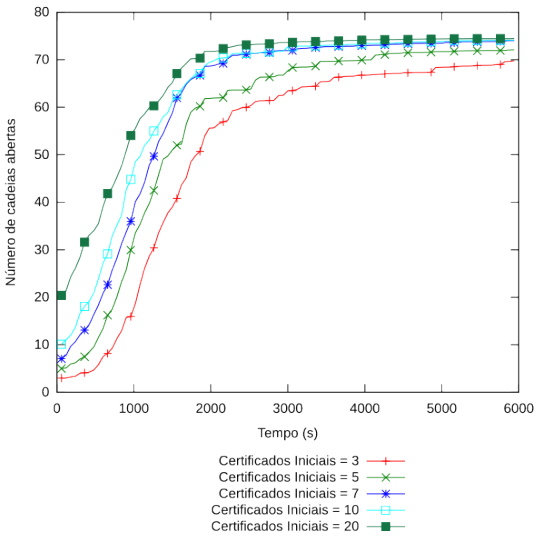
### B.6.9 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 50\%$



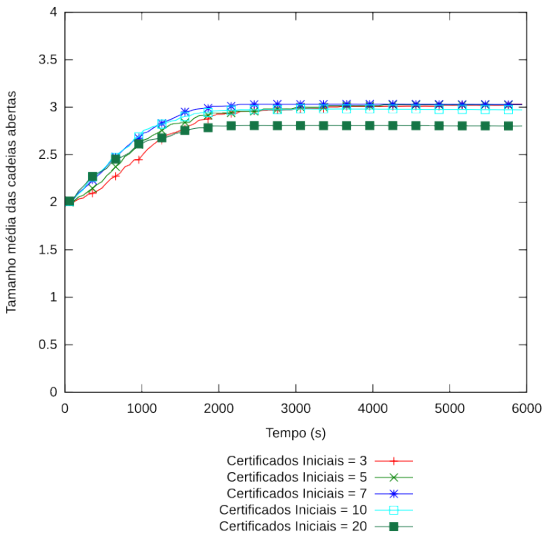

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

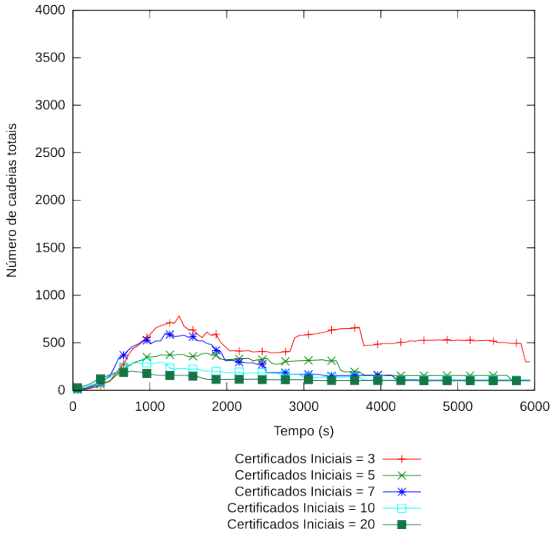



(c) Número de cadeias Abertas

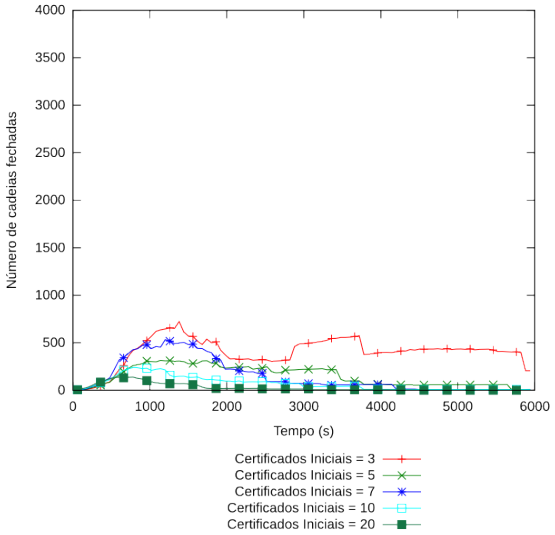



(d) Tamanho médio das cadeias

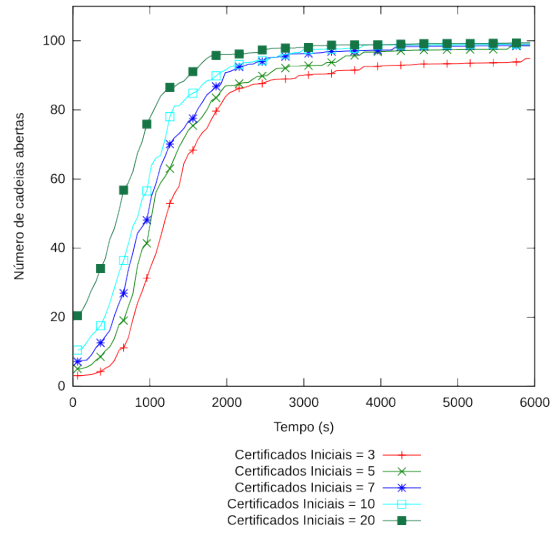
Figura B.75: Resultados para 75 nodos, $m = 50\%$ e $N_a = 50\%$



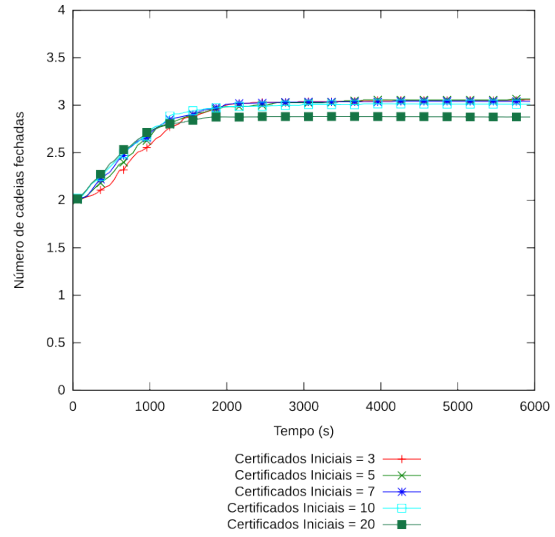

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

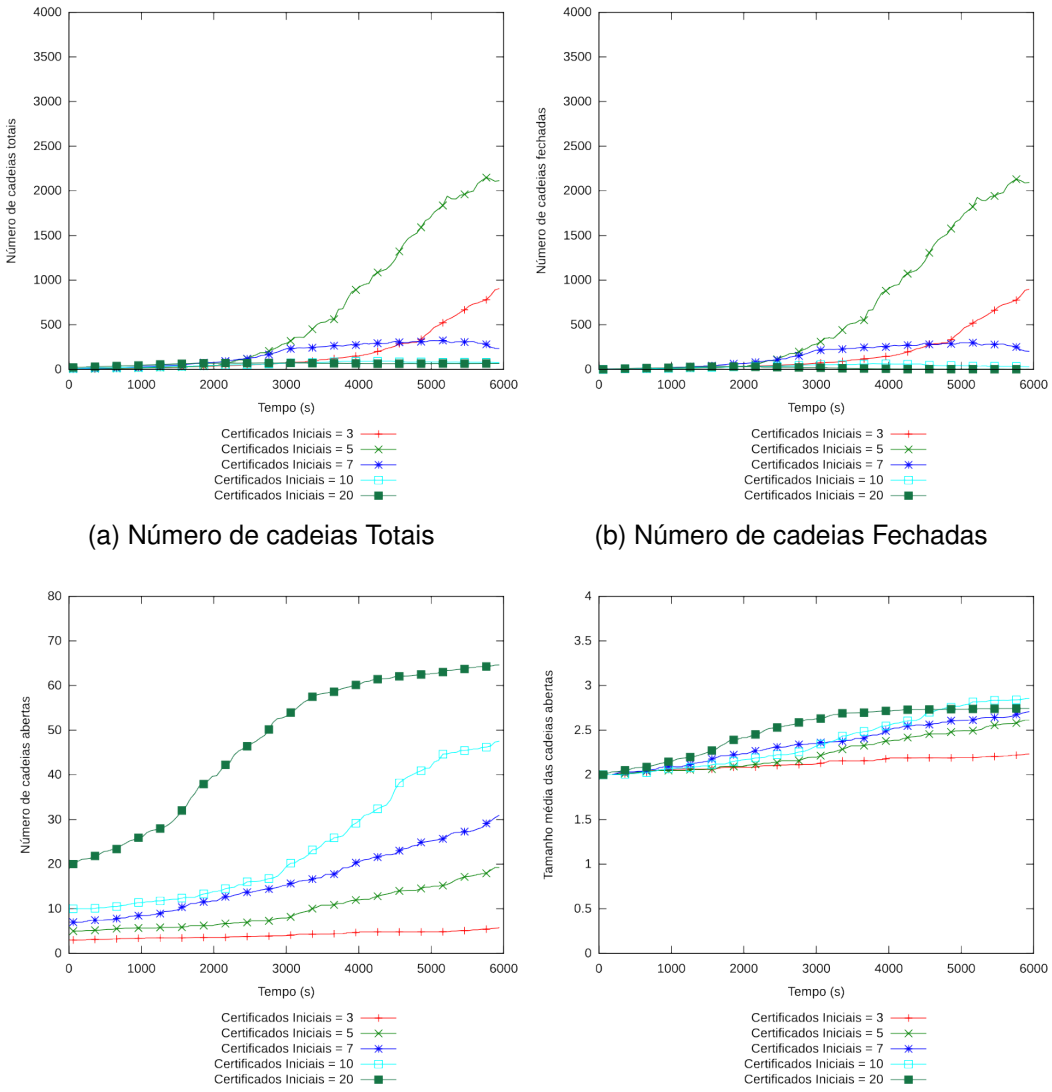



(d) Tamanho médio das cadeias

Figura B.76: Resultados para 100 nodos, $m = 50\%$ e $N_a = 50\%$

## B.7 Ataque de Falsificaçao - Ataque em grupo

### B.7.1 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 10\%$



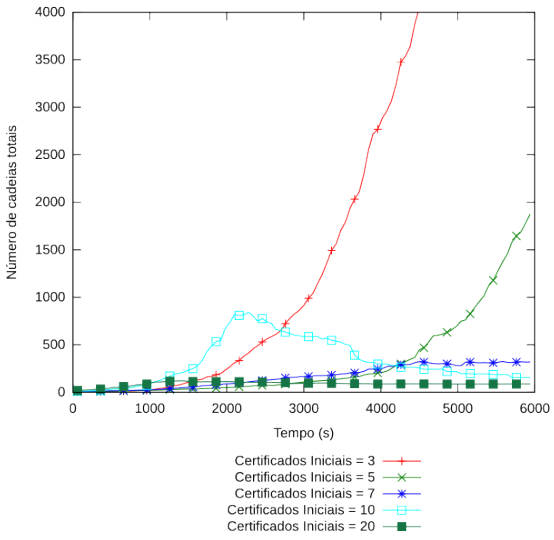

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

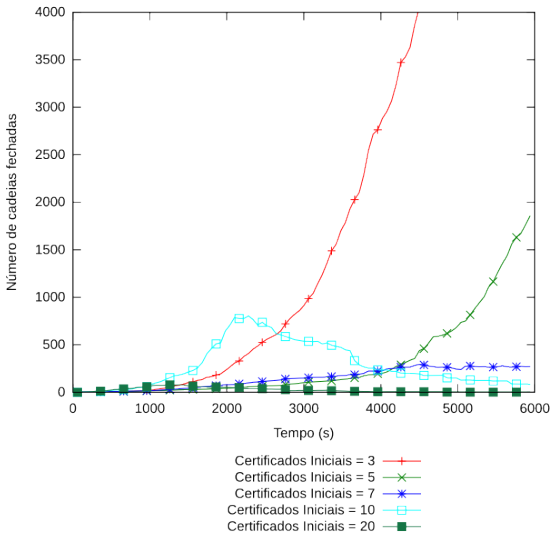
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

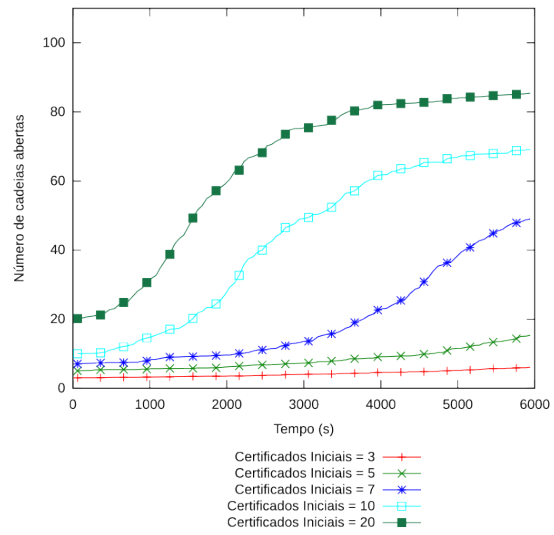
Figura B.77: Resultados para 75 nodos, $m = 10\%$ e $N_a = 10\%$ com ataque em grupo



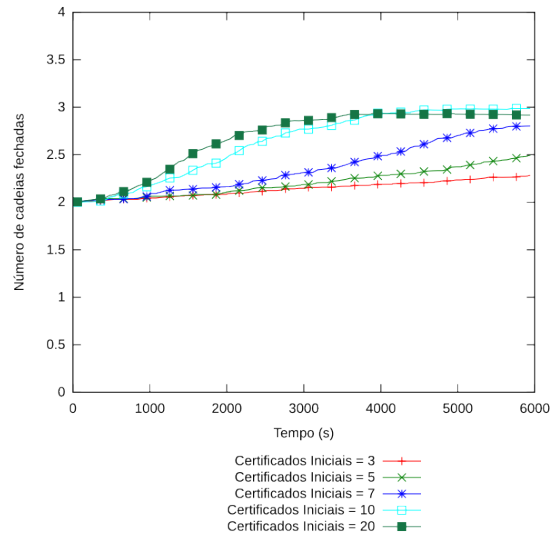

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



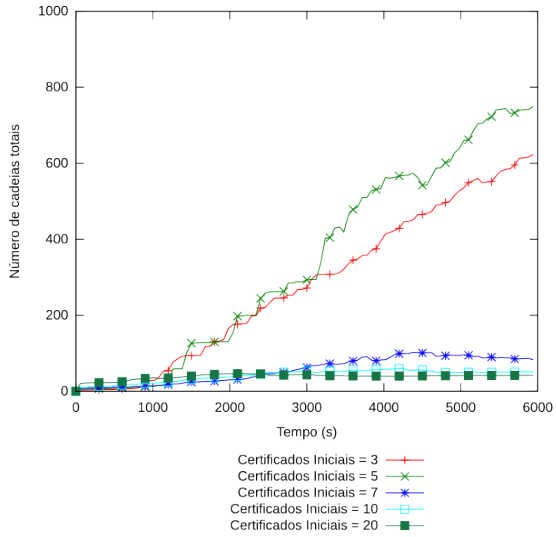

(c) Número de cadeias Abertas



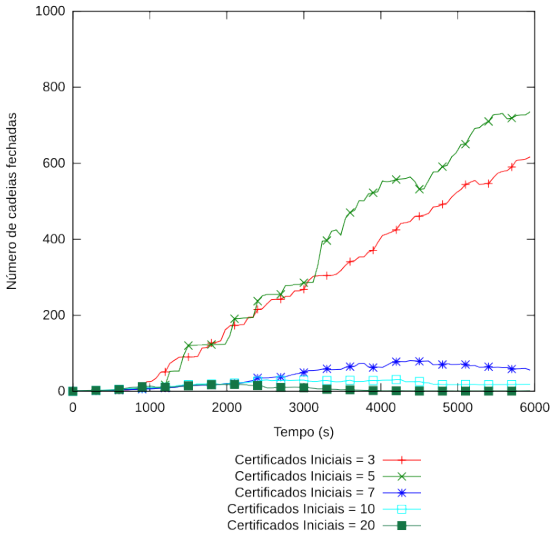

(d) Tamanho médio das cadeias

Figura B.78: Resultados para 100 nodos, $m = 10\%$ e $N_a = 10\%$ com ataque em grupo

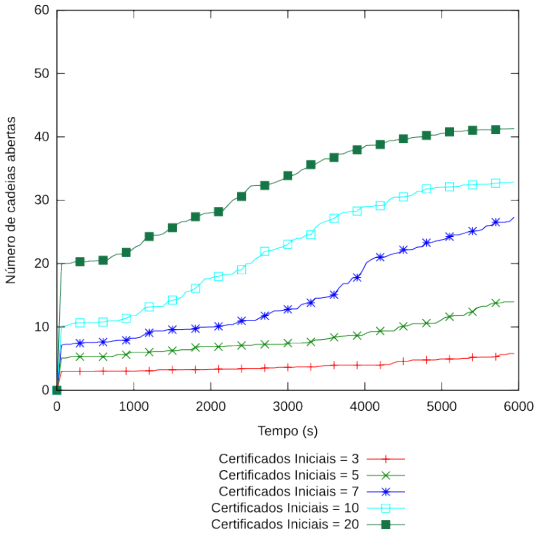
### B.7.2 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 25\%$



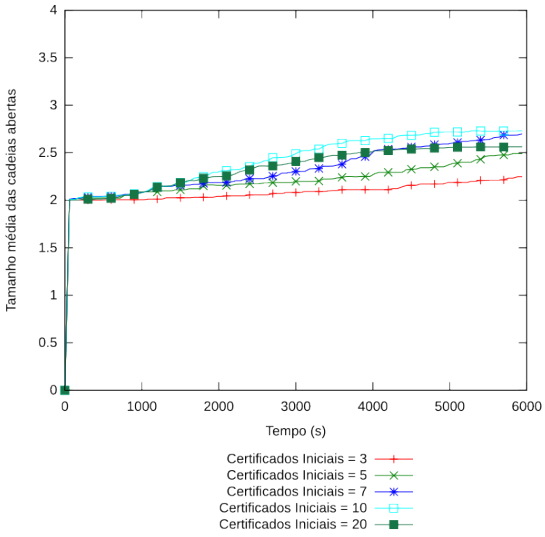

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

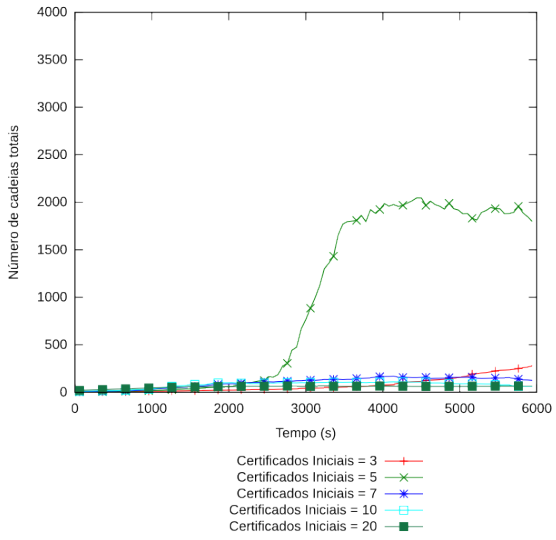



(c) Número de cadeias Abertas

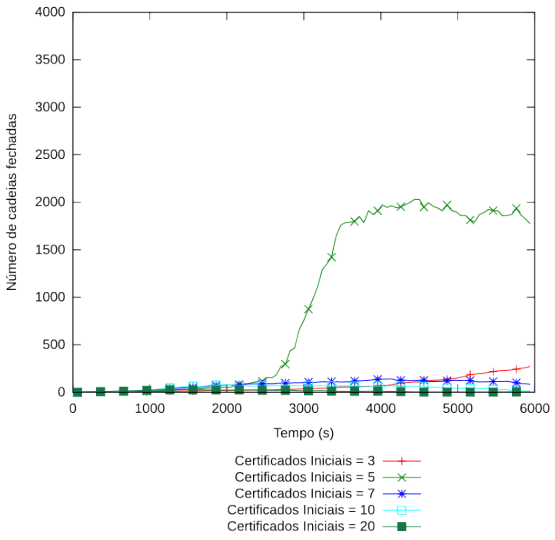



(d) Tamanho médio das cadeias

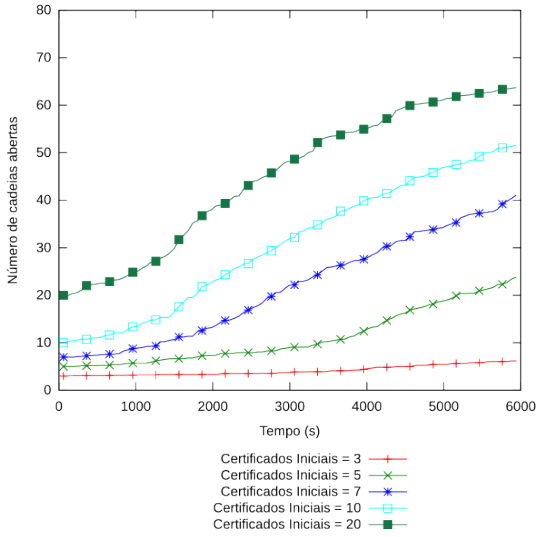
Figura B.79: Resultados para 50 nodos, $m = 10\%$ e $N_a = 25\%$ com ataque em grupo



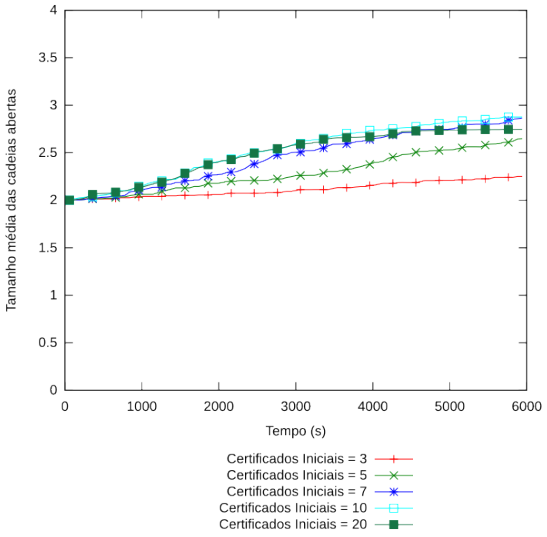

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

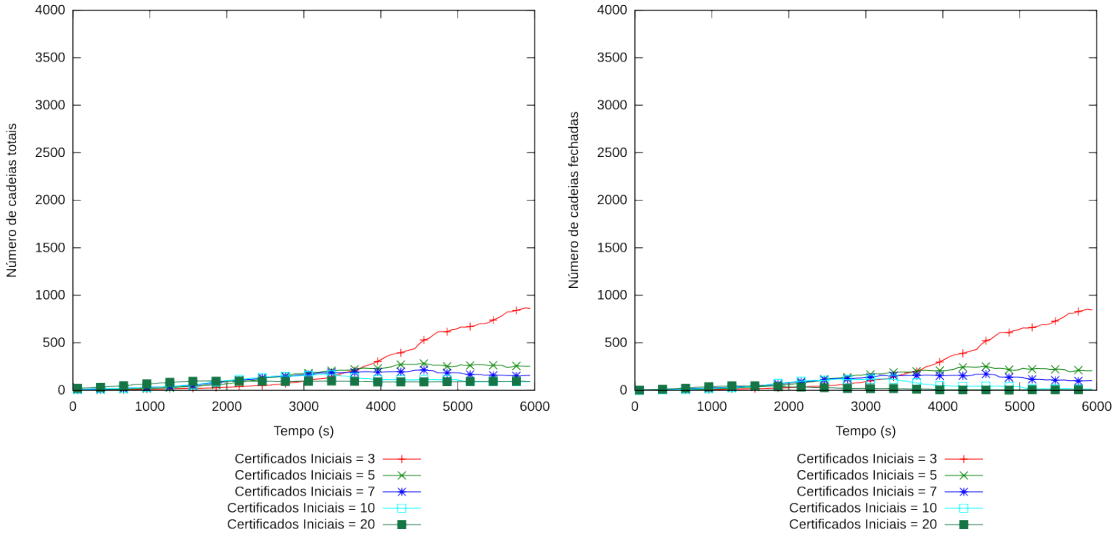



(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

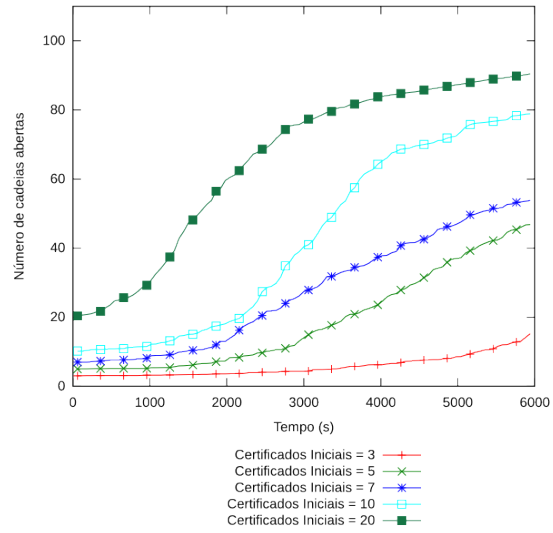
Figura B.80: Resultados para 75 nodos, $m = 10\%$ e $N_a = 25\%$ com ataque em gupo



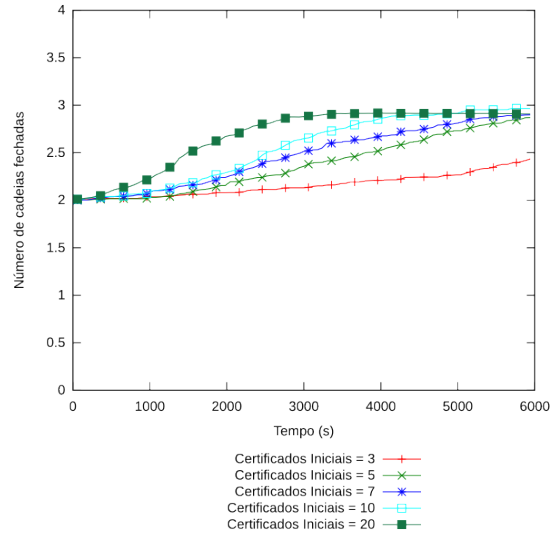

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

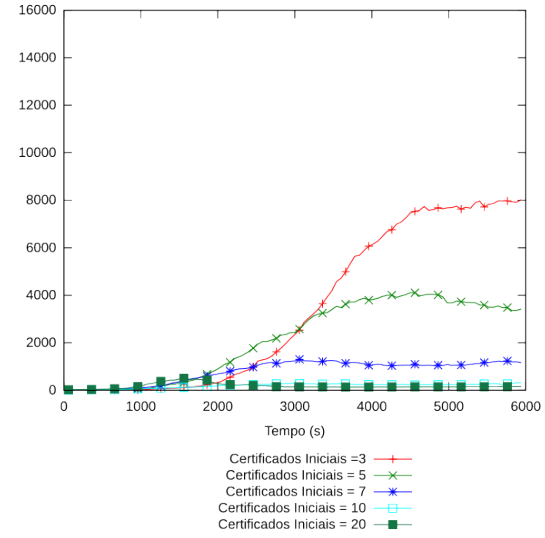



(c) Número de cadeias Abertas

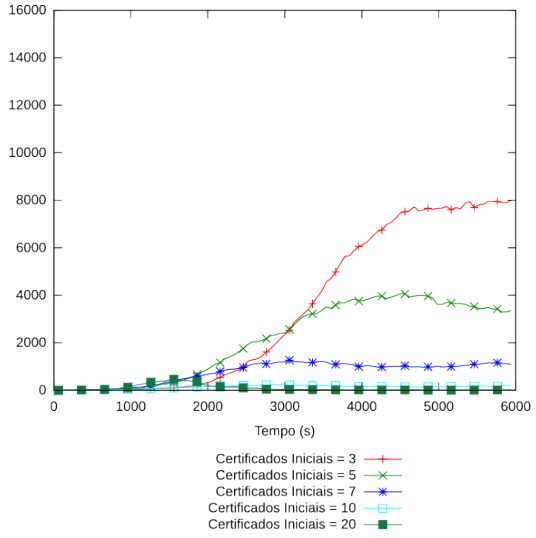



(d) Tamanho médio das cadeias

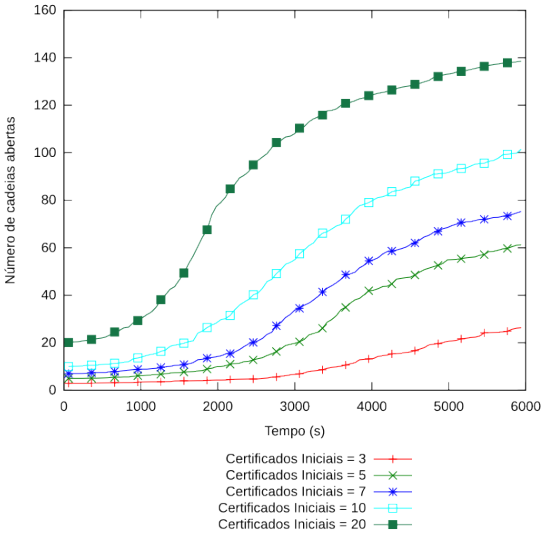
Figura B.81: Resultados para 100 nodos, $m = 10\%$ e $N_a = 25\%$ com ataque em grupo



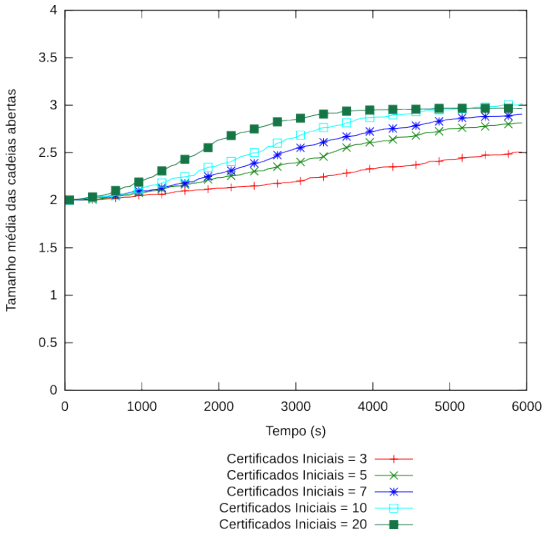

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



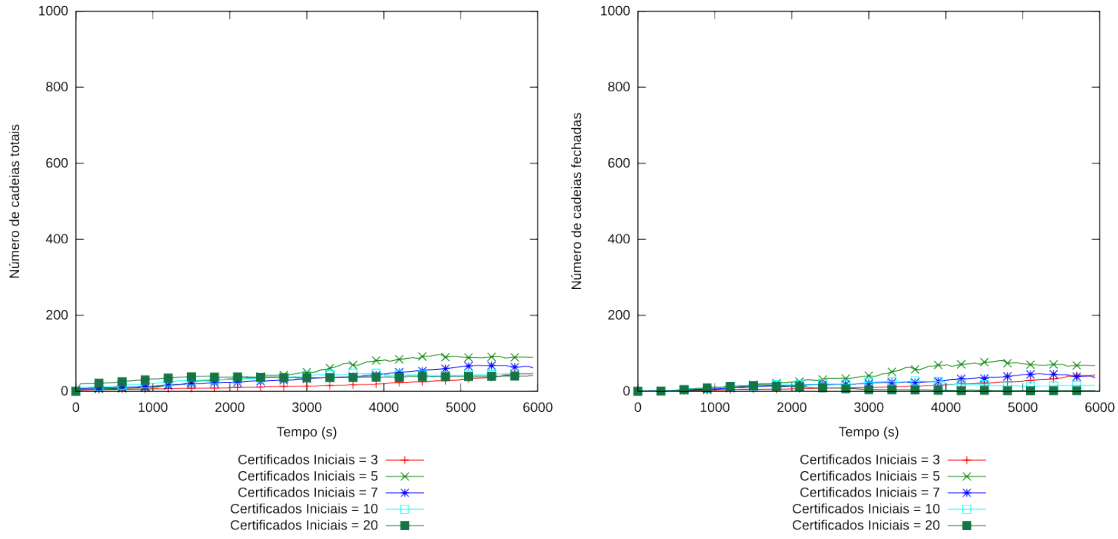

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.82: Resultados para 150 nodos, $m = 10\%$ e $N_a = 25\%$ com ataque em grupo

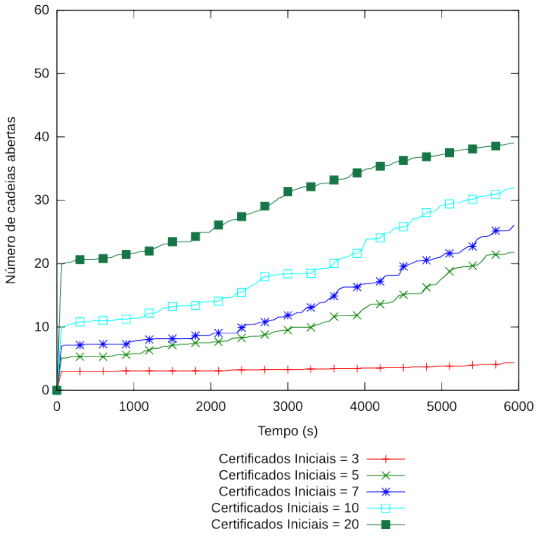
### B.7.3 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 50\%$



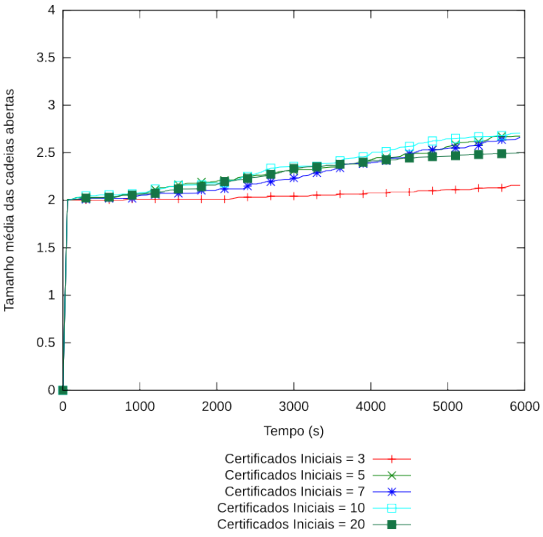

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

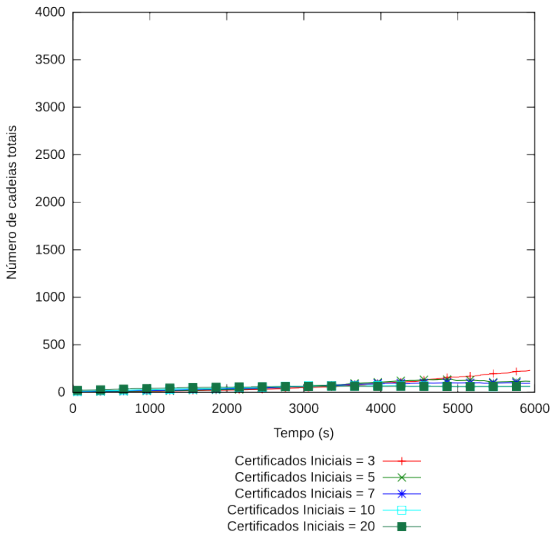



(c) Número de cadeias Abertas

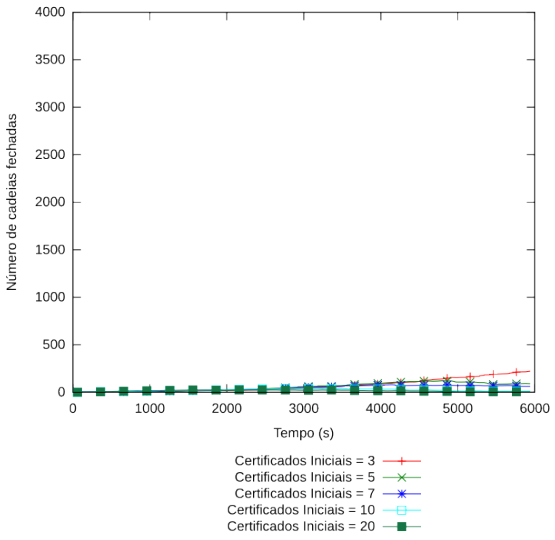



(d) Tamanho médio das cadeias

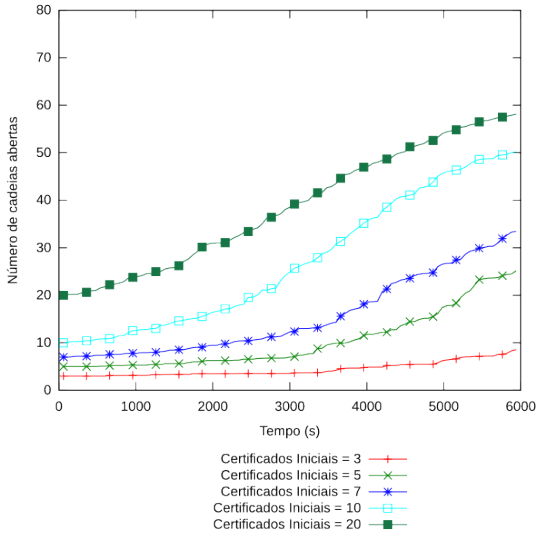
Figura B.83: Resultados para 50 nodos, $m = 10\%$ e $N_a = 50\%$ com ataque em grupo



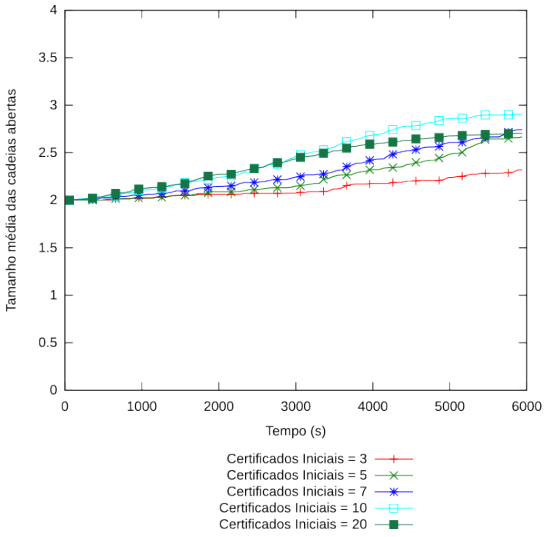

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

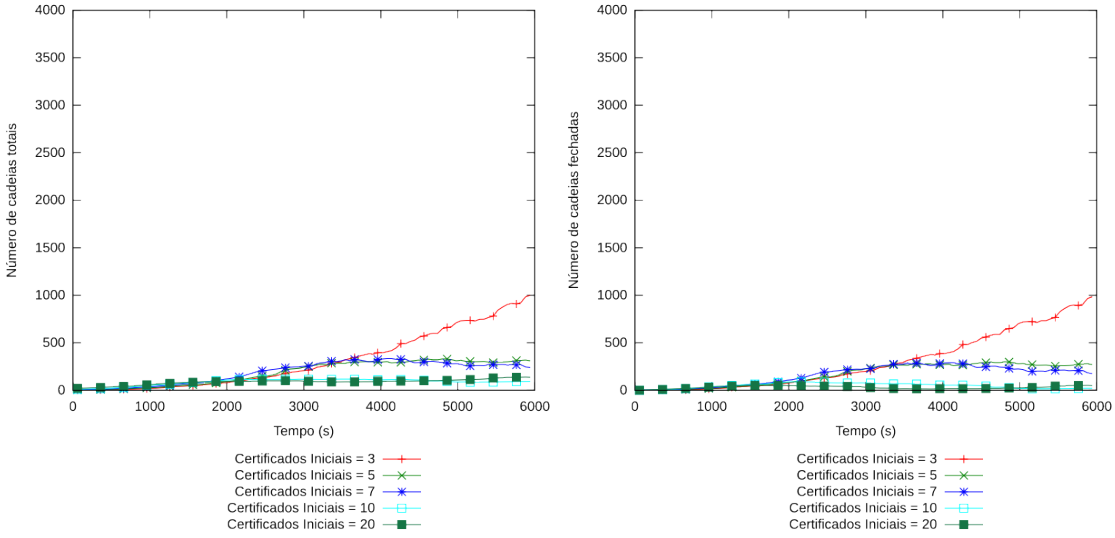



(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

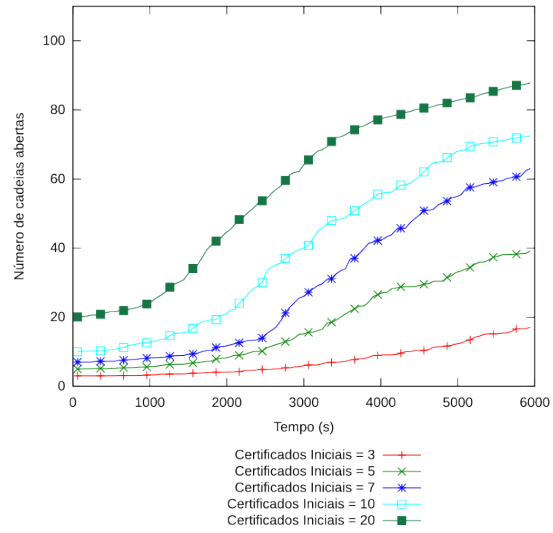
Figura B.84: Resultados para 75 nodos, $m = 10\%$ e $N_a = 50\%$ com ataque em grupo



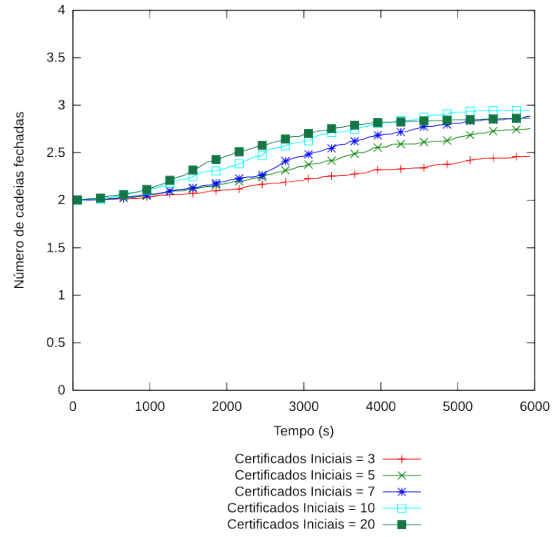

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

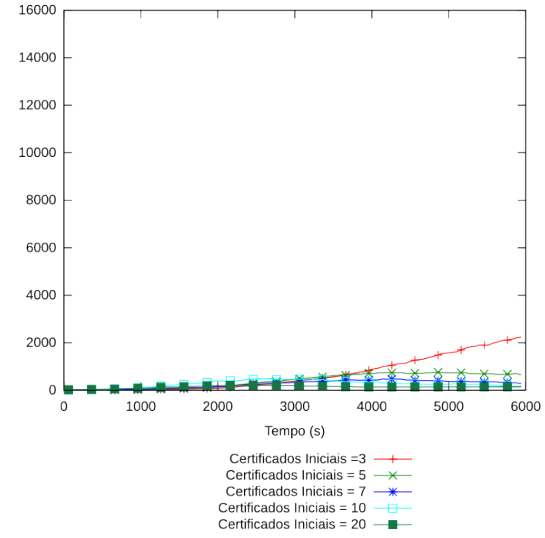



(c) Número de cadeias Abertas

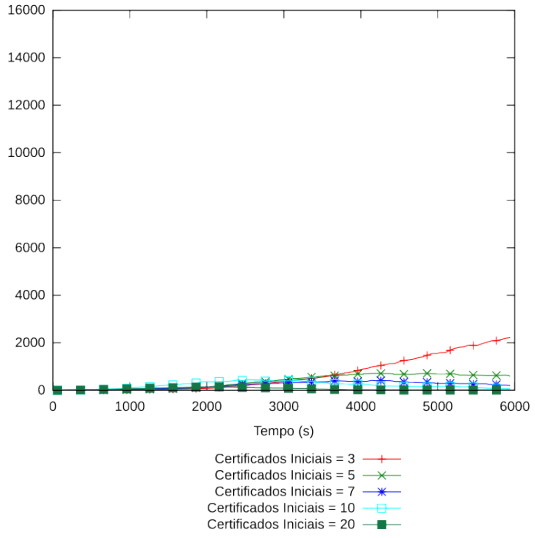



(d) Tamanho médio das cadeias

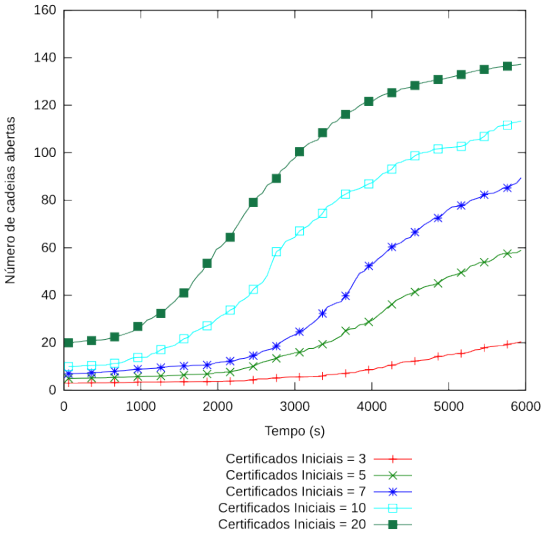
Figura B.85: Resultados para 100 nodos, $m = 10\%$ e $N_a = 50\%$ com ataque em grupo



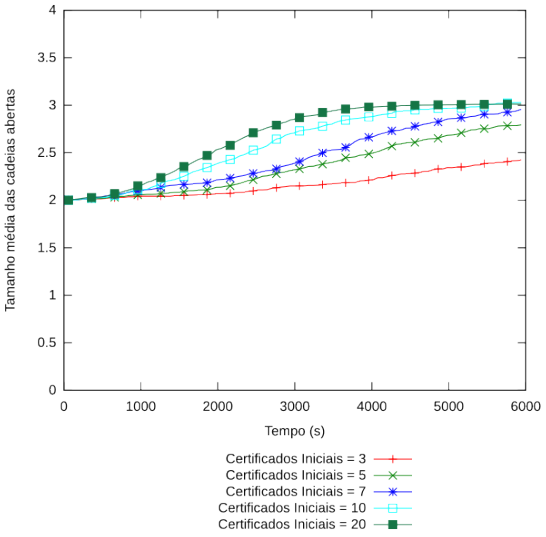

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



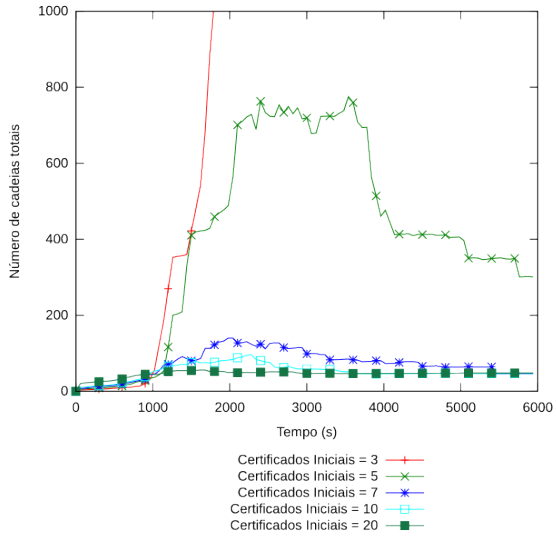

(c) Número de cadeias Abertas



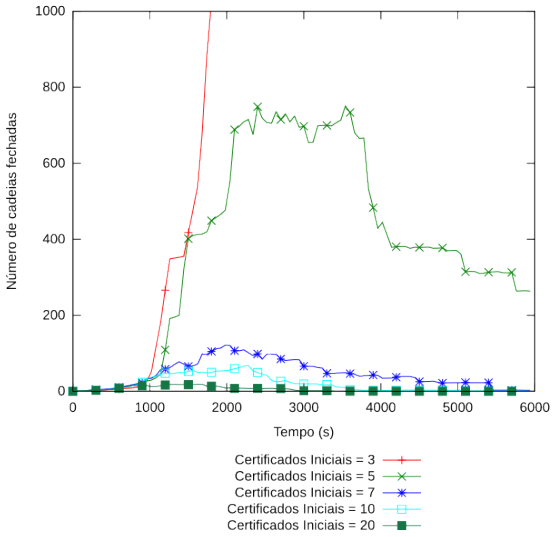

(d) Tamanho médio das cadeias

Figura B.86: Resultados para 150 nodos, $m = 10\%$ e $N_a = 50\%$ com ataque em grupo

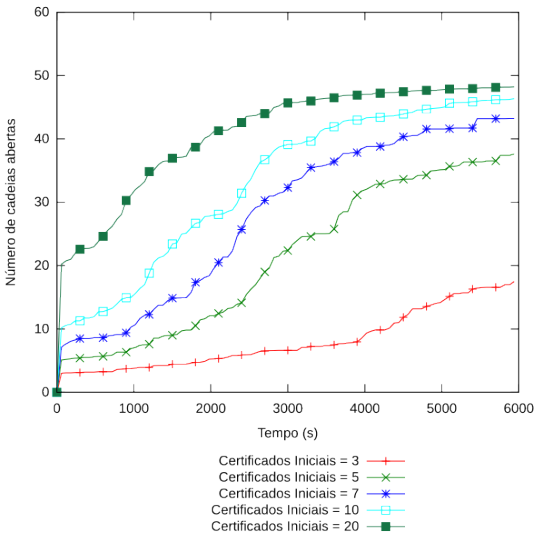
### B.7.4 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 10\%$



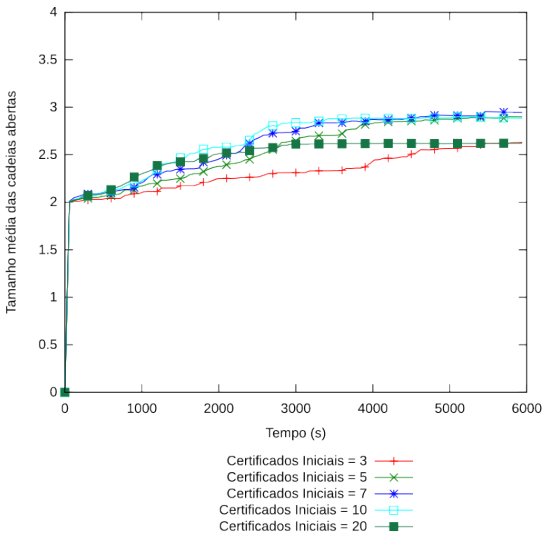

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

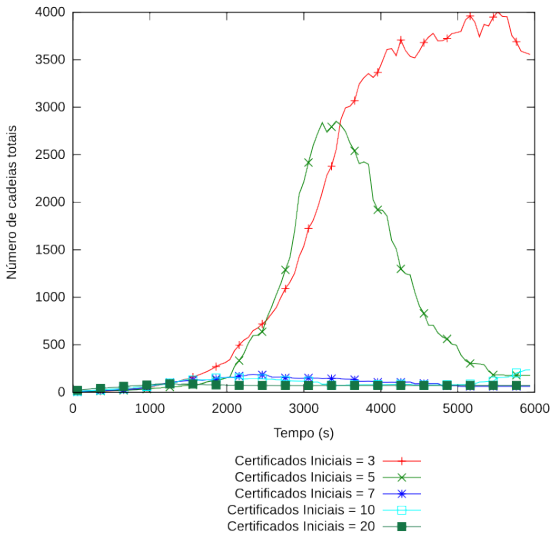



(c) Número de cadeias Abertas

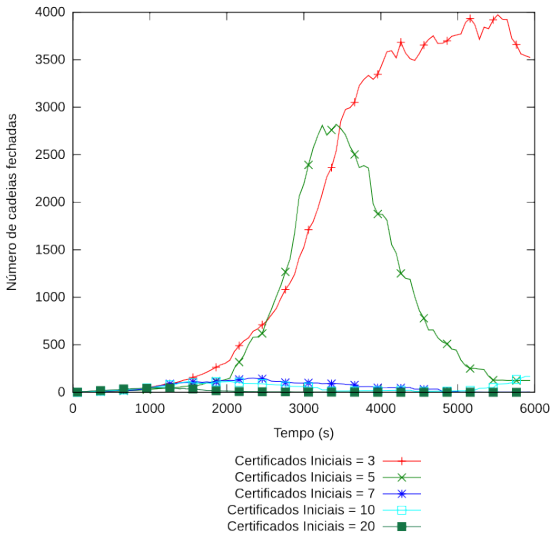



(d) Tamanho médio das cadeias

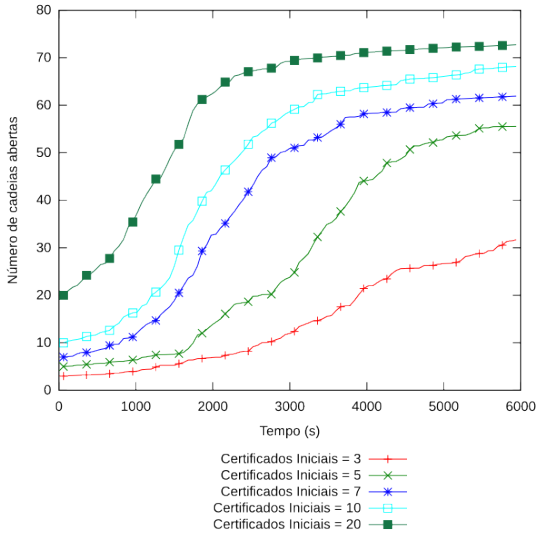
Figura B.87: Resultados para 50 nodos, $m = 20\%$ e $N_a = 10\%$ com ataque em grupo



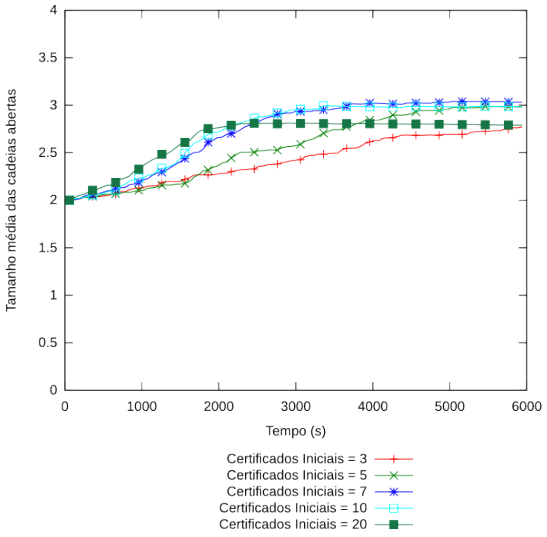

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

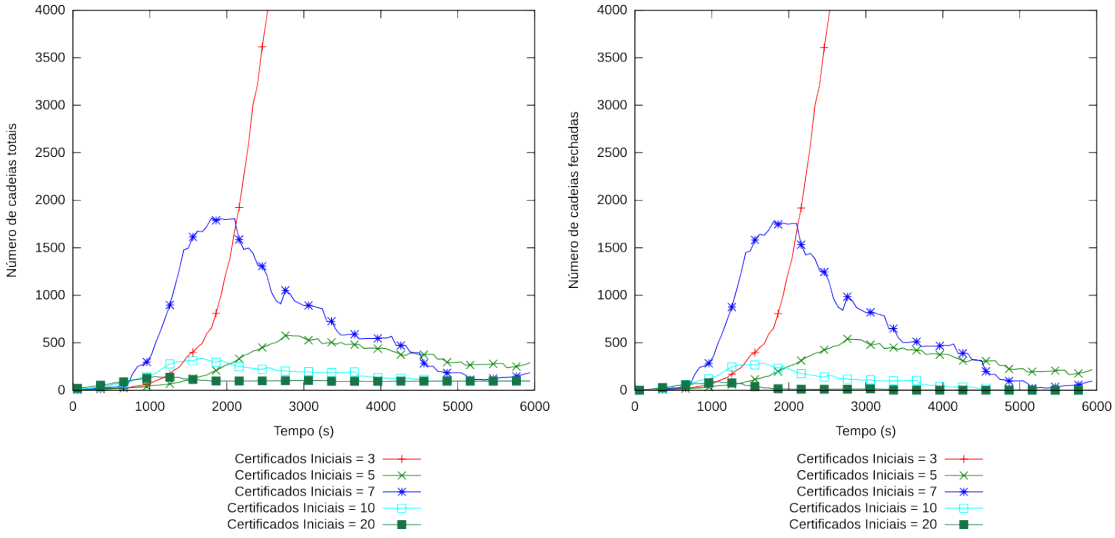



(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

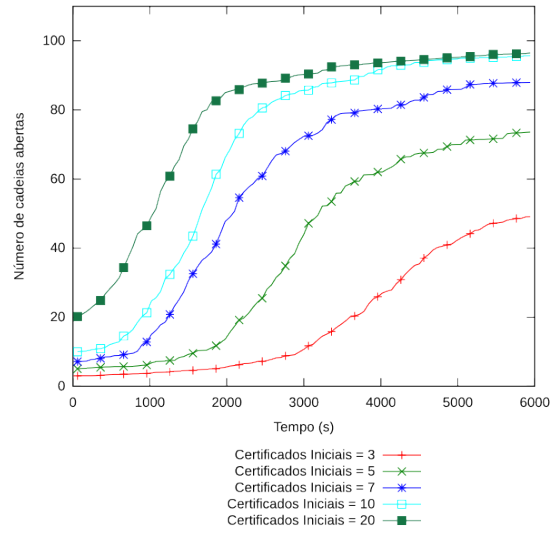
Figura B.88: Resultados para 75 nodos, $m = 20\%$ e $N_a = 10\%$ com ataque em grupo



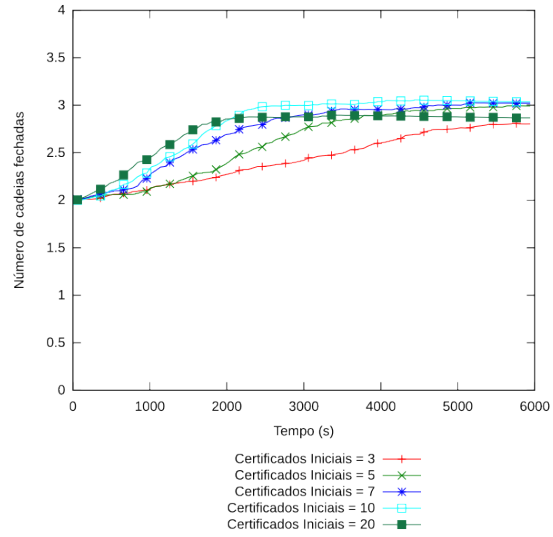

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

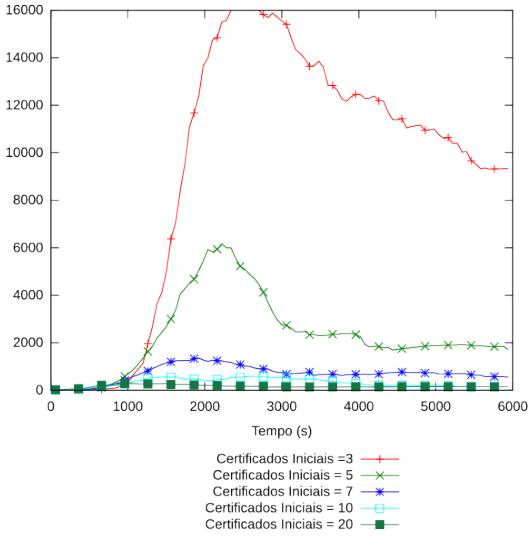



(c) Número de cadeias Abertas

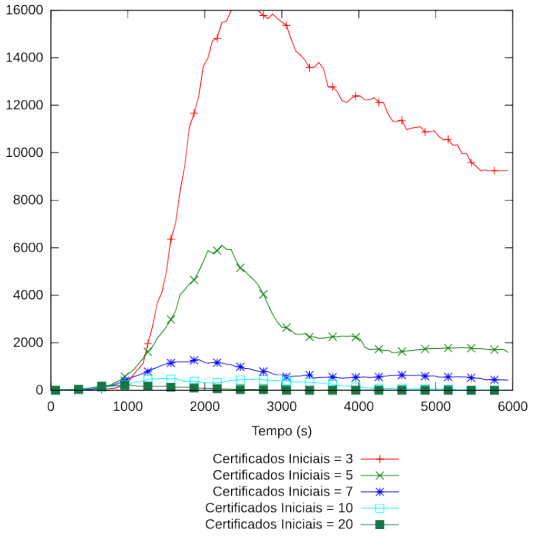



(d) Tamanho médio das cadeias

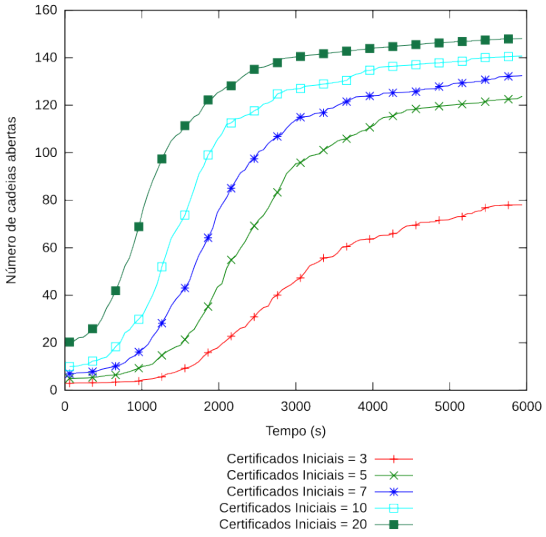
Figura B.89: Resultados para 100 nodos, $m = 20\%$ e $N_a = 10\%$ com ataque em grupo



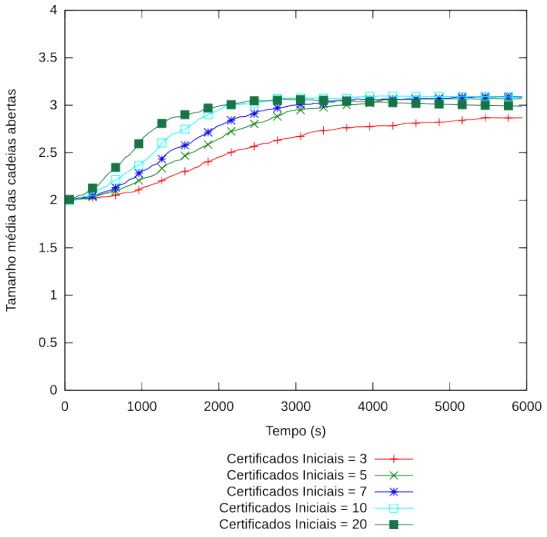

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



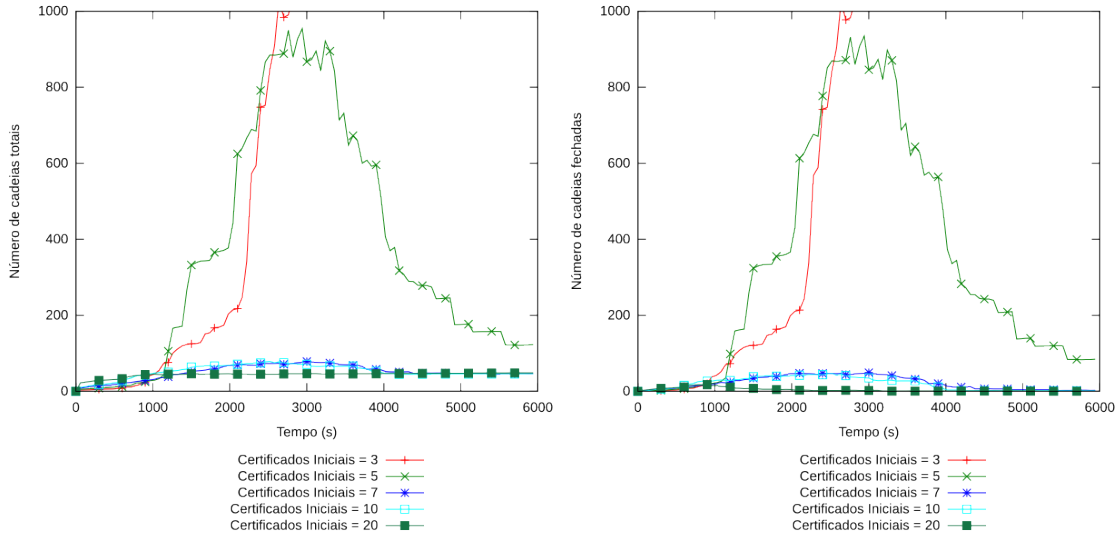

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.90: Resultados para 150 nodos, $m = 20\%$ e $N_a = 10\%$ com ataque em grupo

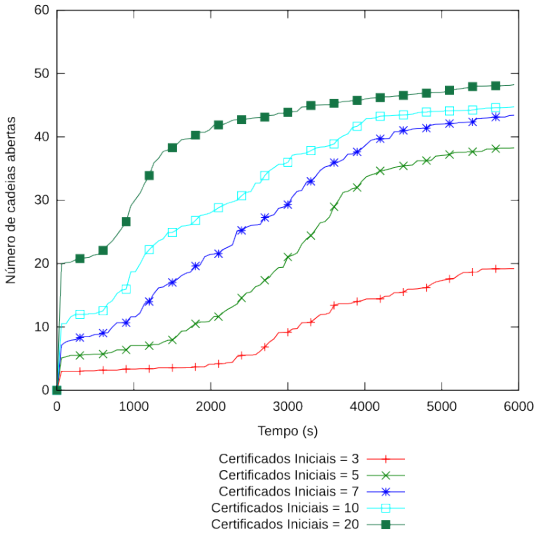
### B.7.5 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 25\%$



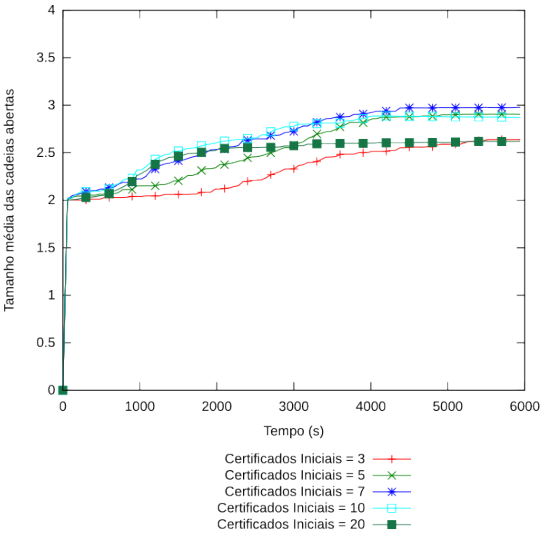

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

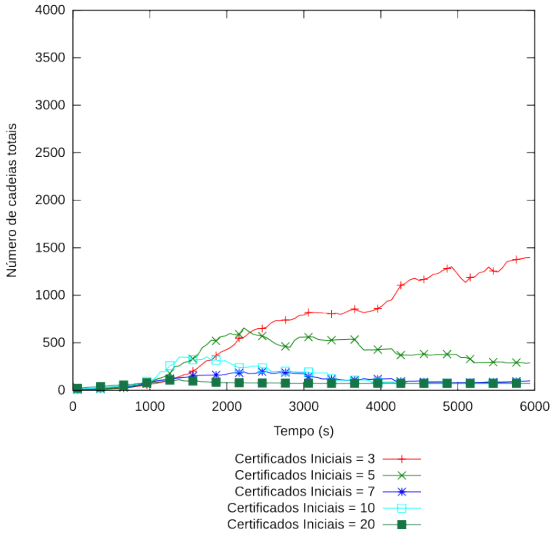



(c) Número de cadeias Abertas

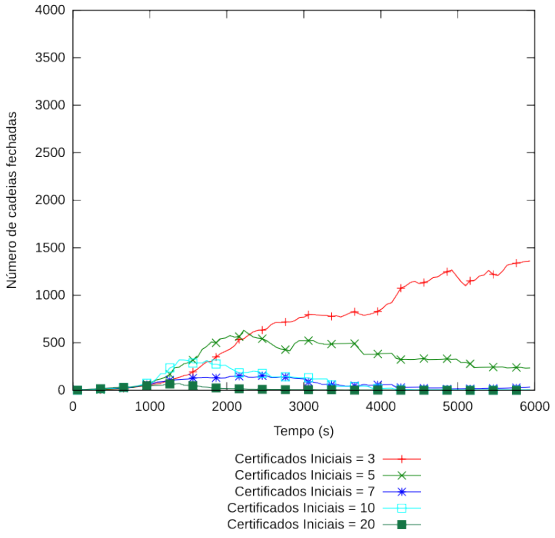



(d) Tamanho médio das cadeias

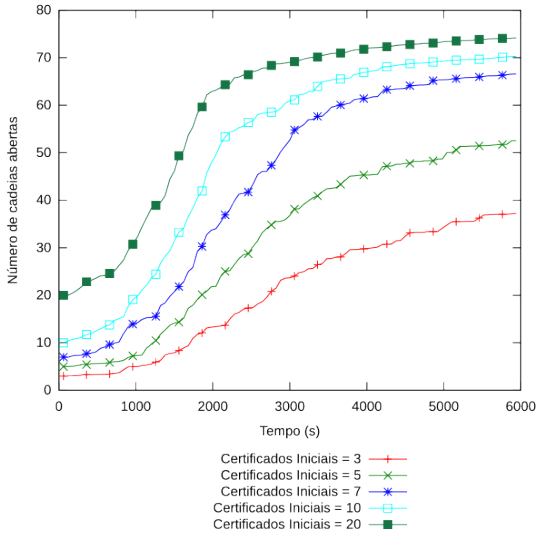
Figura B.91: Resultados para 50 nodos, $m = 20\%$ e $N_a = 25\%$ com ataque em grupo



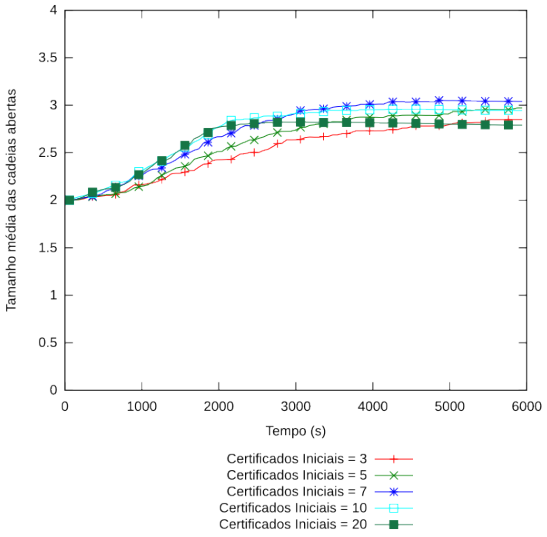

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

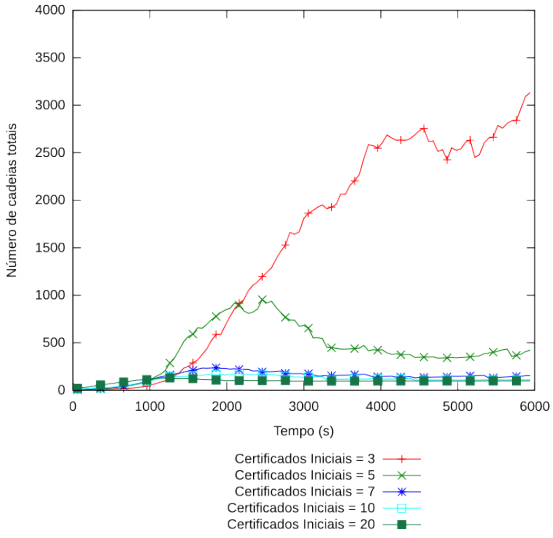



(c) Número de cadeias Abertas

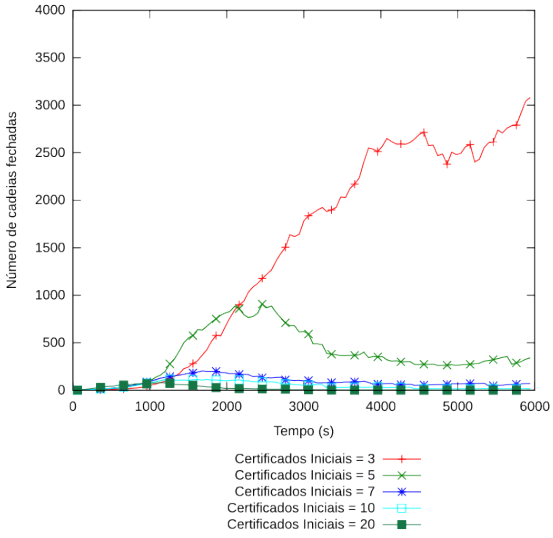



(d) Tamanho médio das cadeias

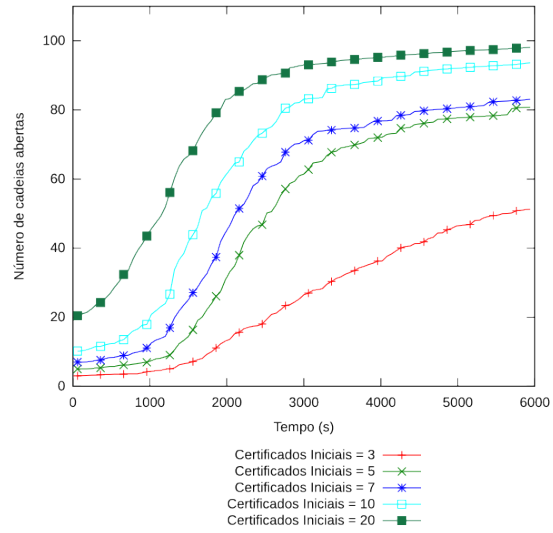
Figura B.92: Resultados para 75 nodos, $m = 20\%$ e $N_a = 25\%$ com ataque em grupo



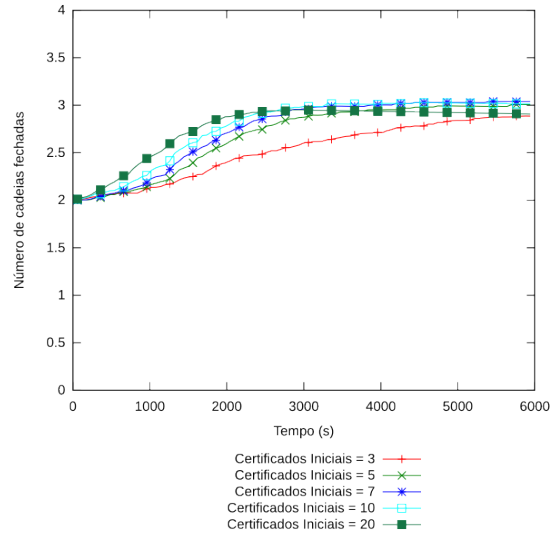

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

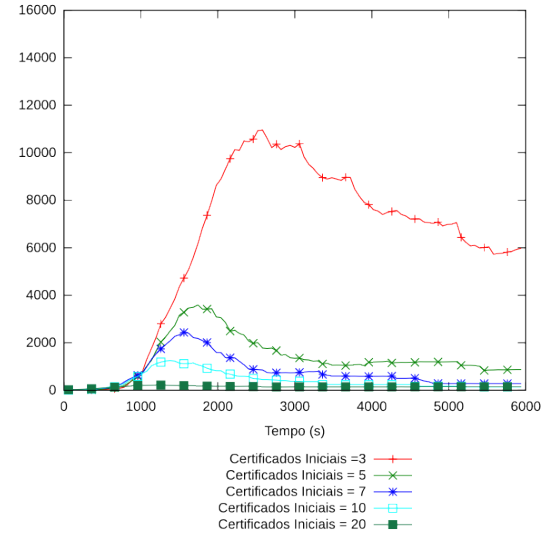



(c) Número de cadeias Abertas

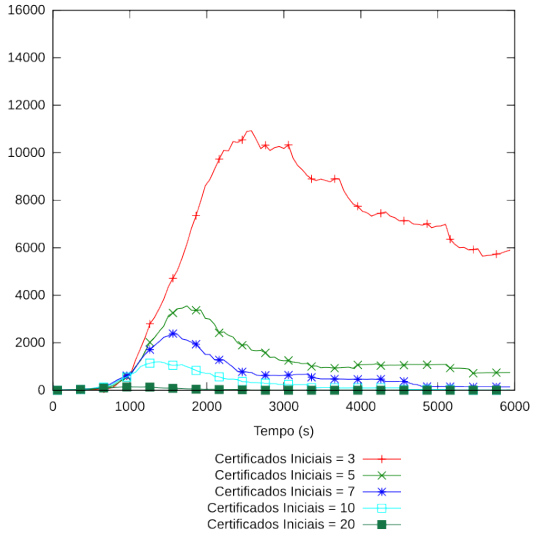



(d) Tamanho médio das cadeias

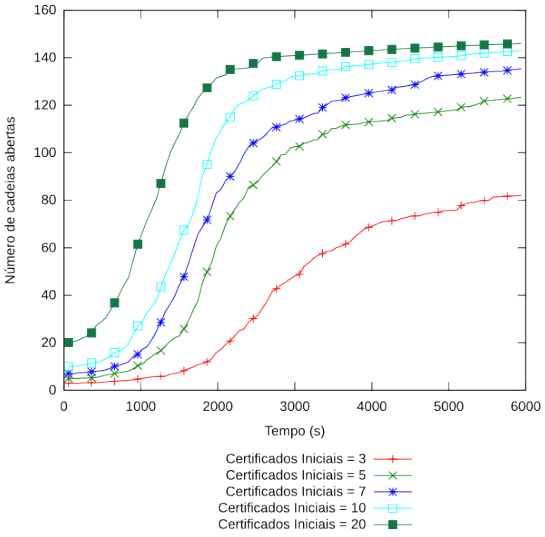
Figura B.93: Resultados para 100 nodos, $m = 20\%$ e $N_a = 25\%$ com ataque em grupo



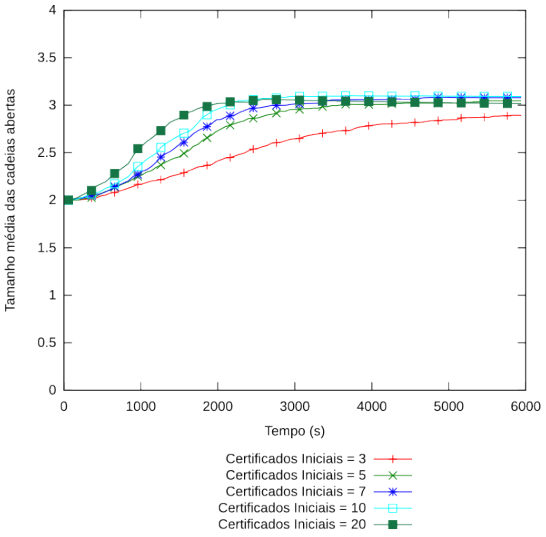

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



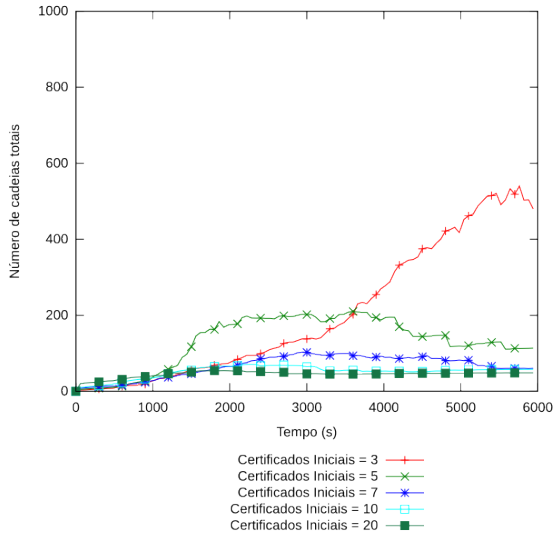

(c) Número de cadeias Abertas



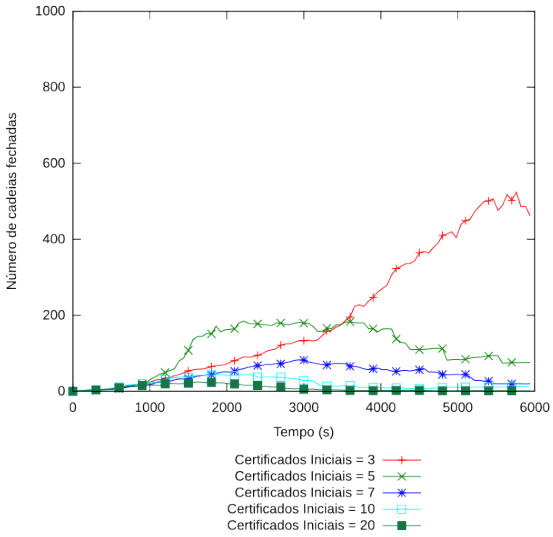

(d) Tamanho médio das cadeias

Figura B.94: Resultados para 150 nodos, $m = 20\%$ e $N_a = 25\%$ com ataque em grupo

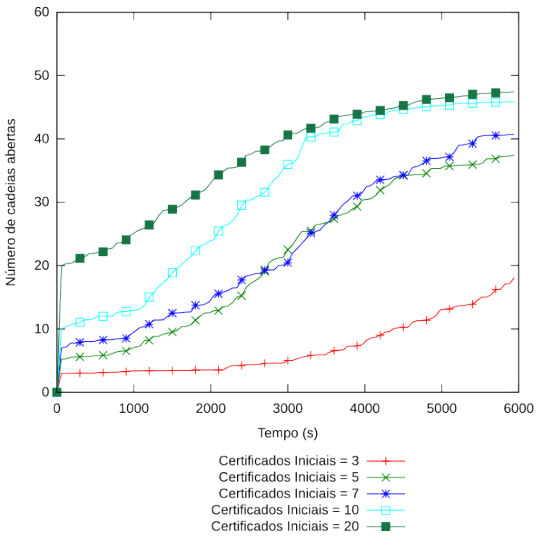
### B.7.6 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 50\%$



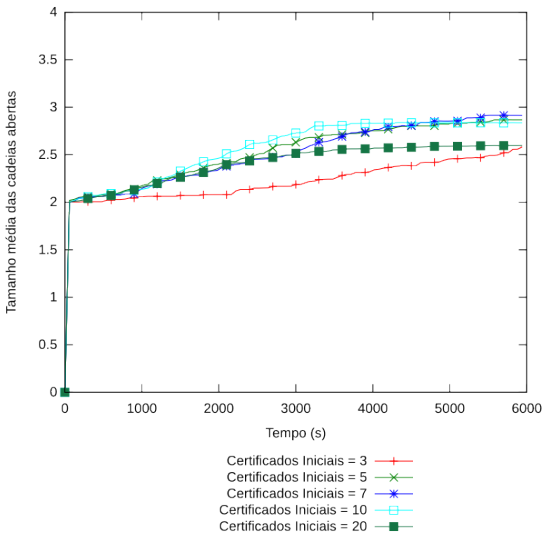

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

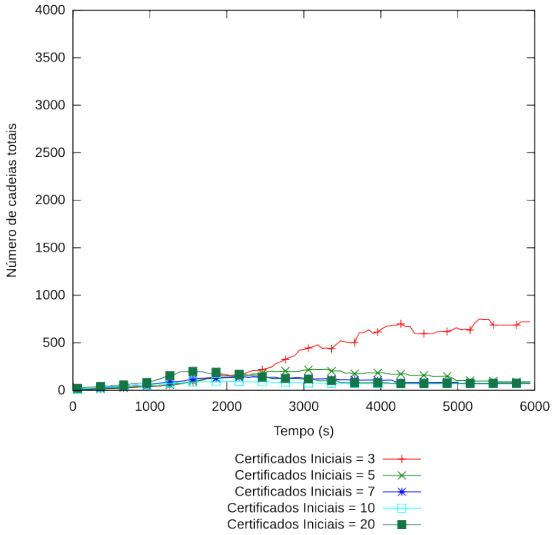



(c) Número de cadeias Abertas

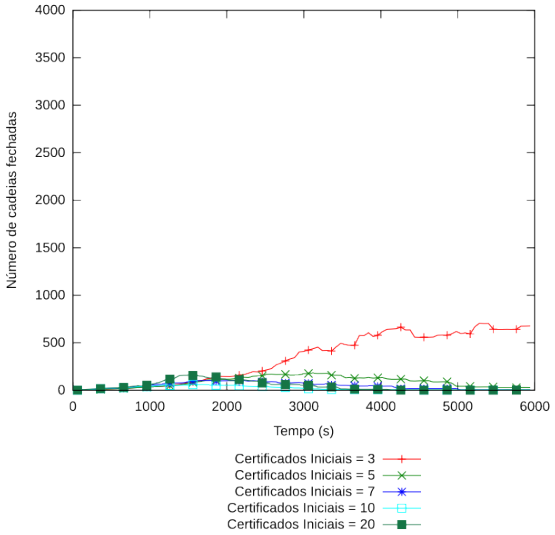



(d) Tamanho médio das cadeias

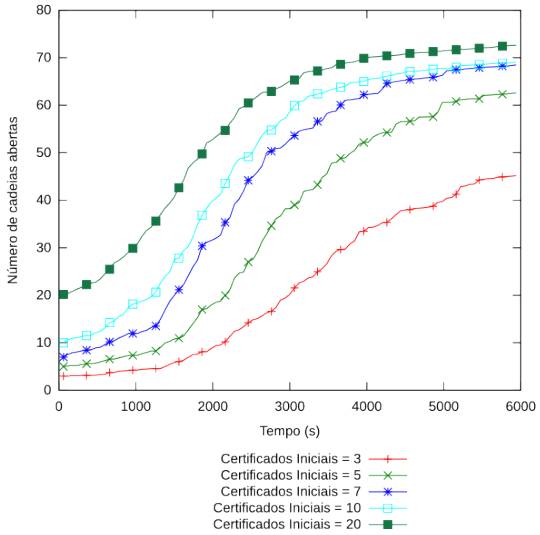
Figura B.95: Resultados para 50 nodos, $m = 20\%$ e $N_a = 50\%$ com ataque em grupo



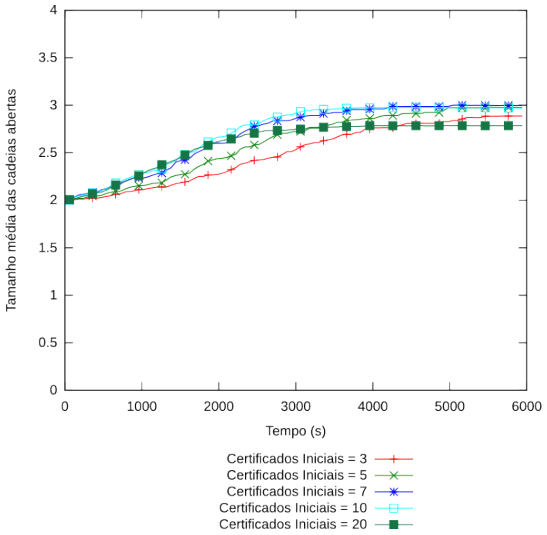

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

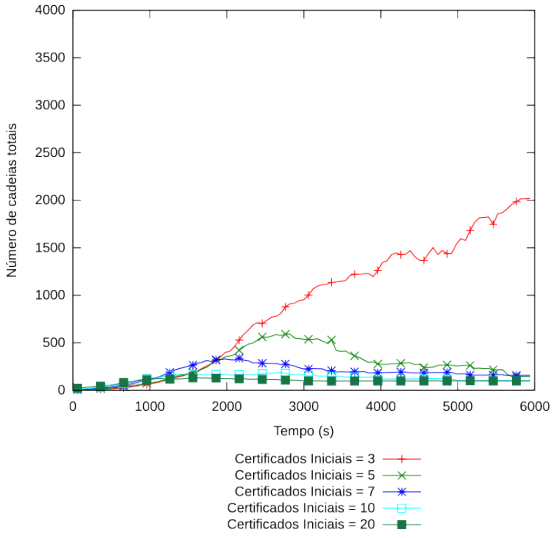



(c) Número de cadeias Abertas

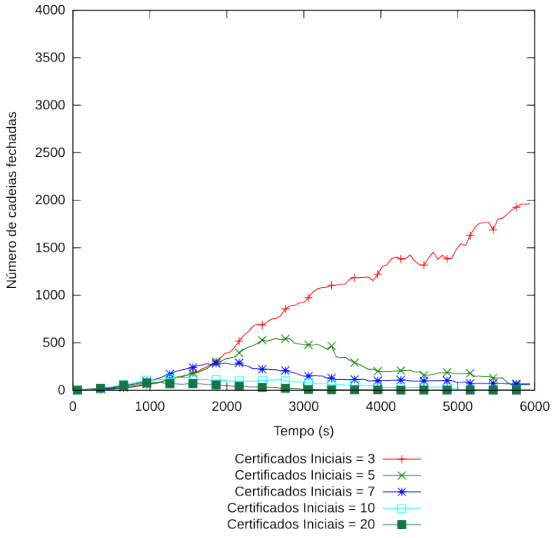



(d) Tamanho médio das cadeias

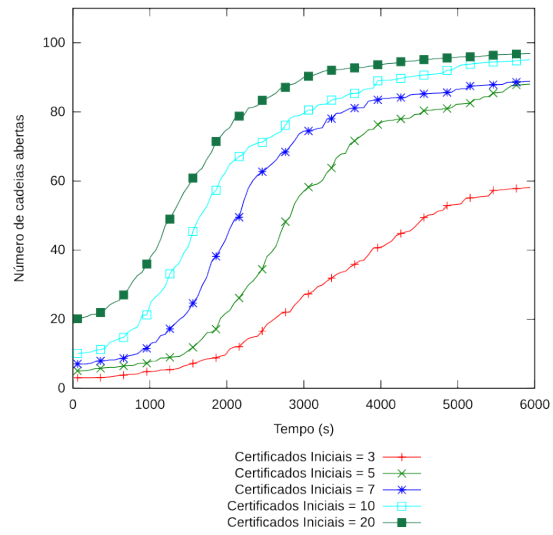
Figura B.96: Resultados para 75 nodos, $m = 20\%$ e $N_a = 50\%$ com ataque em grupo



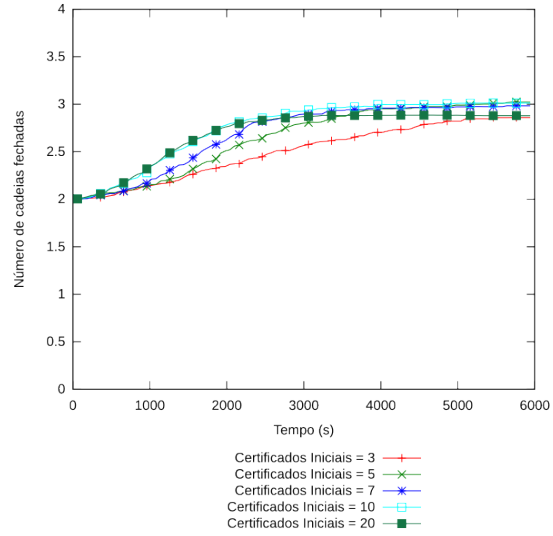

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

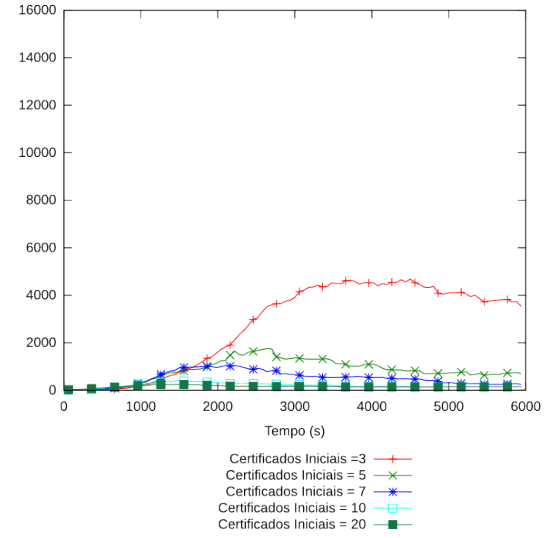



(c) Número de cadeias Abertas

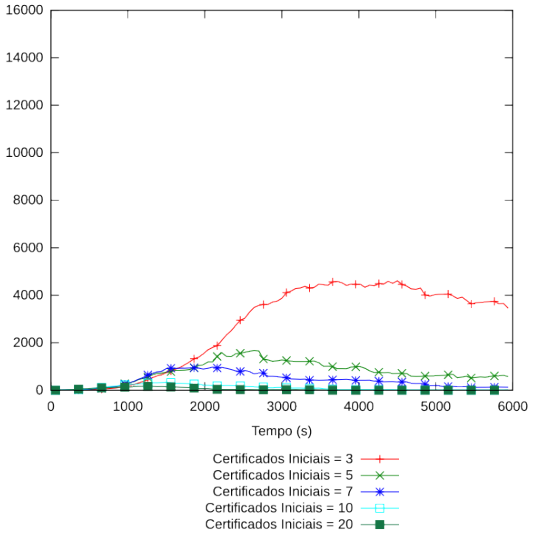



(d) Tamanho médio das cadeias

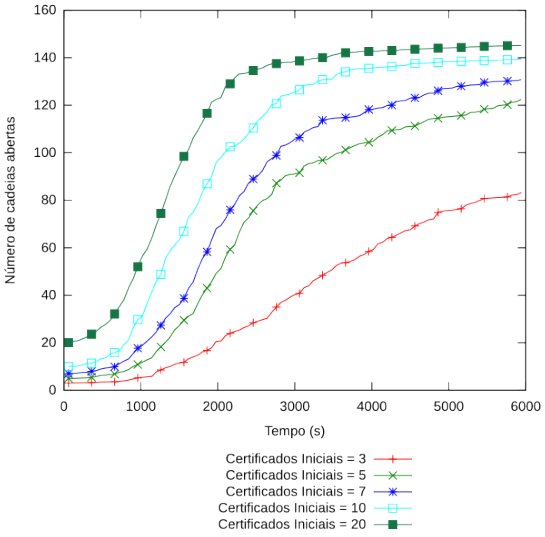
Figura B.97: Resultados para 100 nodos, $m = 20\%$ e $N_a = 50\%$ com ataque em grupo



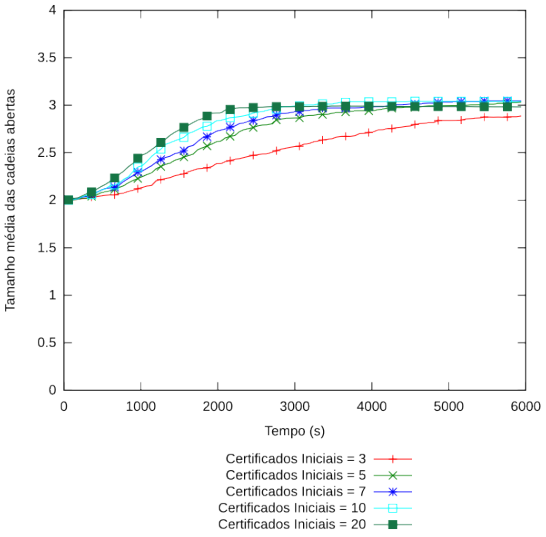

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



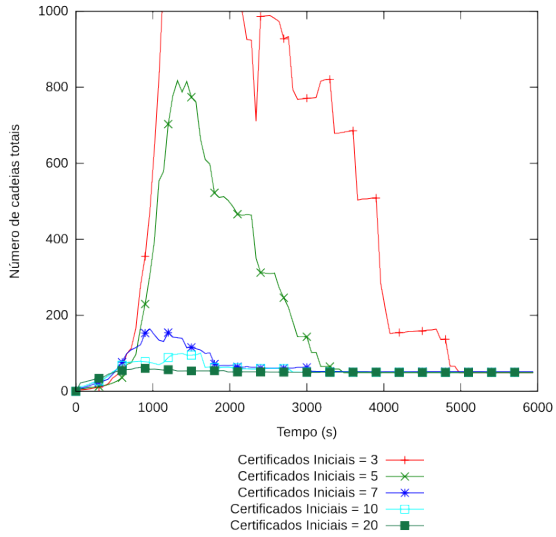

(c) Número de cadeias Abertas



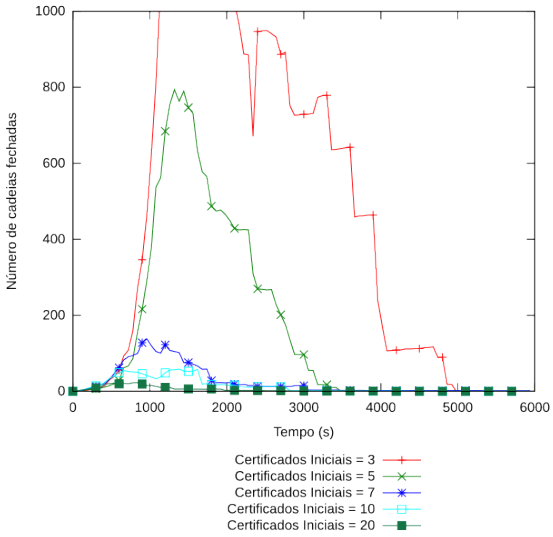

(d) Tamanho médio das cadeias

Figura B.98: Resultados para 150 nodos, $m = 20\%$ e $N_a = 50\%$ com ataque em grupo

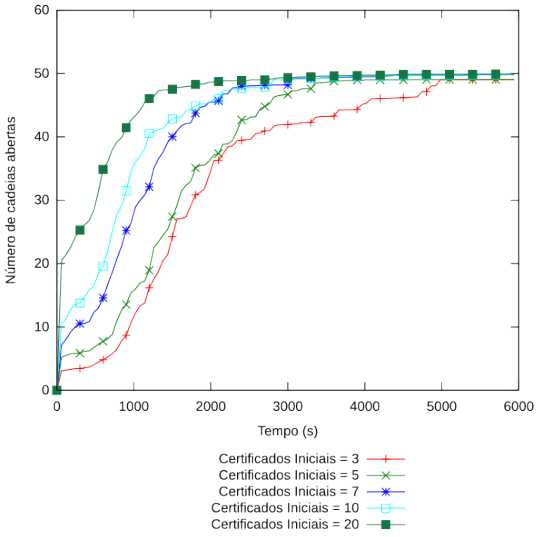
### B.7.7 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 10\%$



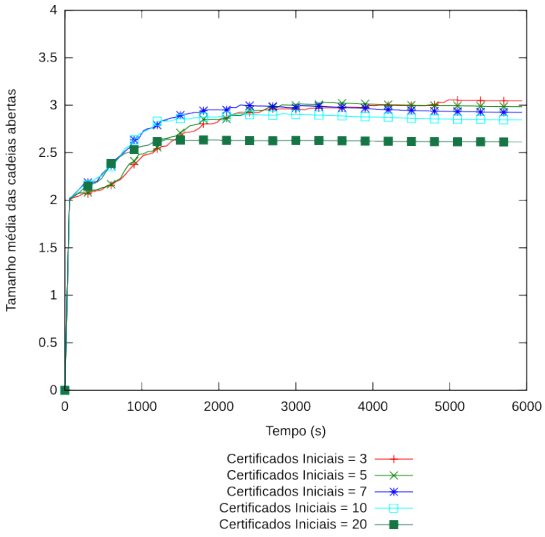

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

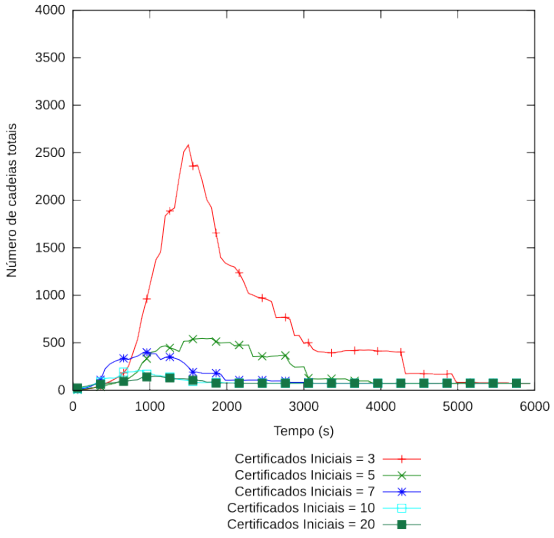



(c) Número de cadeias Abertas

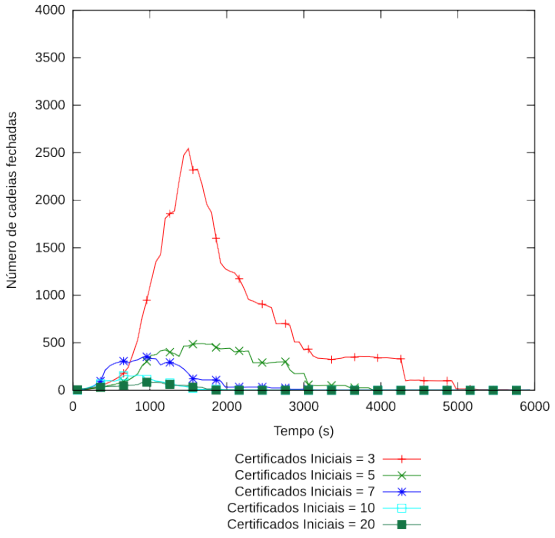



(d) Tamanho médio das cadeias

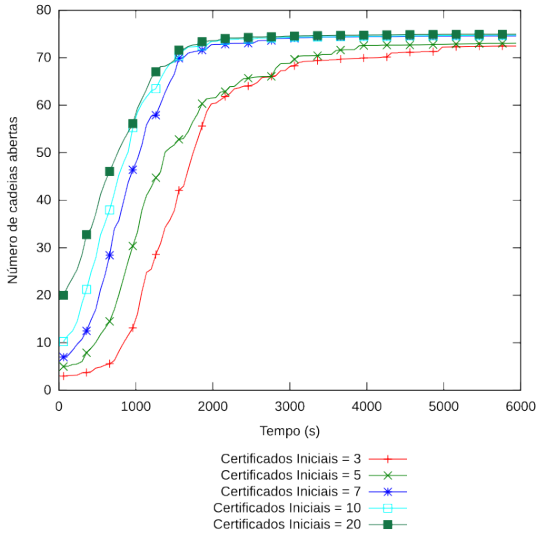
Figura B.99: Resultados para 50 nodos, $m = 50\%$ e $N_a = 10\%$ com ataque em grupo



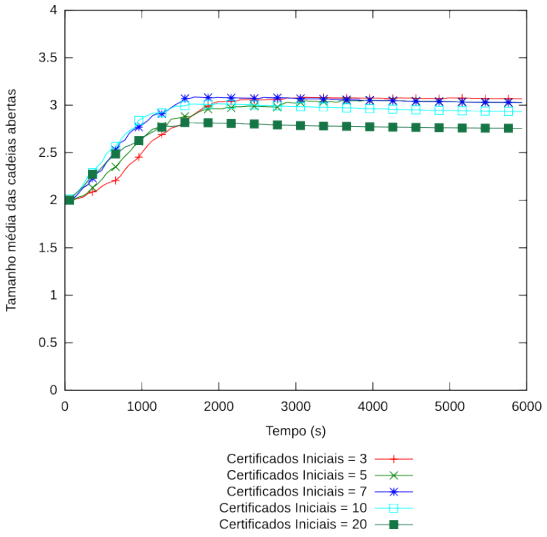

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

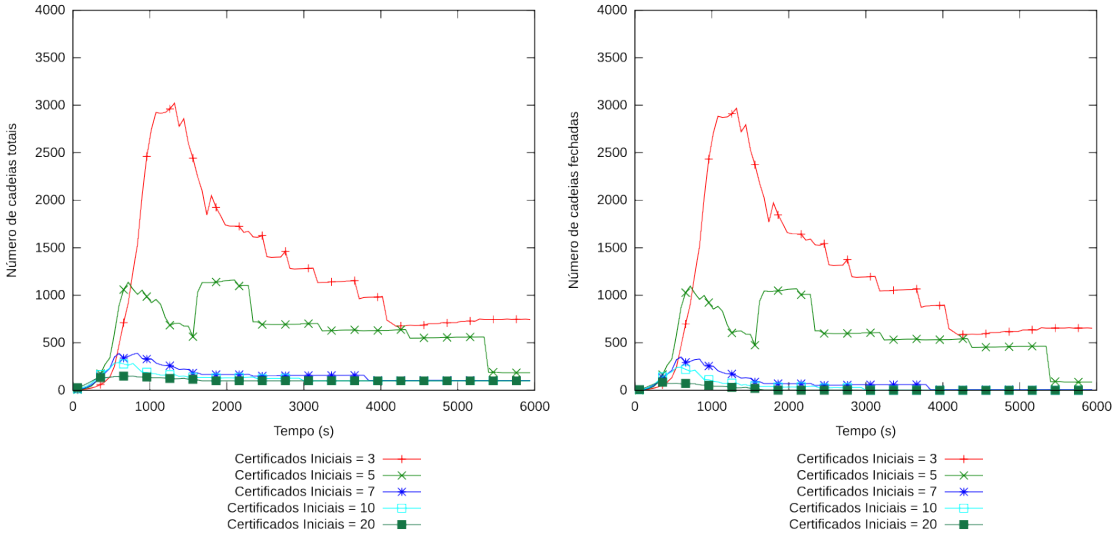



(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

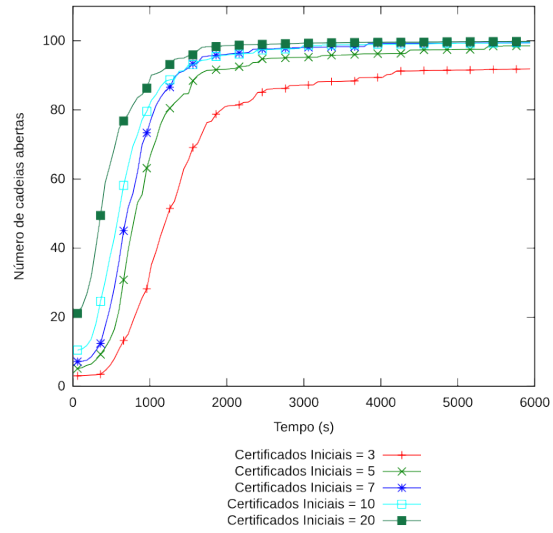
Figura B.100: Resultados para 75 nodos, $m = 50\%$ e $N_a = 10\%$ com ataque em grupo



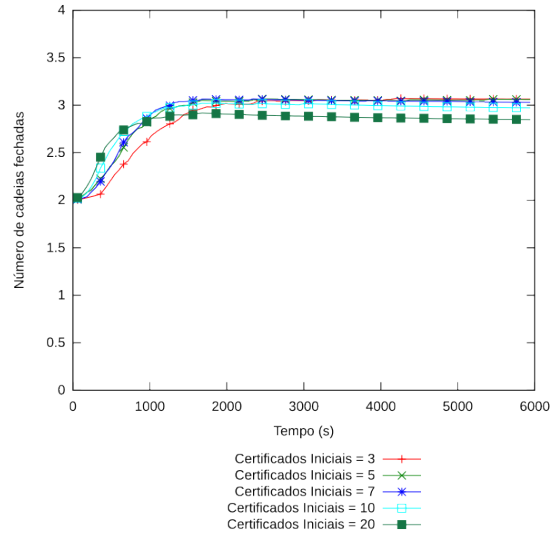

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

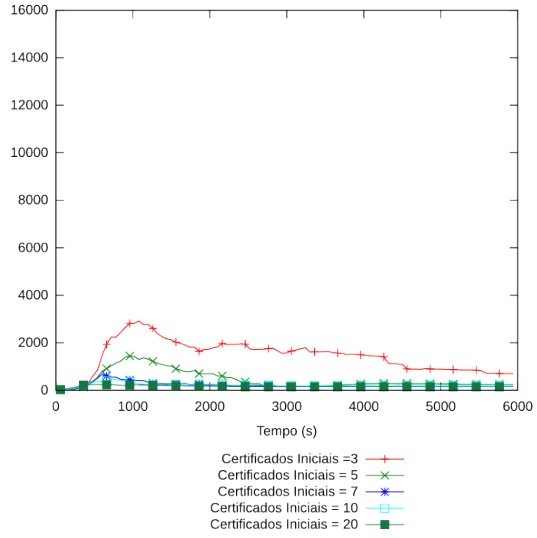



(c) Número de cadeias Abertas

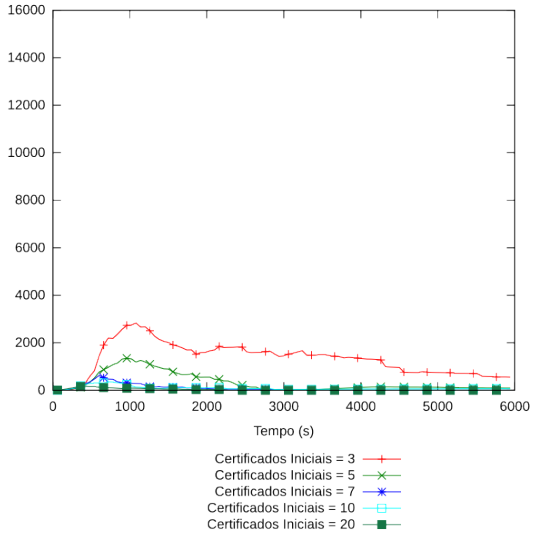



(d) Tamanho médio das cadeias

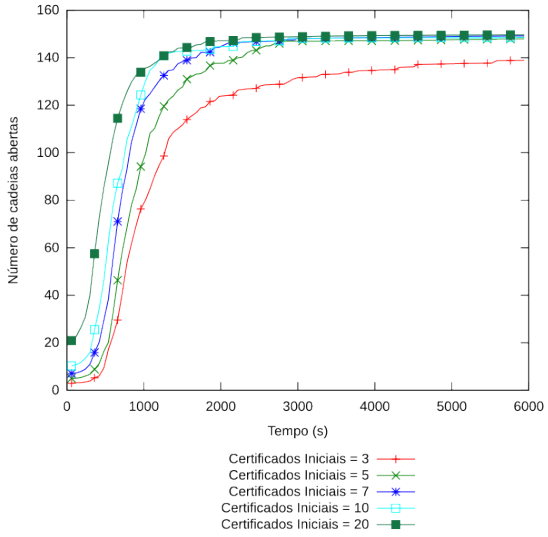
Figura B.101: Resultados para 100 nodos, $m = 50\%$ e $N_a = 10\%$ com ataque em grupo



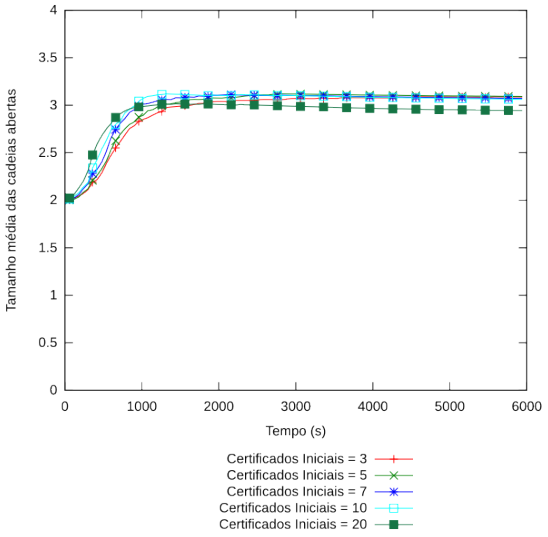

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



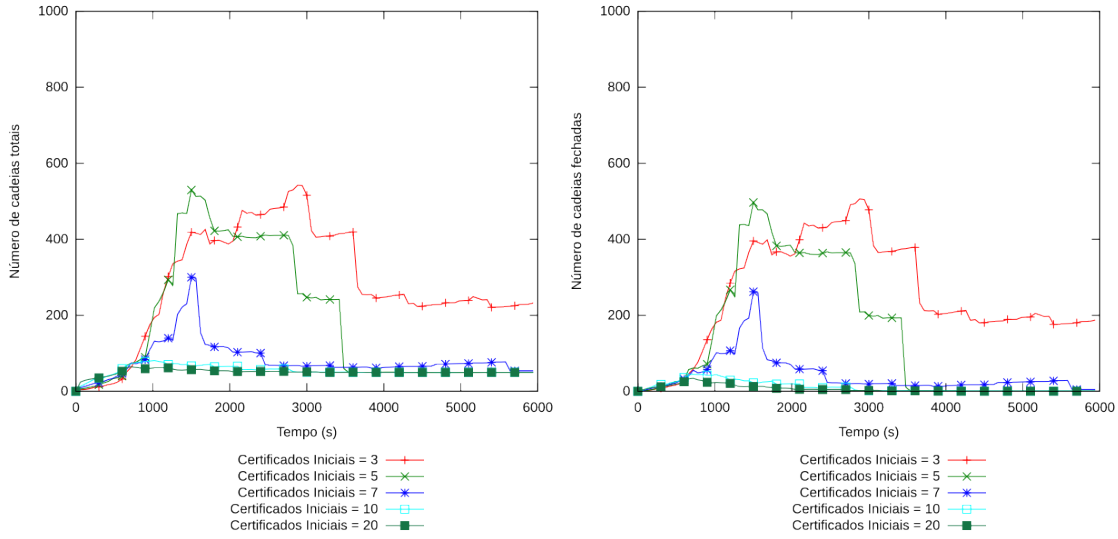

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.102: Resultados para 150 nodos, $m = 50\%$ e $N_a = 10\%$ com ataque em grupo

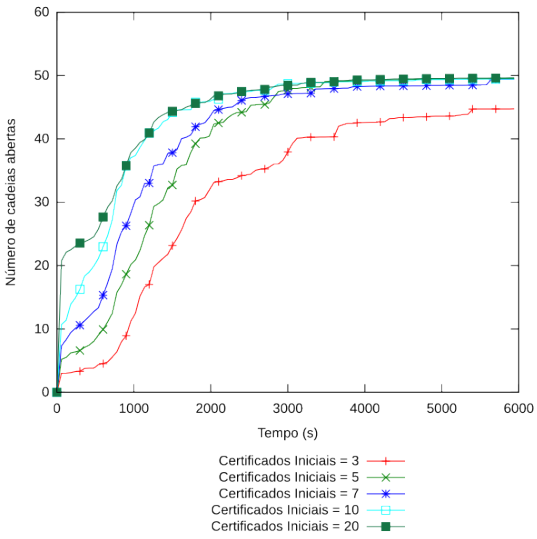
### B.7.8 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 25\%$



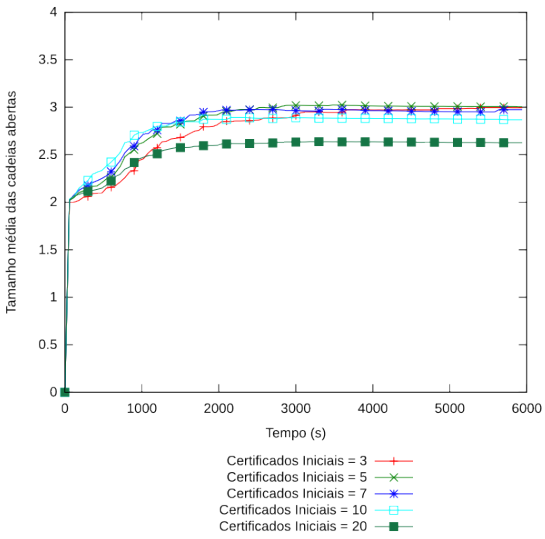

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

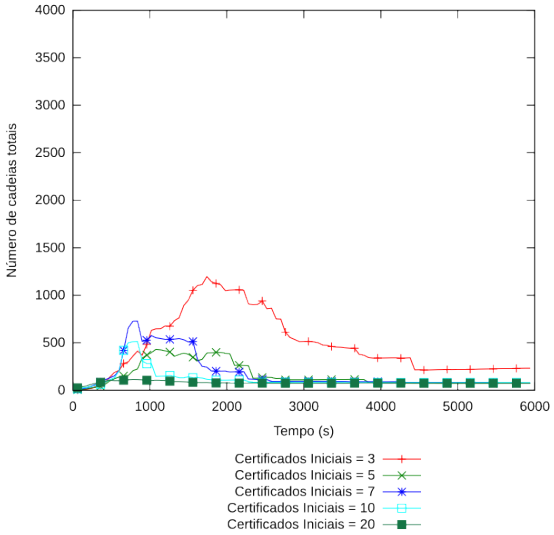



(c) Número de cadeias Abertas

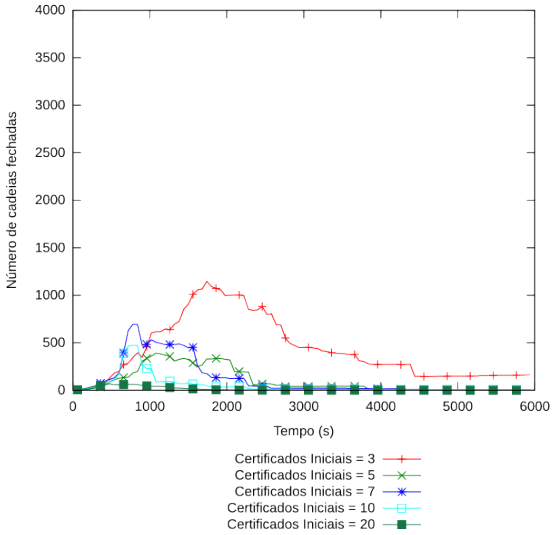



(d) Tamanho médio das cadeias

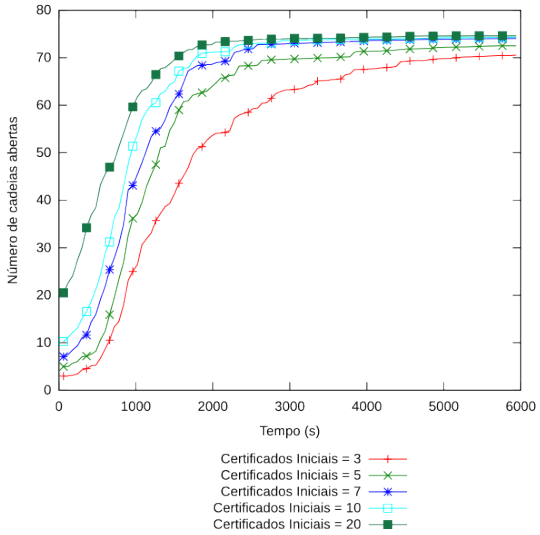
Figura B.103: Resultados para 50 nodos, $m = 50\%$ e $N_a = 25\%$ com ataque em grupo



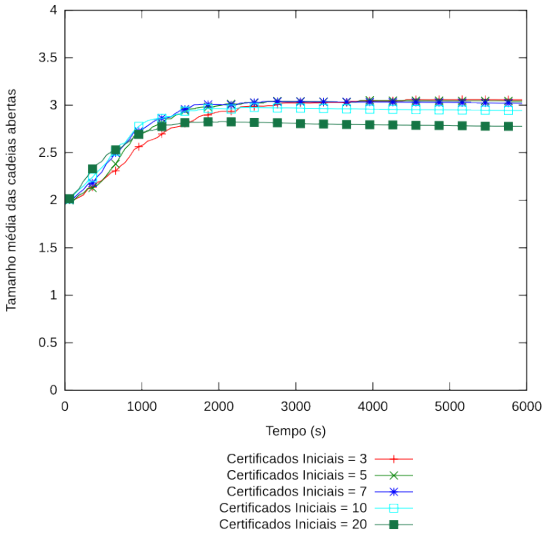

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

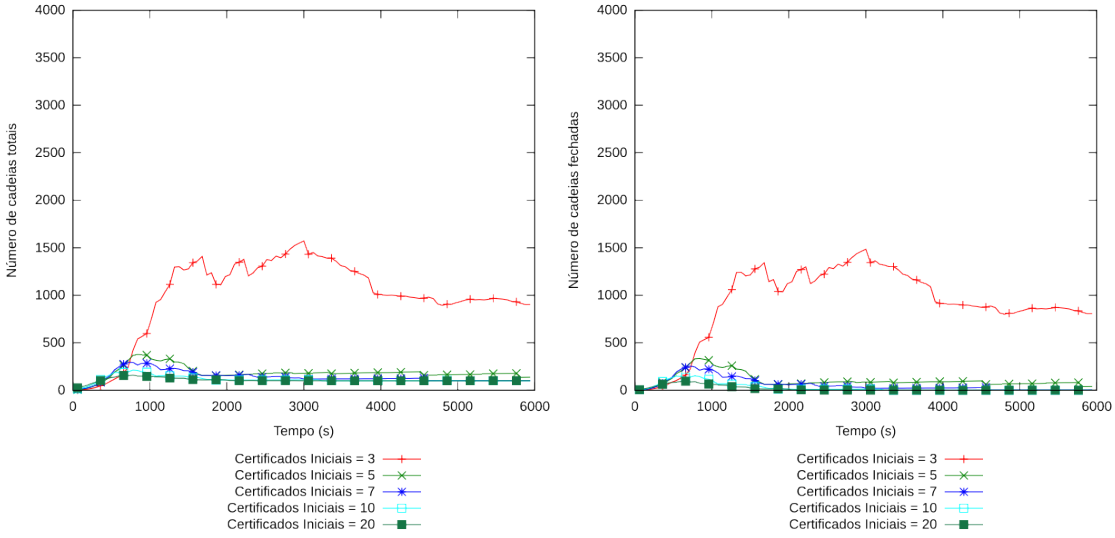



(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

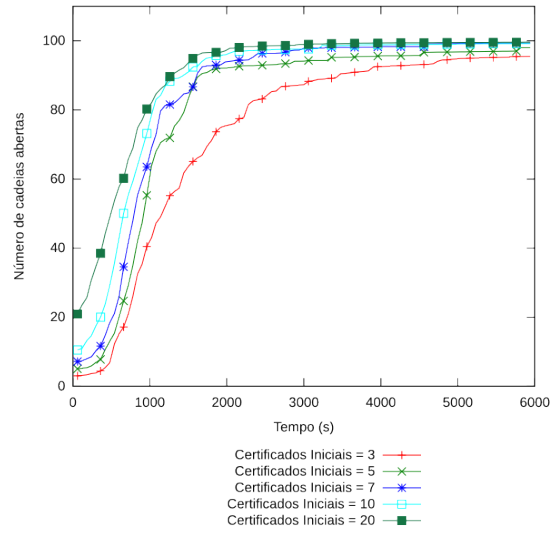
Figura B.104: Resultados para 75 nodos, $m = 50\%$ e $N_a = 25\%$ com ataque em grupo



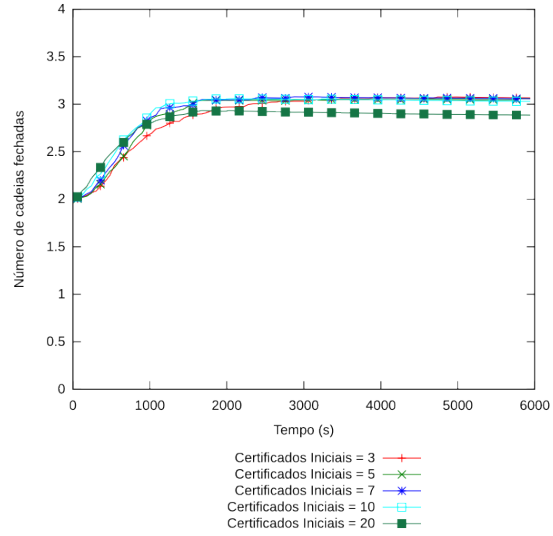

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

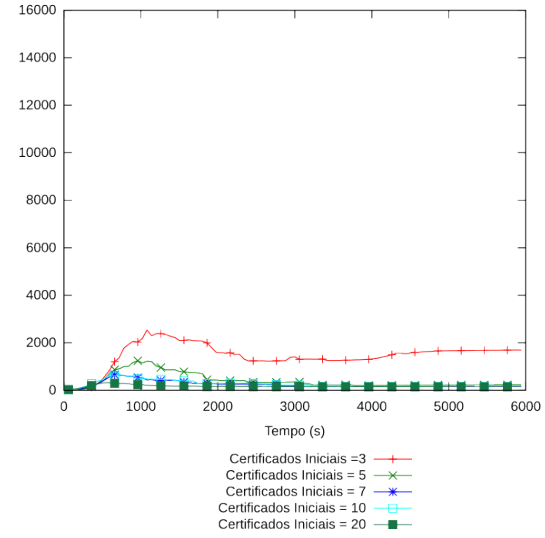



(c) Número de cadeias Abertas

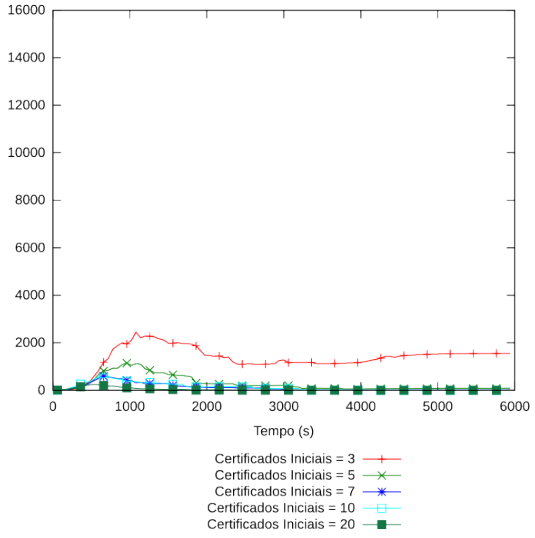



(d) Tamanho médio das cadeias

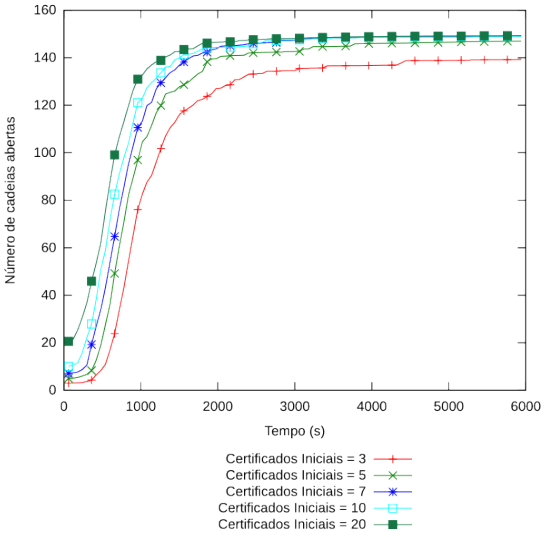
Figura B.105: Resultados para 100 nodos, $m = 50\%$ e $N_a = 25\%$ com ataque em grupo



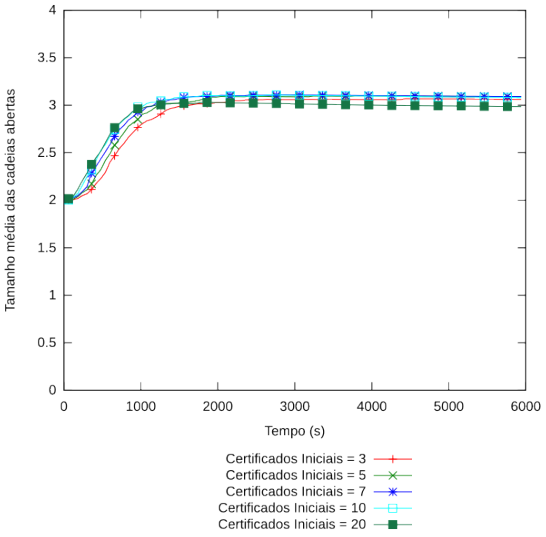

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



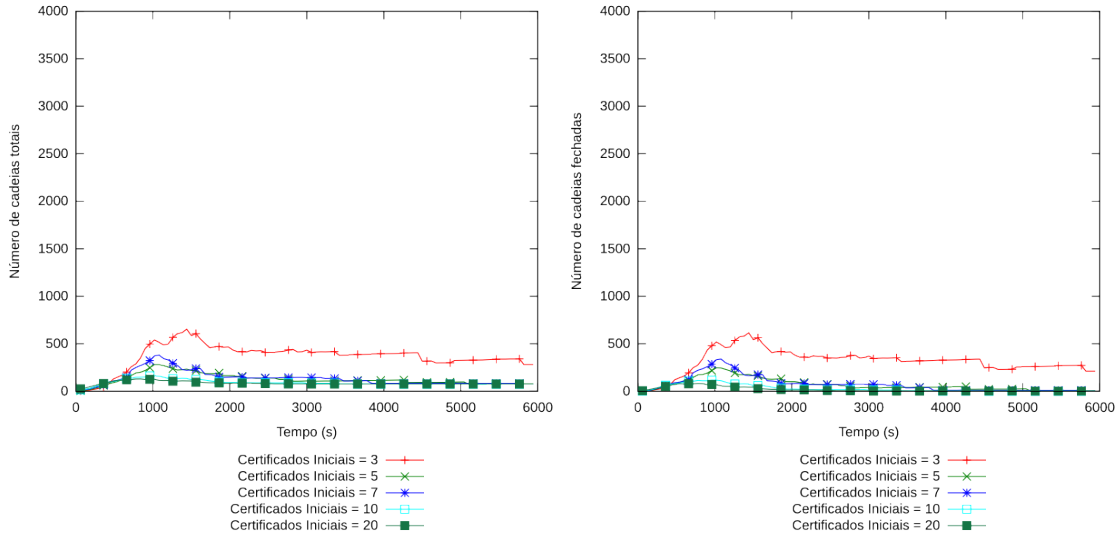

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura B.106: Resultados para 150 nodos, $m = 50\%$ e $N_a = 25\%$ com ataque em grupo

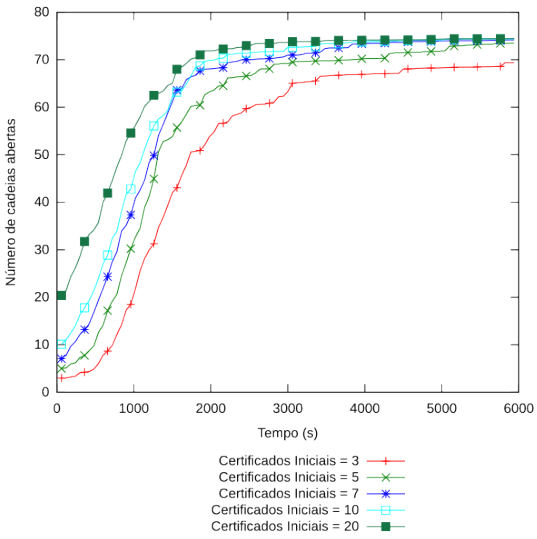
### B.7.9 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 50\%$



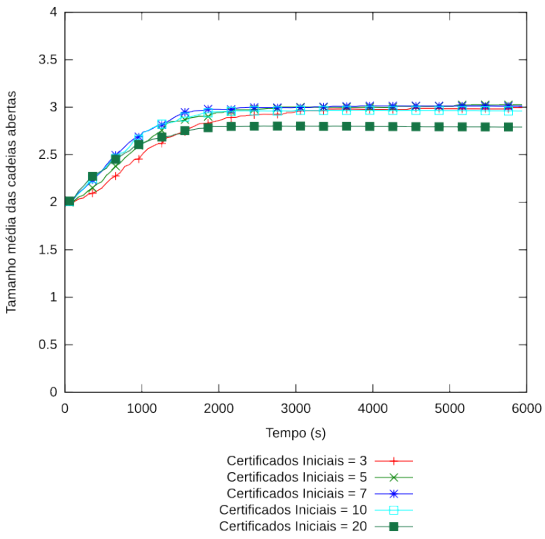

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

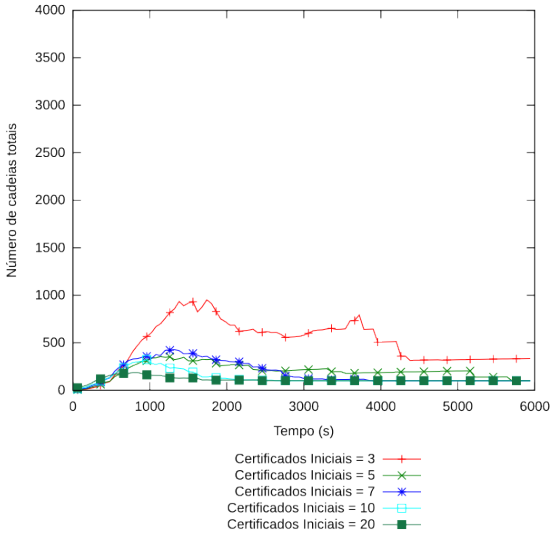



(c) Número de cadeias Abertas

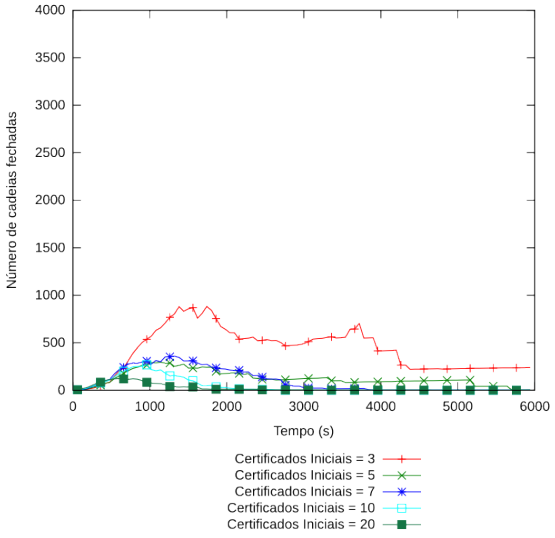



(d) Tamanho médio das cadeias

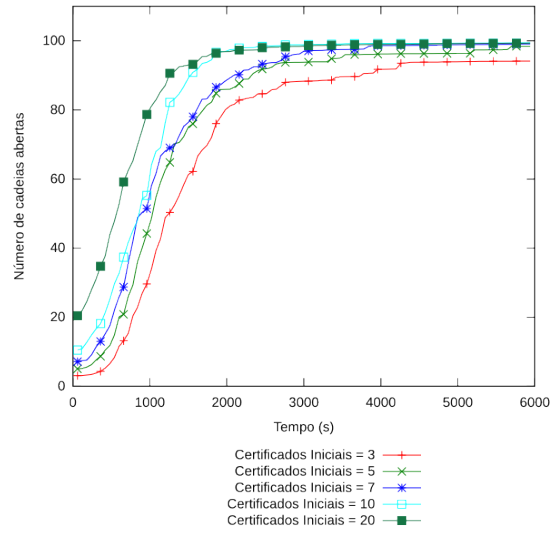
Figura B.107: Resultados para 75 nodos, $m = 50\%$ e $N_a = 50\%$ com ataque em grupo



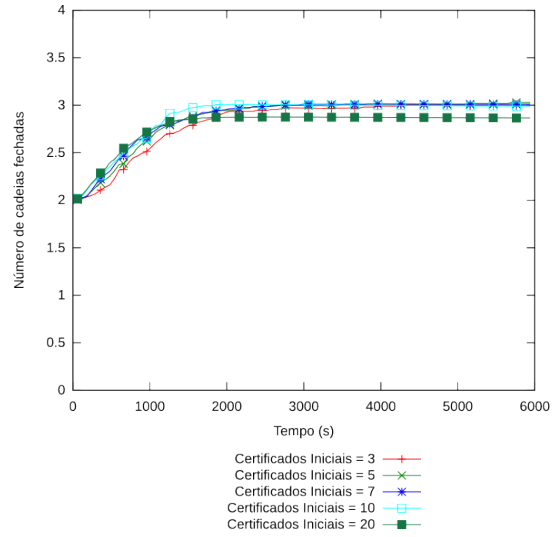

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

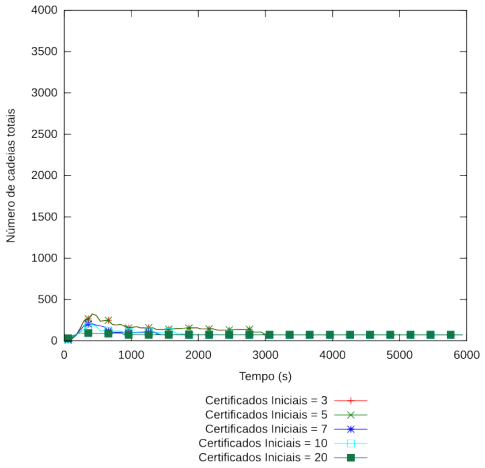
Figura B.108: Resultados para 100 nodos, $m = 50\%$ e $N_a = 50\%$ com ataque em grupo

# APÊNDICE C

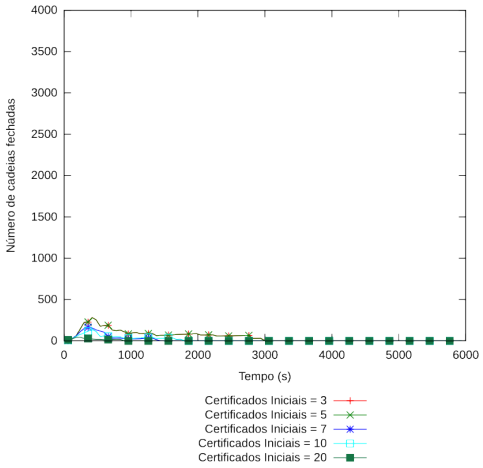
# RESULTADOS - DISTRIBUIÇÃO HETEROGÊNEA DE CERTIFICADOS INICIAIS

Neste apêndice são apresentaddos os gráficos da distribuição heterogênea de certificados iniciais que foram omitidos no Capítulo 4. Os gráficos estão organizados da seguinte forma: Versão Otimizada seguida dos ataques *GreyHole*, *BlackHole*, *Sybil* e de Falsificação.

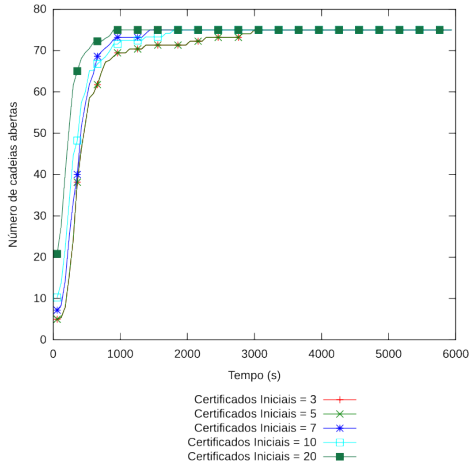
## C.1 Versão Otimizada



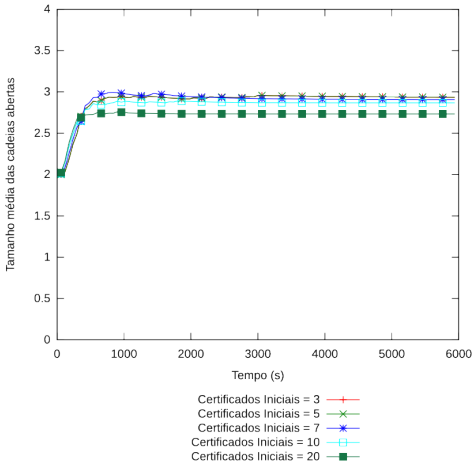

(a) Número de cadeias totais




(b) Número de cadeias fechadas

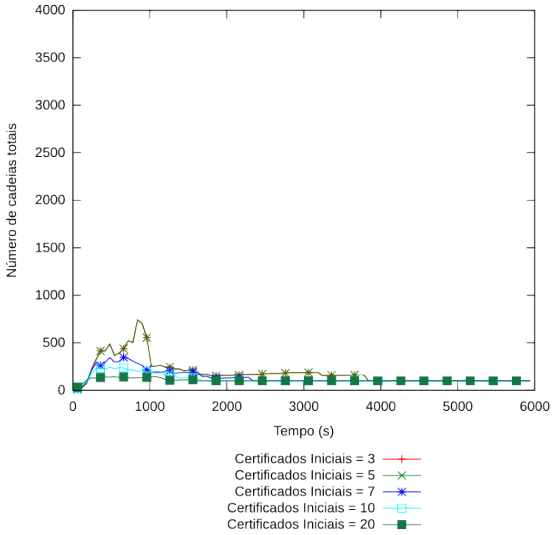



(c) Número de cadeias abertas

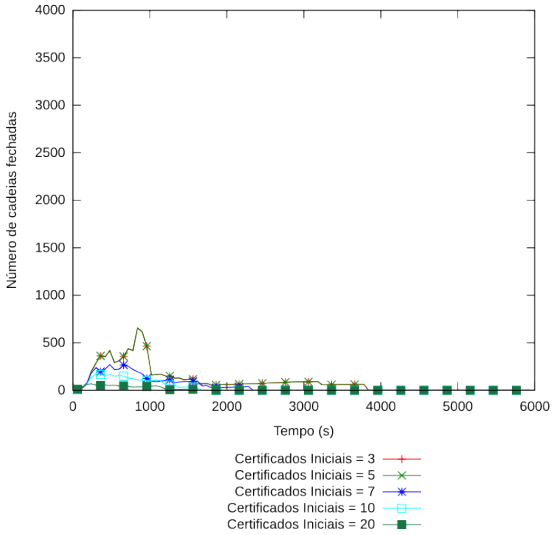



(d) Tamanho médio das cadeias

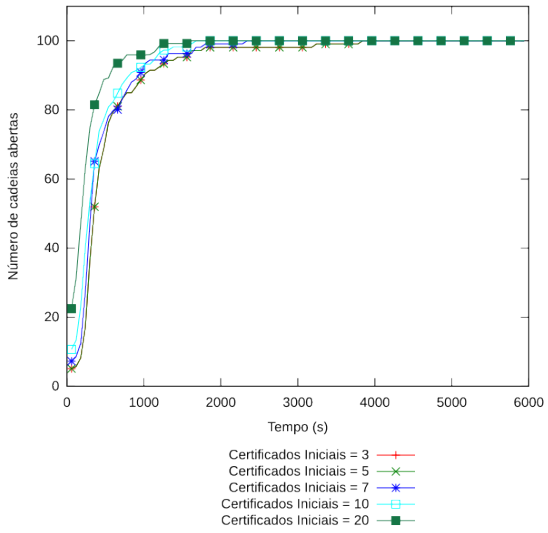
Figura C.1: Resultados com algoritmo otimizado para 75 nodos



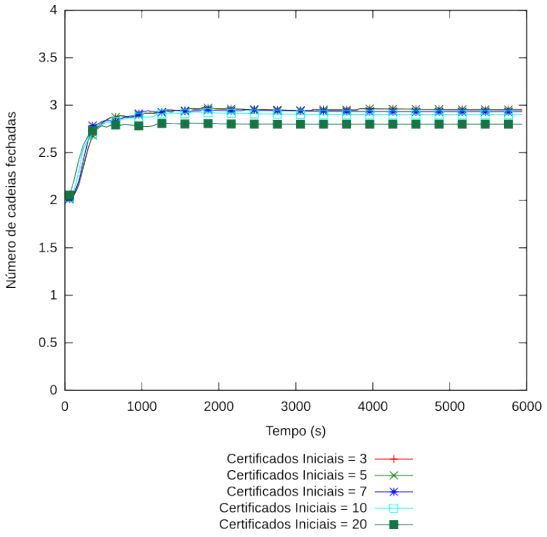

(a) Número de cadeias totais




(b) Número de cadeias fechadas




(c) Número de cadeias abertas

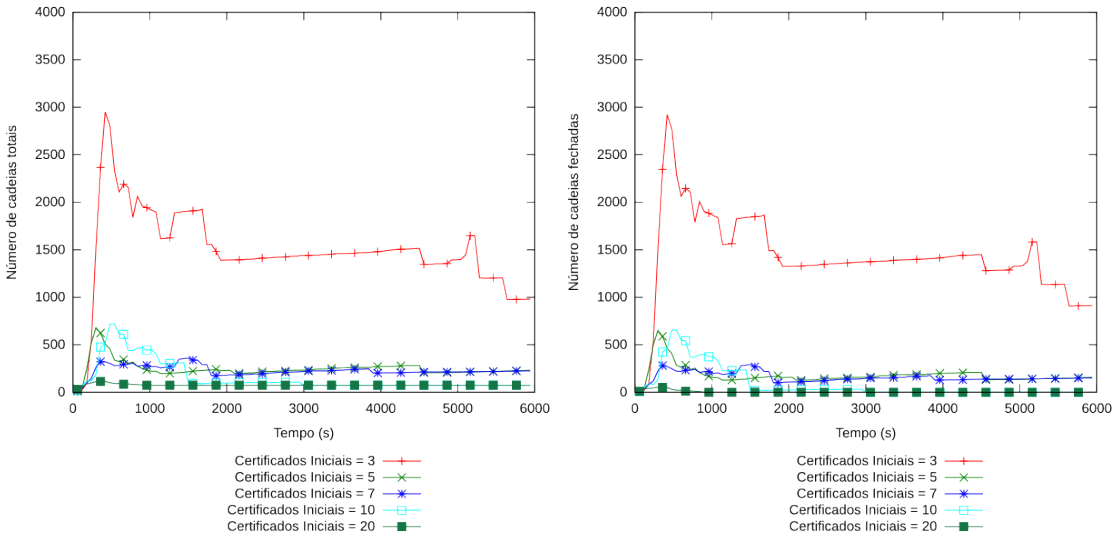



(d) Tamanho médio das cadeias

Figura C.2: Resultados com algoritmo otimizado para 100 nodos

## C.2 Ataque *GreyHole*

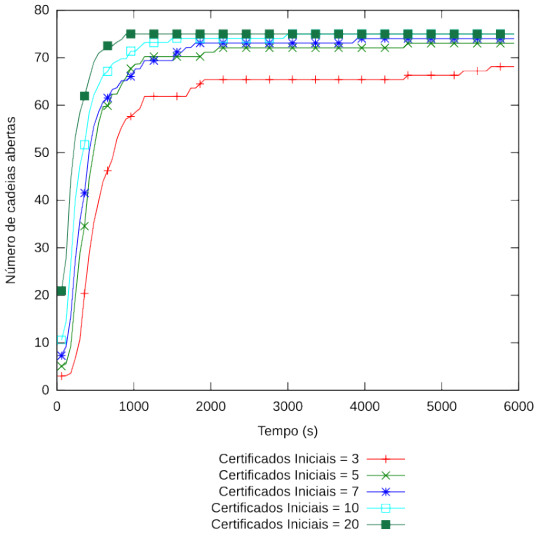
### C.2.1 Ataque *GreyHole* com $m = 10\%$ e $t = 10\%$



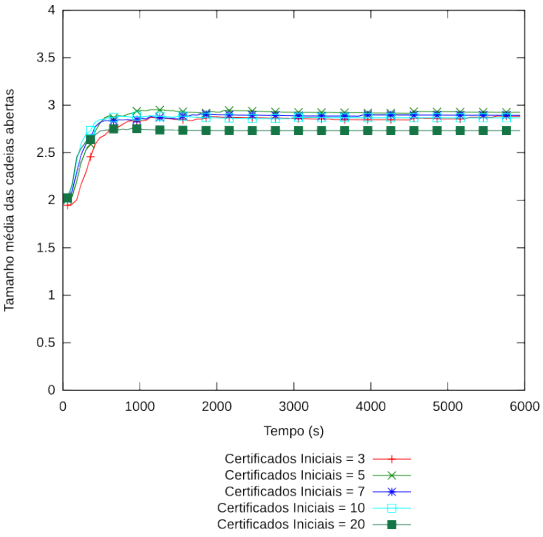

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

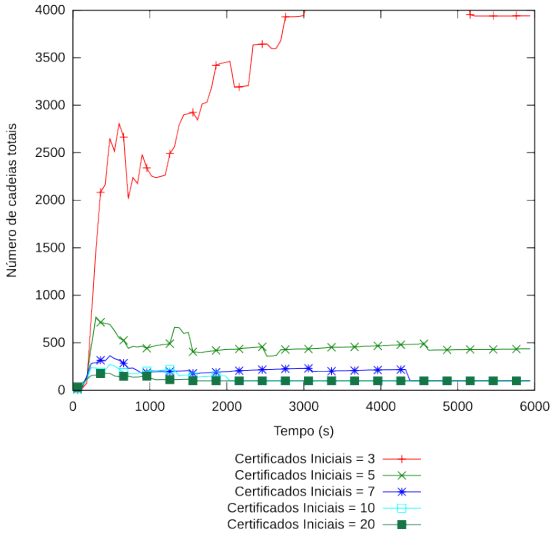



(c) Número de cadeias Abertas

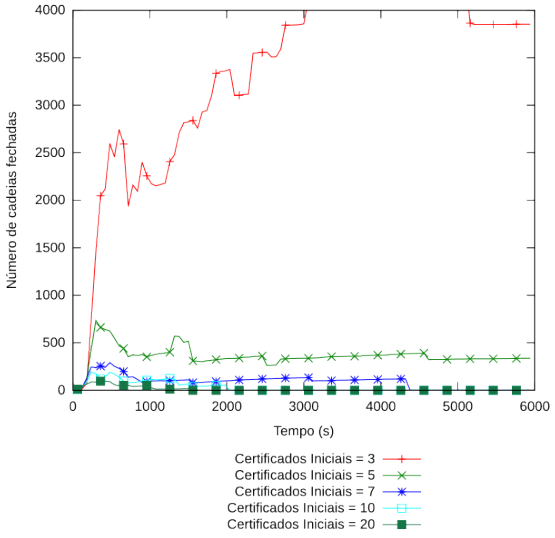



(d) Tamanho médio das cadeias

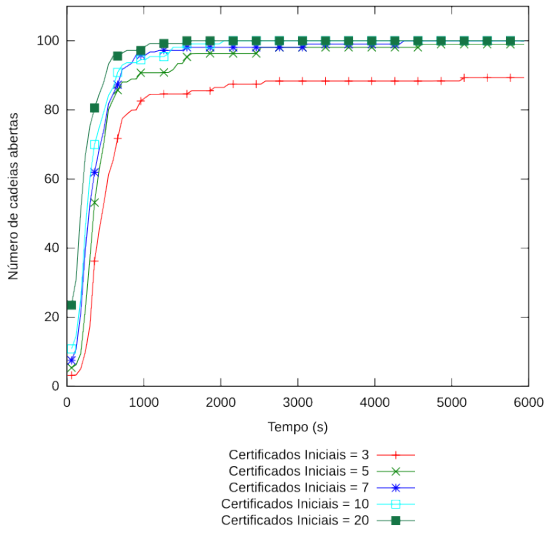
Figura C.3: Resultados para 75 nodos, $m = 10\%$ e $t = 10\%$



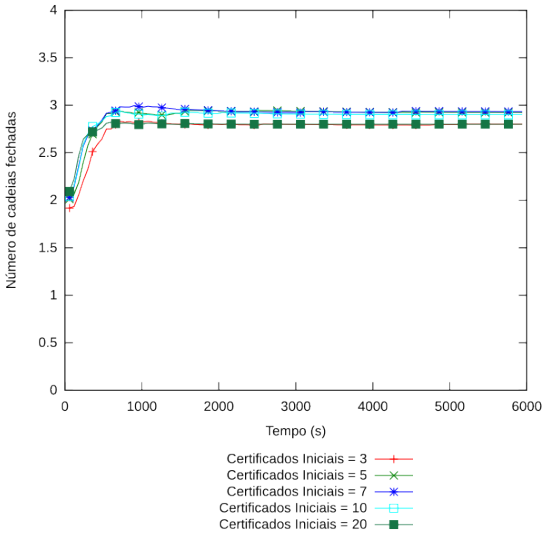

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



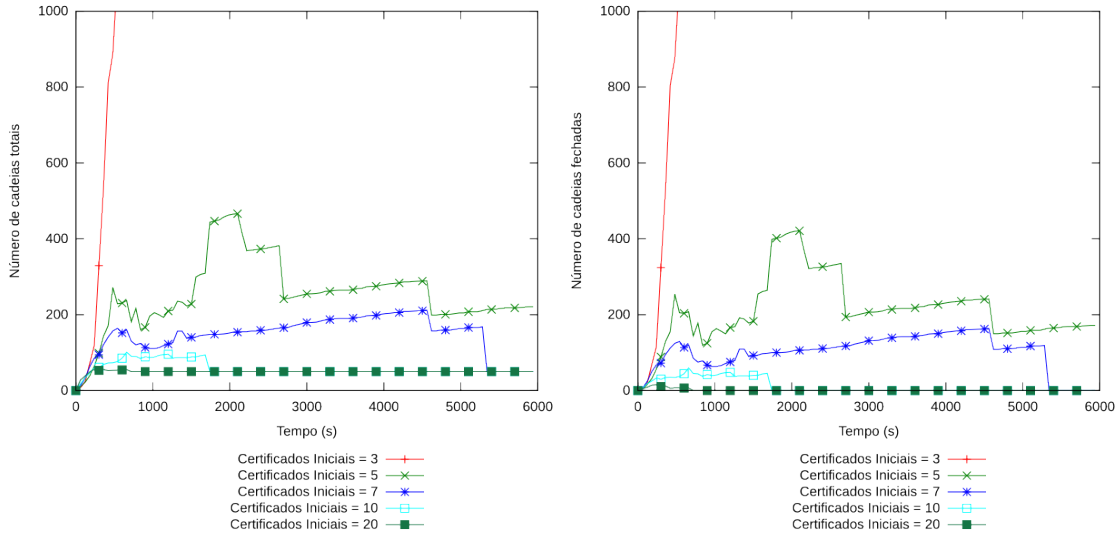

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.4: Resultados para 100 nodos, $m = 10\%$ e $t = 10\%$

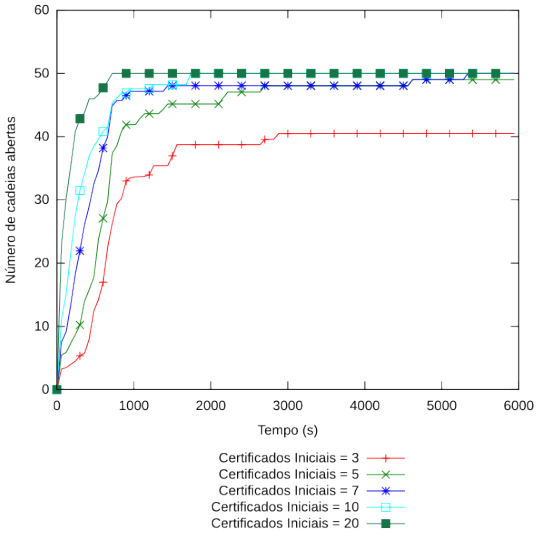
### C.2.2 Ataque *GreyHole* com $m = 10\%$ e $t = 25\%$



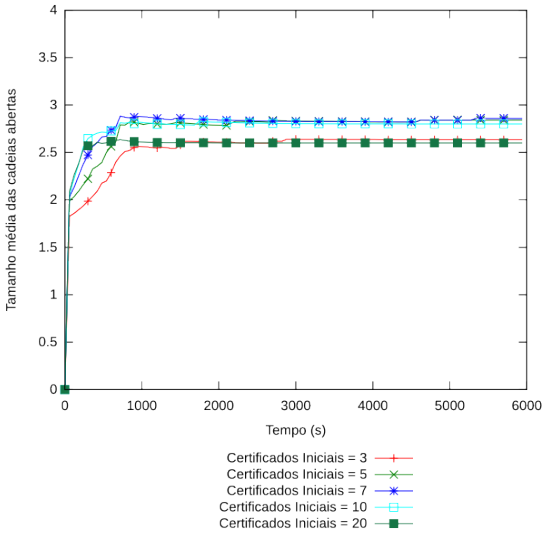

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

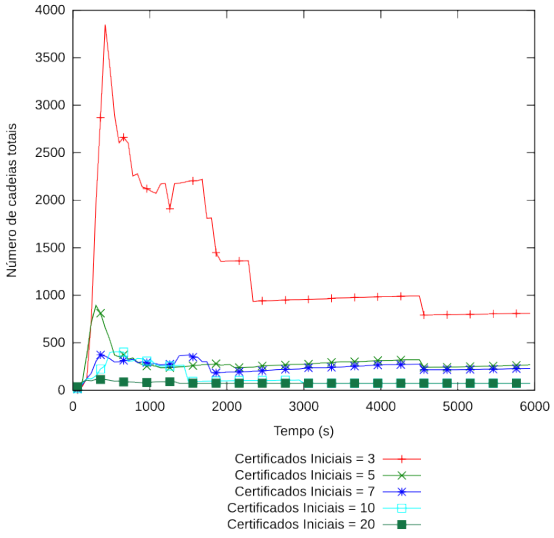



(c) Número de cadeias Abertas

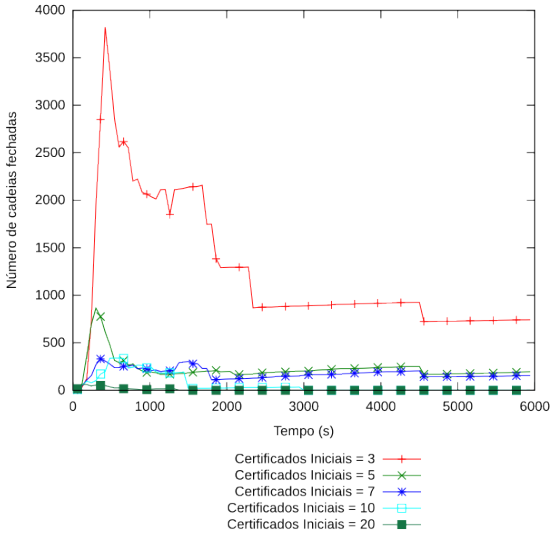



(d) Tamanho médio das cadeias

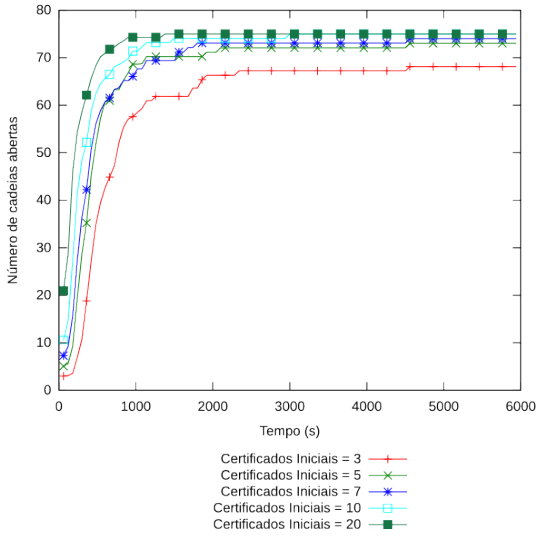
Figura C.5: Resultados para 50 nodos, $m = 10\%$ e $t = 25\%$



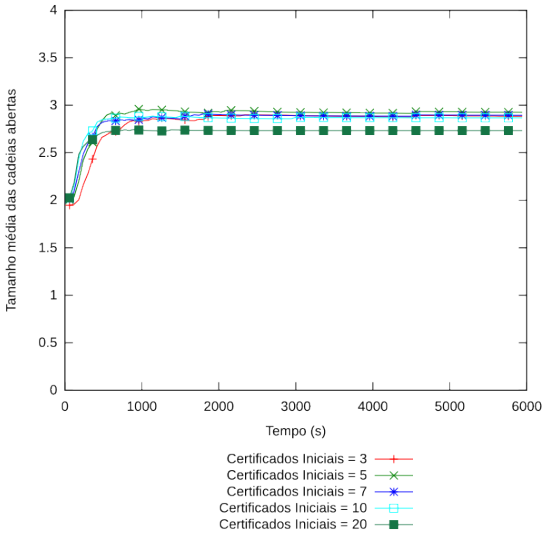

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

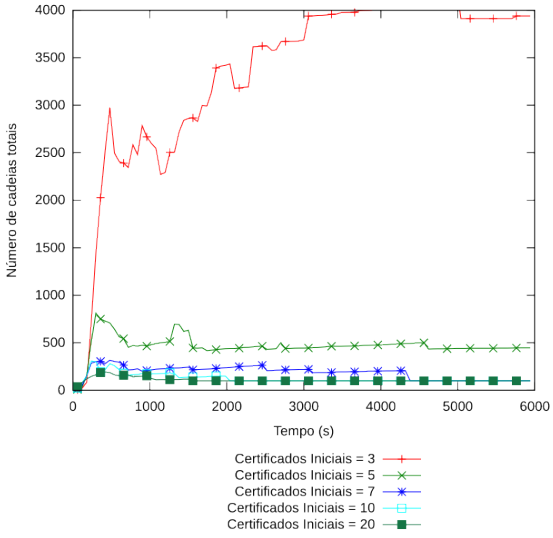



(c) Número de cadeias Abertas

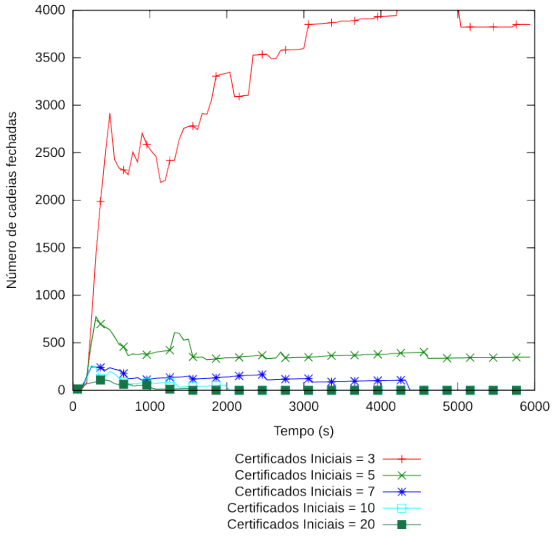



(d) Tamanho médio das cadeias

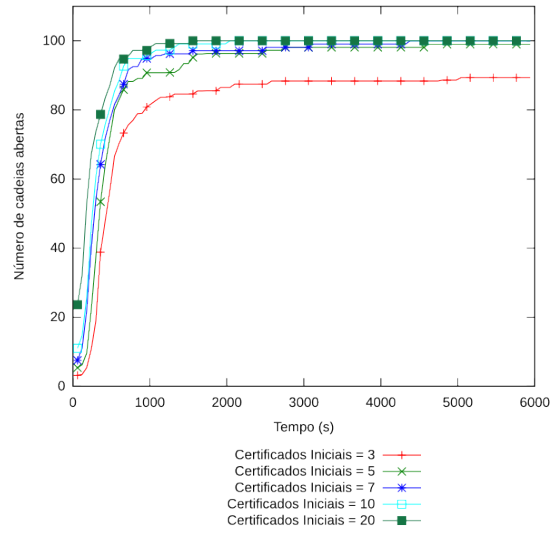
Figura C.6: Resultados para 75 nodos, $m = 10\%$ e $t = 25\%$



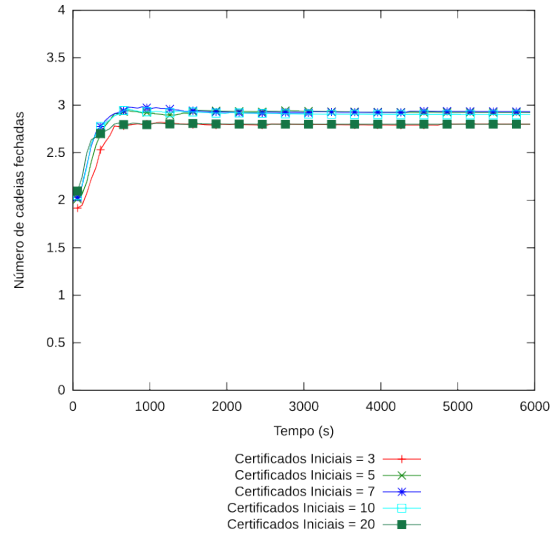

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

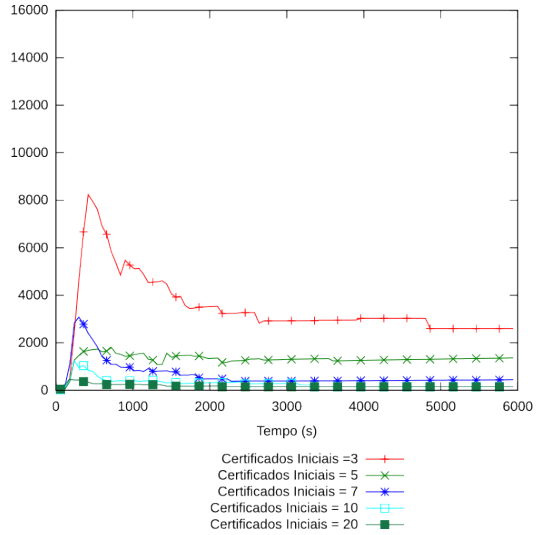



(c) Número de cadeias Abertas

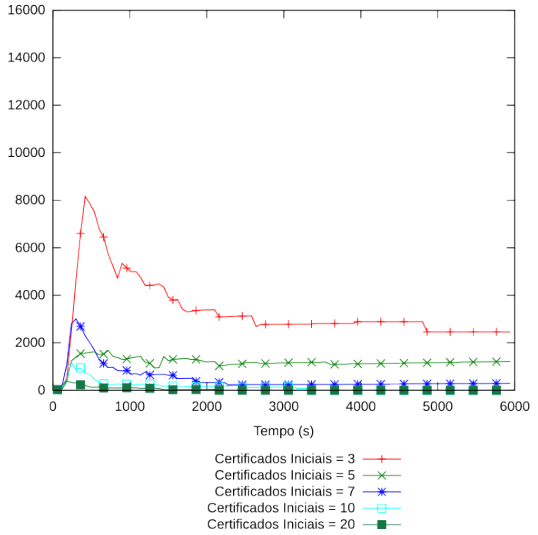



(d) Tamanho médio das cadeias

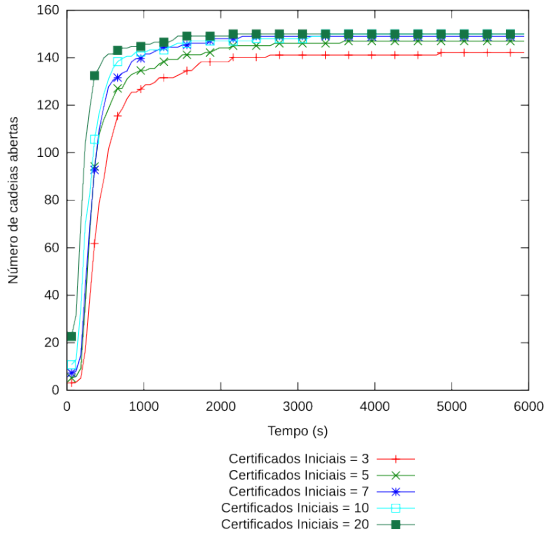
Figura C.7: Resultados para 100 nodos, $m = 10\%$ e $t = 25\%$



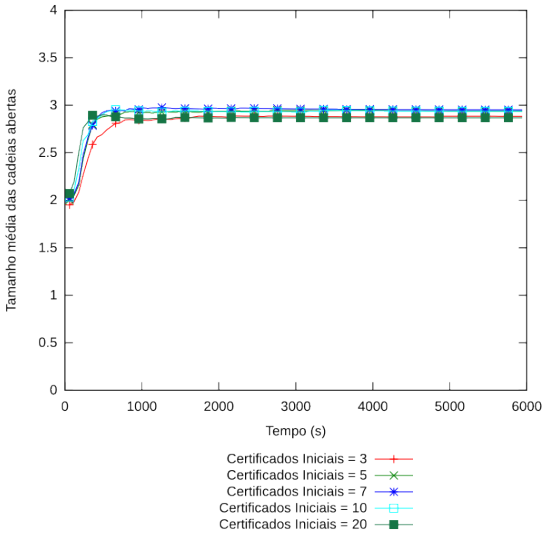

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



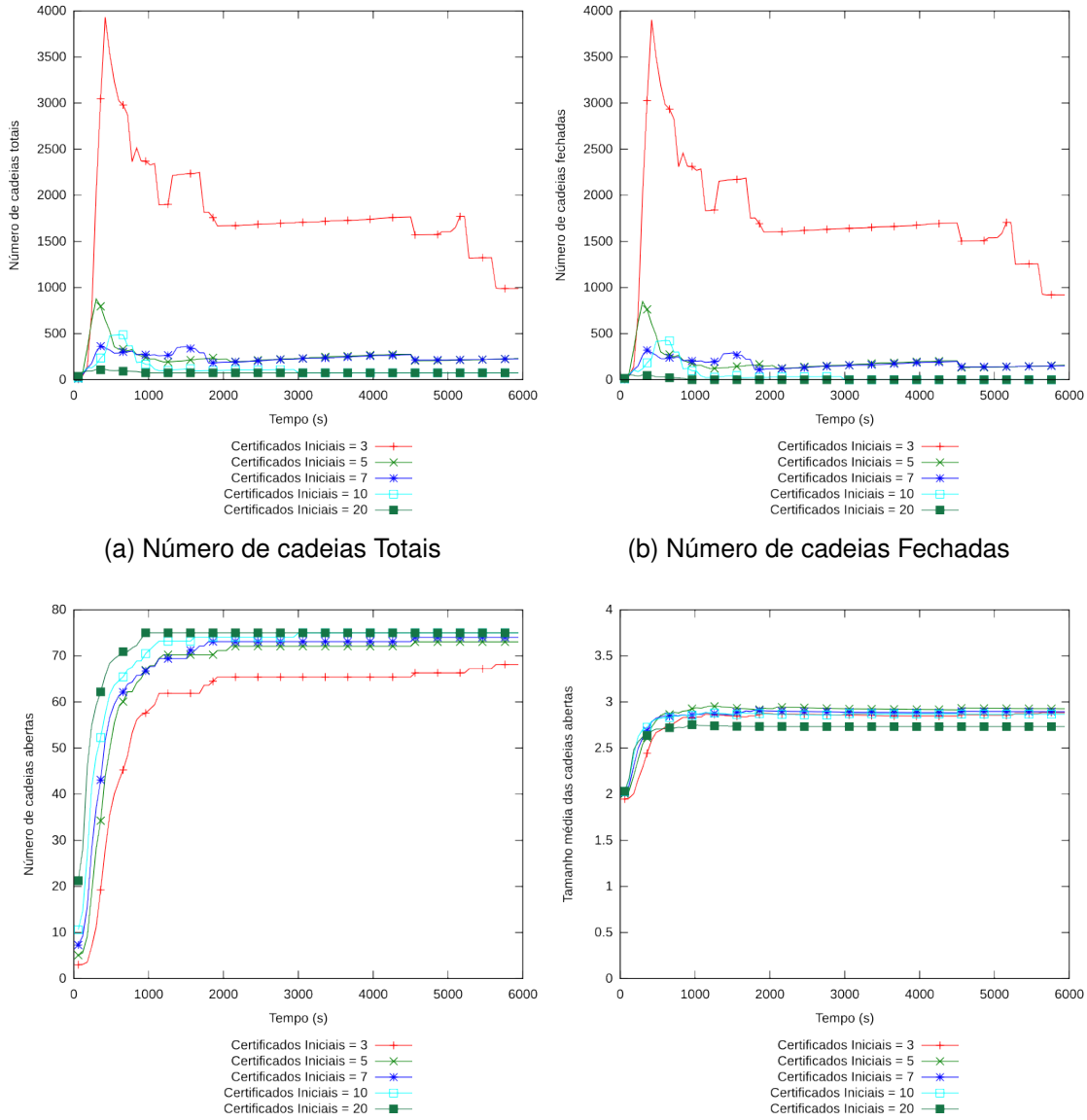

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.8: Resultados para 150 nodos, $m = 10\%$ e $t = 25\%$

### C.2.3 Ataque *GreyHole* com $m = 10\%$ e $t = 50\%$



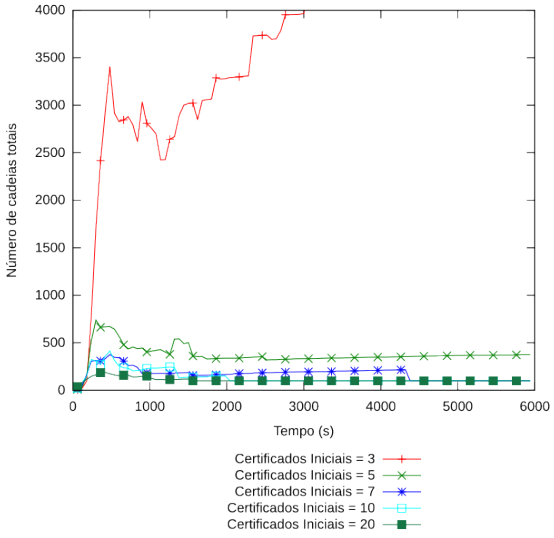

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

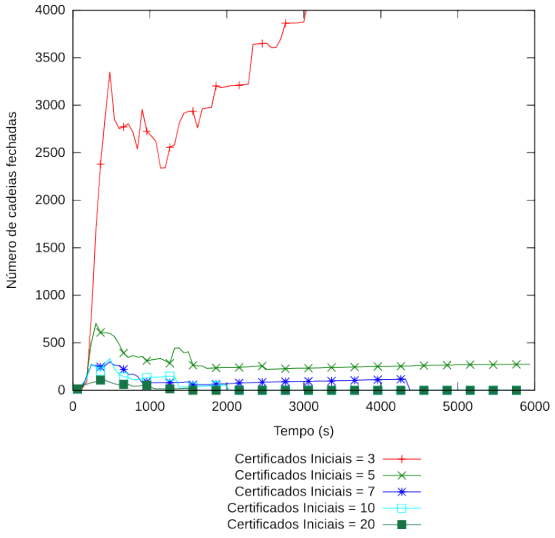
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

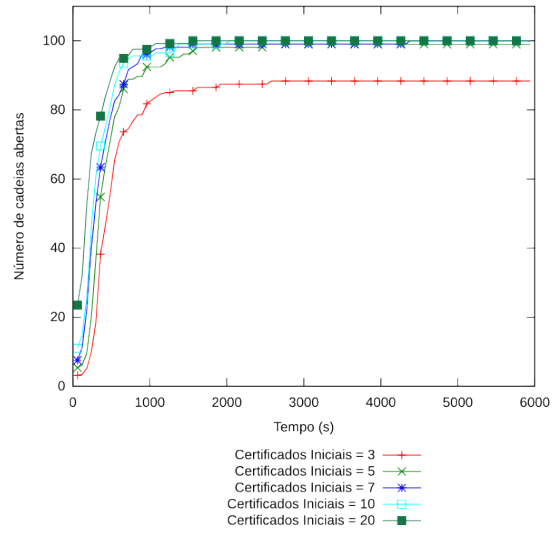
Figura C.9: Resultados para 75 nodos, $m = 10\%$ e $t = 50\%$



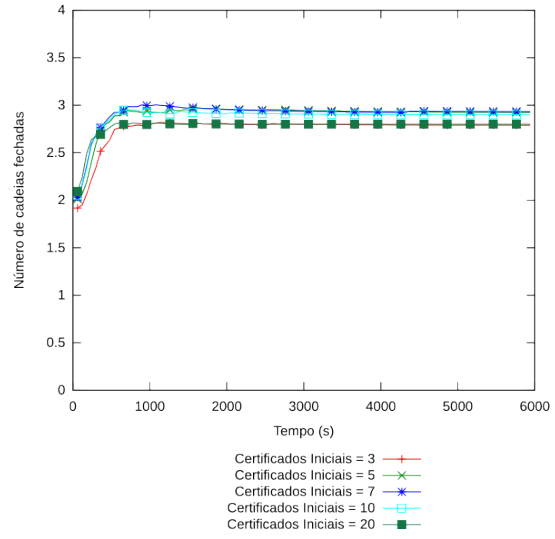

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



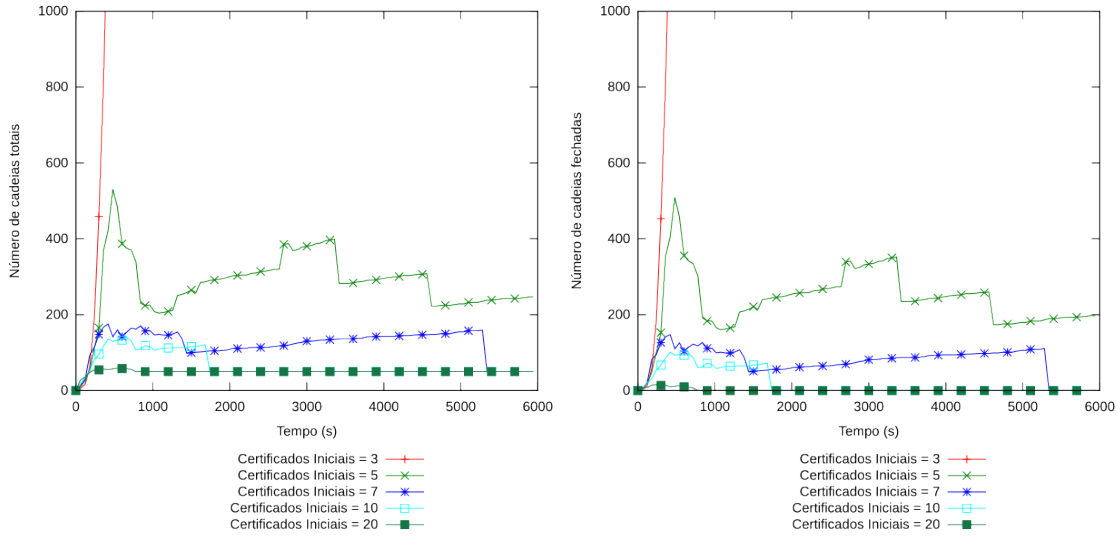

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.10: Resultados para 100 nodos, $m = 10\%$ e $t = 50\%$

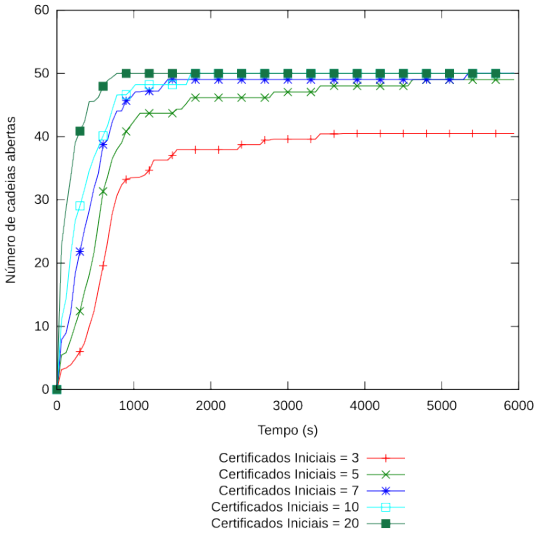
### C.2.4 Ataque *GreyHole* com $m = 20\%$ e $t = 10\%$



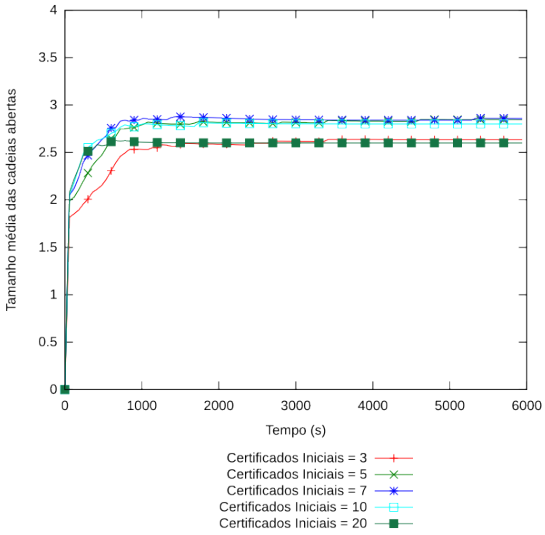

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

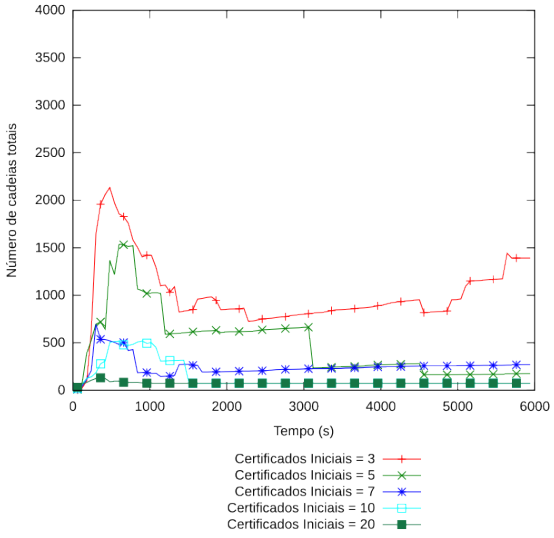



(c) Número de cadeias Abertas

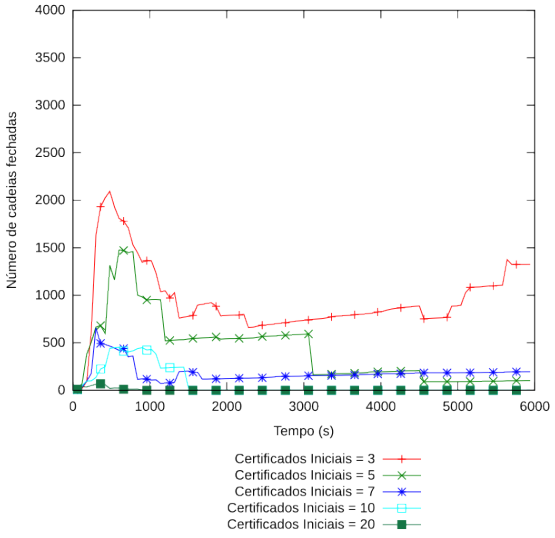



(d) Tamanho médio das cadeias

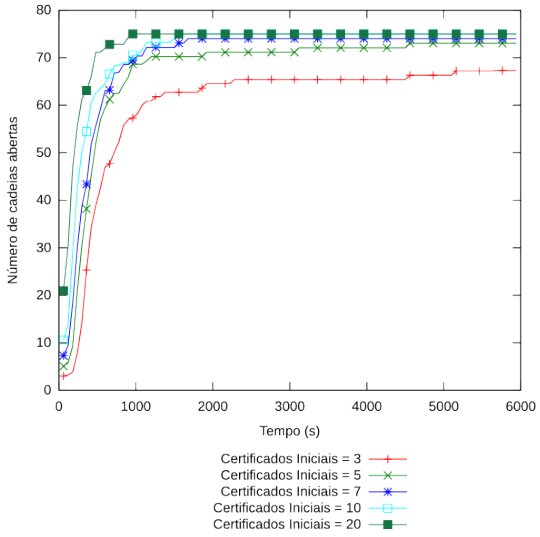
Figura C.11: Resultados para 50 nodos, $m = 20\%$ e $t = 10\%$



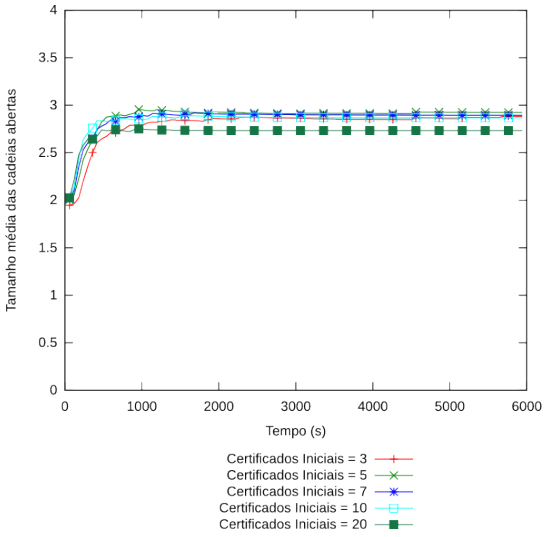

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

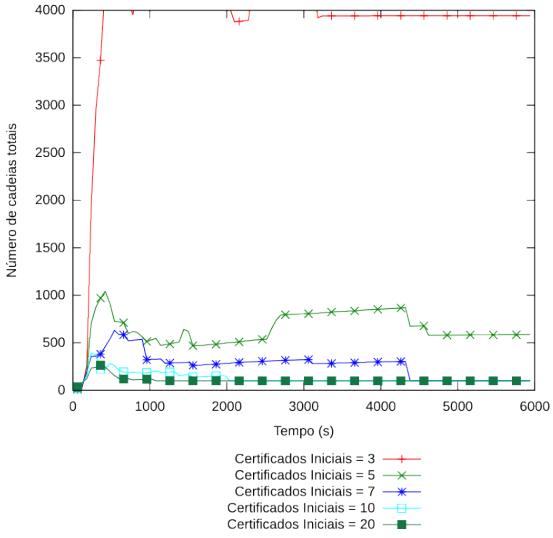



(c) Número de cadeias Abertas

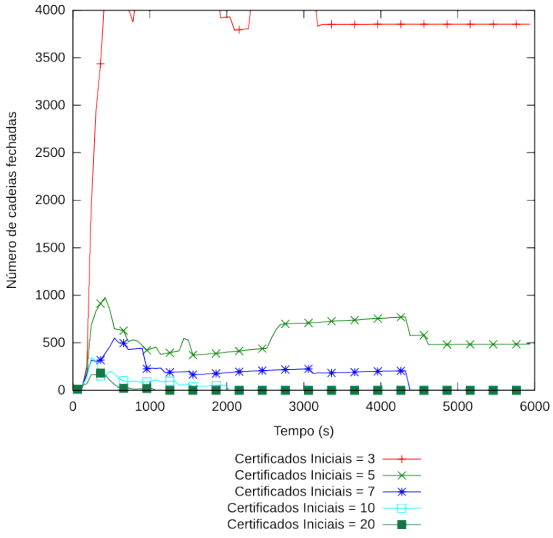



(d) Tamanho médio das cadeias

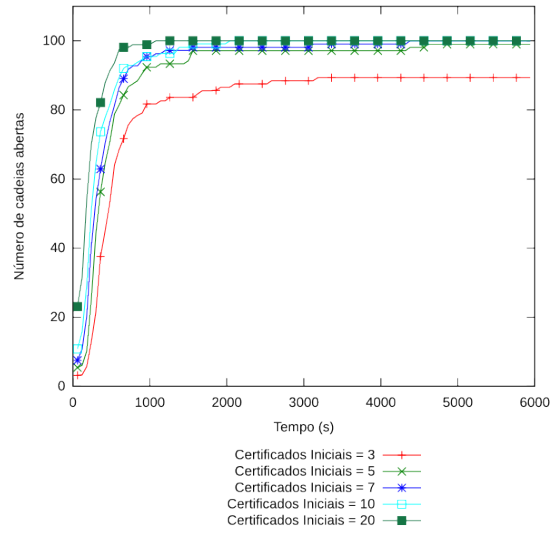
Figura C.12: Resultados para 75 nodos, $m = 20\%$ e $t = 10\%$



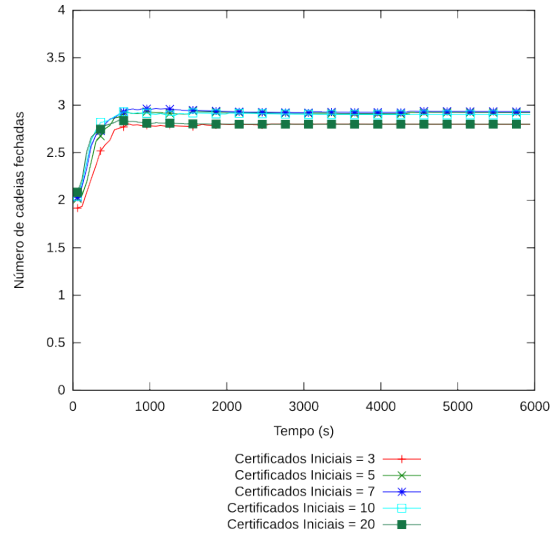

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

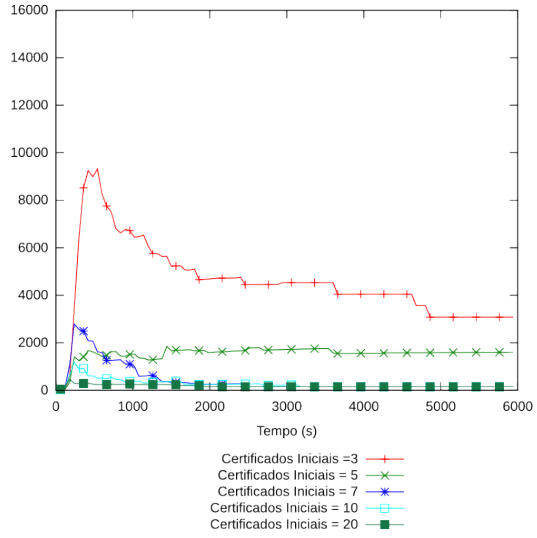



(c) Número de cadeias Abertas

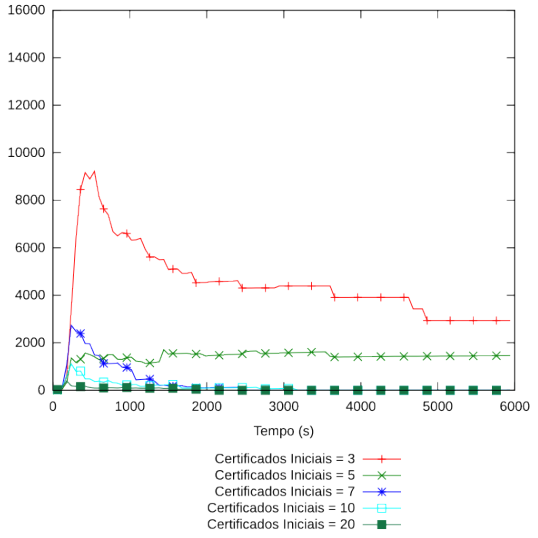



(d) Tamanho médio das cadeias

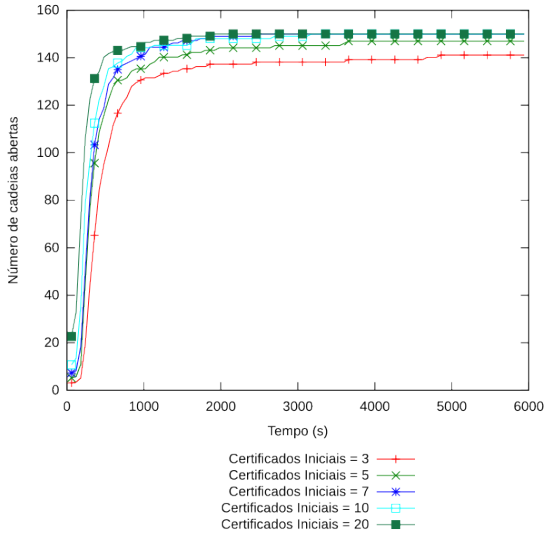
Figura C.13: Resultados para 100 nodos, $m = 20\%$ e $t = 10\%$



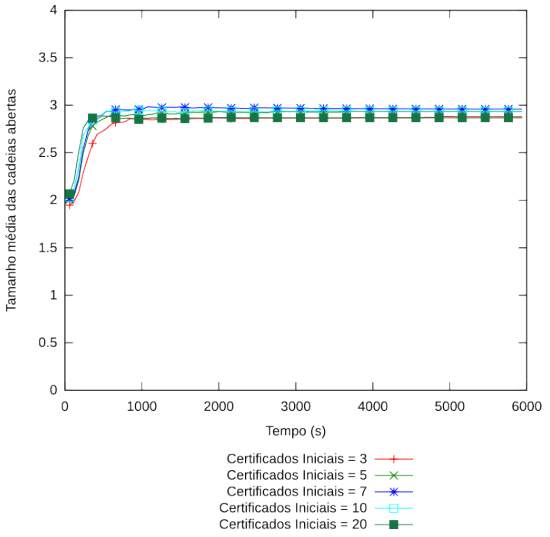

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



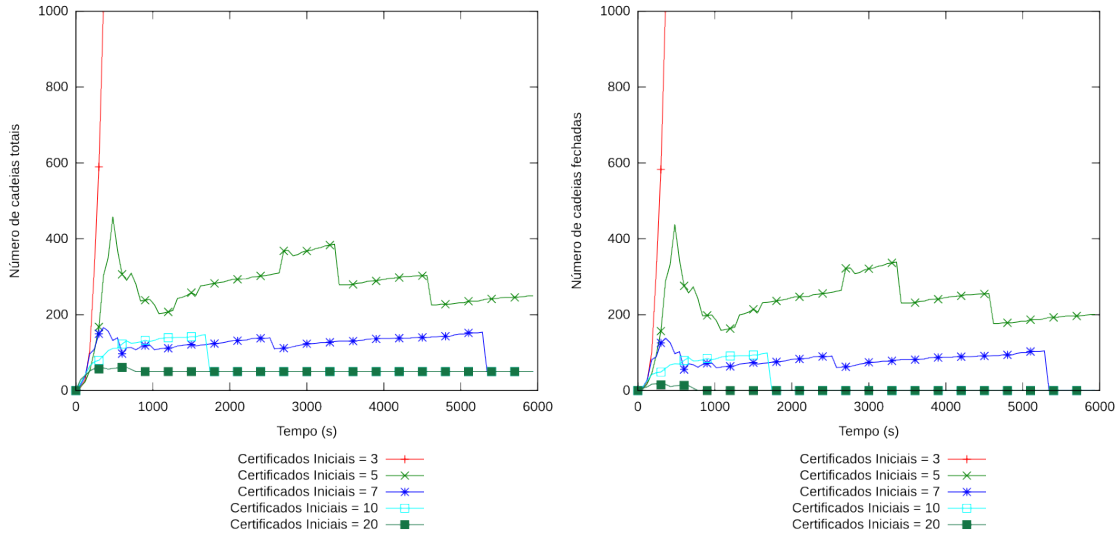

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.14: Resultados para 150 nodos, $m = 20\%$ e $t = 10\%$

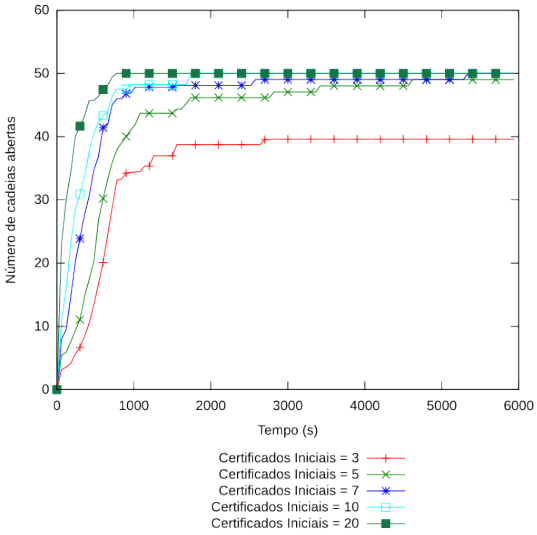
### C.2.5 Ataque *GreyHole* com $m = 20\%$ e $t = 25\%$



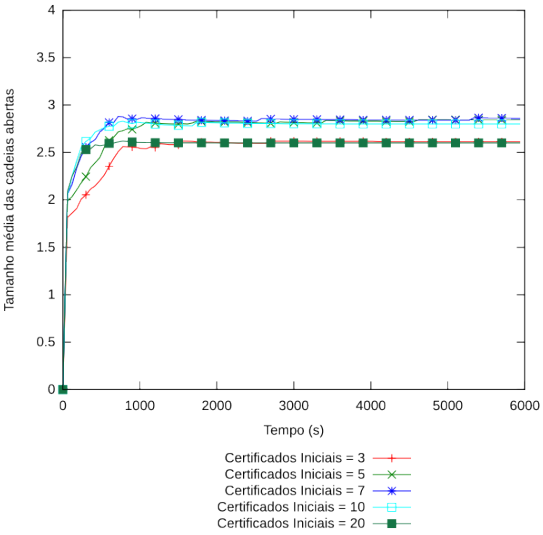

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

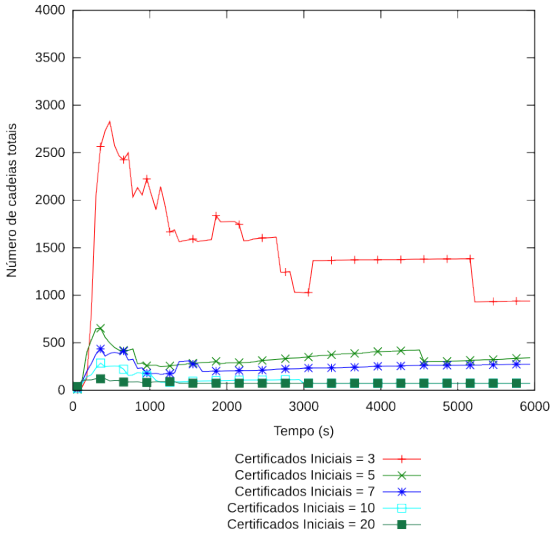



(c) Número de cadeias Abertas

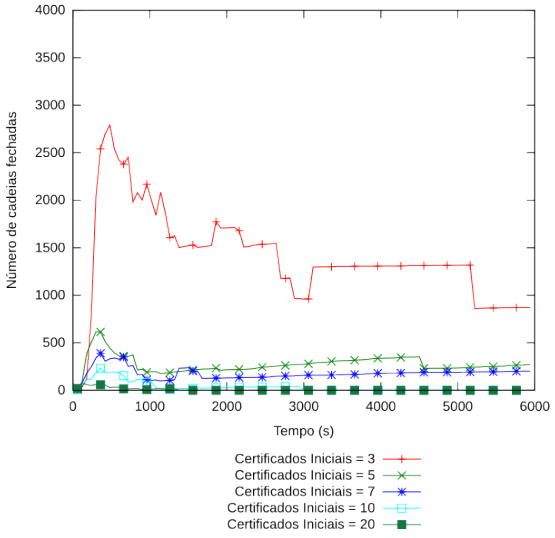



(d) Tamanho médio das cadeias

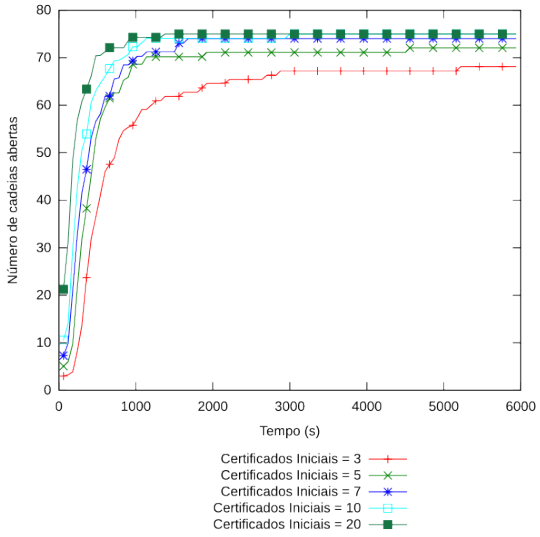
Figura C.15: Resultados para 50 nodos, $m = 20\%$ e $t = 25\%$



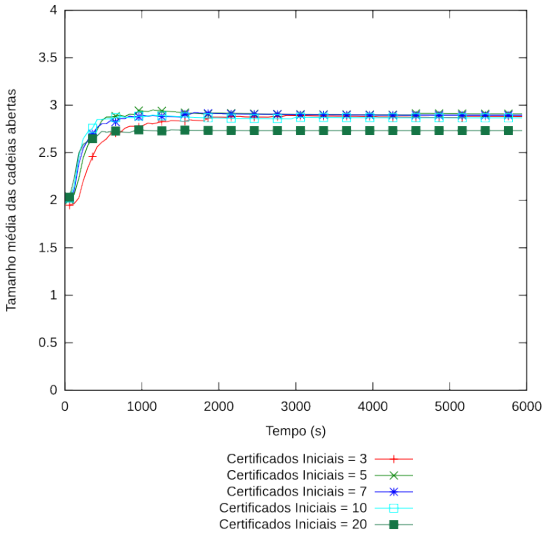

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

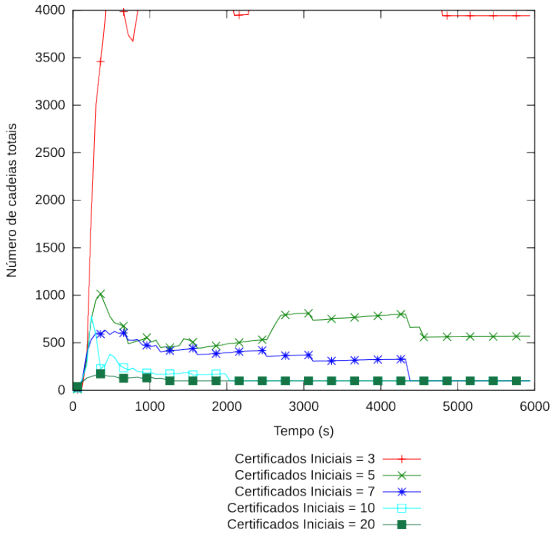



(c) Número de cadeias Abertas

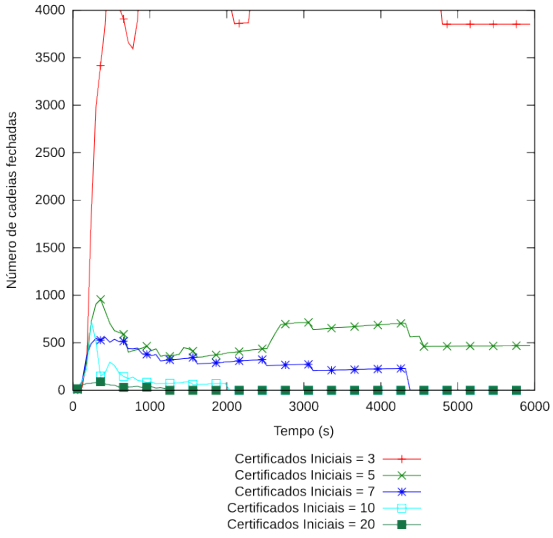



(d) Tamanho médio das cadeias

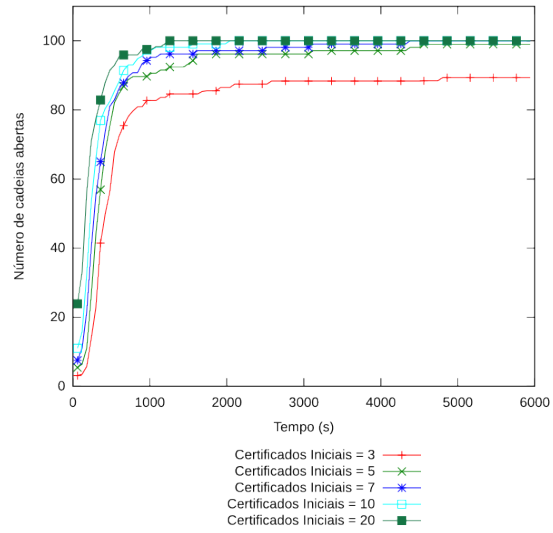
Figura C.16: Resultados para 75 nodos, $m = 20\%$ e $t = 25\%$



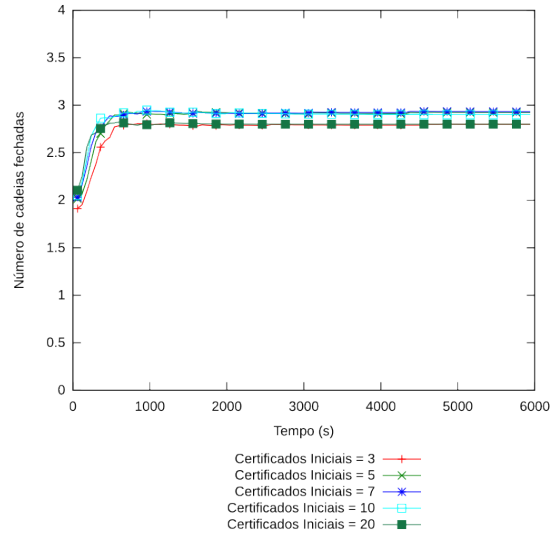

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

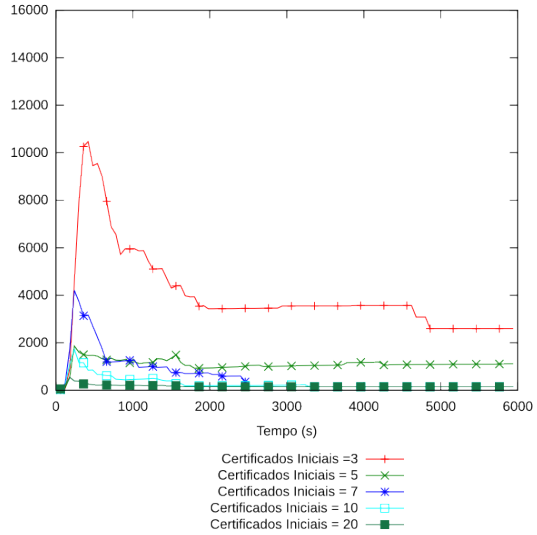



(c) Número de cadeias Abertas

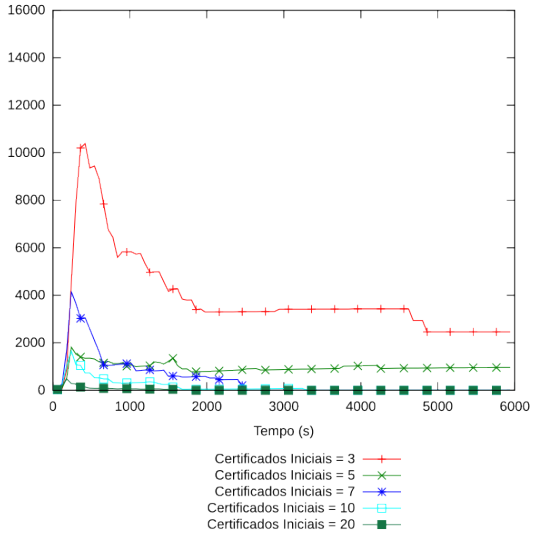



(d) Tamanho médio das cadeias

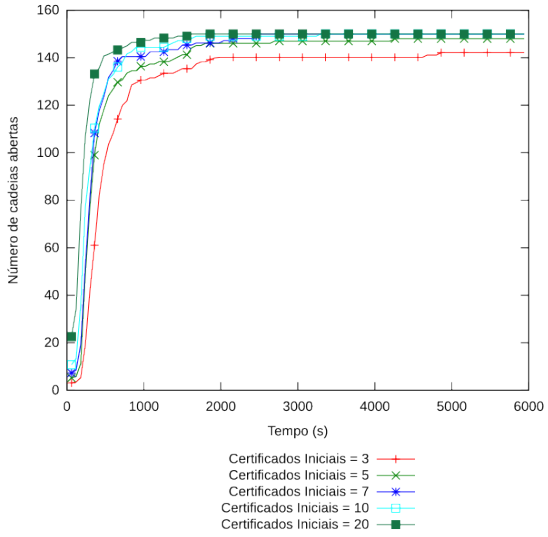
Figura C.17: Resultados para 100 nodos, $m = 20\%$ e $t = 25\%$



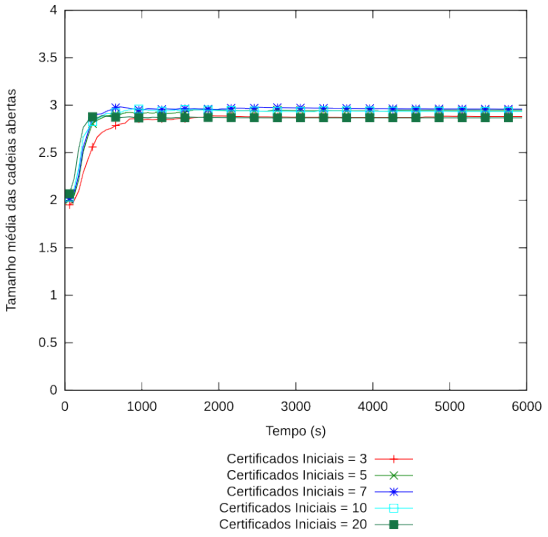

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



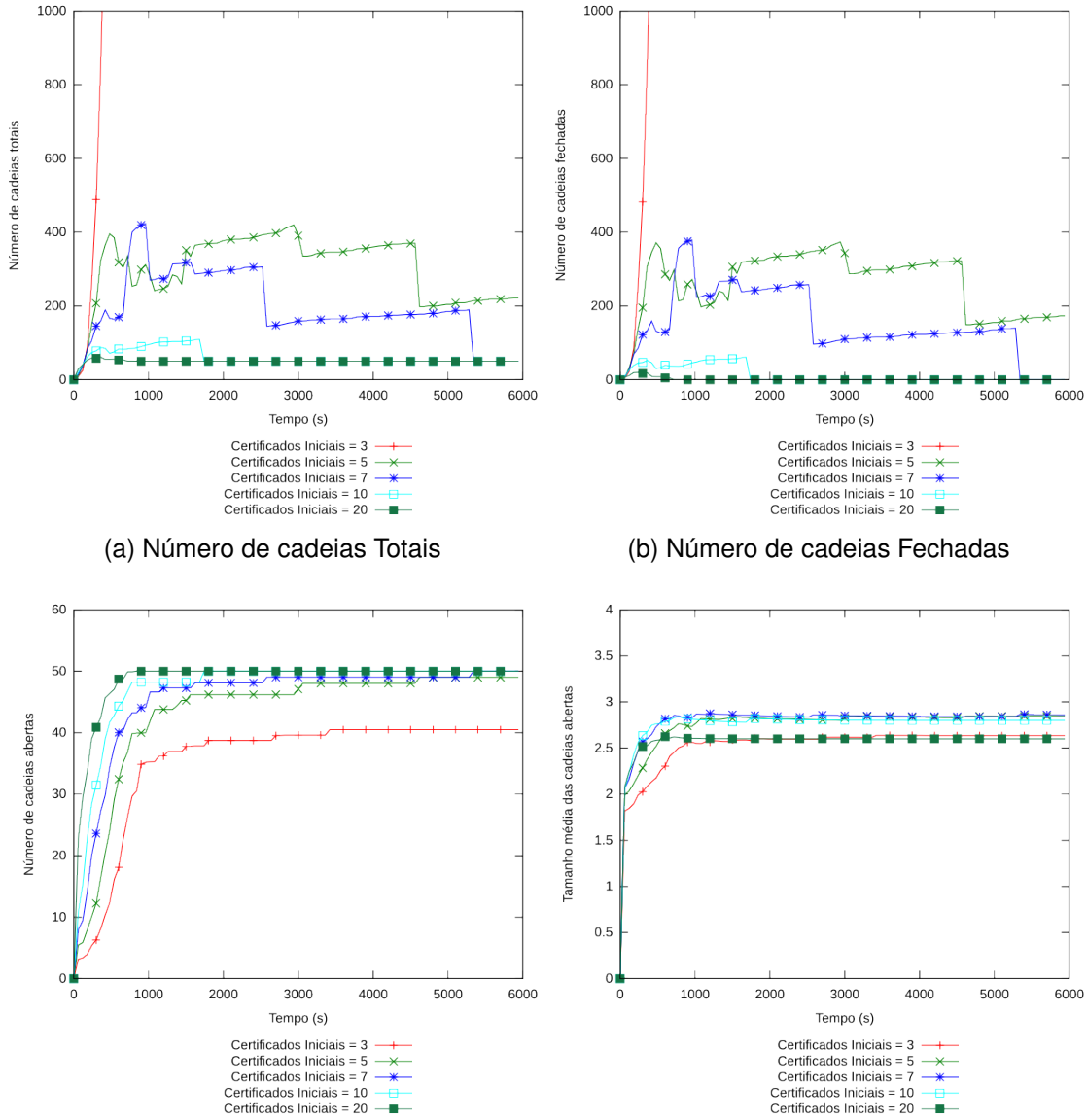

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.18: Resultados para 150 nodos, $m = 20\%$ e $t = 25\%$

### C.2.6 Ataque *GreyHole* com $m = 20\%$ e $t = 50\%$



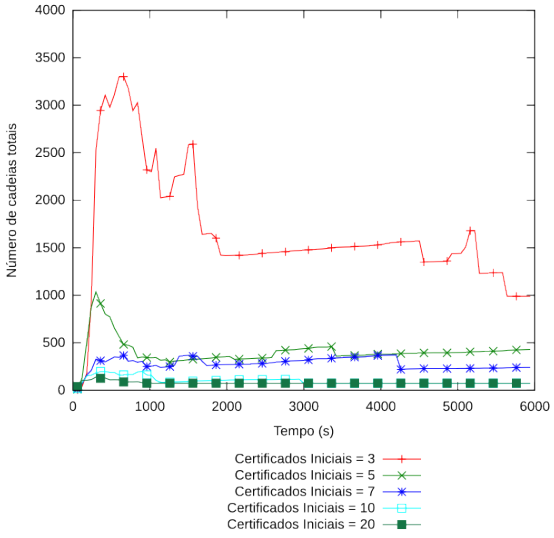

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

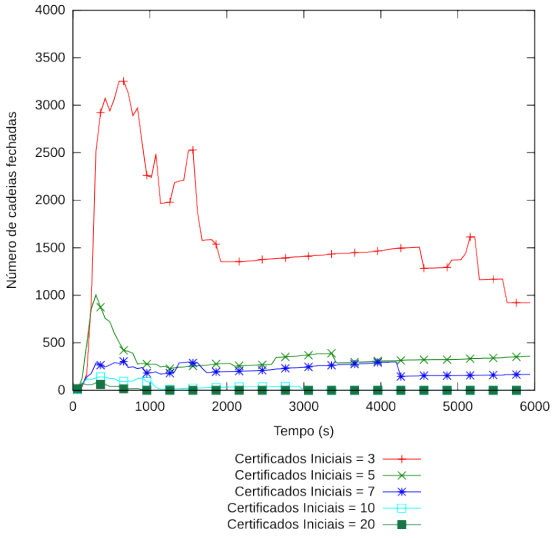
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

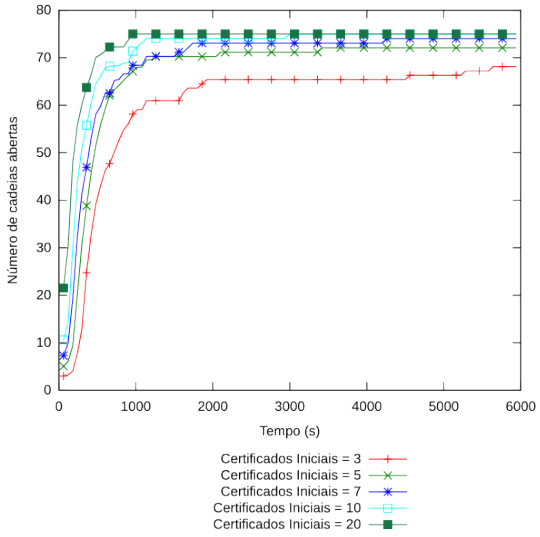
Figura C.19: Resultados para 50 nodos, $m = 20\%$ e $t = 50\%$



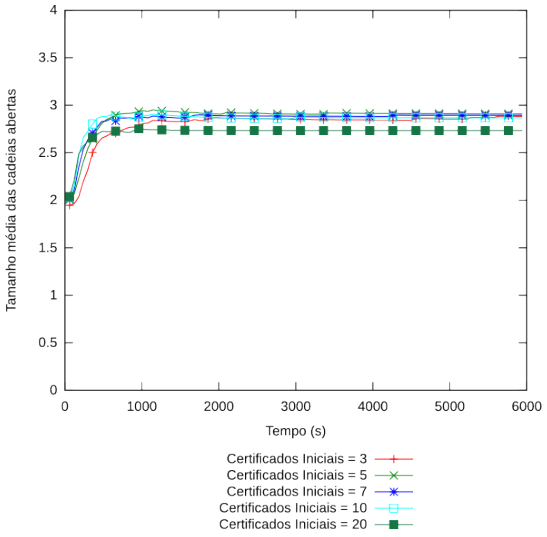

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

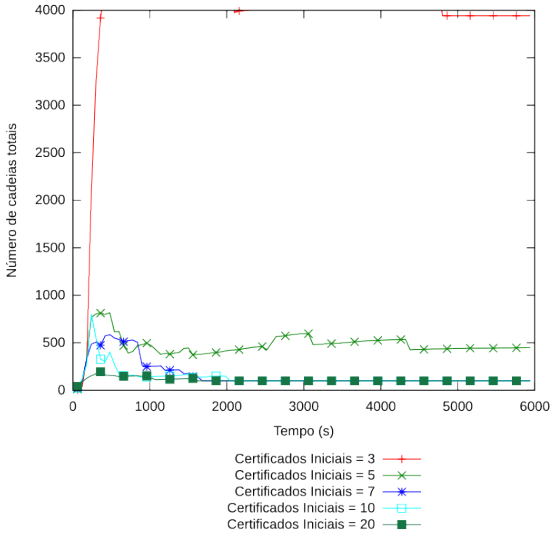



(c) Número de cadeias Abertas

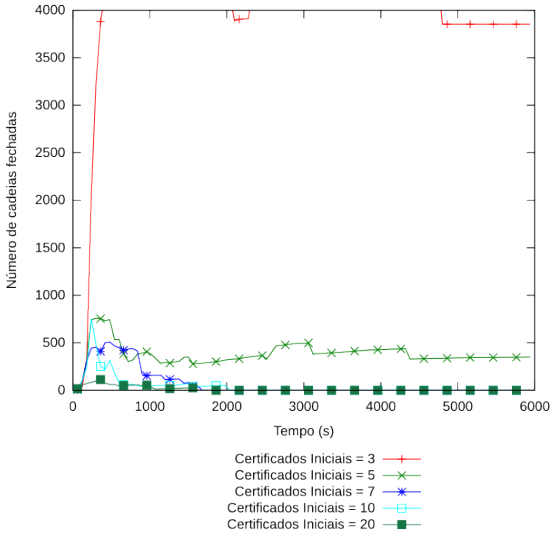



(d) Tamanho médio das cadeias

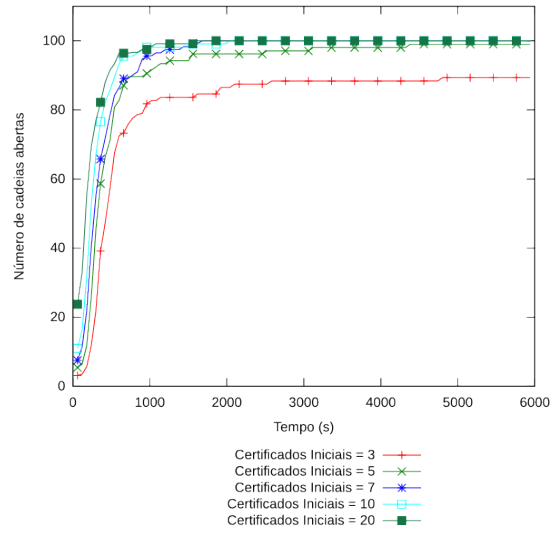
Figura C.20: Resultados para 75 nodos, $m = 20\%$ e $t = 50\%$



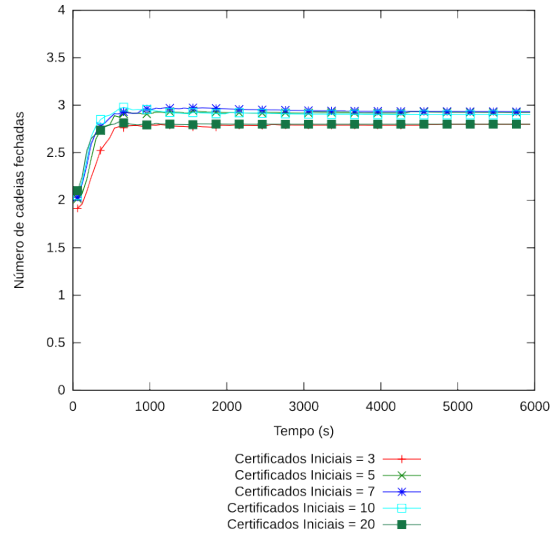

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

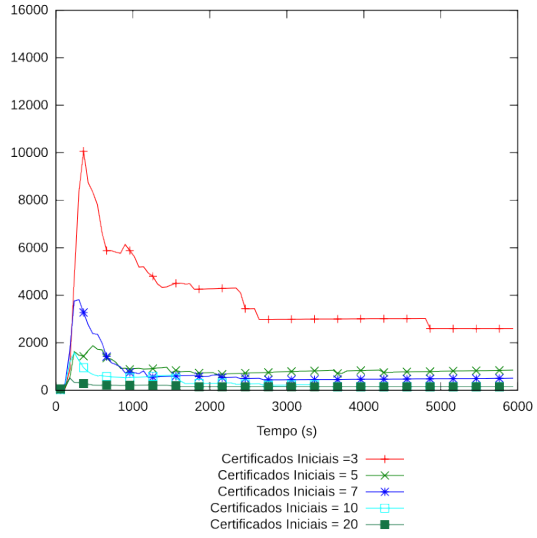



(c) Número de cadeias Abertas

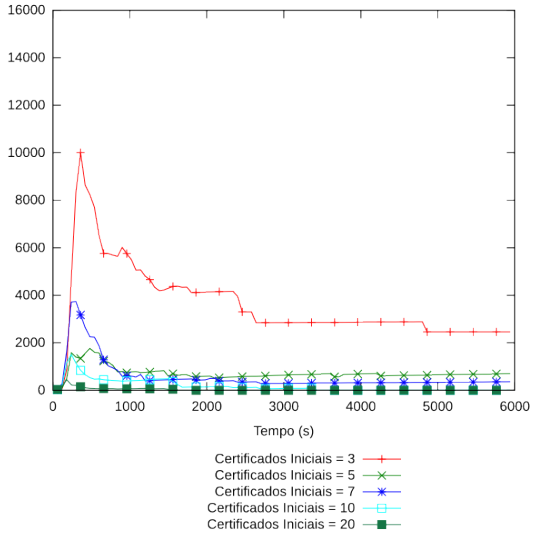



(d) Tamanho médio das cadeias

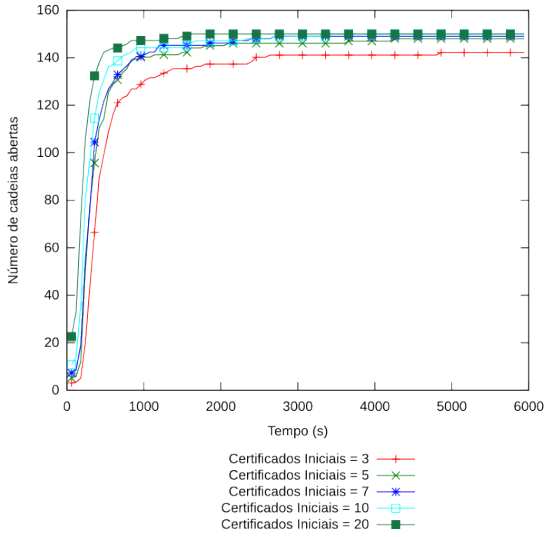
Figura C.21: Resultados para 100 nodos, $m = 20\%$ e $t = 50\%$



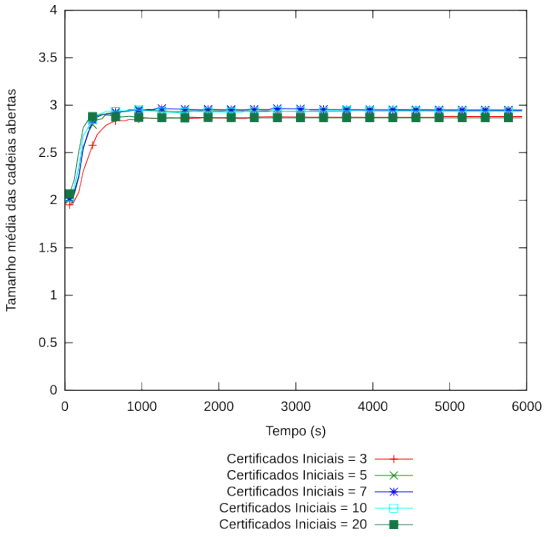

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



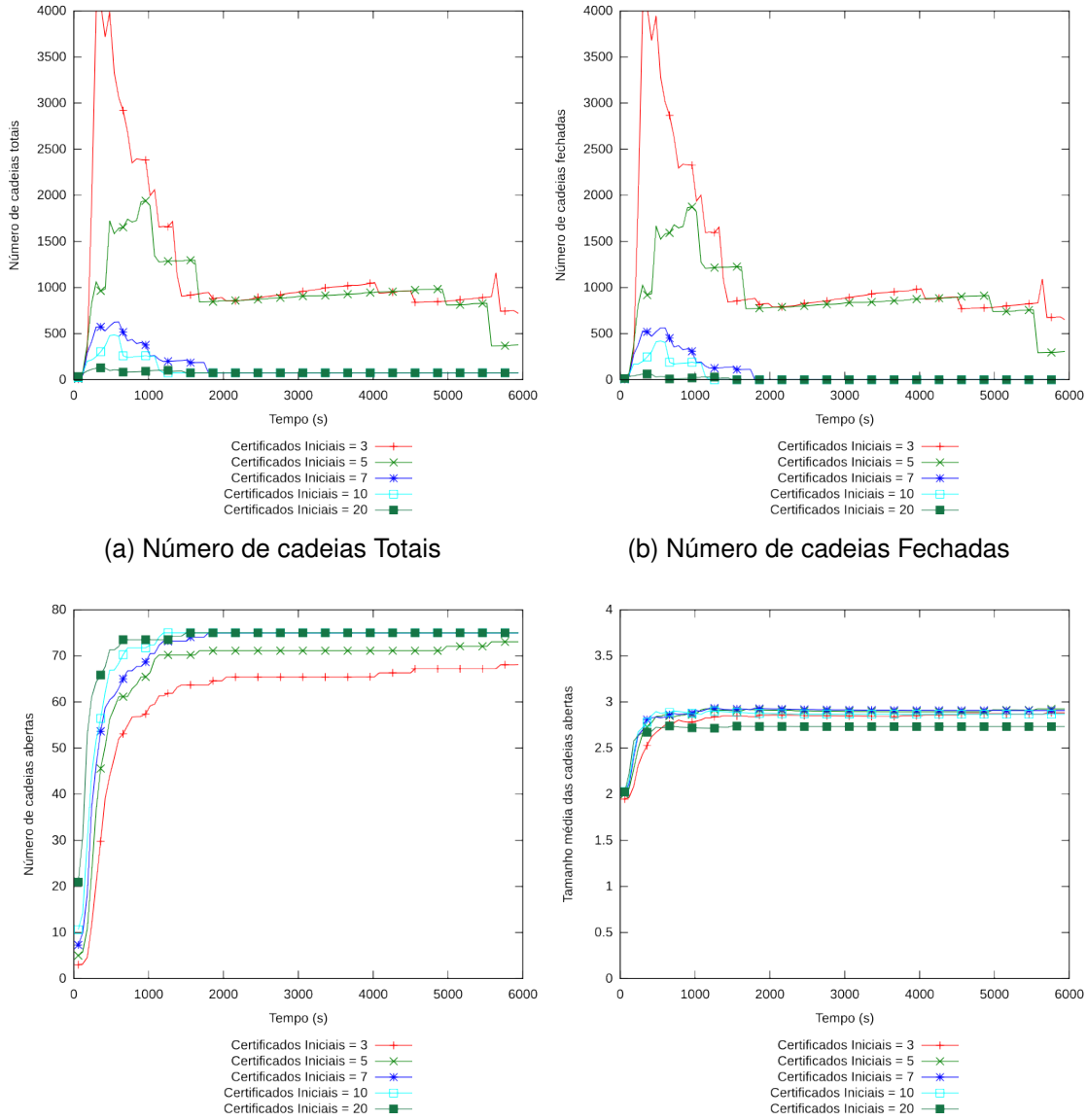

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.22: Resultados para 150 nodos, $m = 20\%$ e $t = 50\%$

### C.2.7 Ataque *GreyHole* com $m = 50\%$ e $t = 10\%$



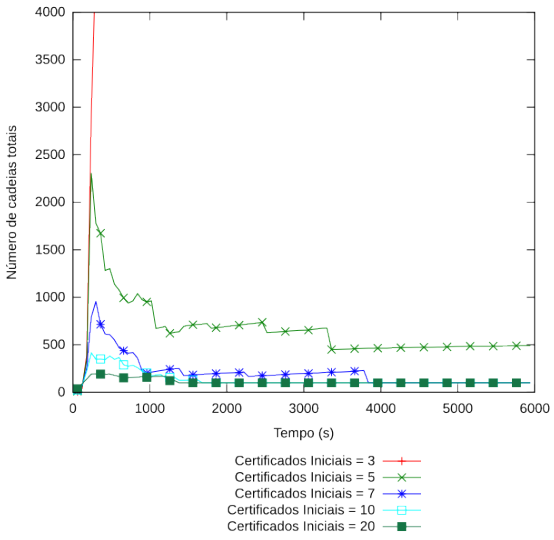

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

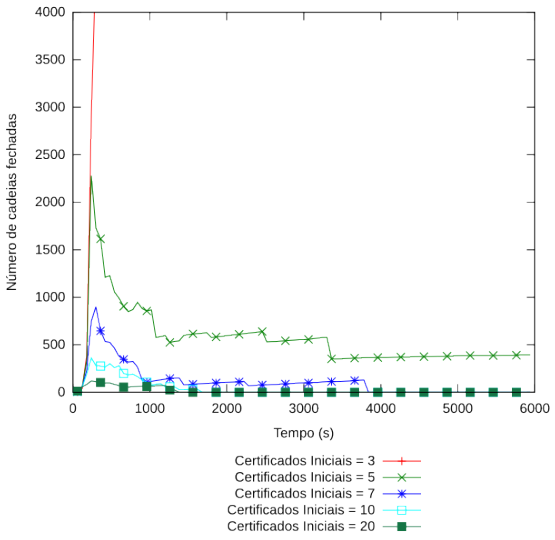
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

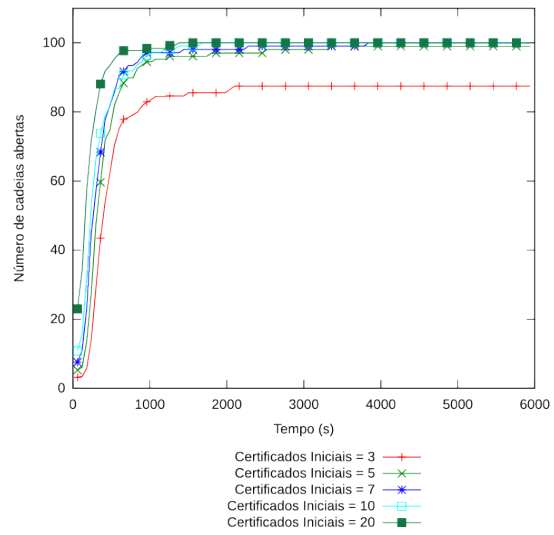
Figura C.23: Resultados para 75 nodos, $m = 50\%$ e $t = 10\%$



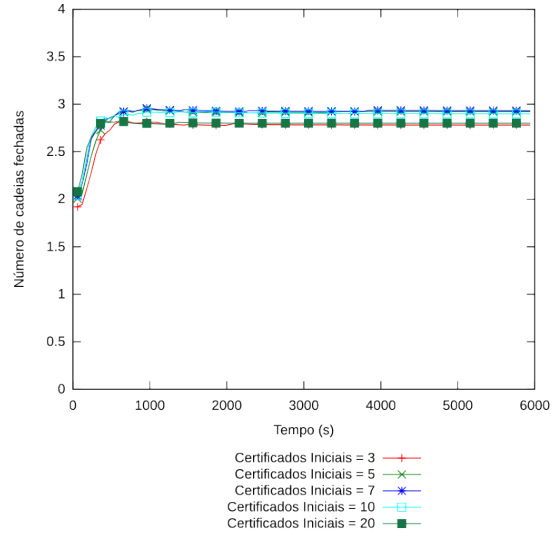

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



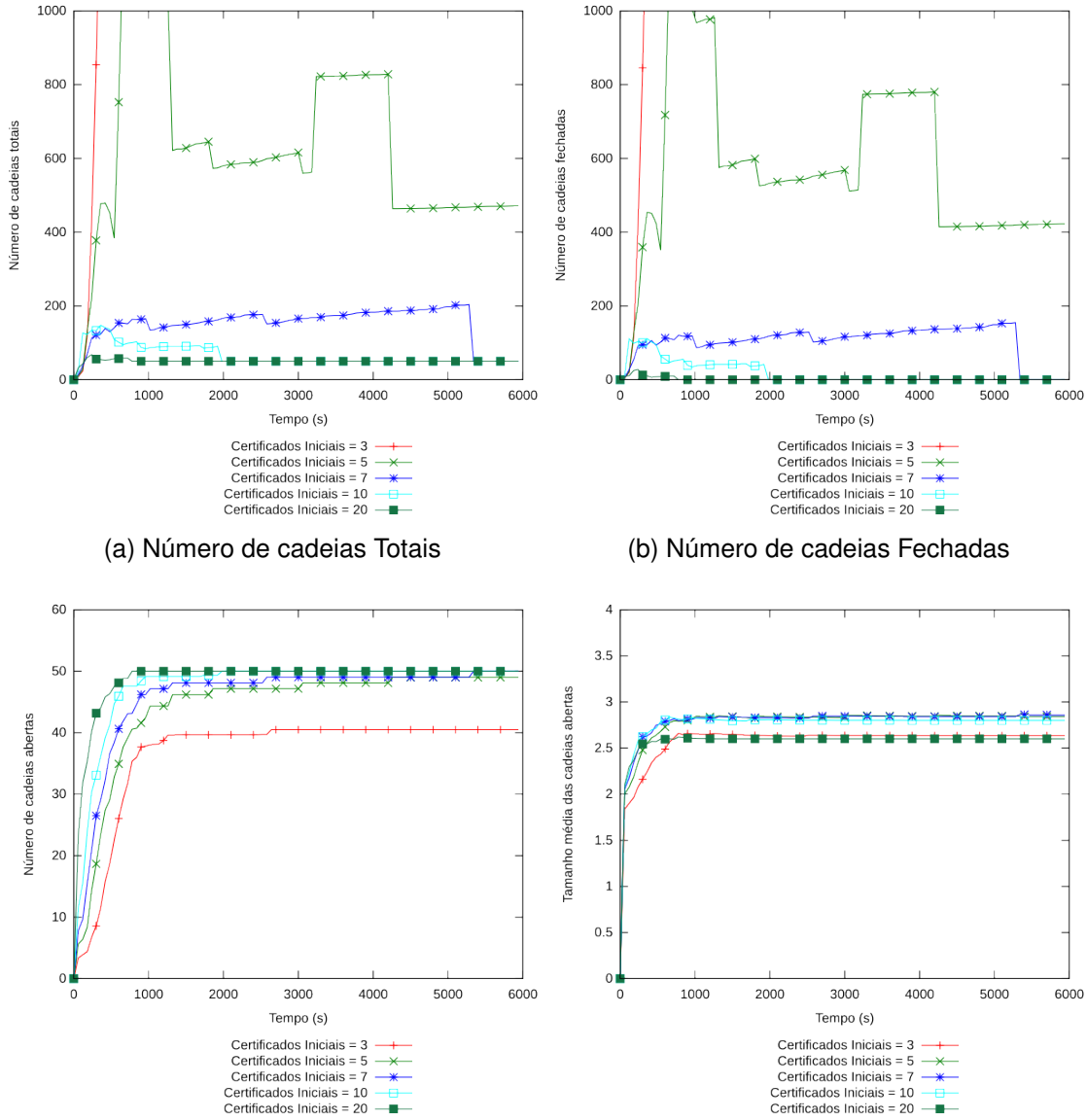

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.24: Resultados para 100 nodos, $m = 50\%$ e $t = 10\%$

### C.2.8 Ataque *GreyHole* com $m = 50\%$ e $t = 25\%$



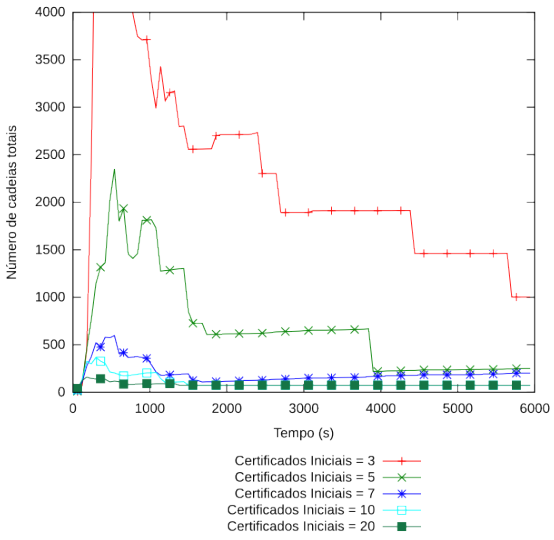

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

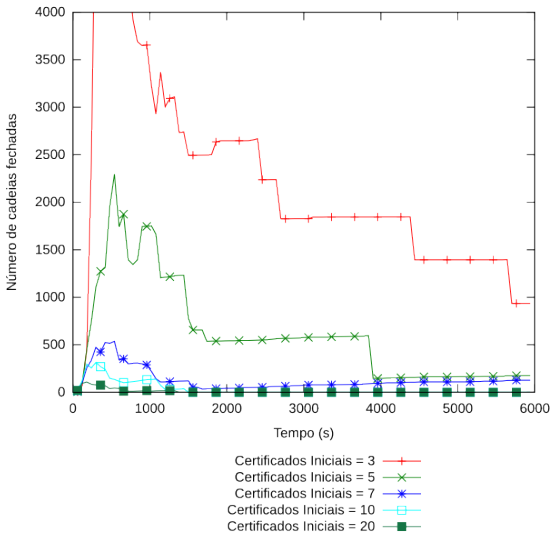
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

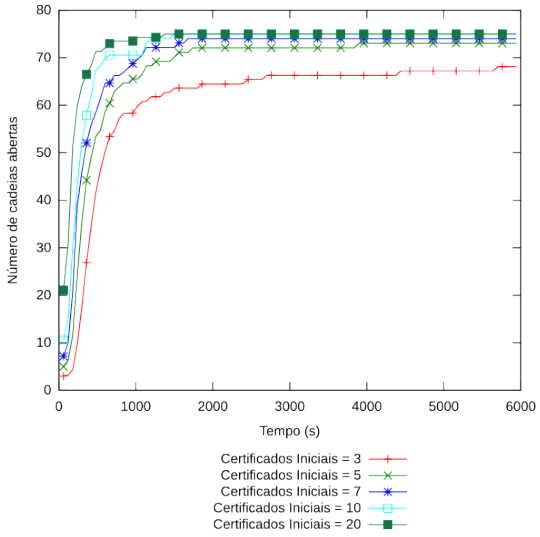
Figura C.25: Resultados para 50 nodos, $m = 50\%$ e $t = 25\%$



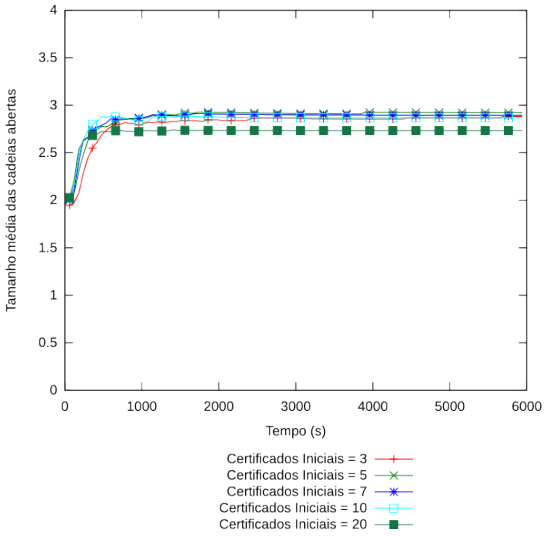

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

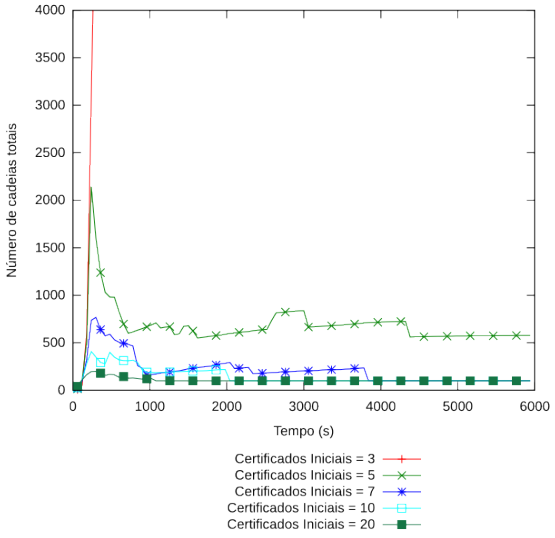



(c) Número de cadeias Abertas

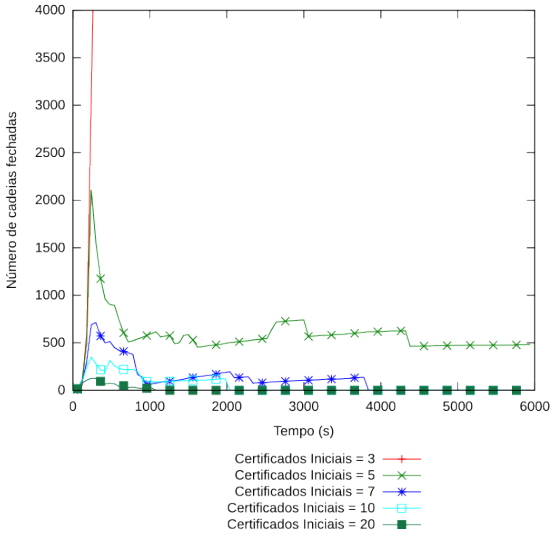



(d) Tamanho médio das cadeias

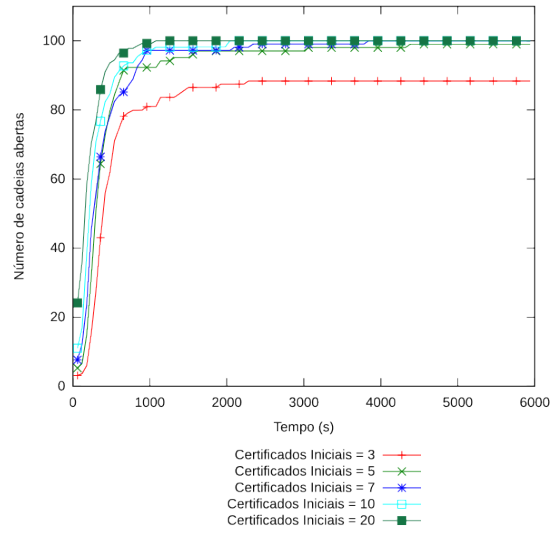
Figura C.26: Resultados para 75 nodos, $m = 50\%$ e $t = 25\%$



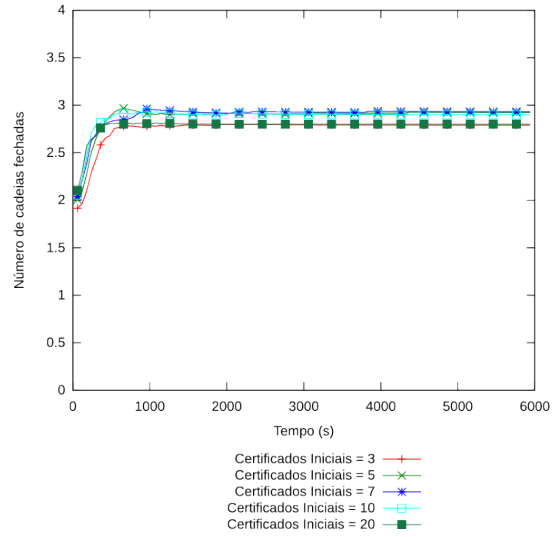

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

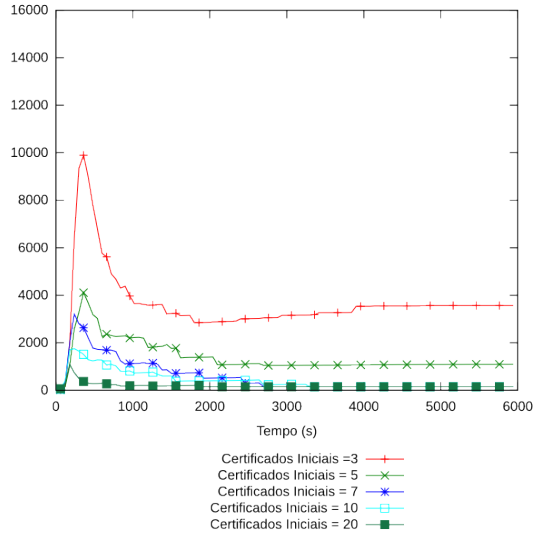



(c) Número de cadeias Abertas

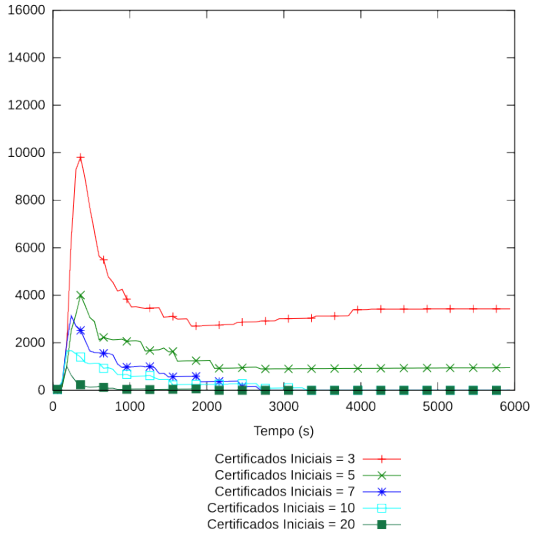



(d) Tamanho médio das cadeias

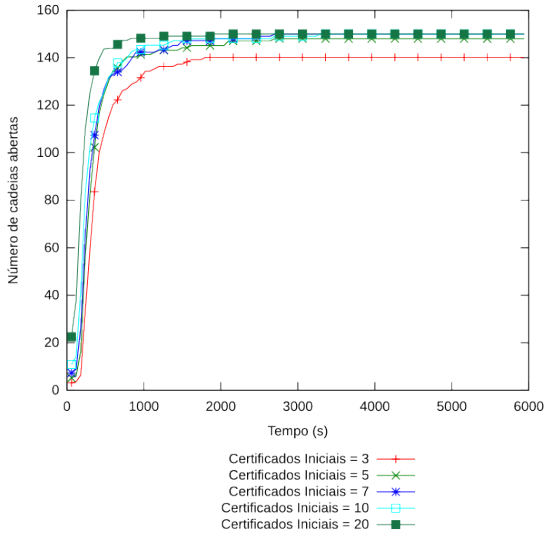
Figura C.27: Resultados para 100 nodos, $m = 50\%$ e $t = 25\%$



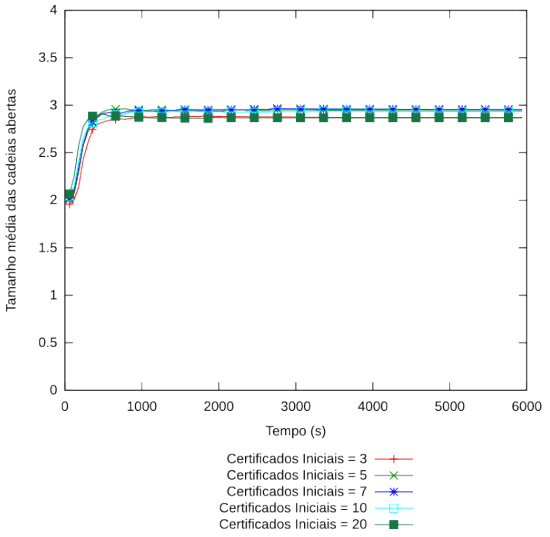

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



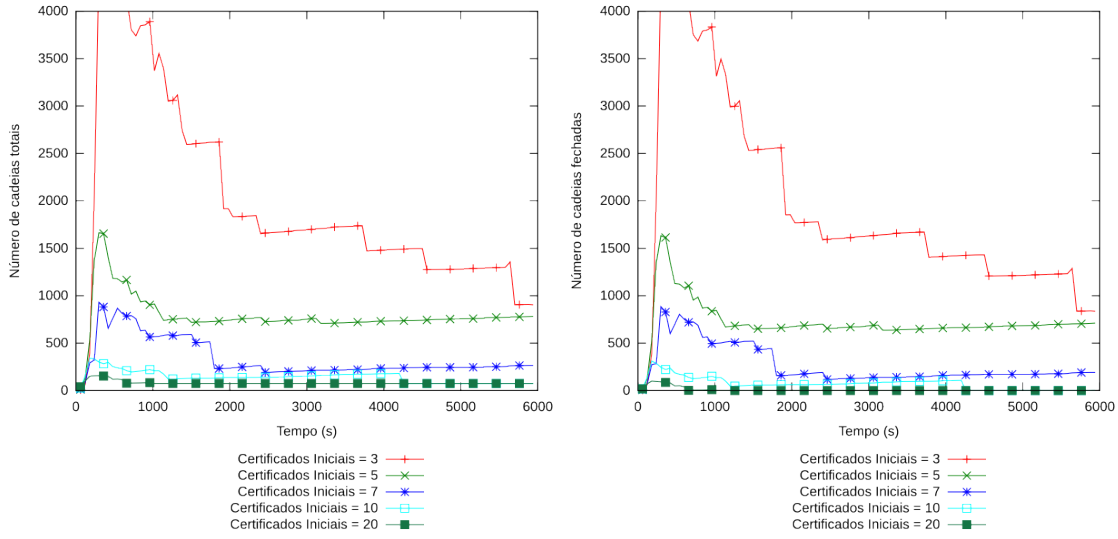

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.28: Resultados para 150 nodos, $m = 50\%$ e $t = 25\%$

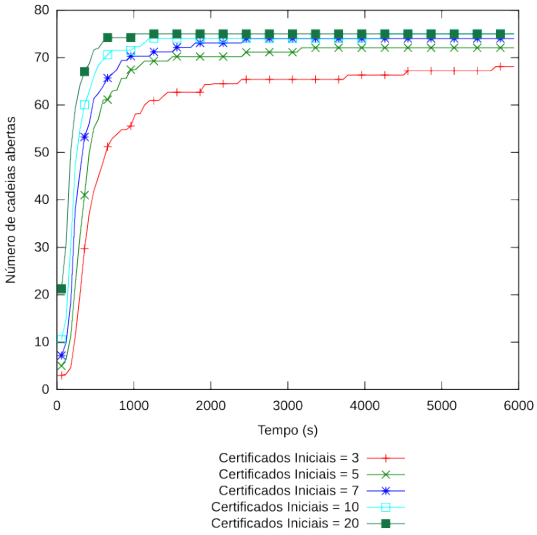
### C.2.9 Ataque *GreyHole* com $m = 50\%$ e $t = 50\%$



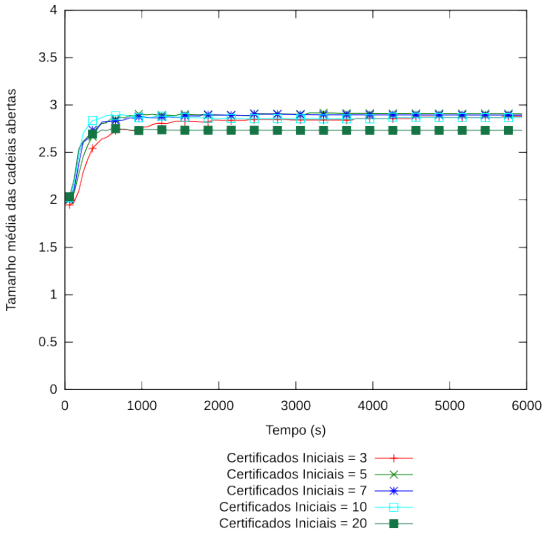

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

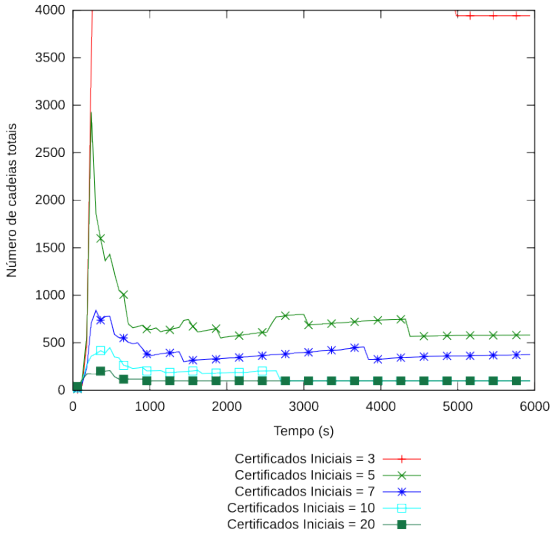



(c) Número de cadeias Abertas

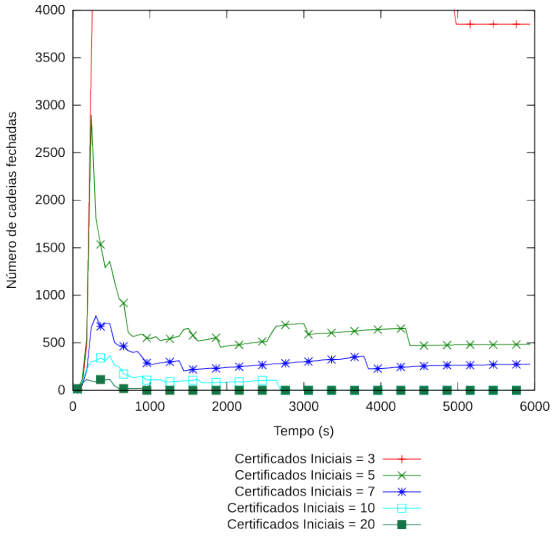



(d) Tamanho médio das cadeias

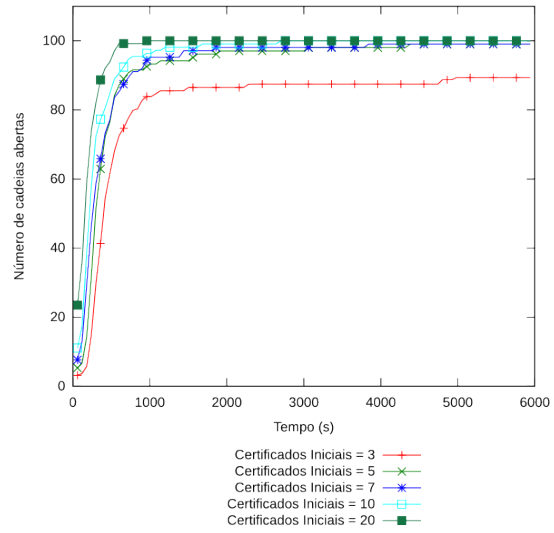
Figura C.29: Resultados para 75 nodos, $m = 50\%$ e $t = 50\%$



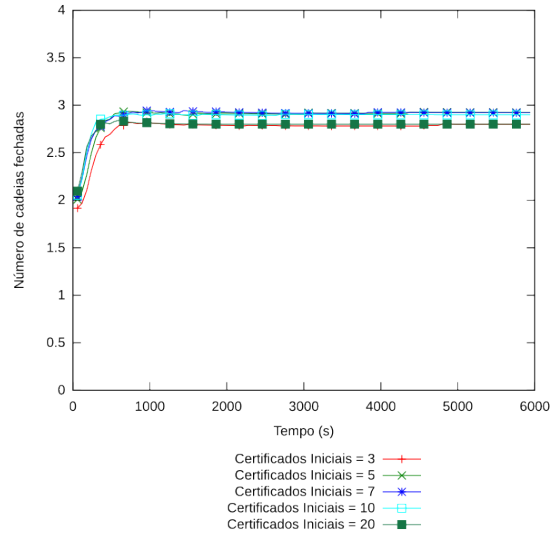

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

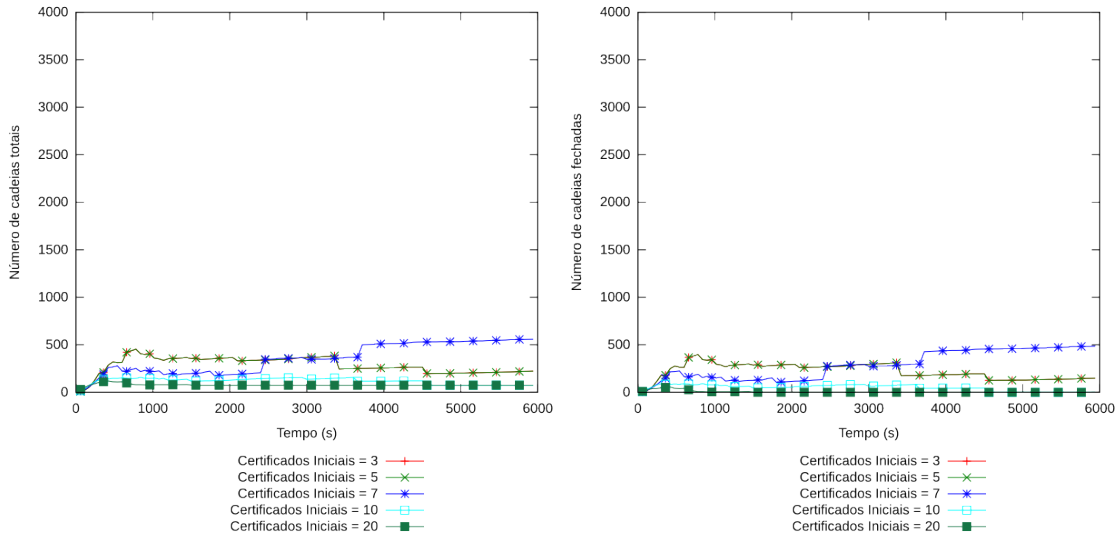



(d) Tamanho médio das cadeias

Figura C.30: Resultados para 100 nodos, $m = 50\%$ e $t = 50\%$

## C.3 Ataque *BlackHole*

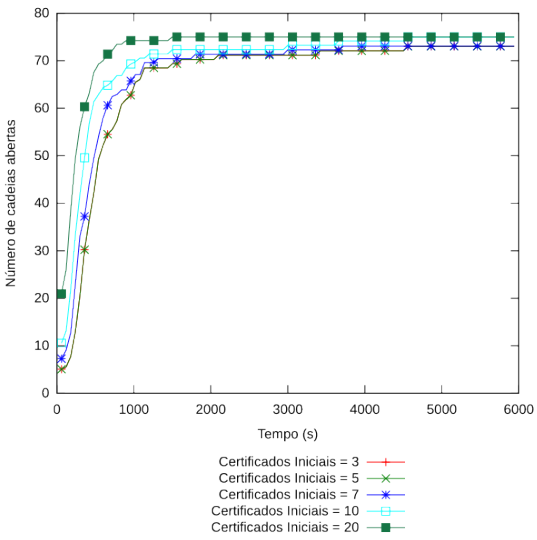
### C.3.1 Ataque *BlackHole* com $m = 10\%$



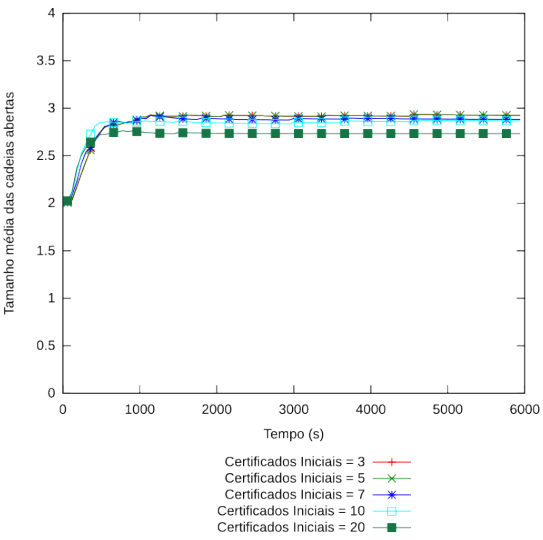

(a) Número de cadeias totais




(b) Número de cadeias fechadas

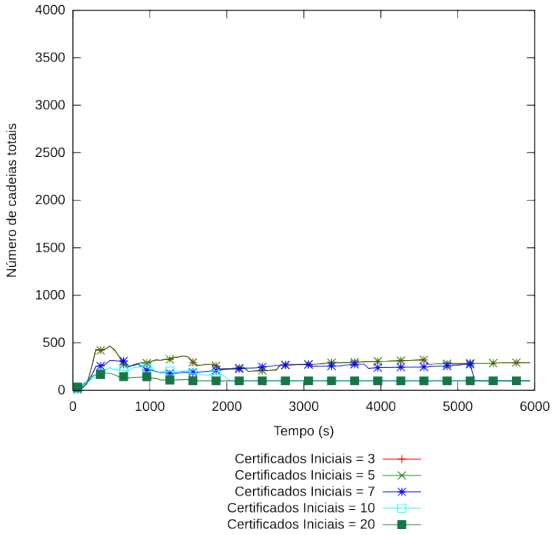



(c) Número de cadeias abertas

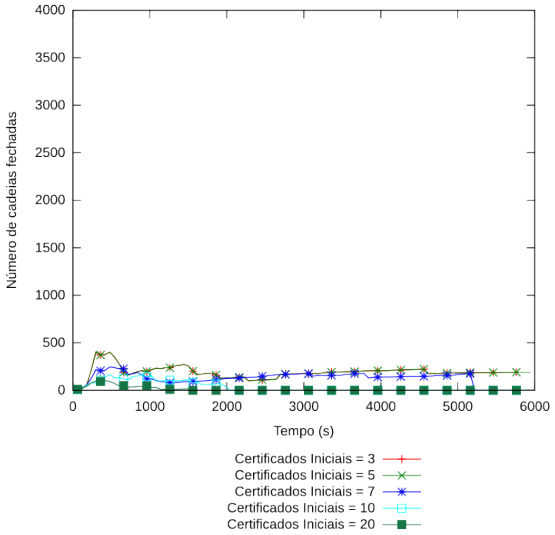



(d) Tamanho médio das cadeias

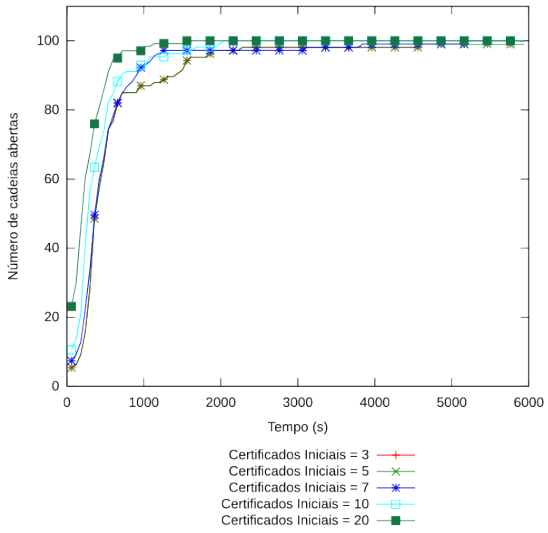
Figura C.31: Resultados para 75 nodos e $m = 10\%$



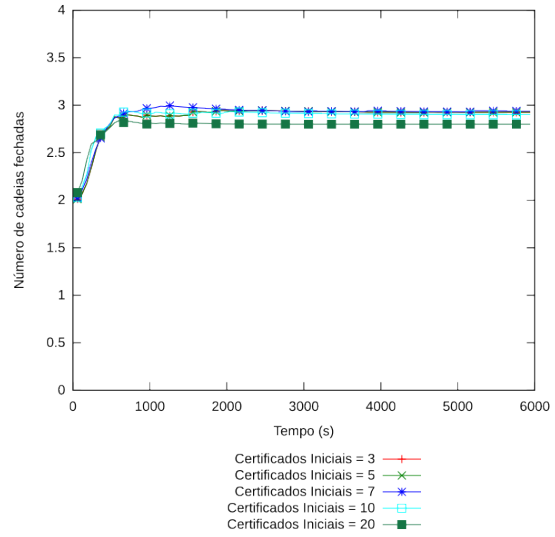

(a) Número de cadeias totais




(b) Número de cadeias fechadas



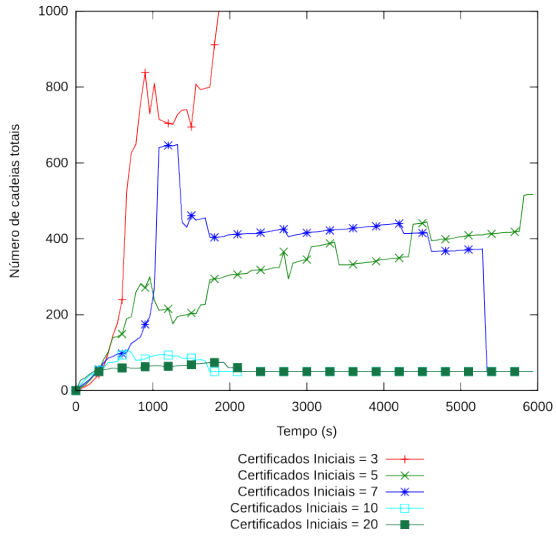

(c) Número de cadeias abertas



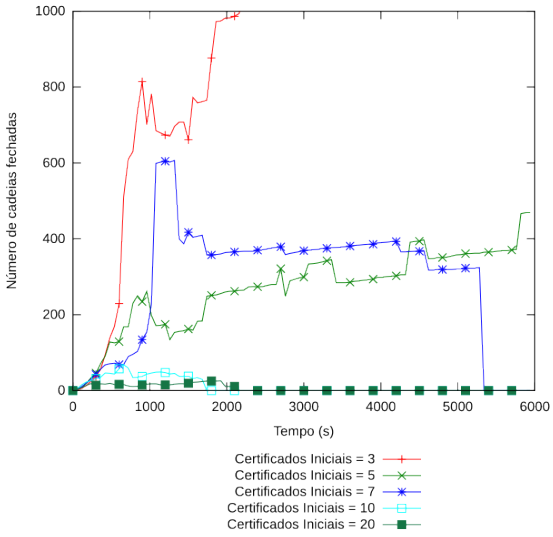

(d) Tamanho médio das cadeias

Figura C.32: Resultados para 100 nodos e $m = 10\%$

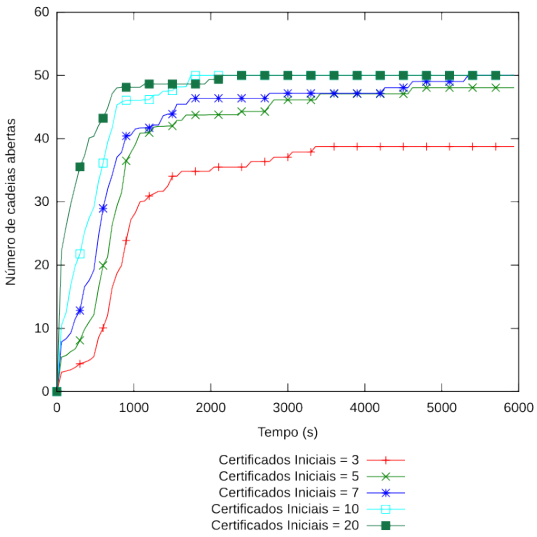
### C.3.2 Ataque *BlackHole* com $m = 20\%$



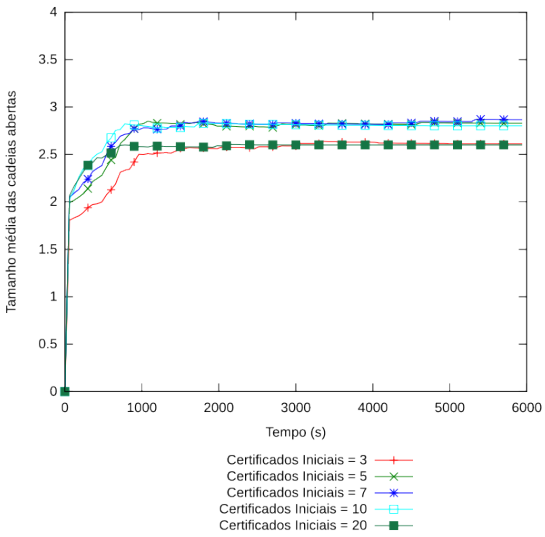

(a) Número de cadeias totais




(b) Número de cadeias fechadas

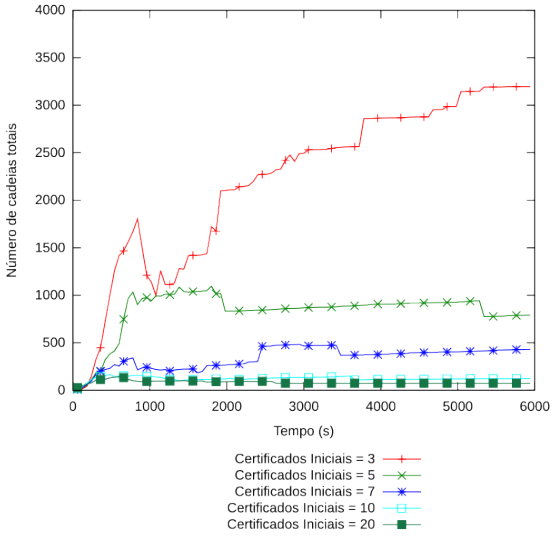



(c) Número de cadeias abertas

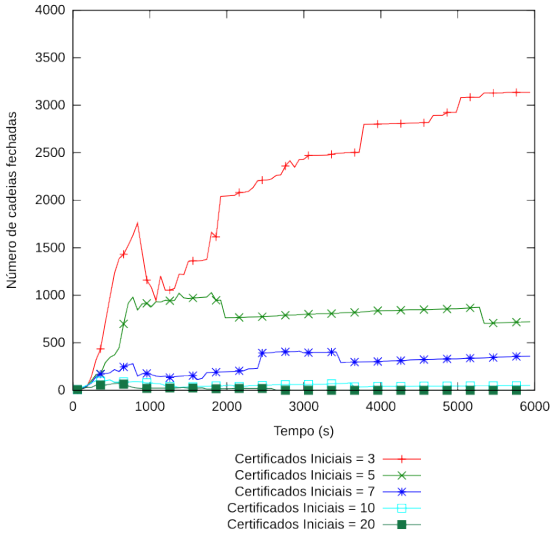



(d) Tamanho médio das cadeias

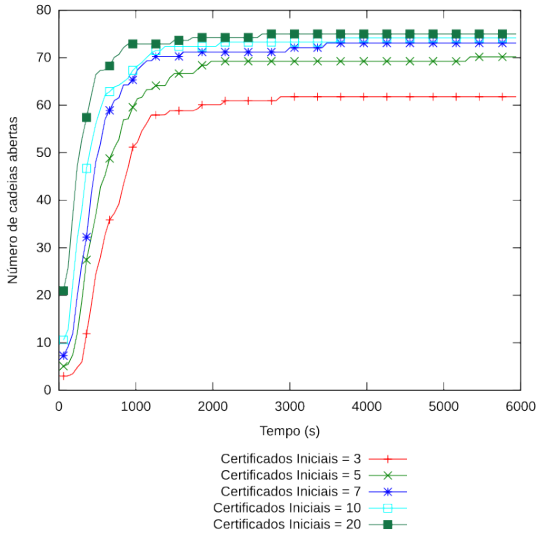
Figura C.33: Resultados para 50 nodos e $m = 20\%$



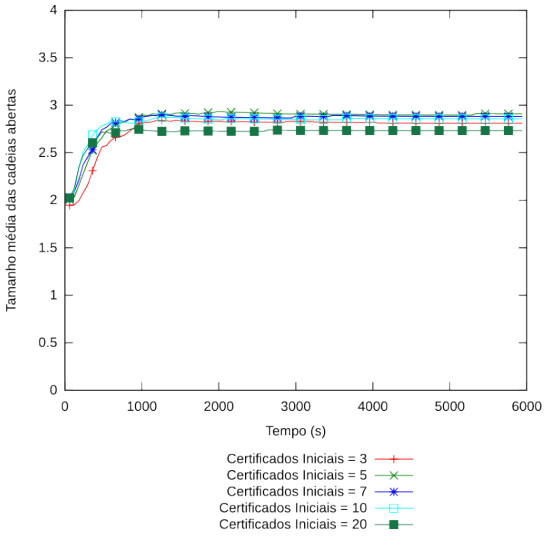

(a) Número de cadeias totais




(b) Número de cadeias fechadas

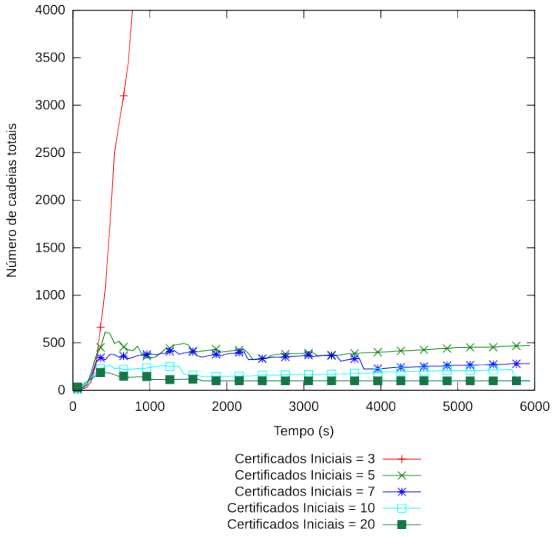



(c) Número de cadeias abertas

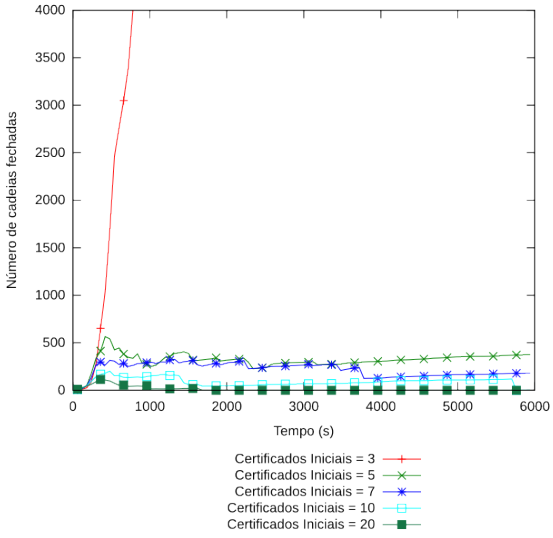



(d) Tamanho médio das cadeias

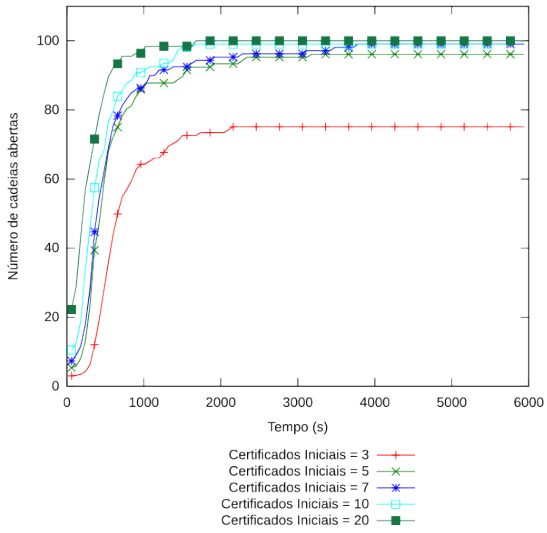
Figura C.34: Resultados para 75 nodos e $m = 20\%$



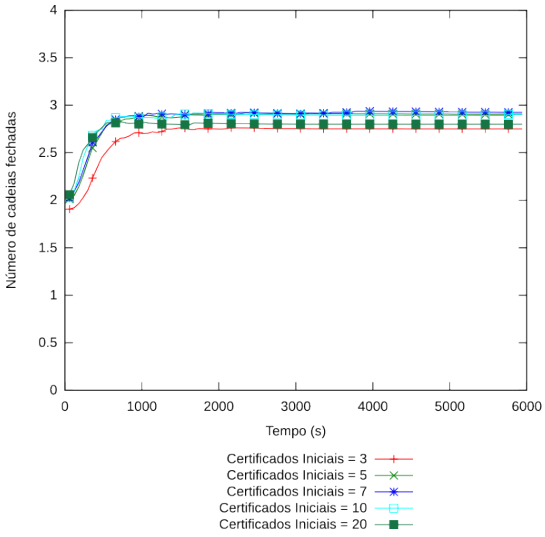

(a) Número de cadeias totais




(b) Número de cadeias fechadas

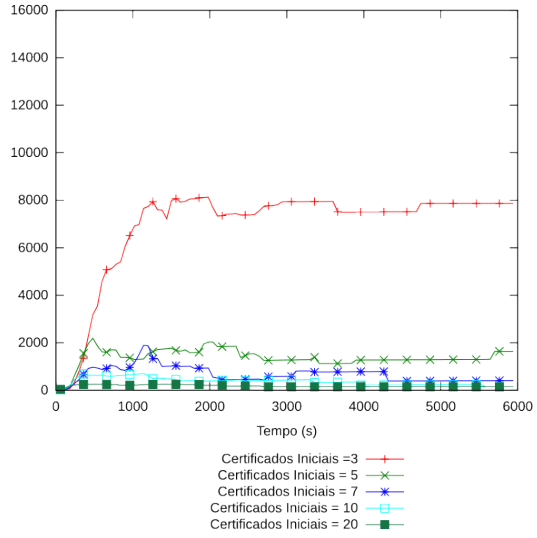



(c) Número de cadeias abertas

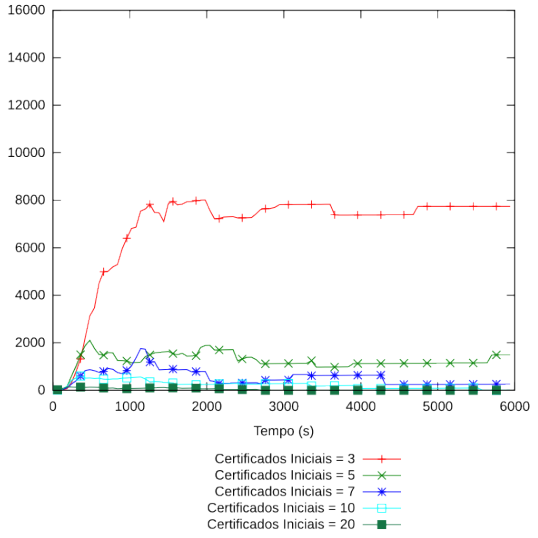



(d) Tamanho médio das cadeias

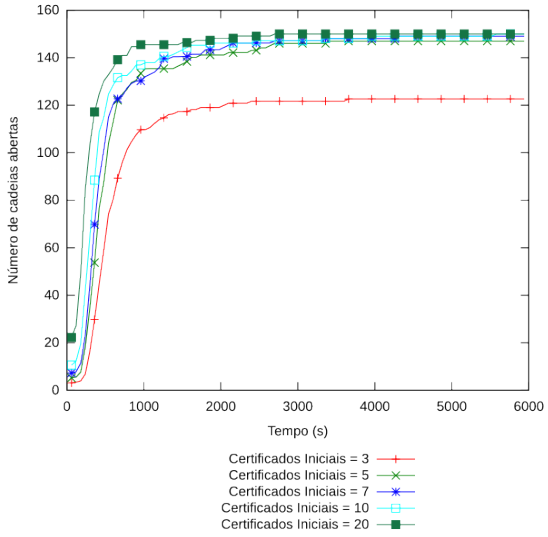
Figura C.35: Resultados para 100 nodos e $m = 20\%$



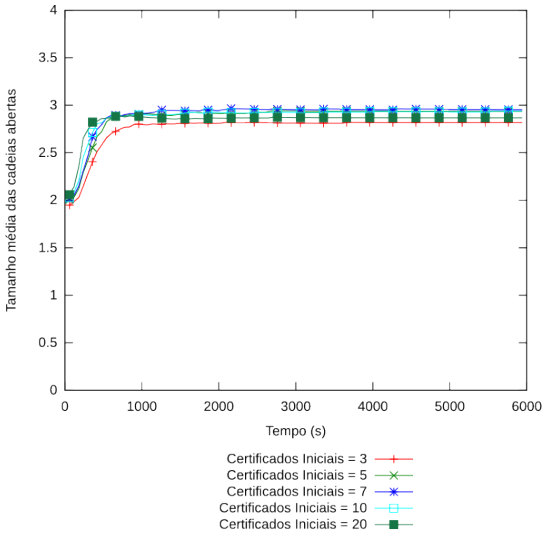

(a) Número de cadeias totais




(b) Número de cadeias fechadas



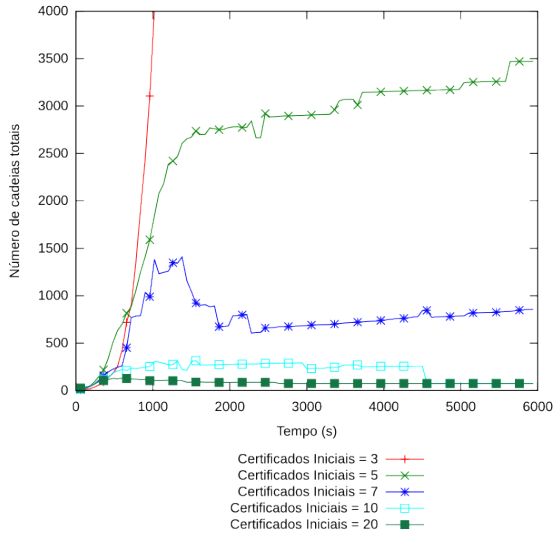

(c) Número de cadeias abertas



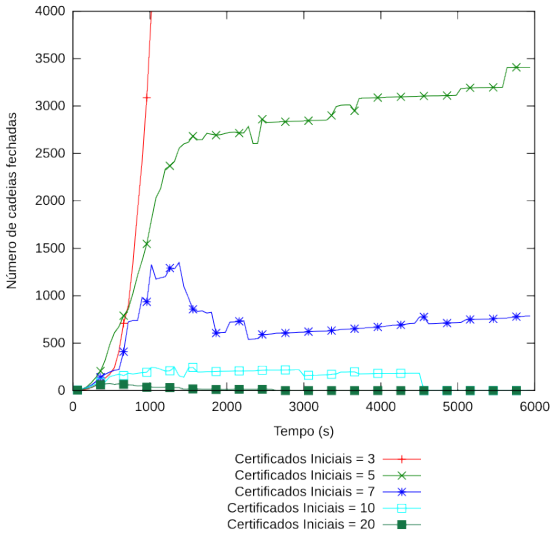

(d) Tamanho médio das cadeias

Figura C.36: Resultados para 150 nodos e $m = 20\%$

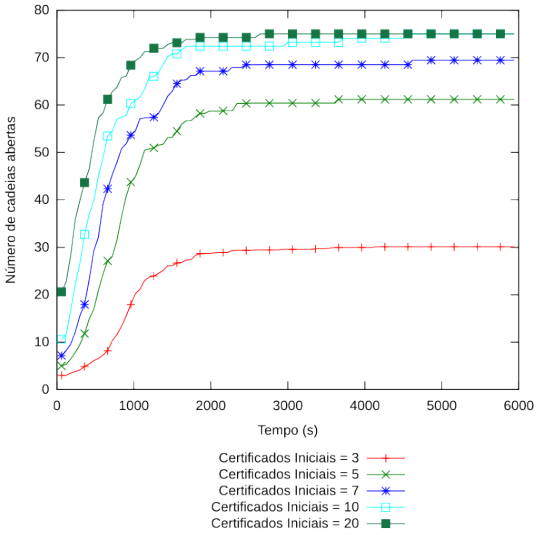
### C.3.3 Ataque *BlackHole* com $m = 50\%$



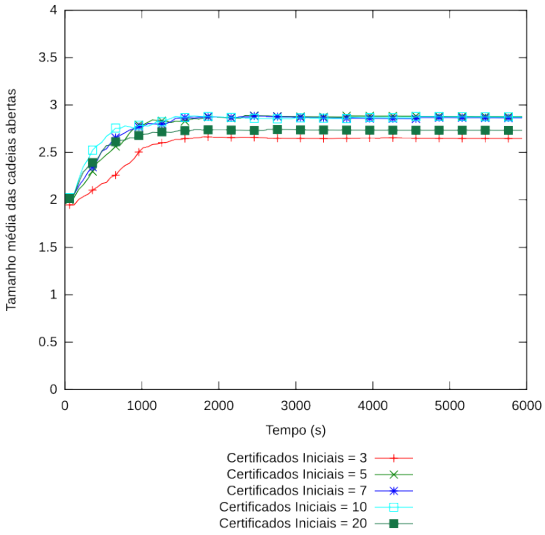

(a) Número de cadeias totais




(b) Número de cadeias fechadas

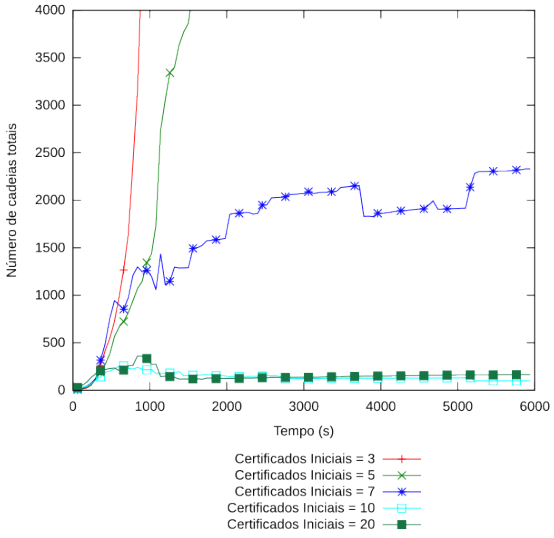



(c) Número de cadeias abertas

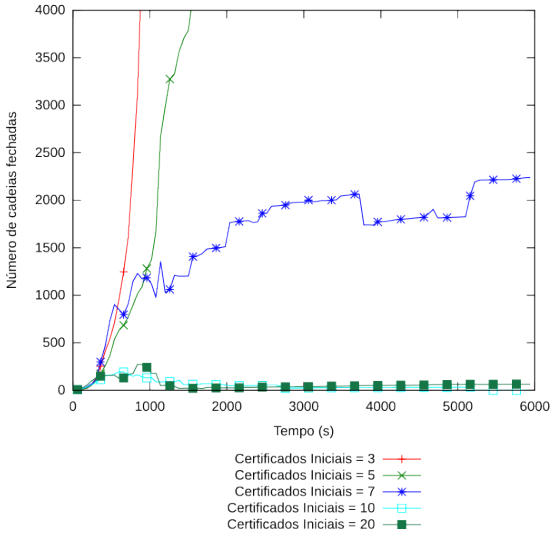



(d) Tamanho médio das cadeias

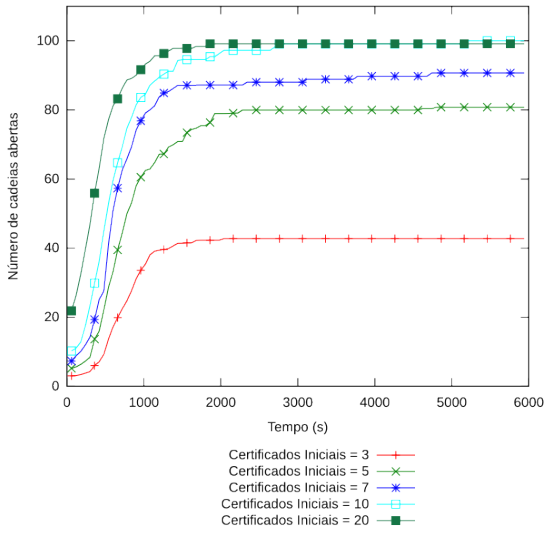
Figura C.37: Resultados para 75 nodos e $m = 50\%$



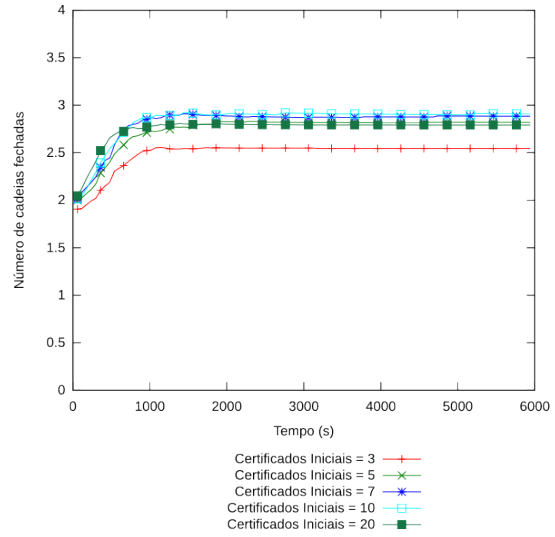

(a) Número de cadeias totais




(b) Número de cadeias fechadas




(c) Número de cadeias abertas

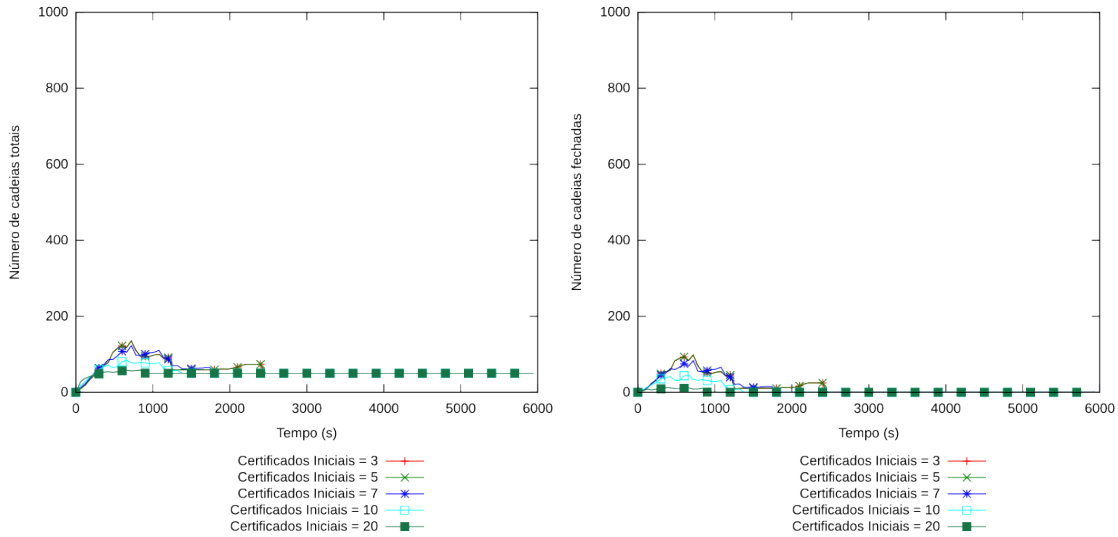



(d) Tamanho médio das cadeias

Figura C.38: Resultados para 100 nodos e $m = 50\%$

## C.4 Ataque *Sybil*

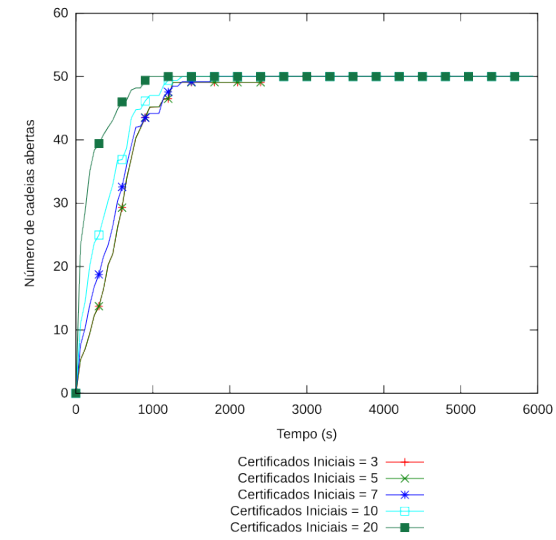
### C.4.1 Ataque *Sybil* com $f = 10\%$



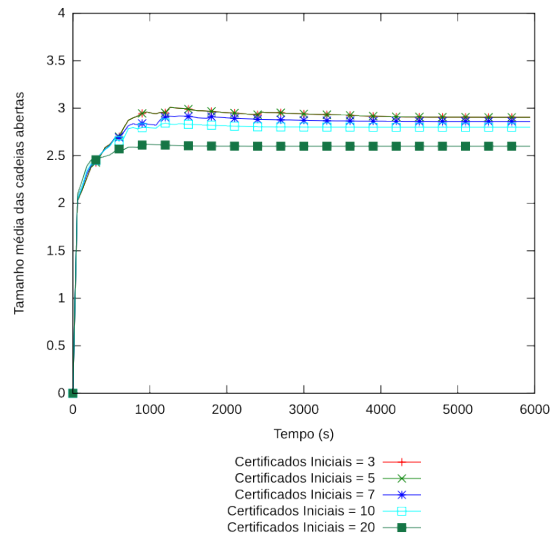

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

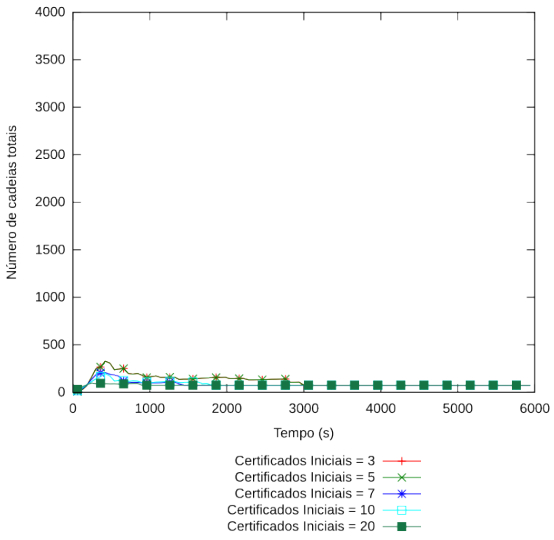



(c) Número de cadeias Abertas

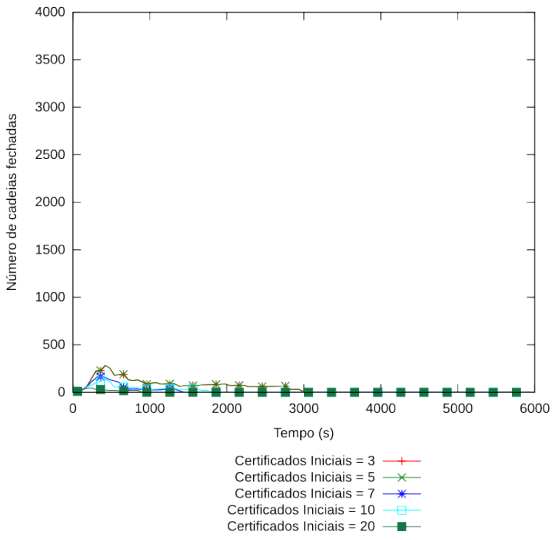



(d) Tamanho médio das cadeias

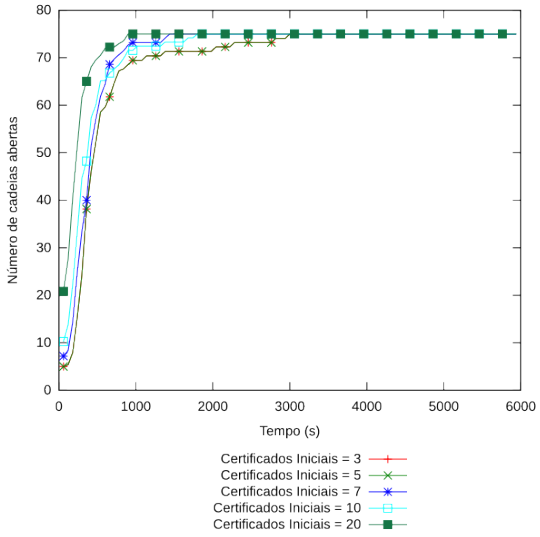
Figura C.39: Resultados para 50 nodos e $f = 10\%$



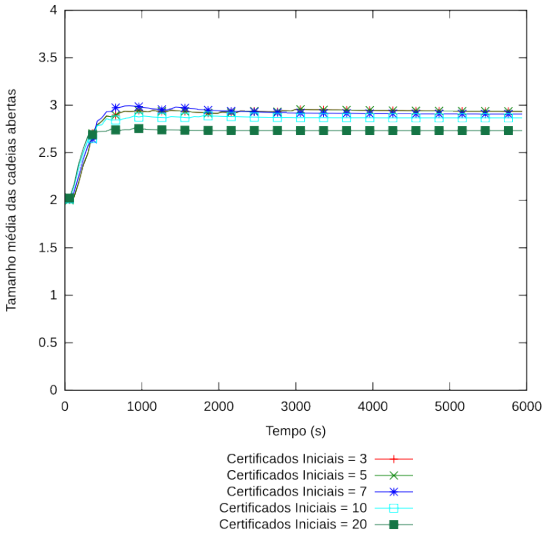

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

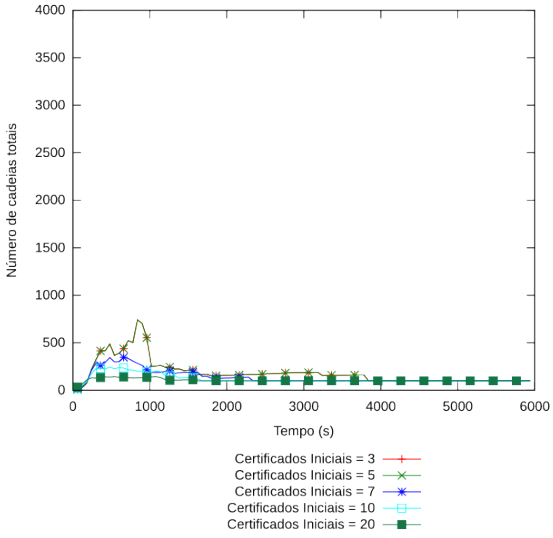



(c) Número de cadeias Abertas

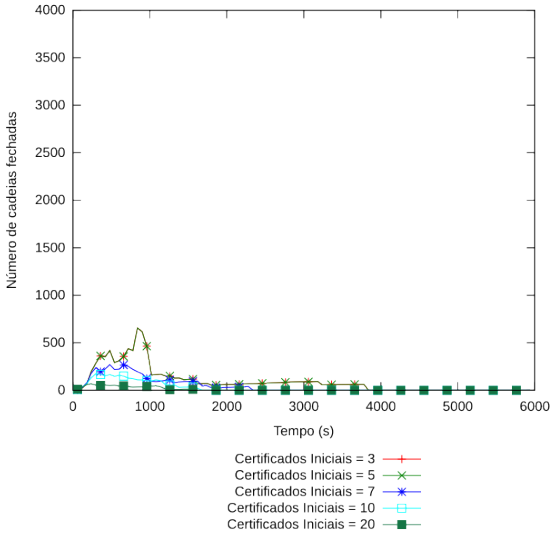



(d) Tamanho médio das cadeias

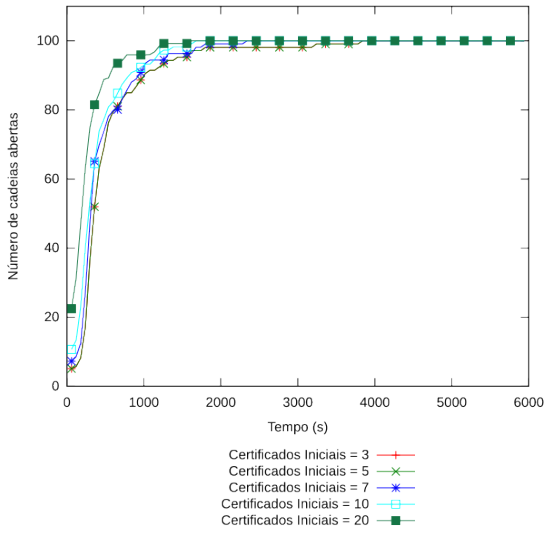
Figura C.40: Resultados para 75 nodos e $f = 10\%$



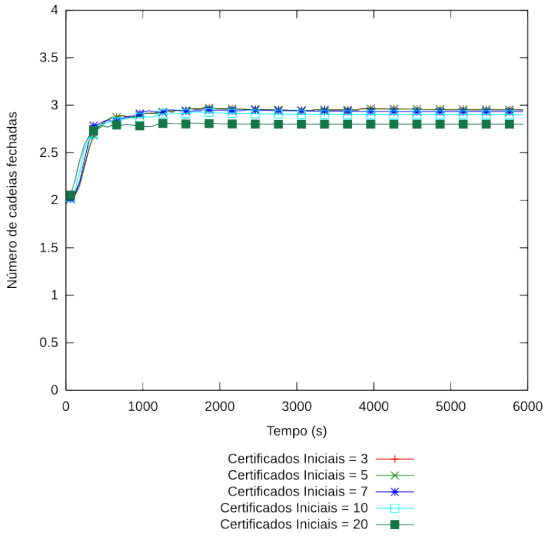

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

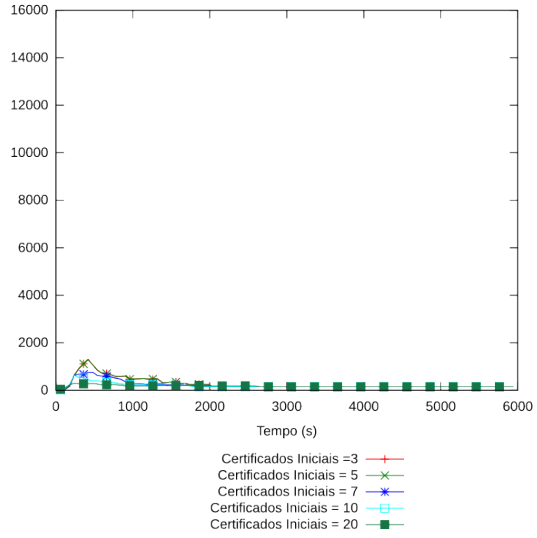



(c) Número de cadeias Abertas

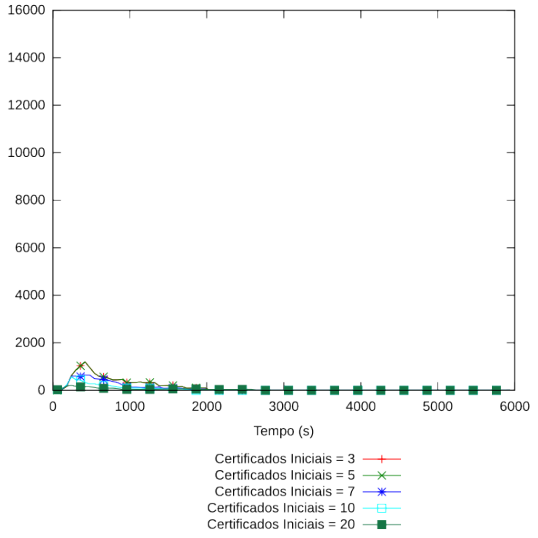



(d) Tamanho médio das cadeias

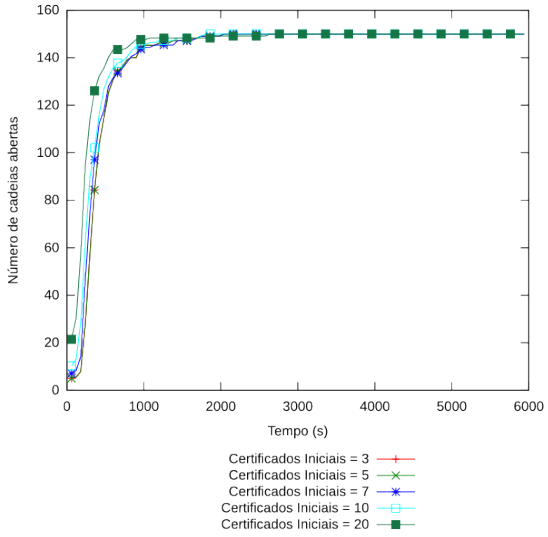
Figura C.41: Resultados para 100 nodos e $f = 10\%$



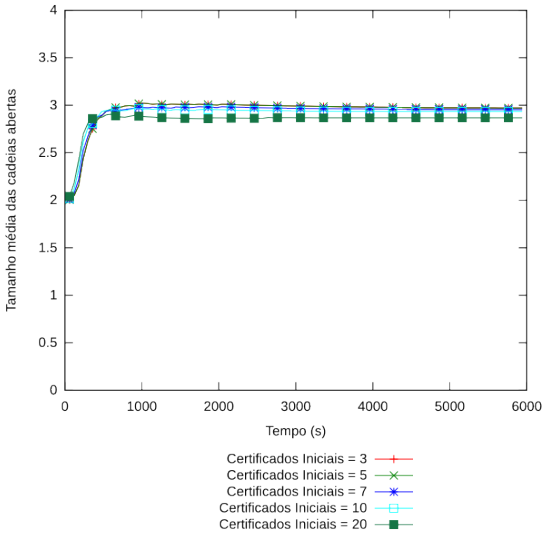

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



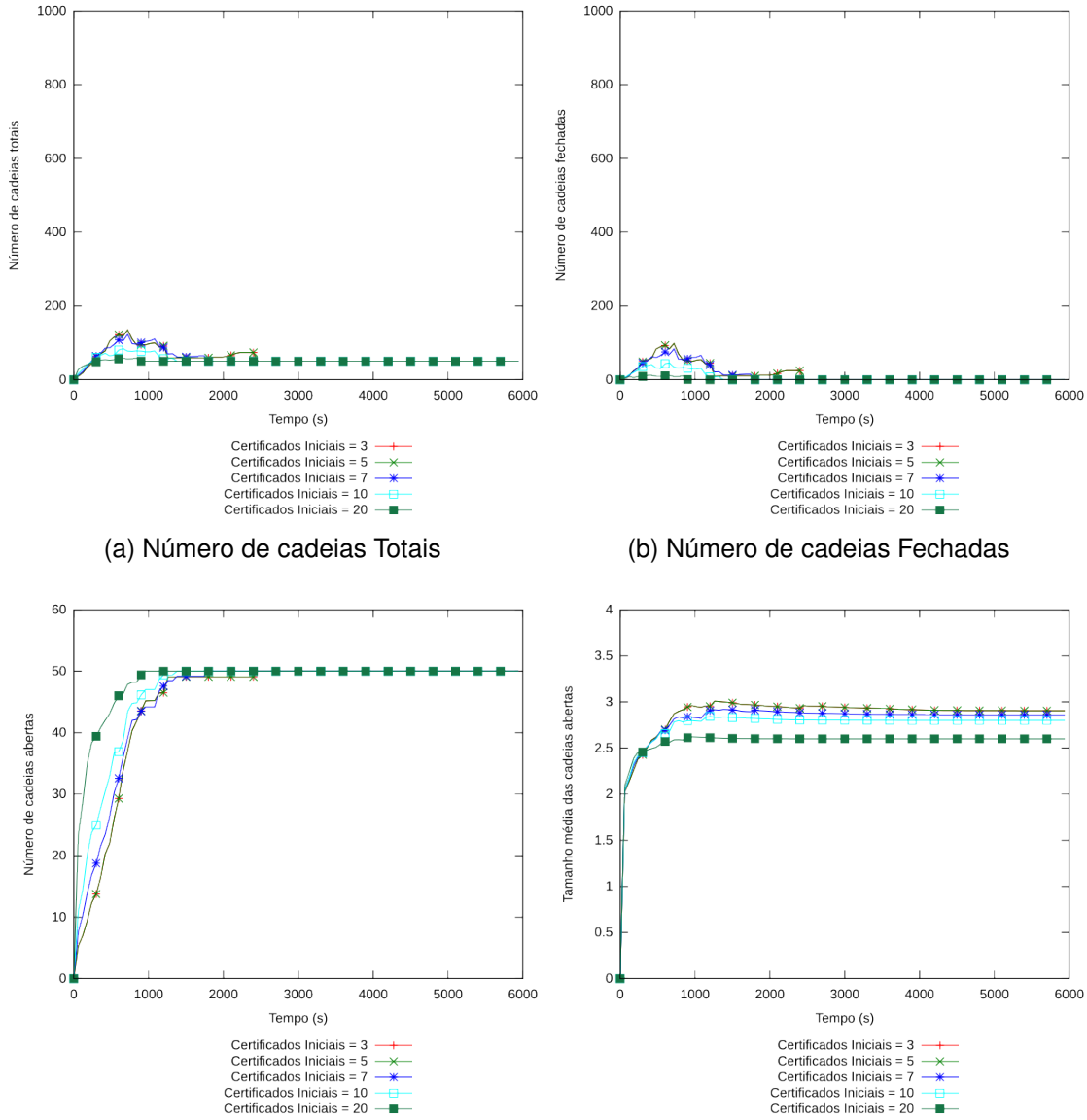

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.42: Resultados para 150 nodos e $f = 10\%$

### C.4.2 Ataque *Sybil* com $f = 20\%$



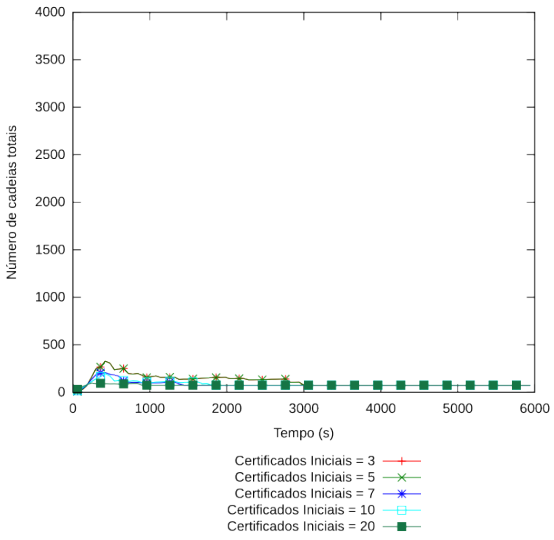

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

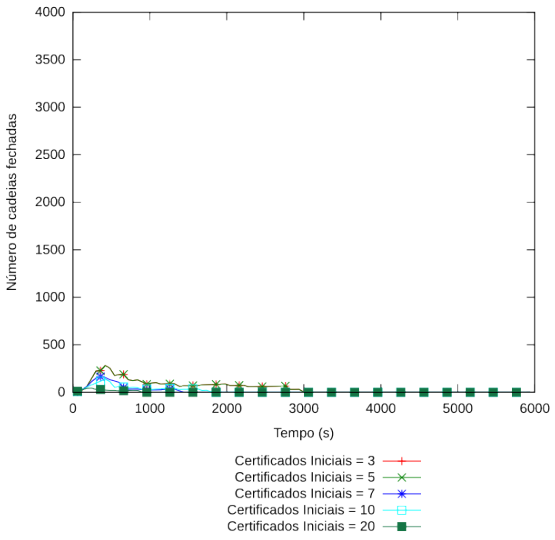
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

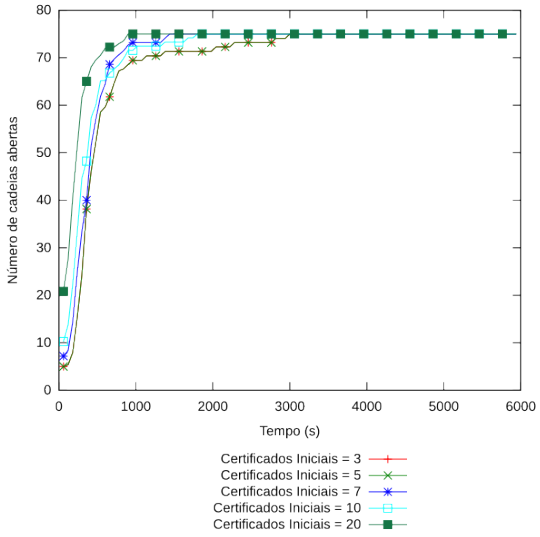
Figura C.43: Resultados para 50 nodos e $f = 20\%$



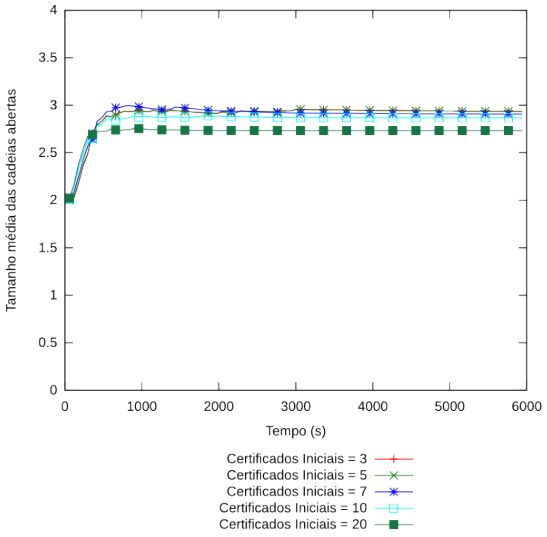

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

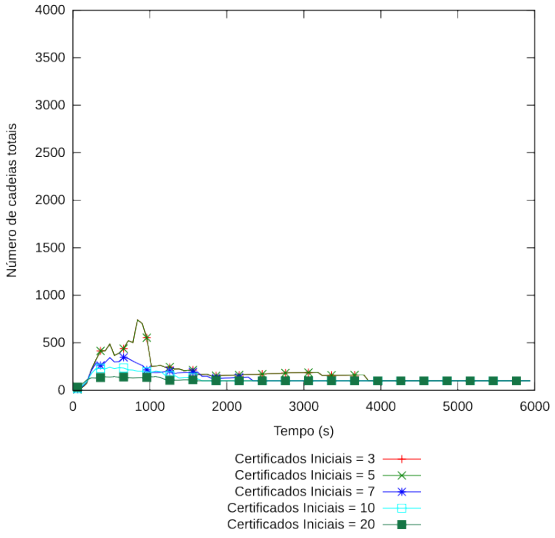



(c) Número de cadeias Abertas

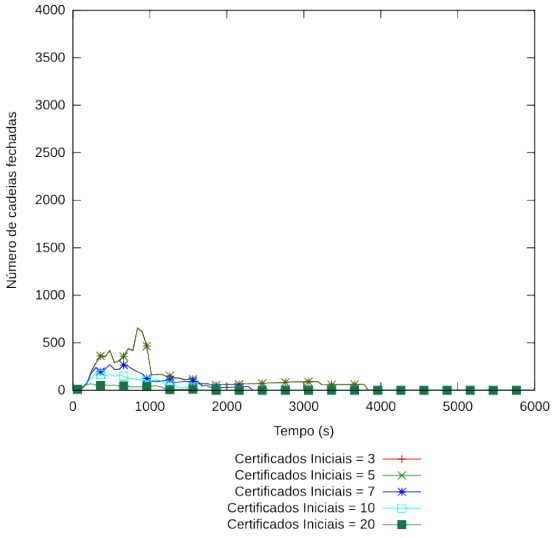



(d) Tamanho médio das cadeias

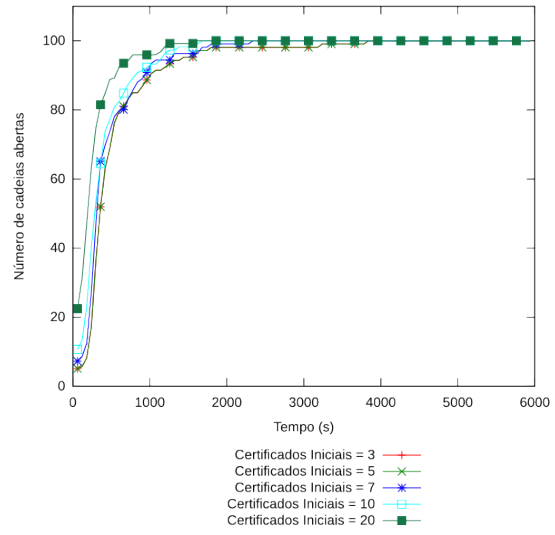
Figura C.44: Resultados para 75 nodos e $f = 20\%$



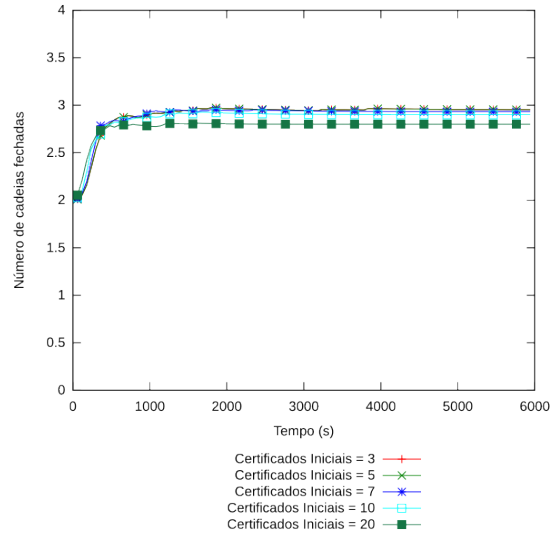

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

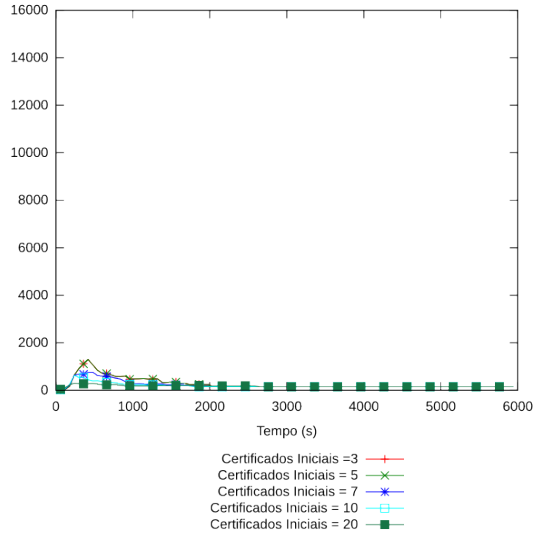



(c) Número de cadeias Abertas

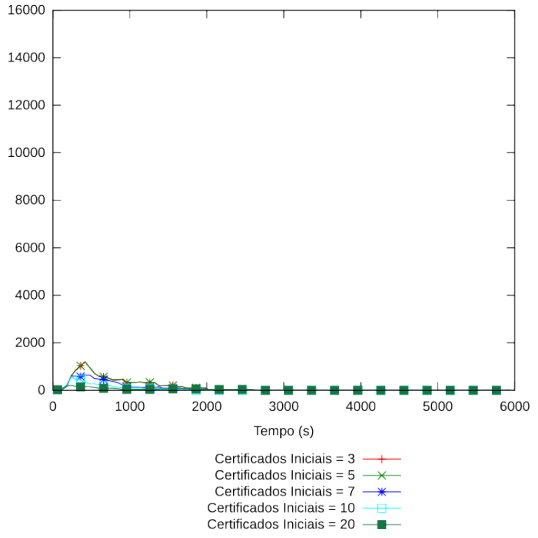



(d) Tamanho médio das cadeias

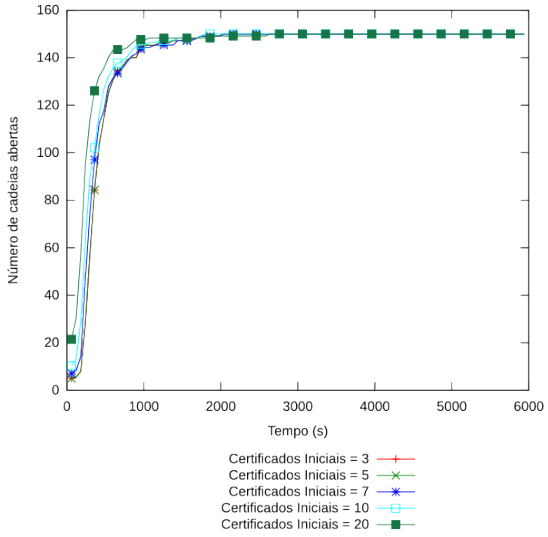
Figura C.45: Resultados para 100 nodos e $f = 20\%$



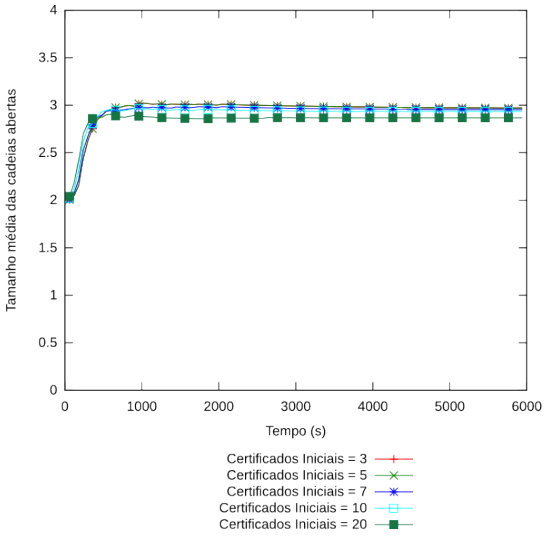

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



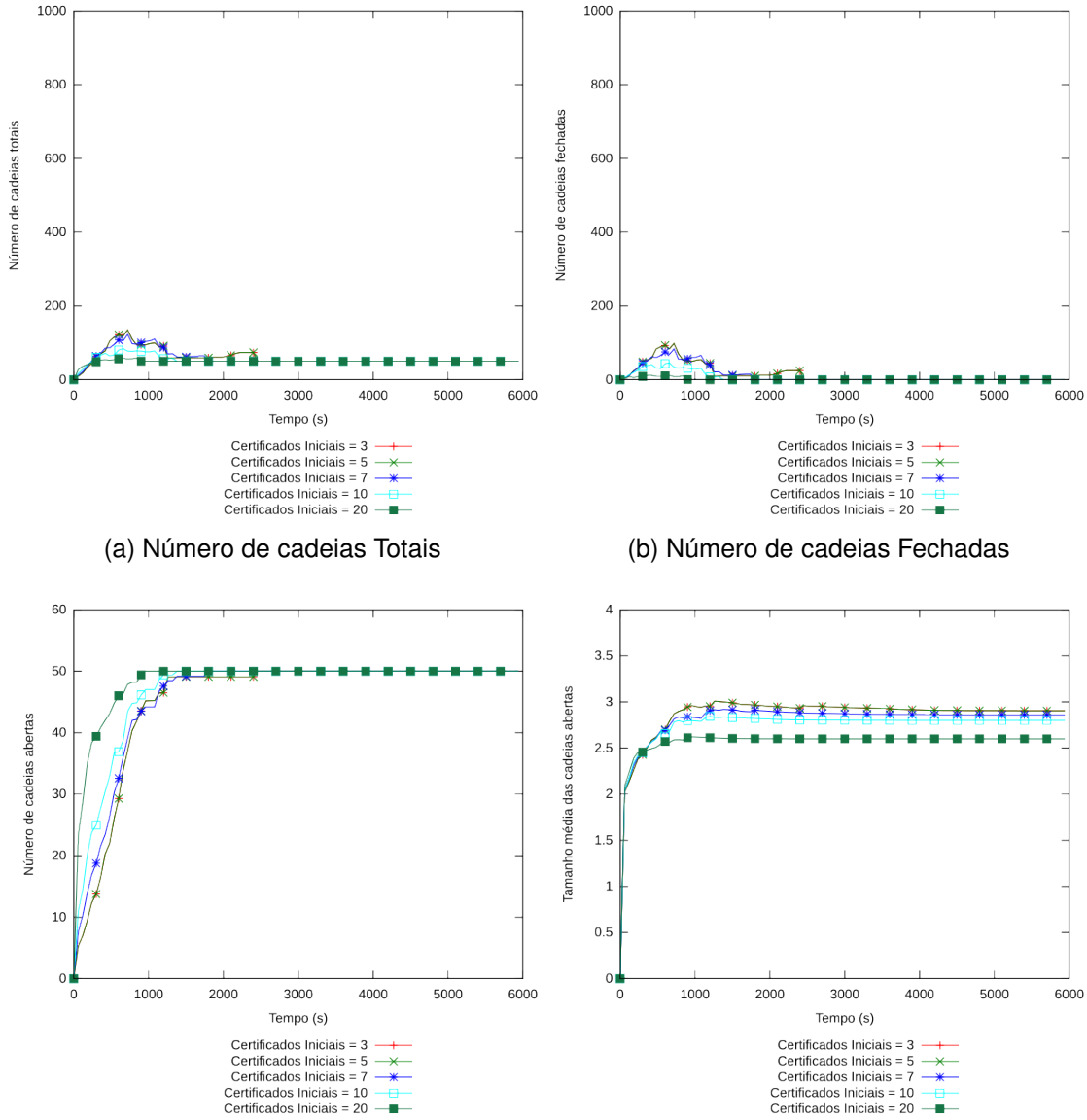

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.46: Resultados para 150 nodos e $f = 20\%$

### C.4.3 Ataque *Sybil* com $f = 50\%$



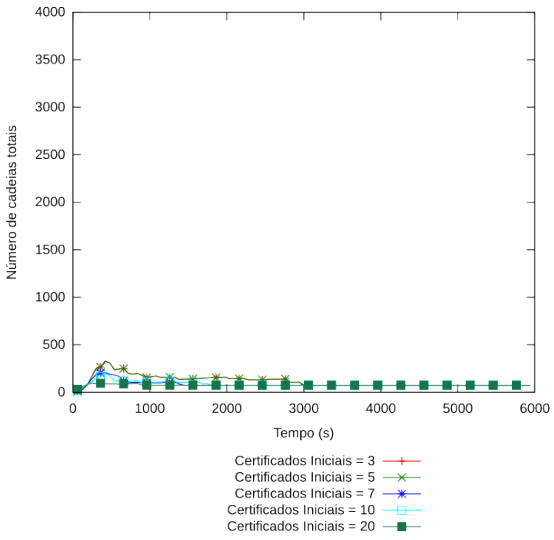

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

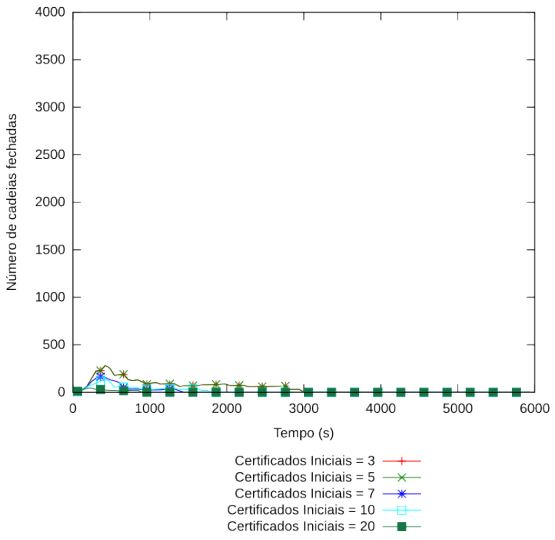
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

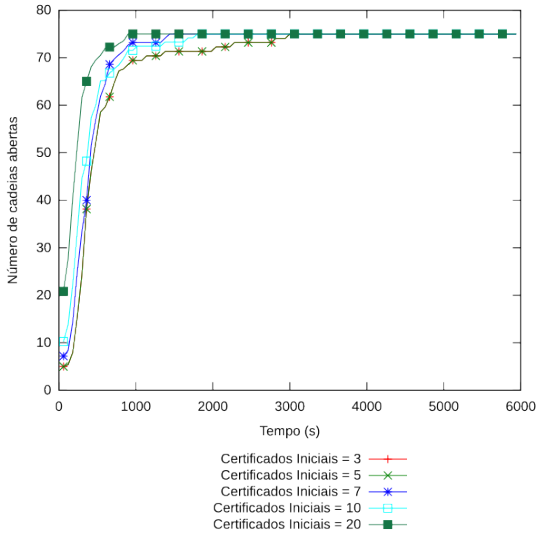
Figura C.47: Resultados para 50 nodos e $f = 50\%$



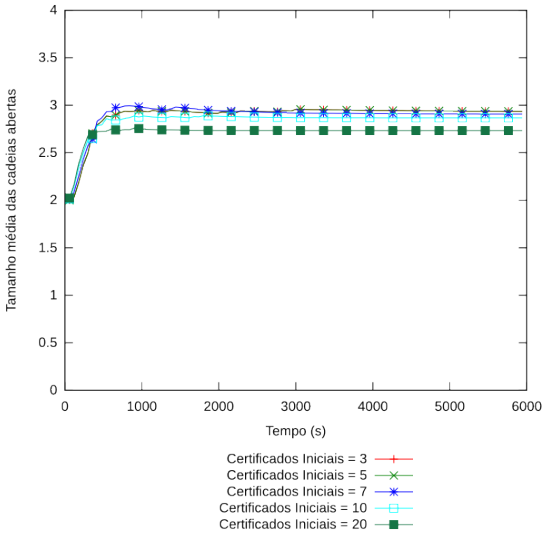

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

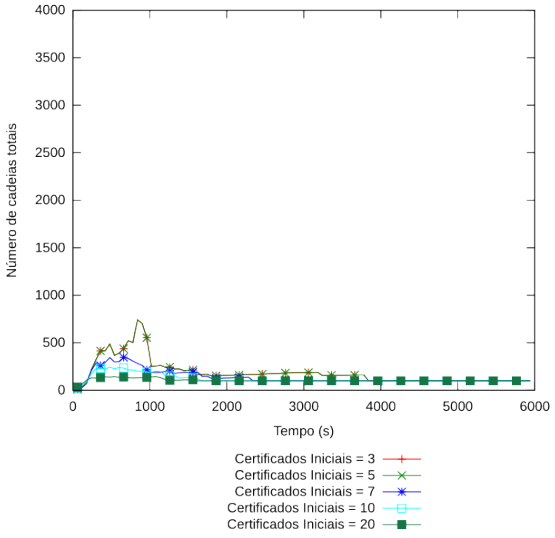



(c) Número de cadeias Abertas

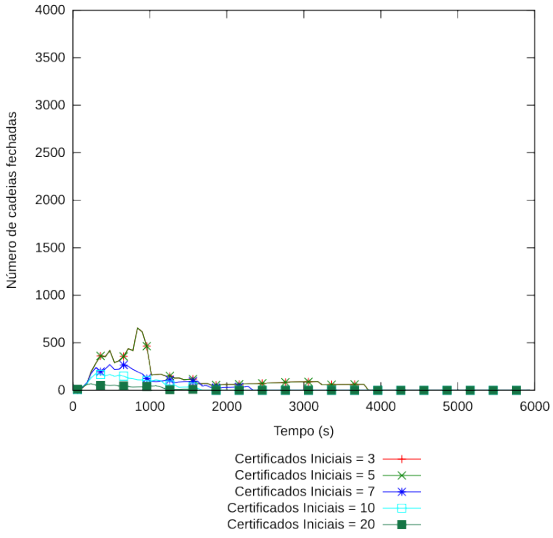



(d) Tamanho médio das cadeias

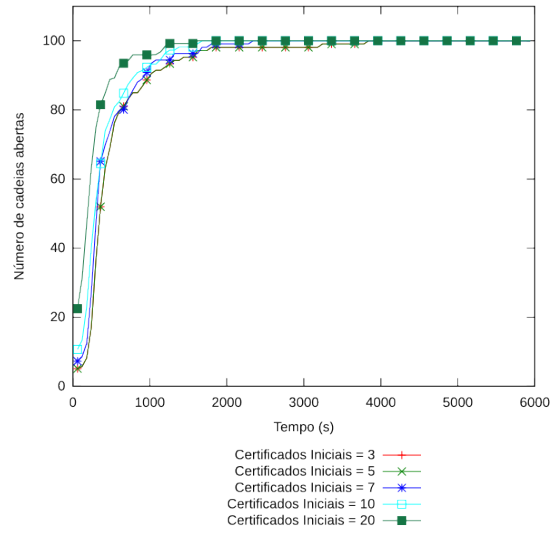
Figura C.48: Resultados para 75 nodos e $f = 50\%$



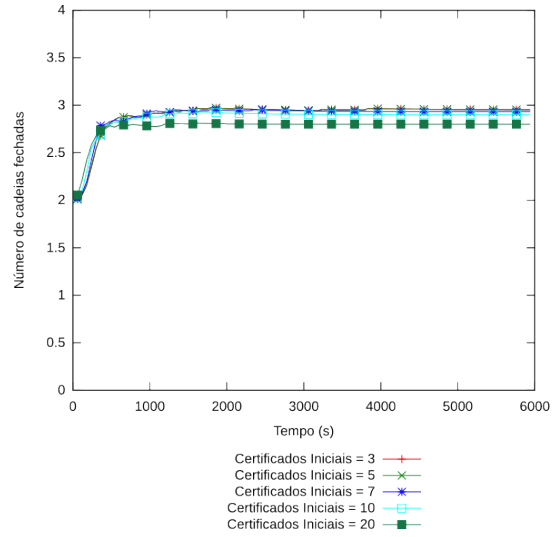

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

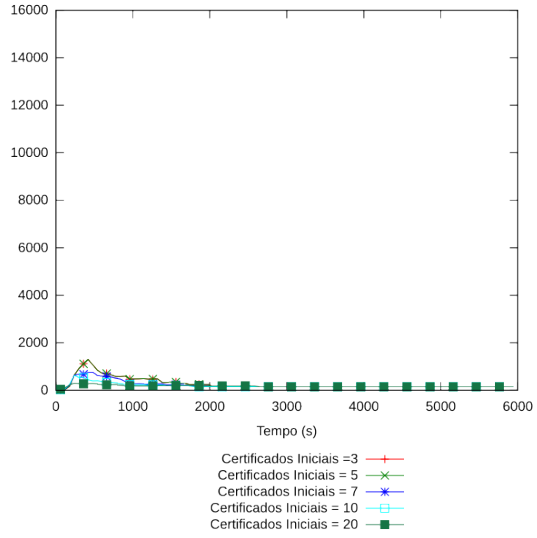



(c) Número de cadeias Abertas

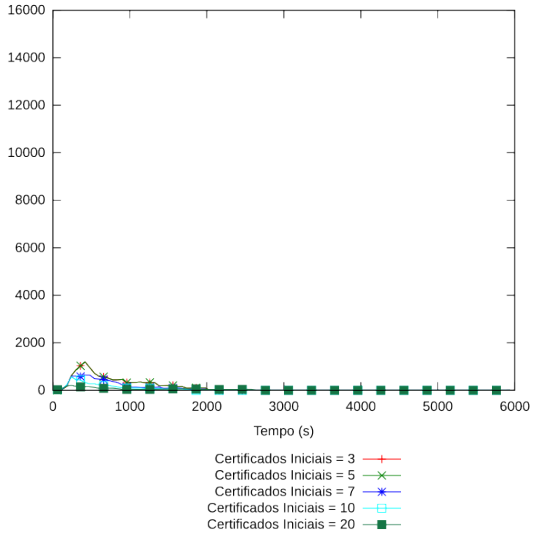



(d) Tamanho médio das cadeias

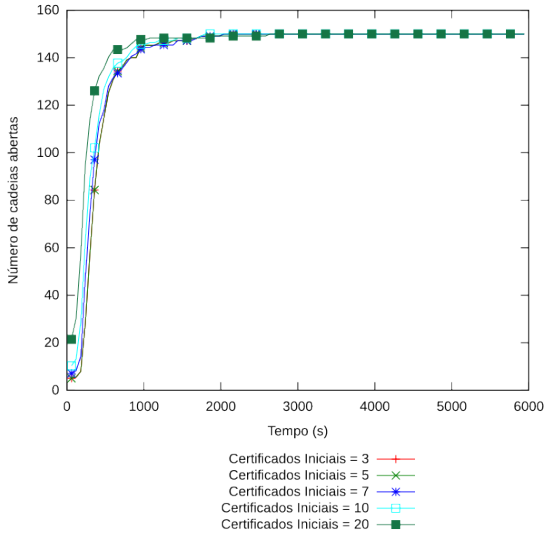
Figura C.49: Resultados para 100 nodos e $f = 50\%$



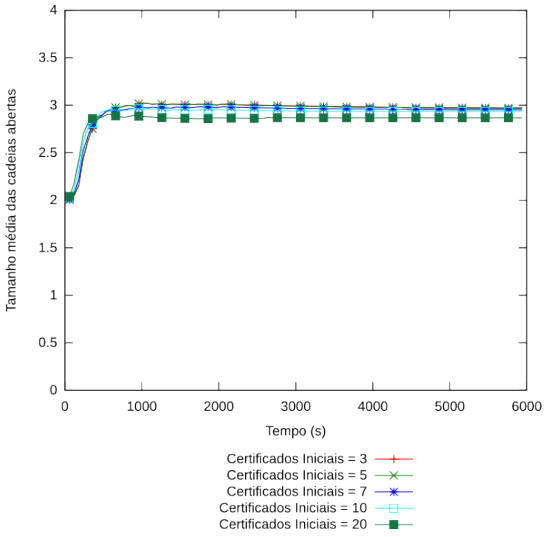

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

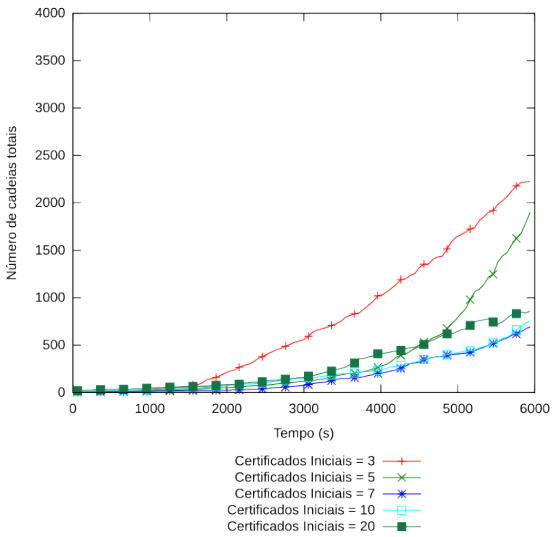



(d) Tamanho médio das cadeias

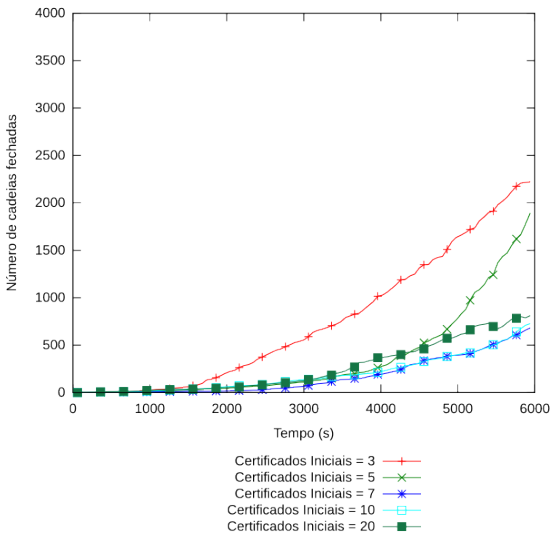
Figura C.50: Resultados para 150 nodos e $f = 50\%$

## C.5 Ataque de Falsificaçao - Ataque independente

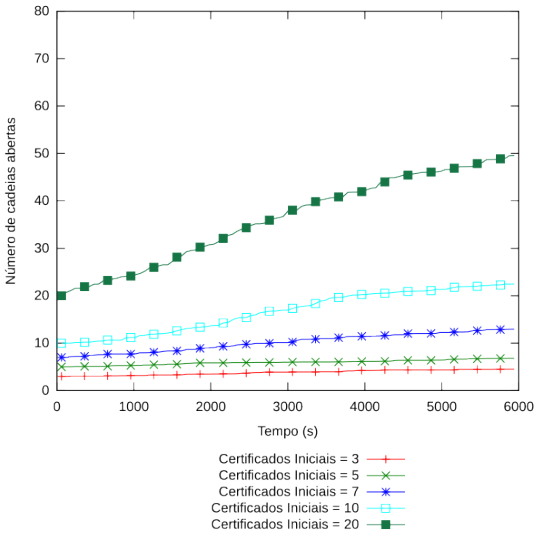
### C.5.1 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 10\%$



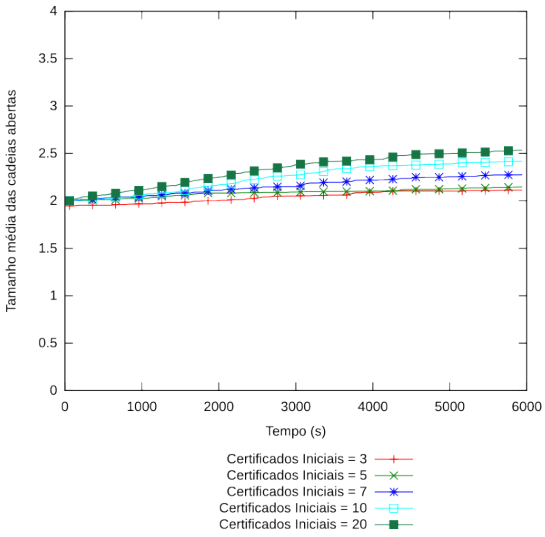

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

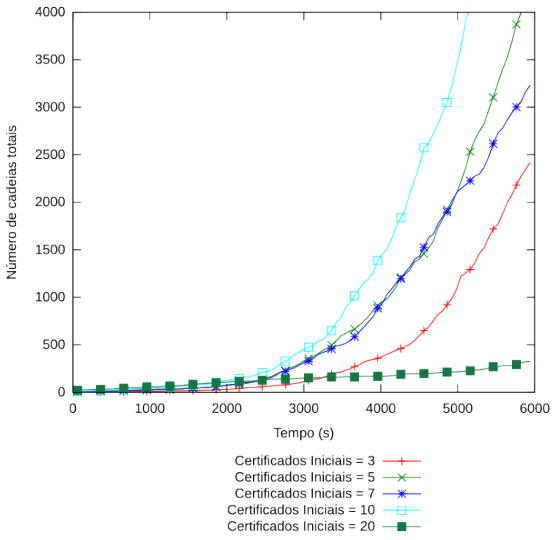



(c) Número de cadeias Abertas

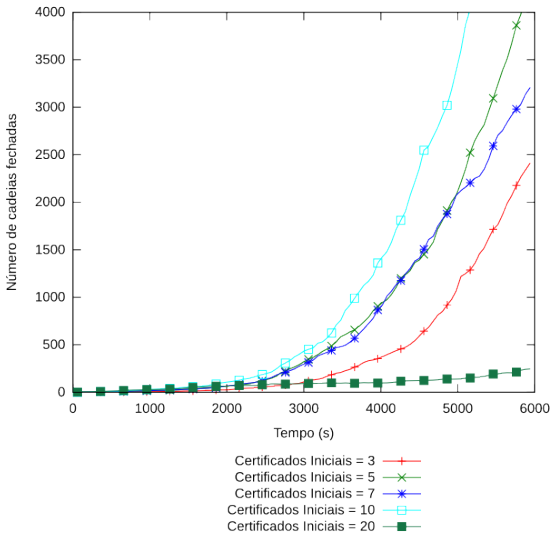



(d) Tamanho médio das cadeias

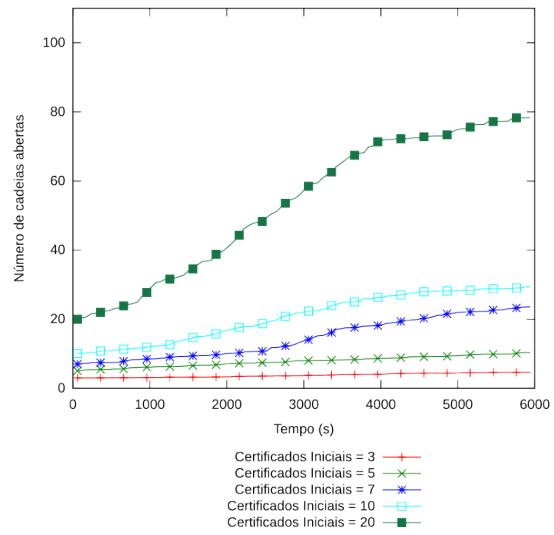
Figura C.51: Resultados para 75 nodos, $m = 10\%$ e $N_a = 10\%$



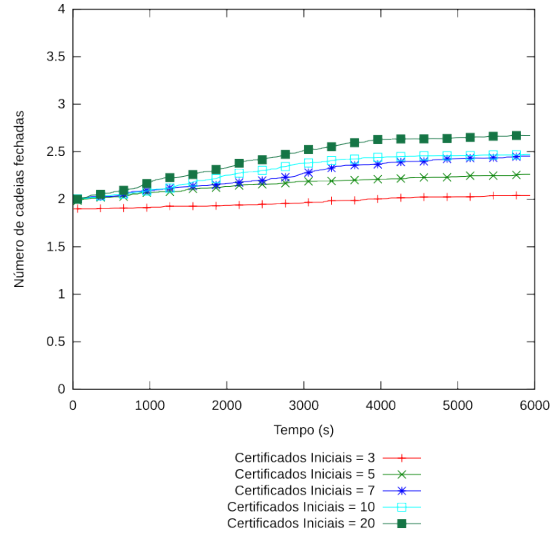

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



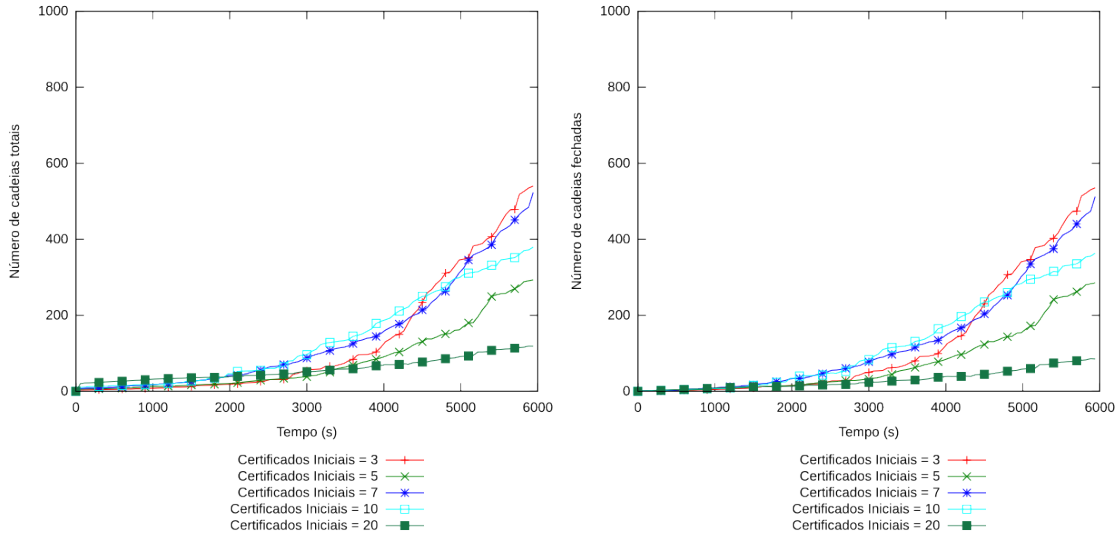

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.52: Resultados para 100 nodos, $m = 10\%$ e $N_a = 10\%$

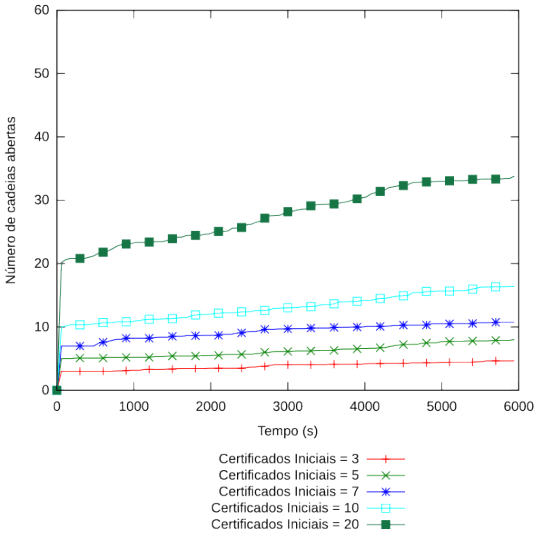
### C.5.2 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 25\%$



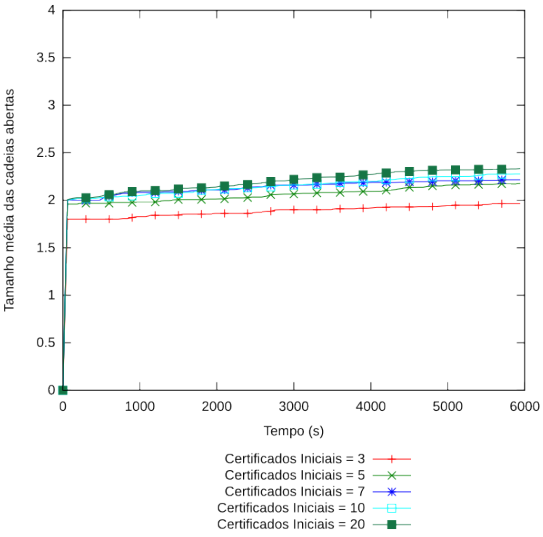

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

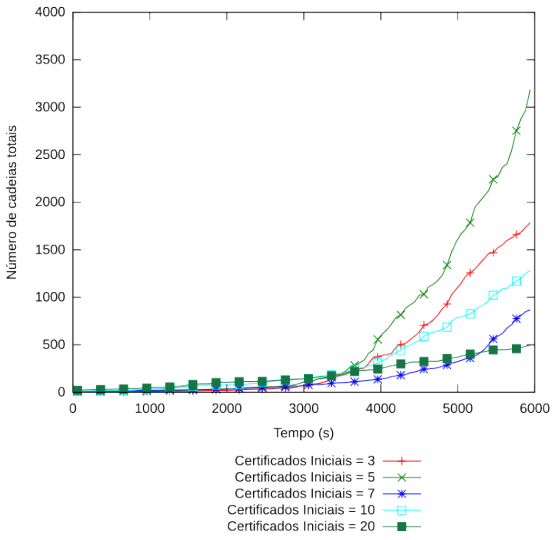



(c) Número de cadeias Abertas

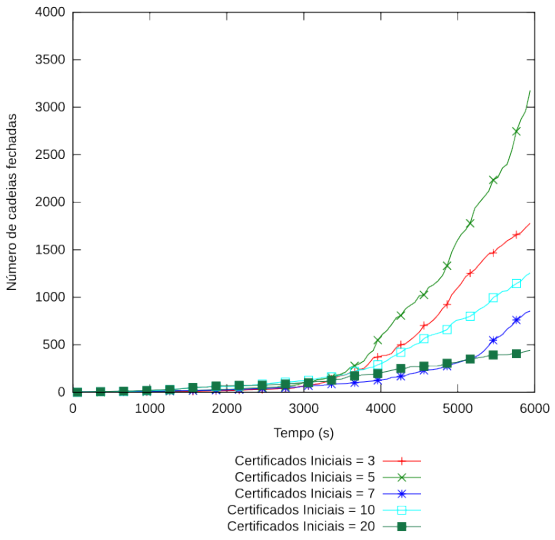



(d) Tamanho médio das cadeias

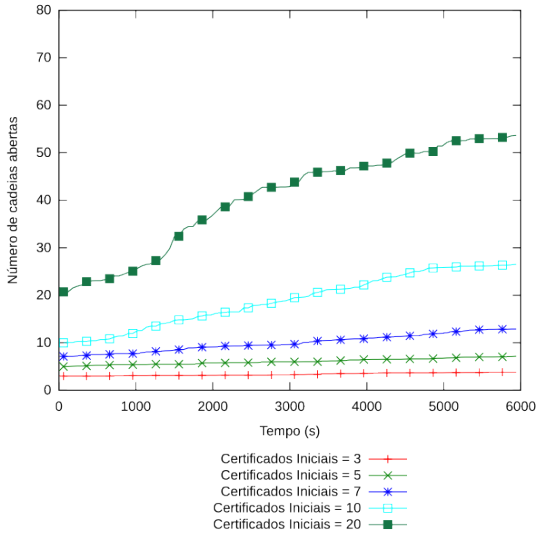
Figura C.53: Resultados para 50 nodos, $m = 10\%$ e $N_a = 25\%$



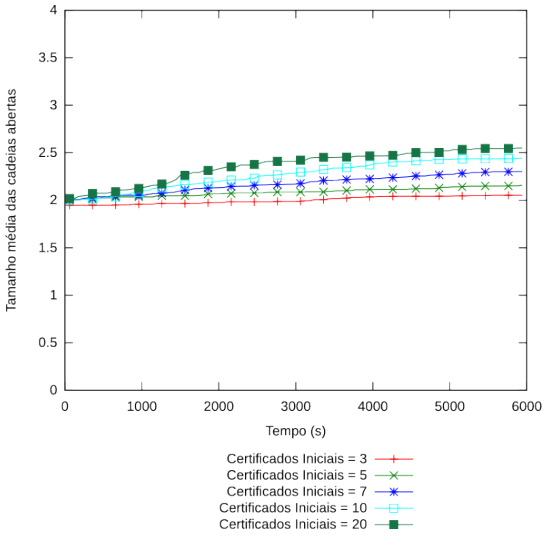

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

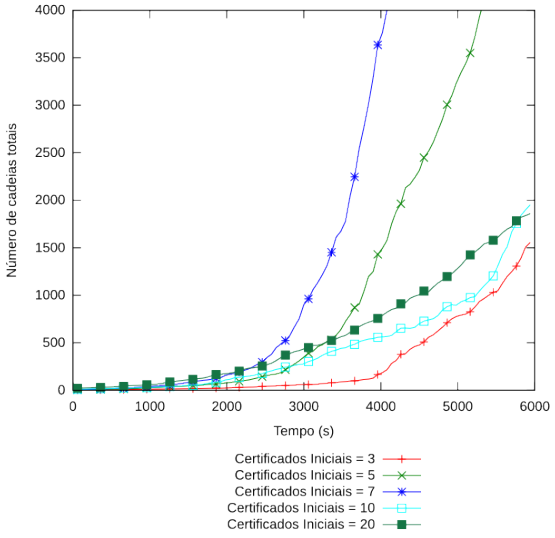



(c) Número de cadeias Abertas

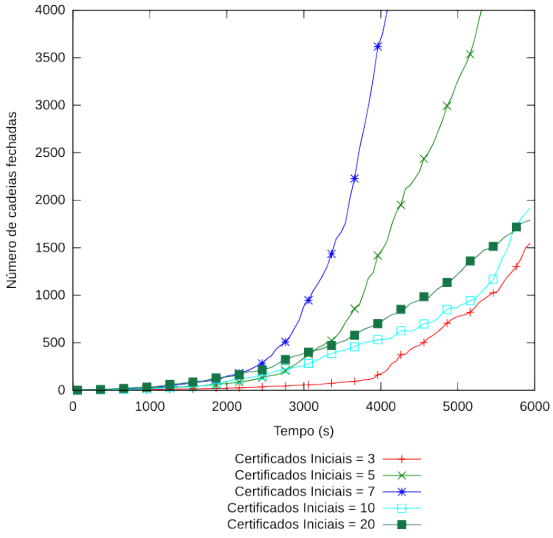



(d) Tamanho médio das cadeias

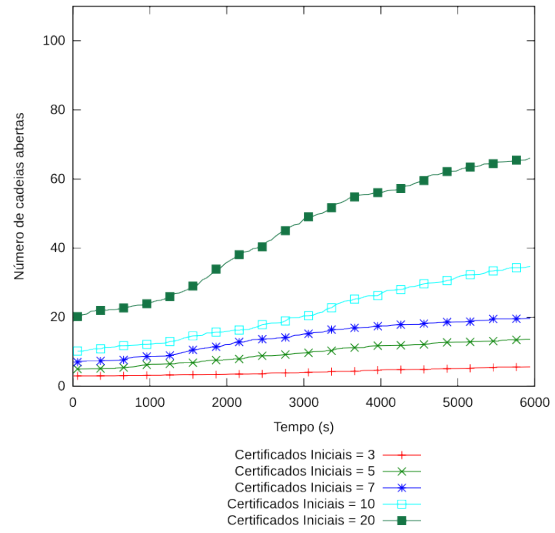
Figura C.54: Resultados para 75 nodos, $m = 10\%$ e $N_a = 25\%$



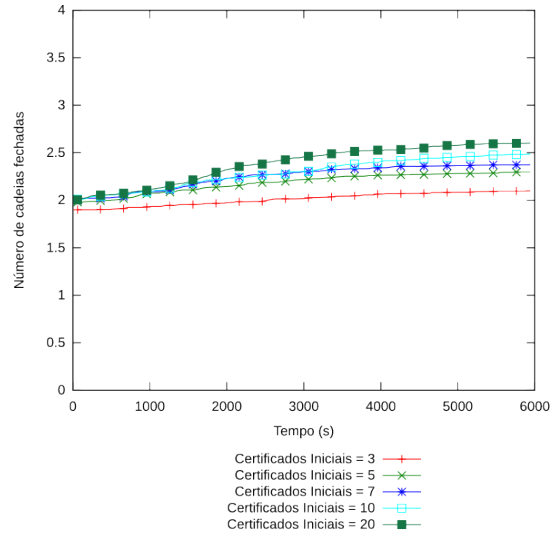

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

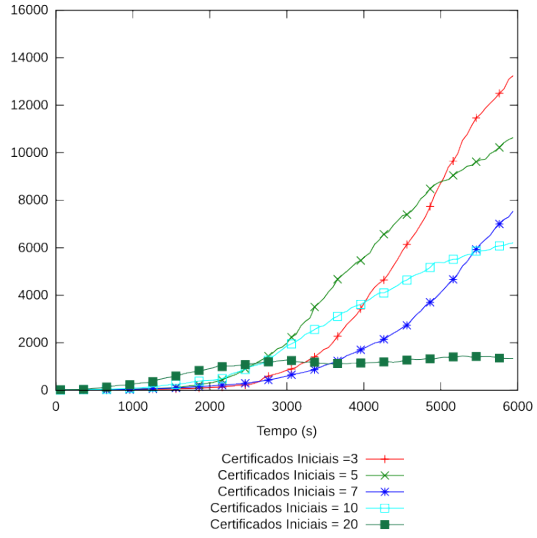



(c) Número de cadeias Abertas

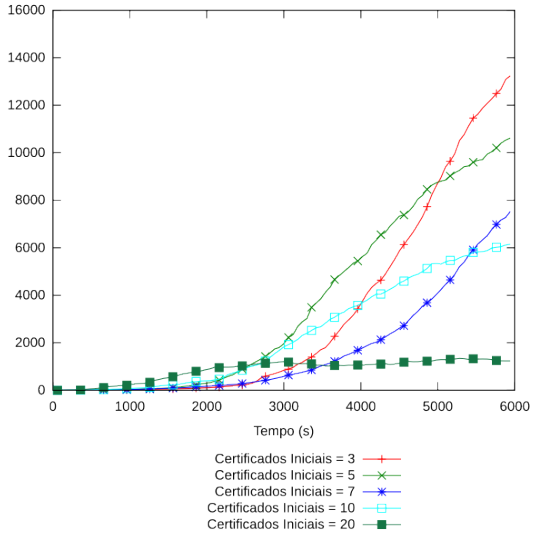



(d) Tamanho médio das cadeias

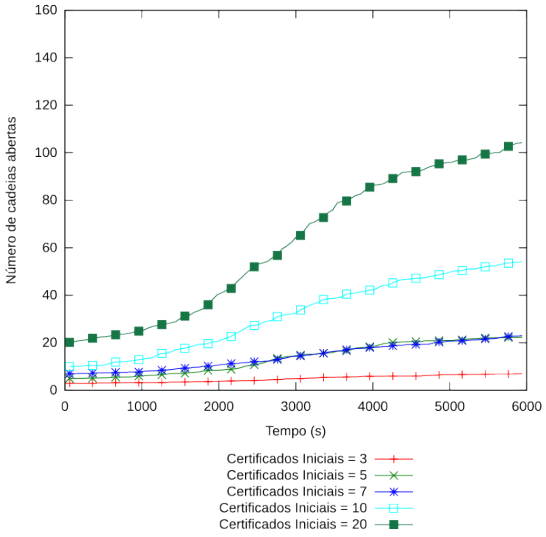
Figura C.55: Resultados para 100 nodos, $m = 10\%$ e $N_a = 25\%$



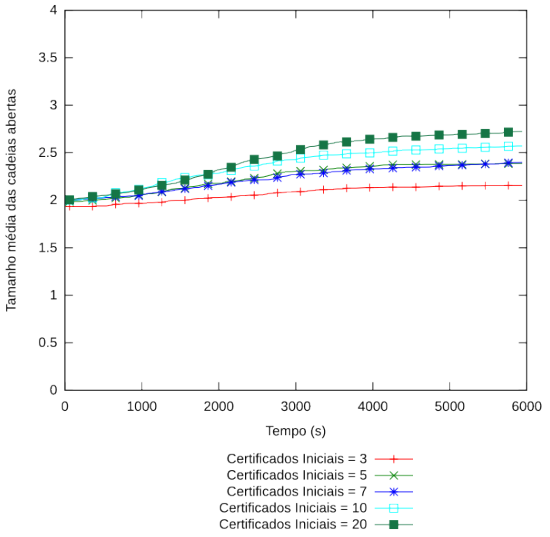

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



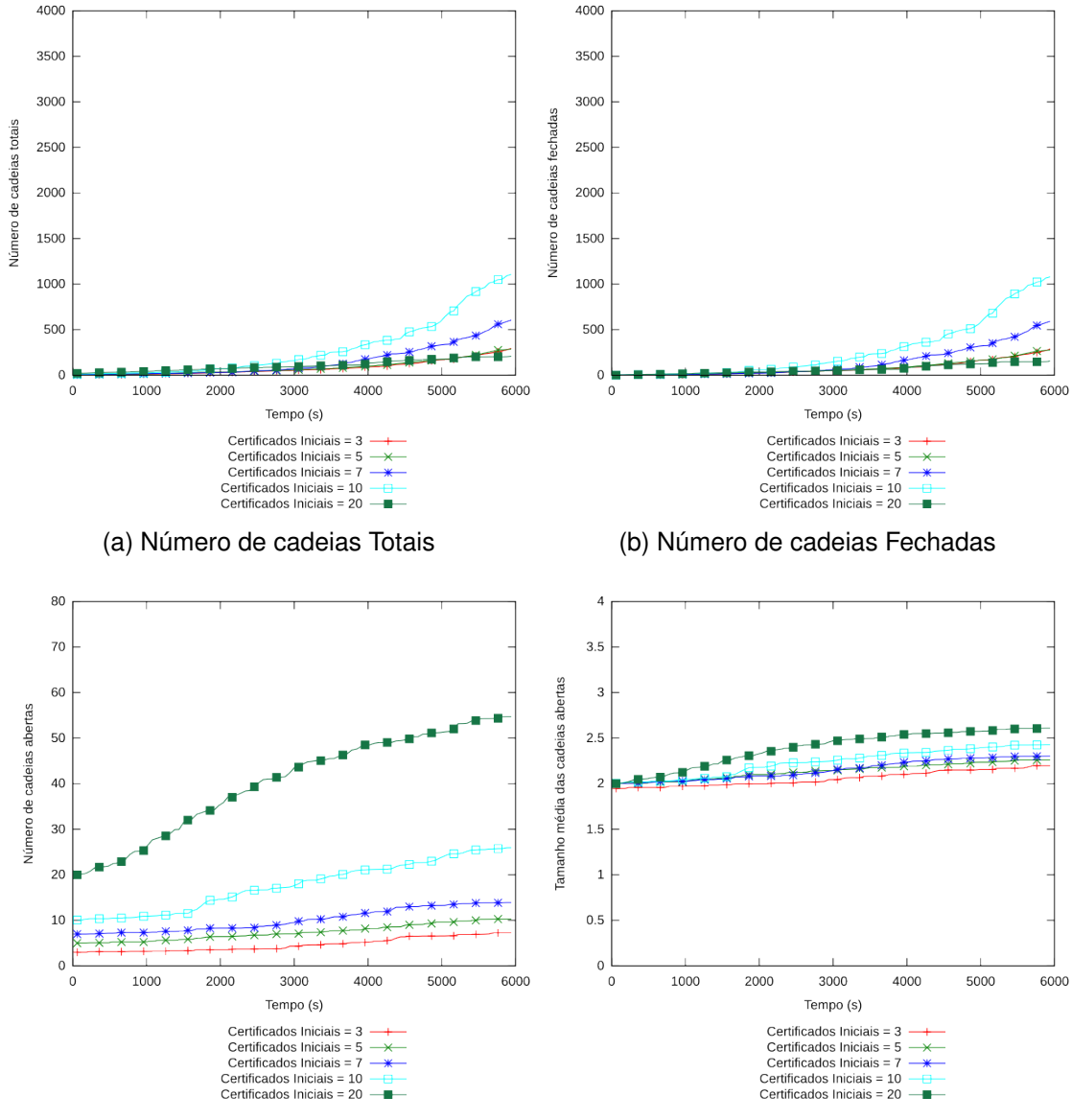

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.56: Resultados para 150 nodos, $m = 10\%$ e $N_a = 25\%$

### C.5.3 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 50\%$



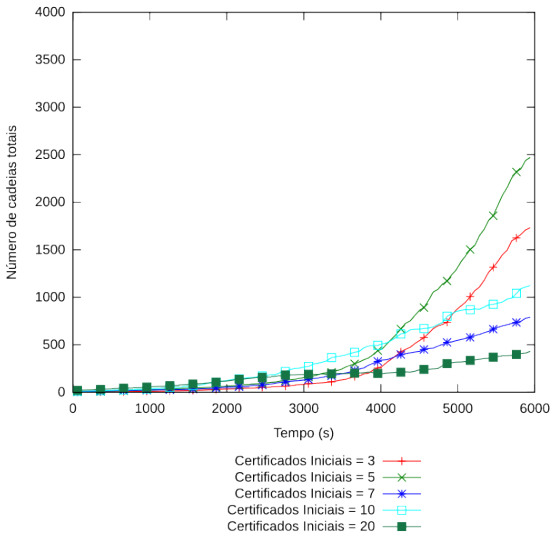

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

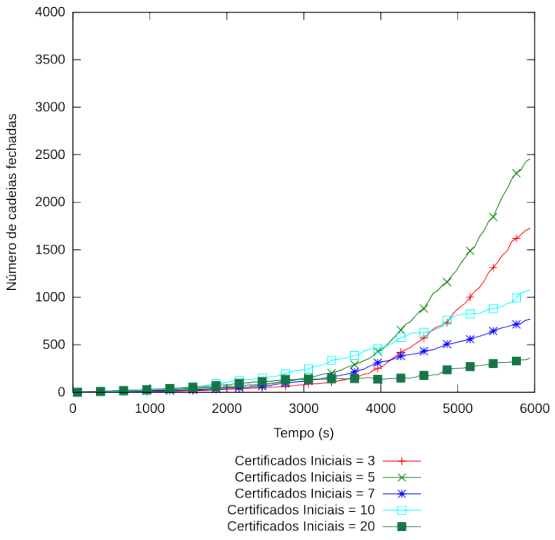
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

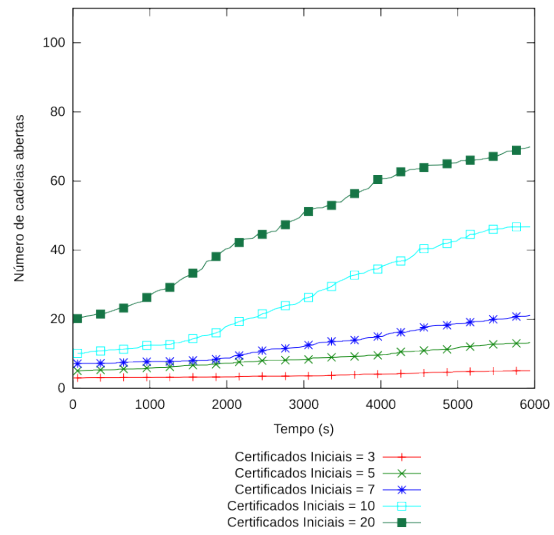
Figura C.57: Resultados para 75 nodos, $m = 10\%$ e $N_a = 50\%$



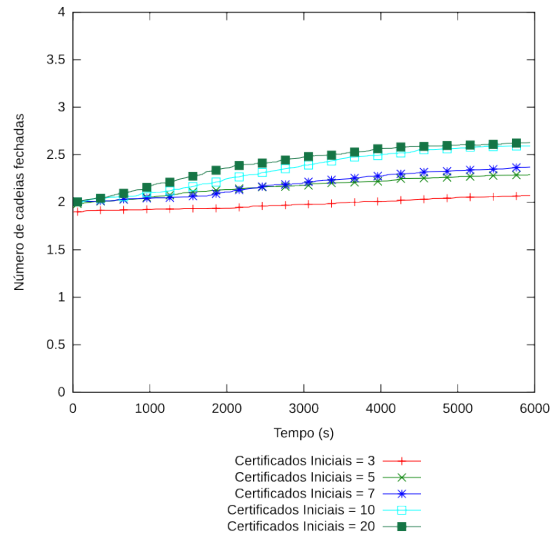

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



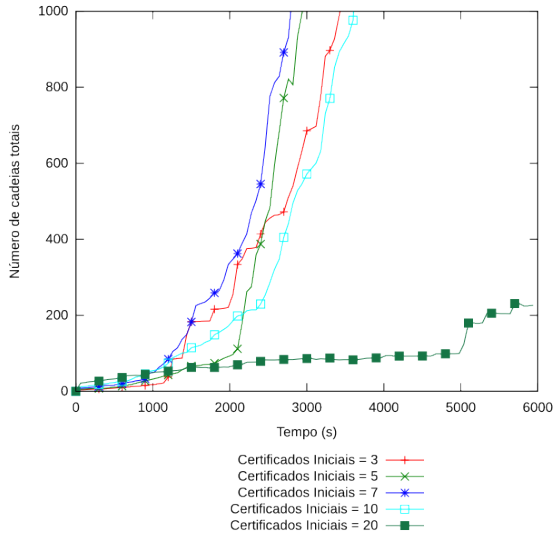

(c) Número de cadeias Abertas



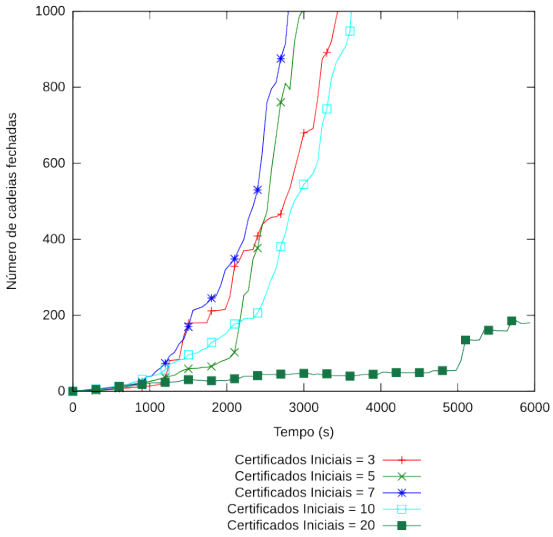

(d) Tamanho médio das cadeias

Figura C.58: Resultados para 100 nodos, $m = 10\%$ e $N_a = 50\%$

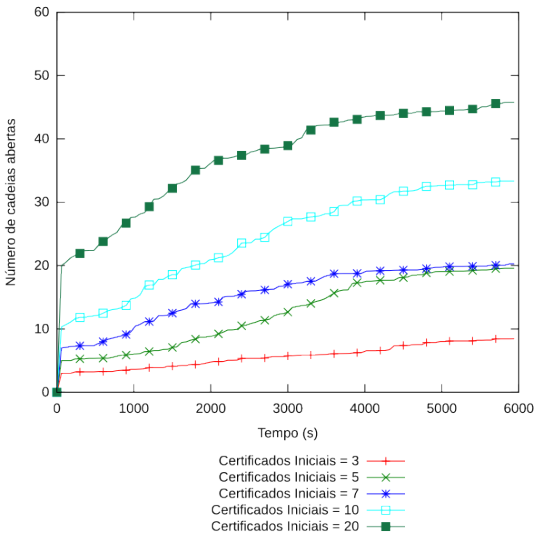
### C.5.4 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 10\%$



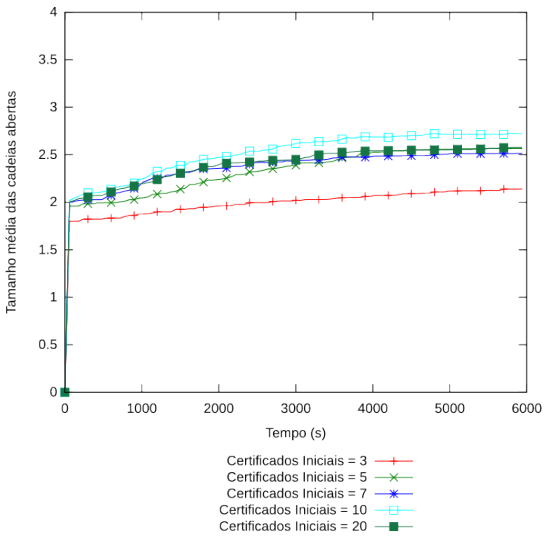

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

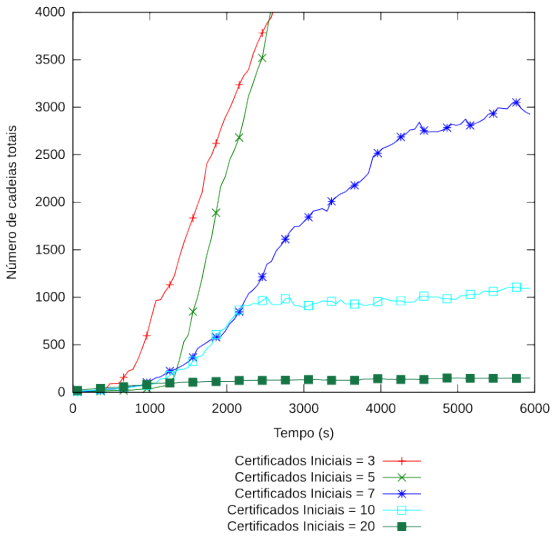



(c) Número de cadeias Abertas

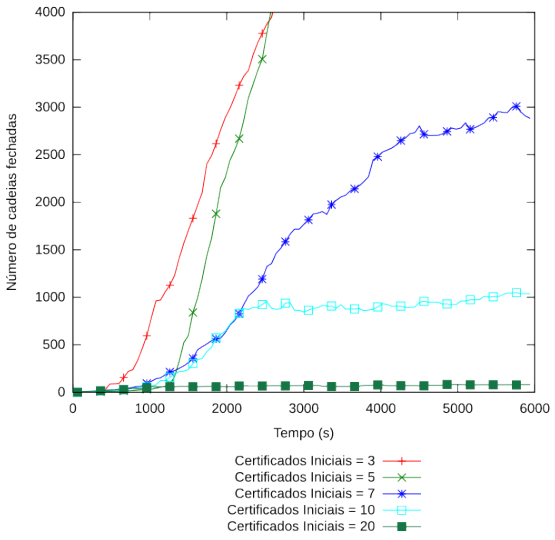



(d) Tamanho médio das cadeias

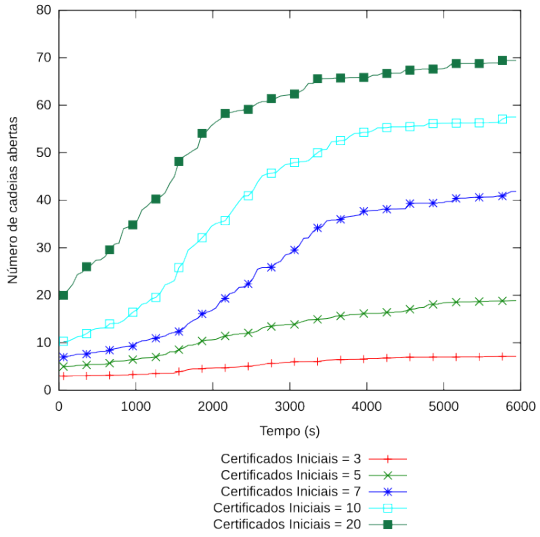
Figura C.59: Resultados para 50 nodos, $m = 20\%$ e $N_a = 10\%$



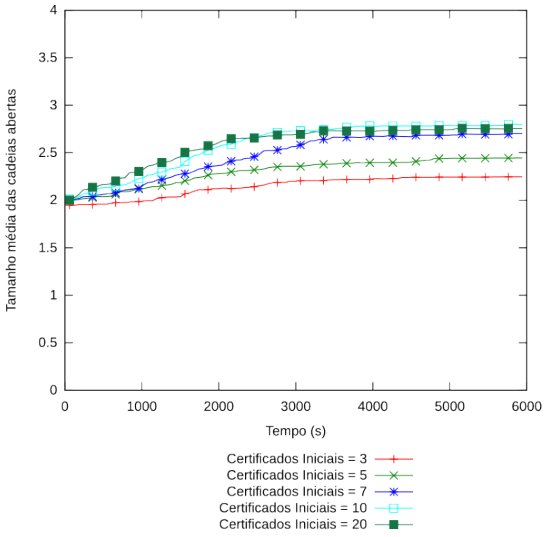

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

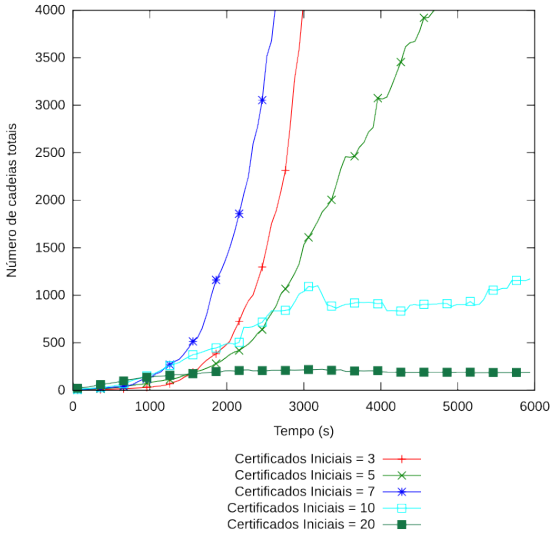



(c) Número de cadeias Abertas

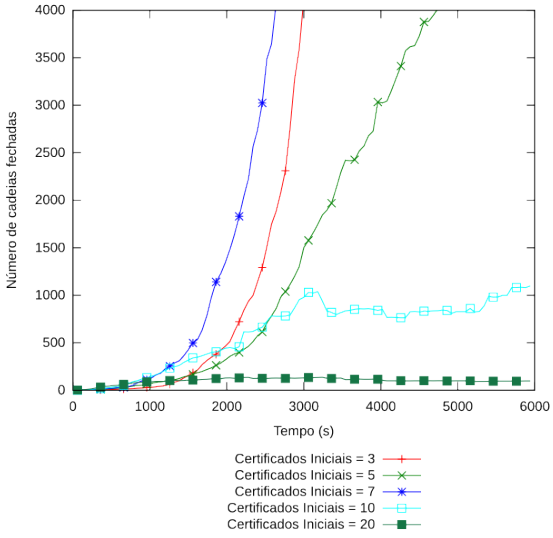



(d) Tamanho médio das cadeias

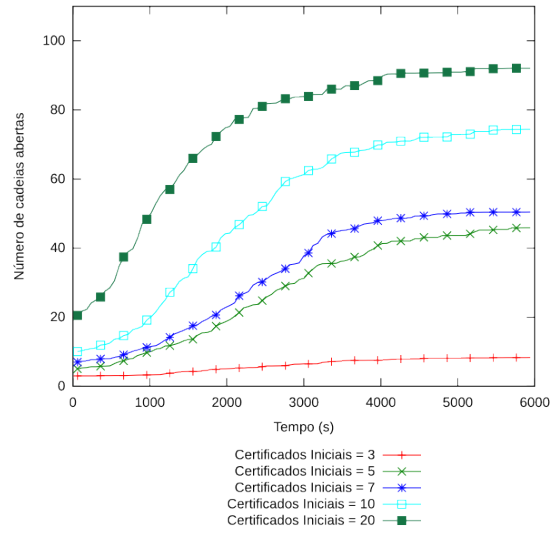
Figura C.60: Resultados para 75 nodos, $m = 20\%$ e $N_a = 10\%$



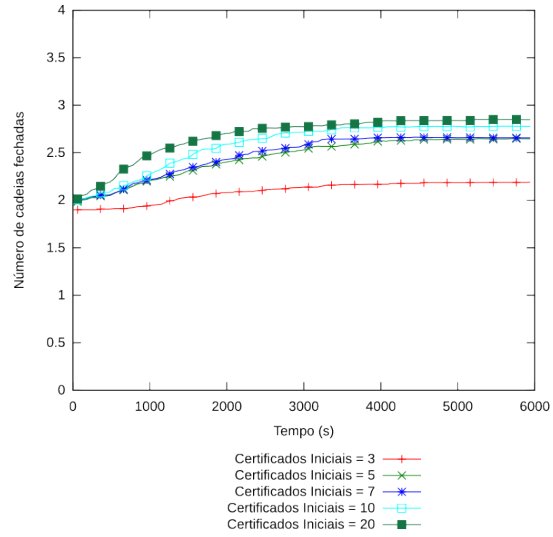

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

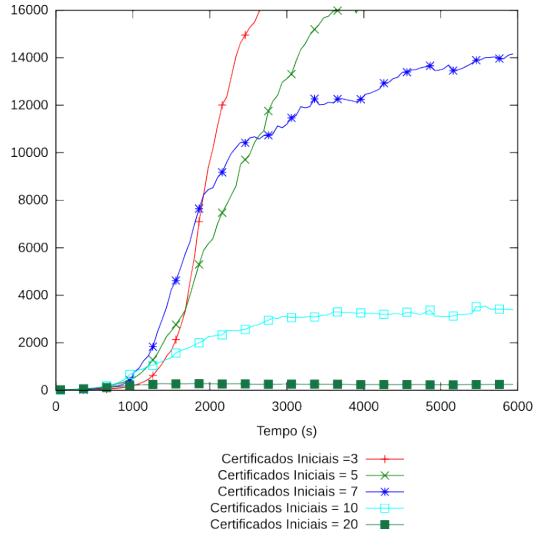



(c) Número de cadeias Abertas

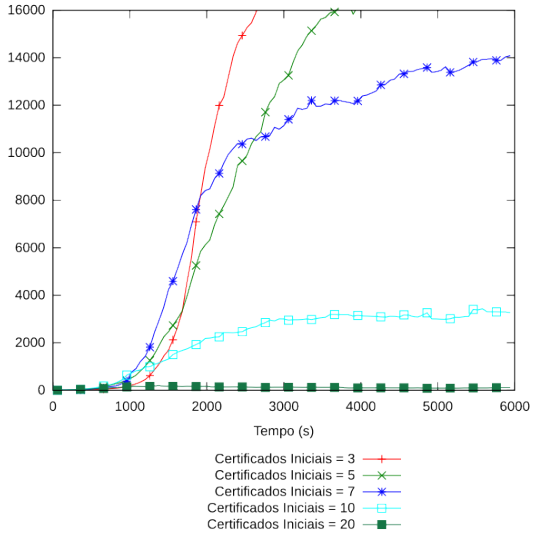



(d) Tamanho médio das cadeias

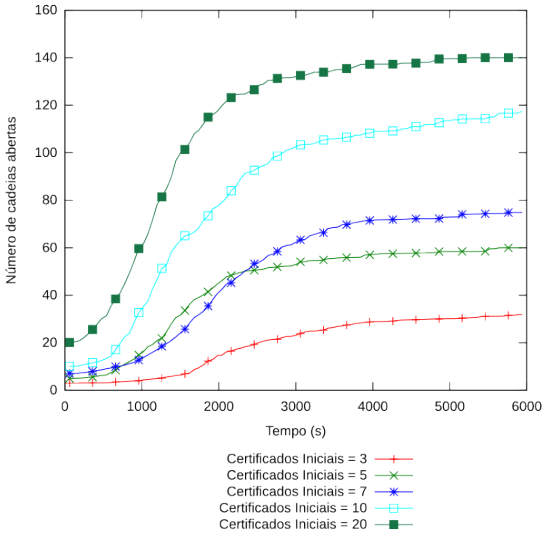
Figura C.61: Resultados para 100 nodos, $m = 20\%$ e $N_a = 10\%$



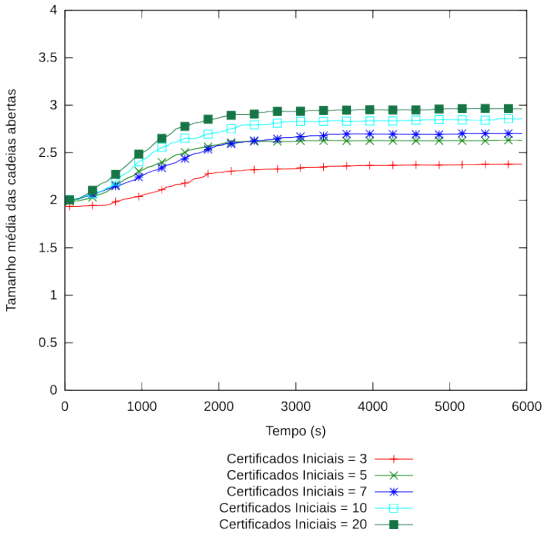

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



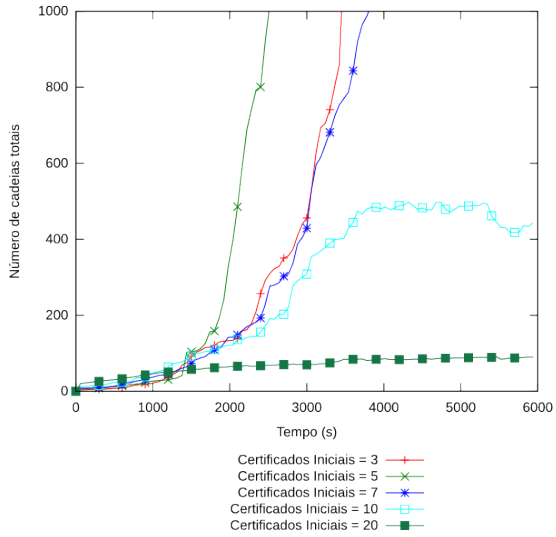

(c) Número de cadeias Abertas



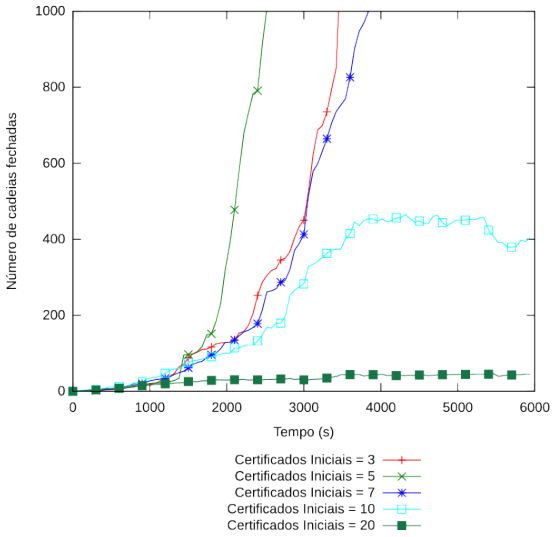

(d) Tamanho médio das cadeias

Figura C.62: Resultados para 150 nodos, $m = 20\%$ e $N_a = 10\%$

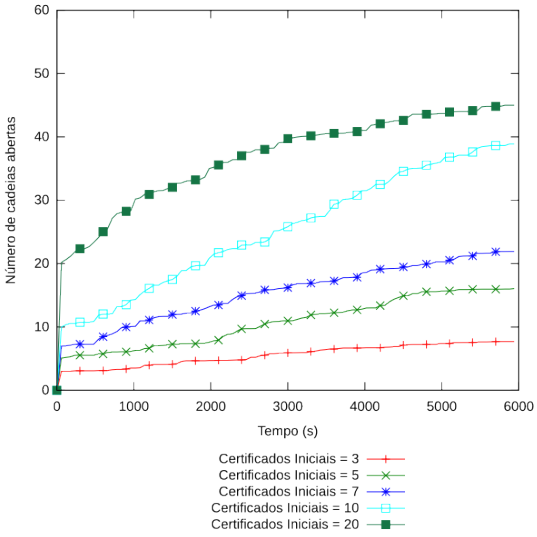
### C.5.5 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 25\%$



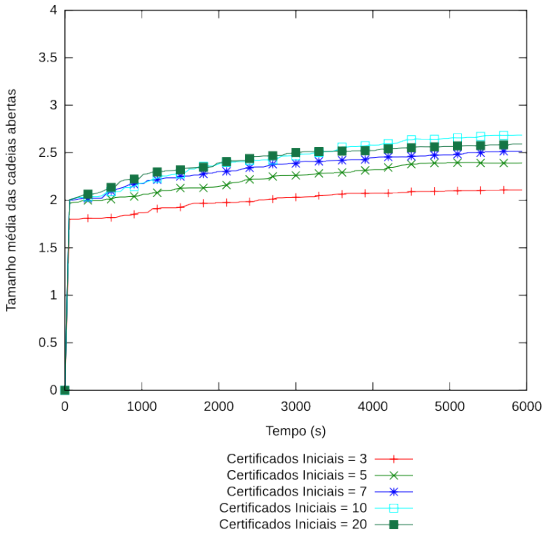

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

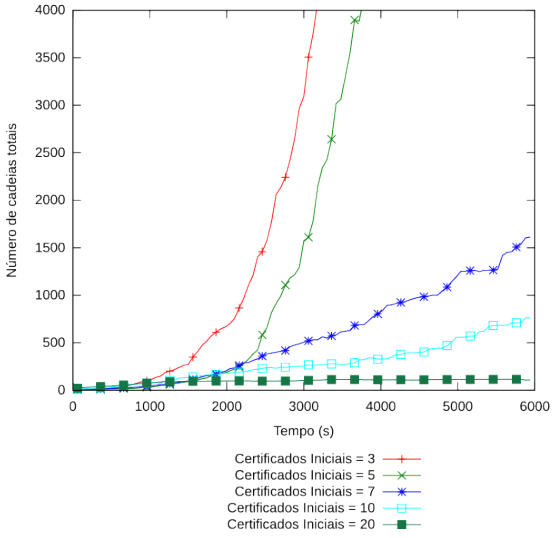



(c) Número de cadeias Abertas

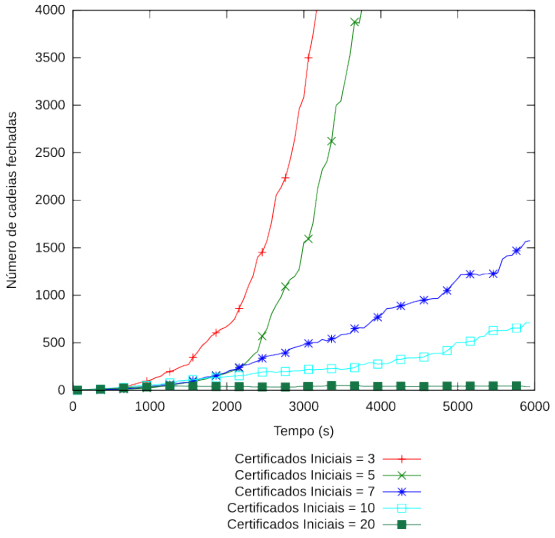



(d) Tamanho médio das cadeias

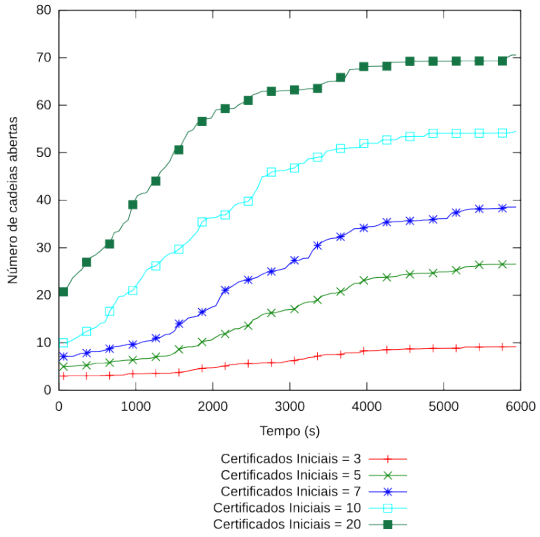
Figura C.63: Resultados para 50 nodos, $m = 20\%$ e $N_a = 25\%$



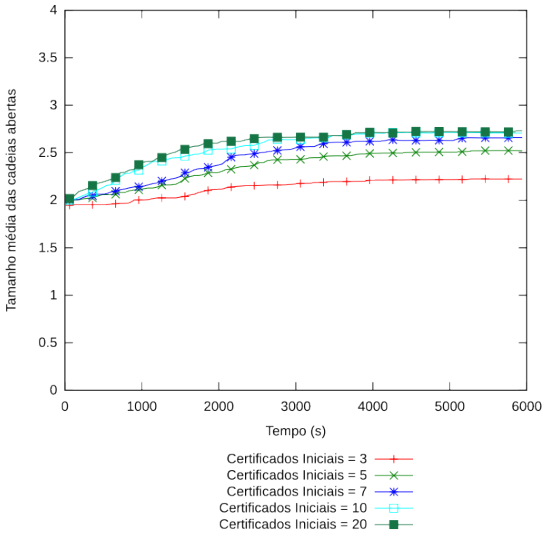

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

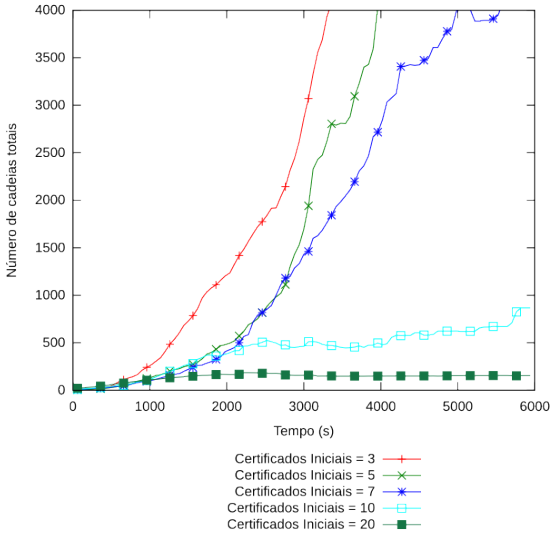



(c) Número de cadeias Abertas

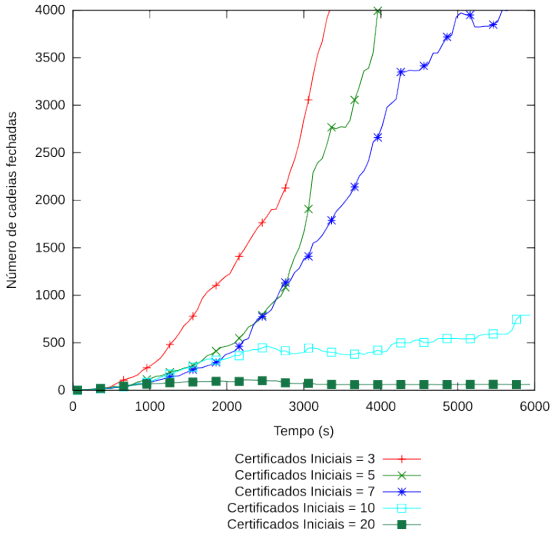



(d) Tamanho médio das cadeias

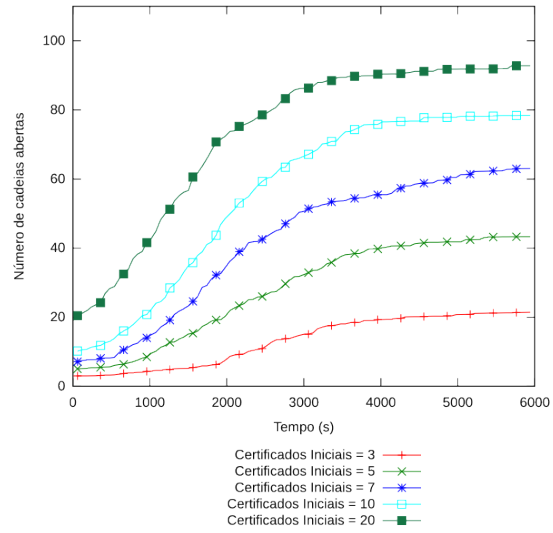
Figura C.64: Resultados para 75 nodos, $m = 20\%$ e $N_a = 25\%$



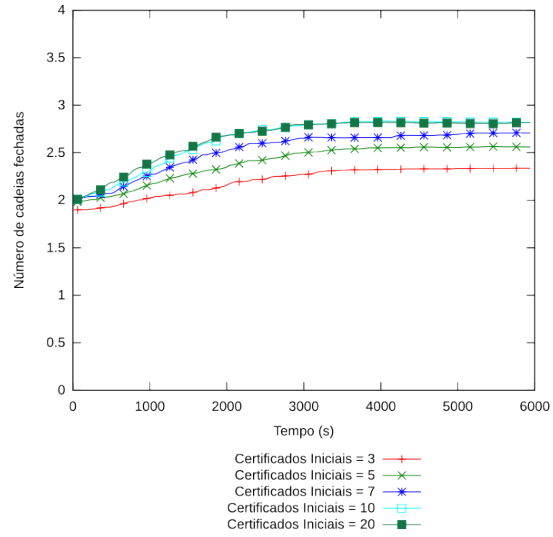

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

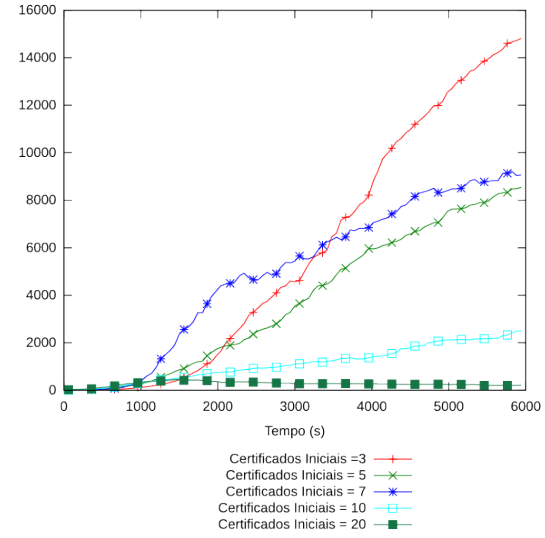



(c) Número de cadeias Abertas

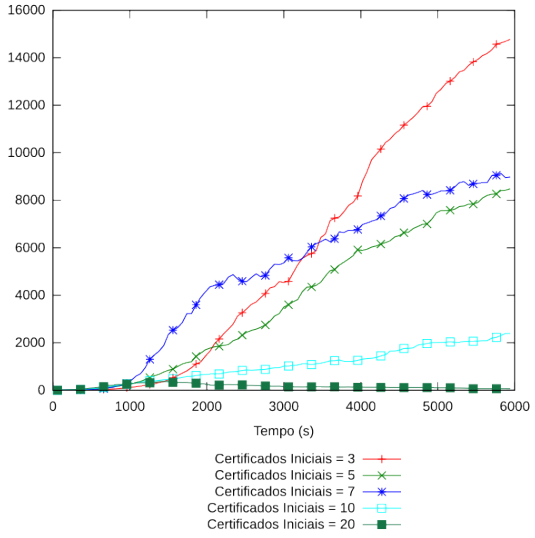



(d) Tamanho médio das cadeias

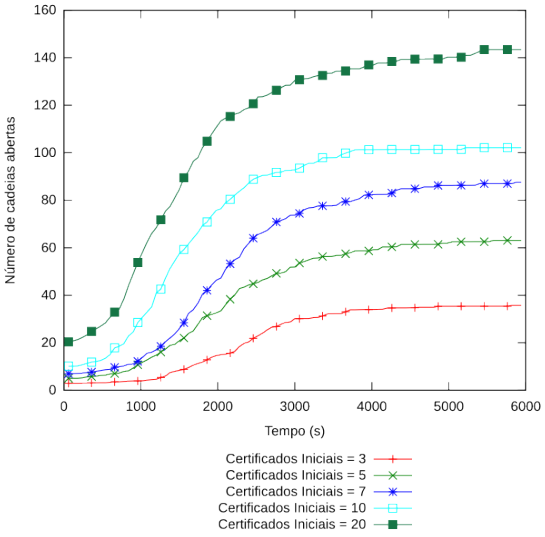
Figura C.65: Resultados para 100 nodos, $m = 20\%$ e $N_a = 25\%$



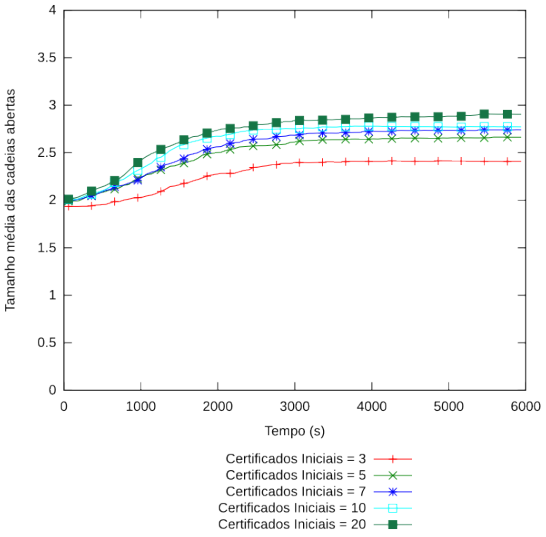

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



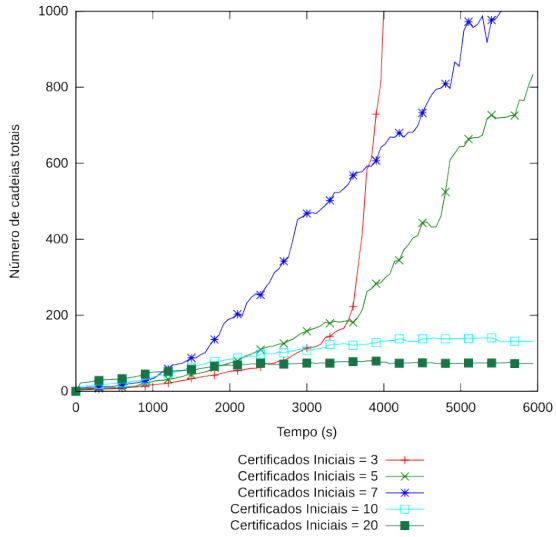

(c) Número de cadeias Abertas



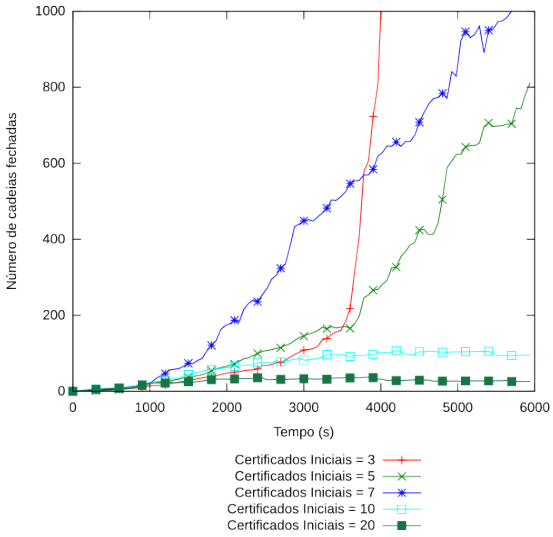

(d) Tamanho médio das cadeias

Figura C.66: Resultados para 150 nodos, $m = 20\%$ e $N_a = 25\%$

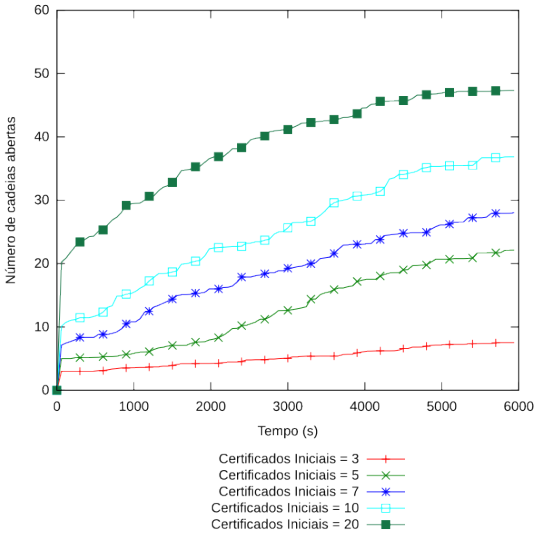
### C.5.6 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 50\%$



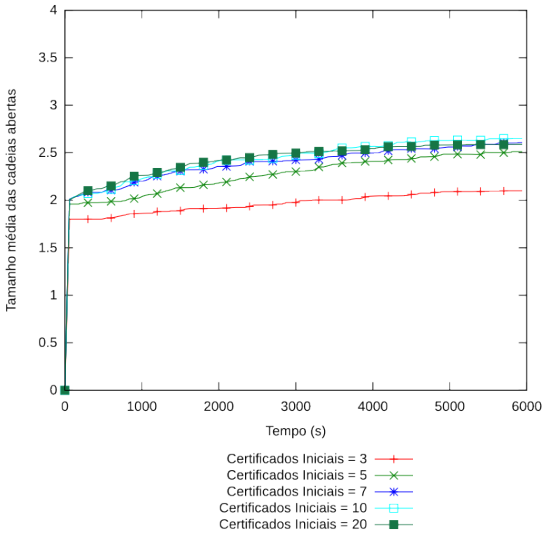

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

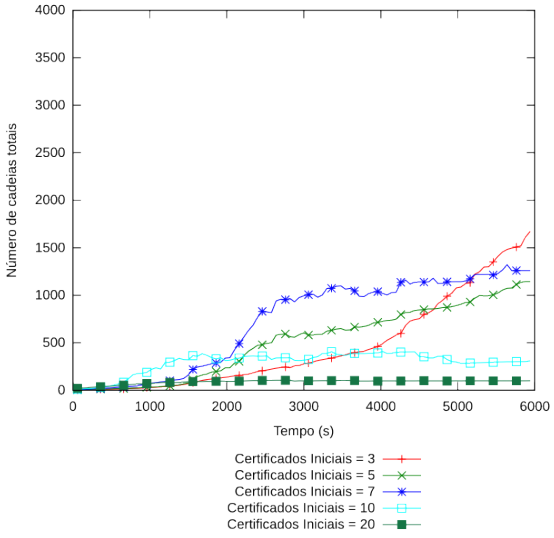



(c) Número de cadeias Abertas

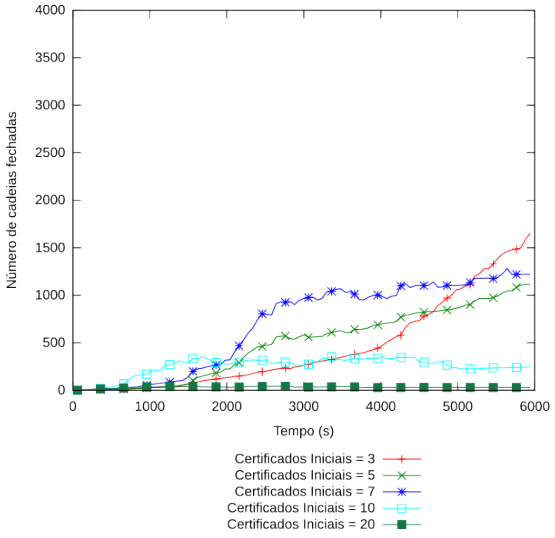



(d) Tamanho médio das cadeias

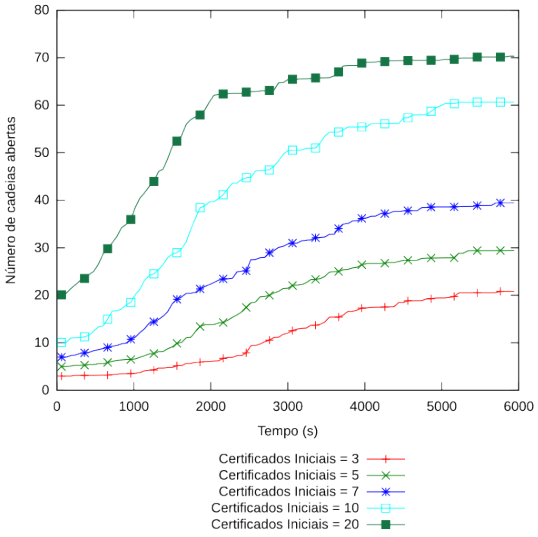
Figura C.67: Resultados para 50 nodos, $m = 20\%$ e $N_a = 50\%$



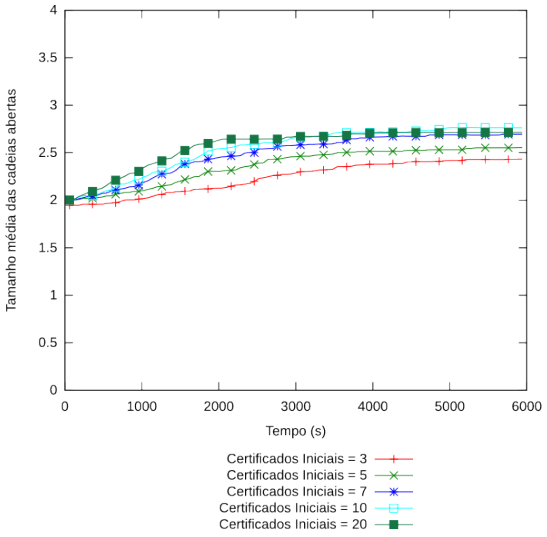

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

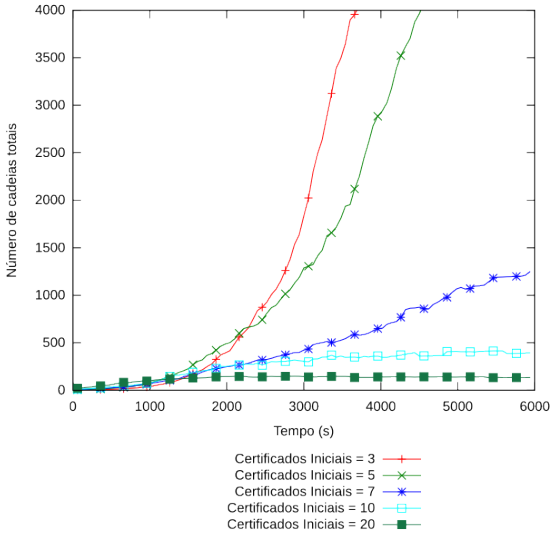



(c) Número de cadeias Abertas

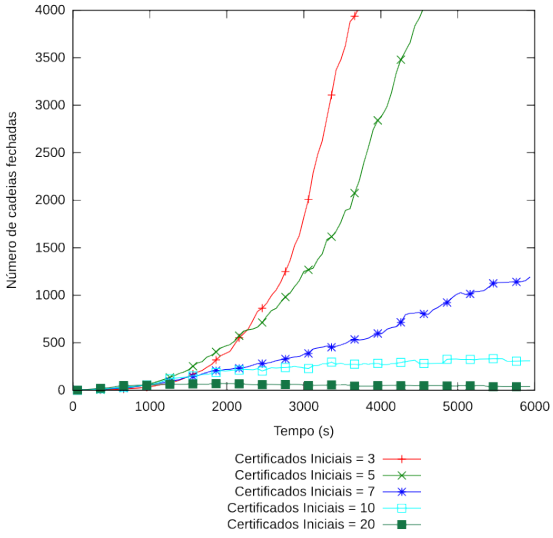



(d) Tamanho médio das cadeias

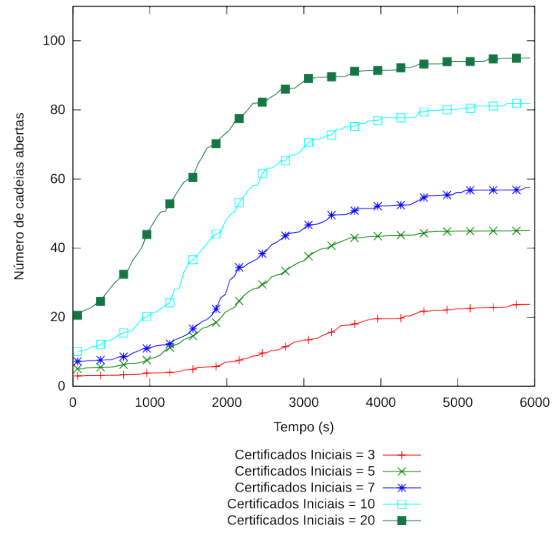
Figura C.68: Resultados para 75 nodos, $m = 20\%$ e $N_a = 50\%$



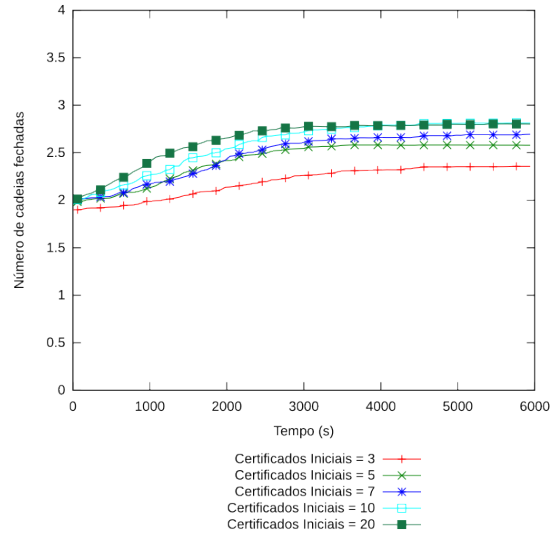

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

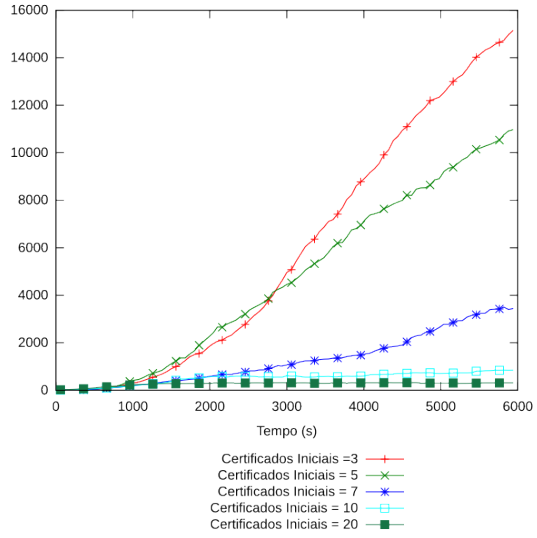



(c) Número de cadeias Abertas

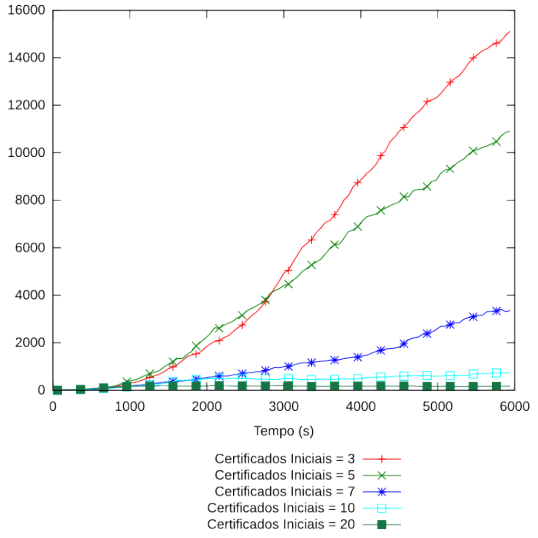



(d) Tamanho médio das cadeias

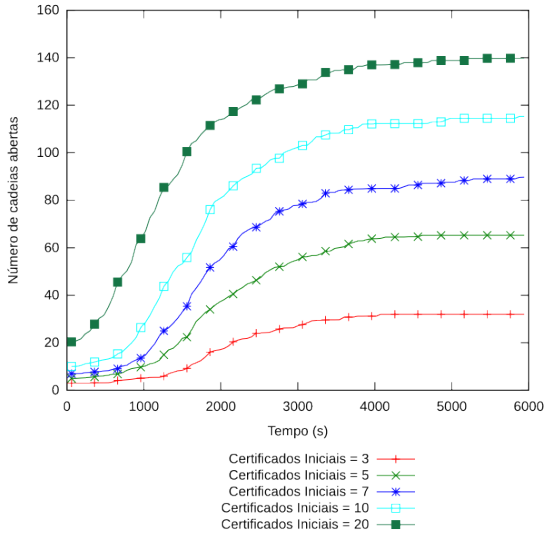
Figura C.69: Resultados para 100 nodos, $m = 20\%$ e $N_a = 50\%$



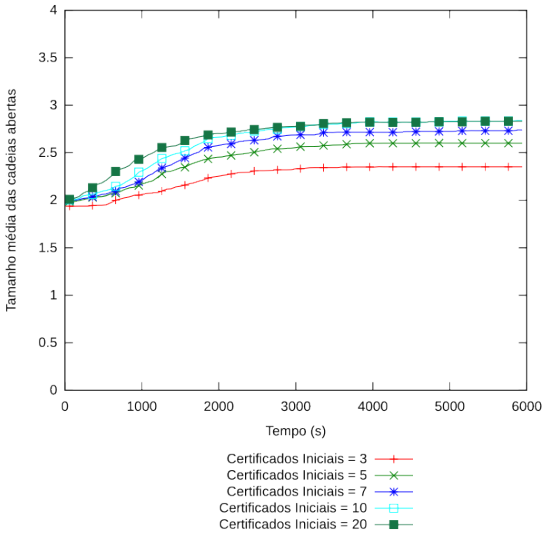

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



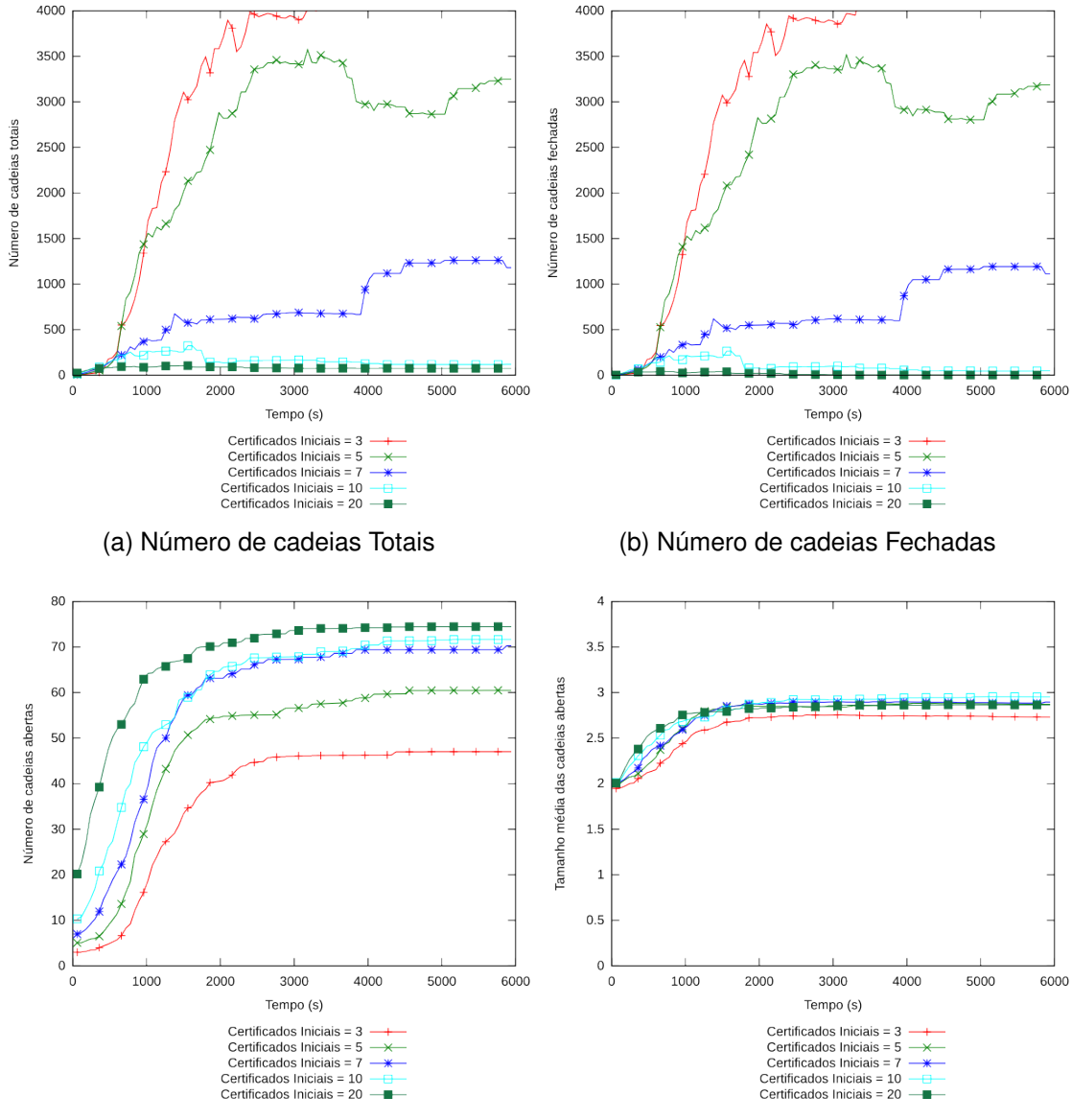

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.70: Resultados para 150 nodos, $m = 20\%$ e $N_a = 50\%$

### C.5.7 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 10\%$



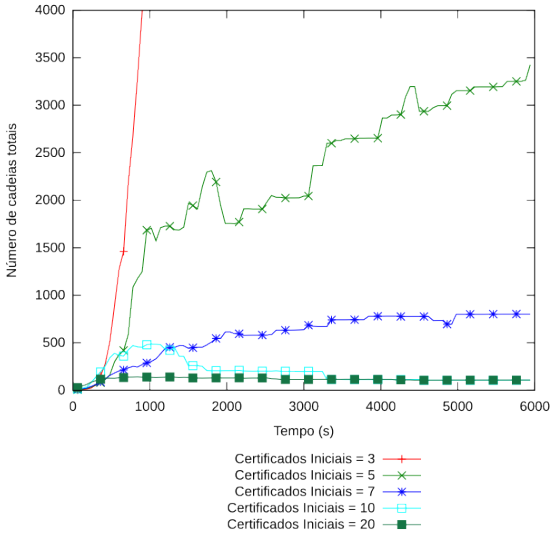

(a) Número de cadeias Totais

(b) Número de cadeias Fechadas

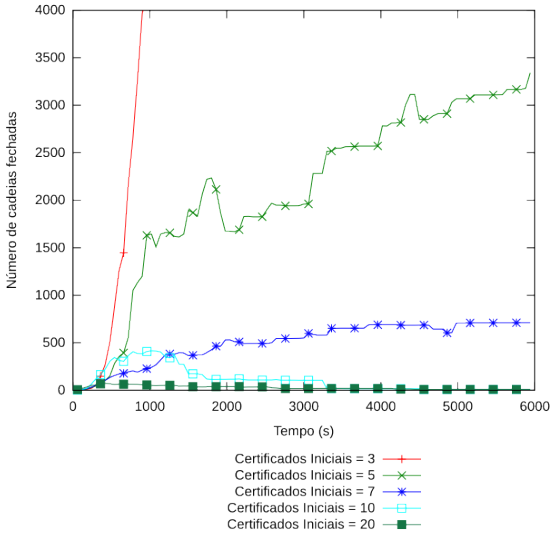
(c) Número de cadeias Abertas

(d) Tamanho médio das cadeias

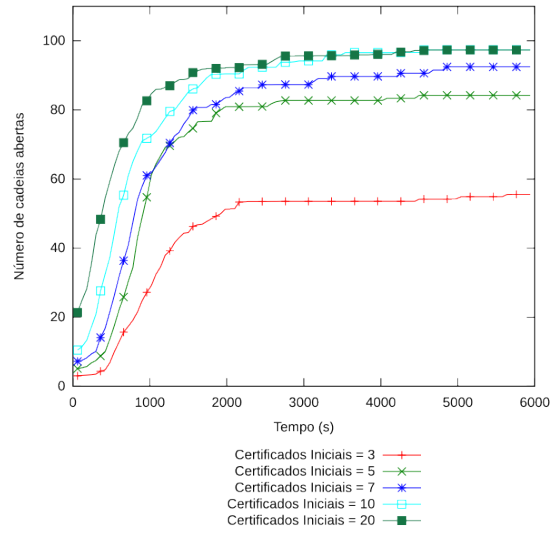
Figura C.71: Resultados para 75 nodos, $m = 50\%$ e $N_a = 10\%$



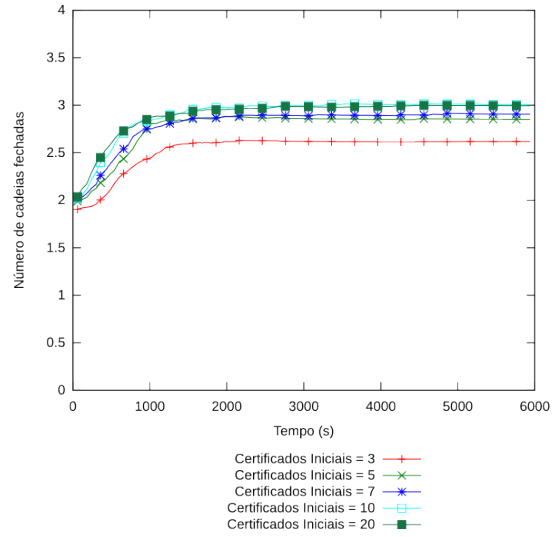

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



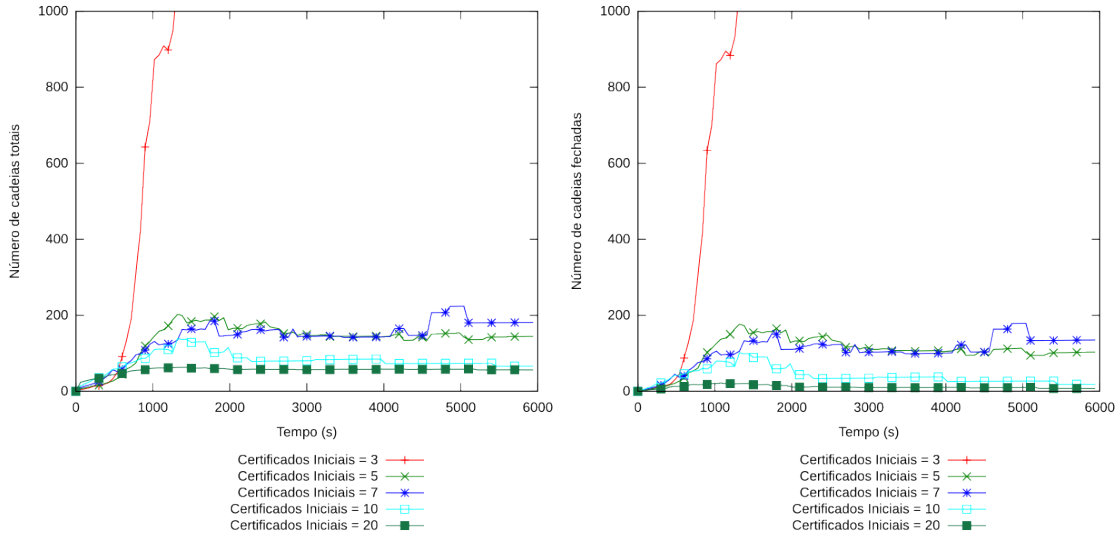

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.72: Resultados para 100 nodos, $m = 50\%$ e $N_a = 10\%$

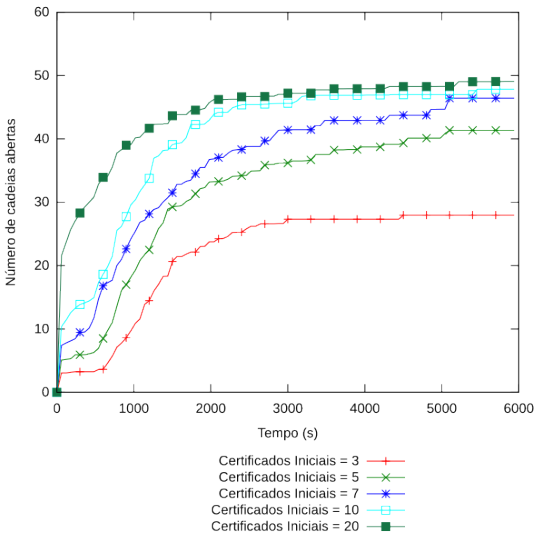
### C.5.8 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 25\%$



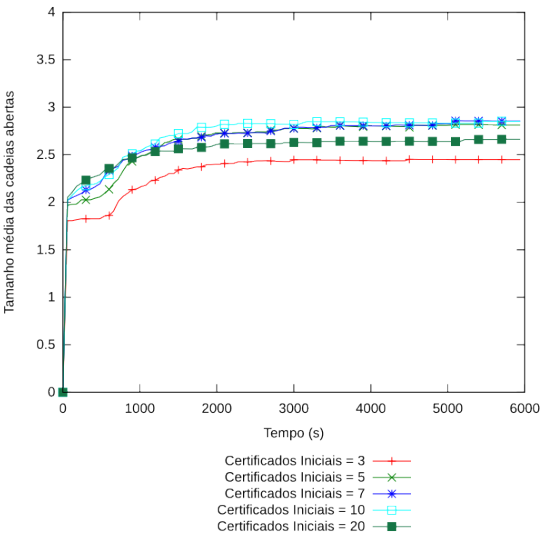

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

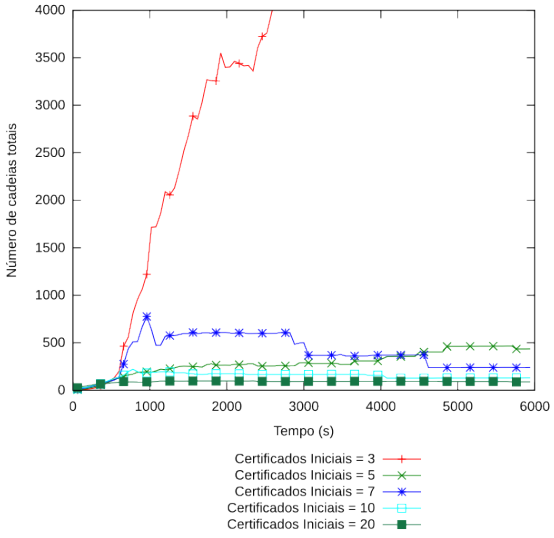



(c) Número de cadeias Abertas

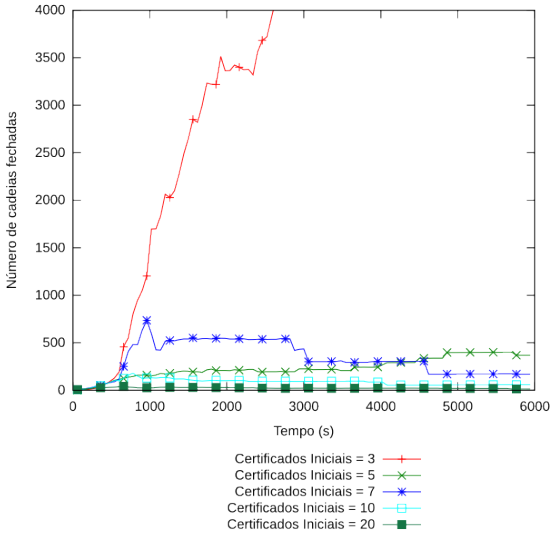



(d) Tamanho médio das cadeias

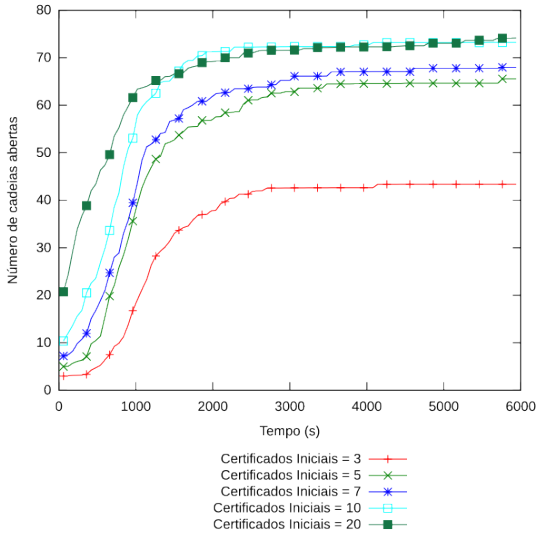
Figura C.73: Resultados para 50 nodos, $m = 50\%$ e $N_a = 25\%$



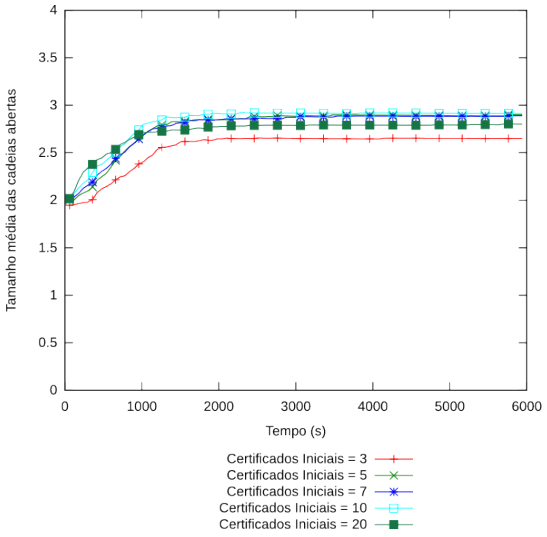

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

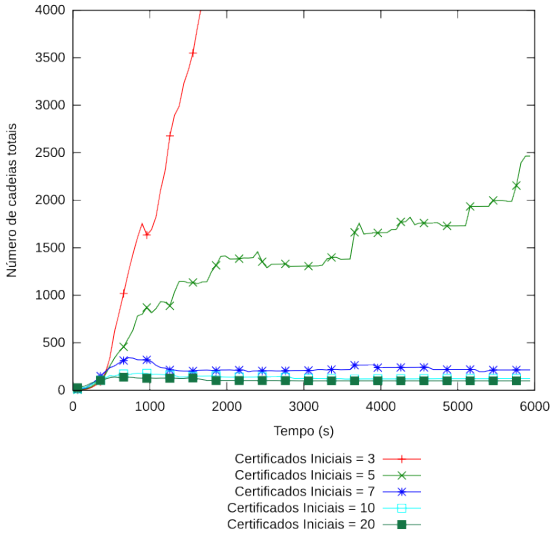



(c) Número de cadeias Abertas

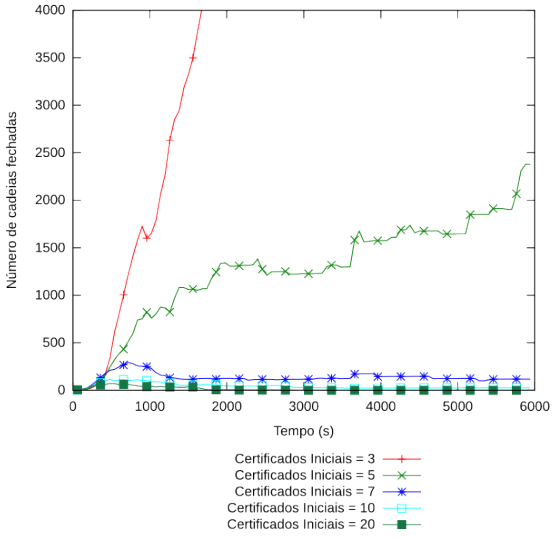



(d) Tamanho médio das cadeias

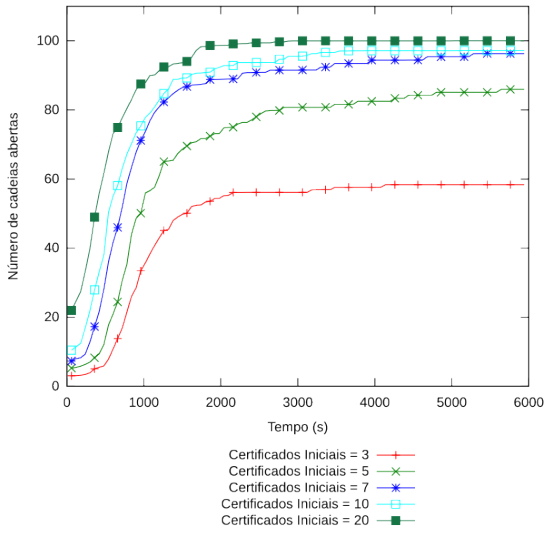
Figura C.74: Resultados para 75 nodos, $m = 50\%$ e $N_a = 25\%$



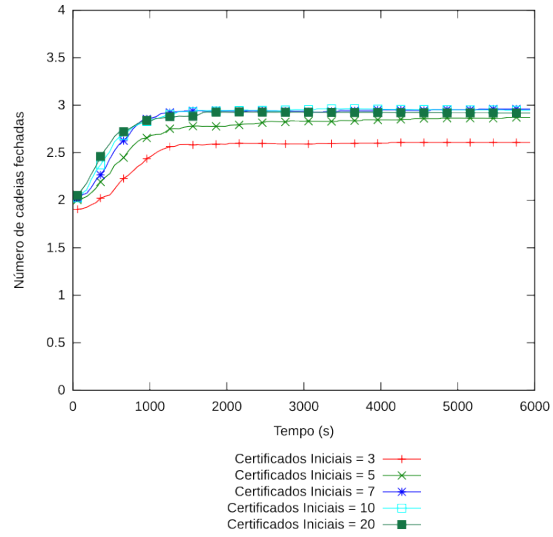

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

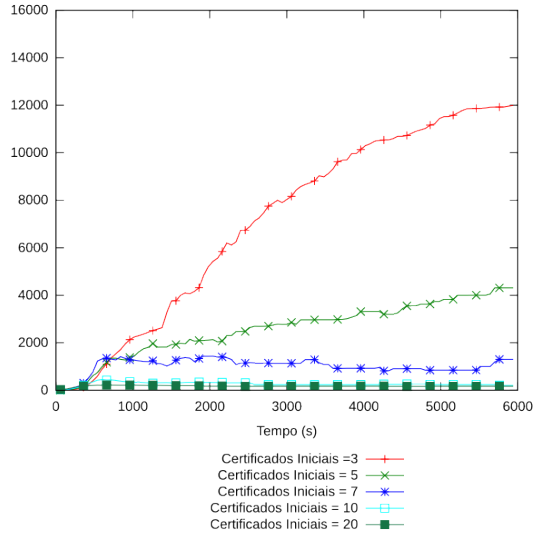



(c) Número de cadeias Abertas

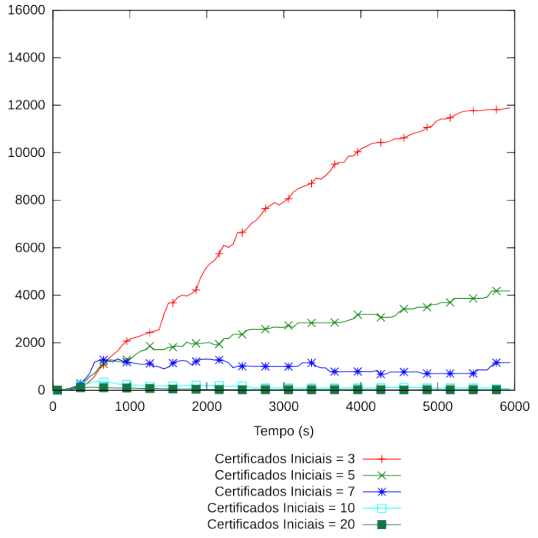



(d) Tamanho médio das cadeias

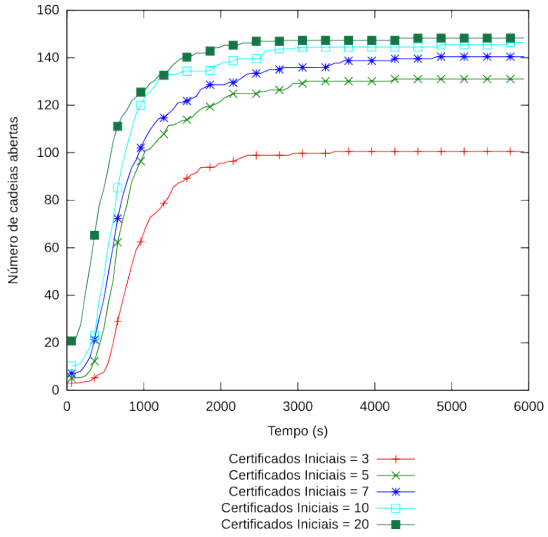
Figura C.75: Resultados para 100 nodos, $m = 50\%$ e $N_a = 25\%$



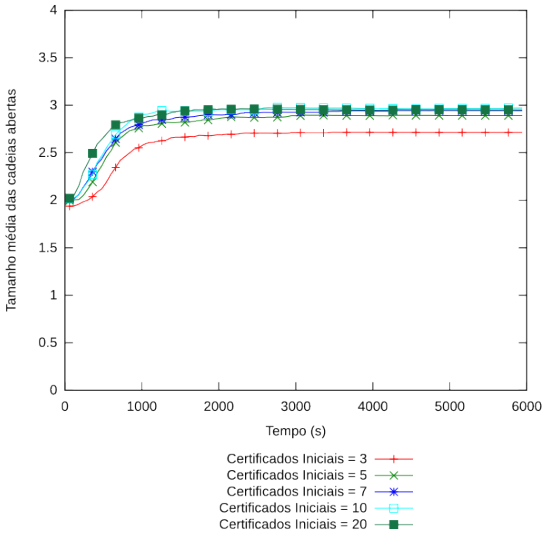

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



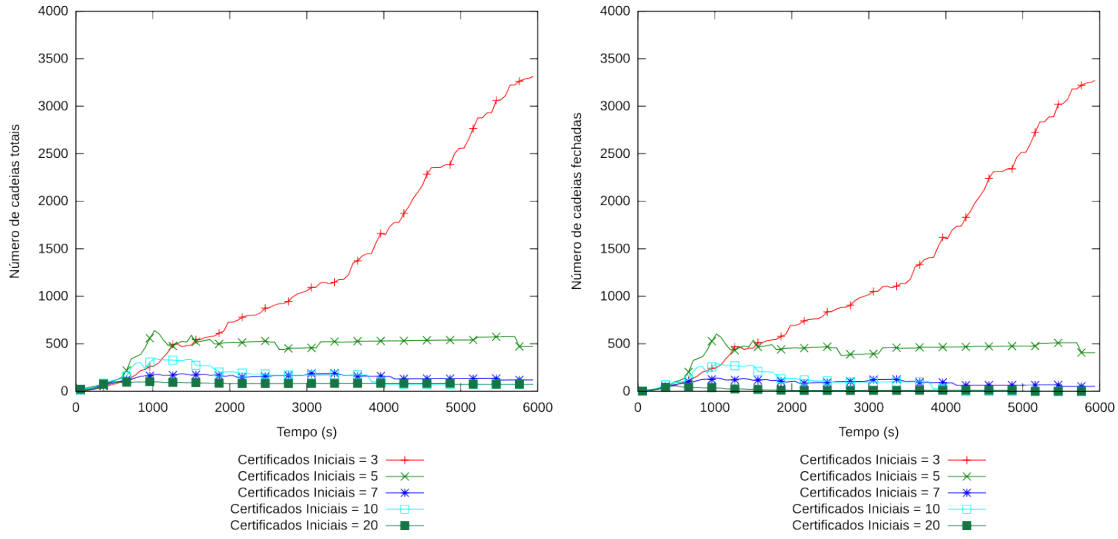

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura C.76: Resultados para 150 nodos, $m = 50\%$ e $N_a = 25\%$

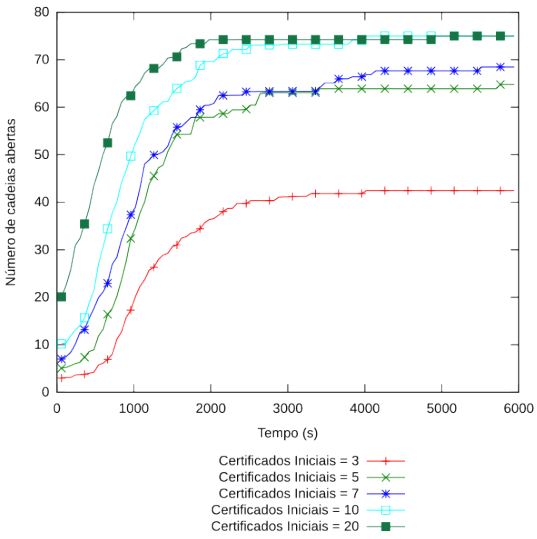
### C.5.9 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 50\%$



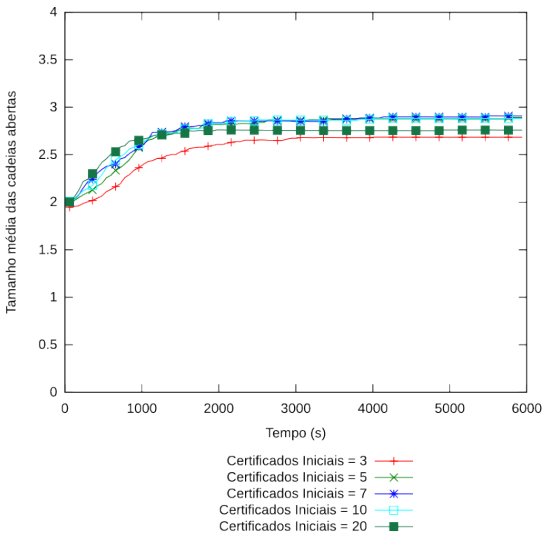

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

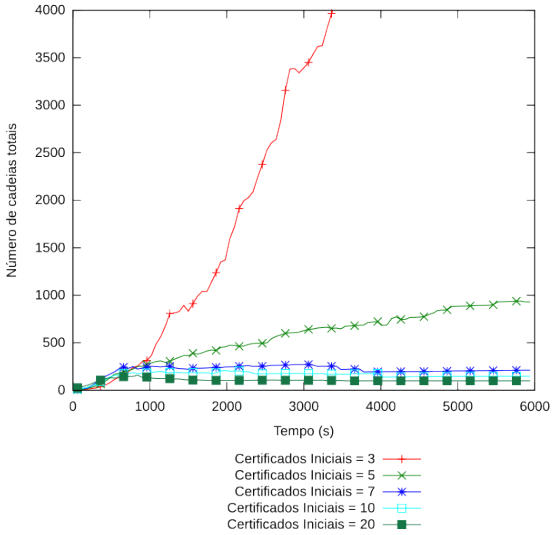



(c) Número de cadeias Abertas

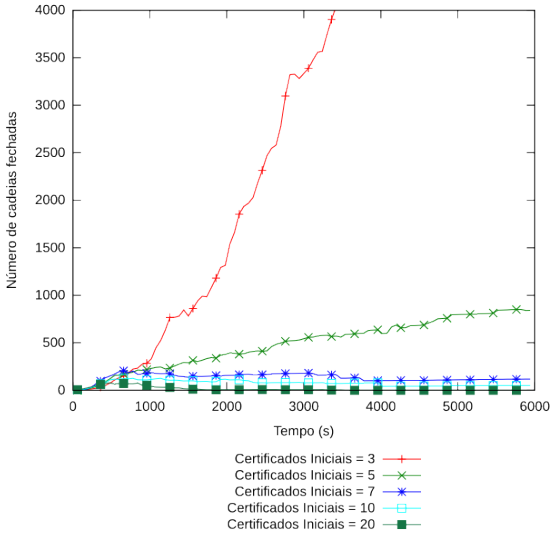



(d) Tamanho médio das cadeias

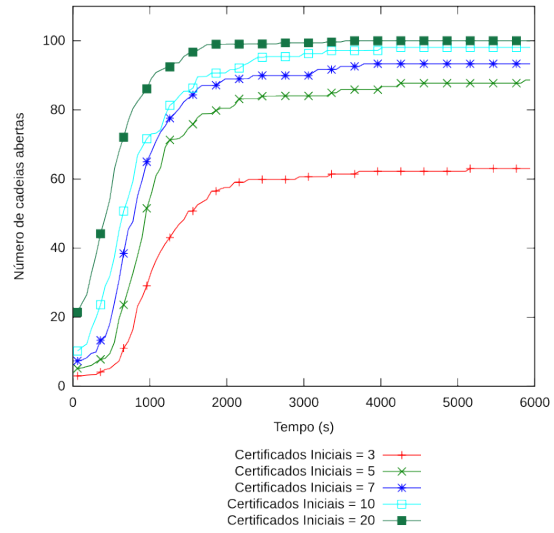
Figura C.77: Resultados para 75 nodos, $m = 50\%$ e $N_a = 50\%$



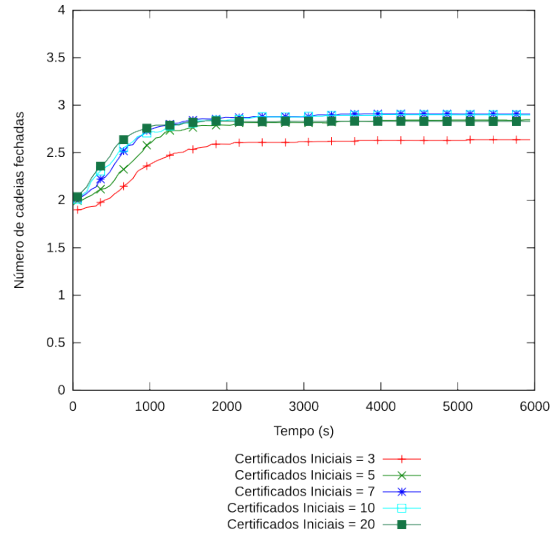

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

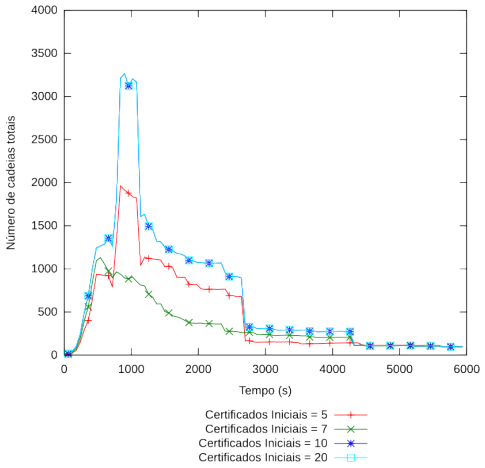
Figura C.78: Resultados para 100 nodos, $m = 50\%$ e $N_a = 50\%$

# APÊNDICE D

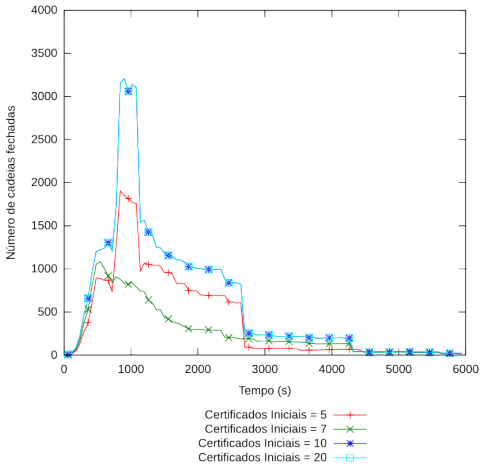
# RESULTADOS - DISTRIBUIÇÃO CENTRALIZADA DE CERTIFICADOS INICIAIS EM 10% DOS NODOS

Neste apêndice são apresentaddos os gráficos omitidos no Capítulo 4 da distribuição centralizada de certificados iniciais em 10% dos nodos. Os gráficos estão organizados da seguinte forma: Versão Otimizada seguida dos ataques *GreyHole*, *BlackHole*, *Sybil* e de Falsificação.

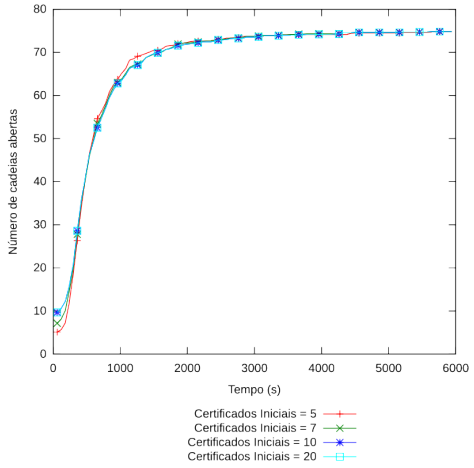
## D.1 Versão Otimizada



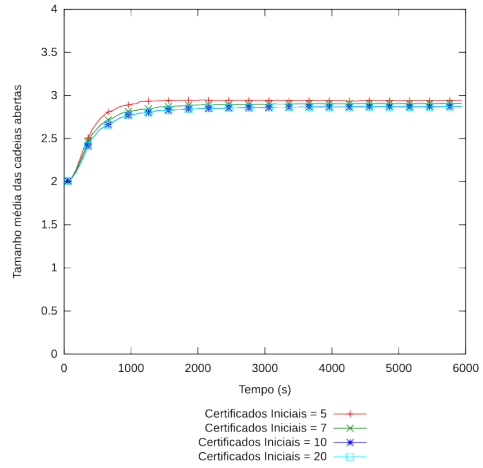

(a) Número de cadeias totais




(b) Número de cadeias fechadas

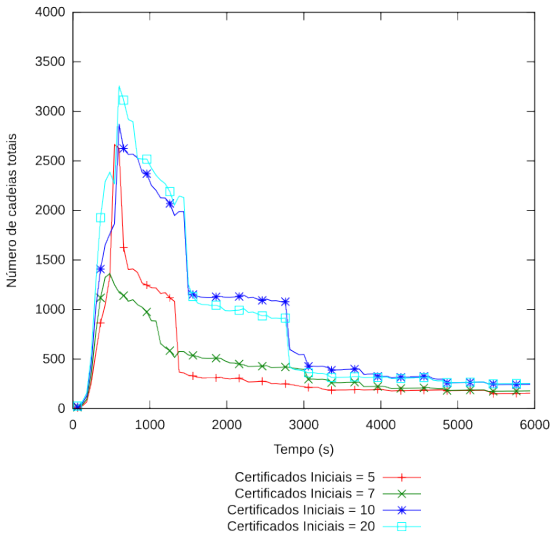



(c) Número de cadeias abertas

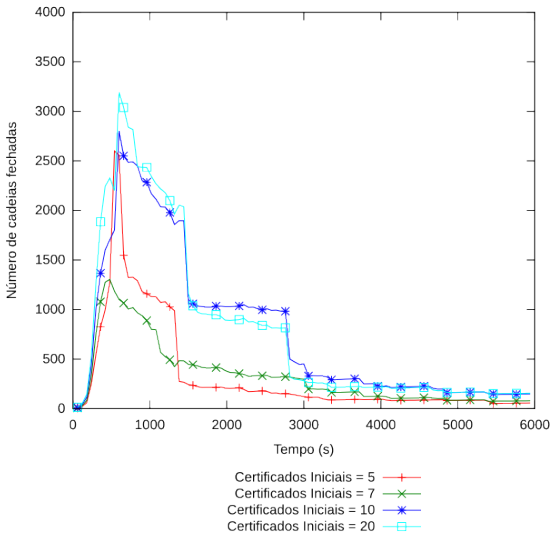



(d) Tamanho médio das cadeias

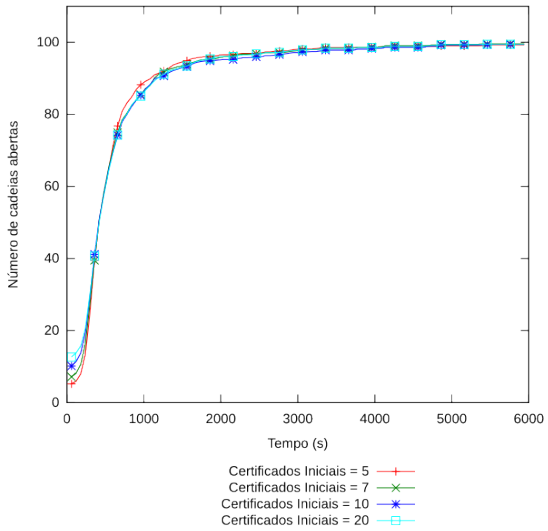
Figura D.1: Resultados com algoritmo otimizado para 75 nodos



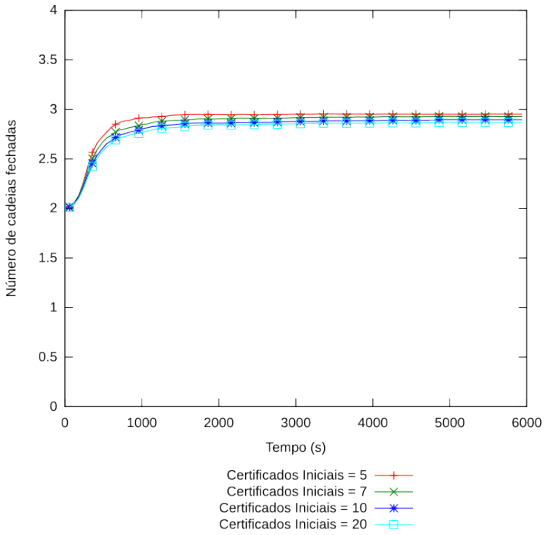

(a) Número de cadeias totais




(b) Número de cadeias fechadas




(c) Número de cadeias abertas

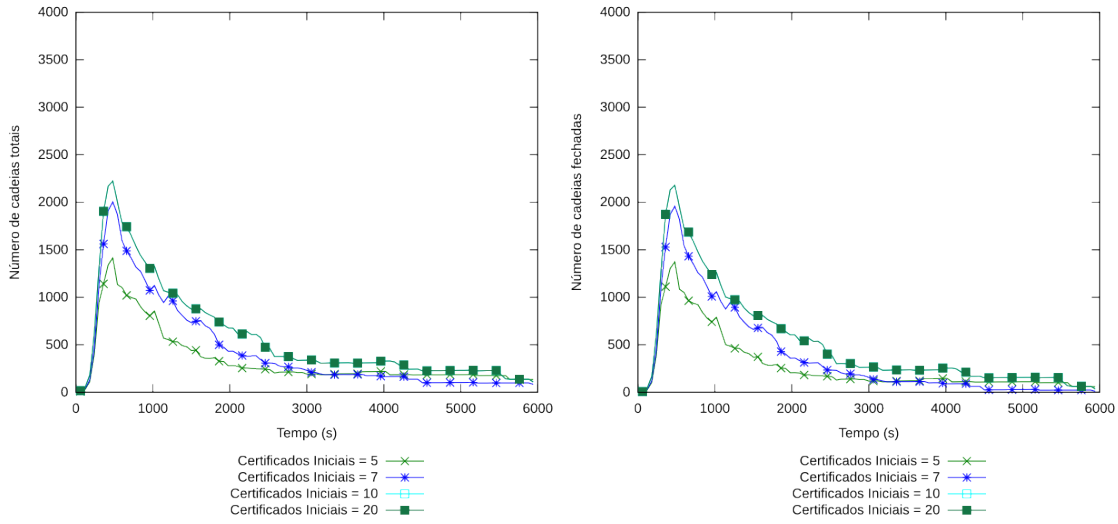



(d) Tamanho médio das cadeias

Figura D.2: Resultados com algoritmo otimizado para 100 nodos

## D.2 Ataque *GreyHole*

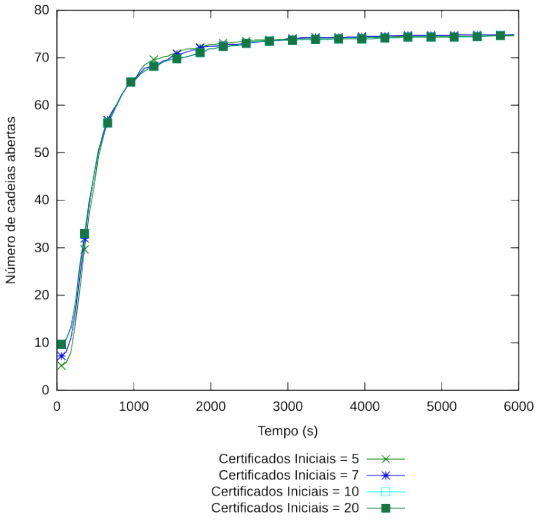
### D.2.1 Ataque *GreyHole* com $m = 10\%$ e $t = 10\%$



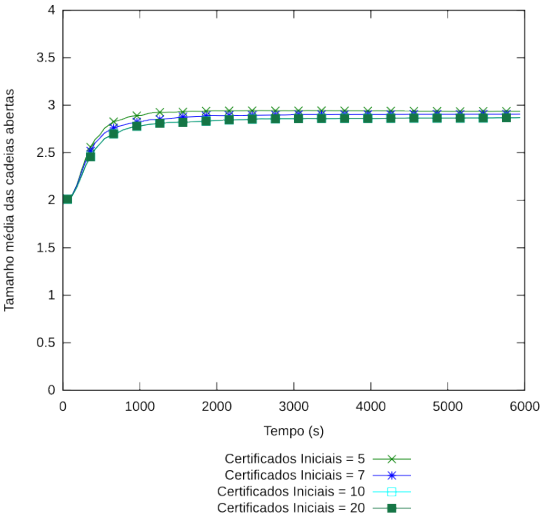

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

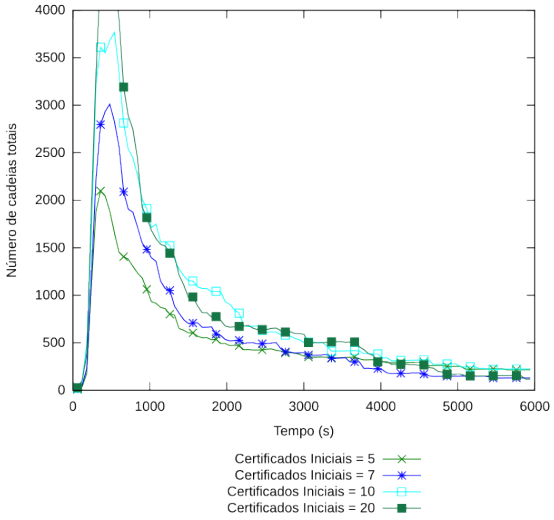



(c) Número de cadeias Abertas

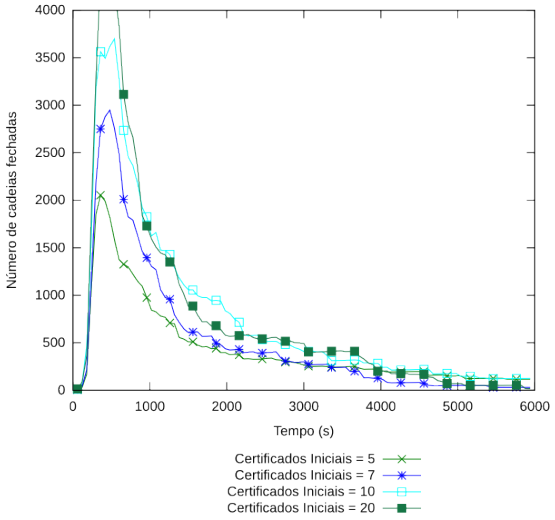



(d) Tamanho médio das cadeias

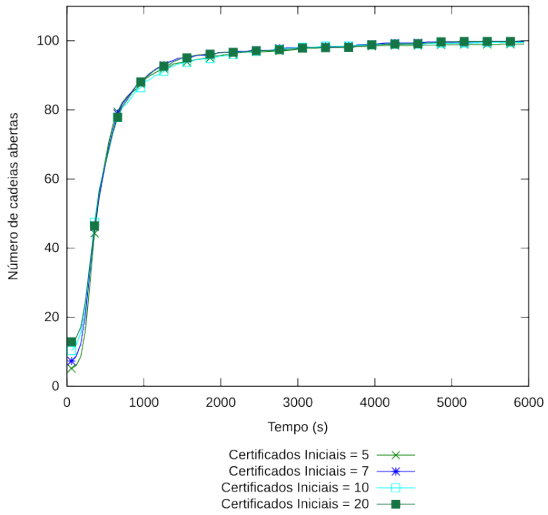
Figura D.3: Resultados para 75 nodos, $m = 10\%$ e $t = 10\%$



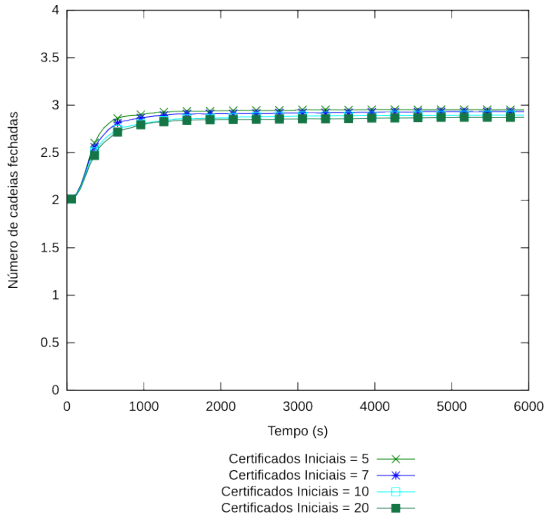

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



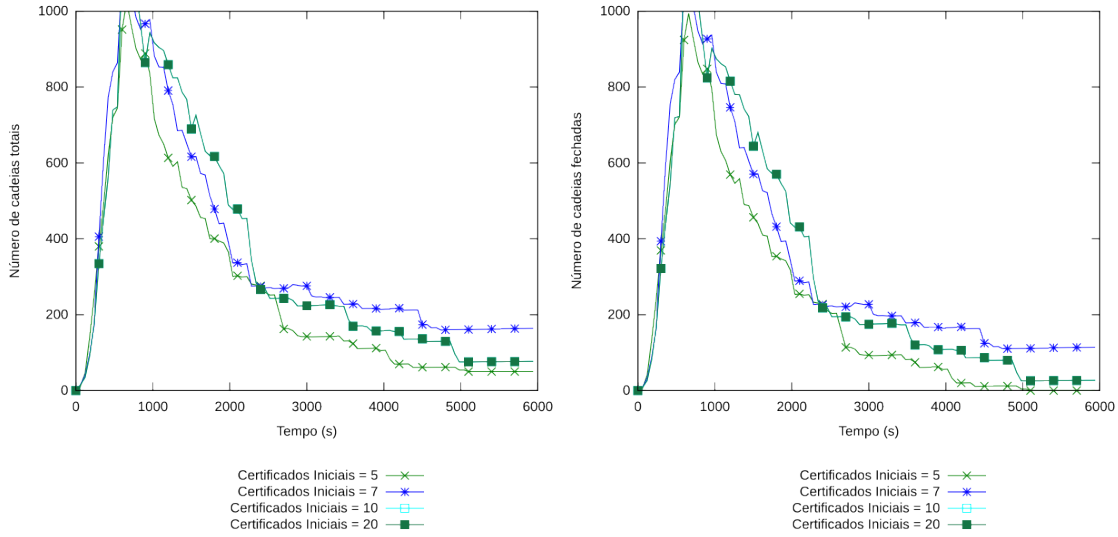

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura D.4: Resultados para 100 nodos, $m = 10\%$ e $t = 10\%$

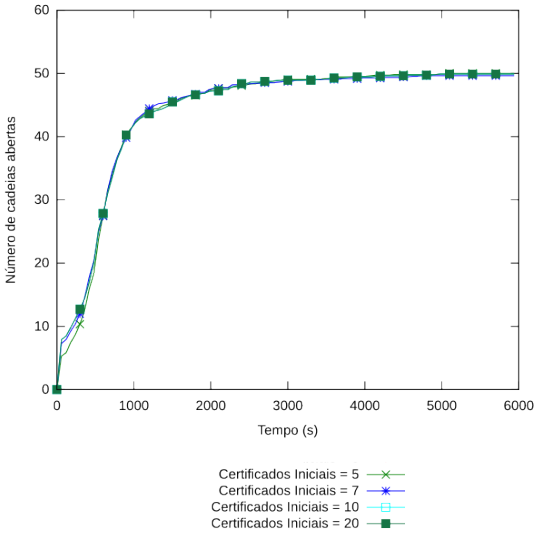
### D.2.2 Ataque *GreyHole* com $m = 10\%$ e $t = 25\%$



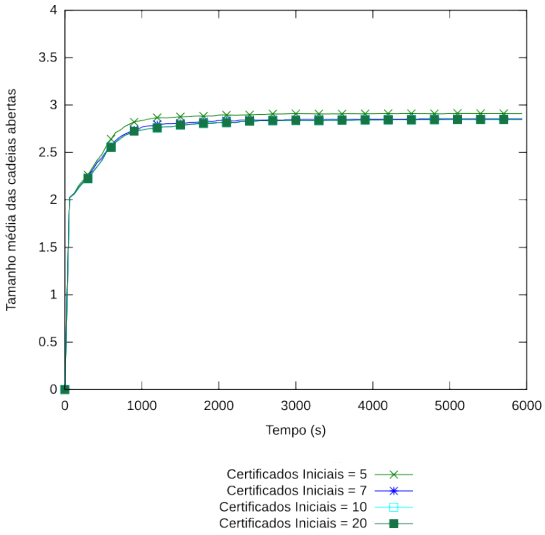

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

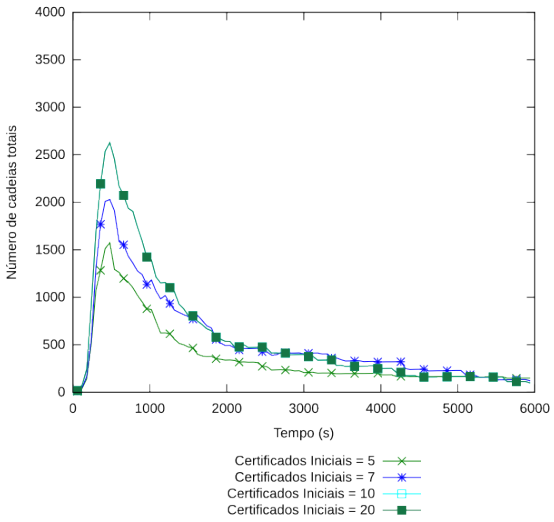



(c) Número de cadeias Abertas

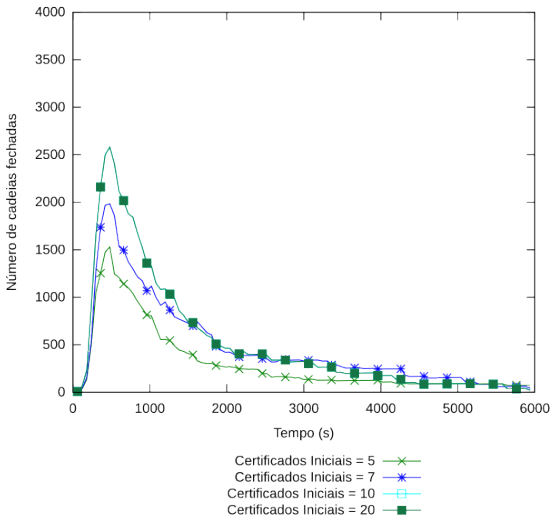



(d) Tamanho médio das cadeias

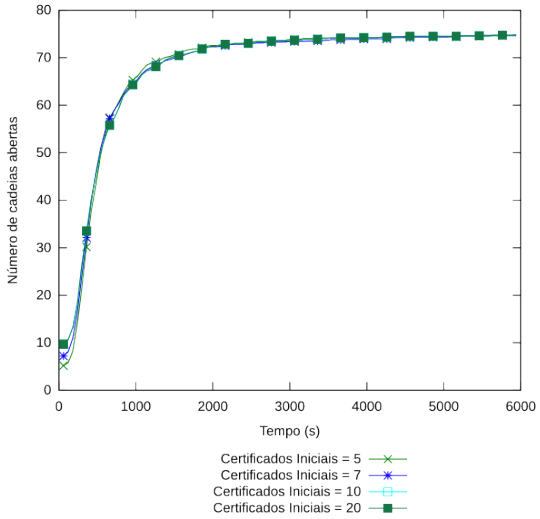
Figura D.5: Resultados para 50 nodos, $m = 10\%$ e $t = 25\%$



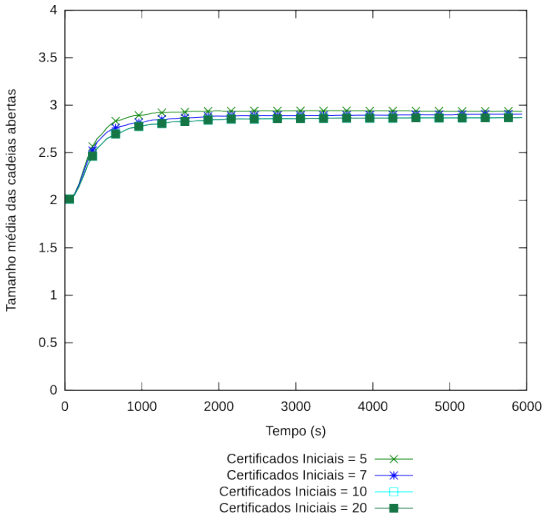

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

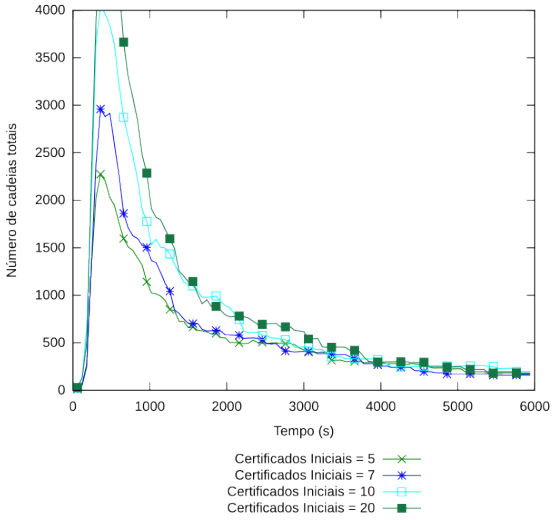



(c) Número de cadeias Abertas

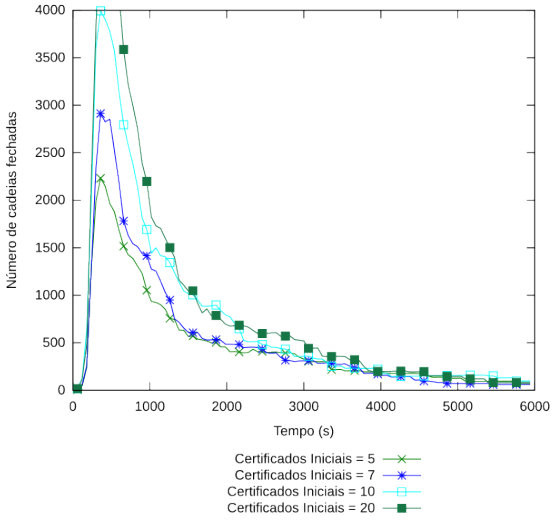



(d) Tamanho médio das cadeias

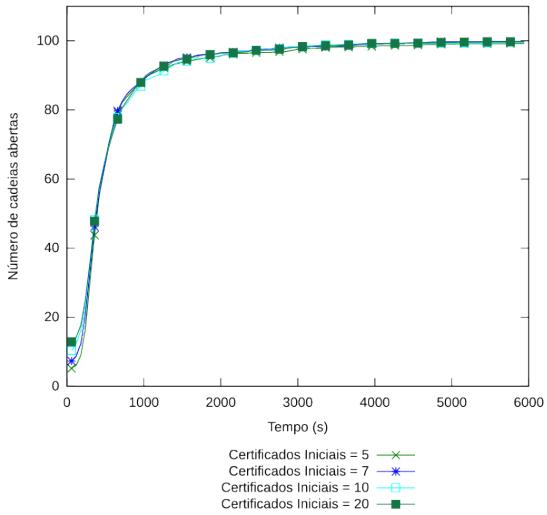
Figura D.6: Resultados para 75 nodos, $m = 10\%$ e $t = 25\%$



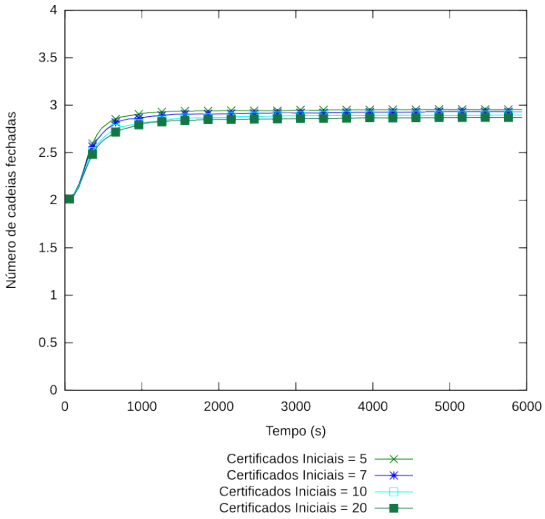

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

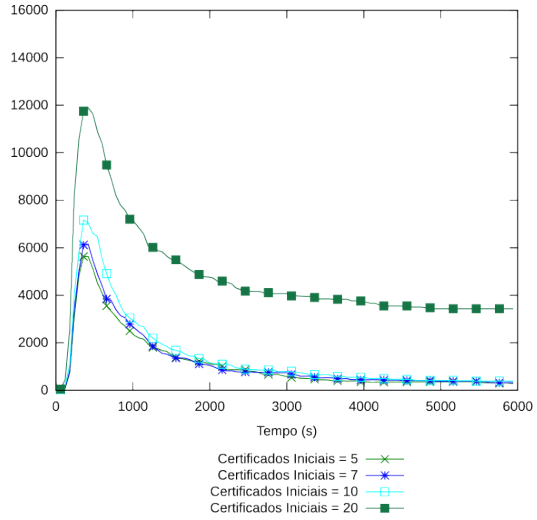



(c) Número de cadeias Abertas

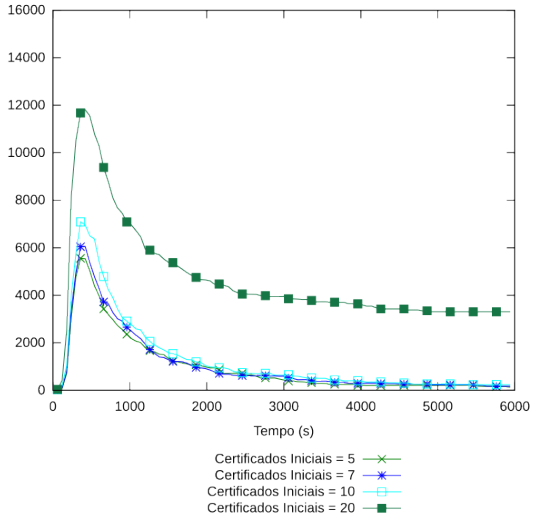



(d) Tamanho médio das cadeias

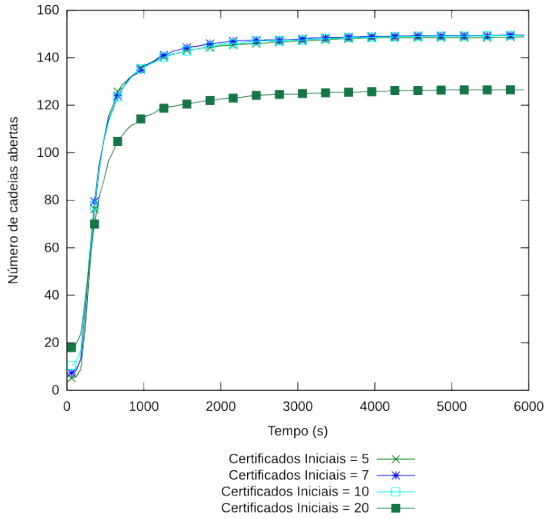
Figura D.7: Resultados para 100 nodos, $m = 10\%$ e $t = 25\%$



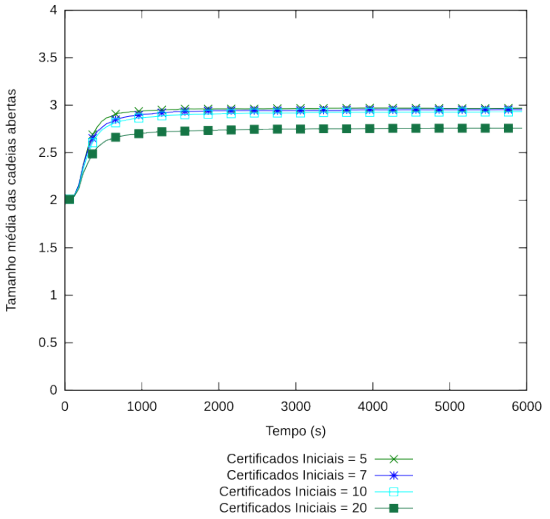

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



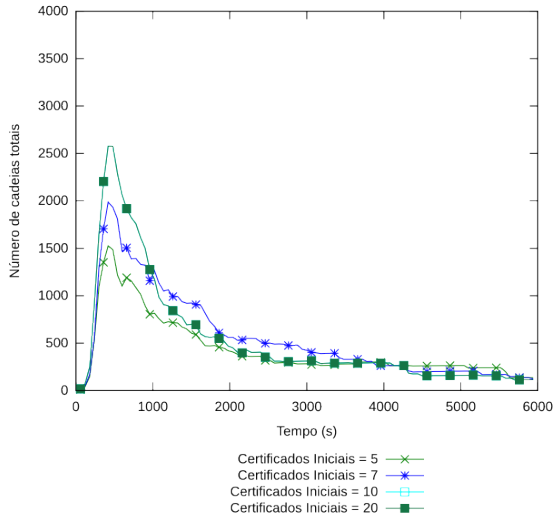

(c) Número de cadeias Abertas



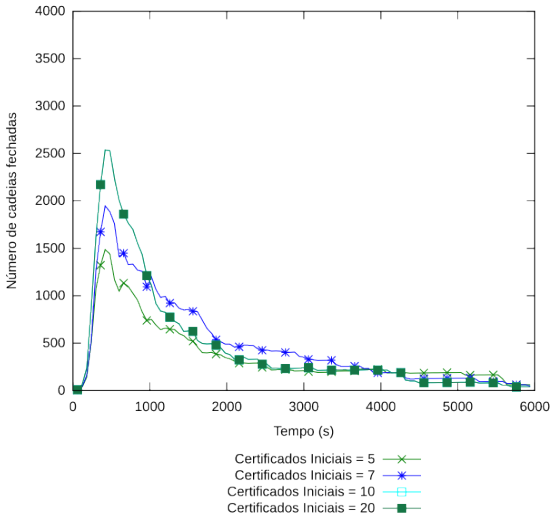

(d) Tamanho médio das cadeias

Figura D.8: Resultados para 150 nodos, $m = 10\%$ e $t = 25\%$

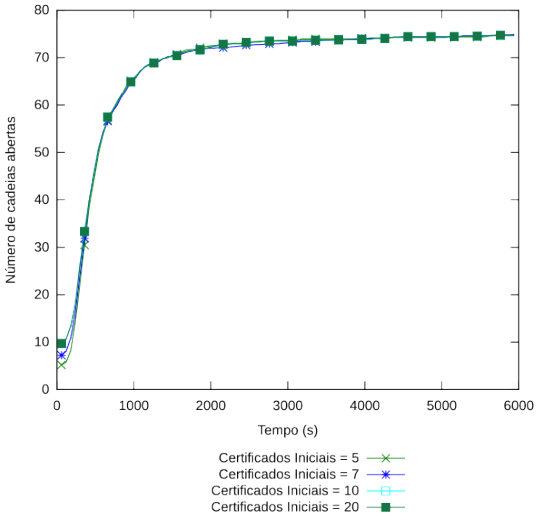
### D.2.3 Ataque *GreyHole* com $m = 10\%$ e $t = 50\%$



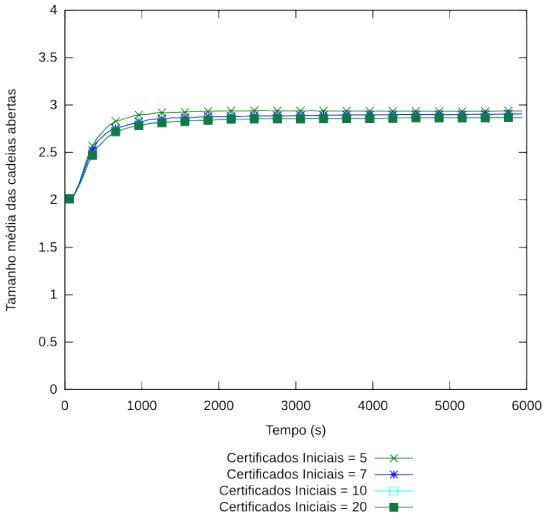

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

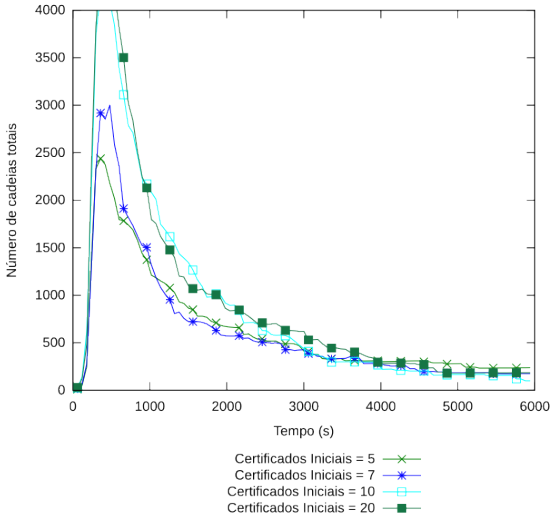



(c) Número de cadeias Abertas

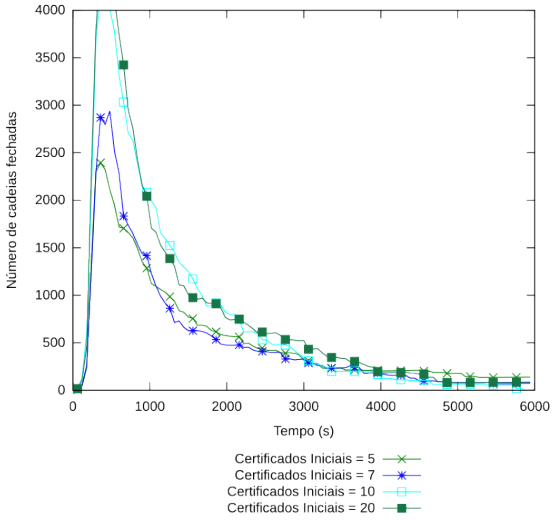



(d) Tamanho médio das cadeias

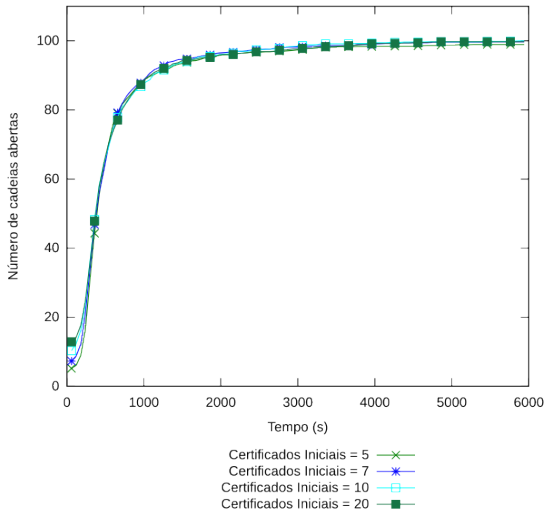
Figura D.9: Resultados para 75 nodos, $m = 10\%$ e $t = 50\%$



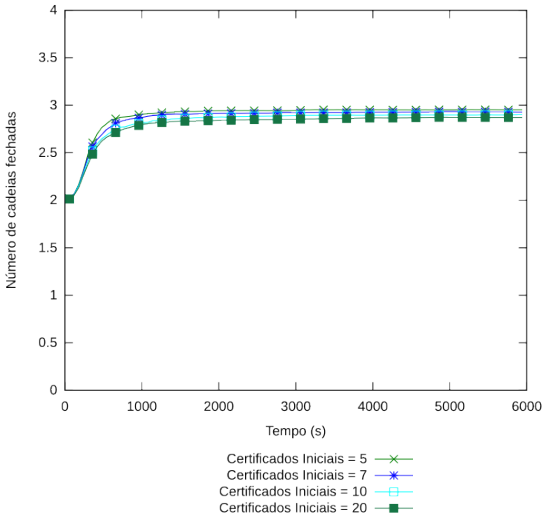

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



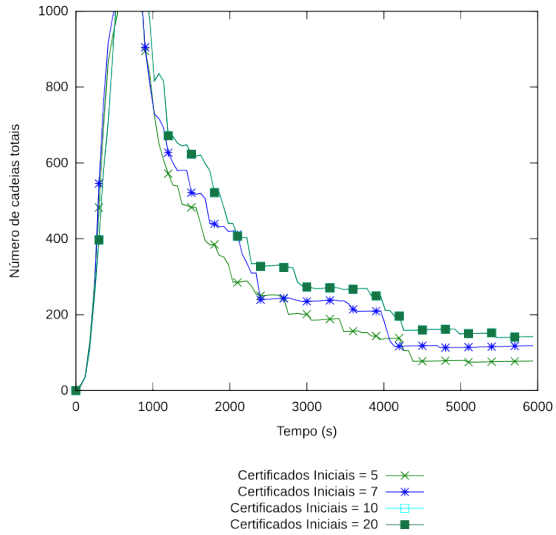

(c) Número de cadeias Abertas



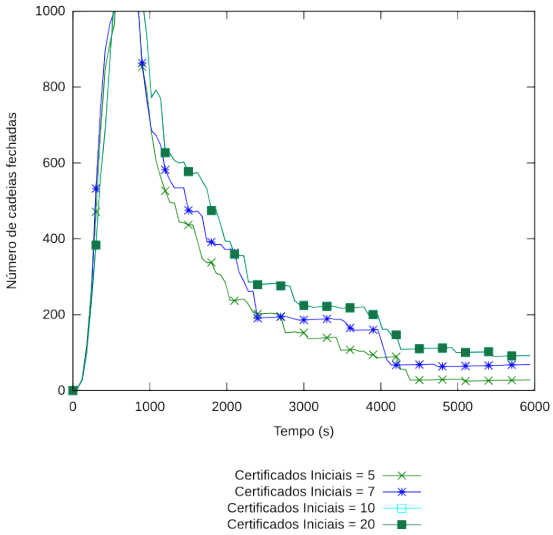

(d) Tamanho médio das cadeias

Figura D.10: Resultados para 100 nodos, $m = 10\%$ e $t = 50\%$

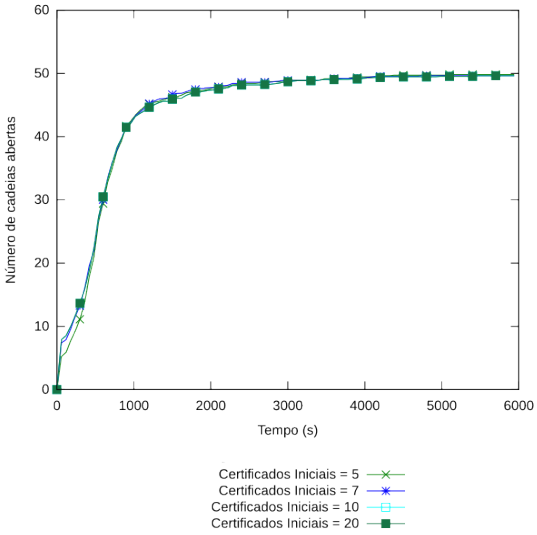
### D.2.4 Ataque *GreyHole* com $m = 20\%$ e $t = 10\%$



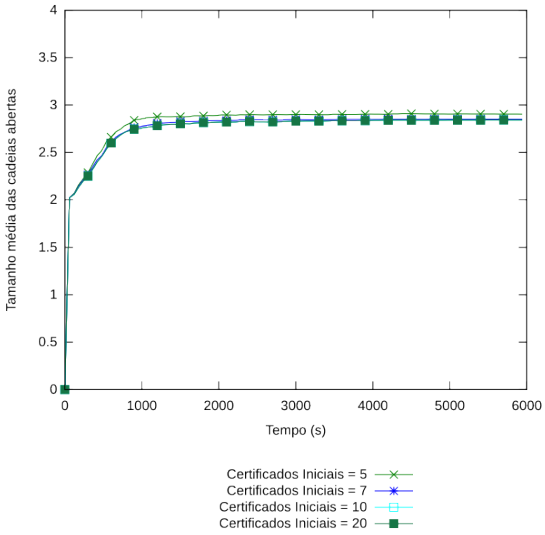

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

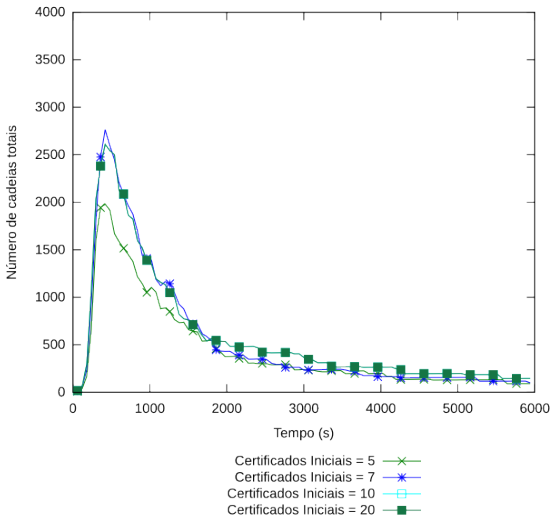



(c) Número de cadeias Abertas

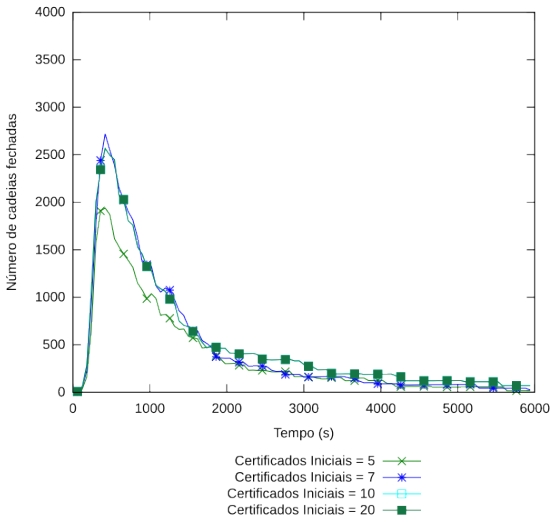



(d) Tamanho médio das cadeias

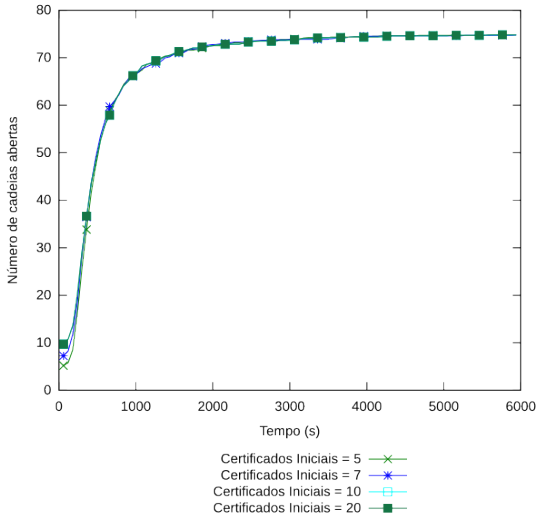
Figura D.11: Resultados para 50 nodos, $m = 20\%$ e $t = 10\%$



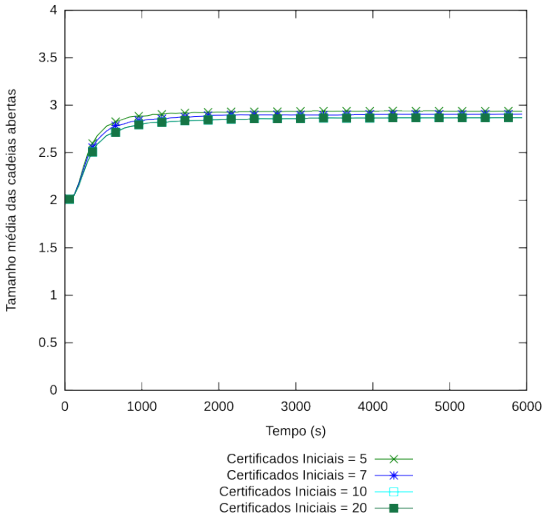

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

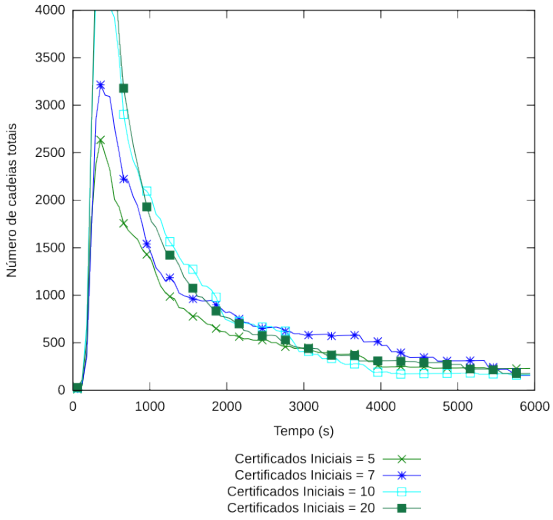



(c) Número de cadeias Abertas

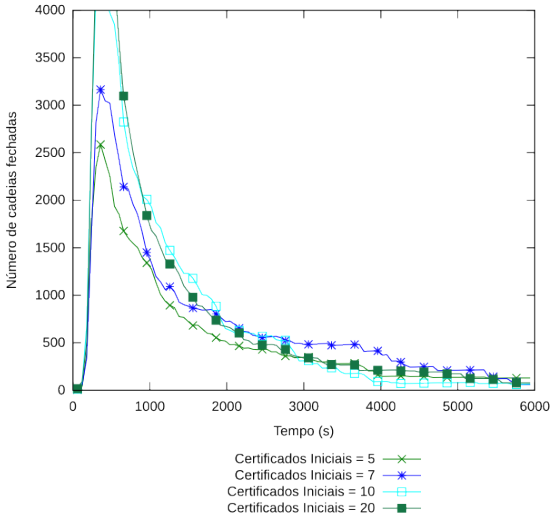



(d) Tamanho médio das cadeias

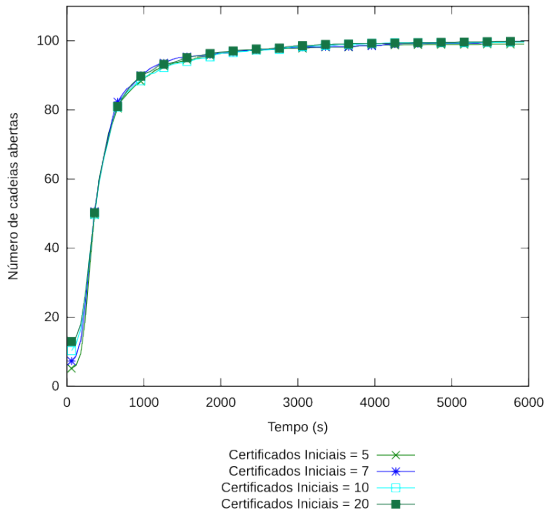
Figura D.12: Resultados para 75 nodos, $m = 20\%$ e $t = 10\%$



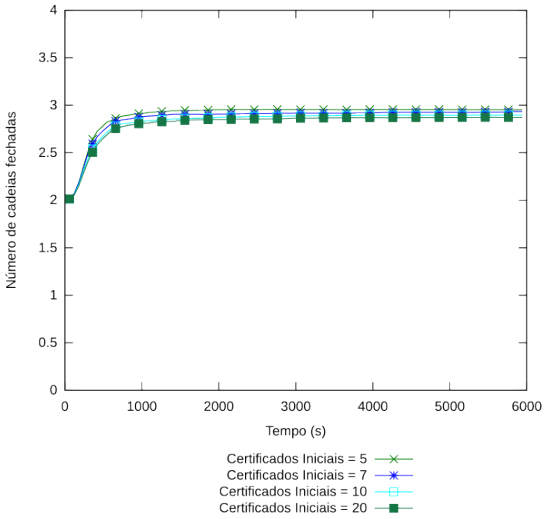

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

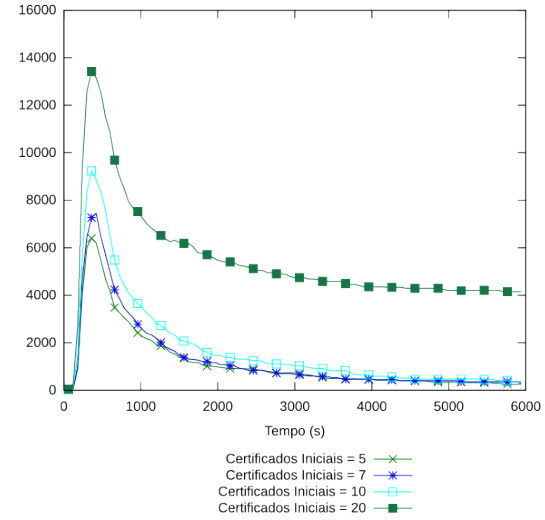



(c) Número de cadeias Abertas

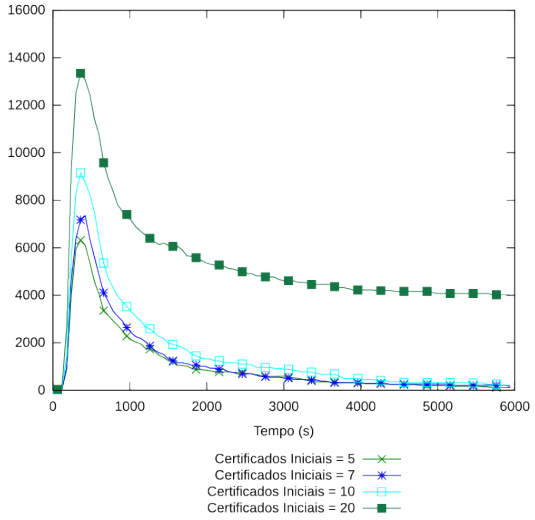



(d) Tamanho médio das cadeias

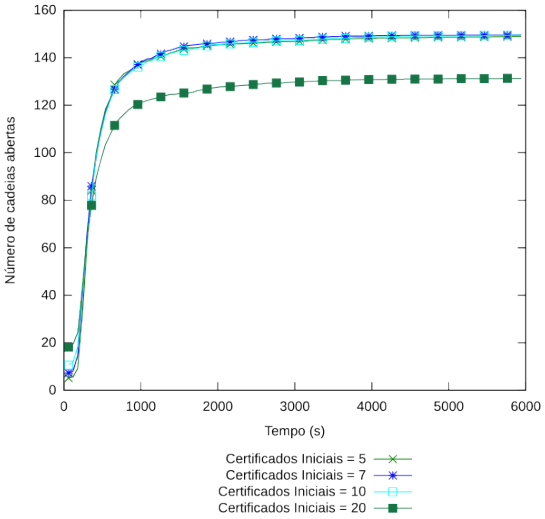
Figura D.13: Resultados para 100 nodos, $m = 20\%$ e $t = 10\%$



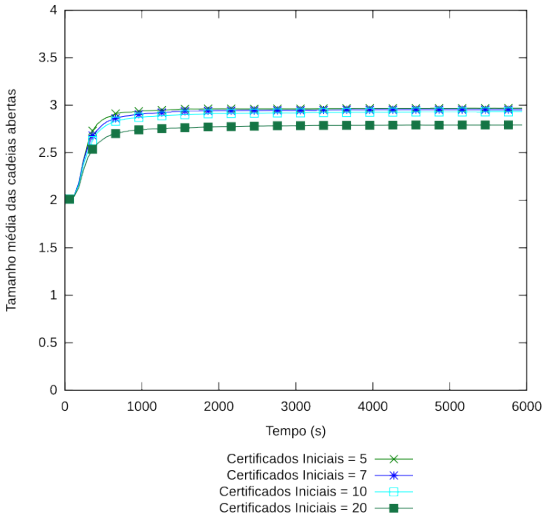

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



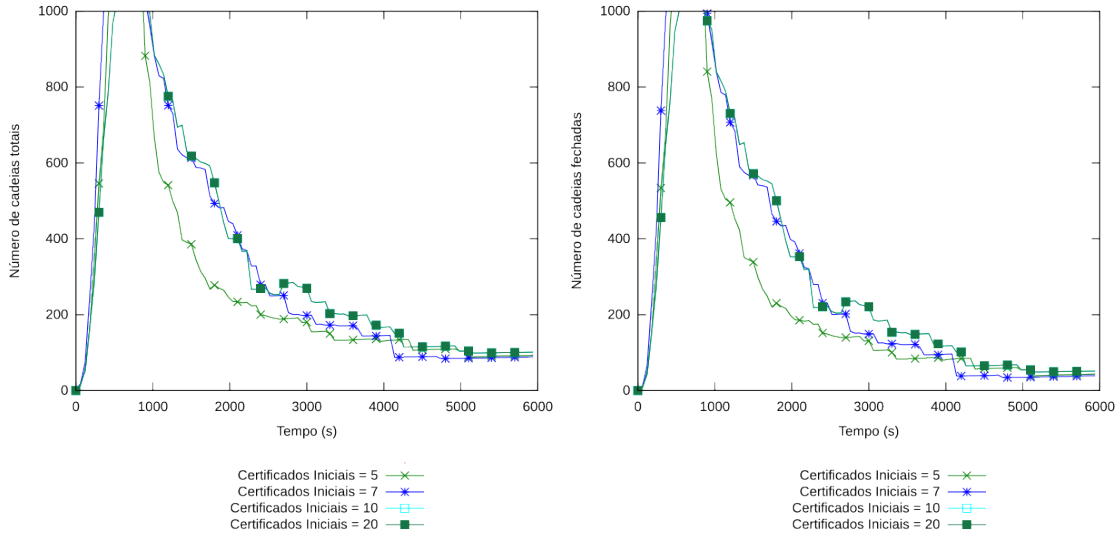

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura D.14: Resultados para 150 nodos, $m = 20\%$ e $t = 10\%$

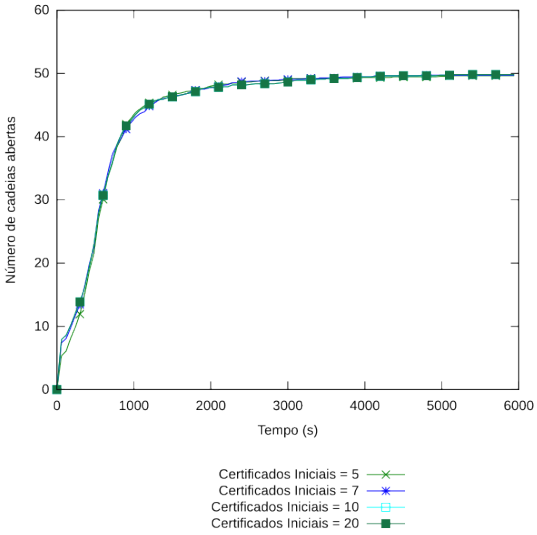
### D.2.5 Ataque *GreyHole* com $m = 20\%$ e $t = 25\%$



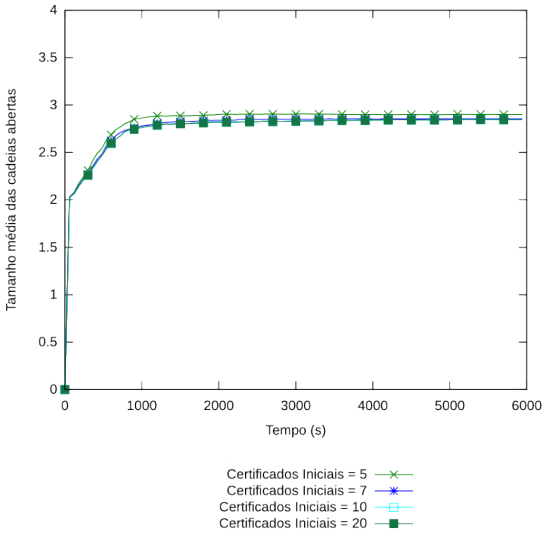

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

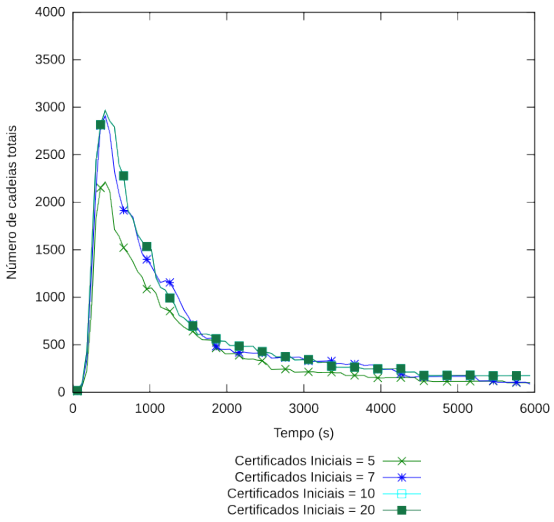



(c) Número de cadeias Abertas

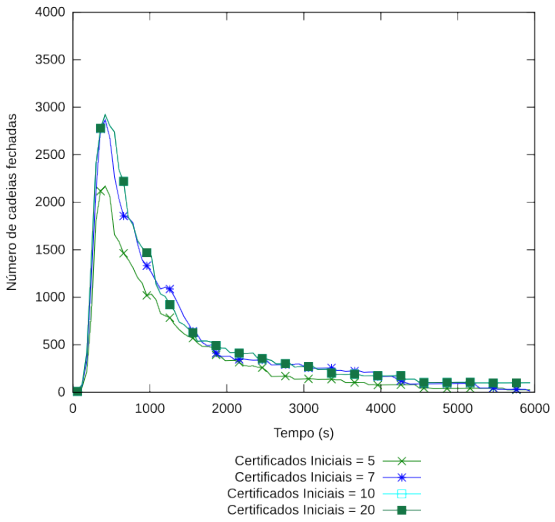



(d) Tamanho médio das cadeias

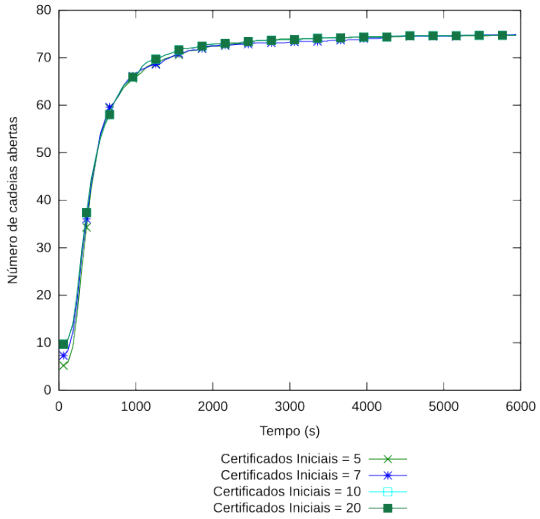
Figura D.15: Resultados para 50 nodos, $m = 20\%$ e $t = 25\%$



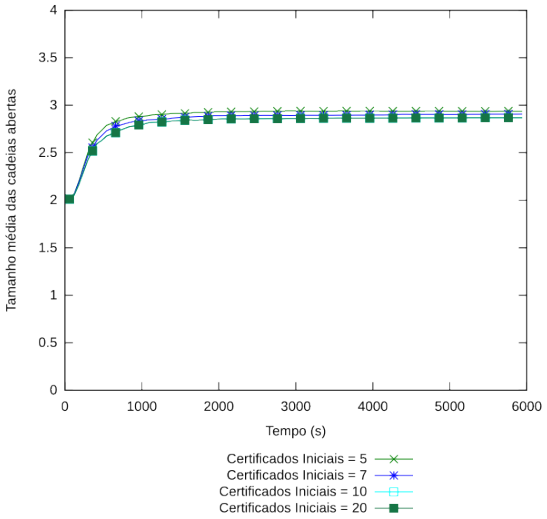

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

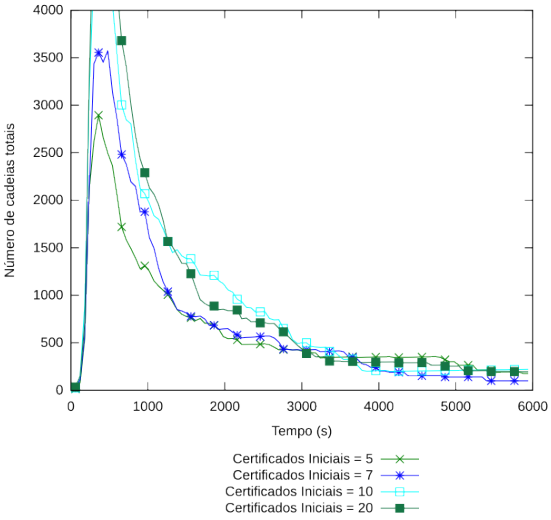



(c) Número de cadeias Abertas

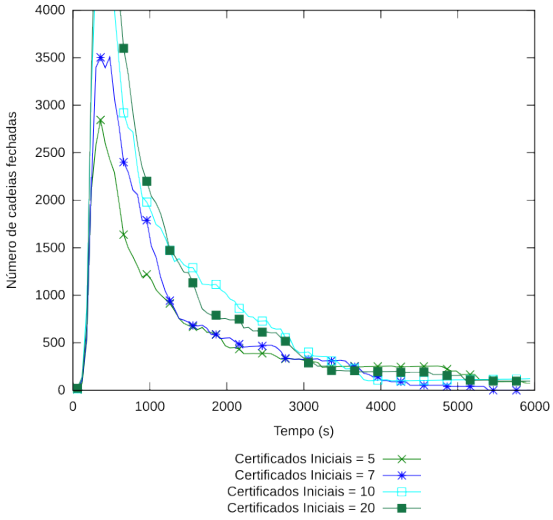



(d) Tamanho médio das cadeias

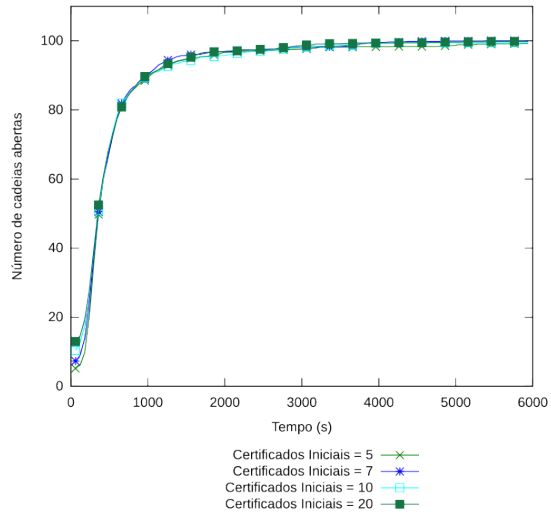
Figura D.16: Resultados para 75 nodos, $m = 20\%$ e $t = 25\%$



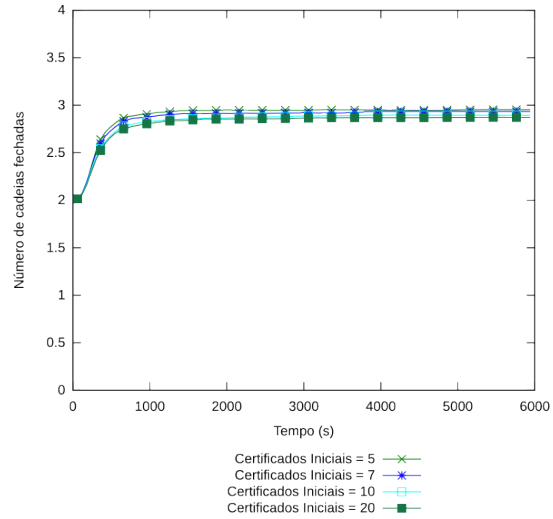

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

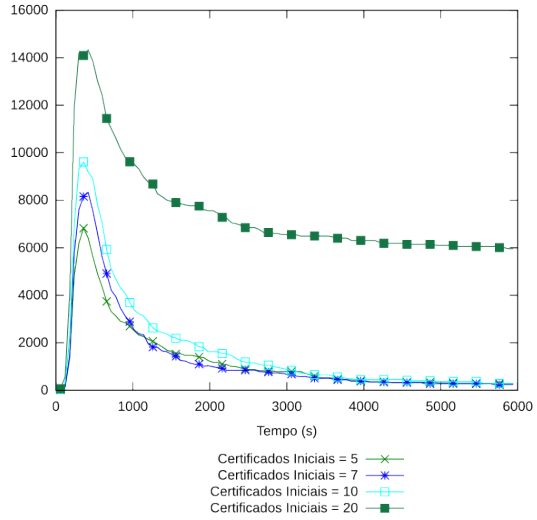



(c) Número de cadeias Abertas

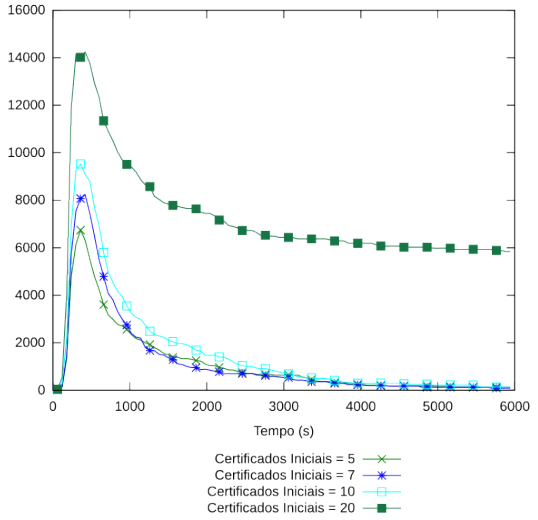



(d) Tamanho médio das cadeias

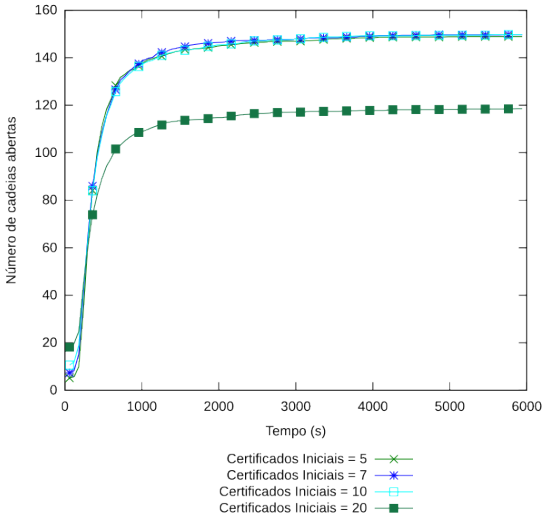
Figura D.17: Resultados para 100 nodos, $m = 20\%$ e $t = 25\%$



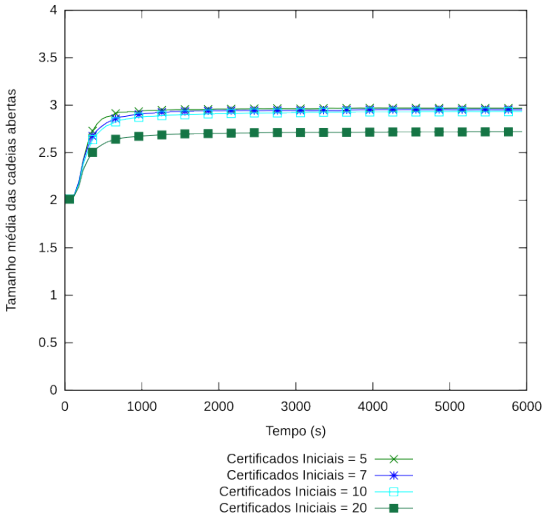

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



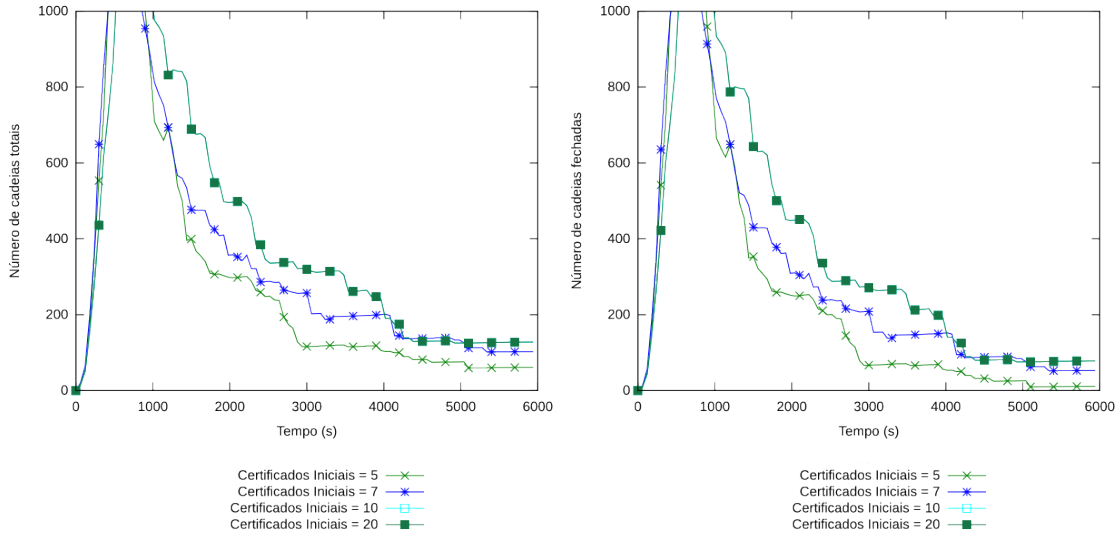

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura D.18: Resultados para 150 nodos, $m = 20\%$ e $t = 25\%$

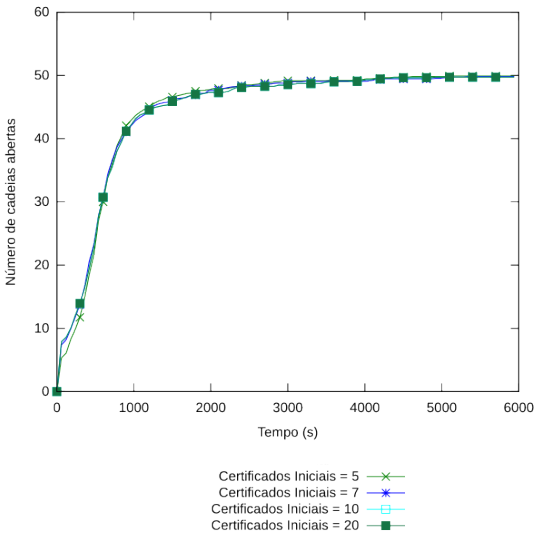
### D.2.6 Ataque *GreyHole* com $m = 20\%$ e $t = 50\%$



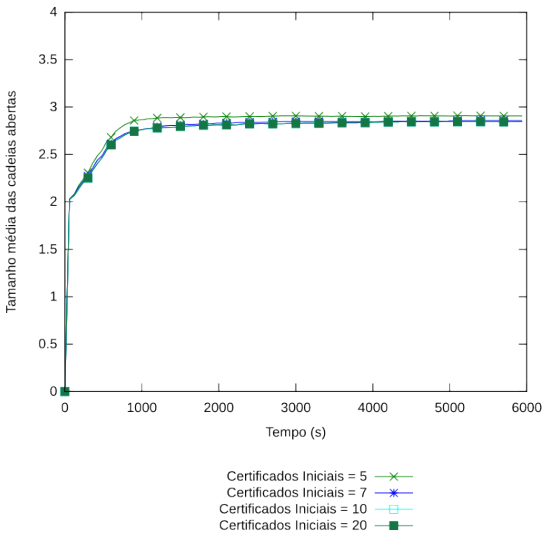

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

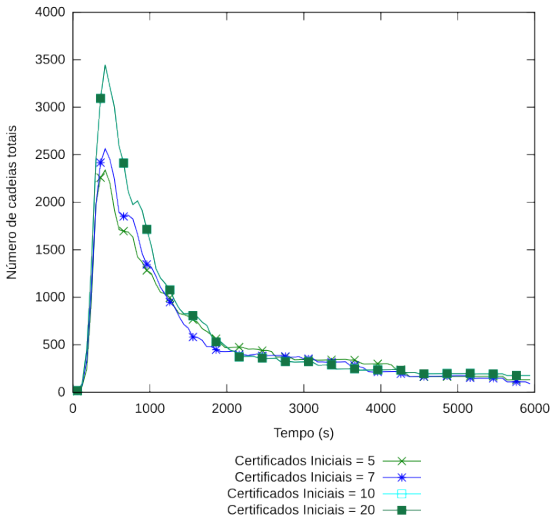



(c) Número de cadeias Abertas

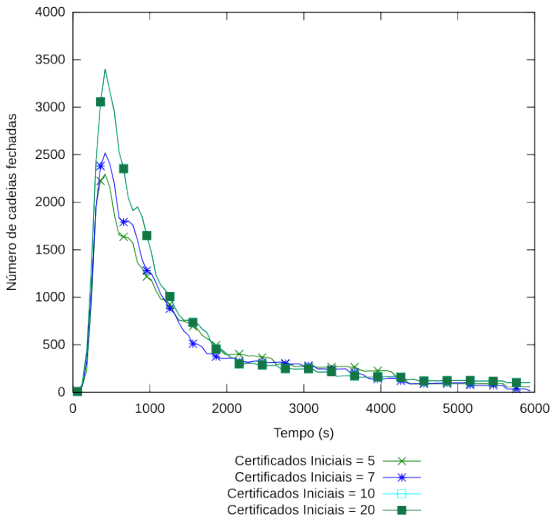



(d) Tamanho médio das cadeias

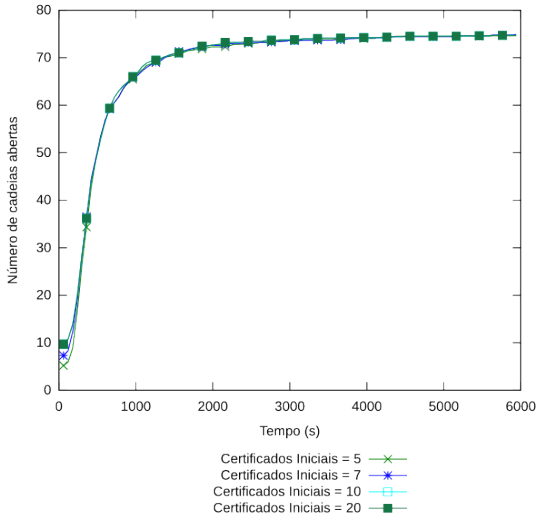
Figura D.19: Resultados para 50 nodos, $m = 20\%$ e $t = 50\%$



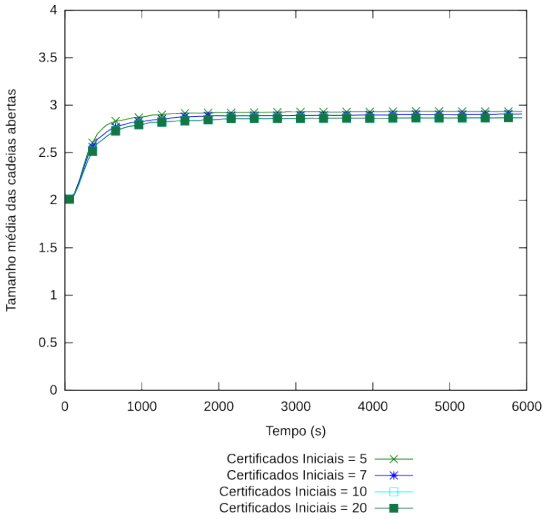

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

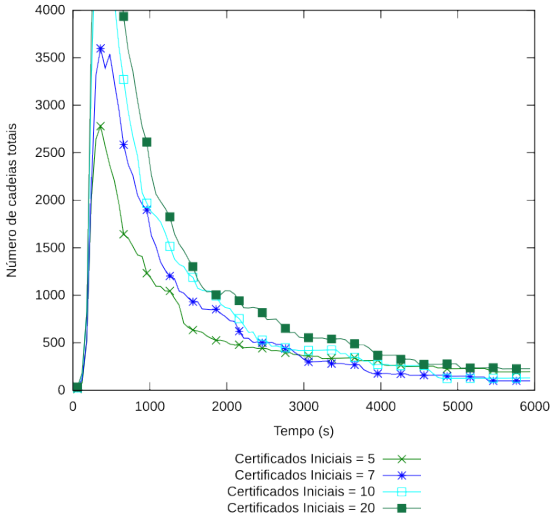



(c) Número de cadeias Abertas

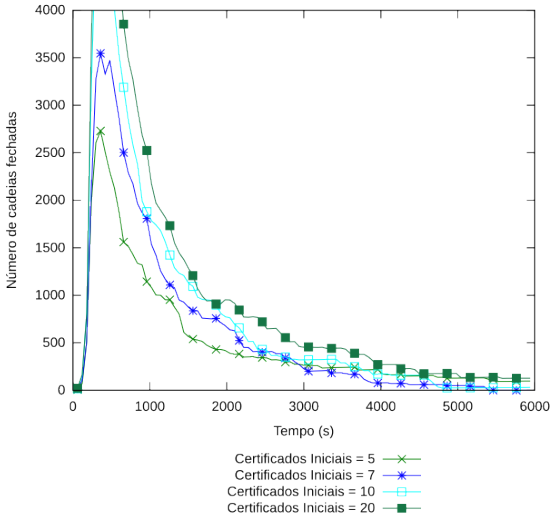



(d) Tamanho médio das cadeias

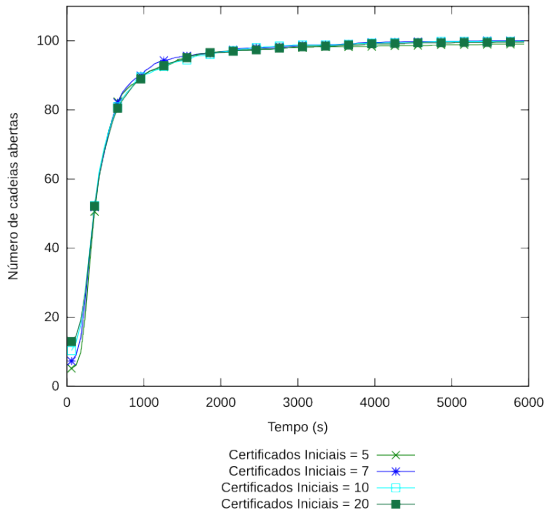
Figura D.20: Resultados para 75 nodos, $m = 20\%$ e $t = 50\%$



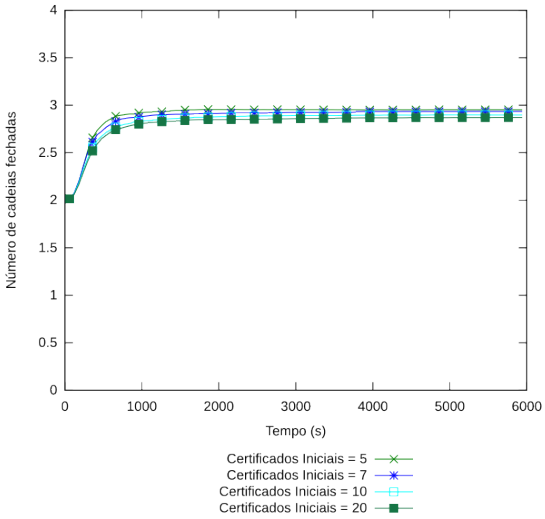

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

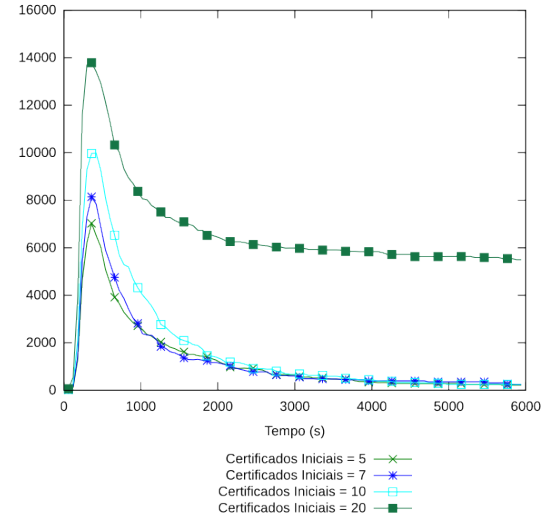



(c) Número de cadeias Abertas

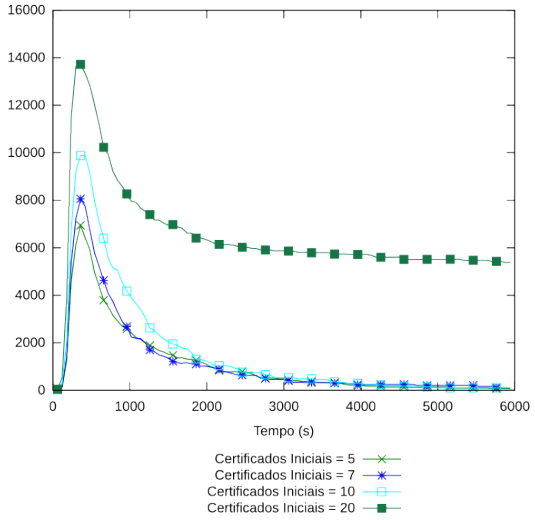



(d) Tamanho médio das cadeias

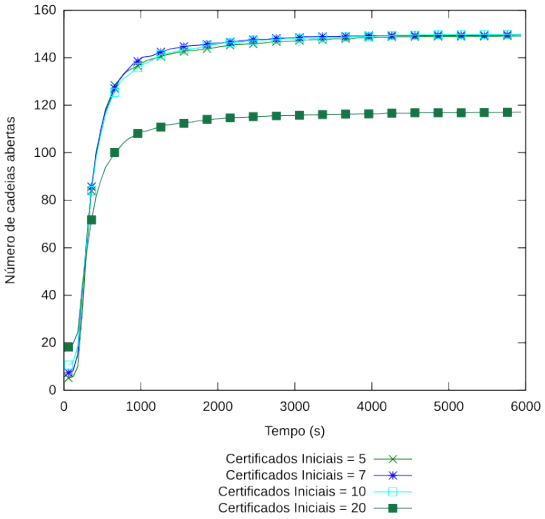
Figura D.21: Resultados para 100 nodos, $m = 20\%$ e $t = 50\%$



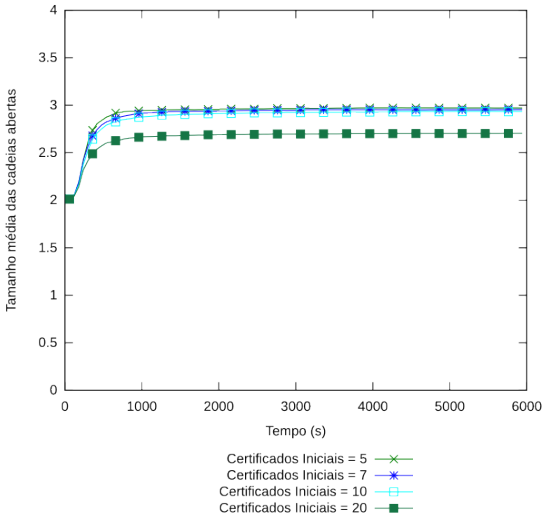

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



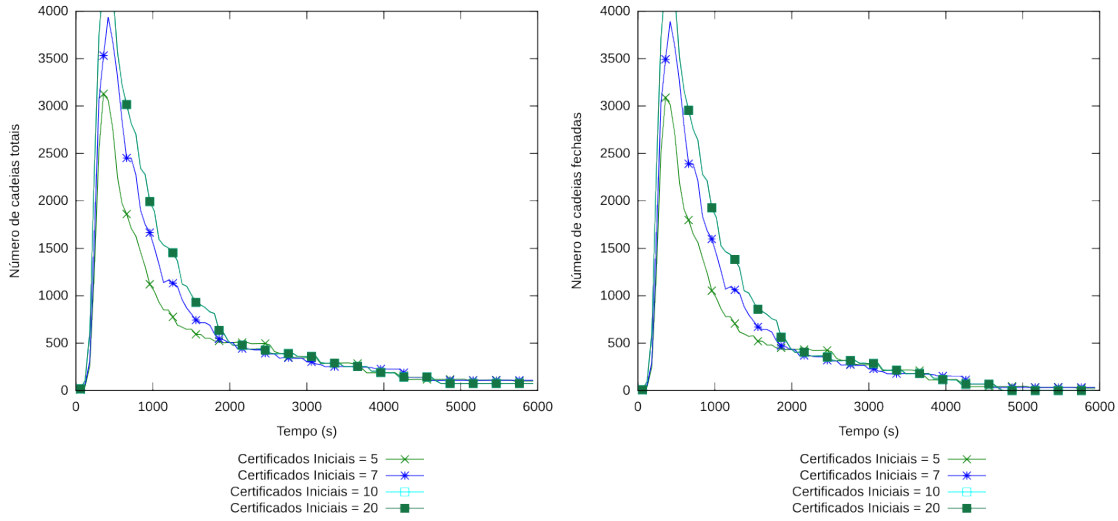

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura D.22: Resultados para 150 nodos, $m = 20\%$ e $t = 50\%$

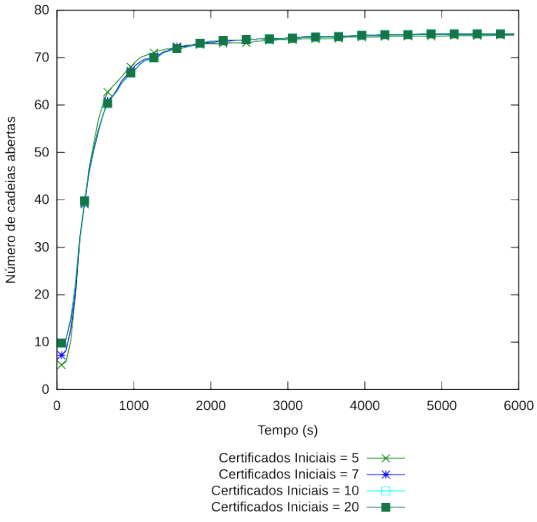
### D.2.7 Ataque *GreyHole* com $m = 50\%$ e $t = 10\%$



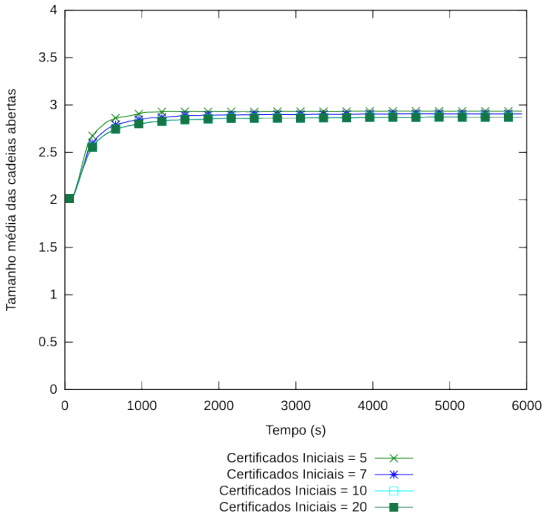

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

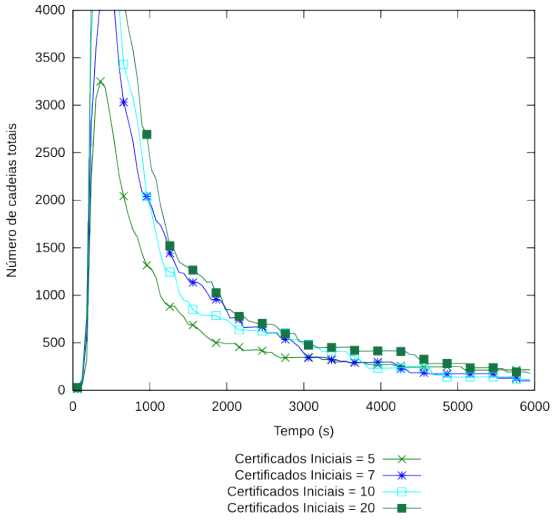



(c) Número de cadeias Abertas

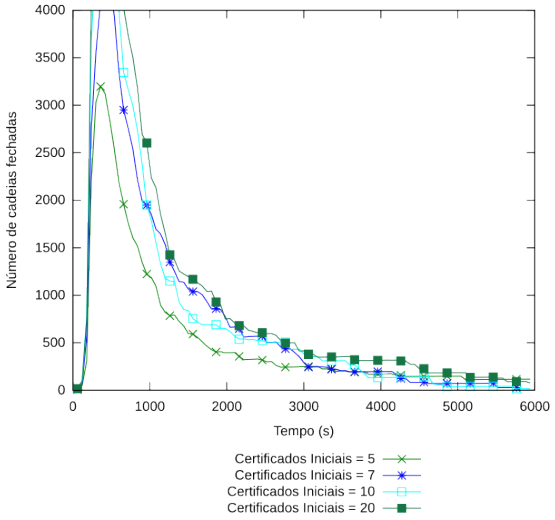



(d) Tamanho médio das cadeias

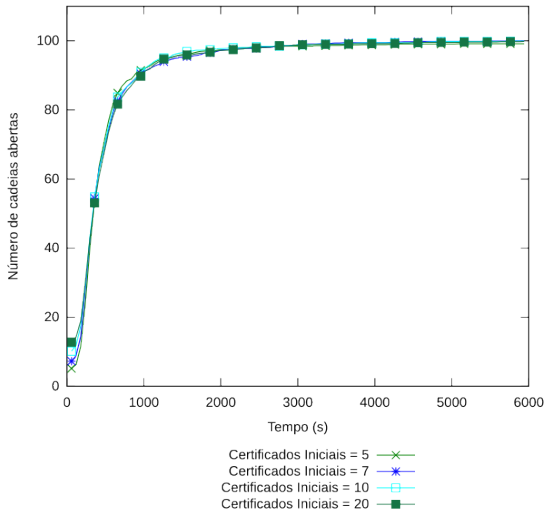
Figura D.23: Resultados para 75 nodos, $m = 50\%$ e $t = 10\%$



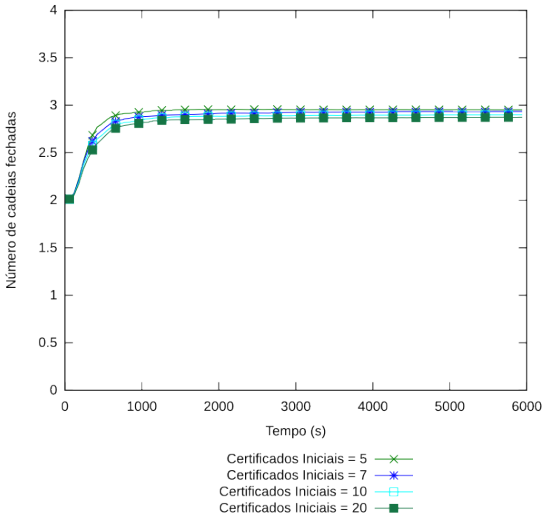

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



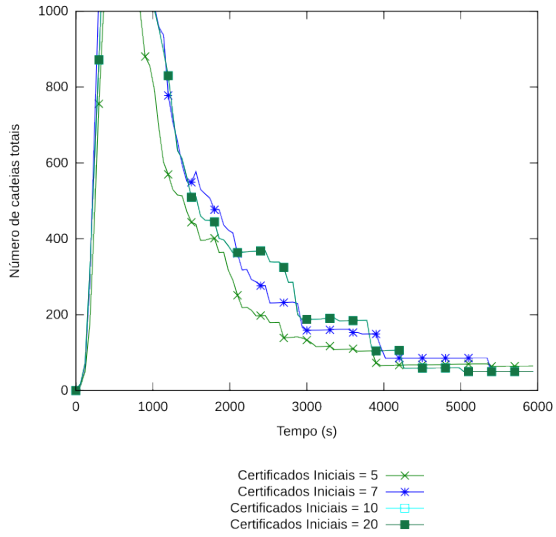

(c) Número de cadeias Abertas



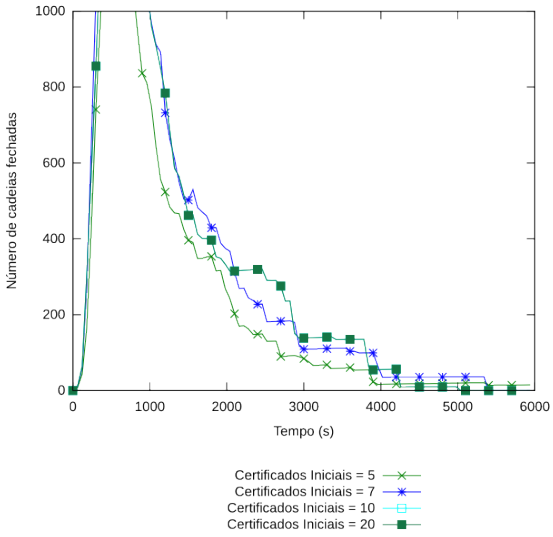

(d) Tamanho médio das cadeias

Figura D.24: Resultados para 100 nodos, $m = 50\%$ e $t = 10\%$

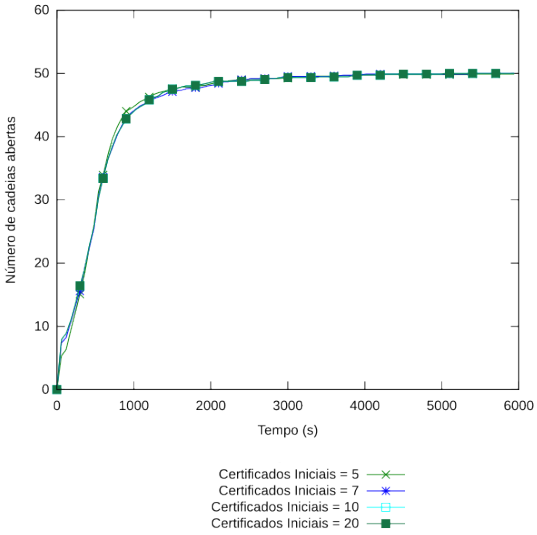
### D.2.8 Ataque *GreyHole* com $m = 50\%$ e $t = 25\%$



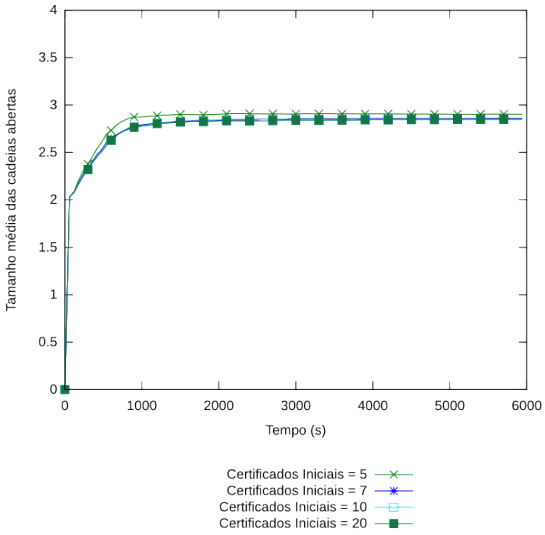

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

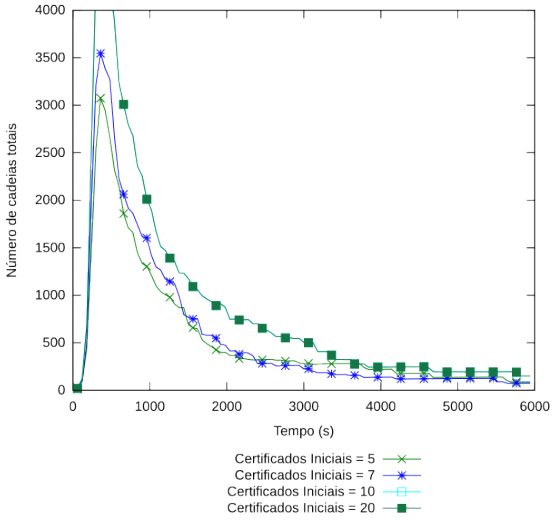



(c) Número de cadeias Abertas

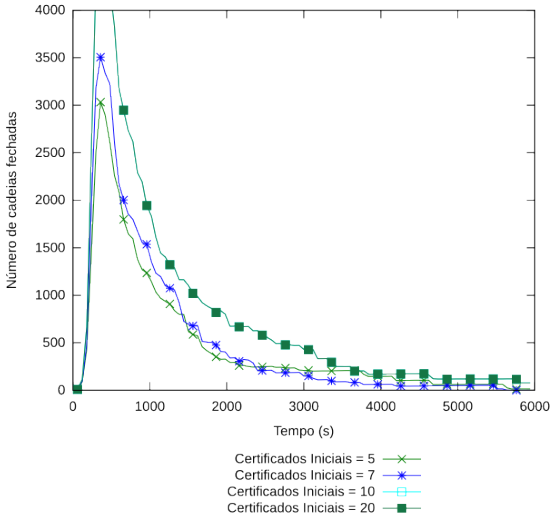



(d) Tamanho médio das cadeias

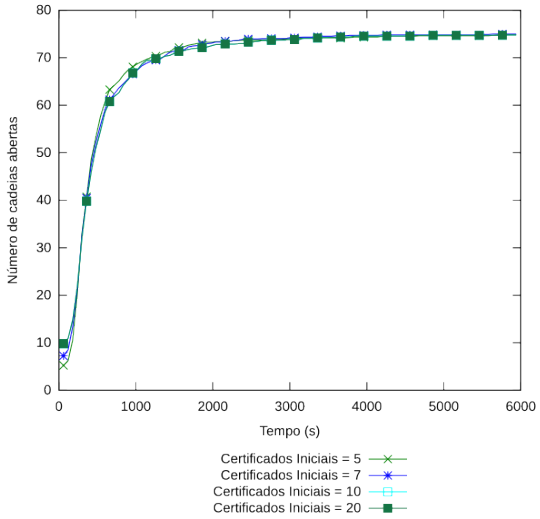
Figura D.25: Resultados para 50 nodos, $m = 50\%$ e $t = 25\%$



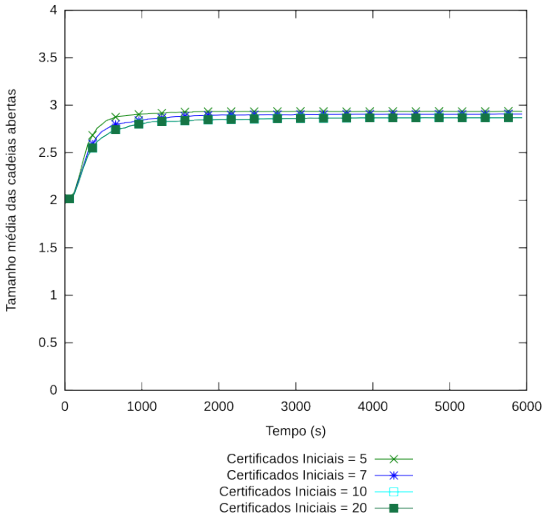

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

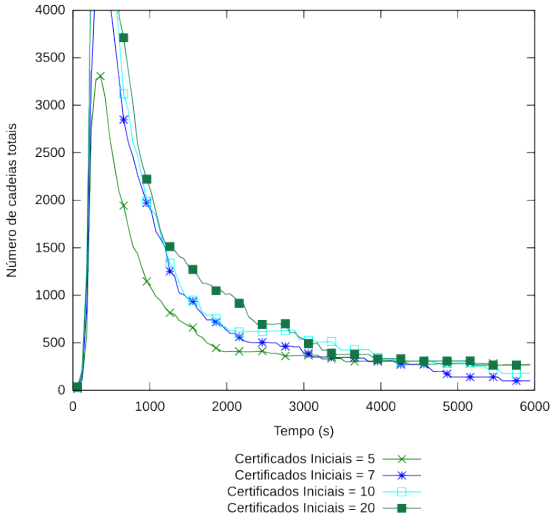



(c) Número de cadeias Abertas

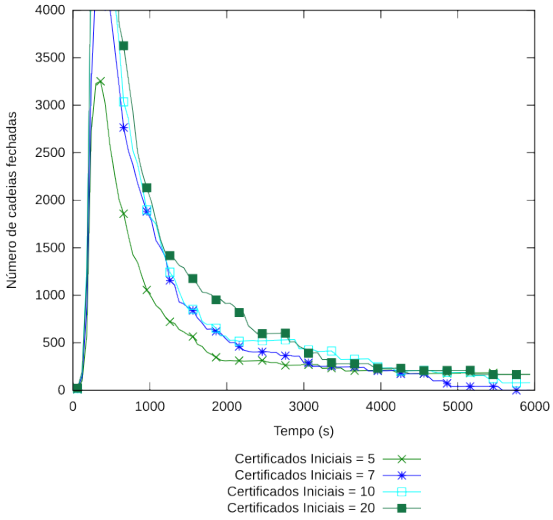



(d) Tamanho médio das cadeias

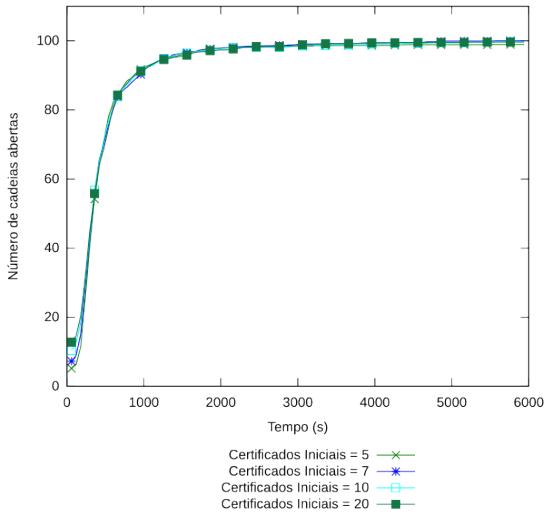
Figura D.26: Resultados para 75 nodos, $m = 50\%$ e $t = 25\%$



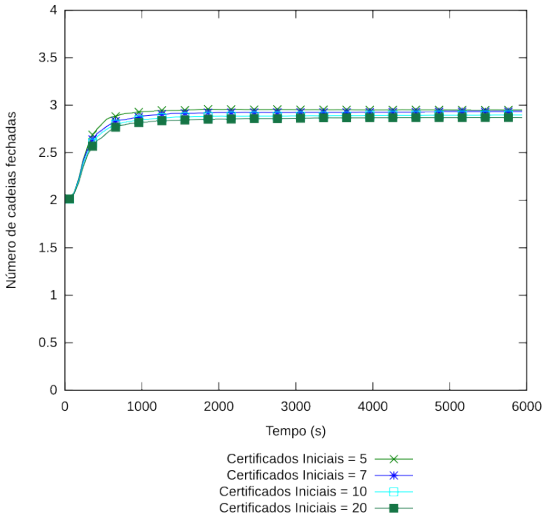

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

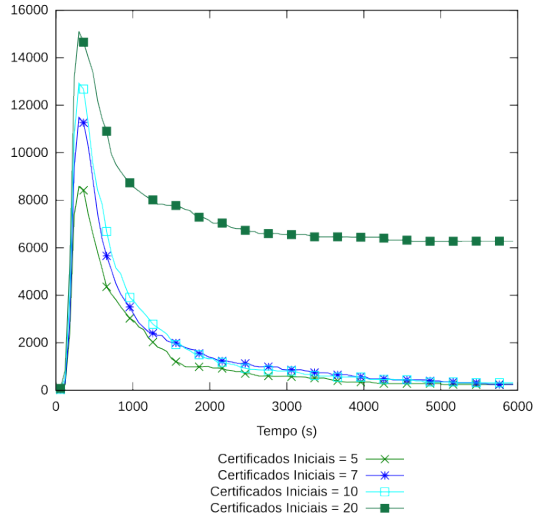



(c) Número de cadeias Abertas

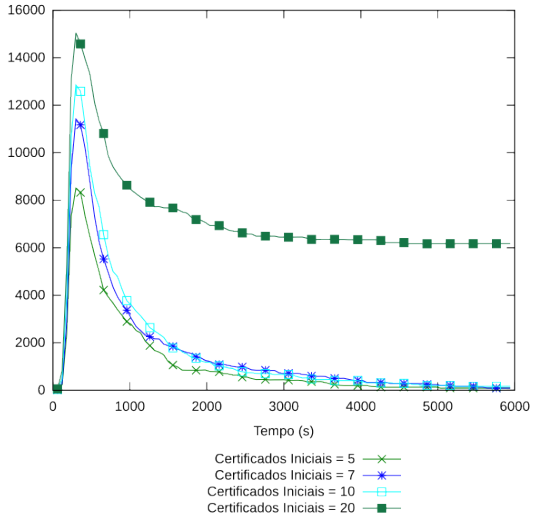



(d) Tamanho médio das cadeias

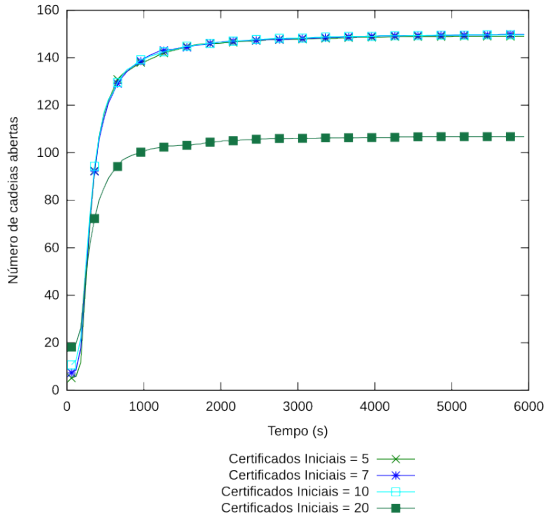
Figura D.27: Resultados para 100 nodos, $m = 50\%$ e $t = 25\%$



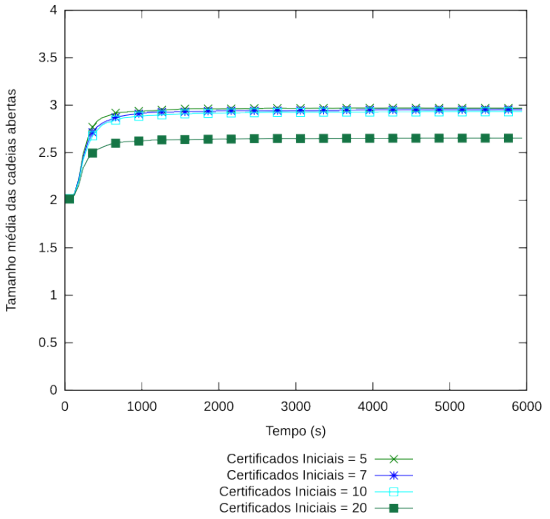

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



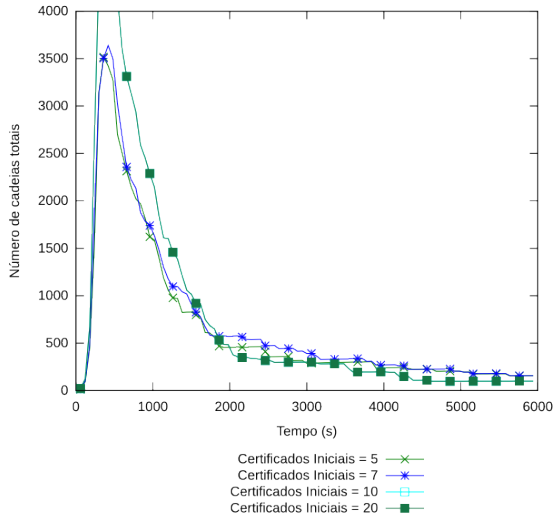

(c) Número de cadeias Abertas



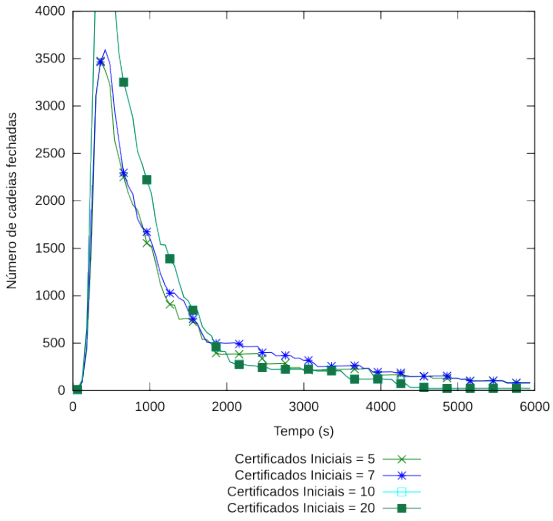

(d) Tamanho médio das cadeias

Figura D.28: Resultados para 150 nodos, $m = 50\%$ e $t = 25\%$

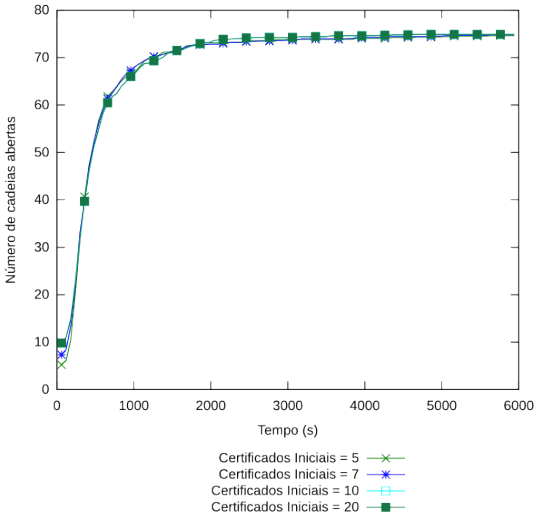
### D.2.9 Ataque *GreyHole* com $m = 50\%$ e $t = 50\%$



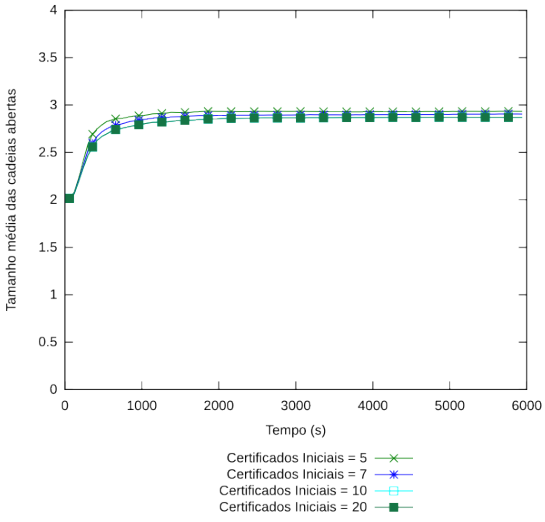

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

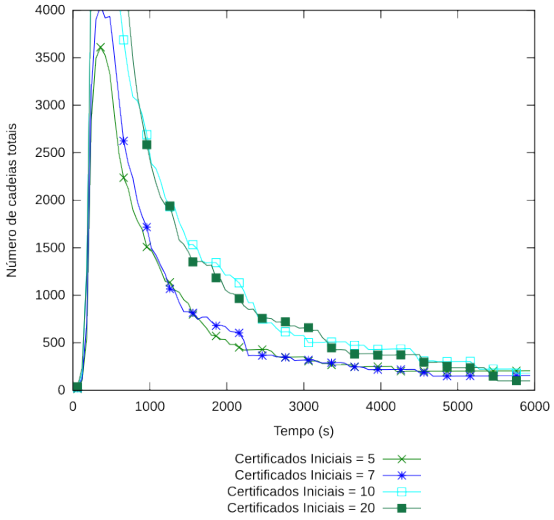



(c) Número de cadeias Abertas

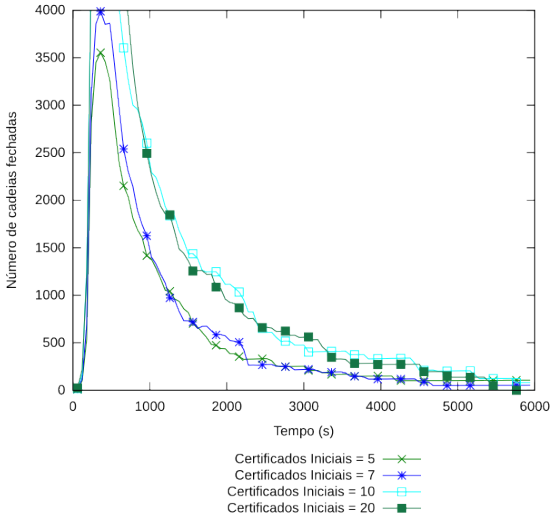



(d) Tamanho médio das cadeias

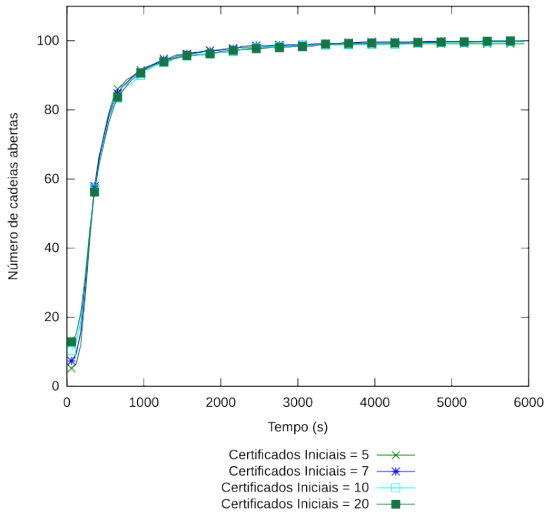
Figura D.29: Resultados para 75 nodos, $m = 50\%$ e $t = 50\%$



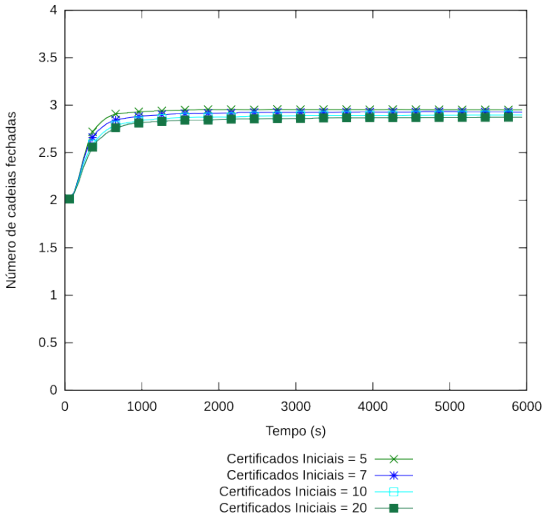

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

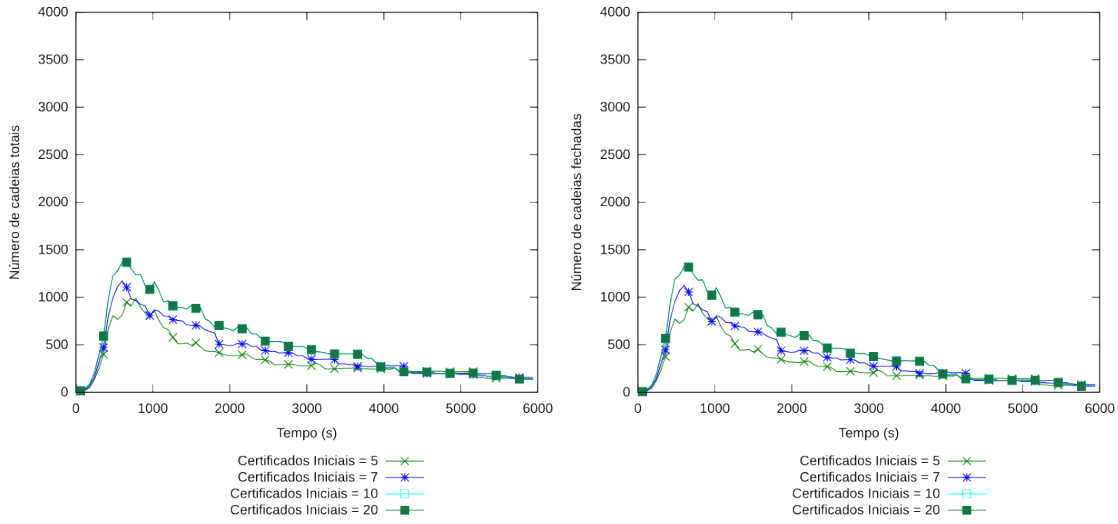



(d) Tamanho médio das cadeias

Figura D.30: Resultados para 100 nodos, $m = 50\%$ e $t = 50\%$

## D.3 Ataque *BlackHole*

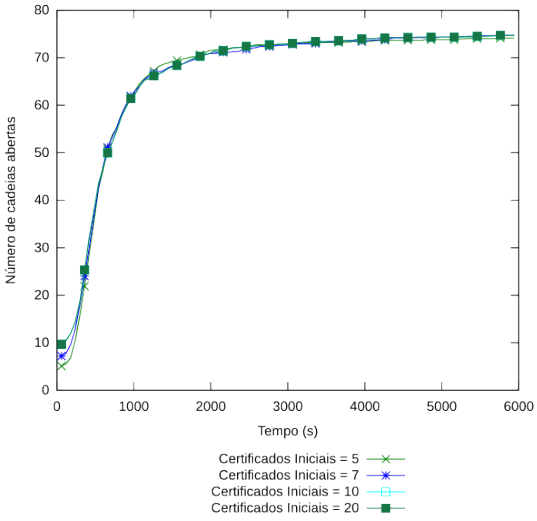
### D.3.1 Ataque *BlackHole* com $m = 10\%$



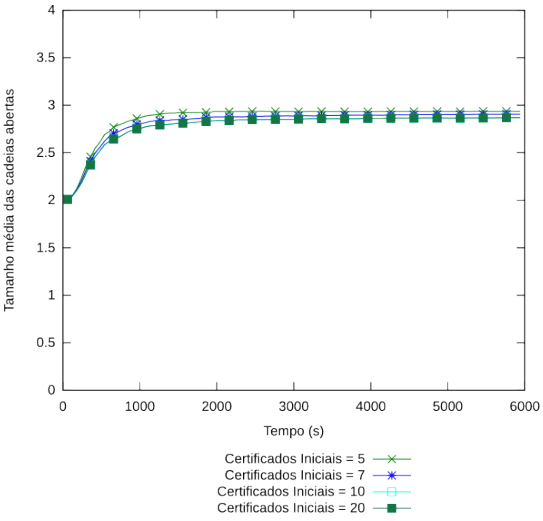

(a) Número de cadeias totais




(b) Número de cadeias fechadas

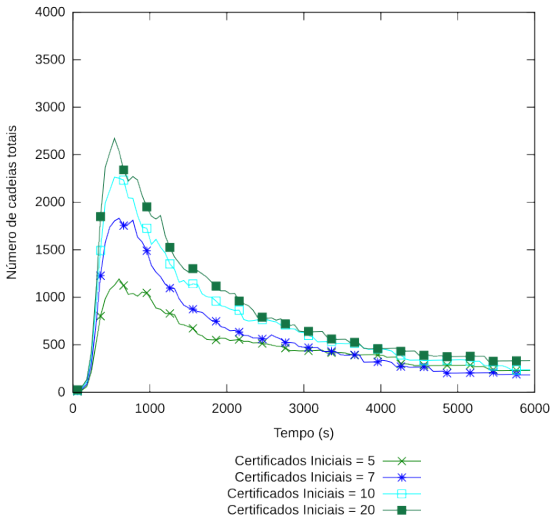



(c) Número de cadeias abertas

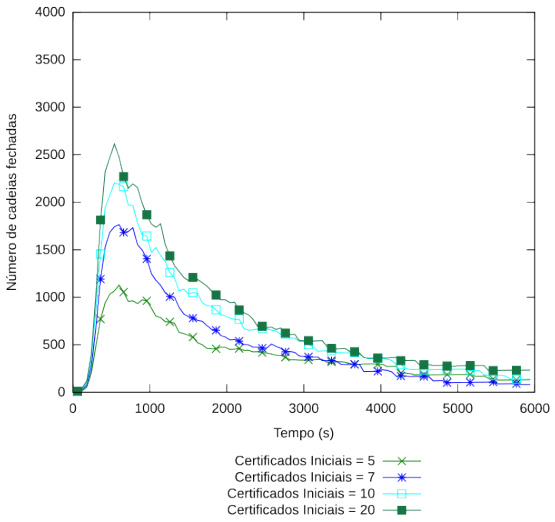



(d) Tamanho médio das cadeias

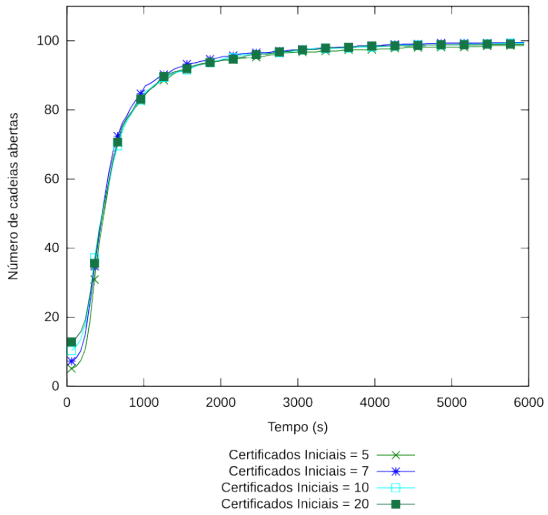
Figura D.31: Resultados para 75 nodos e $m = 10\%$



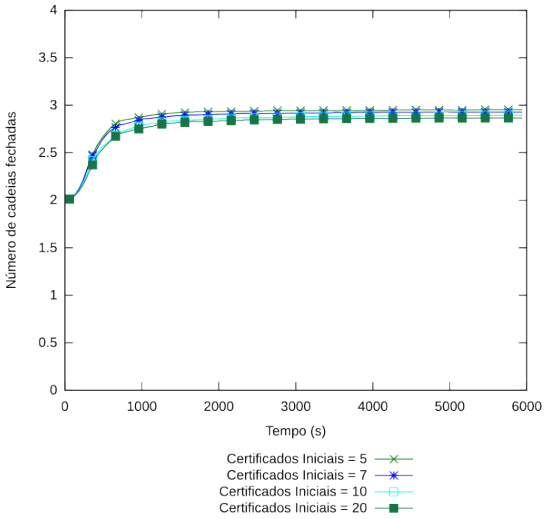

(a) Número de cadeias totais




(b) Número de cadeias fechadas



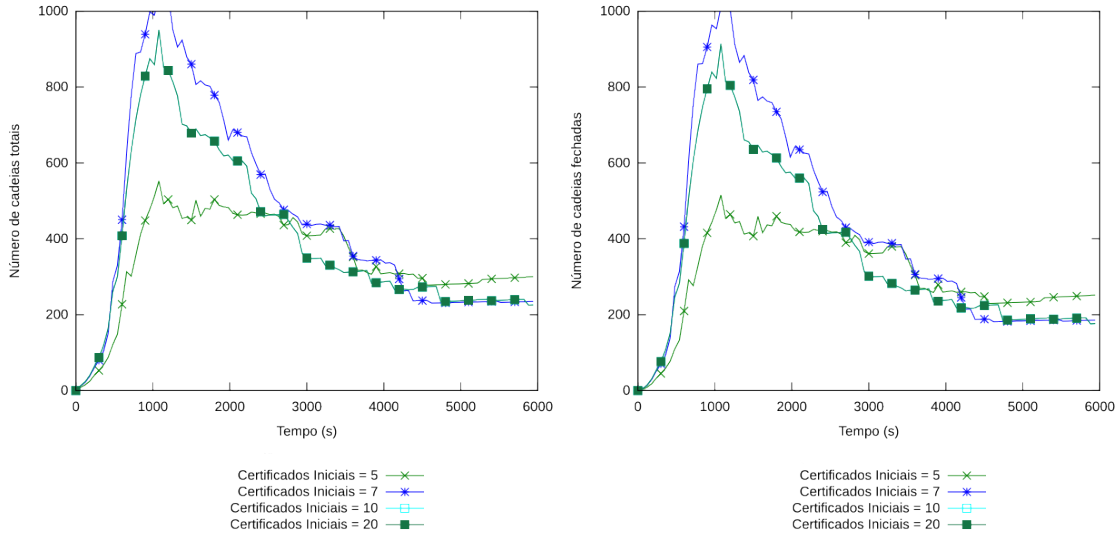

(c) Número de cadeias abertas




(d) Tamanho médio das cadeias

Figura D.32: Resultados para 100 nodos e $m = 10\%$

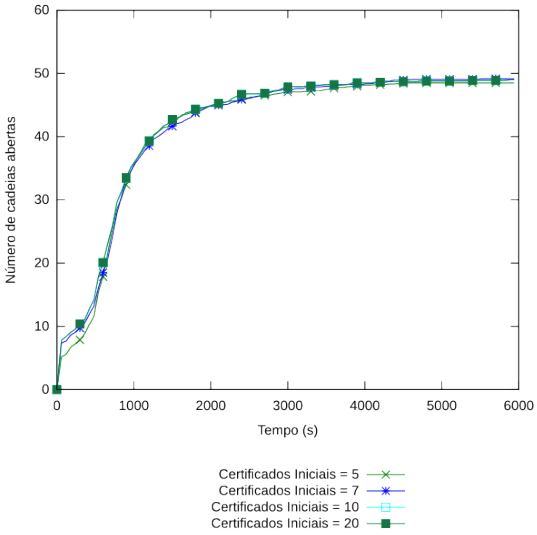
### D.3.2 Ataque *BlackHole* com $m = 20\%$



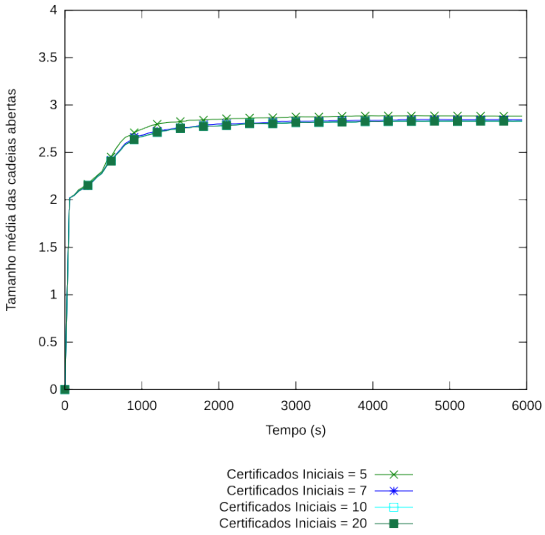

(a) Número de cadeias totais




(b) Número de cadeias fechadas

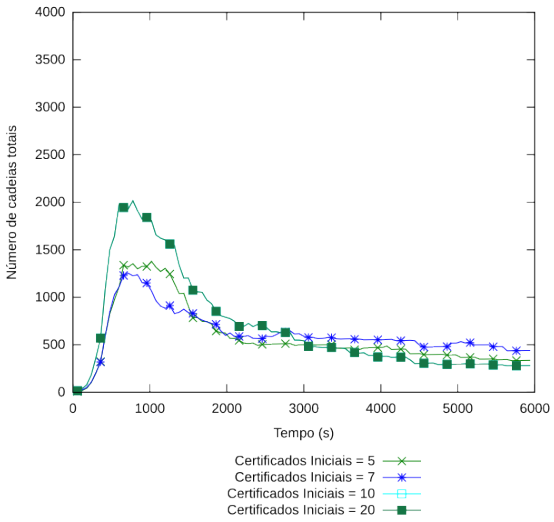



(c) Número de cadeias abertas

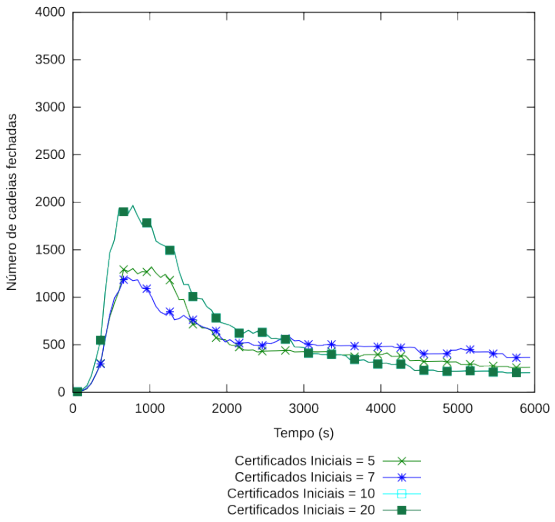



(d) Tamanho médio das cadeias

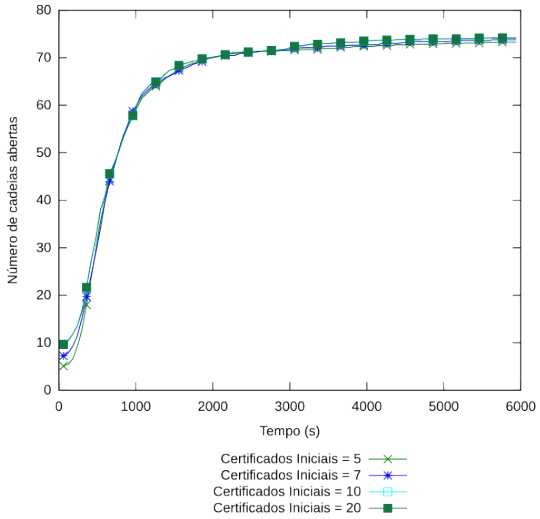
Figura D.33: Resultados para 50 nodos e $m = 20\%$



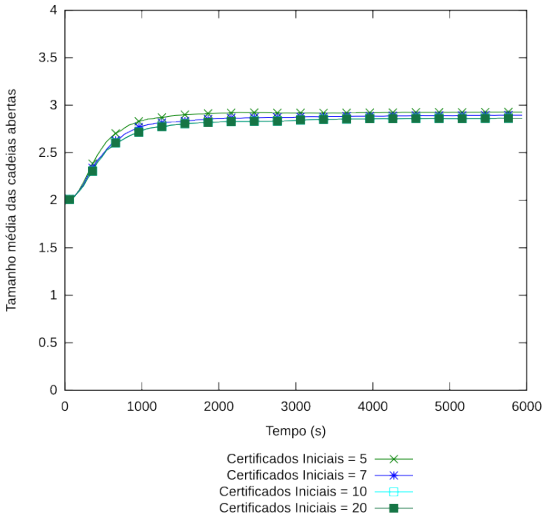

(a) Número de cadeias totais




(b) Número de cadeias fechadas

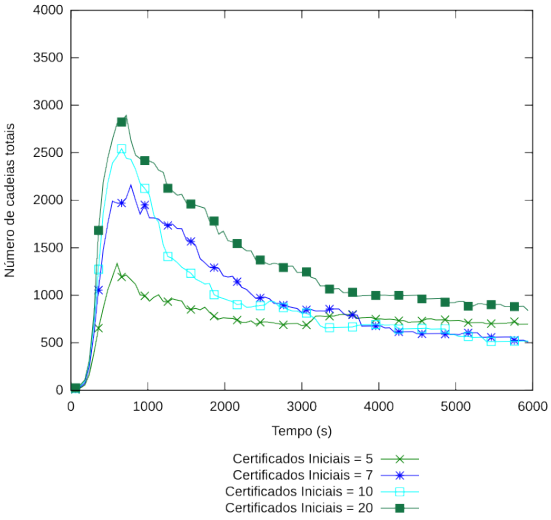



(c) Número de cadeias abertas

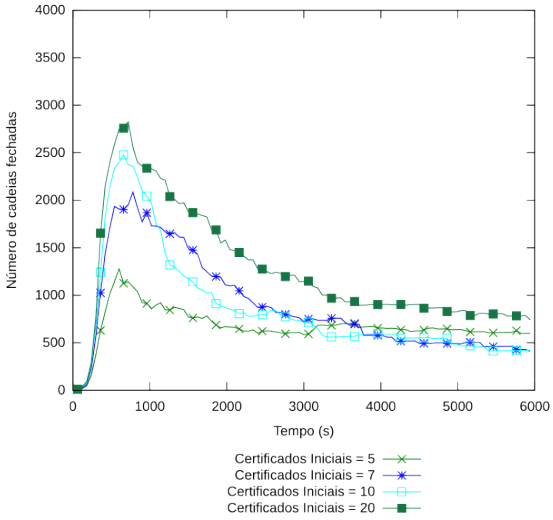



(d) Tamanho médio das cadeias

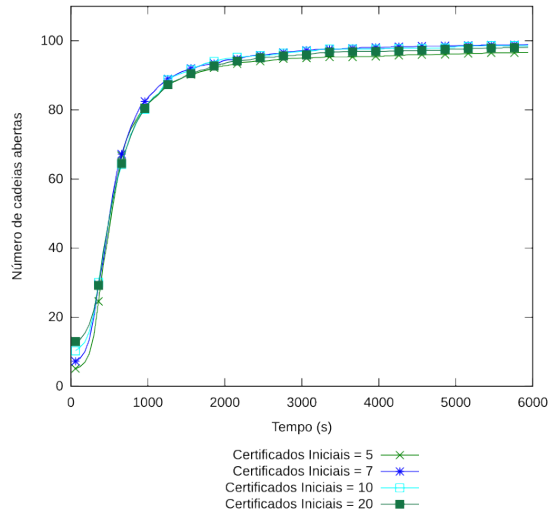
Figura D.34: Resultados para 75 nodos e $m = 20\%$



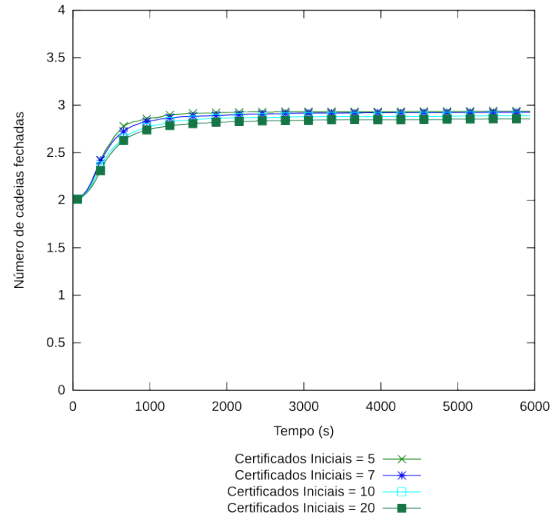

(a) Número de cadeias totais




(b) Número de cadeias fechadas

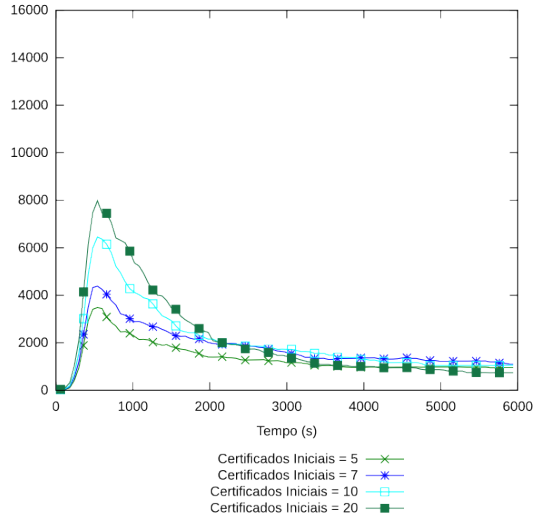



(c) Número de cadeias abertas

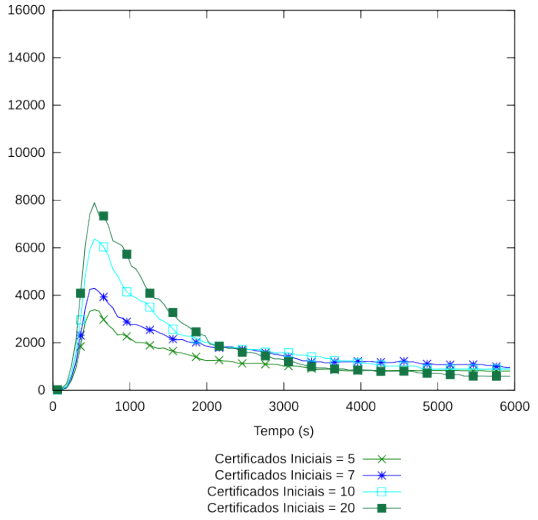



(d) Tamanho médio das cadeias

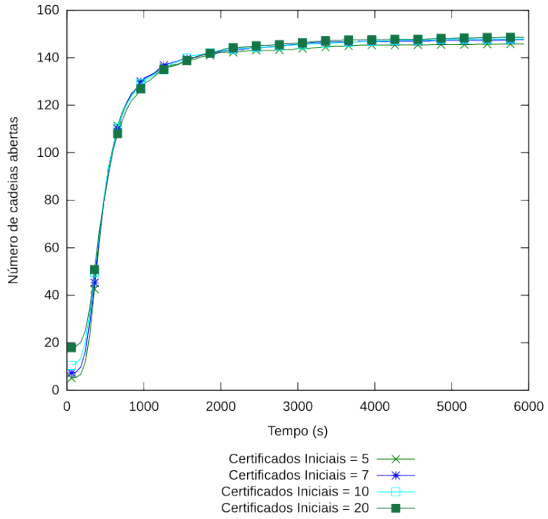
Figura D.35: Resultados para 100 nodos e $m = 20\%$



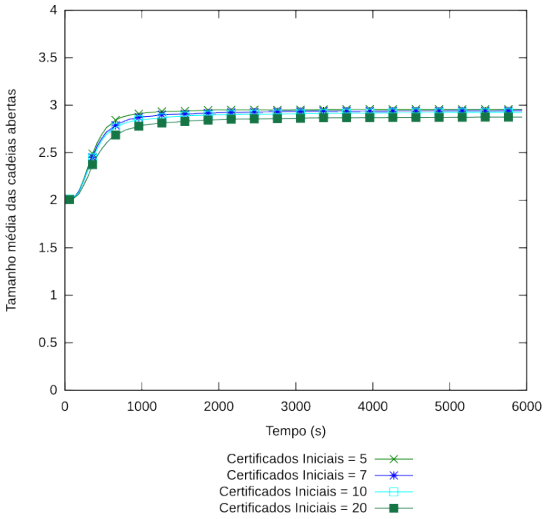

(a) Número de cadeias totais




(b) Número de cadeias fechadas



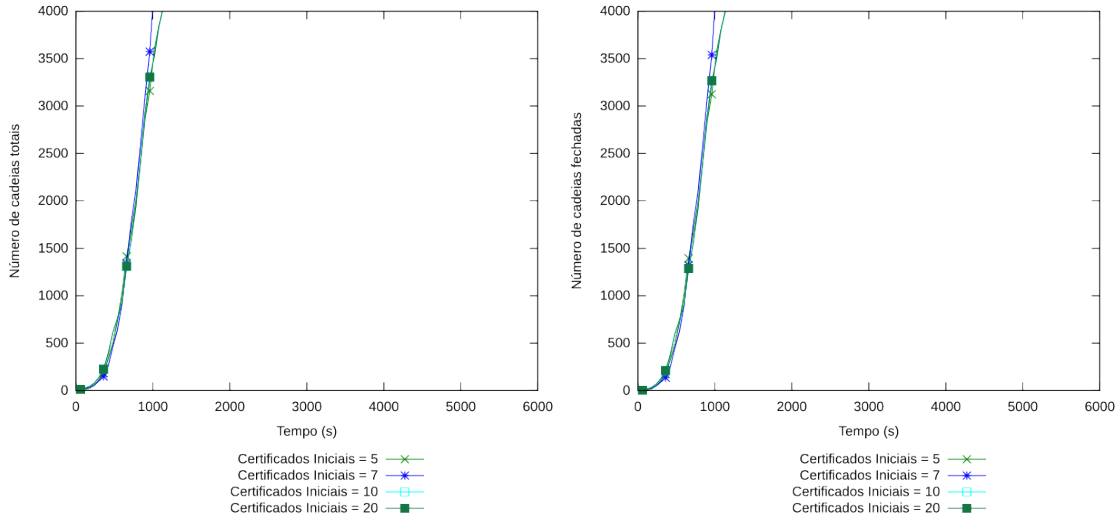

(c) Número de cadeias abertas




(d) Tamanho médio das cadeias

Figura D.36: Resultados para 150 nodos e $m = 20\%$

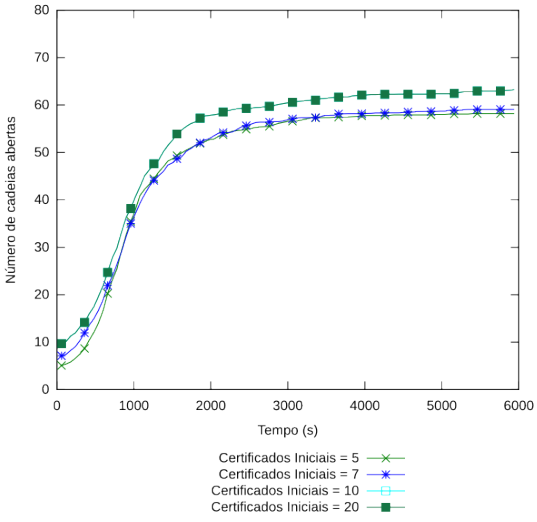
### D.3.3 Ataque *BlackHole* com $m = 50\%$



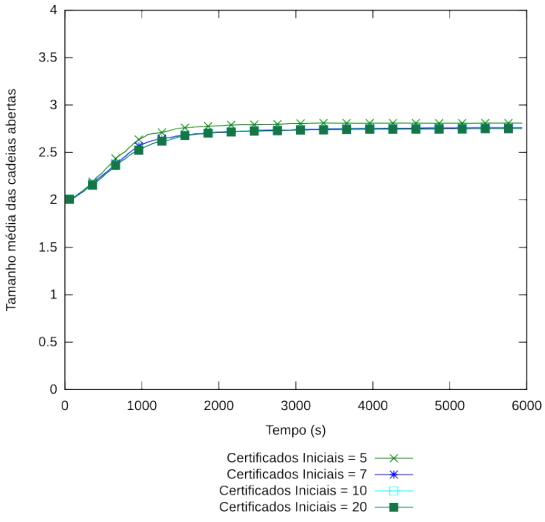

(a) Número de cadeias totais




(b) Número de cadeias fechadas

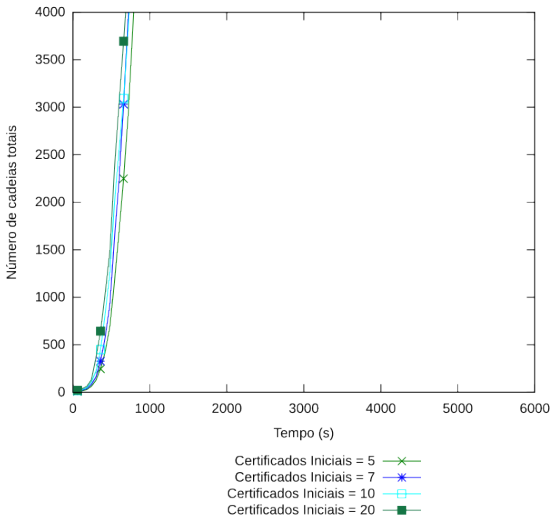



(c) Número de cadeias abertas

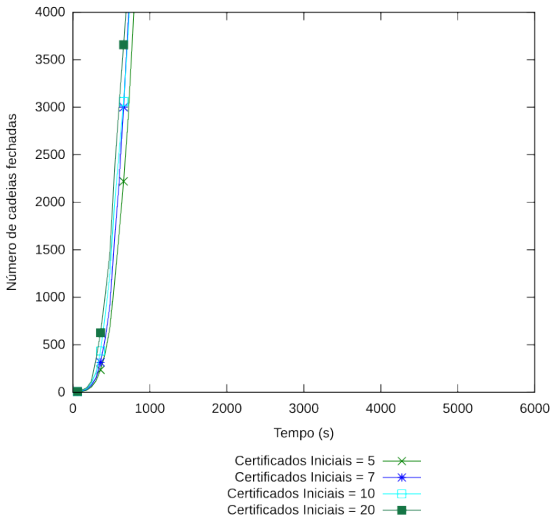



(d) Tamanho médio das cadeias

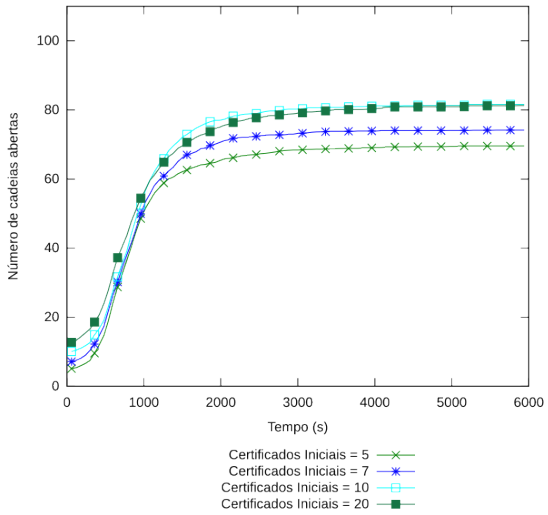
Figura D.37: Resultados para 75 nodos e $m = 50\%$



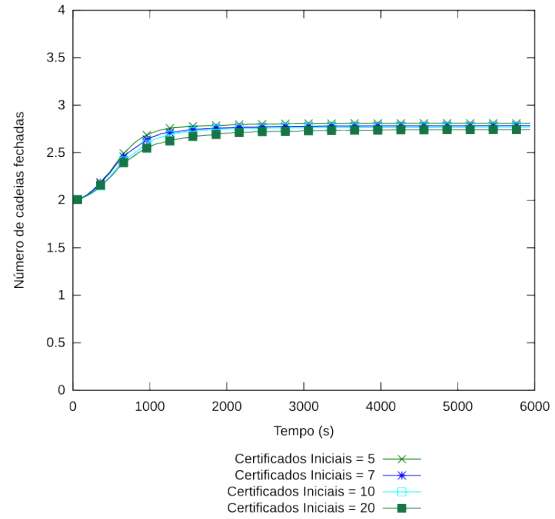

(a) Número de cadeias totais




(b) Número de cadeias fechadas




(c) Número de cadeias abertas

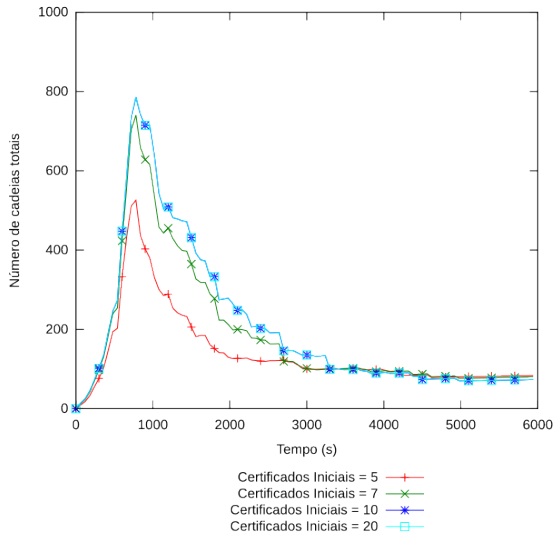



(d) Tamanho médio das cadeias

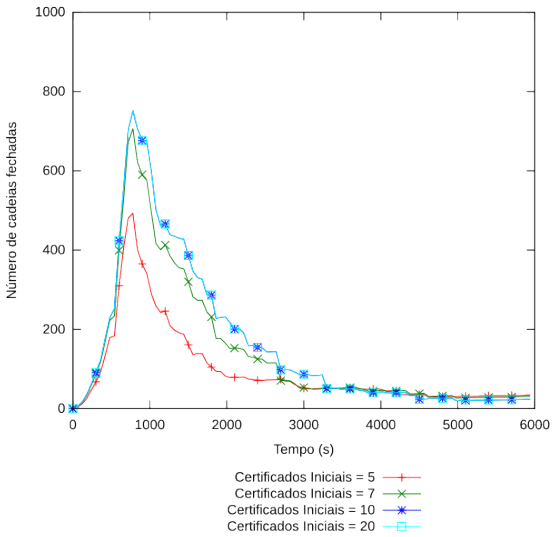
Figura D.38: Resultados para 100 nodos e $m = 50\%$

## D.4 Ataque *Sybil*

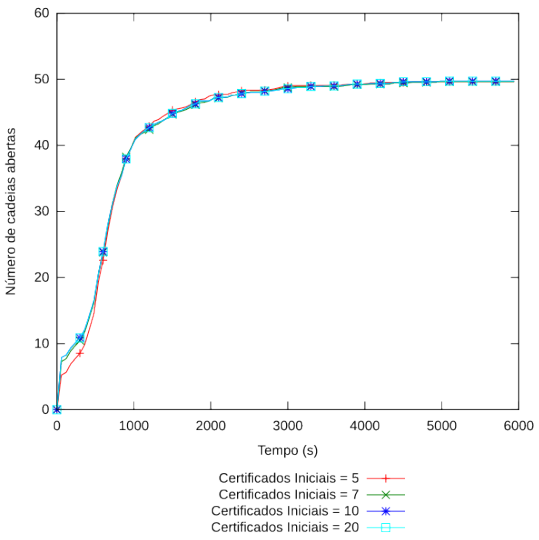
### D.4.1 Ataque *Sybil* com $f = 10\%$



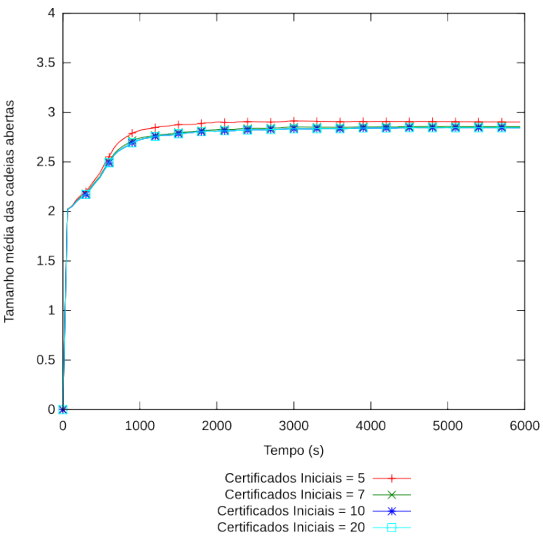

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

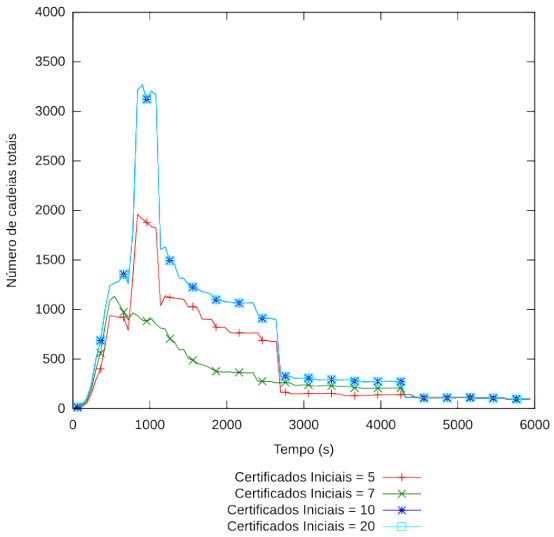



(c) Número de cadeias Abertas

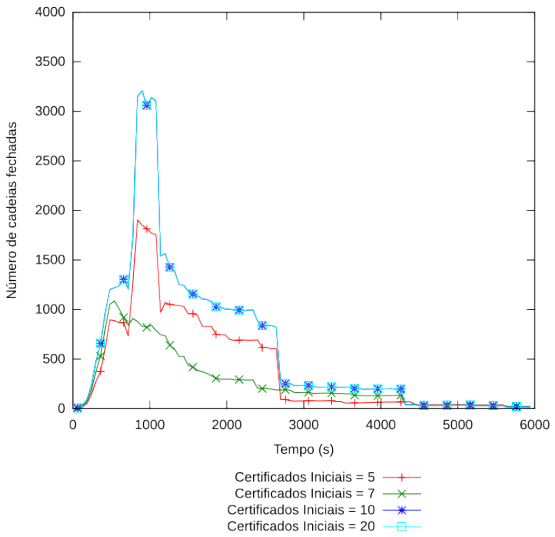



(d) Tamanho médio das cadeias

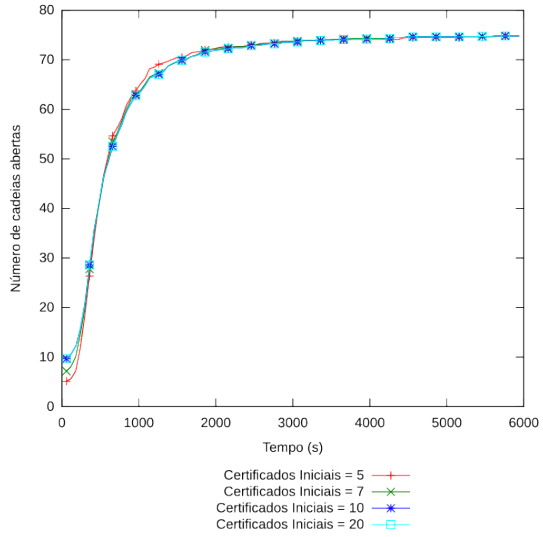
Figura D.39: Resultados para 50 nodos e $f = 10\%$



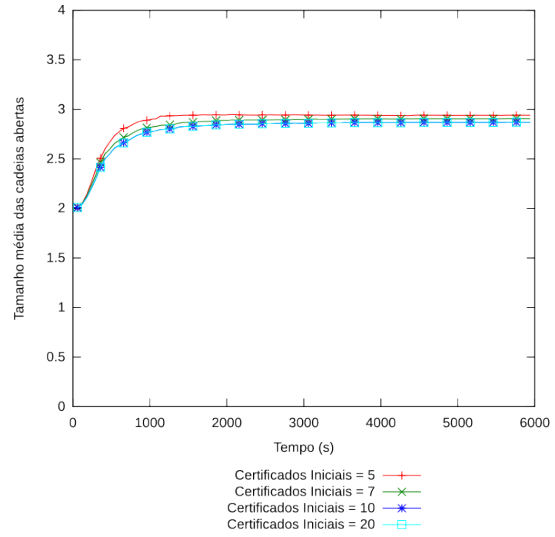

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

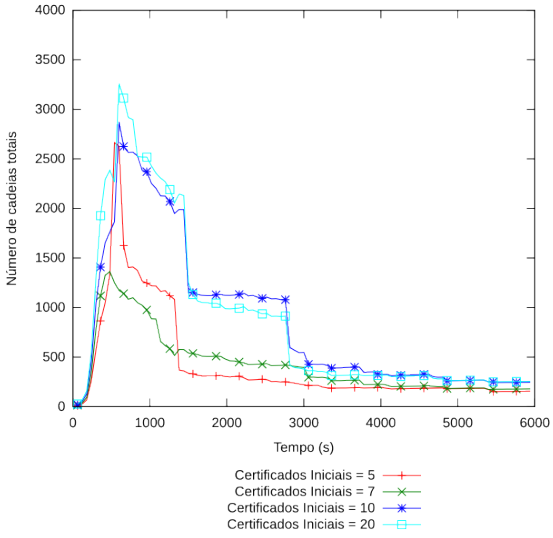



(c) Número de cadeias Abertas

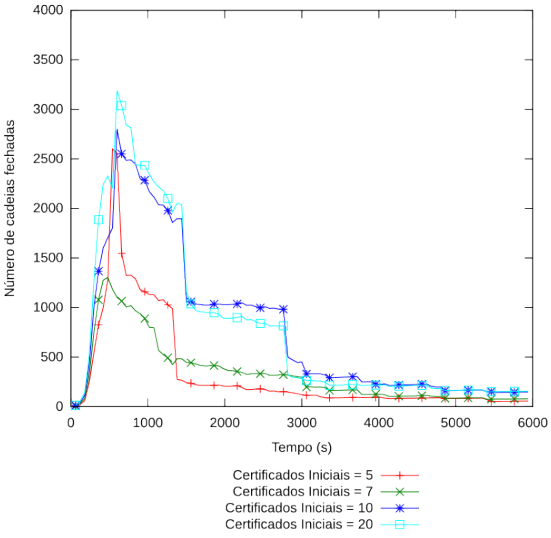



(d) Tamanho médio das cadeias

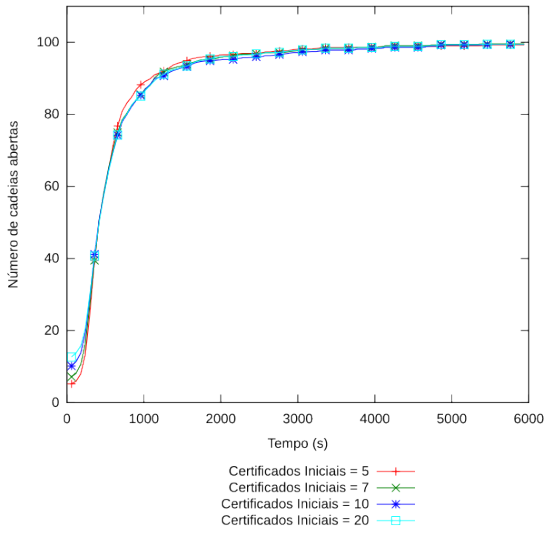
Figura D.40: Resultados para 75 nodos e $f = 10\%$



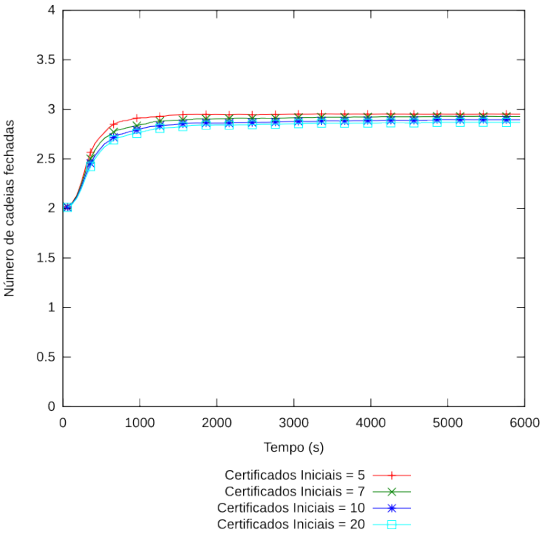

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

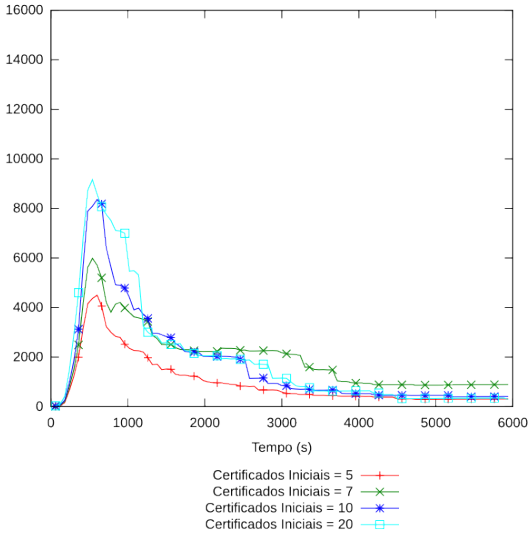



(c) Número de cadeias Abertas

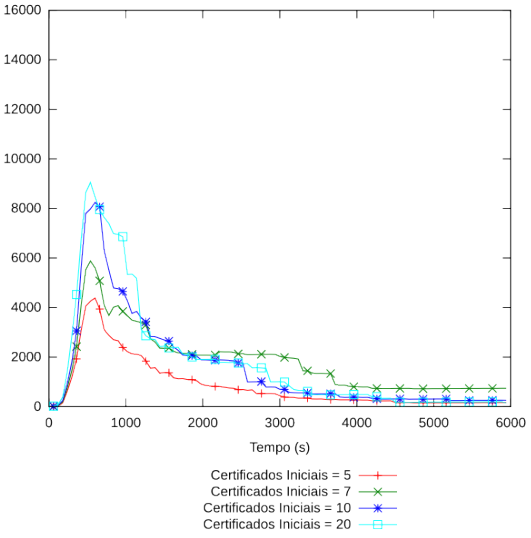



(d) Tamanho médio das cadeias

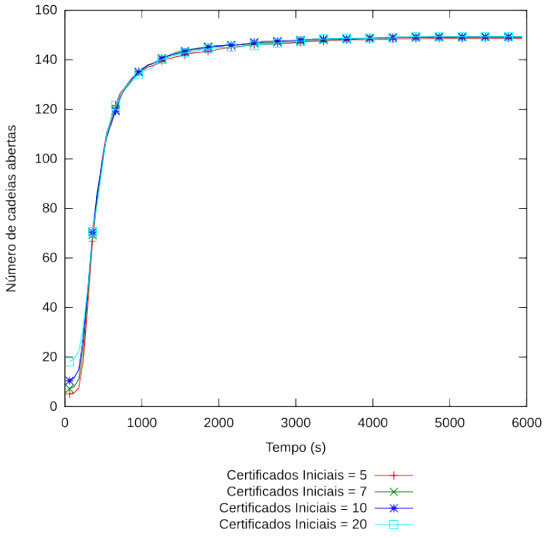
Figura D.41: Resultados para 100 nodos e $f = 10\%$



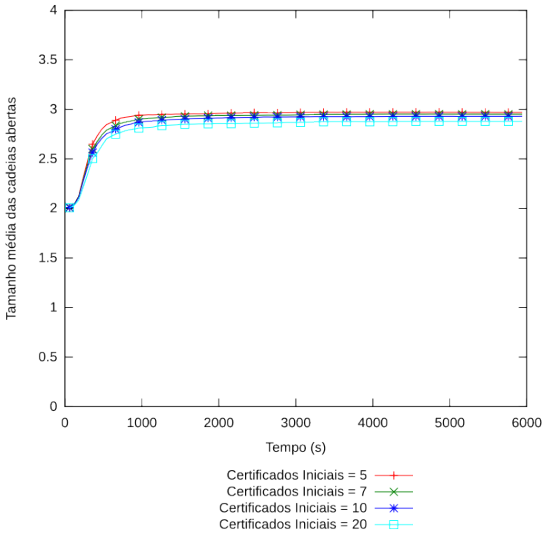

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



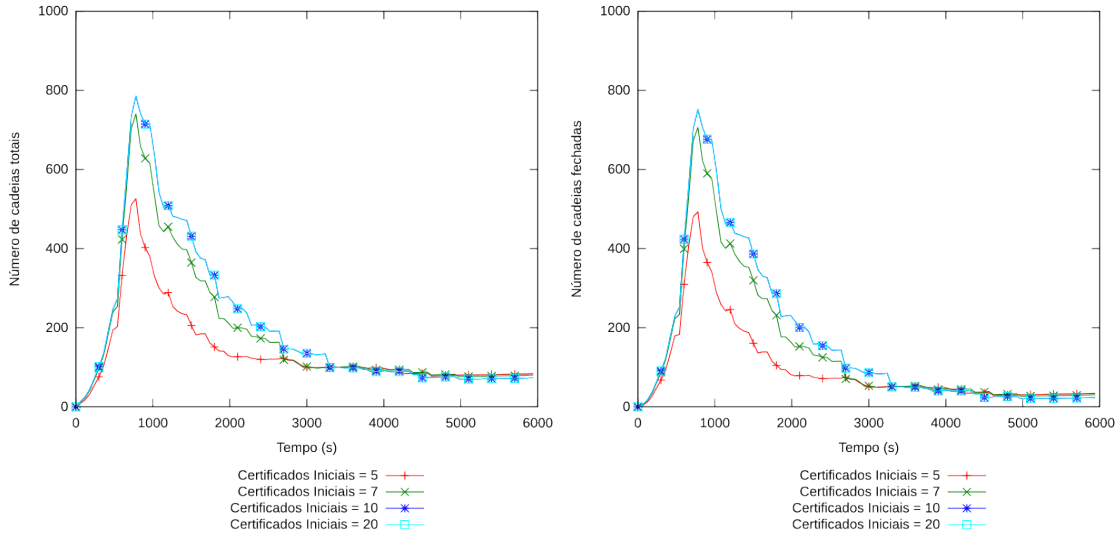

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura D.42: Resultados para 150 nodos e $f = 10\%$

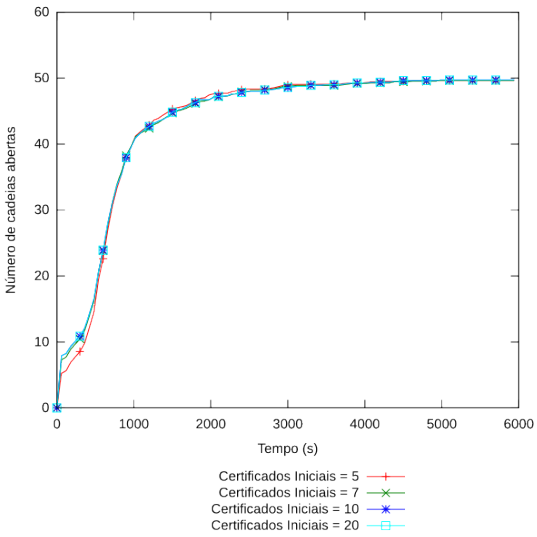
### D.4.2 Ataque *Sybil* com $f = 20\%$



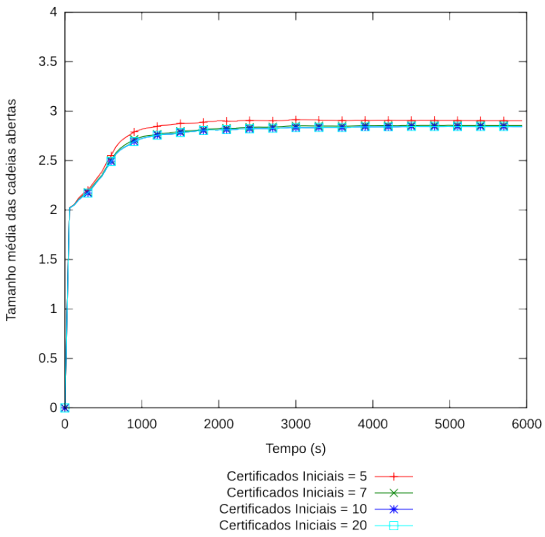

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

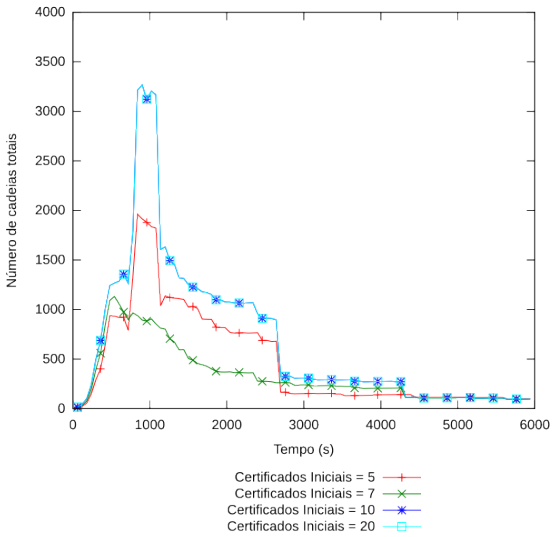



(c) Número de cadeias Abertas

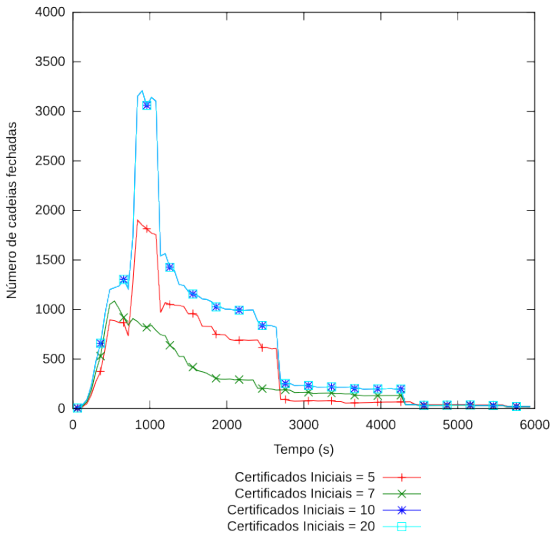



(d) Tamanho médio das cadeias

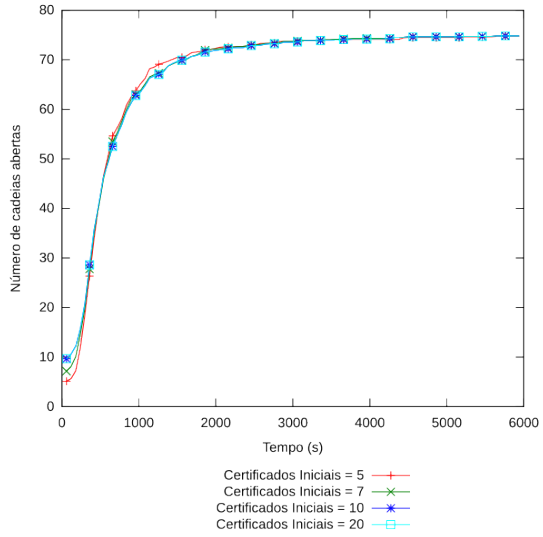
Figura D.43: Resultados para 50 nodos e $f = 20\%$



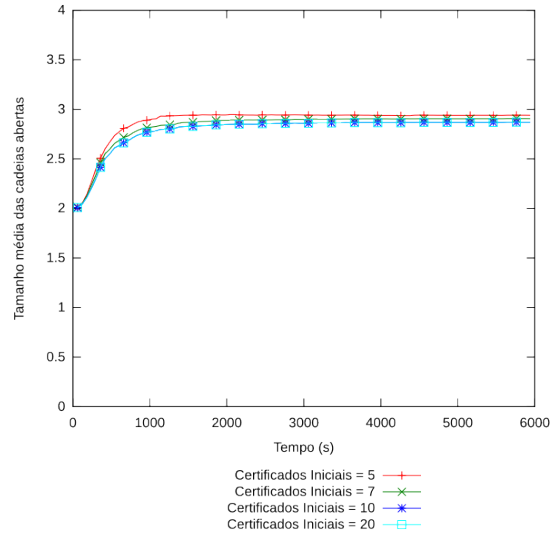

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

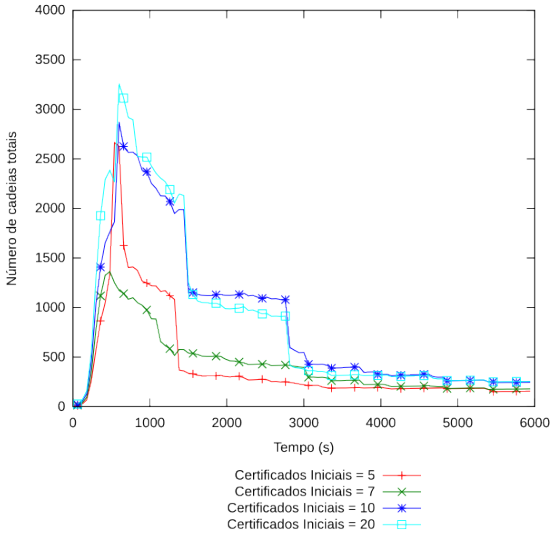



(c) Número de cadeias Abertas

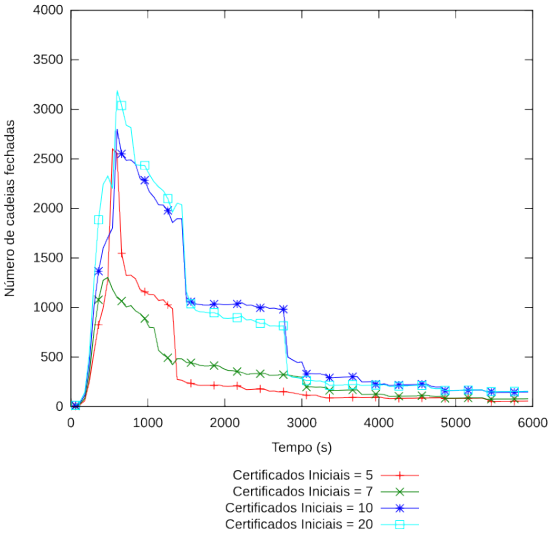



(d) Tamanho médio das cadeias

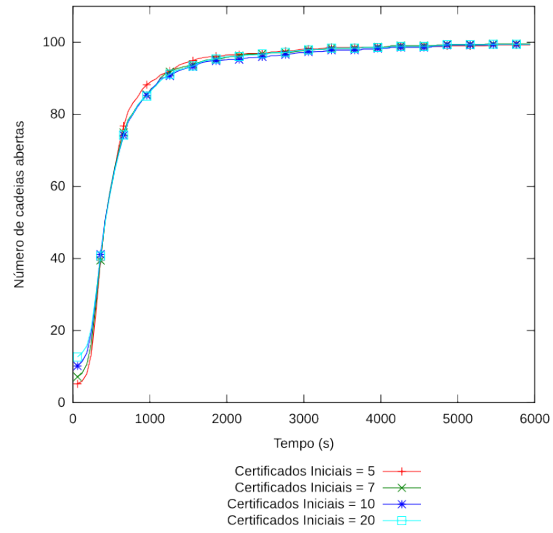
Figura D.44: Resultados para 75 nodos e $f = 20\%$



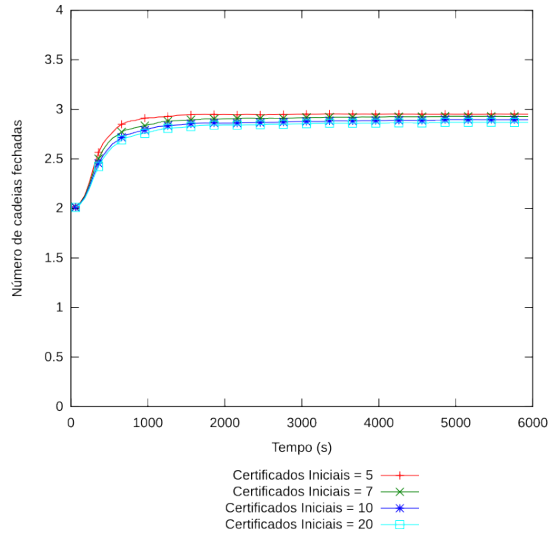

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

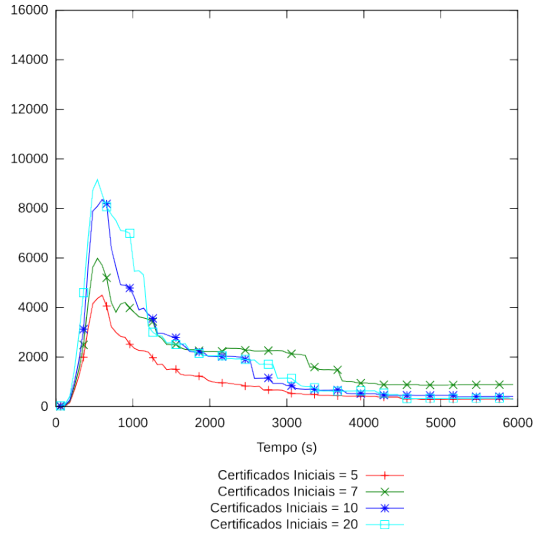



(c) Número de cadeias Abertas

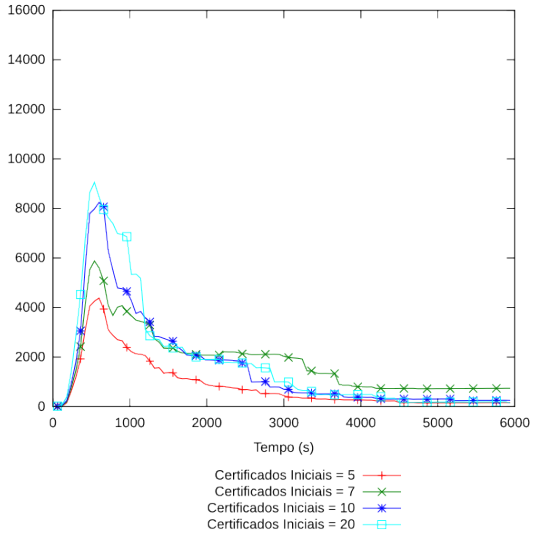



(d) Tamanho médio das cadeias

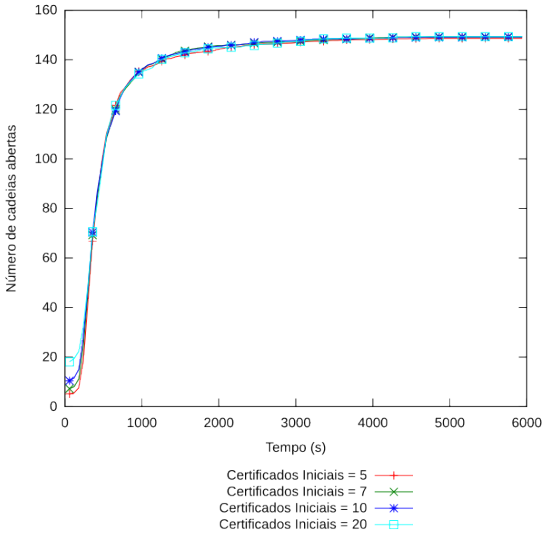
Figura D.45: Resultados para 100 nodos e $f = 20\%$



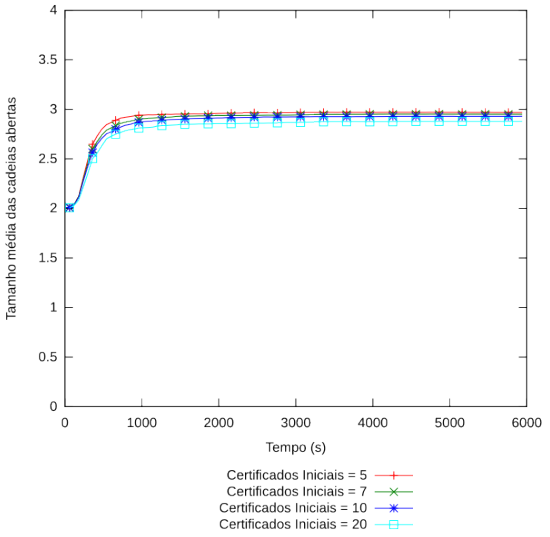

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



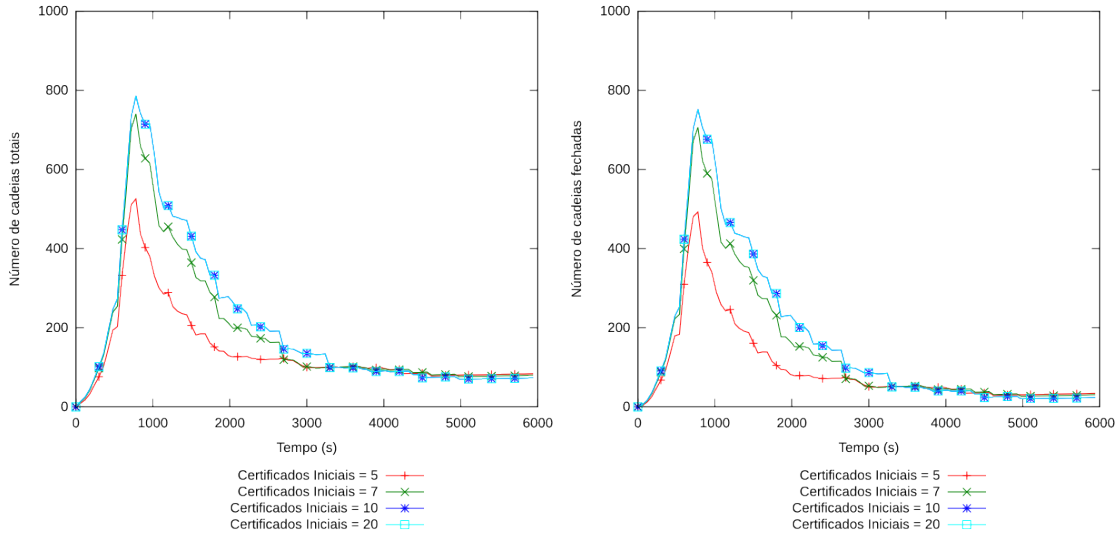

(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura D.46: Resultados para 150 nodos e $f = 20\%$

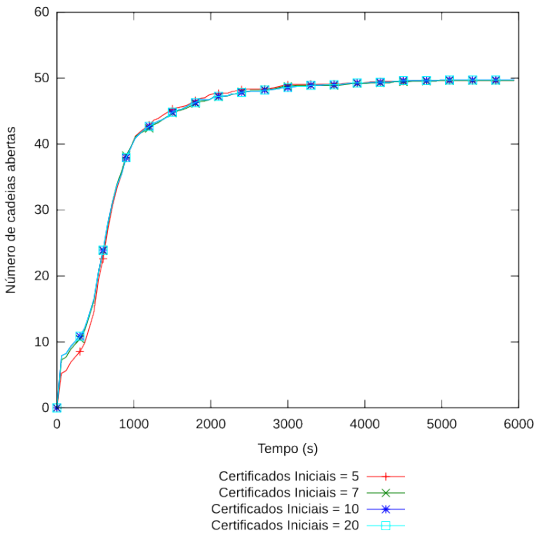
### D.4.3 Ataque *Sybil* com $f = 50\%$



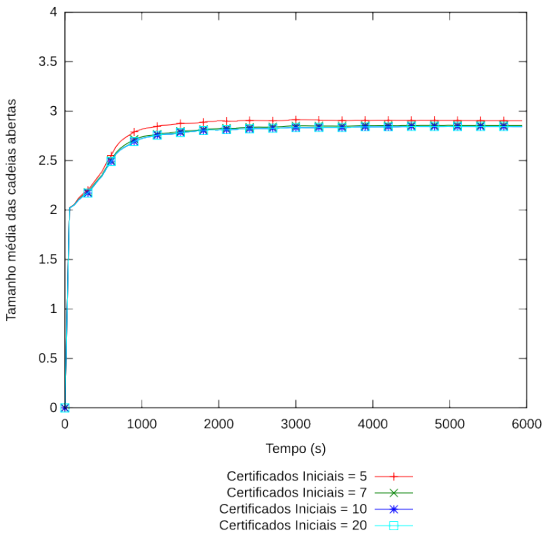

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

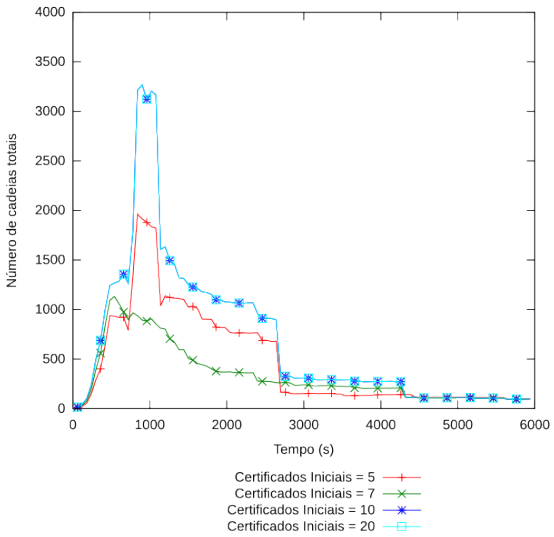



(c) Número de cadeias Abertas

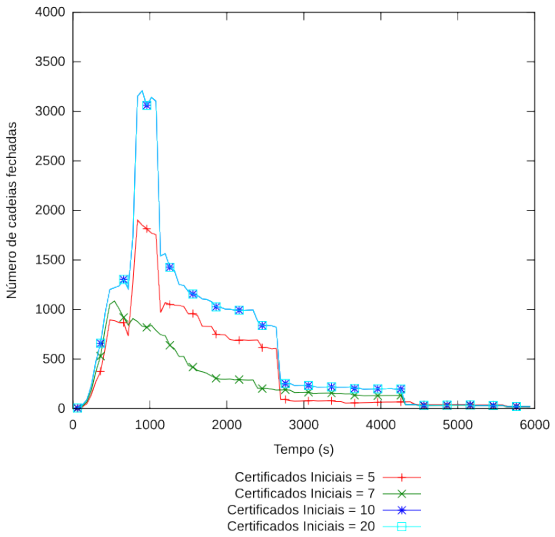



(d) Tamanho médio das cadeias

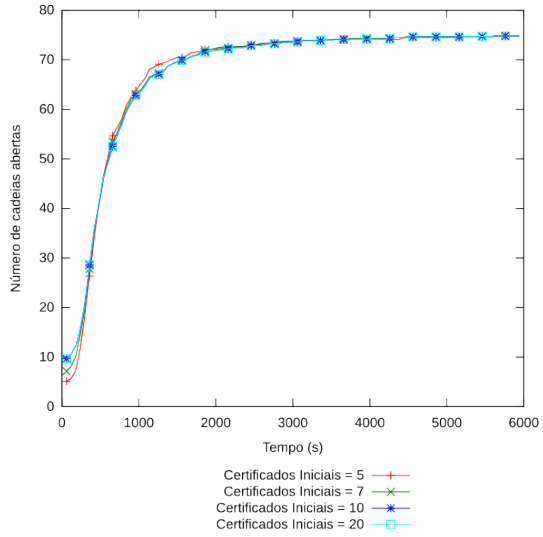
Figura D.47: Resultados para 50 nodos e $f = 50\%$



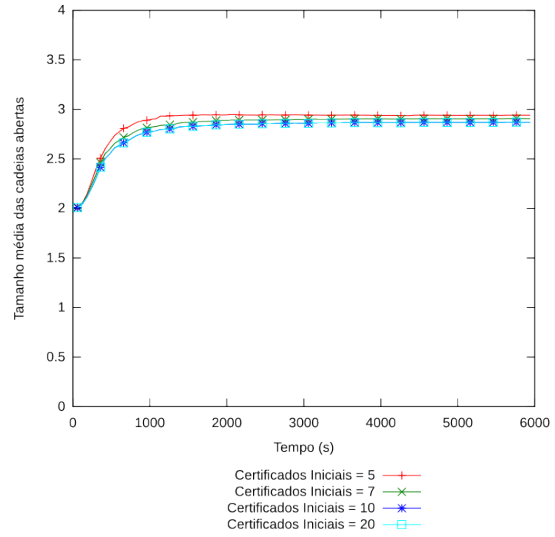

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

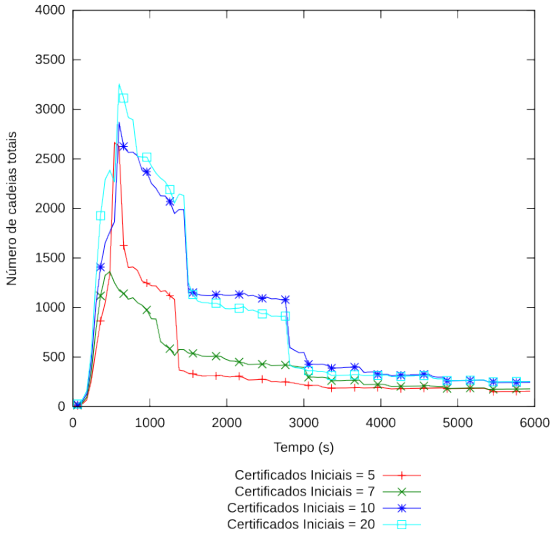



(c) Número de cadeias Abertas

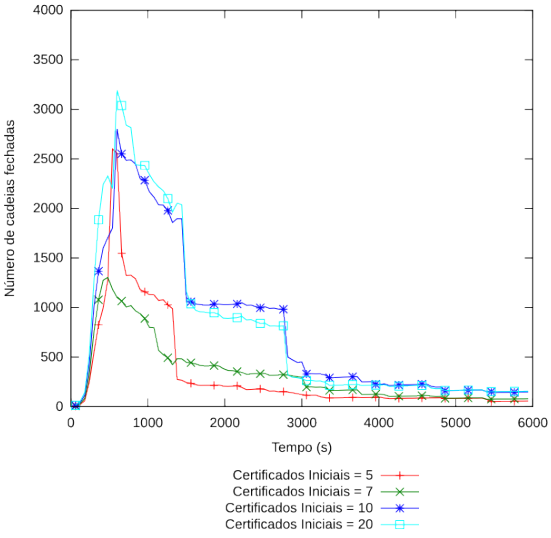



(d) Tamanho médio das cadeias

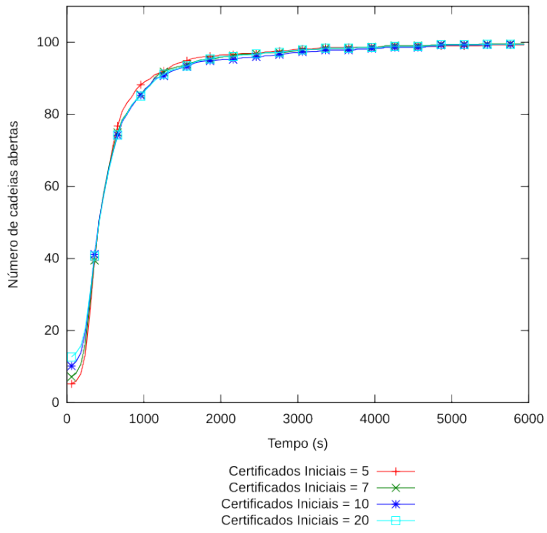
Figura D.48: Resultados para 75 nodos e $f = 50\%$



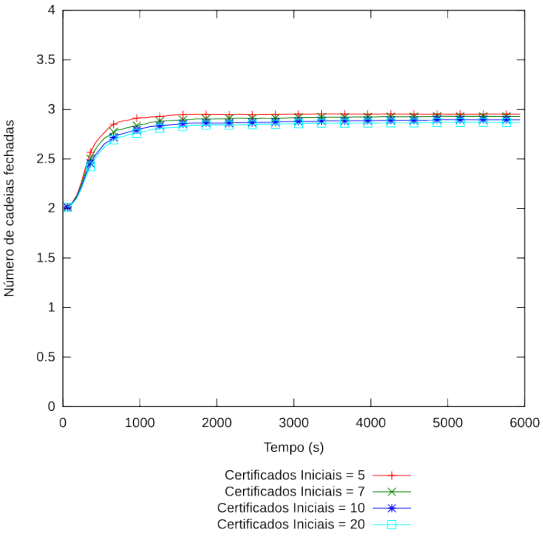

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

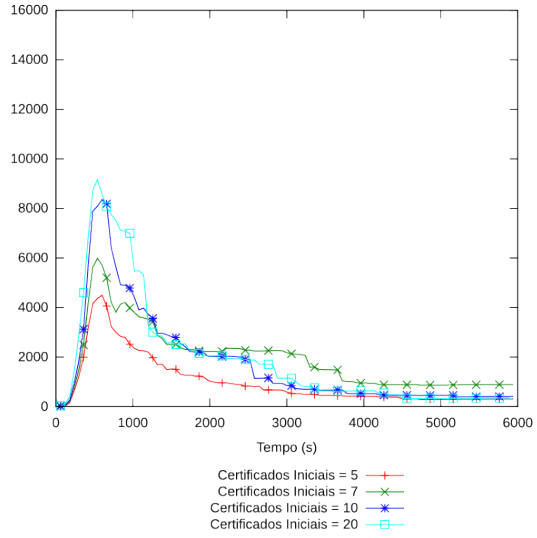



(c) Número de cadeias Abertas

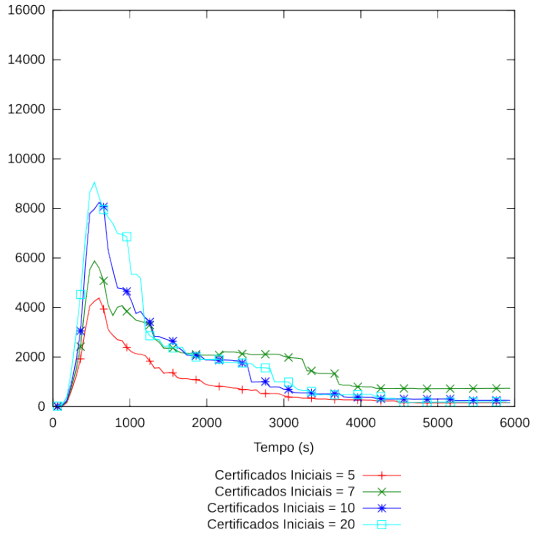



(d) Tamanho médio das cadeias

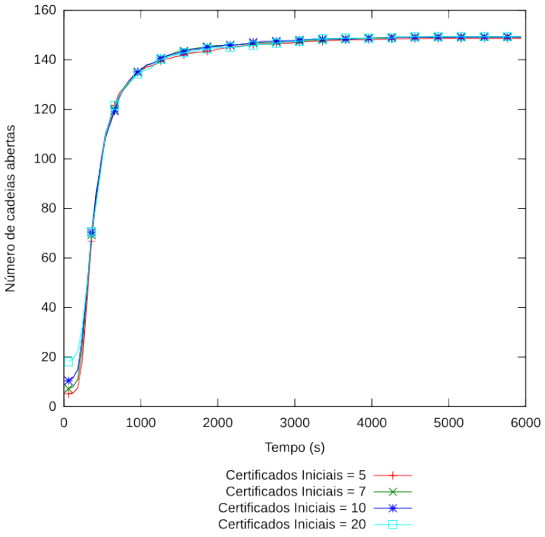
Figura D.49: Resultados para 100 nodos e $f = 50\%$



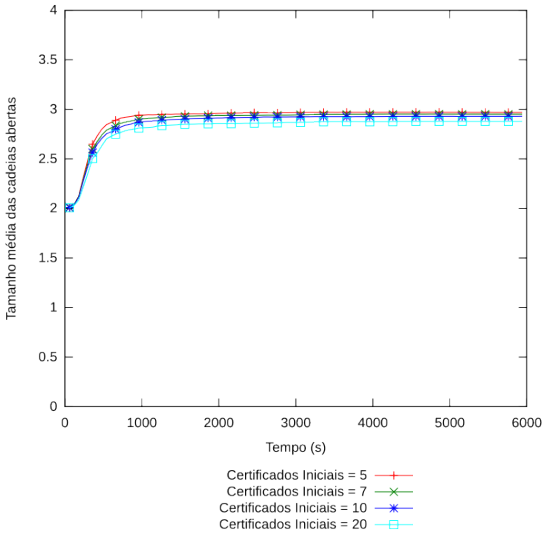

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas

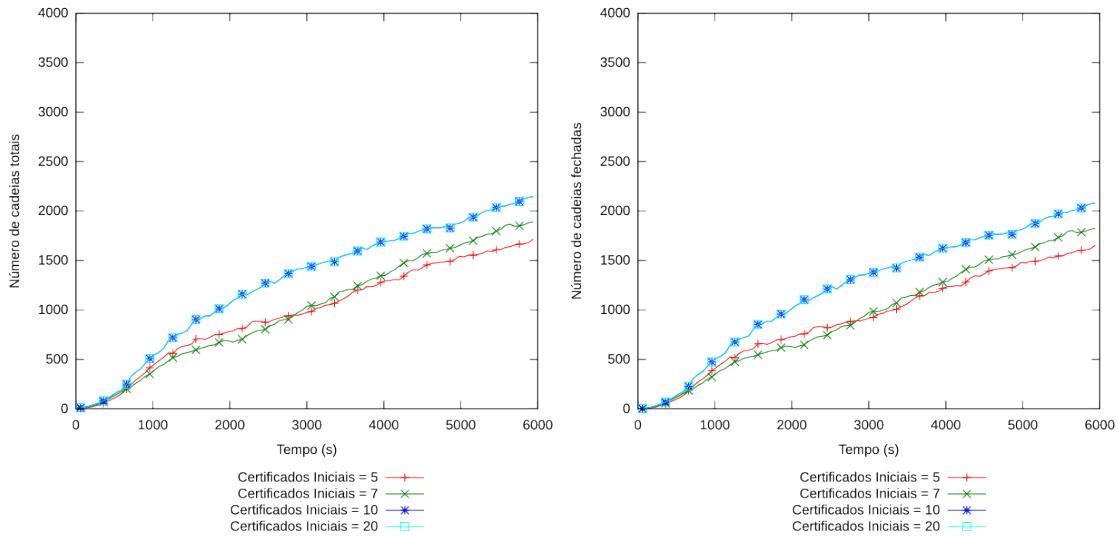



(d) Tamanho médio das cadeias

Figura D.50: Resultados para 150 nodos e $f = 50\%$

## D.5 Ataque de Falsificaçao - Ataque independente

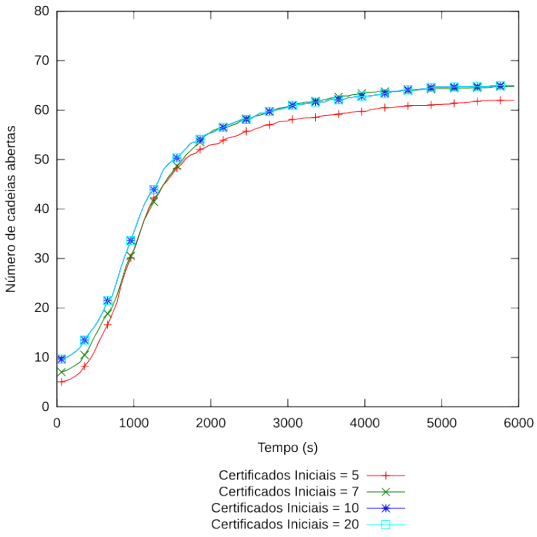
### D.5.1 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 10\%$



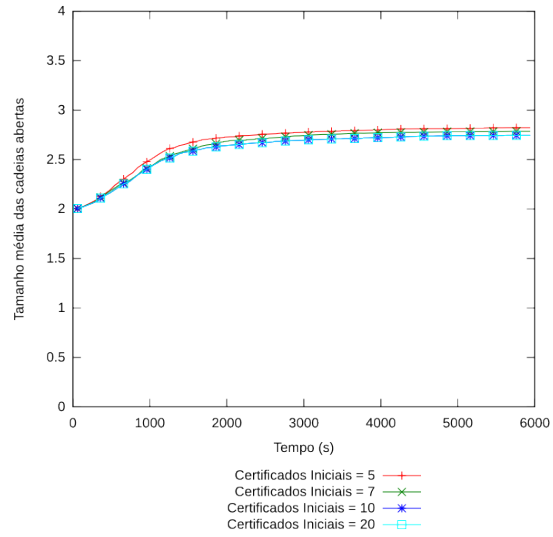

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

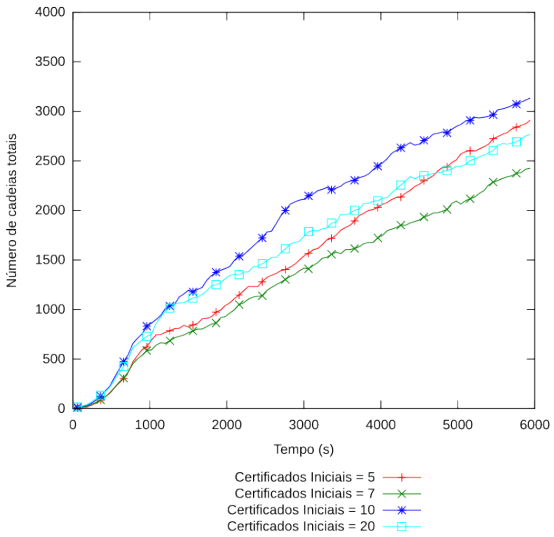



(c) Número de cadeias Abertas

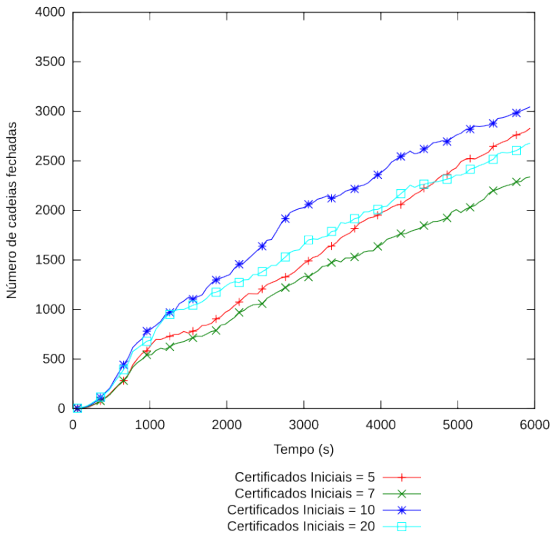



(d) Tamanho médio das cadeias

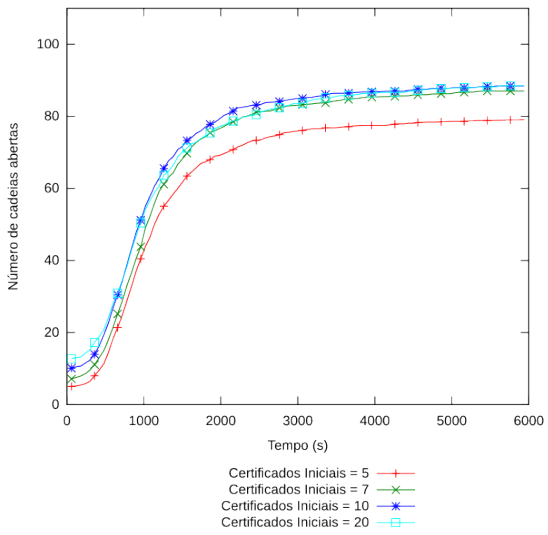
Figura D.51: Resultados para 75 nodos, $m = 10\%$ e $N_a = 10\%$



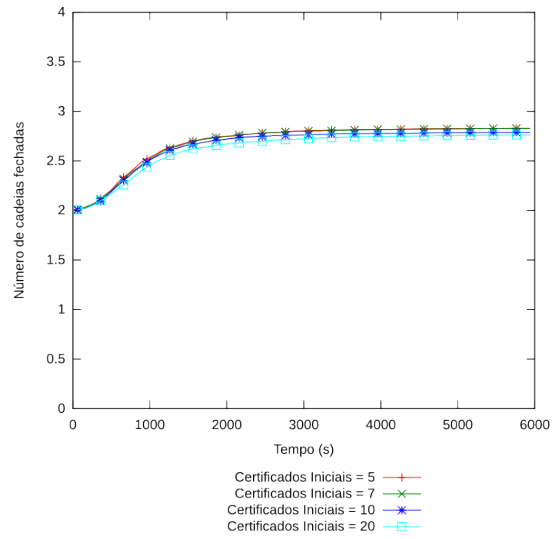

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



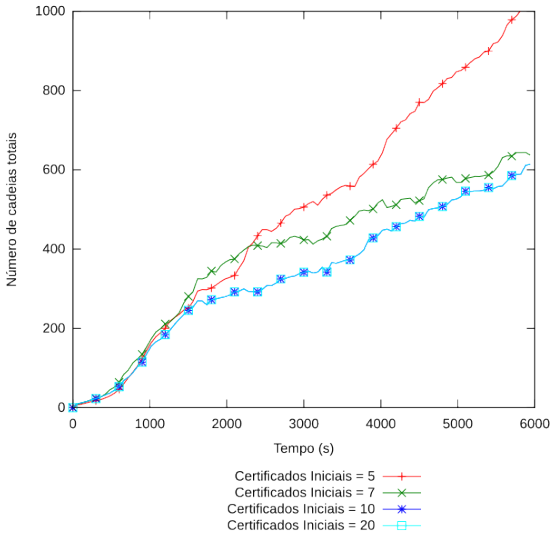

(c) Número de cadeias Abertas



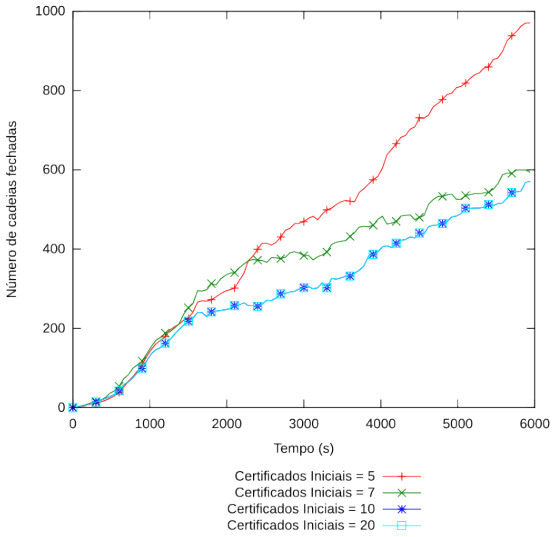

(d) Tamanho médio das cadeias

Figura D.52: Resultados para 100 nodos, $m = 10\%$ e $N_a = 10\%$

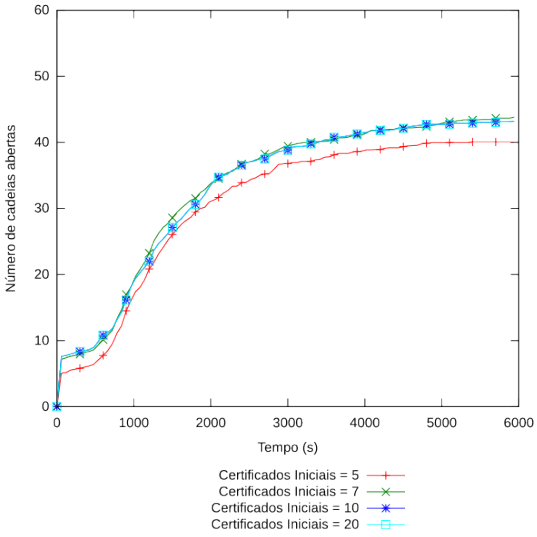
### D.5.2 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 25\%$



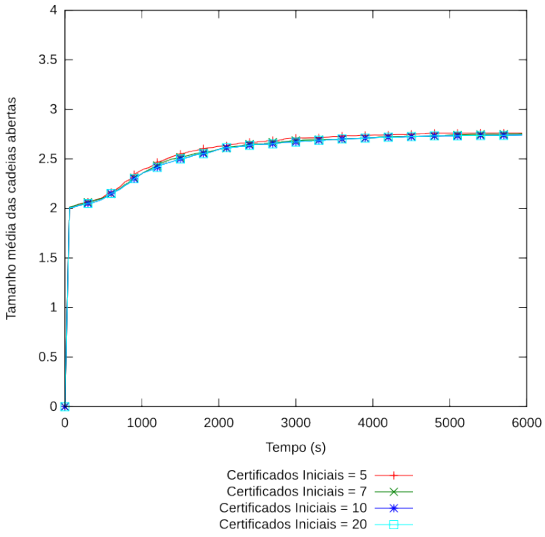

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

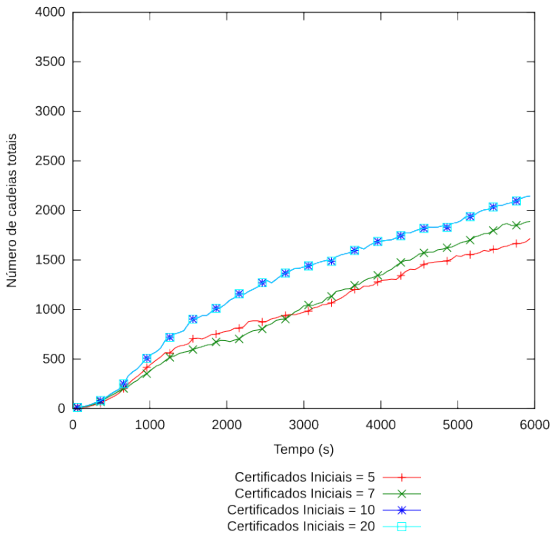



(c) Número de cadeias Abertas

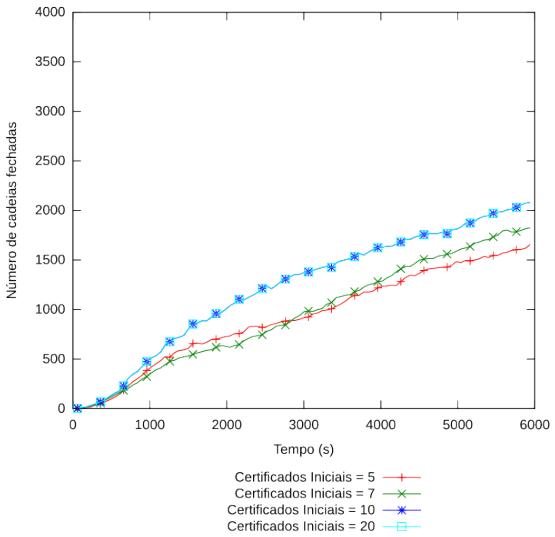



(d) Tamanho médio das cadeias

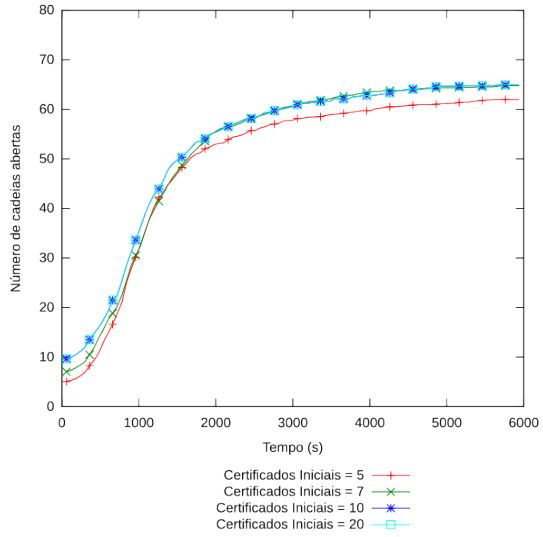
Figura D.53: Resultados para 50 nodos, $m = 10\%$ e $N_a = 25\%$



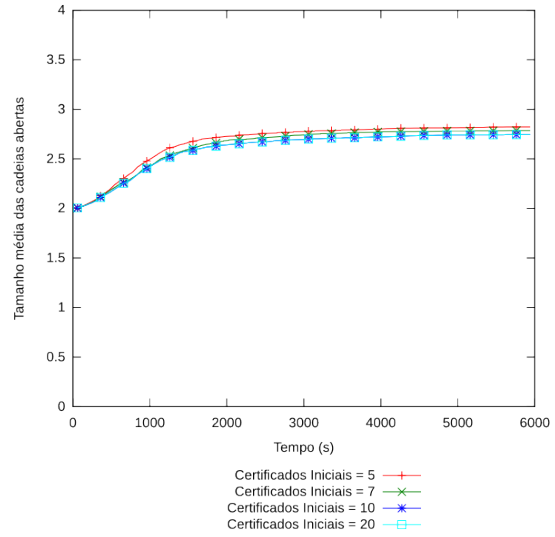

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

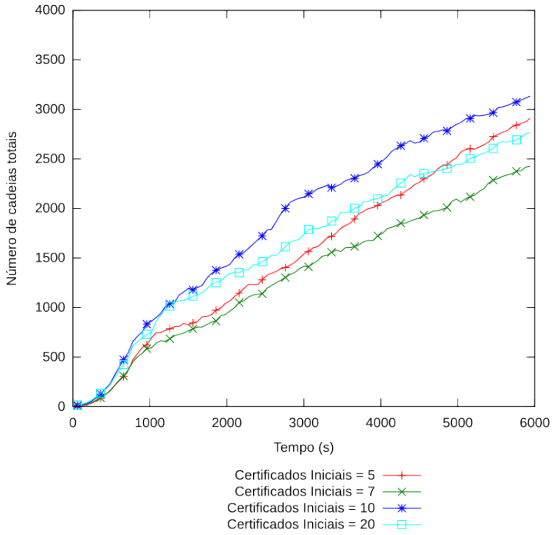



(c) Número de cadeias Abertas

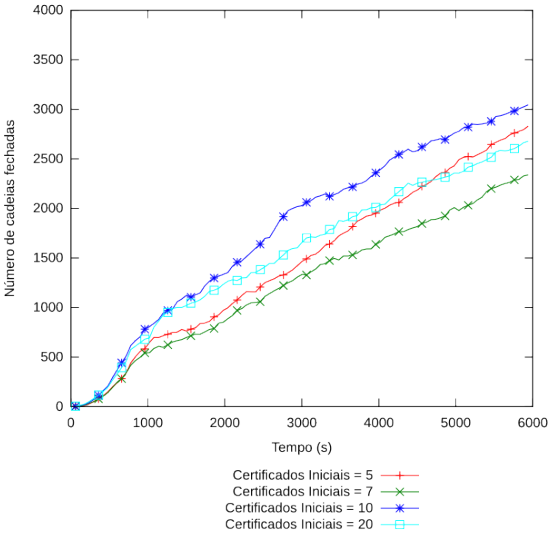



(d) Tamanho médio das cadeias

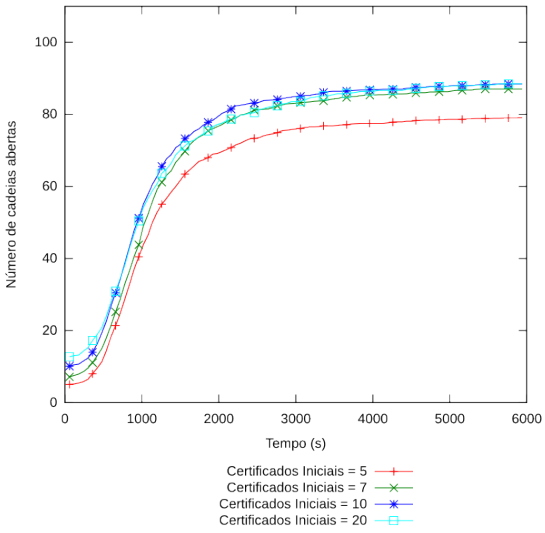
Figura D.54: Resultados para 75 nodos, $m = 10\%$ e $N_a = 25\%$



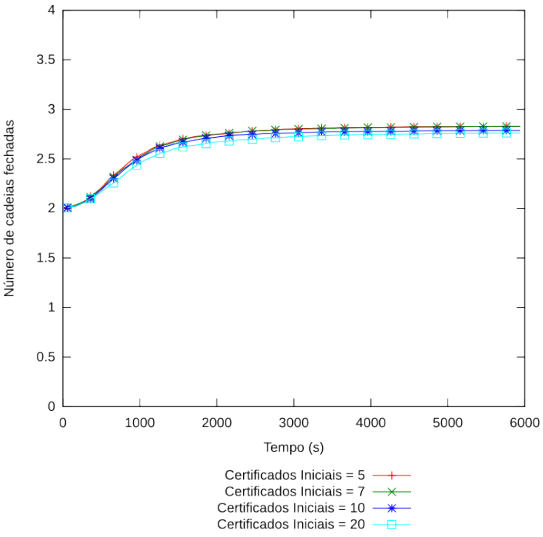

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

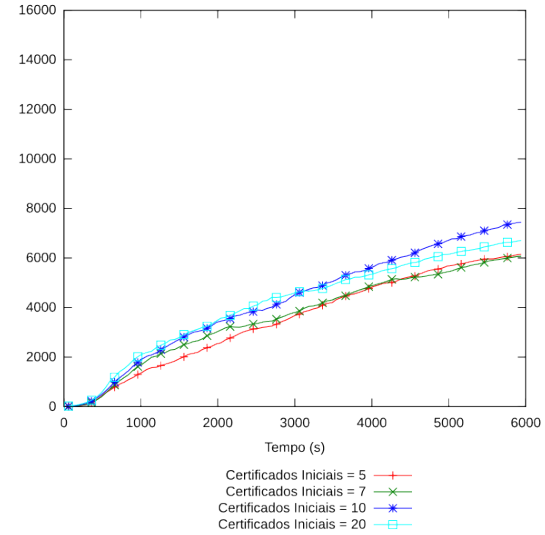



(c) Número de cadeias Abertas

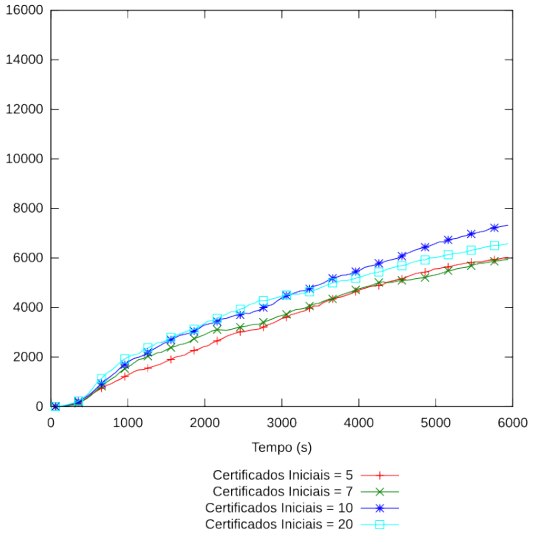



(d) Tamanho médio das cadeias

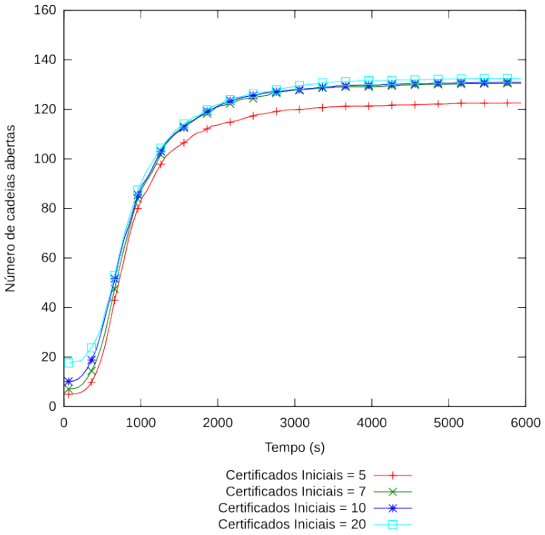
Figura D.55: Resultados para 100 nodos, $m = 10\%$ e $N_a = 25\%$



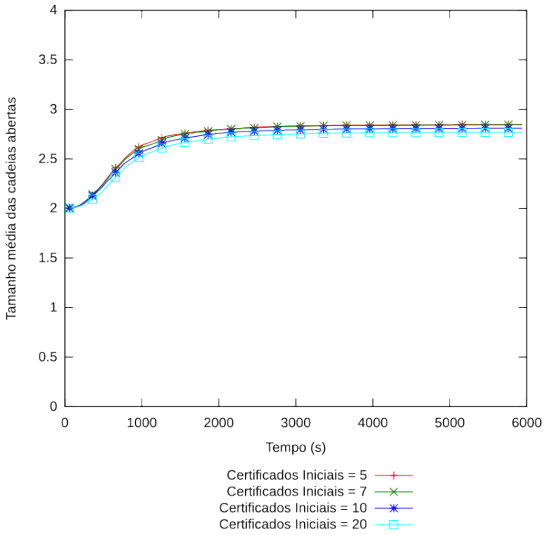

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



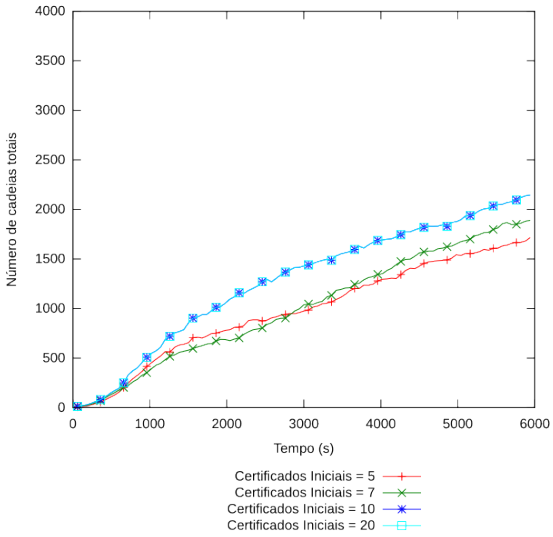

(c) Número de cadeias Abertas



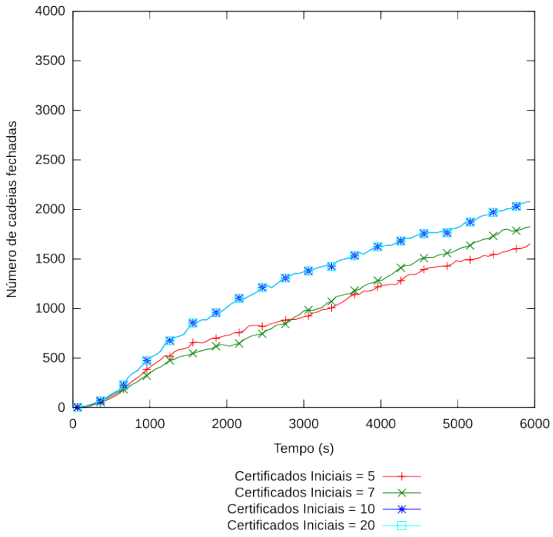

(d) Tamanho médio das cadeias

Figura D.56: Resultados para 150 nodos, $m = 10\%$ e $N_a = 25\%$

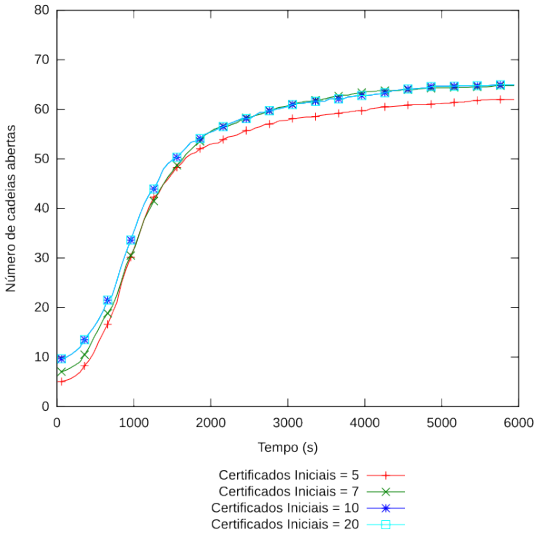
### D.5.3 Ataque de Falsificaçao com $m = 10\%$ e $N_a = 50\%$



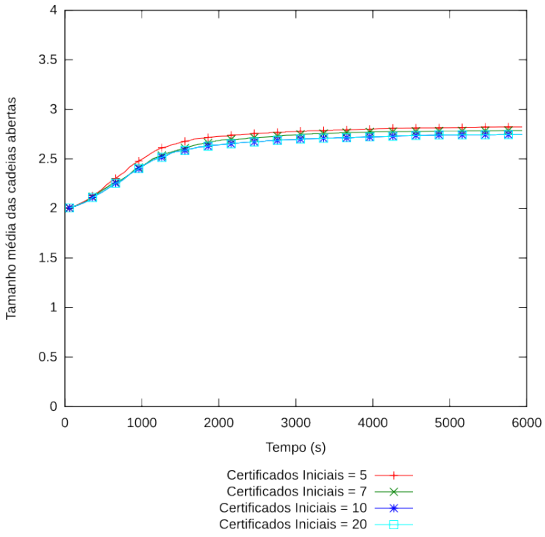

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

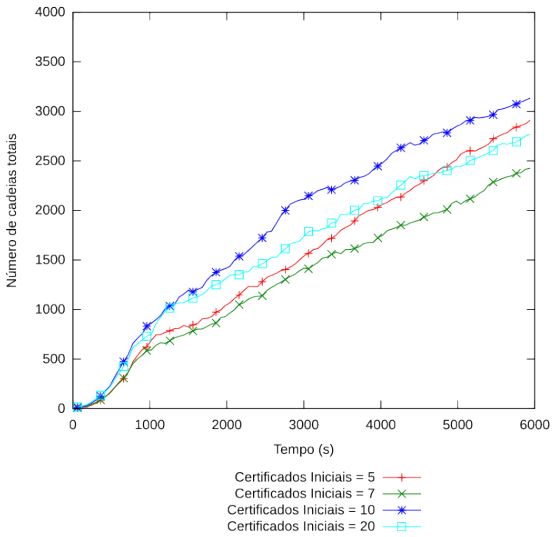



(c) Número de cadeias Abertas

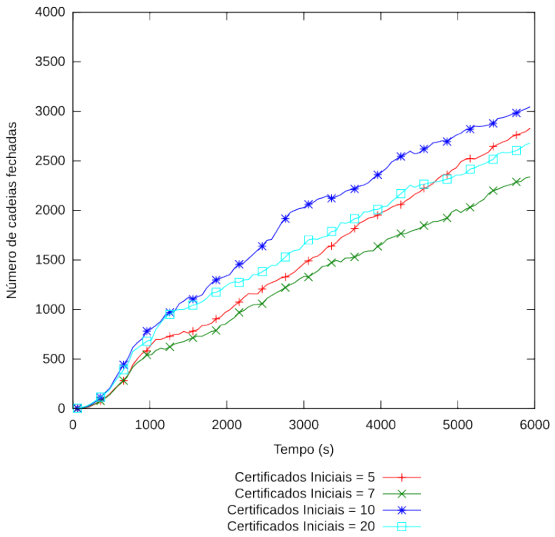



(d) Tamanho médio das cadeias

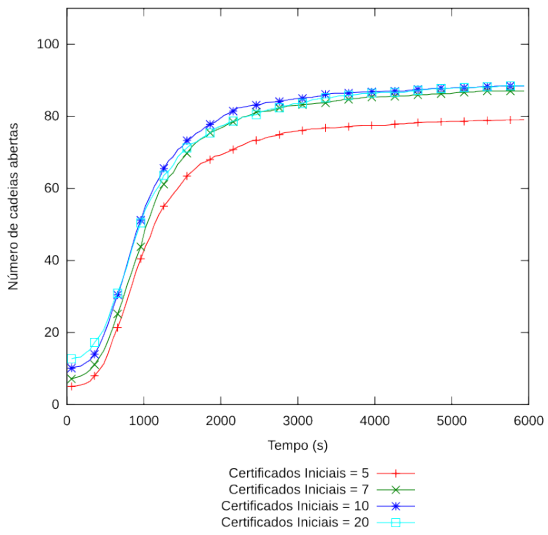
Figura D.57: Resultados para 75 nodos, $m = 10\%$ e $N_a = 50\%$



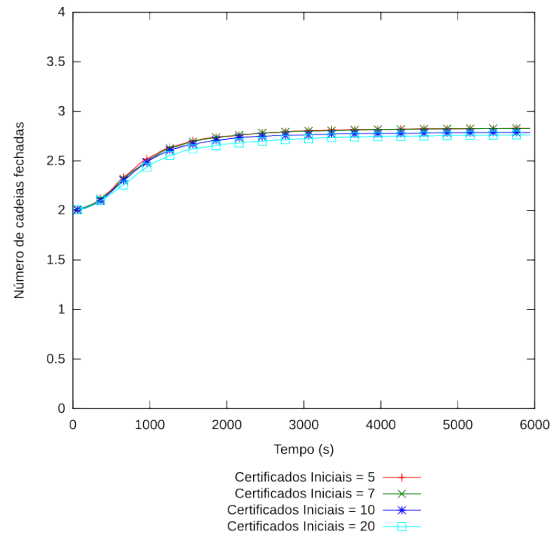

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



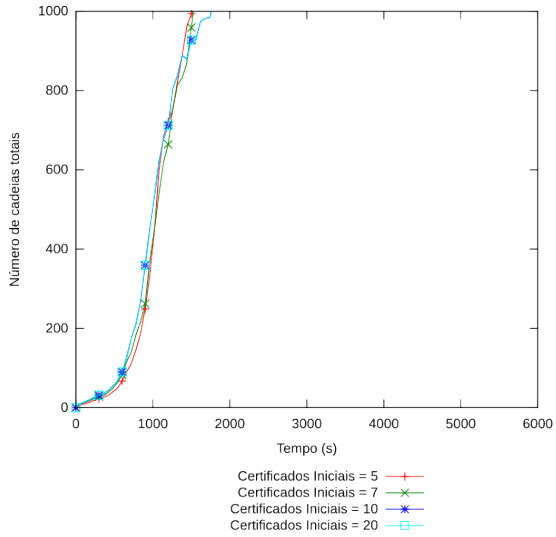

(c) Número de cadeias Abertas



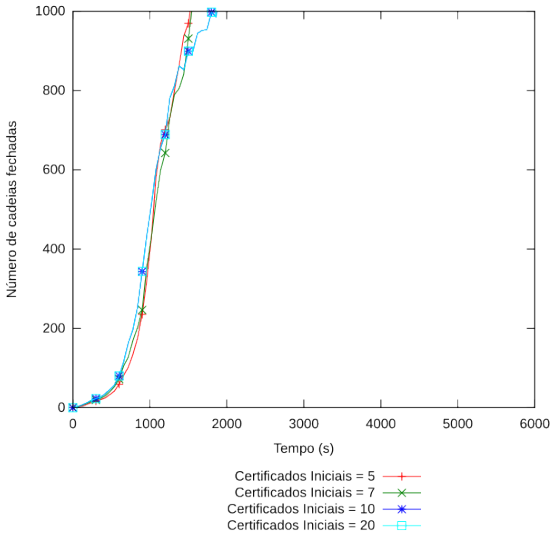

(d) Tamanho médio das cadeias

Figura D.58: Resultados para 100 nodos, $m = 10\%$ e $N_a = 50\%$

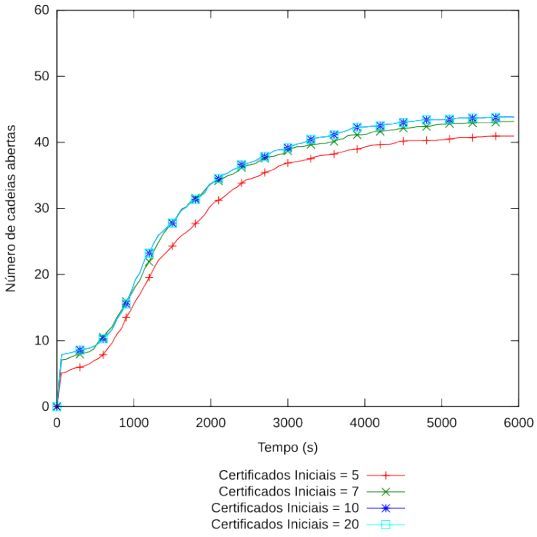
### D.5.4 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 10\%$



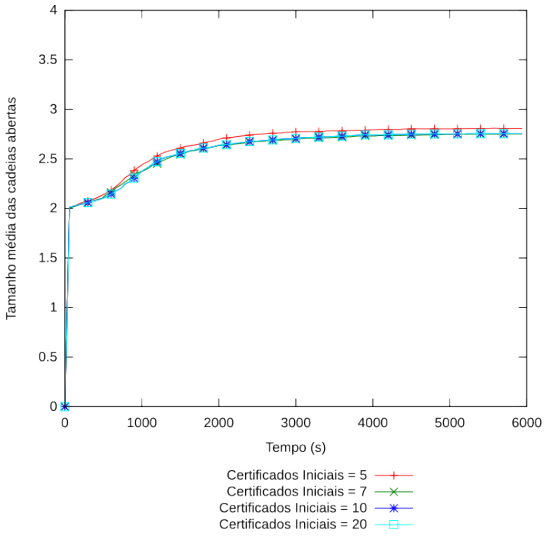

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

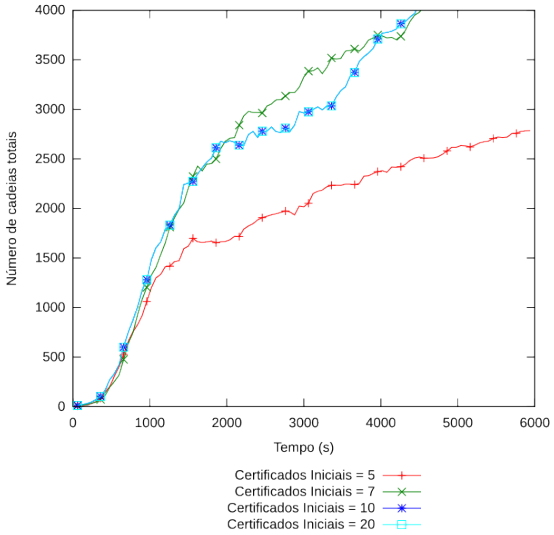



(c) Número de cadeias Abertas

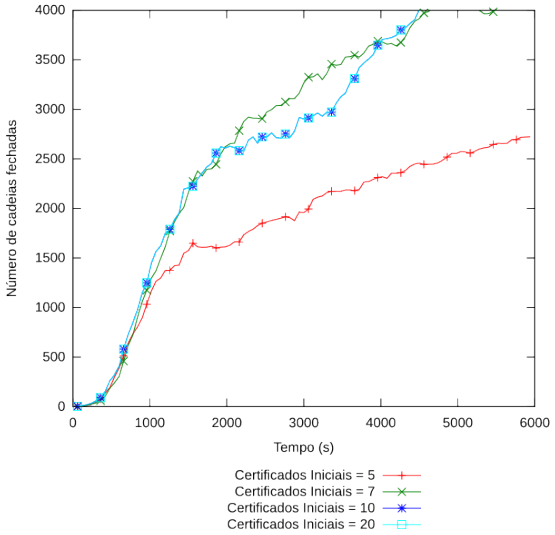



(d) Tamanho médio das cadeias

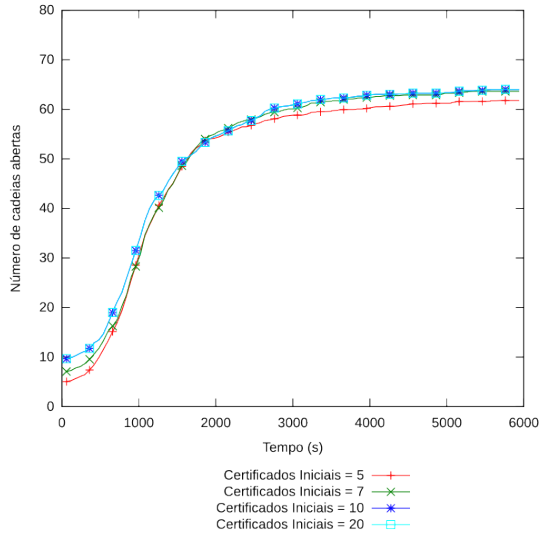
Figura D.59: Resultados para 50 nodos, $m = 20\%$ e $N_a = 10\%$



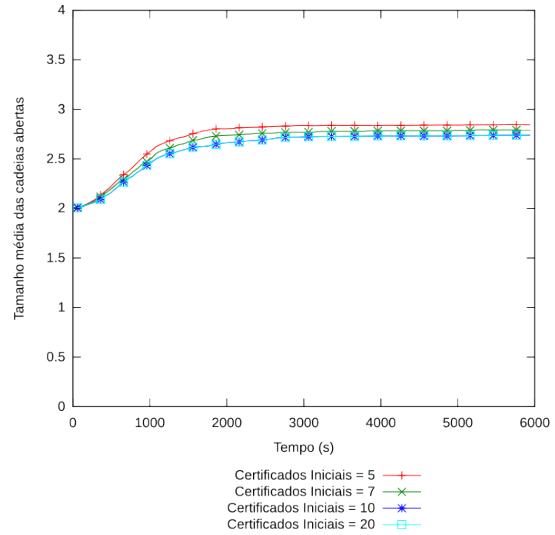

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

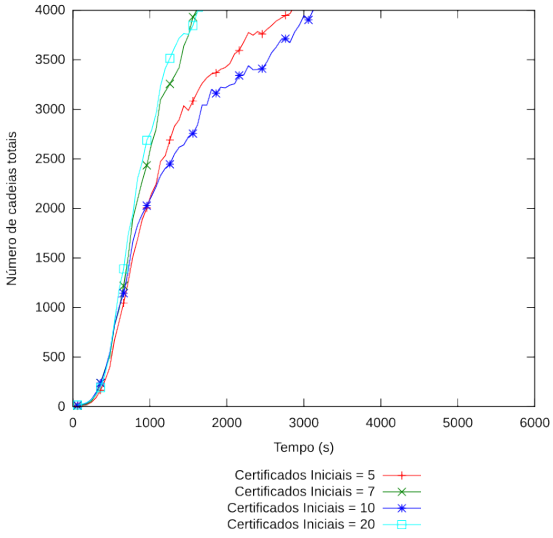



(c) Número de cadeias Abertas

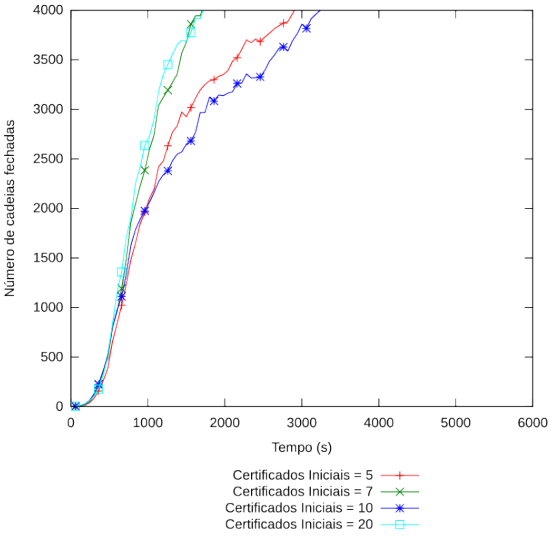



(d) Tamanho médio das cadeias

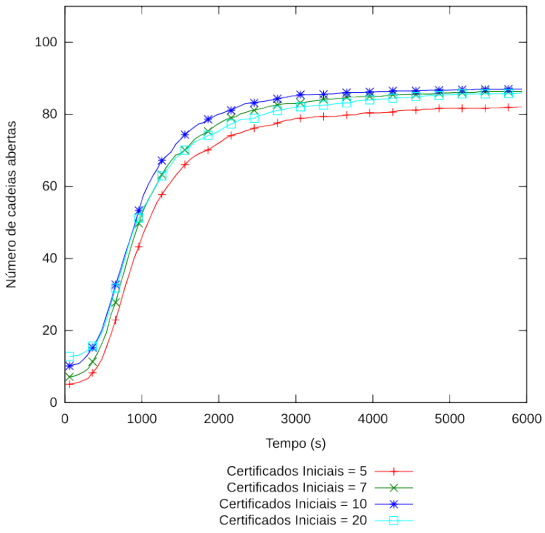
Figura D.60: Resultados para 75 nodos, $m = 20\%$ e $N_a = 10\%$



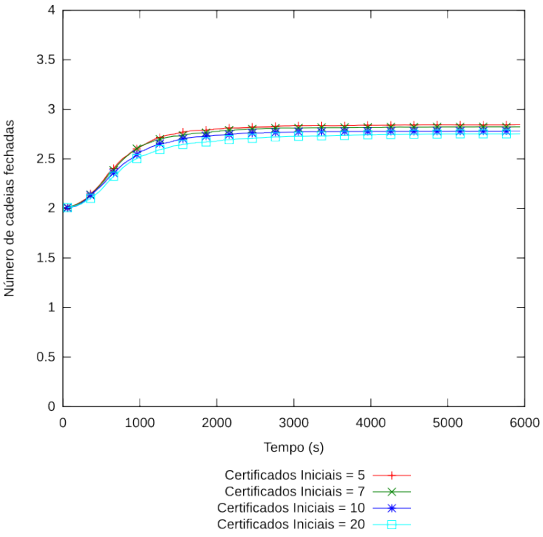

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

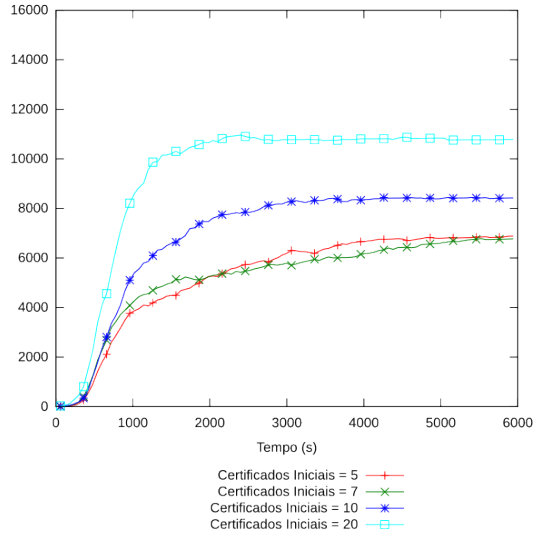



(c) Número de cadeias Abertas

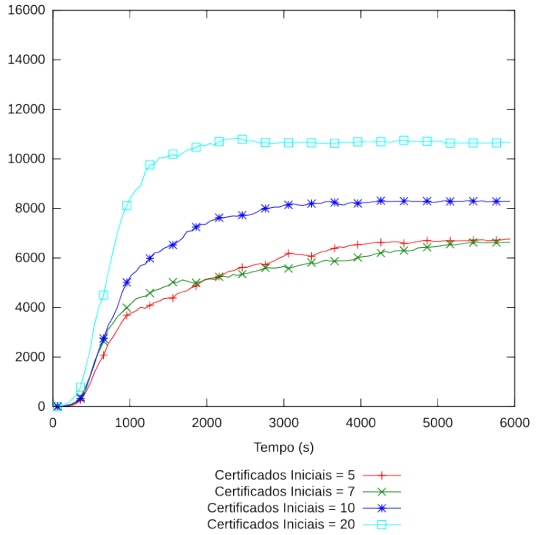



(d) Tamanho médio das cadeias

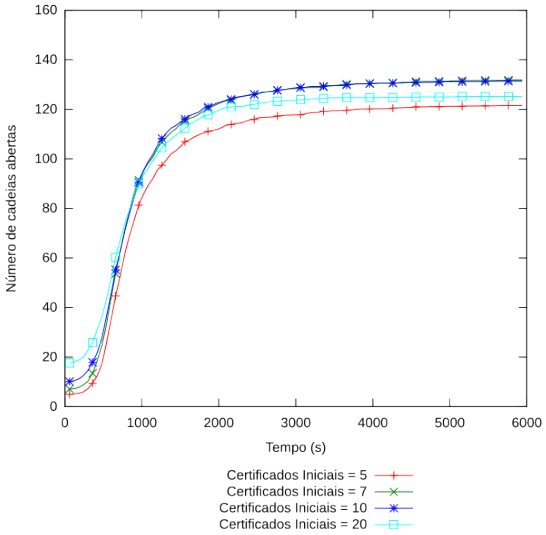
Figura D.61: Resultados para 100 nodos, $m = 20\%$ e $N_a = 10\%$



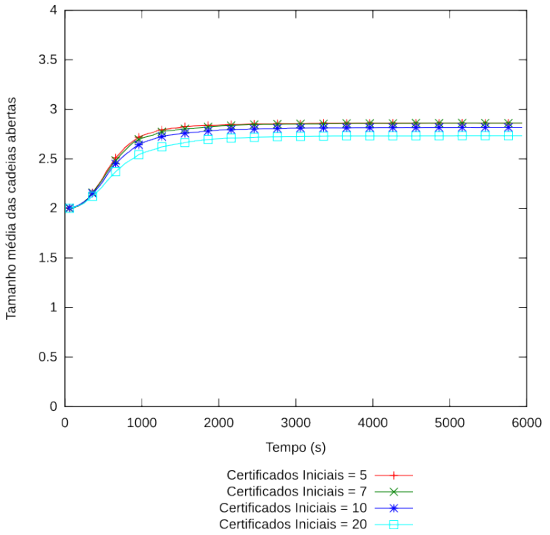

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



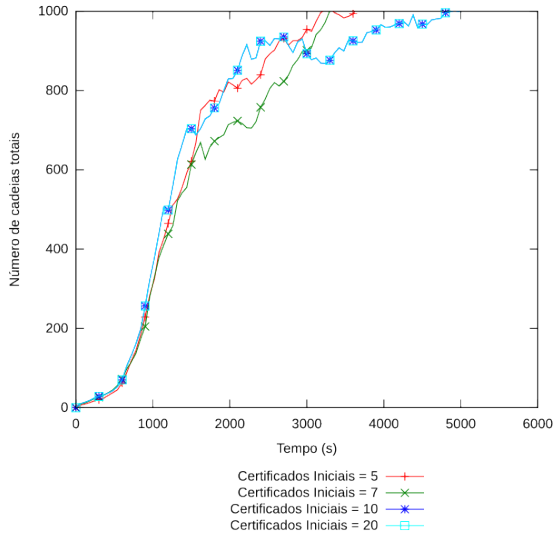

(c) Número de cadeias Abertas



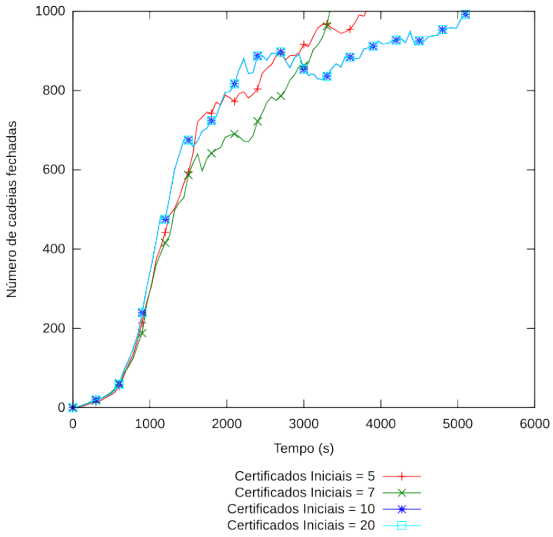

(d) Tamanho médio das cadeias

Figura D.62: Resultados para 150 nodos, $m = 20\%$ e $N_a = 10\%$

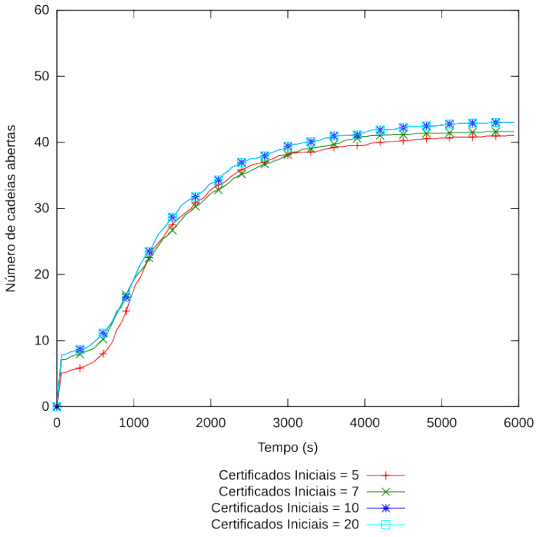
### D.5.5 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 25\%$



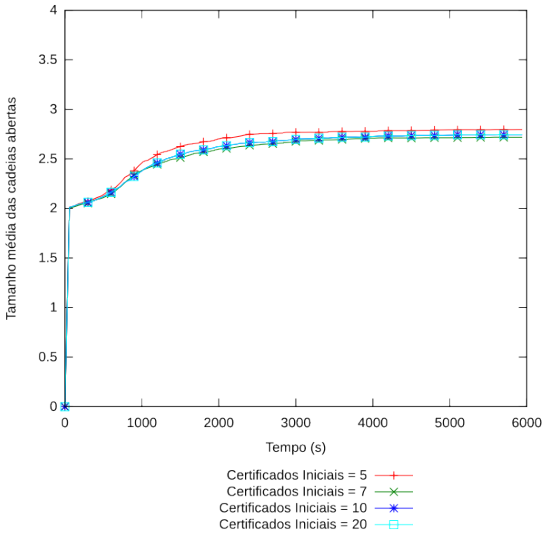

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

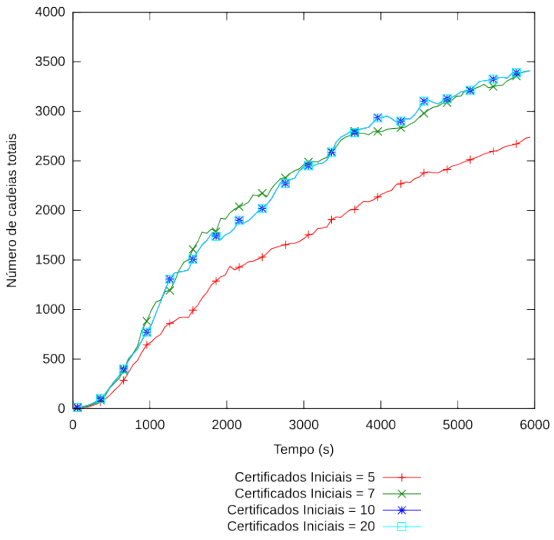



(c) Número de cadeias Abertas

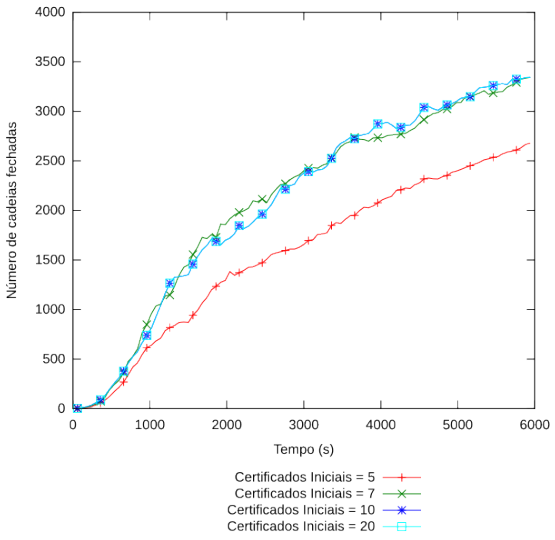



(d) Tamanho médio das cadeias

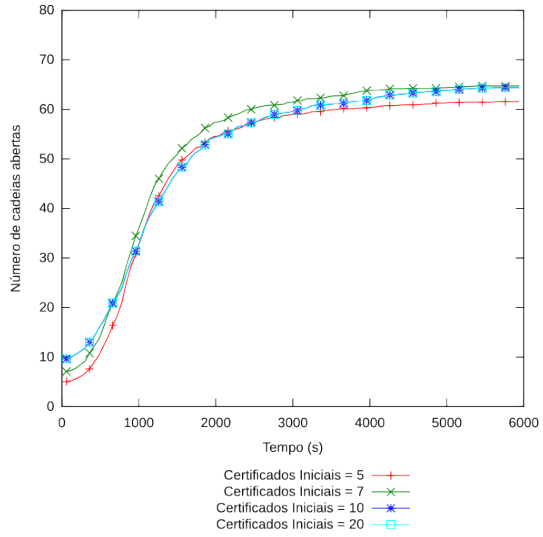
Figura D.63: Resultados para 50 nodos, $m = 20\%$ e $N_a = 25\%$



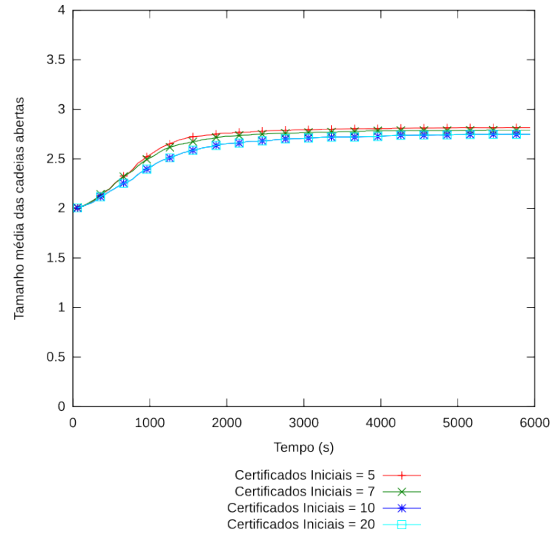

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

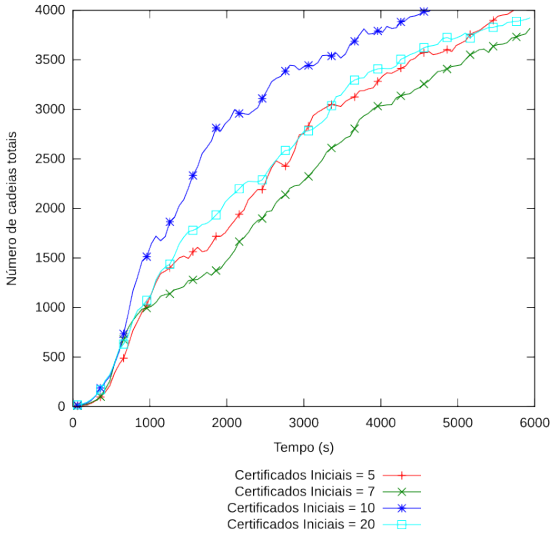



(c) Número de cadeias Abertas

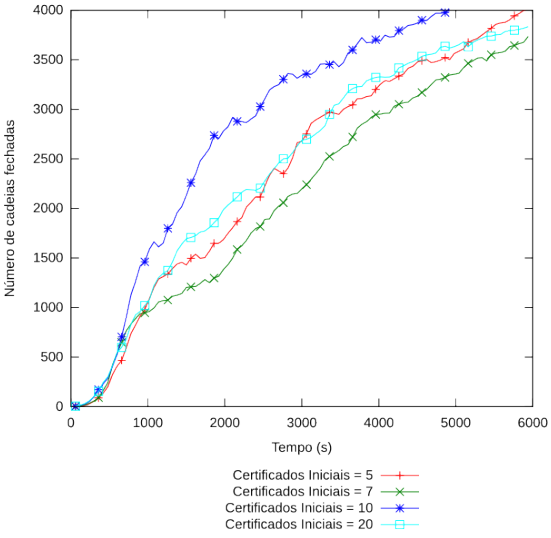



(d) Tamanho médio das cadeias

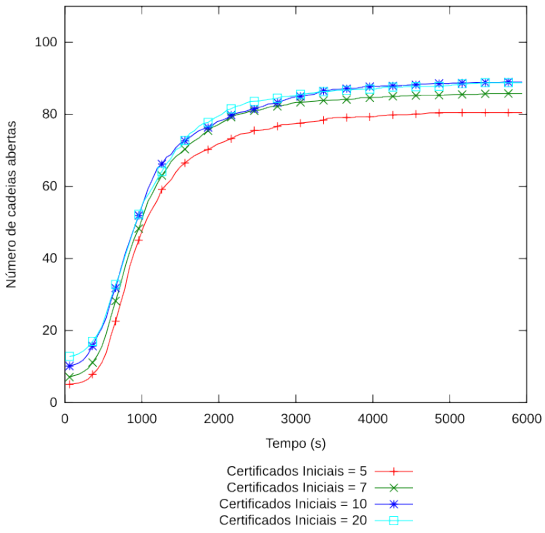
Figura D.64: Resultados para 75 nodos, $m = 20\%$ e $N_a = 25\%$



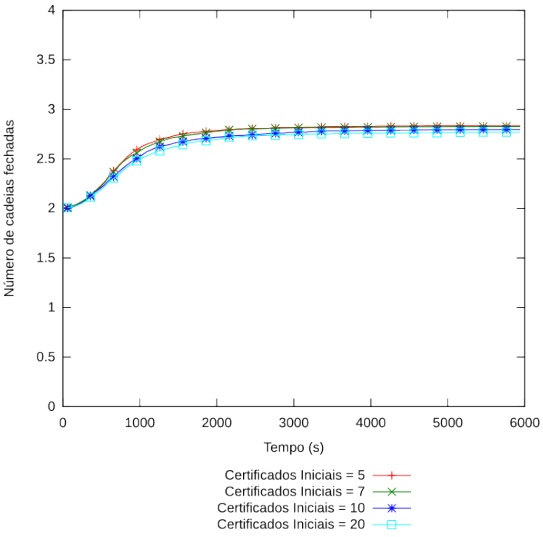

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

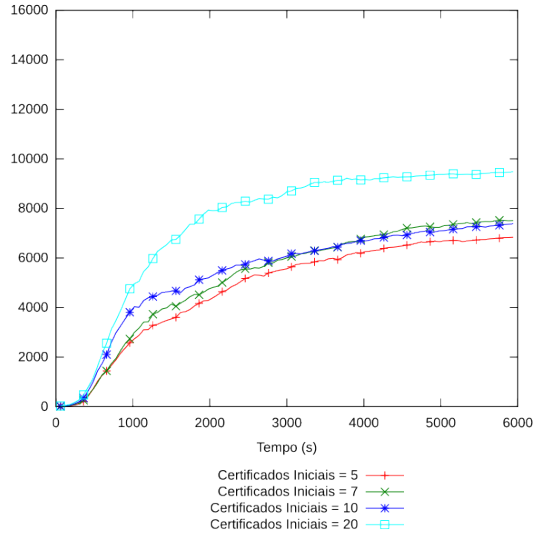



(c) Número de cadeias Abertas

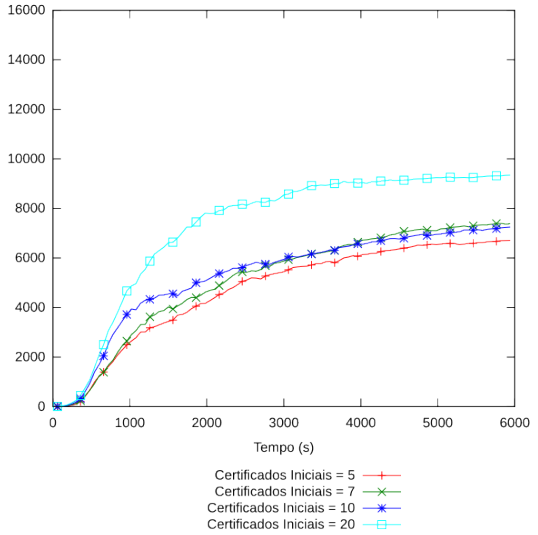



(d) Tamanho médio das cadeias

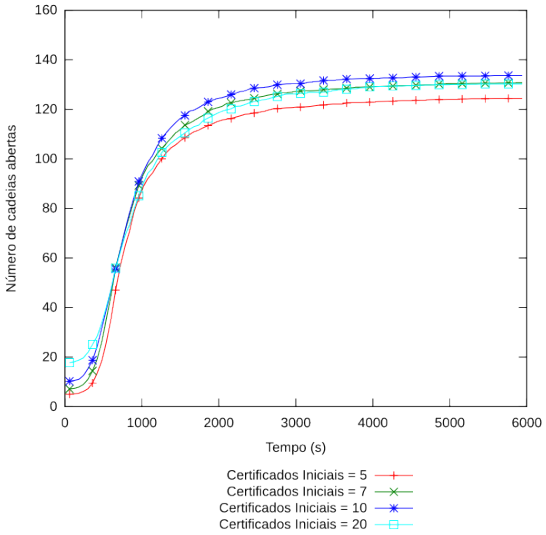
Figura D.65: Resultados para 100 nodos, $m = 20\%$ e $N_a = 25\%$



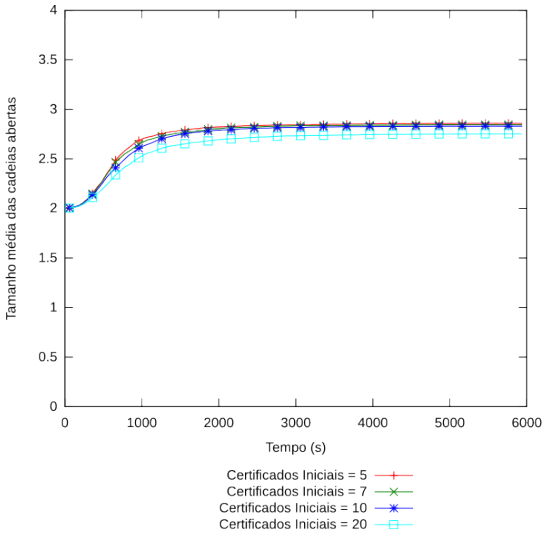

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



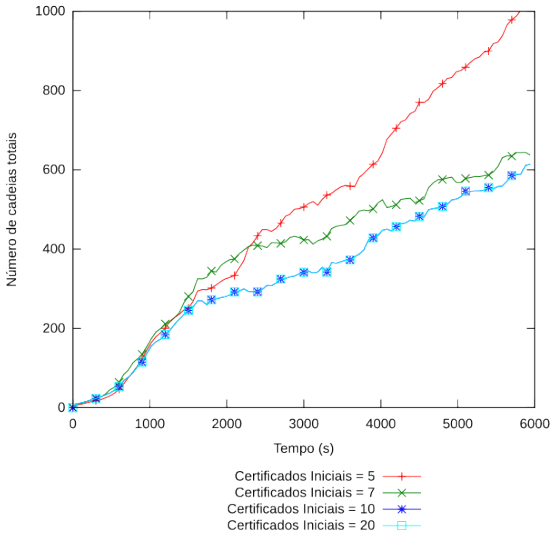

(c) Número de cadeias Abertas



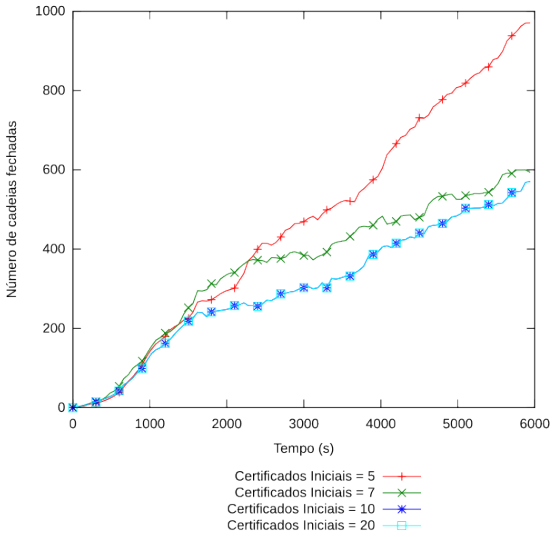

(d) Tamanho médio das cadeias

Figura D.66: Resultados para 150 nodos, $m = 20\%$ e $N_a = 25\%$

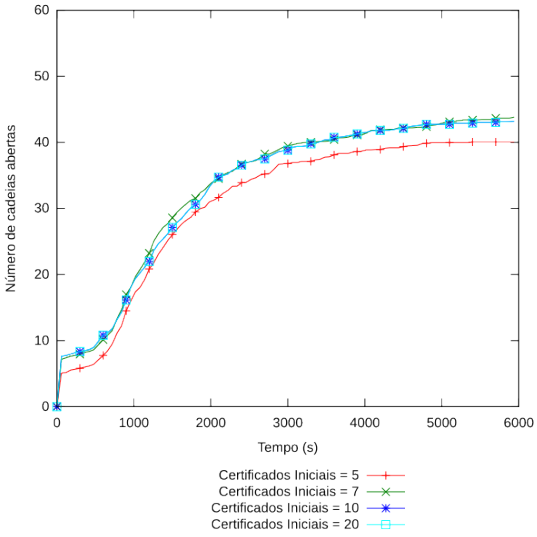
### D.5.6 Ataque de Falsificaçao com $m = 20\%$ e $N_a = 50\%$



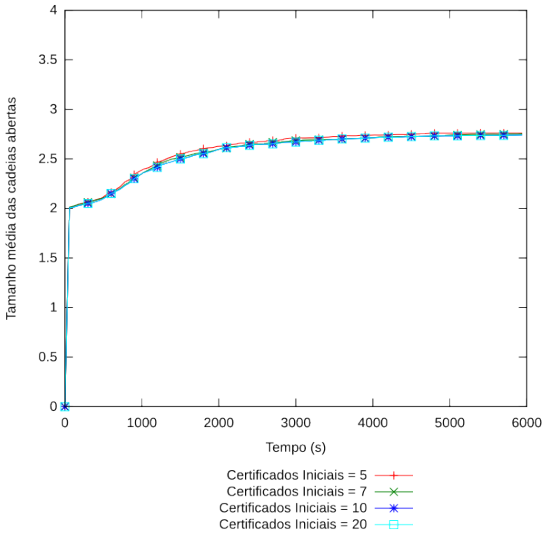

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

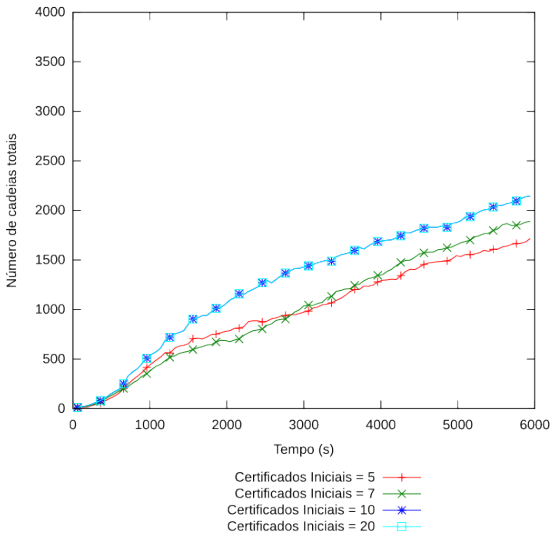



(c) Número de cadeias Abertas

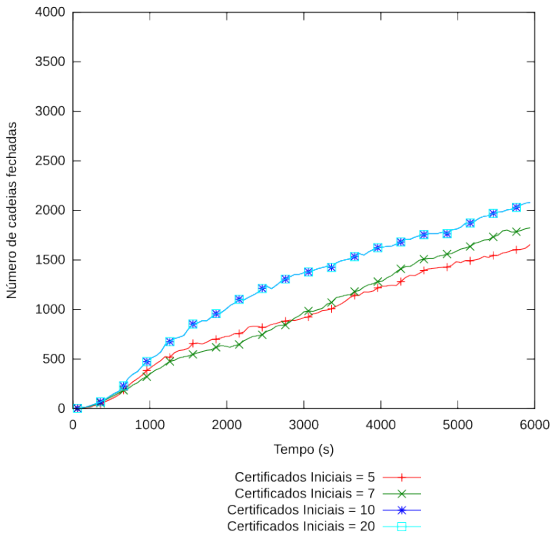



(d) Tamanho médio das cadeias

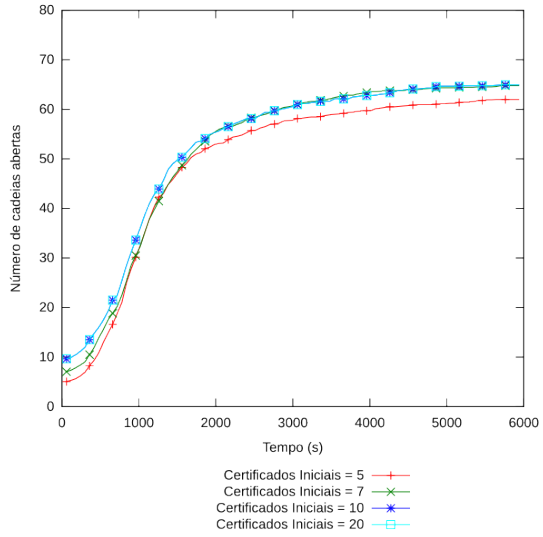
Figura D.67: Resultados para 50 nodos, $m = 20\%$ e $N_a = 50\%$



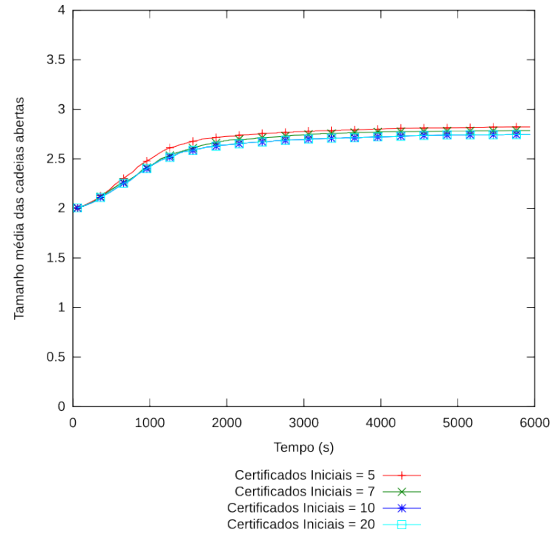

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

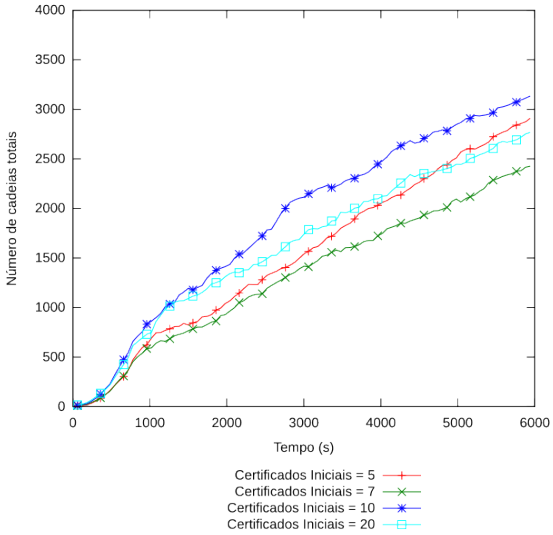



(c) Número de cadeias Abertas

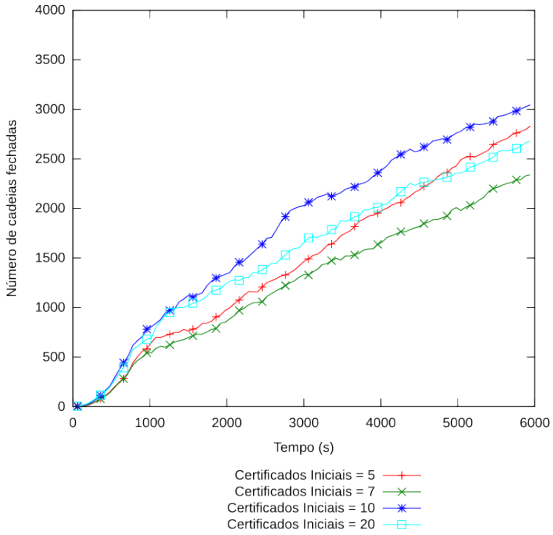



(d) Tamanho médio das cadeias

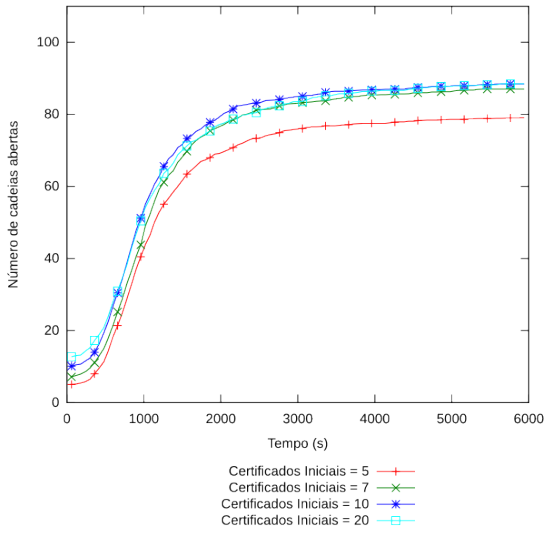
Figura D.68: Resultados para 75 nodos, $m = 20\%$ e $N_a = 50\%$



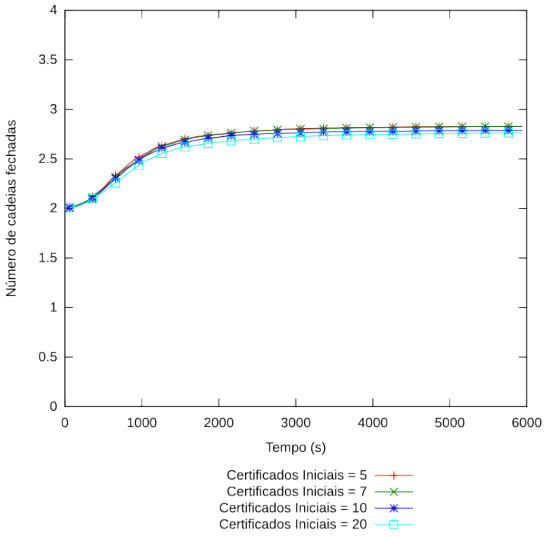

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

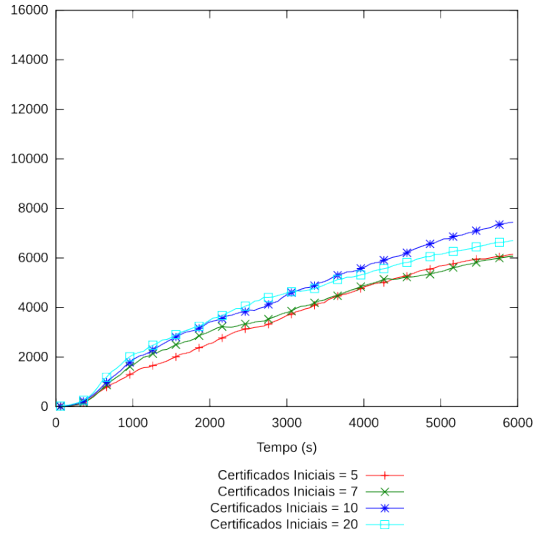



(c) Número de cadeias Abertas

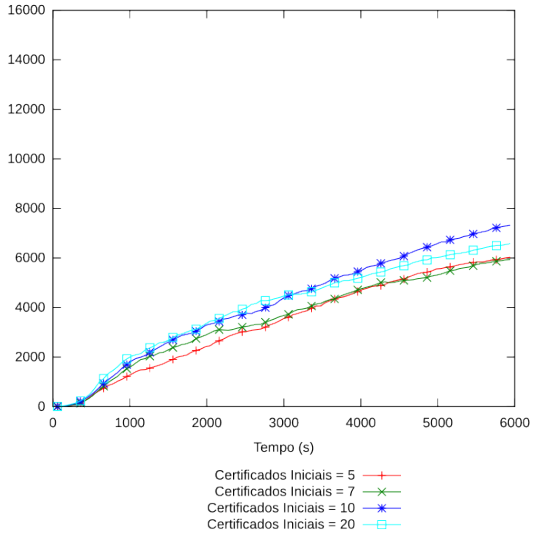



(d) Tamanho médio das cadeias

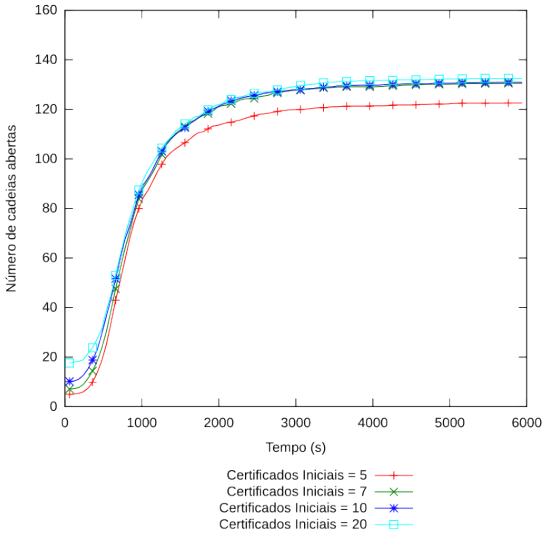
Figura D.69: Resultados para 100 nodos, $m = 20\%$ e $N_a = 50\%$



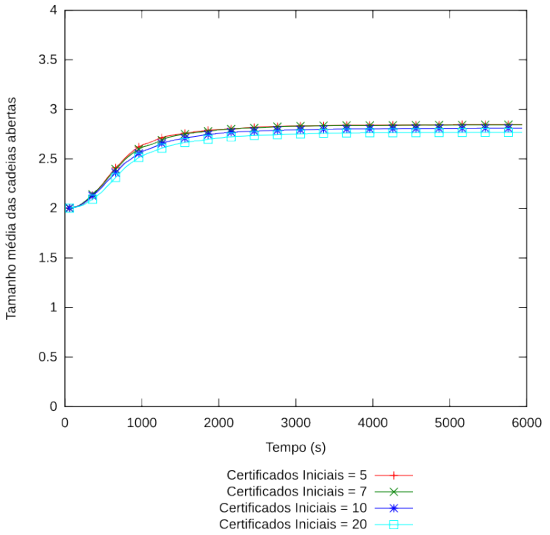

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



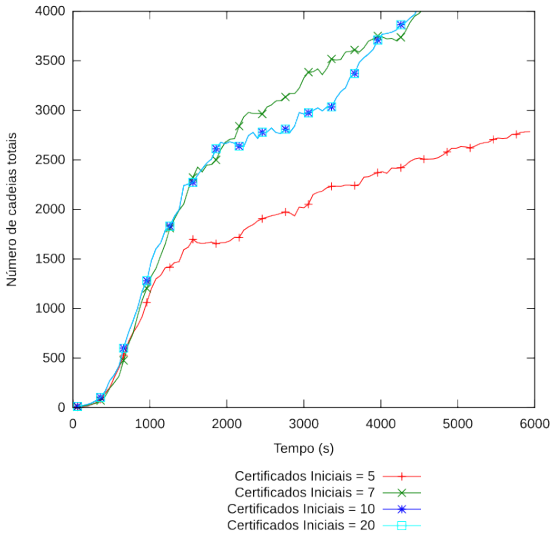

(c) Número de cadeias Abertas



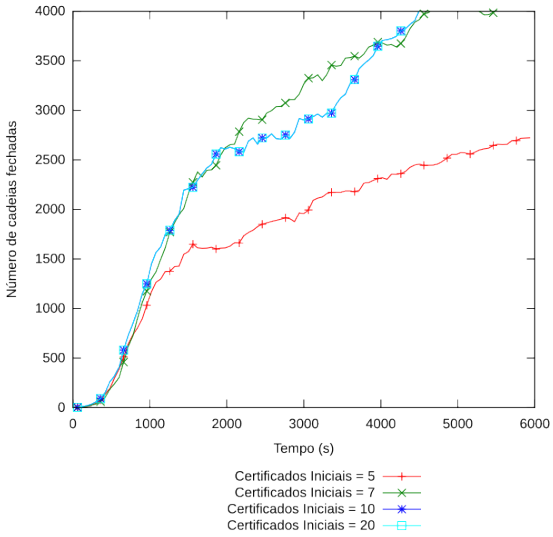

(d) Tamanho médio das cadeias

Figura D.70: Resultados para 150 nodos, $m = 20\%$ e $N_a = 50\%$

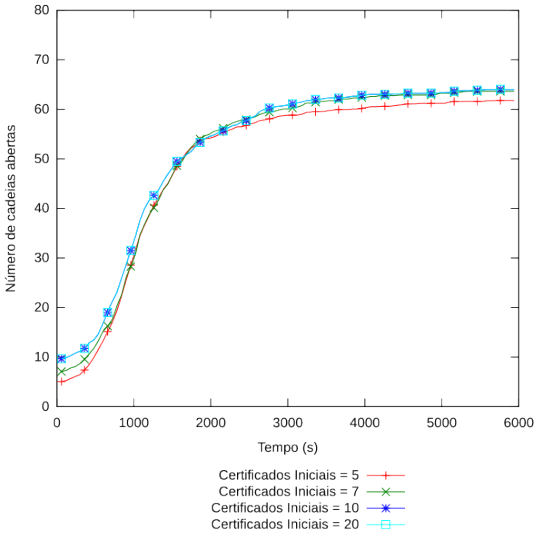
### D.5.7 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 10\%$



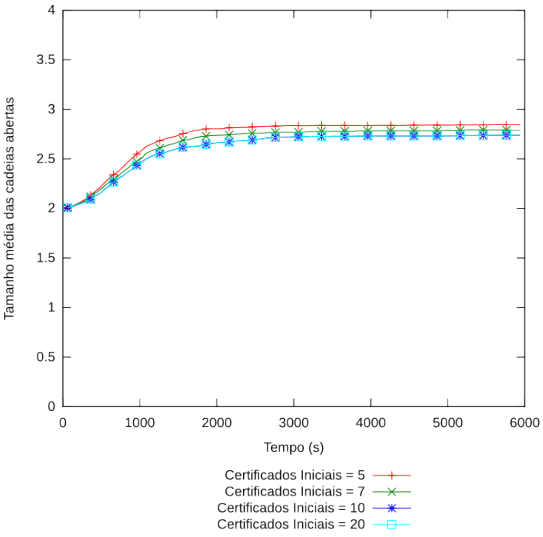

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

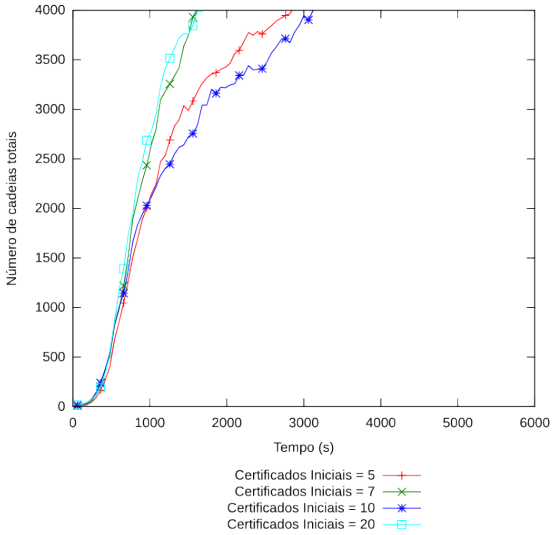



(c) Número de cadeias Abertas

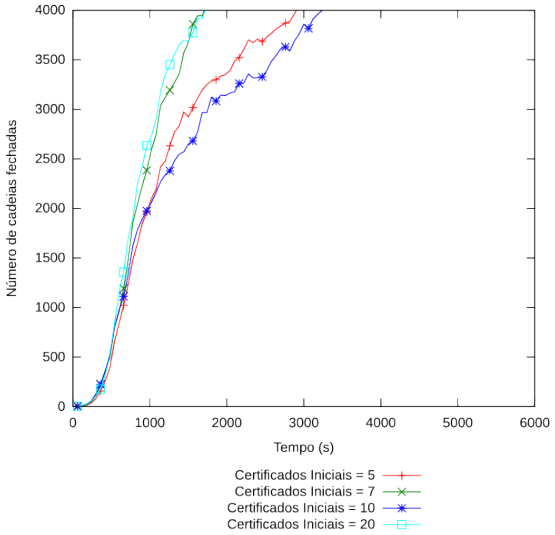



(d) Tamanho médio das cadeias

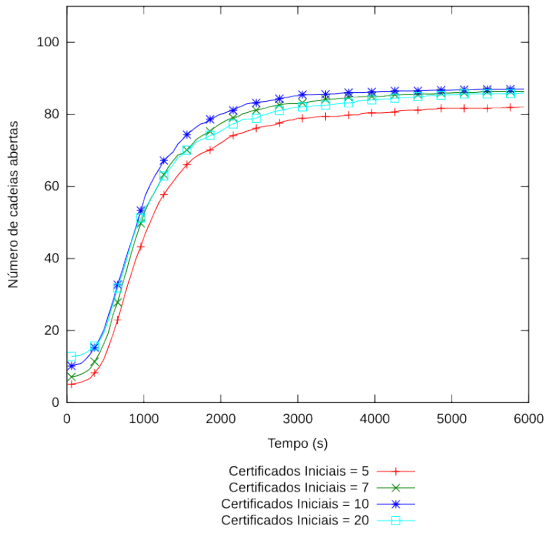
Figura D.71: Resultados para 75 nodos, $m = 50\%$ e $N_a = 10\%$



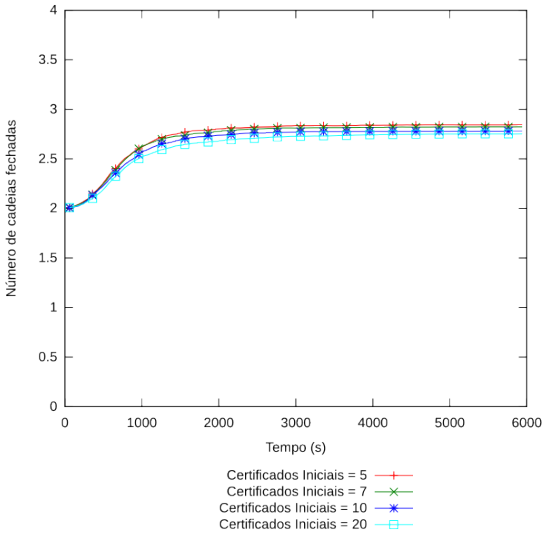

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



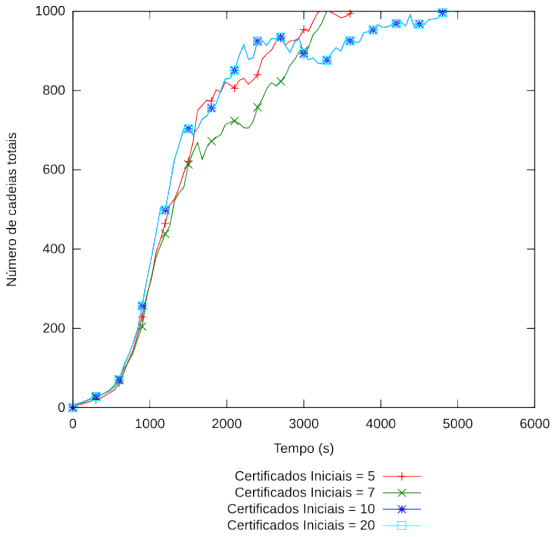

(c) Número de cadeias Abertas



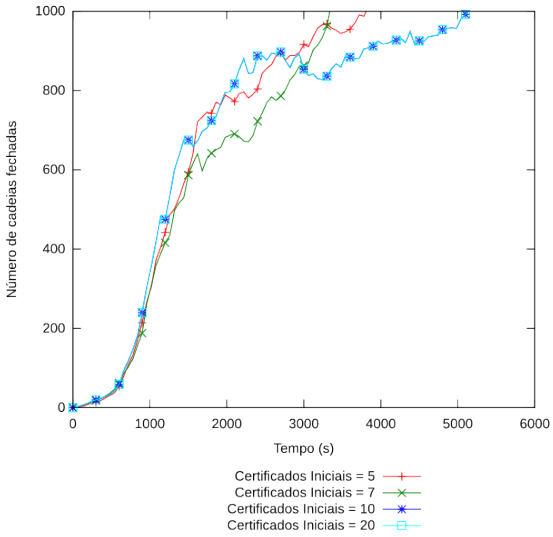

(d) Tamanho médio das cadeias

Figura D.72: Resultados para 100 nodos, $m = 50\%$ e $N_a = 10\%$

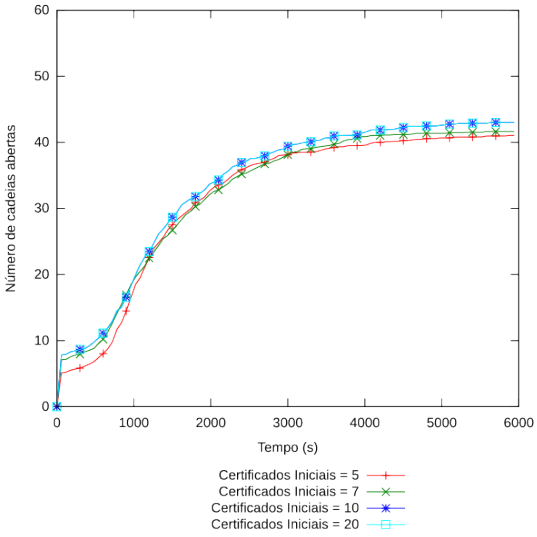
### D.5.8 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 25\%$



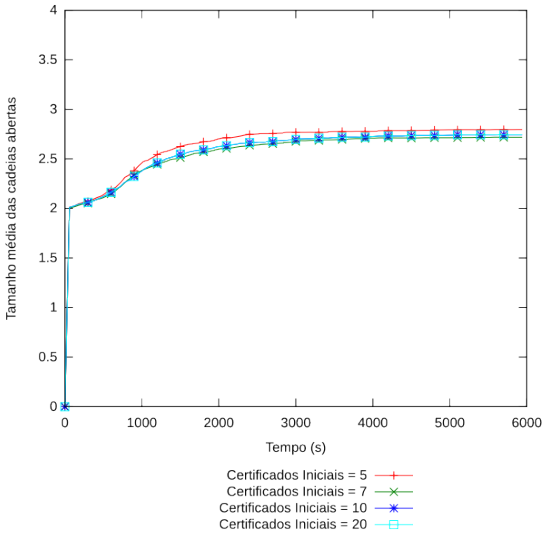

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

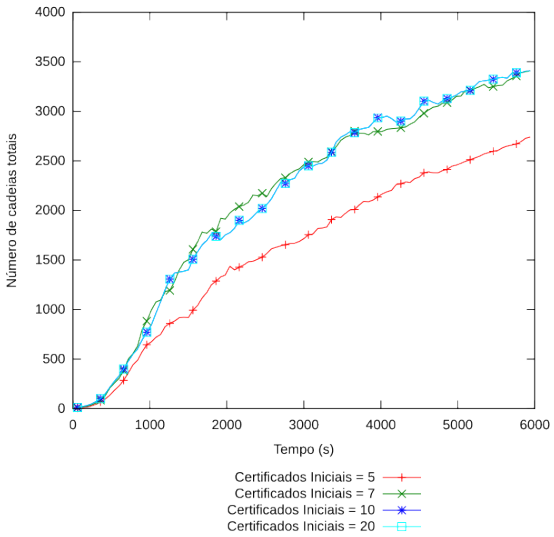



(c) Número de cadeias Abertas

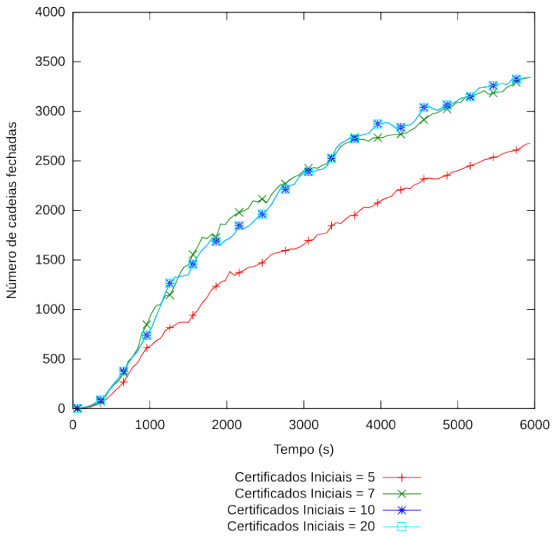



(d) Tamanho médio das cadeias

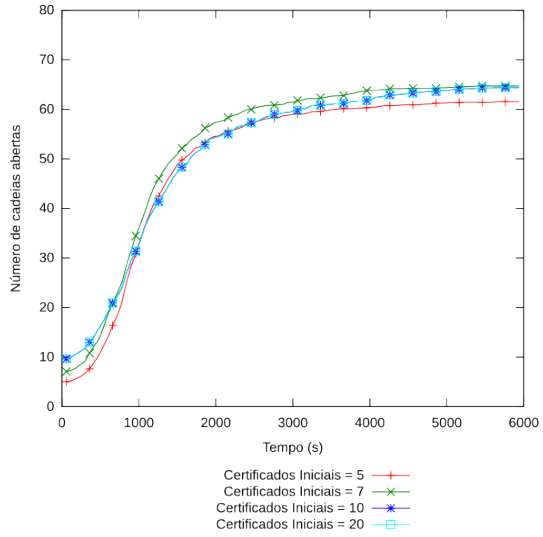
Figura D.73: Resultados para 50 nodos, $m = 50\%$ e $N_a = 25\%$



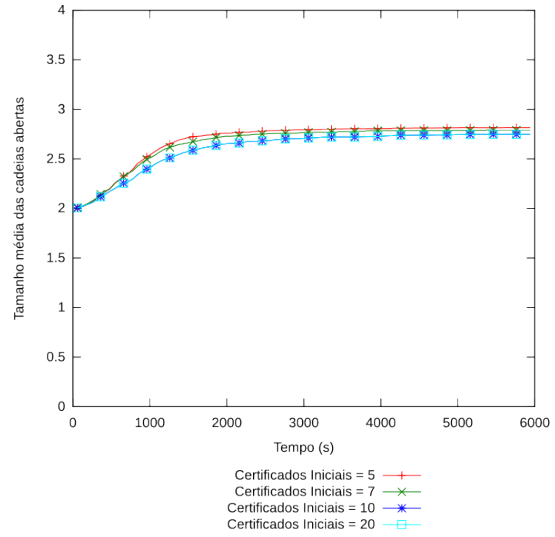

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

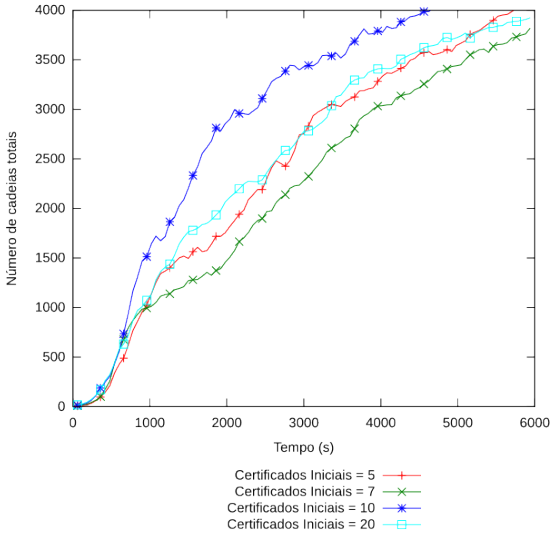



(c) Número de cadeias Abertas

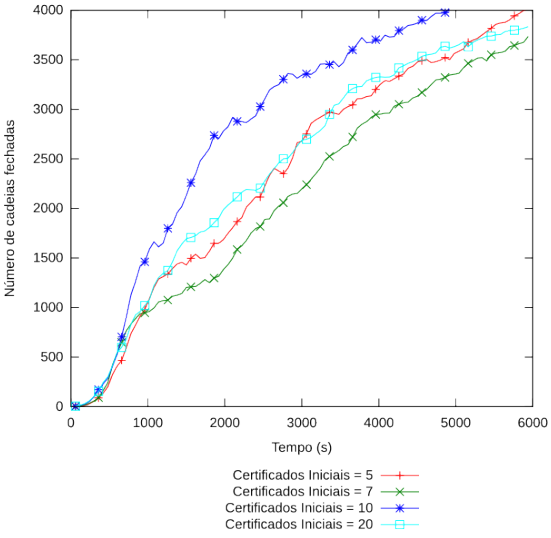



(d) Tamanho médio das cadeias

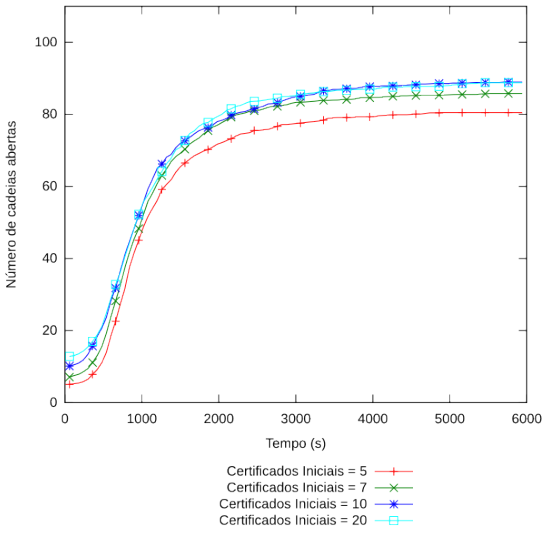
Figura D.74: Resultados para 75 nodos, $m = 50\%$ e $N_a = 25\%$



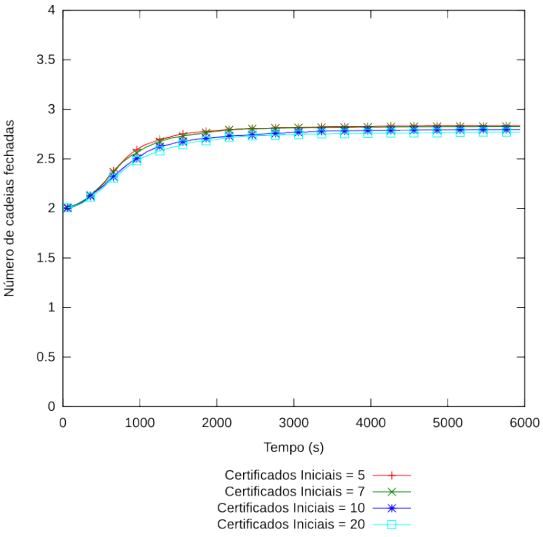

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

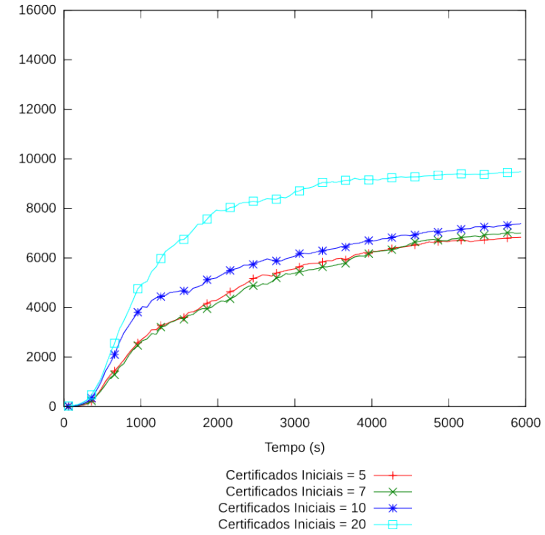



(c) Número de cadeias Abertas

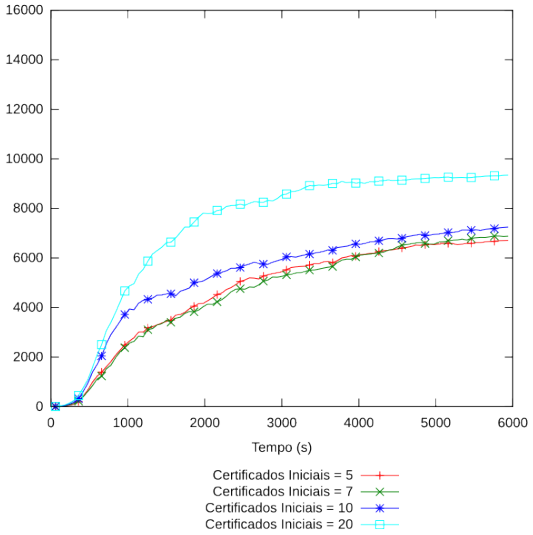



(d) Tamanho médio das cadeias

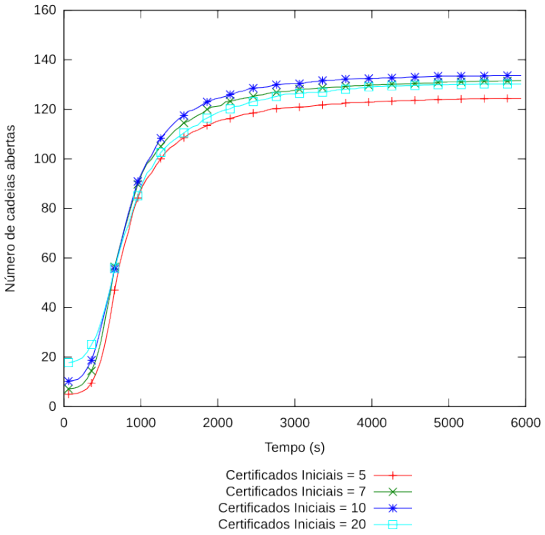
Figura D.75: Resultados para 100 nodos, $m = 50\%$ e $N_a = 25\%$



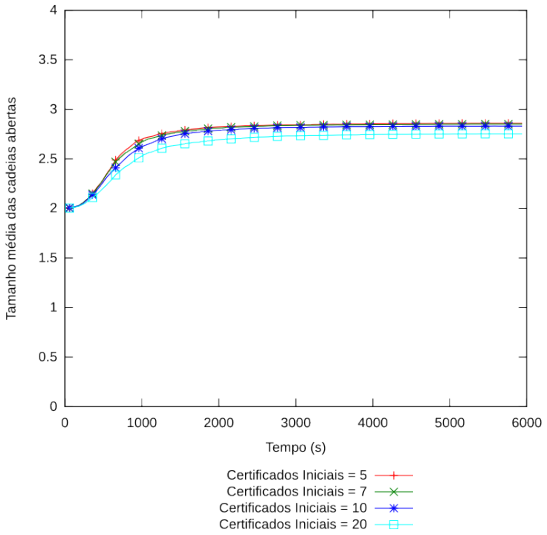

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas



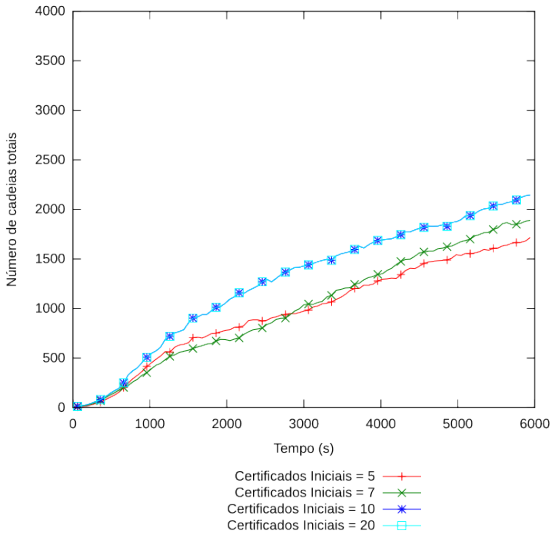

(c) Número de cadeias Abertas



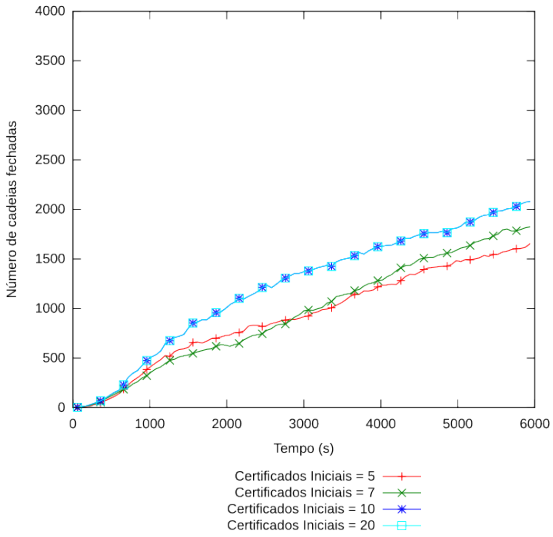

(d) Tamanho médio das cadeias

Figura D.76: Resultados para 150 nodos, $m = 50\%$ e $N_a = 25\%$

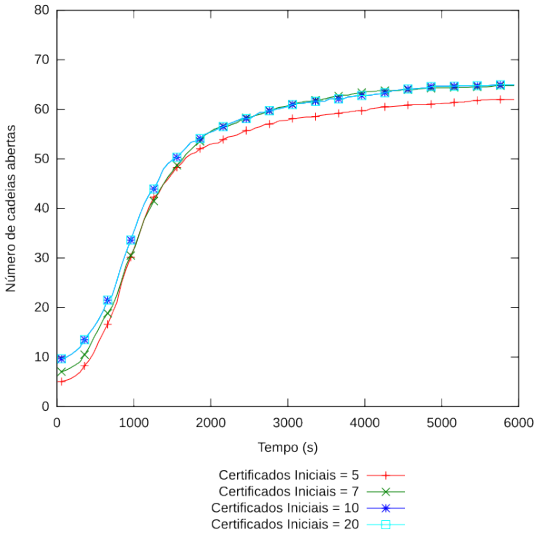
### D.5.9 Ataque de Falsificaçao com $m = 50\%$ e $N_a = 50\%$



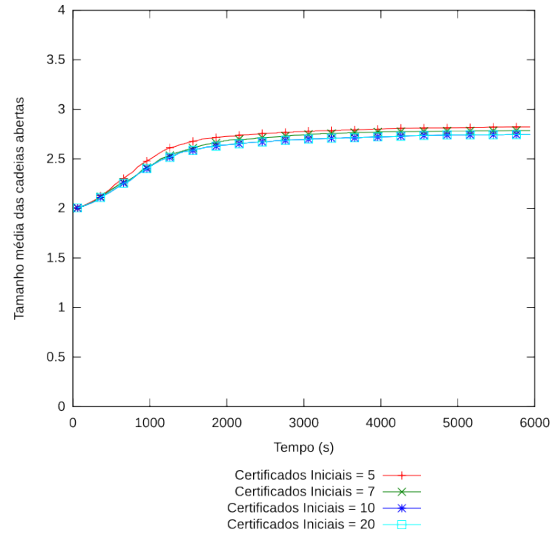

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas

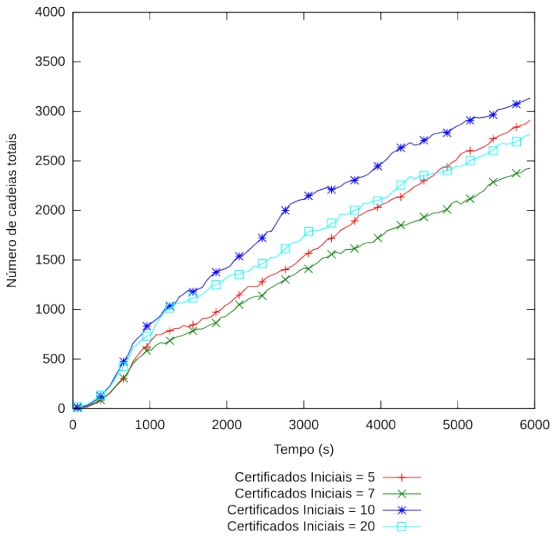



(c) Número de cadeias Abertas

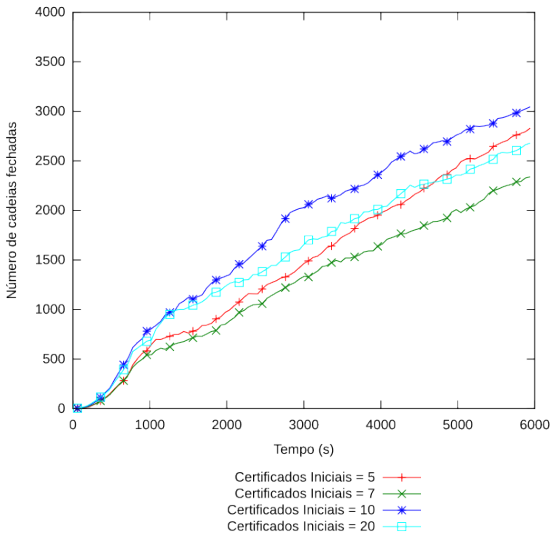



(d) Tamanho médio das cadeias

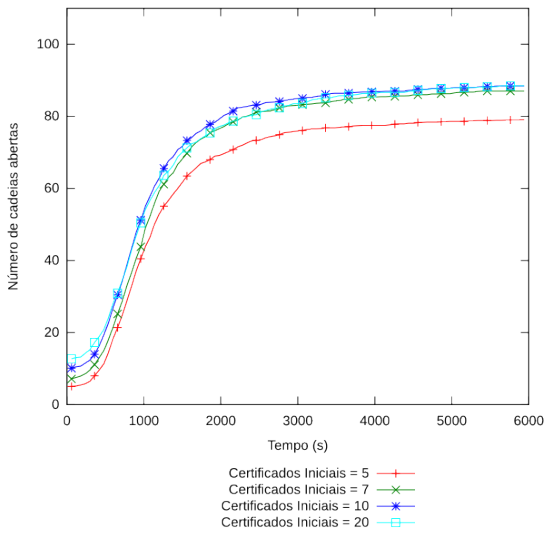
Figura D.77: Resultados para 75 nodos, $m = 50\%$ e $N_a = 50\%$



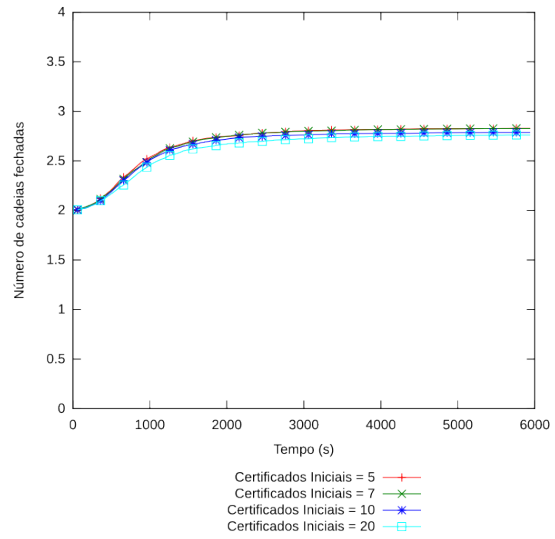

(a) Número de cadeias Totais




(b) Número de cadeias Fechadas




(c) Número de cadeias Abertas




(d) Tamanho médio das cadeias

Figura D.78: Resultados para 100 nodos, $m = 50\%$ e $N_a = 50\%$