CAIO RUAN NICHELE

MODELO DE CONFIANÇA PARA REDES AD HOC BASEADO EM TEORIA DE JOGOS

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.
Orientador: Prof. Dr. Luiz Carlos Pessoa Albini
Coorientador: Prof. Dr. André L. Vignatti

CURITIBA

2012

Nichele, Caio Ruan
Modelo de confiança para redes Ad Hoc baseado em teoria de jogos / Caio Ruan Nichele. - Curitiba, 2012.
60 f. : il., graf., tab.

Dissertação (Mestrado) – Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-Graduação em Informática.
Orientador: Luiz Carlos Pessoa Albini
Coorientador: André L. Vignatti

1. Teoria dos jogos. 2. Sistemas de comunicação móvel. 3. Redes de computadores. I. Albini, Luiz Carlos Pessoa. II. Vignatti, André L. III. Título.

CDD 004.65

AGRADECIMENTOS

Em qualquer lista de agradecimentos eventualmente pecamos pela ausência de uma ou outra pessoa que teve papel, mesmo que pequeno, na conclusão de um projeto como este. Mesmo assim, arrisco-me a relacionar os nomes de todos que me ajudaram nessa caminhada, e aqueles que me deram estrutura para chegar até aqui.

Aos meus pais Luiz Carlos e Terezinha, pela formação que me permitiram ter e pela educação. Aos meus irmãos pela parceria de uma vida inteira juntos, um ao lado do outro.

À minha esposa Tammy, pelo amor incondicional e incentivo em todos os momentos, essencial nessa trajetória.

Ao meu orientador Prof. Dr. Luiz Carlos Pessoa Albini, pela paciência e principalmente por todo o conhecimento passado. Foi fundamental em todos os momentos e decisões.

Ao meu coorientador Prof. Dr. André L. Vignatti, pelo conhecimento e ajuda na fundamentação teórica e modelagem do projeto.

Ao grupo de pesquisa em Redes Sem Fio e Redes Avançadas (NR2), pelo suporte e apoio em alguns momentos. Estendo esse agradecimento aos demais colegas e aos professores que fazem parte desse grupo.

Ao Programa de Pós-Graduação em Informática da UFPR, pela infraestrutura tornada disponível para o desenvolvimento deste e de outros trabalhos e ao seu pessoal técnico e administrativo, que, de uma forma ou de outra, acabou por participar deste projeto.

E por fim, a todos os meus amigos, colegas, familiares, pessoas próximas que, no dia-a-dia, me passaram confiança, força de vontade e amizade, tão importante nesta caminhada longa.

"Quem sabe concentrar-se numa coisa e insistir
nela como único objetivo, obtém, ao fim e ao cabo,
a capacidade de fazer qualquer coisa."
Mahatma Gandhi

"Nós somos aquilo que fazemos repetidamente.
Excelência, então, não é um modo de agir, mas um hábito."
Aristóteles

RESUMO

Confiança é tratada como uma explicação para a diferença entre o comportamento humano real e aquele que pode ser explicado pelo desejo individual para maximizar a própria utilidade. Em termos gerais, a confiança é uma atribuição à relação entre indivíduos ou grupos. Este trabalho propõe um modelo de confiança para Redes Ad Hoc baseado em Teoria de Jogos com o objetivo de responder a seguinte questão: Qual a confiança de um nó em outro? O modelo de confiança proposto, chamado TrustUm, calcula o valor de confiança através de informações trocadas entre os próprios nós e de testes realizados em seus vizinhos. O TrustUm está dividido em três etapas: monitoramento de vizinhos, troca de informações e cálculo de confiança. A troca de informações utiliza os conceitos de Teoria de Jogos, utilizando o Jogo do Ultimato, através do qual o comportamento dos nós da rede é analisado. Através dos resultados obtidos dessa análise é calculado um valor de confiança para cada nó da rede. Os resultados demostram que o modelo consegue inicialmente realizar as trocas de mensagens, otimizando o recebimento de informações confiáveis. Também o resultado aponta um valor de confiança embasado na ancianidade das informações trocadas e baseado nas informações dos próprios nós. Os resultados apontam uma diminuição de até 70% de informações maliciosas trocadas na rede, além de um cálculo de confiança mais preciso.

ABSTRACT

Trust is treated as an explanation for the difference between real and human behavior which can be explained by the desire to maximize their own utility. In general, trust is an assignment to the relationship between individuals or groups. This project proposes a trust model for ad hoc networks based on game theory. The proposal aims to answer the following question: How much a given node trusts another given node? The proposed trust model, called TrustUm calculates the trust value through information exchanged with the nodes themselves and with tests of its neighbors. To this end, some mathematical models were used to guide the calculation, and also by parameters set by the application that will use this model. The TrustUm is divided into three steps: monitoring neighbors, exchange of information and calculation of trust. The exchange of information uses the concepts of Game Theory, using the Ultimatum Game, where the behavior of the network nodes will be analyzed and the results obtained through this analysis will be calculated a trust value to each network node. The results show that the model can first select the message exchanges, optimizing the receipt of reliable information. Furthermore, the result indicates a trust value based on old information and based on information from the nodes. The results show a decrease of 30% to 70% of malicious information exchanged in the network, and a more precise trust value.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

CAPÍTULO 1

INTRODUÇÃO

Redes Ad Hoc Móveis (*Mobile Ad Hoc Networks* - MANETs) são redes sem infraestrutura, formadas por dispositivos móveis e com recursos limitados."Ad Hoc"é uma expressão do latim que significa "para este fim". Geralmente é utilizada para denominar situações específicas em que os problemas são resolvidos de maneira improvisada. Uma rede Ad Hoc permite que dispositivos móveis possam formar uma rede em áreas onde não há uma infraestrutura pré-definida de comunicações. A comunicação entre pares de dispositivos dentro da rede é feita diretamente entre os membros da rede. Pela falta de cobertura de sinal entre o par que deseja se conectar, podem ser necessários outros membros da rede para que a conexão seja realizada [42].

Cada membro da rede, denominado nó, é responsável pelo gerenciamento de suas informações e das informações encaminhadas por ele. Essa responsabilidade deriva de uma característica das redes Ad Hoc, a não existência de um ponto de acesso central que gerencie todas as informações. A ligação entre cada nó é independente das outras existentes na rede. Assim, se uma ligação falhar, seja por perda de conexão ou por falha do próprio dispositivo, as outras ligações podem continuar funcionando.

Assume-se então que todos os nós da rede se comportam de acordo com as especificações das aplicações e dos protocolos utilizados. Contudo, seja por restrições de recursos ou por má-fé, essa premissa nem sempre é verdadeira. Consequentemente, o comportamento dos nós pode não corresponder exatamente ao definido pela aplicação ou protocolo, prejudicando, ou em alguns casos inviabilizando, o funcionamento da rede. Deste modo, o correto funcionamento da rede exige alto consumo de recursos e por consequência, maior exposição à ataques, resultando na queda da eficiência da rede.

A utilização de Redes Ad Hoc [42] apresenta a vantagem de reorganização, quando uma rota encontra-se indisponível, i.e. a funcionalidade da rede pode ser mantida ape-

nas reorganizando rotas. Outra vantagem está na simplicidade, uma vez que não são necessários servidores ou pontos de acesso para gerenciar requisições de outros clientes. Ainda cabe ressaltar que uma rede inteira pode se mover de uma localidade a outra.

No entanto, as Redes Ad Hoc apresentam algumas desvantagens: a mobilidade gera constantes alterações de rotas na rede, isto afeta o processo de roteamento, deixando-o extremamente complicado. Outro problema está na cooperação dos nós em Redes Ad Hoc: a interação dos nós na rede, transmitindo mensagens de terceiros e participando dos processos de roteamento [9].

A cooperação implica confiança, uma vez que os nós cooperam de acordo com relações criadas entre eles. Confiança é um conceito global que abrange diversas definições [33], tratada como uma explicação para a diferença entre o comportamento humano real e aquele que pode ser explicado pelo desejo individual para maximizar a própria utilidade. Em termos gerais, a confiança é uma atribuição à relação entre indivíduos ou grupos.

Atentos as desvantagens apresentadas e a necessidade de um mecanismo a partir do qual os nós da rede possam inferir a confiabilidade dos demais nós, muitos pesquisadores desenvolveram estratégias e soluções na área de confiança. A Confiança é definida em várias áreas: psicologia [19][47], sociologia [1] e economia [25], entre outros. Através dela é possível destacar o comportamento de cada nó, desviando serviços e informações caso o nó não seja confiável. Diversas pesquisas surgiram propondo vários modelos de confiança para qualificar os nós da rede e também para incentivar a cooperação mútua. Um modelo de confiança é uma abstração conceitual de comportamentos a fim de criar mecanismos para a atribuição de um valor, atualizando e utilizando os níveis de confiança entre as entidades de um sistema distribuído. De maneira geral, o modelo de confiança permite o estabelecimento de relações entre as diferentes entidades para uma determinada ação [32].

Já existem modelos de confiança para Redes Ad Hoc [28] [34] [59] [60], porém limitam-se a estimar a confiança de nós vizinhos, isto é, a um salto de distância. Todavia não existem modelos que estimem a confiança de qualquer nó da rede, seja ele vizinho ou não.

1.1 Problema

Como não existe um ambiente ideal, onde todos os nós são confiáveis, é necessário qualificar os dispositivos móveis de acordo com seu comportamento e, por consequência, premiar os melhores e penalizar os nós maliciosos.

Considera-se que existem nós maliciosos na rede [33], isto é, nós cujas ações são inesperadas ou até incorretas. Tais nós precisam ser identificados e isolados pelos demais, a fim de manter o correto funcionamento da rede e estabelecer confiabilidade à rede. Todavia, qualquer ação tomada a fim de selecionar um nó deve ter algum embasamento lógico, ou matemático.

Existem modelos que estimam a confiança, porém se limitam a estimar a confiança dos nós vizinhos, isto é, a um salto de distância [10] [34] [59]. É necessário um mecanismo que faça mais que isso, estimando a confiança de todos os nós da rede. Esse mecanismo acarreta um novo desafio: estimar a confiança de nós desconhecidos.

1.2 Objetivos

Diante de todos os problemas mencionados anteriormente, é preciso criar um modelo de confiança que estime um valor de confiança dentre os nós da rede.

O primeiro objetivo é gerenciar o envio e recebimento das confianças atribuídas pelos vizinhos, selecionando quais informações serão enviadas e por consequência, quais informações serão recebidas. Para isso, serão utilizados conceitos de Teoria de Jogos e a aplicação do Jogo do Ultimato.

O segundo objetivo é utilizar as informações coletadas para calcular um valor de confiança para qualquer nó da rede no instante de tempo desejado, que reflita o comportamento de cada nó.

1.3 Organização do texto

Este trabalho está subdividido da seguinte forma: no Capítulo 2 há uma revisão teórica sobre Teoria de Jogos, contemplando o histórico, principais jogos utilizados e estudos

relacionados. No Capítulo 3 será apresentada a Teoria de Jogos aplicada a Redes Ad Hoc, mostrando principais estudos a cerca deste tema, bem como modelos de confiança baseados nesta teoria. No Capítulo 4 temos a apresentação do modelo proposto ao projeto, bem como a modelagem matemática da proposta. No Capítulo 5 temos as simulações e os resultados da proposta. O Capítulo 6 consiste na conclusão do projeto.

CAPÍTULO 2

TEORIA DE JOGOS

Teoria de Jogos é uma área da matemática aplicada que estuda situações estratégicas, modelando-as em situações específicas (jogos) da interação entre diversas "entidades" [51]. Um jogo consiste em um conjunto de jogadores, um conjunto de estratégias disponíveis [40] para cada jogador e *payoffs*, ou recompensas.

Teoria de jogos é aplicada em diversas áreas do conhecimento. Em 1944, Von Neumann e Morgenstern [54] forneceram um contexto econômico para a Teoria de Jogos. Eles estabeleceram um sistema de axiomas para uma ferramenta numérica, conhecida como a função de utilidade de Von Neumann Morgenstern, o que representou um grande avanço na construção da Teoria de Jogos sob risco e situações de incerteza. Os autores conseguiram estruturar matematicamente a noção de que cada indivíduo escolhe uma alternativa de acordo com certa probabilidade de acerto, de modo a maximizar o *payoff*.

Em 1951, John Nash adicionou alguns conceitos e resultados à teoria de jogos [26] [21], incluindo o conceito de Equilíbrio de Nash, no qual os jogos não são de um único vencedor e um único perdedor, é possível que os jogadores escolham suas estratégias a fim de chegarem a uma situação onde todos estão satisfeitos com a estratégia escolhida, ou seja, não vale a pena trocarem de estratégia. Segundo Nash [21], existe um ponto de equilíbrio que orienta os jogos, de maneira que o adversário não irá mudar de estratégia, e por consequência, o outro jogador também não. Nash, no entanto, assumiu que as decisões devem ser racionais. No entanto, nem sempre as decisões são estritamente matemáticas, e com isso, o ponto de equilíbrio pode não ser utilizado.

Um jogo pode ser visualizado de duas formas [36]: normal e extensiva. De maneira geral, cada forma explora um ponto de vista diferente do problema. A forma normal, geralmente visualizada como uma matriz explora jogadores, estratégias e ações. Geralmente é utilizada em jogos de dois jogadores. Desta forma, um jogador é disposto sobre

as linhas e outro sobre as colunas. Em cada linha ou coluna, são definidas estratégias para cada jogador. Em cada campo da matriz, são expressos os resultados, seguindo o formato de uma tupla, ou seja, (*resultado do jogador 1*, *resultado do jogador 2*). Desta forma, presume-se que os jogadores jogam de maneira simultânea, isto é, suas ações são realizadas sem a dependência de uma ação anterior. A forma extensiva é apresentada em formato de árvore no qual os vértices são ações, os nós são os jogadores e os nodos terminais são os resultados. Neste formato, a ordem das ações pode ser visualizada e, desta forma, é possível analisar comportamentos.

Como são várias as características e particularidades dos diversos jogos existentes e, explorando as principais similaridades entre eles, existem algumas propriedades [5] [15] [36] que padronizam os jogos conforme suas características. Abaixo segue um resumo das principais propriedades pelas quais os jogos podem ser classificados.

- **Cooperativo ou Não-cooperativo:** Um jogo é dito cooperativo [3] se os jogadores são capazes de manter relações com os demais jogadores. Um jogo é não-cooperativo quando os jogadores agem de maneira independente e suas ações tem o objetivo de maximizar o *payoff* individual.

- **Simultâneo ou Sequencial:** Um jogo é dito simultâneo quando é assumido que as estratégias são somente jogadas uma única vez e ao mesmo tempo (também chamado do jogo "one-shot"). Um jogo é sequencial quando existe uma ordem na execução das ações entre os jogadores.

- **Soma Zero ou Soma Diferente de Zero:** Um jogo é dito de soma zero quando o sucesso de um jogador implica na derrota do outro. Em um jogo com soma diferente de zero, não necessariamente há ganhadores ou perdedores e sim diferentes *payoffs* para cada resultado (solução) do jogo. É uma generalização do jogo de soma zero.

- **Informação Perfeita ou Informação Imperfeita**: Informação Perfeita é quando os jogadores têm conhecimento completo dos seus *payoffs* e dos *payoffs* dos outros jogadores, dependendo das estratégias utilizadas por todos. Informação imperfeita é quando não se tem todas as informações de *payoff* disponíveis (por exemplo, em

leilões um comprador não sabe quanto um item vale para outros compradores, desta forma, ele não sabe quanto serão os lances pelo item).

Existem diversos jogos estudados que serão apresentados a seguir, cada qual com suas particularidades, sendo possível avaliar a importância do tema para diferentes situações a serem exploradas. Como são vários estudos, será dado maior enfoque para os temas relacionados a modelos de confiança e ao jogo do ultimato, que são as bases deste projeto.

2.1 Dilema do Prisioneiro

O Dilema do Prisioneiro é um problema clássico em Teoria de Jogos. Foi criado pelos pesquisadores Merrill Flood e Melvin Dresher [45] e posteriormente publicado por Albert W. Tucker [45]. O jogo consiste em dois jogadores A e B suspeitos, que foram presos pela polícia, porém não há provas suficientes para condená-los. Ao separar os prisioneiros, a polícia oferece a ambos o mesmo acordo: se um dos prisioneiros confessa e testemunha contra o outro e esse outro permanece em silêncio, o que confessou sai livre enquanto o cúmplice silencioso cumpre 10 (dez) anos de sentença. Se ambos ficam em silêncio, a polícia só pode condená-los a 6 (seis) meses de cadeia. Se ambos traírem um ao outro, cada um leva 5 (cinco) anos de cadeia. Cada prisioneiro faz a sua decisão sem saber que decisão o outro vai tomar e nenhum tem certeza da decisão do outro.

Dado que nenhum dos jogadores pode ter a certeza da cooperação do outro, o resultado final será que ambos irão optar por denunciar o colega [45]. Desta forma, têm a certeza que terão, na pior das hipóteses, uma pena de 10 (dez) anos e, na melhor, sairão em liberdade. Já se cooperarem, terão uma pena bem menor. O principal ponto tratado neste jogo está no paradoxo criado através das opções de cada jogador. Por um lado, a melhor opção individual é trair. Contudo, levando-se em conta "ambos"os prisioneiros, a melhor opção é um cooperar com o outro. A utilização deste jogo implica na combinação de ações entre os jogadores. Ainda que um jogador não queira prejudicar o outro, seu benefício implica na punição do outro jogador.

Em 2007, os pesquisadores Matja Per e Attila Szolnoki [41] modelaram a diversidade

social na sociedade através do Jogo do Dilema do Prisioneiro. Através da localização física dos jogadores, eles determinaram uma melhor posição cuja energia seria mais bem utilizada por todos, através da cooperação. Dentro da pesquisa, ficou evidenciada a existência de grupos de preferência, cujas ações são determinadas por membros específicos, dito líderes. O resultado aponta que a diversidade social tem relação direta com a evolução da cooperação através de membros egoístas.

Em 2010, os pesquisadores Dirk Helbing e Sergi Lozano [22] estudaram as diferentes transições entre rotas de cooperação através do Jogo do Dilema do Prisioneiro. O estudo revelou que existem situações em que os indivíduos podem cooperar e se prejudicar, mas também podem ganhar. Segundo os autores, após classificar os casos de equilíbrio, é possível avaliar se uma transação pode interferir no estado do jogador.

2.2 Problema da Negociação

O problema da negociação ou da barganha foi criado pelo pesquisador John Nash, em 1950 [37] e consiste em uma negociação de dois jogadores, que exigem uma parte de algum bem (geralmente certa quantidade de dinheiro). Se o montante total solicitado pelos jogadores é menor que o disponível, ambos os jogadores têm o seu pedido aceito, se o seu pedido total é superior ao disponível, nenhum jogador recebe seu pedido [44].

Em 2008, os pesquisadores Zhang et. al. [58] propuseram uma estratégia de cooperação baseada no problema da negociação cujo proposito visa resolver duas questões: quando e como cooperar. Neste modelo, os autores identificaram que a cooperação necessita de banda, isto é, quanto mais afastados os membros da rede estiverem, maior será o tráfego da rede para que os nós possam cooperar. Os resultados da simulação demonstram que quando a cooperação ocorre os usuários que utilizam a estratégia se beneficiam, isto é, os nós mais distantes ganham maior banda para transmitir os seus dados.

Em 2011, os pesquisadores Omer Alper e Ron Nickel [2] realizaram um estudo sobre o problema de escolha de projetos militares propostos por organizações concorrentes. Tais projetos devem ser selecionados de acordo com uma avaliação baseada em riscos. Neste artigo, os autores propõem uma solução do problema da negociação como uma regra de

seleção, a qual consiste em uma noção de justiça, com custo baixo de decisão ao avaliador.

Em 2012, os pesquisadores Zhang et. al. [56] realizaram um estudo sobre alocação de energia e espectro entre os nós de origem e informações retransmitidas. Segundo os autores, tais métricas são necessárias para ampliar a capacidade de transmissão de forma eficiente. Foi utilizado o Problema da Negociação para resolver esse problema, onde os resultados mostram que a utilização deste jogo remete a uma boa troca entre complexidade computacional e eficiência do sistema.

2.3 Jogo Bayesiano

No jogo bayesiano [20], ou Jogo de Informação Incompleta, a função *payoff* de pelo menos um jogador não é de conhecimento comum, o que denota incerteza. Um exemplo de jogos de informação incompleta são os leilões fechados. Cada participante ("*Bidder*") sabe a sua própria avaliação do bem leiloado, mas não conhece as avaliações dos demais participantes. Os lances ("*Bids*") são submetidos em envelopes fechados, de modo que os movimentos são considerados simultâneos.

Em 2006, os pesquisadores Liu et. al. [29] propuseram um *framework* em Teoria de Jogos para analisar as interações de nós, visualizando as ações de ataque/defesa. Segundo eles, o jogo de informação incompleta é um modelo mais realista, uma vez que permite ao defensor manter sua estratégia de comportamento no decorrer do jogo. É sugerida uma nova abordagem na detecção de intrusão, baseado em jogo bayesiano, que promete um ganho energético ao defensor, melhorando o poder de detecção.

2.4 Jogo do Ditador

No jogo do ditador [4], o primeiro jogador, também chamado líder, determina uma alocação como um prêmio em dinheiro. O segundo jogador simplesmente recebe a doação que o primeiro jogador deixou. O papel do segundo jogador é inteiramente passivo e o resultado do líder depende apenas de suas próprias ações.

O jogo do Ditador dá ao líder a oportunidade de dividir os valores da maneira que

achar melhor [43], enquanto o receptor só pode aceitá-lo, sem jamais recusar. Desta forma, o receptor não tem escolha de rejeitar a oferta. A explicação para esse jogo recai sobre a reputação que o líder tenta construir. Quanto maior a oferta, maior a aceitação do líder pelo receptor.

Em 1994, os pesquisadores Bolton et. al. [6] estudaram as reações do Jogo do Ditador. Segundo eles, existem diversas variações nas quantias que o ditador reparte com o outro jogador, e elas estão associadas a contextos nos quais os ditadores estão inseridos.

Em 2009, os pesquisadores Rigdona et. al. [46] realizaram um estudo a cerca das características do Jogo do Ditador. Através de experimentos, os autores verificaram que a distância social entre os jogadores afeta a partilha do ditador, identificando possíveis causadores biológicos para este comportamento.

2.5 Jogo do Ultimato

O jogo do ultimato foi definido em 1982 por Guth et. al. [18]. O jogo funciona da seguinte forma: dois jogadores devem dividir uma determinada quantia entre eles. Um deles propõe uma divisão e o outro pode "aceitar" ou "rejeitar" esta proposta. Caso a resposta seja "aceitar", a quantia será repartida de acordo com o proposto, caso contrário, ambos não recebem nada. Este jogo se tornou o mais popular jogo para experimentos em economia, uma vez que consegue tratar de comportamentos aparentemente irracionais.

Eles iniciaram a pesquisa supondo que ambos os jogadores iriam ser racionais, teorizando sobre o que iria acontecer em uma negociação. Suponha que o jogador 1, ao propor uma divisão desigual com o jogador 2, considera óbvio que o jogador 2 irá aceitar sua divisão, uma vez que é melhor do que nada. Porém, se o jogador 2 conseguir visualizar que o valor é irrisório, pode considerar um insulto e rejeitar a oferta. Nesta ótica, alguns questionamentos [16] [52] foram realçados: Qual o valor mínimo pelo qual o jogador 2 aceitaria? Qual a melhor estratégia?

A Tabela 2.1 contem a classificação dos jogos apresentados acima:

Jogo	Sequencial	Soma Zero	Informação Perfeita
Dilema do Prisioneiro	Não	Não	Não
Problema da Negociação	Não	Não	Não
Jogo Bayesiano	Não	Sim	Não
Jogo do Ditador	-	Sim	-
Jogo do Ultimato	Sim	Não	Sim

Tabela 2.1: Tabela de classificação de jogos.

2.6 Modelagem do Jogo do Ultimato

O Jogo do Ultimato consiste na divisão de algum dinheiro (ex. 1 real) entre dois jogadores i e j seguindo algumas regras específicas:

(i) O jogador i propõe uma divisão ao jogador j. O jogador i determina quanto quer ficar pra si, e quanto quer dar ao jogador j;

(ii) O jogador j tem a opção de aceitar ou rejeitar a divisão;

(iii) Se o jogador j aceitar, cada pessoa recebe a divisão proposta. Caso o jogador j rejeite a oferta, ambos não recebem nada.

Ainda, assume-se que os jogadores i e j se comunicam através de mensagens instantâneas de diferentes locais. Também é analisado se os jogadores já tiveram algum contato anterior e se terão contato futuro. Suponha inicialmente que ambos os jogadores desejam maximizar a divisão. No caso de j, qualquer valor ofertado por i é lucro, visto que se j rejeitar ele recebe 0 (zero). No caso de i, quanto menos ele ofertar, maior o lucro. Este é um caso que teoricamente funciona, mas na prática não reflete o comportamento humano. Num estudo realizado em 1982, Guth, Schmittberger e Schwarze [18] propuseram diversos experimentos estudando o comportamento dos jogadores no Jogo do Ultimato. Eles identificaram que o jogador que faz a oferta tende a oferecer uma pequena parte da quantia. Todavia, muitos dos jogadores que tem a opção de aceitar ou rejeitar a oferta a rejeitaram, por considerarem ofertas baixas. Ainda, existe um limite entre aceitar e rejeitar uma oferta, todavia o risco de perder tudo deve ser considerado.

2.7 Aplicação do Jogo do Ultimato

Existem diversos estudos [12] [13] [17] [31] [38] [48] [49] [50] [52] [55] que utilizam o Jogo do Ultimato como embasamento teórico, a fim de modelar as ações de acordo com as movimentações caracterizadas no jogo do ultimato. Alguns foram selecionados e serão explicados em seguida.

2.7.1 *Analyzing the Payoff of a Heterogeneous Population in the Ultimatum Game*

Em 2007, os pesquisadores Roberto da Silva e Gustavo Adolfo Kellerman publicaram um artigo [49] onde demonstraram como formulações matemáticas podem ser empregadas para retratar as relações entre populações heterogêneas e o jogo do ultimato. Segundo os autores, é possível estabelecer uma estratégia dominante para um conjunto de parâmetros de entrada. Segundo eles, as estratégias são descritas como distribuições de probabilidade. Simulações foram realizadas utilizando o conceito de etapas, no qual em cada etapa o jogador joga apenas uma vez. Após um elevado número de etapas, é possível criar um diagrama e assim dizer qual a melhor estratégia.

O objetivo dos autores era mostrar analiticamente um procedimento para calcular os momentos de pagamento dos jogadores na população heterogênea de acordo com uma determinada estratégia.

Neste estudo, a análise dos *payoffs* consiste de um cenário cuja população utilizada é heterogênea. Desta forma, as características da população são consideradas e não interferem no cálculo. Ainda, a utilização de etapas é usada na escolha do nós que são analisados.

2.7.2 *Expectations and outcome: The role of Proposer features in the Ultimatum Game*

Nas tomadas de decisões sociais, os indivíduos fazem escolhas através de um contexto interativo e suas decisões podem ser influenciadas por informações que recebem sobre as

características do outro jogador.

Em 2011, os pesquisadores Marchetti et. al. [31] relacionaram o impacto das decisões e as informações de características entre os jogadores através do Jogo do Ultimato. Estes resultados confirmaram a relevância dos efeitos da decisão devido a tendências sociais de aceitar ou rejeitar uma oferta.

Este estudo simulou variações de comportamento baseadas em aspectos físicos, psicológicos e sociais. Tais variações competem com ofertas justas e injustas, resultando num banco de dados interessante, com tendências e porcentagens características para cada grupo avaliado. Sua utilização dentro do projeto está a cargo da aplicação, caso seja interessante envolver outras características aos nós.

2.7.3 *Individual and Group Behavior in the Ultimatum Game: Are Groups More "Rational" Players?*

Em 1998, os pesquisadores Gary Bornstein e Ilan Yaniv [8] apresentaram um estudo onde duas experiências são realizadas confrontando o Jogo do Ultimato desempenhado por um indivíduo e por grupos de três jogadores. Nas decisões individuais, os membros realizavam o jogo da forma original, sem qualquer tipo de variação. Nas decisões em grupo, os membros do grupo realizam uma breve discussão entre os jogadores, e definiam uma proposta de divisão para o grupo.

A mesma coisa acontece quando o grupo é o destinatário e tem que aceitar ou rejeitar uma oferta. Caso a oferta seja aceita pelo grupo, cada jogador receberá o valor dividido, isto é, o valor será três vezes menor que a divisão individual. Em ambos os experimentos, os grupos ofereceram menos do que o indivíduo. Mas, como indicado pela baixa taxa de rejeição em ambos os tratamentos, os grupos foram também dispostos a aceitar menos.

2.8 Teoria de Jogos aplicada a Redes Ad Hoc

Redes Ad Hoc têm diversos problemas devido as desvantagens apresentadas anteriormente. Tais problemas remetem à soluções muitas vezes não triviais e algumas dependem

de ferramentas auxiliares. Teoria de Jogos vem sendo aplicada a redes Ad Hoc, uma vez que contêm conceitos específicos que podem serem incorporados em diversos momentos do funcionamento delas. Existem diversos estudos [11] [14] [23] [27] [35] [53] que retratam a utilização de Teoria de Jogos aplicada a redes Ad Hoc.

Em 2002, Pietro Michiardi e Refik Molv [35] desenvolveram uma análise da segurança de Redes Ad Hoc utilizando Teoria de Jogos. Através do jogo do Dilema do Prisioneiro foi possível modelar as interações entre nós da rede e focar qual estratégia cada nó irá utilizar durante a operação. Uma vez que a análise esteja concluída, é possível estabelecer critérios de segurança que tenham impacto no comportamento da rede.

Em 2003, Félegyházi et. al. [11] avaliaram os benefícios da cooperação entre os nós. Segundo o artigo, existe um momento em que um mecanismo de incentivo pode ser utilizado de modo a estimular a cooperação. Ainda, foi proposto um modelo em Teoria de Jogos baseado no jogo bayesiano que identifica as condições nas quais as estratégias de cooperação podem ser utilizadas, proporcionando um equilíbrio na rede.

Em 2003, Crowcroft et. al. [53] propuseram um modelo de incentivo à cooperação em Redes Ad Hoc baseado no jogo bayesiano. Segundo o estudo, políticas de incentivo podem ser integradas dentro de uma operação de Redes Ad Hoc, uma vez que os resultados demostram que qualquer participante está em desvantagem. Porém em um determinado espaço de tempo, existe uma compensação tendendo ao equilíbrio. Segundo eles, toda cooperação demanda uma maior utilização de memória, energia e processamento, todavia se todos cooperarem, um nó qualquer utilizará de recursos de outros nós.

Em 2007, Komathy e Narayanasamy [27] relacionaram problemas em Redes Ad Hoc referentes a auto organização da rede. Neste estudo, os autores introduzem uma estratégia para troca de informações através da escolha de vizinhos para cooperar baseada em Teoria de Jogos utilizando o jogo do ditador modificado. Através deste modelo, é possível selecionar o melhor vizinho, baseado em cooperação.

Em 2009, Juan José Jaramillo e R. Srikant [23] realizaram um estudo sobre mecanismos de reputação para incentivar a cooperação em redes Ad Hoc. Eles verificaram que a necessidade de um mecanismo de incentivo decorre do problema de colisão de pacotes,

que acaba por atrapalhar a cooperação entre os nós. Utilizando Teoria de Jogos, foi proposto um mecanismo chamado DARWIN, cuja função é evitar situações de retaliação após um nó ser considerado malicioso, e restaurar a cooperação rapidamente.

O modelo proposto no capítulo 4 tem alguns diferenciais em relação aos estudos mencionados acima. Primeiro, por não tratar a cooperação impondo políticas de incentivo. Neste modelo, a cooperação tem benefício mútuo, quanto maior for a cooperação, maior a troca de informações e por consequência, maior o recebimento de informações confiáveis. Segundo, porque a utilização de Teoria de Jogos está associada diretamente as informações trocadas pelos nós, isto é, a avaliação varia de acordo com o comportamento da rede.

CAPÍTULO 3

MODELOS DE CONFIANÇA

Modelos de confiança tem a função de moldar analiticamente comportamentos de um determinado conjunto de objetos ou pessoas, a fim de expor padrões de confiança e qualificá-los através de um número, cuja tradução significa o grau de confiança [24]. Confiança pode ser calculada de diversas formas e por diversas definições específicas [28] [34] [59] [60]. A seguir têm-se as propostas envolvendo Modelos de Confiança em Redes Ad Hoc.

3.1 *Robust cooperative trust establishment for MANETs*

Em 2006, Zouridaki et. al. [60] realizaram um estudo sobre confiança em Redes Ad Hoc. Eles propuseram um esquema de cálculo de confiança através da cooperação dos nós. No esquema proposto, cada nó determina a confiabilidade dos outros nós com respeito ao encaminhamento de pacotes confiáveis através de duas formas: da comparação de informações de observações diretas da camada MAC e da informação de confiança obtida através de recomendações de outros nós.

O esquema funciona da seguinte forma: num primeiro momento, cada nó monitora seus vizinhos, verificando se eles encaminham os pacotes corretamente, isto é, sem modificá-los ou extraviá-los. Após um determinado número de pacotes, tem-se uma razão que indica a confiança para aquele nó. Tendo esses valores calculados, é necessário compartilhar essas informações com os demais nós. Essas informações são enviadas através de mensagens ACK de pacotes de dados. Por fim tem-se a função de opinião, que tem como objetivo repassar a confiança solicitada, com uma avaliação previamente estabelecida.

Nesta proposta, a utilização da métrica para a avaliação de confiança pode ser facilmente distorcida se a rede apresentar muitas colisões de pacotes. Também, as informações são enviadas dentro de mensagens ACK e isso também pode ser alterado, comprometendo todo o estudo. Todavia a comparação de mensagens diretamente na camada MAC trás

grande confiabilidade ao valor de confiança gerado.

3.2 *An Objective Trust Management Framework for Mobile Ad Hoc Networks*

Em 2007, Li et. al. [28] realizaram um estudo sobre cooperação em Redes Ad Hoc. Segundo eles, cada nó não deve funcionar apenas para si, mas deve cooperar com os outros nós, todavia alguns nós podem se comportar mal, cada um com seus interesses individuais. Eles propuseram um modelo de confiança para Redes Ad Hoc, no qual um nó avalia a confiabilidade de outro nó de forma objetiva com base não apenas em observações diretas, mas com informações de outros nós.

O esquema proposto está dividido em quatro etapas. No início, os nós são responsáveis pelo monitoramento de seus vizinhos através do mecanismo *watchdog* [57]. Na segunda etapa, cada nó é responsável por enviar as informações coletadas para todos os demais. A terceira etapa consiste no cálculo da confiança. Através das informações coletadas, cada nó forma uma opinião sobre os demais nós. A quarta e última etapa consiste na determinação da confiabilidade através da combinação dos valores obtidos anteriormente.

Neste estudo, o mecanismo *watchdog*, por mais eficiente que seja, consome uma quantidade grande de energia para funcionar. Tratando-se de Redes Ad Hoc, onde uma das principais limitações é o consumo de energia, tal mecanismo se torna um problema e não uma solução.

3.3 *A game theoretic trust model for on-line distributed evolution of cooperation in MANETs*

Em 2010, Mejia et. al. [34] apresentaram um artigo sobre cooperação em MANETs. Neste artigo, eles propõem um modelo de confiança baseado no Jogo do Dilema do Prisioneiro que usa um algoritmo bioinspirado em bactérias para simular o comportamento dos nós. O modelo é totalmente distribuído, alcança valores de cooperação em uma pequena fração de tempo em comparação com algoritmos centralizados e adapta-se eficazmente às mudanças

relacionadas ao ambiente das bactérias.

É possível visualizar neste artigo diferentes formas de quantificar confiança. Conquanto exista um modelo que também quantifica confiança, as etapas para se chegar ao valor desejado são bem diferentes, onde são utilizadas as informações dos próprios nós para calcular a confiança. Todavia, o estudo explora o comportamento dos nós baseado na similaridade do comportamento biológico de bactérias, o que distoa da aplicabilidade real.

3.4 *Exploiting Trust Relations for Nash Equilibrium Efficiency in Ad Hoc Networks*

Neste artigo, apresentado em 2011 [59], é feita uma abordagem a fim de estabelecer relações de confiança entre os nós para orientar tomadas de decisão e, com isso, incentivar a cooperação entre os nós, promovendo melhor benefício global. Para isso, primeiramente é feita uma análise da Teoria de Jogos para a eficiência do estabelecimento de confiança para melhorar a cooperação entre os nós e, desta forma, formular um novo jogo quel atende a Centralidade de Bonacich [7]. Ainda, o modelo se reserva a calcular a confiança somente dos vizinhos e sem mobilidade.

A modelagem das relações de confiança segue como uma rede ponderada de confiança, onde os *payoffs* são responsáveis pelas alterações de confianças entre os nós. Também, o autor mostra uma relação entre o Equilíbrio de Nash e a Centralidade de Bonacich. Com isso, propõem a introdução de recursos diferenciados para nós de acordo com sua centralidade.

O modelo proposto no capítulo 4 tem algumas vantagens se comparados aos estudos vistos acima. Inicialmente, o modelo proposto não utiliza mensagens de roteamento, uma vez que cada roteamento tem suas particularidades, todavia utiliza mensagens *Broadcast*. Também, o modelo está subdividido em três partes, uma utilizando alguma avaliação já existente, uma utilizando Teoria de Jogos e outra utilizando cálculos matemáticos. Desta forma é possível analisar o comportamento de um nó nas três etapas simultaneamente.

O modelo proposto analisa o comportamento dos nós baseado em relações sociais, mais próximas dos cenários reais.

CAPÍTULO 4

TRUSTUM: UM NOVO MODELO DE CONFIANÇA

Denominado TrustUm (*TRUST with ultimatUM game*), o novo modelo de confiança engloba várias questões relacionadas à interação de diversos nós dentro de uma rede. Nesse modelo, supõem-se a existência de nós maliciosos. Tal suposição se faz necessária visto que, em um ambiente livre de nós maliciosos, todos os nós se confiam, e com isso, nenhuma anomalia acontece.

Uma vez que existem nós maliciosos é necessário identificá-los. Uma forma para isto é avaliar seu funcionamento através de uma parametrização específica, a qual irá transformar seu comportamento em um número real, que será o valor de confiança entre o nó que avalia e o nó avaliado. É possível que um nó seja malicioso para alguns nós e para outros não. Esse fato é facilmente constatado quando existem grupos de preferências, isto é, um nó prefere trocar informações com determinados nós diante de algum motivo específico, excluindo os demais. A mudança de estado de um nó, malicioso para confiável ou vice versa, está prevista neste modelo.

O TrustUm está subdividido em três etapas subsequentes, que são independentes, mas complementares. A primeira etapa consiste no monitoramento dos vizinhos. Nesta etapa é possível avaliar o comportamento dos nós vizinhos, isto é, a um pulo de distância. A segunda etapa consiste na troca de informações entre os nós da rede alimentando uma estrutura chamada de Matriz de Confiança. A terceira etapa consiste no cálculo da confiança através dos dados armazenados na Matriz de Confiança. É possível visualizar as relações entre as etapas na Figura 4.1.

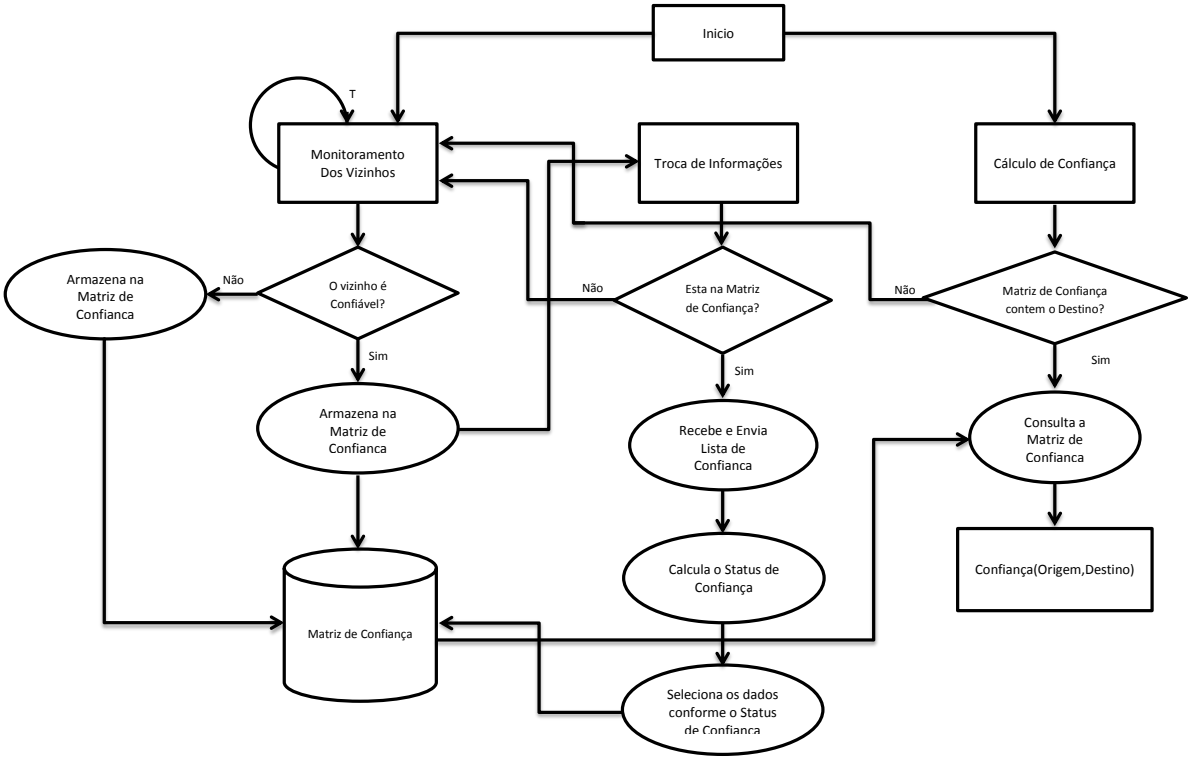


Figura 4.1: Diagrama do Proposta

O trustUm utiliza as seguintes estruturas:

- **Matriz de Confiança:** Guarda todas as informações obtidas e serve de banco de dados para o cálculo da confiança. São armazenadas as confianças juntamente com o instante de tempo em que tais informações foram recebidas.
- **Lista de Confiança:** É utilizada no envio das informações entre os nós da rede. A lista contém apenas as informações obtidas pelo nó que está enviando as informações. Estas informações são obtidas através dos testes realizados nos nós vizinhos. Não são enviados os instantes de tempos em que as informações foram obtidas.

4.1 Monitoramento dos Vizinhos

O monitoramento dos vizinhos é a primeira etapa do modelo. Esta etapa consiste na avaliação do comportamento de um nó a um salto de distância, isto é, entre vizinhos. A avaliação consiste somente em duas classificações: confiável e malicioso.

Existem diversas propostas na literatura que abordam cálculo de confiança a um salto de distância [10] [34] [59] [60]. O TrustUm pode utilizar qualquer destas abordagens, neste trabalho consideramos esta: *A game theoretic trust model for on-line distributed evolution of cooperation in MANETs* [34]. As informações obtidas nesta etapa são guardadas dentro da Matriz de Confiança.

4.2 Troca de Informações

Nesta etapa os nós atualizam sua Matriz de Confiança através de informações de seus vizinhos. As trocas de informações utilizam mensagens de *broadcast* controlado, limitado a um pulo de distância, sem necessidade de roteamento ou qualquer gerenciamento.

Ao utilizar mensagens de *broadcast*, a convergência da rede depende da taxa de mobilidade dos nós da rede, uma vez que esse tipo de mensagem somente alcança um raio de cobertura física pré-definido. As informações enviadas são as confianças obtidas através do monitoramento dos vizinhos.

Cada nó recebe solicitações de troca de informações em seu raio de cobertura. Ao receber uma solicitação, o nó verifica se a origem é maliciosa. Caso não disponha dessa informação, o nó irá realizar a etapa do Monitoramento dos Vizinhos para avaliar esse nó. Caso disponha, o receptor analisa o status de confiança do emissor para atualizar as informações.

O Status de Confiança é baseado no Jogo do Ultimato e depende de informações já coletadas da Matriz de Confiança. Através dele é possível comparar comportamentos dentre dois nós avaliados e atribuir um percentual analítico. Este valor determina a quantidade de informação compartilhada, conforme os conceitos aplicados em Teoria de Jogos.

O Status de Confiança favorece os nós mais confiáveis. Quanto maior for o valor do Status de Confiança, maior a concentração de informações confiáveis que o nó irá deter, portanto o nó receberá um número menor de informações do nó com menor Status de Confiança. Na Teoria de Jogos, o Status de Confiança é associado ao *payoff*. Posteriormente na Sessão 4.4 será apresentado o cálculo do Status de Confiança.

Após a definição do Status de Confiança a troca é realizada. Os valores são copiados da Lista de Confiança para a Matriz de Confiança e o tempo do recebimento é adicionado a cada informação.

4.3 Cálculo da Confiança

O cálculo de confiança proposto pode ser realizado a qualquer momento, todavia o valor apresentado pode variar. A variação existe devido a diversas variáveis que compõem o cálculo.

Todas as variáveis do cálculo serão explicadas pontualmente a seguir:

- **Informação de i sobre j (s_i^j):** As informações de i sobre j estão guardadas na Matriz de Confiança. Esses valores são obtidos nas trocas de informações e no monitoramento de vizinhos. São através dessas informações que o valor de confiança será calculado.

- **Instante de tempo (t):** O instante de tempo determina em qual momento o cálculo está sendo realizado. A principal função consiste em determinar a ancianidade da informação e com isso ponderá-la de acordo com o intervalo de tempo já decorrido. A ideia é que informações antigas terão menos peso no cálculo do que informações mais atuais.

- **Quantidade de nós (n):** A quantidade de nós é utilizada pois determina o tamanho da estrutura, bem como determina a quantidade de informação armazenada.

- **Pesos (p_1 e p_2):** Com o intuito de potencializar algumas informações, dois pesos foram inseridos para premiar alguma informação em especial. O peso p_1 é responsável por potencializar a ancianidade das informações e o peso p_2 é responsável por acentuar a informação própria do nó com relação a informação obtidas dos outros nós. A ideia é que a informação própria pode ser mais confiável do que a informação dos outros.

O cálculo da confiança de i em j no tempo t é dado por:

$$Confianca_i(j) = \frac{\sum_{k=0}^{n}(s_k^j \cdot (1 - \frac{t-t_k^j}{t}) \cdot p_1)}{\sum_{k=0}^{n} |s_k^j|} + s_i^j \cdot p_2 \quad (4.1)$$

que consiste na soma dos s_k^j recebidos ao longo do tempo multiplicado pela ancienidade de cada informação t_k^j multiplicado por um peso p_1, dividido pela quantidade de informações disponíveis. Ainda esse valor deve ser somado ao valor atribuído pelo nó i ao nó j multiplicado por um peso p_2 definido.

A lógica matemática desde cálculo está na média ponderada das confianças recebidas multiplicada pelos intervalos de tempos em que foram recebidas mais a confiança atribuída. A princípio, todas as informações são importantes, porém a confiança atribuída pelo próprio nó precisa ter um peso diferente, bem como a ancianidade da informação deve ser considerada em cada informação recebida. Vale considerar que a cada tempo t os valores do cálculo de confiança serão diferentes, pois algumas informações serão mais recentes e outras mais antigas.

4.4 Modelagem do TrustUm

Neste sessão será apresentada a modelagem matemática do TrustUm. A Rede Ad Hoc é definida por um grafo $G_t = (V, A_t)$, onde V representa o conjunto dos vértices de tamanho $n = |V|$ e A_t o conjunto das arestas no tempo t. Os vértices são os nós da rede e as arestas são as ligações físicas entre os nós. Nas Redes Ad Hoc os vértices se movem no decorrer do tempo, por isso não há garantia de que as ligações entre os nós serão mantidas. Quando o instante de tempo t não for utilizado, o grafo será representado simplesmente por $G = (V, A)$.

Na modelagem de jogos, os *jogadores* são os nós de V. Cada jogador $i \in V$ tem uma Matriz de confiança, aqui tratada como *conjunto de estratégias* S_i. Uma estratégia $s_i = (s_i^1, ..., s_i^n) \in S_i$ do jogador i é um vetor de tamanho $n = |V|$, onde $s_i^j = 1$ se i *confia* em j, $s_i^j = -1$ se i *não confia* em j e $s_i^j = 0$ se i *desconhece* j, isto é, i não tem nenhuma informação sobre j.

O monitoramento de vizinhos, juntamente com a troca de informações ocorre em

intervalos de tempo ΔT. Para a troca de informações é necessário definir o Status de Confiança que determinará a fração de informações que serão aceitas por cada nó. O cálculo do Status de Confiança baseia-se no Jogo do Ultimato, sendo utilizado como os *payoffs* dos jogadores.

O *payoff* (ou Status de Confiança) de i e j:

$$Payoff_i(j) = \frac{m_i}{m_i + m_j} \tag{4.2}$$

onde m_i e m_j são definidos da seguinte forma:

$$m_x = \frac{\sum_{k=0}^{n} s_k^x}{\sum_{k=0}^{n} |s_k^x|} \tag{4.3}$$

Desta forma, m_k é a soma das estratégias s_k^x da Matriz de Confiança S_x dividido pela quantidade de nós cujo valor de s_k^x é diferente de 0, ou seja, a quantidade de informações que será recebida por k é proporcional ao $payoff_x(k)$, resultando a x a outra parte da proporção.

A relação entre os *payoffs* e o Jogo do Ultimato é que quanto maior for o Status de Confiança de um nó, suas informações serão mais confiáveis, portanto a quantidade de informação recebida será menor. Do mesmo modo, se o nó tiver um baixo Status de Confiança, a quantidade de informação que será recebida será maior.

Após ser calculado os Status de Confiança, as informações são enviadas através de uma Lista de Confiança. Caso j seja identificado por i como não confiável, as informações serão descartadas. Caso contrário, a quantidade previamente calculada será recebida.

Todavia este modelo não prevê a ancianidade das informações. Para isso, é necessário quantificar o tempo juntamente com a informação passada.

$$Confianca_i(j) = \frac{\sum_{k=0}^{n} (s_k^j \cdot (1 - \frac{t - t_k^j}{t}))}{\sum_{k=0}^{n} |s_k^j|} + s_i^j \tag{4.4}$$

onde $1 - \frac{t - t_k^j}{t}$ corresponde a relação entre o tempo da troca da informação t_k^j e o tempo atual t e k é necessariamente diferente de i. Quanto mais recente a informação, maior o valor resultante, variando no intervalo de $[0, 1]$. A ancianidade da informação de i não

é calculada, pois essa informação foi calculada por i, sendo de sua responsabilidade a validade da informação.

Ainda, é possível definir pesos nas informações, uma vez que a informação atribuída por i é mais importante que as informações passadas pelos demais nós. Desta forma, a fórmula final da confiança de i em j é:

$$Confianca_i(j) = \frac{\sum_{k=0}^{n}(s_k^j \cdot (1 - \frac{t - t_k^j}{t}) \cdot p_1)}{\sum_{k=0}^{n} |s_k^j|} + s_i^j \cdot p_2 \tag{4.5}$$

CAPÍTULO 5

SIMULAÇÕES E RESULTADOS

Neste capítulo serão descritos os resultados obtidos pelo TrustUm. Todos os resultados foram produzidos através de simulações computacionais realizadas na ferramenta Network Simulator 2.34 [39] (NS-2).

NS-2 é um simulador de eventos discretos [30]. Implementado em C++ e na linguagem de *script* OTcl, o NS-2 oferece suporte nativo para as redes Ad Hoc.

5.1 Cenário de simulação

Os cenários do Teste possuem dimensões de 1000m x 1000m e 1500m x 300m. As simulações rodam com 50 nós no padrão 802.11 sem nenhum tipo de roteamento por 3000 segundos. Foram utilizados dois raios de cobertura, 125m e 250m. Foram simuladas 6 velocidades: 0, 4, 8, 12, 16 e 20 m/s. Por fim, para cada Teste foram utilizados 10% e 50% de nós maliciosos, isso para simular a reação da rede para dois cenários de cooperação diferentes.

Ainda, são gerados 35 cenários diferentes para cada Teste. A Tabela 5.1 apresenta os parâmetros dos cenários de simulação e a Tabela 5.2 apresenta os parâmetros do NS-2 para o Teste.

Parâmetros	Valor
Dimensão	1000x1000 / 1500x300
Nós	50
Raios	125 / 250
Velocidades	0 / 4 / 8 / 12 / 16 / 20
Tempo de simulação	3000 s
Intervalo de Troca de Informações	1 s

Tabela 5.1: Tabela de parâmetros de simulação.

Parâmetros	Valor
Tipo de canal	Channel/WirelessChanne
Modelo de propagação de rádio	Propagation/TwoRayGround
Tipo de antena	Antenna/OmniAntenna
Tipo da camada de enlace	LL
Tipo da fila	Queue/DropTail/PriQueue
Número máximo de pacotes na fila	50
Tipo da interface de rede	Phy/WirelessPhy
Tipo da camada MAC	Mac/802_11
Raio 125	Phy/WirelessPhy set RXThresh_ 5.8442e-09
	Phy/WirelessPhy set freq_ 9.14e+08
Raio 250	Phy/WirelessPhy set RXThresh_ 3.65262e-10
	Phy/WirelessPhy set freq_ 9.14e+08

Tabela 5.2: Tabela de parâmetros do ns-2.34.

5.2 Resultados

Os testes foram divididos em três partes: convergência da rede, convergência de cada nó e propagação de informação maliciosa.

A convergência de rede é analisada para visualizar as trocas de informações entre os nós da rede. Quanto maior a convergência, maior a quantidade de informações trocadas, confiáveis ou maliciosas. O TrustUm tem por objetivo diminuir a troca de informações maliciosas, mantendo somente as confiáveis.

A convergência de cada nó é analisada uma vez que, devido à mau comportamento dos nós, alguns nós podem ficar isolados. Tem-se a convergência de cada nó quando um nó detém informações sobre todos os outros, isto é, quando um nó encontra todos os outros nós e verifica se é malicioso ou não.

Foram realizados três testes: o primeiro teste analisa o tempo de convergência da rede somente com as trocas de informações e sem avaliação de confiança. O segundo teste simula a troca de informações somente de nós confiáveis e por fim o terceiro teste simula o TrustUm.

O Teste 1 tem por objetivo analisar o gargalo do envio e recebimento de informações. Através disso Teste é possível verificar o máximo de informação transmitida na rede, e com isso determinar a Convergência da Rede.

O Teste 2 tem por objetivo analisar o caso da rejeição total dos nós maliciosos. Tal

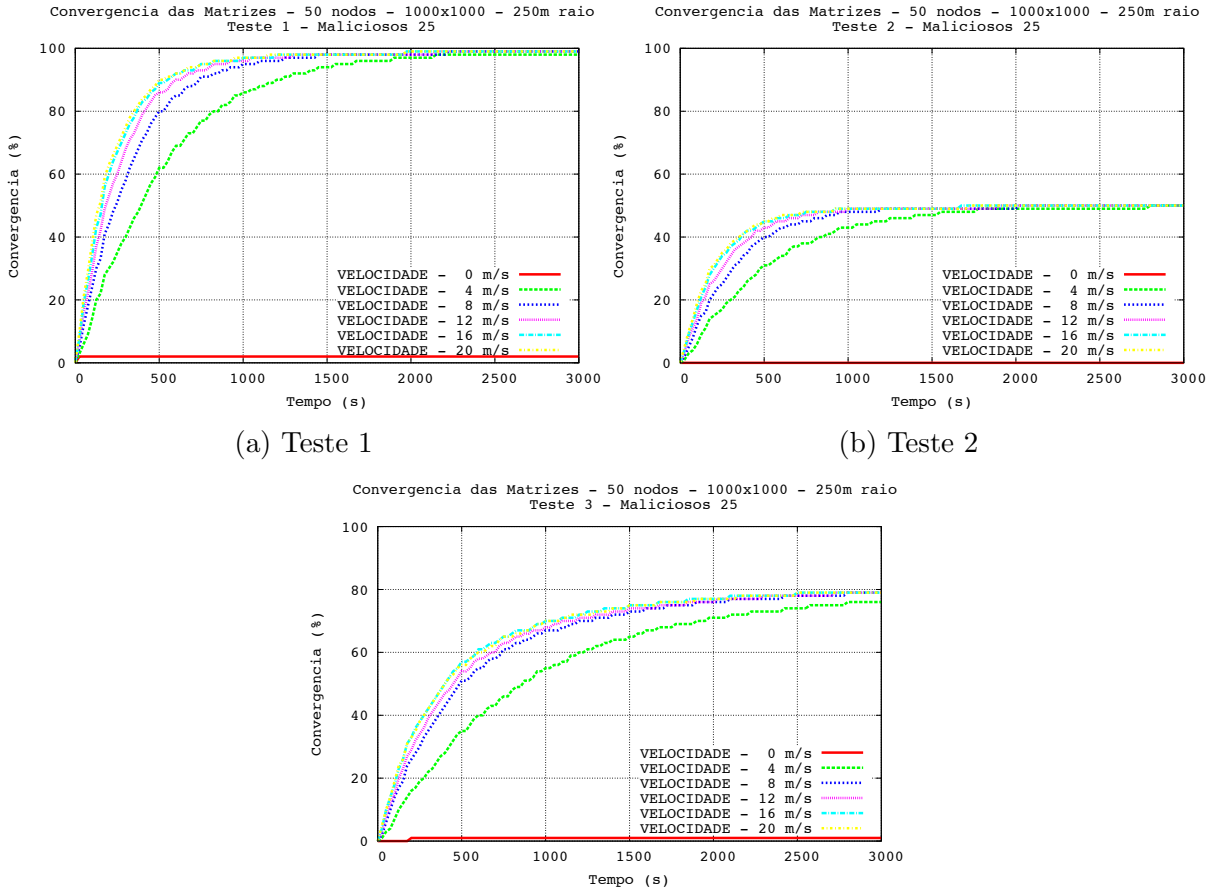
cenário é ideal, porém é praticamente impossível na vida real, uma vez que não é possível de antemão um nó deter a informação sobre todos os demais nós que são maliciosos. Desta forma consegue-se quantificar a convergência da rede neste caso, bem como analisar quanta informação foi trocada, verificando a perda de informações confiáveis.

Por fim, o Teste 3 contém o TrustUm, onde as trocas de informações são realizadas de acordo com o Status de Confiança de cada nó. Utilizando a Teoria de Jogos neste modelo, o Jogo do Ultimato consegue explorar os valores dos Status de Confiança de cada nó, e a partir desse *payoff*, é possível quantificar a troca de informações de maneira justa e correta.

Para a Teste 3, o TrustUm não utilizou os pesos tanto da própria informação como dos tempos. Tais pesos são interessantes na utilização para quem vai aplicar o modelo, pois pondera as informações de acordo com a aplicação desejada. Para comparar o TrustUm com simulações diferentes, utilizar os pesos pode tornar a análise confusa.

5.2.1 Cenário 1

O primeiro cenário a ser testado contém uma área de 1000 x 1000, com 50 nós sendo 25 maliciosos, 250 de raio.



(a) Teste 1

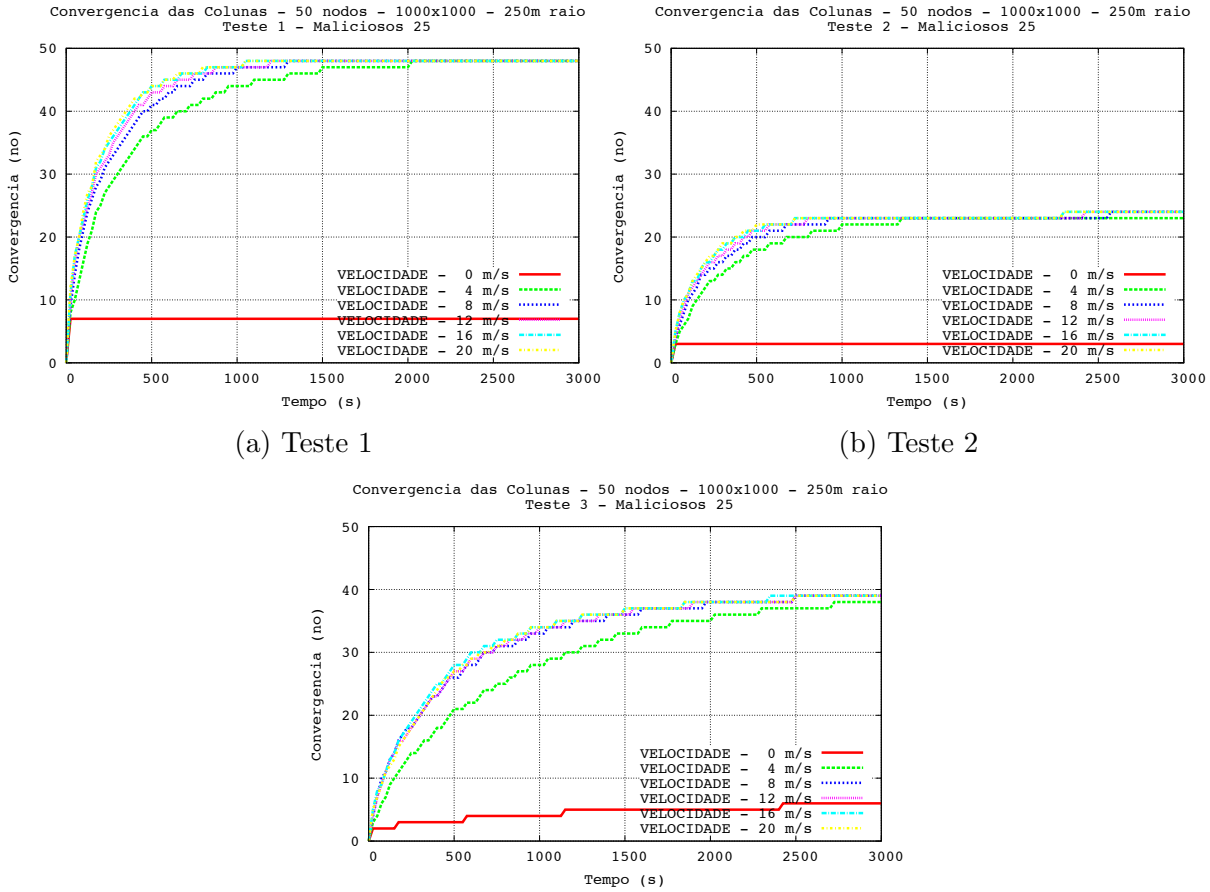
(b) Teste 2

(c) Teste 3

Figura 5.1: Simulações de convergência da rede com cenário de 50 nós, sendo 25 nós maliciosos, dimensão de 1000 x 1000 e raio de 250.

Através da Figura 5.1 é possível analisar a convergência da rede nos três testes diferentes. Na Figura 5.1b é verifica-se que o Teste 2 tem uma convergência da rede muito baixa, se comparada ao Teste 1, da Figura 5.1a, 50% e 100% respectivamente. Esse comportamento deve-se a rejeição total das informações enviadas por nós maliciosos. Tal comportamento não é desejável visto que uma avaliação inicial errada sobre a malicidade do nó compromete em definitivo seu funcionamento.

Ainda, constata-se que na Figura 5.1c onde o Teste 3 foi realizada, o TrustUm consegue gerenciar a convergência da rede a ponto de reduzir a troca de informações maliciosas, sem ter que ignorar as informações confiáveis na mesma proporção. Isso fica evidenciado na Figura 5.3.



(a) Teste 1

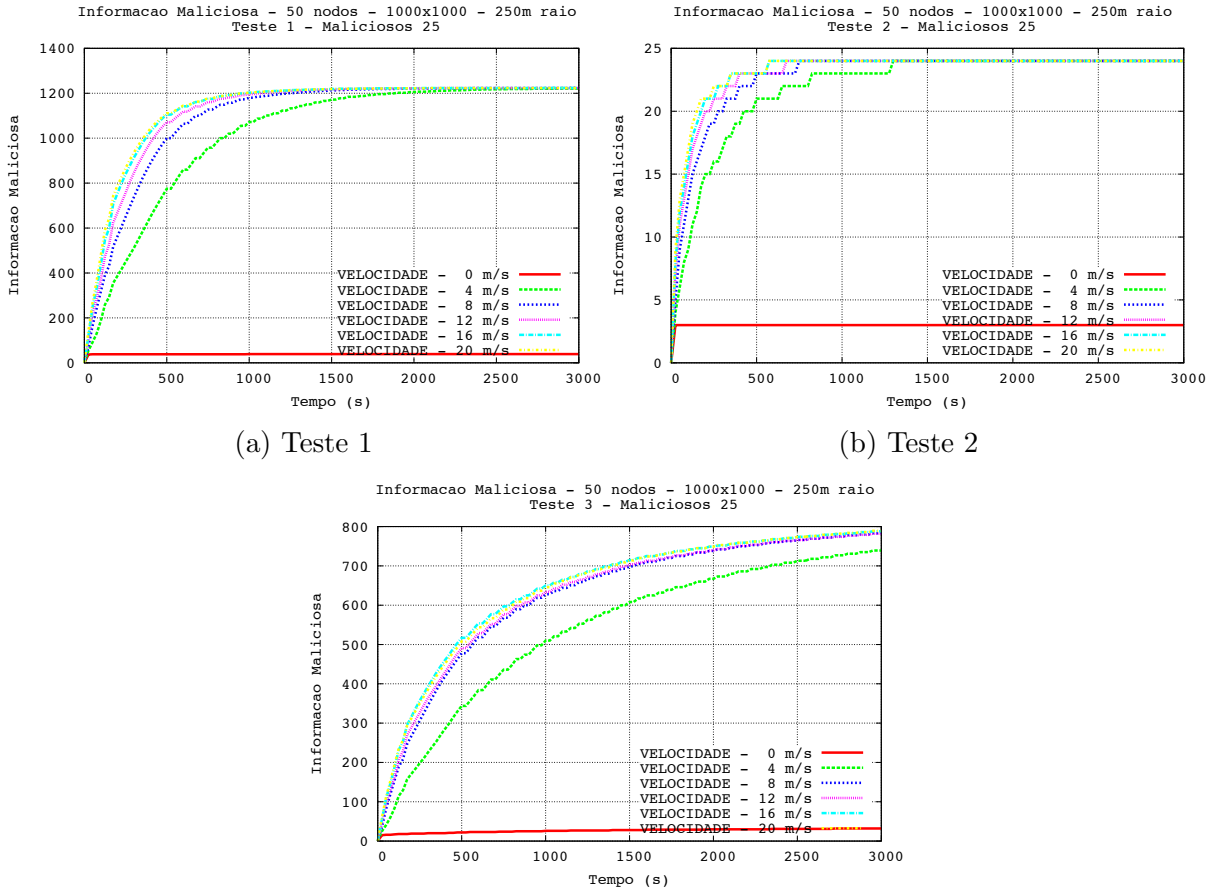
(b) Teste 2

(c) Teste 3

Figura 5.2: Simulações de convergência da cada nó com cenário de 50 nós, sendo 25 nós maliciosos, dimensão de 1000 x 1000 e raio de 250.

Através da Figura 5.2 é possível verificar a convergência de cada nó. Os resultados são bastante semelhantes à Convergência de Rede, todavia é possível verificar na Figura 5.2c que na velocidade 0 (zero) a convergência continua aumentando, diferente dos Testes 1 e 2. Esse comportamento mostra que os nós trocam informações sobre outros nós, que é uma vantagem sobre os modelos existentes de Cálculo de Confiança.

Por fim, também é prudente verificar que na Figura 5.2b a convergência chega a 25 nós, exatamente como o esperado, uma vez que o cenário contém 25 nós maliciosos e todos esses são ignorados pelos demais.



(a) Teste 1

(b) Teste 2

(c) Teste 3

Figura 5.3: Simulações de propagação de informação maliciosa com cenário de 50 nós, sendo 25 nós maliciosos, dimensão de 1000 x 1000 e raio de 250.

Na Figura 5.3 encontram-se os testes da propagação de informação maliciosa. As escalas dos gráficos estão diferentes para uma melhor visualização dos resultados. Analisando os gráficos, percebe-se que a propagação das informações maliciosas no Teste 3 da Figura 5.3c é 33% menor que a Figura 5.3a. Isso é consequência da utilização do TrustUm na troca das informações dos nós maliciosos.

Vale ressaltar que o valor alto do raio propicia um maior contato entre os nós, e por consequência, uma maior troca de informações, o que culmina em uma propagação maior de informação maliciosa.

Através da Tabela 5.3 é possível observar algumas características do Cálculo da Confiança. No exemplo, os nós maliciosos são os nós pares. Primeiramente os valores calculados para a Velocidade 0 são mais imprecisos que nas demais velocidades, todavia o Nó 1 conseguiu identificar alguns nós maliciosos, como os Nós 22 e 42 por exemplo. Nas

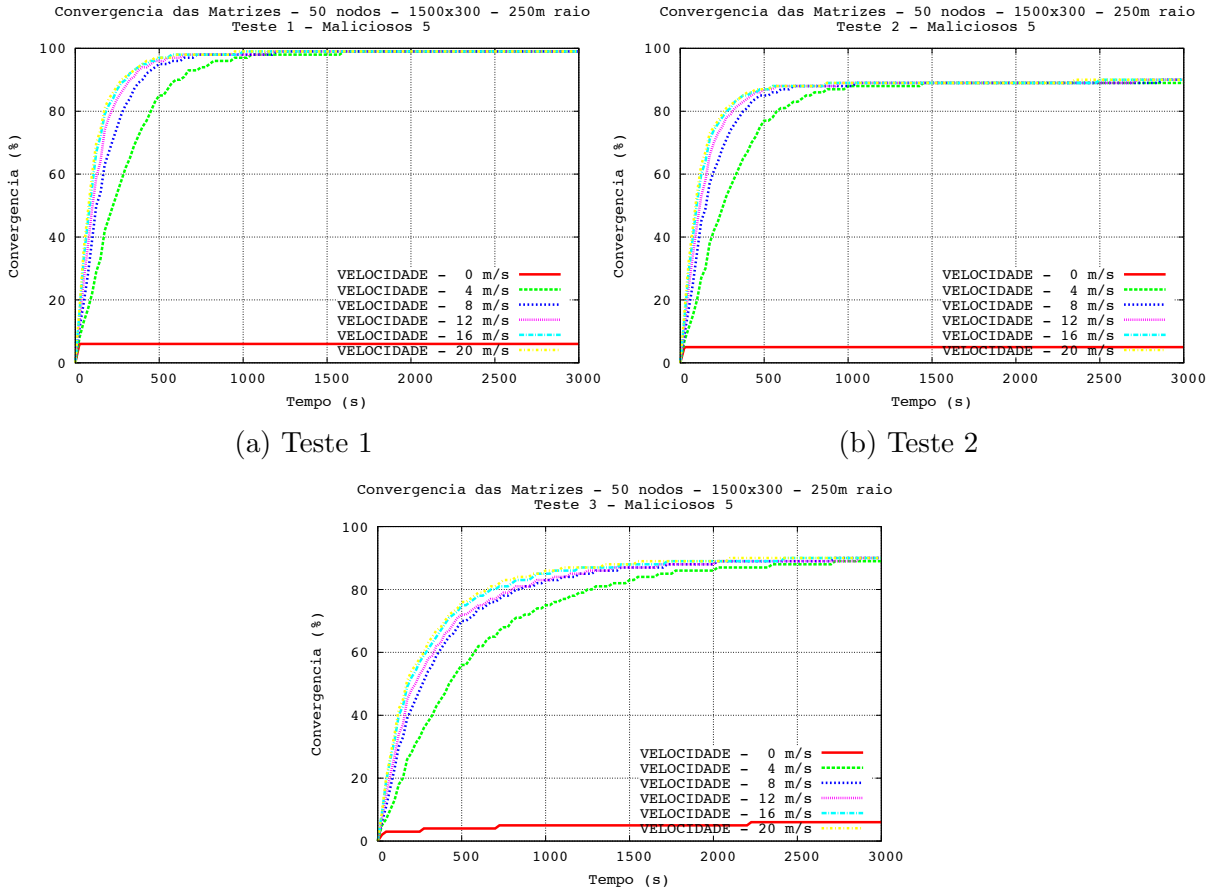
	Velocidade 0		Velocidade 4		Velocidade 8		Velocidade 12		Velocidade 16		Velocidade 20	
Nó	500	1500	500	1500	500	1500	500	1500	500	1500	500	1500
1	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
2	0.5	0.5	-1.5	-1.5	-1.5	-1.5	-1.6	-1.6	-1.6	-1.4	-1.3	-1.4
3	0.5	0.5	1.4	1.4	1.4	1.4	1.5	1.4	1.5	1.9	1.5	1.6
4	0.5	0.5	-1.2	-1.5	-1.2	-1.5	-1.4	-1.5	-0.5	-1.8	-1.3	-1.4
5	0.5	0.5	1.5	1.5	1.5	1.4	1.3	1.3	1.9	1.7	1.7	1.5
6	0.5	0.5	-1.5	-1.8	-1.4	-1.4	-1.7	-1.5	-1.7	-1.5	-1.6	-1.6
7	0.5	0.5	1.4	1.5	1.5	1.7	1.9	1.7	1.7	1.6	1.5	1.8
8	0.5	0.5	-1.4	-1.5	-0.5	-0.5	-1.6	-1.5	-1.3	-1.6	-1.8	-1.7
9	1.6	1.5	1.5	1.7	1.5	1.7	1.5	1.5	1.6	1.6	1.4	1.3
10	0.5	0.5	-1.5	-1.7	-0.3	-1.3	-1.5	-1.5	-1.5	-1.5	-1.4	-1.7
11	1.4	1.6	1.5	1.5	1.9	1.6	1.8	1.7	1.6	1.5	1.4	1.4
12	0.5	0.5	-1.6	-1.4	-1.5	-1.5	-1.5	-1.3	-0.5	-1.6	-1.8	-1.5
13	0.7	0.7	0.5	1.8	1.6	1.4	1.7	1.6	1.5	1.5	1.8	1.7
14	0.5	0.5	-1.7	-1.4	-1.7	-1.6	-1.6	-1.7	-1.6	-1.7	-0.5	-1.7
15	0.5	0.5	1.2	1.4	1.8	1.7	1.8	1.6	1.4	1.7	1.6	1.5
16	0.5	0.5	-0.5	-1.5	-1.7	-1.6	-1.2	-1.6	-0.5	-1.6	-1.6	-1.6
17	0.5	0.5	1.5	1.7	1.5	1.3	1.5	1.8	1.6	1.7	1.3	1.6
18	0.5	0.5	-0.5	-0.5	-1.9	-1.6	-1.5	-1.4	-1.3	-1.5	-1.7	-1.6
19	0.5	0.5	1.6	1.6	1.3	1.6	1.9	1.5	1.5	1.9	1.5	1.6
20	-0.2	-0.2	-1.6	-1.5	-0.5	-1.8	-1.8	-1.6	-1.6	-1.7	-1.5	-1.4
21	0.5	0.5	1.7	1.7	1.6	1.5	1.6	1.5	1.4	1.4	1.5	1.5
22	-0.5	-1.2	-1.4	-1.4	-1.7	-1.7	-1.3	-1.6	-1.5	-1.4	-1.5	-1.5
23	1.3	1.3	1.8	1.7	1.5	1.5	1.5	1.8	1.8	1.7	1.6	1.5
24	-0.4	-0.4	-1.3	-1.2	-1.8	-1.4	-0.5	-1.9	-1.5	-1.5	-1.5	-1.5
25	1.5	1.3	1.3	1.7	1.6	1.6	1.6	1.7	1.7	1.7	1.7	1.7
26	0.5	0.5	-0.5	-1.6	-1.6	-1.6	-1.3	-1.4	-1.7	-1.7	-1.7	-1.7
27	1.3	1.3	1.5	1.5	1.8	1.6	1.8	1.8	1.6	1.6	1.4	1.3
28	0.5	0.5	-1.6	-1.4	-1.7	-1.7	-1.2	-1.2	-1.4	-1.4	-1.6	-1.5
29	0.5	0.5	1.5	1.5	0.5	1.5	1.3	1.7	1.3	1.5	1.5	1.5
30	-1.2	-1.7	-1.5	-1.3	-0.5	-1.4	-1.6	-1.6	-1.4	-1.3	-1.2	-1.7
31	0.5	0.5	1.5	1.7	1.7	1.5	1.6	1.8	1.7	1.7	1.6	1.4
32	0.5	0.5	-0.7	-1.7	-0.5	-0.5	-1.6	-1.7	-1.5	-1.7	-1.6	-1.5
33	0.5	0.5	1.5	1.4	1.5	1.6	1.8	1.6	1.5	1.5	1.5	1.8
34	0.5	0.5	-1.5	-1.4	-1.3	-1.5	-1.7	-1.6	-1.5	-1.4	-1.4	-1.3
35	0.5	0.5	1.7	1.6	1.6	1.8	1.6	1.6	1.5	1.5	1.8	1.7
36	0.5	0.5	-0.5	-1.5	-1.6	-1.6	-0.5	-1.7	-1.7	-1.5	-1.5	-1.6
37	0.5	0.4	1.5	1.4	1.5	1.6	1.8	1.6	1.7	1.7	1.3	1.5
38	0.5	0.5	-0.5	-1.8	-1.7	-1.8	-1.6	-1.6	-1.6	-1.6	-1.3	-1.6
39	0.5	0.5	0.7	1.7	1.6	1.5	1.9	1.7	1.8	1.7	1.6	1.6
40	0.5	0.5	-1.3	-1.3	-1.7	-1.5	-1.6	-1.5	-1.6	-1.6	-1.6	-1.5
41	0.5	0.5	1.8	1.7	1.6	1.5	1.8	1.6	1.5	1.6	1.3	1.4
42	-0.5	-1.6	-1.6	-1.6	-1.7	-1.7	-1.4	-1.6	-1.6	-1.5	-1.7	-1.6
43	0.5	0.5	1.5	1.5	2.0	1.8	1.8	1.7	1.4	1.4	1.6	1.8
44	0.5	0.5	-0.5	-1.7	-1.8	-1.6	-1.8	-1.8	-1.2	-1.4	-1.6	-1.5
45	0.5	0.5	1.5	1.5	1.5	1.4	1.5	1.9	1.5	1.7	1.5	1.6
46	0.5	0.5	0.5	-1.8	-1.9	-1.6	-1.8	-1.7	-0.5	-1.7	-1.5	-1.5
47	0.5	0.5	1.5	1.5	1.5	1.5	1.4	1.6	1.6	1.6	1.4	1.5
48	0.5	0.5	-1.5	-1.4	-1.3	-1.6	-0.6	-1.6	-1.3	-1.5	-1.6	-1.5
49	0.5	0.5	1.5	1.4	1.5	1.5	1.6	1.7	1.7	1.5	1.8	1.7
50	0.5	-0.2	-1.6	-1.6	-0.5	-1.7	-1.4	-1.6	-1.6	-1.6	-1.7	-1.6

Tabela 5.3: Cálculo de Confiança do nó 1 nos tempos 500 e 1500 do Cenário 1 do Teste 3

demais velocidades, a detecção é total, pois a convergência propicia isso.

5.2.2 Cenário 2

O segundo cenário a ser testado contém uma área de 1500 x 300, com 50 nós sendo 5 maliciosos, 250 de raio.



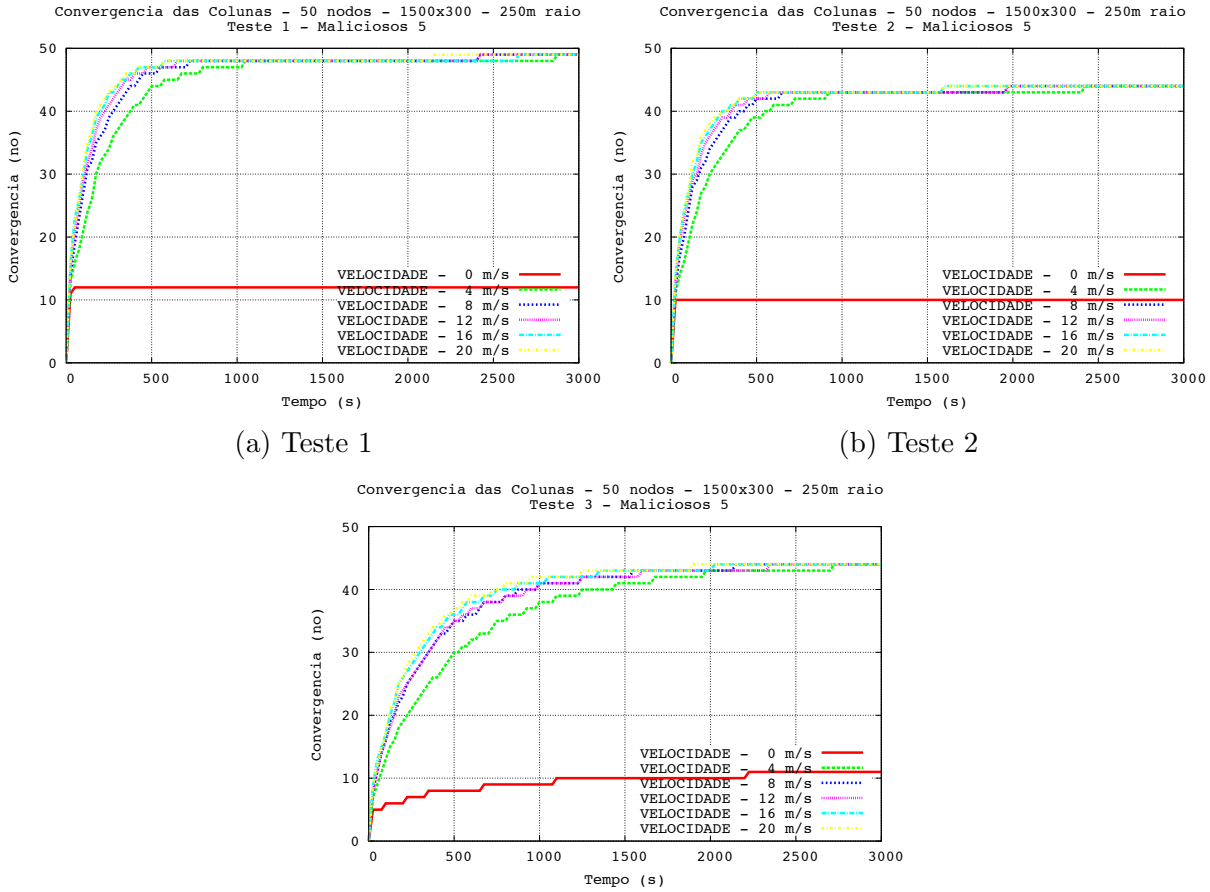
(a) Teste 1

(b) Teste 2

(c) Teste 3

Figura 5.4: Simulações de convergência da rede com cenário de 50 nós, sendo 5 nós maliciosos, dimensão de 1500 x 300 e raio de 250.

Através da Figura 5.4 é possível analisar a convergência da rede nos três testes. Neste cenário, é possível verificar que o Teste 2 (Figura 5.4b) e Teste 3 (Figura 5.4c) tem convergências próximas. Fato esse decorrente do raio de cobertura alto, bem como do número de nós maliciosos baixo.



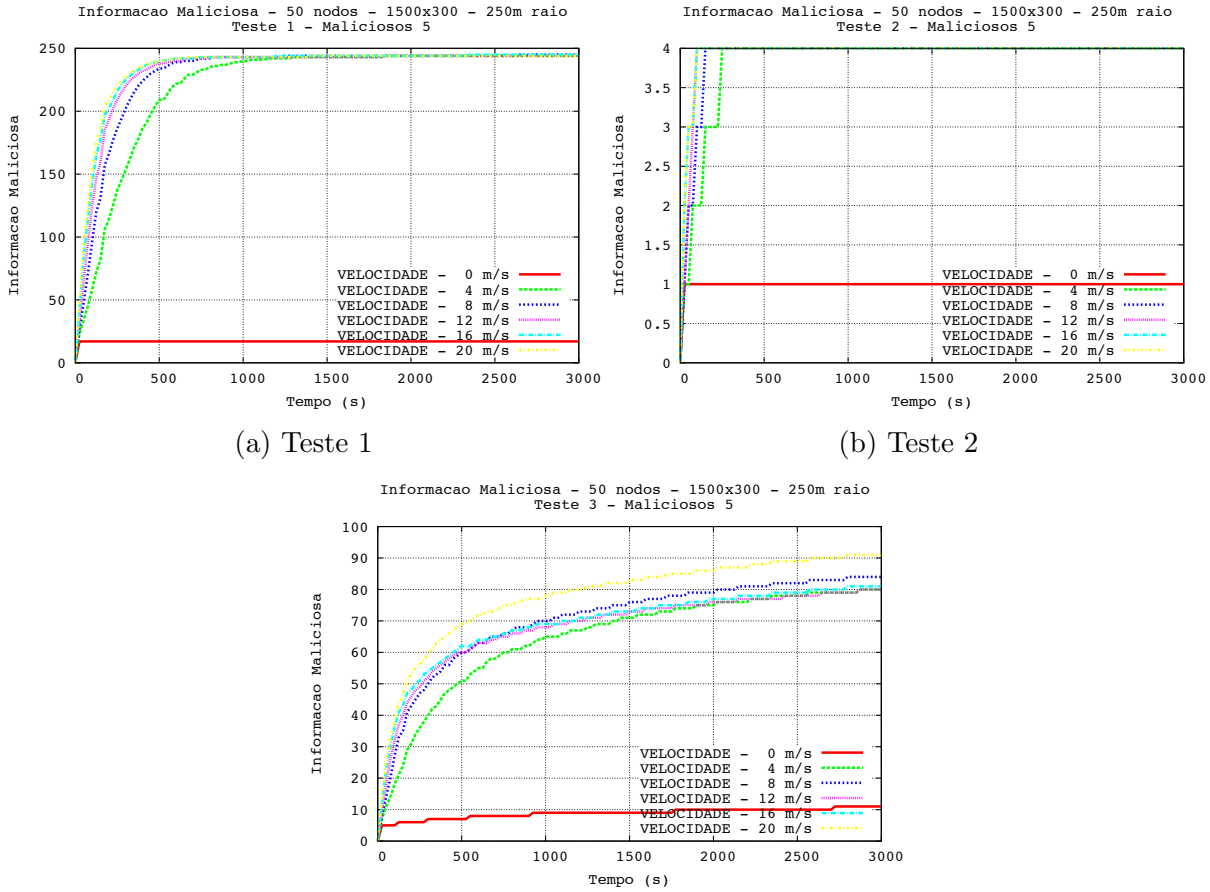
(a) Teste 1

(b) Teste 2

(c) Teste 3

Figura 5.5: Simulações de convergência de cada nó com cenário de 50 nós, sendo 5 nós maliciosos, dimensão de 1500 x 300 e raio de 250.

Da mesma forma que ocorre com a convergência da Figura 5.4, na Figura 5.5 a convergência de cada nó é mais acentuada no Teste 1 por não haver análise de confiança. Já nos Testes 2 e 3 as convergências se equivalem, sendo no Teste 2 o processo um pouco mais rápido, uma vez que o Status de Confiança utilizado no Teste 3 seleciona os dados antes da troca de informações. Todavia o Teste 3 demora o dobro de tempo dos Testes 1 e 2 em média para atingir a convergência.



(a) Teste 1

(b) Teste 2

(c) Teste 3

Figura 5.6: Simulações de propagação de informação maliciosa com cenário de 50 nós, sendo 5 nós maliciosos, dimensão de 1500 x 300 e raio de 250.

Agora analisando a Figura 5.6 percebe-se uma queda de 64% na quantidade de informações maliciosa propagada, isso comparados os Testes 1 e 3. Tal diminuição se deve a seleção que o Status de Confiança realiza nas informações antes de serem compartilhadas. Para a configuração de 50 nós tem-se no máximo 250 informações maliciosas.

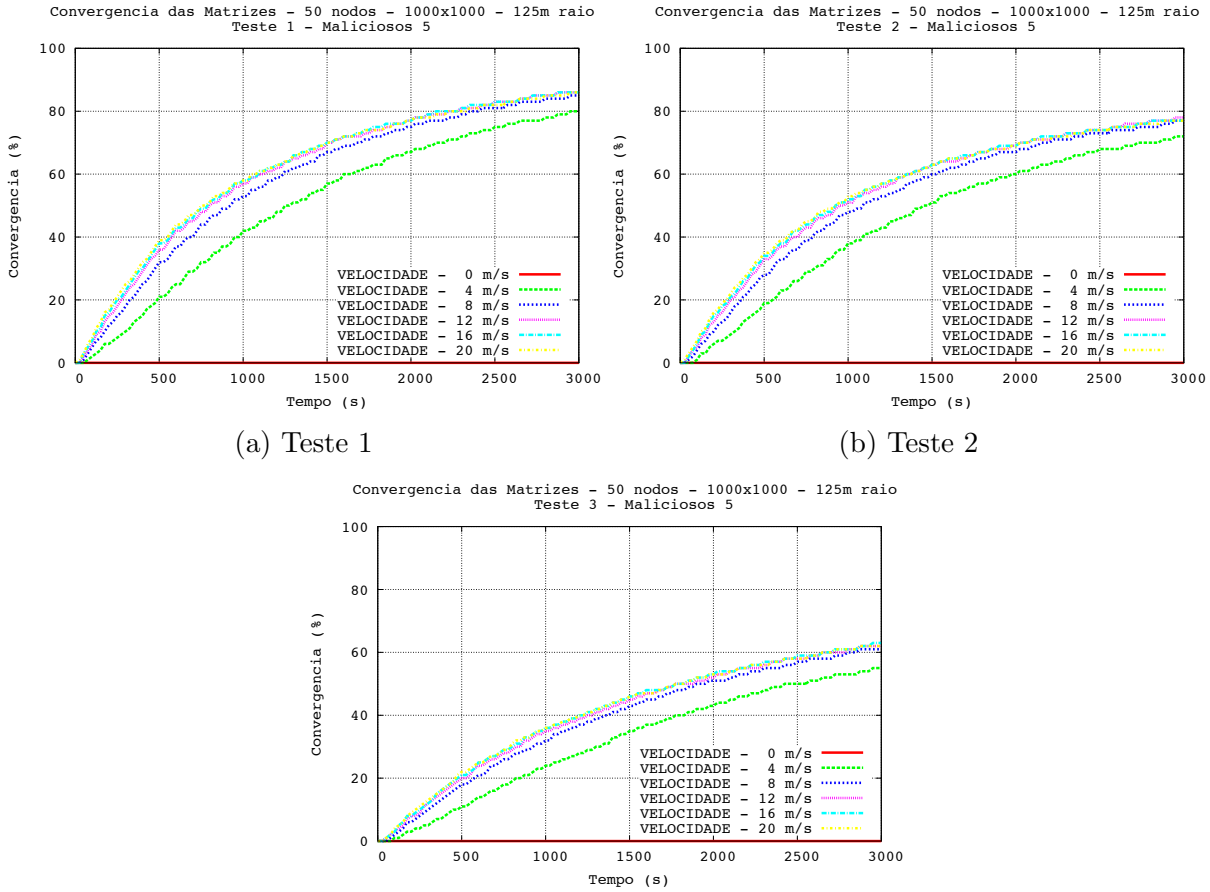
Através da Tabela 5.4 é possível verificar a Matriz de Confiança do Nó 3 nos tempos 500 e 1500. Neste cenário, são 5 os nós maliciosos, os Nós 2, 4, 6, 8 e 10. Fica evidente pelos resultados qual nó é confiável e qual nó é malicioso. Ainda, podemos verificar que os valores calculados pelo Nó 3 variam de acordo com cada nó observado. Analisando os valores, é possível identificar preferências de acordo com o comportamento de cada um.

	Velocidade 0		Velocidade 4		Velocidade 8		Velocidade 12		Velocidade 16		Velocidade 20	
Nó	500	1500	500	1500	500	1500	500	1500	500	1500	500	1500
1	0.5	0.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5
2	0.5	0.5	-1.8	-1.8	-1.7	-1.7	-1.8	-1.8	-1.8	-1.7	-1.8	-1.7
3	1.8	1.7	1.5	1.8	1.7	1.8	1.6	1.8	1.7	1.8	1.8	1.8
4	-0.5	-0.4	-0.5	-1.9	-1.7	-1.9	-1.8	-1.8	-1.7	-1.8	-1.6	-1.8
5	0.5	0.5	1.8	1.8	1.8	1.8	1.8	1.8	1.8	1.8	1.9	1.7
6	0.5	0.5	-1.8	-1.7	-1.7	-1.7	-1.8	-1.6	-1.7	-1.8	-0.5	-1.6
7	0.7	0.5	1.5	1.9	1.7	1.7	1.8	1.7	1.7	1.7	1.6	1.7
8	-1.0	-1.7	-0.5	-1.8	-1.7	-1.8	-0.5	-1.6	-1.7	-1.8	-1.6	-1.8
9	1.4	1.7	1.8	1.6	1.7	1.8	1.5	1.8	1.7	1.8	1.9	1.8
10	-1.6	-1.6	-1.8	-1.7	-1.8	-1.8	-1.5	-1.9	-1.7	-1.7	-1.8	-1.7
11	1.5	1.7	1.5	1.7	1.8	1.9	1.6	1.7	1.8	1.8	1.9	1.6
12	0.5	0.5	1.8	1.8	1.8	1.7	1.9	1.8	1.7	1.7	1.8	1.6
13	0.5	0.5	1.5	1.9	1.8	1.8	1.6	1.9	1.8	1.8	1.6	1.6
14	0.5	0.5	1.7	1.8	1.7	1.8	1.8	1.6	1.8	1.8	1.8	1.7
15	0.5	0.5	1.8	1.8	1.6	1.8	1.4	1.9	1.8	1.8	1.7	1.9
16	0.5	0.5	1.5	1.8	1.8	1.8	1.5	1.9	1.8	1.8	1.9	1.8
17	0.5	0.5	1.8	1.9	1.8	1.8	1.8	1.9	1.8	1.8	1.7	1.8
18	0.7	0.7	1.7	1.7	1.8	1.8	1.6	1.8	1.7	1.8	1.5	1.8
19	0.5	0.5	1.5	1.9	1.7	1.7	1.6	1.8	1.8	1.8	1.9	1.7
20	0.5	0.5	1.5	1.9	1.8	1.8	1.8	1.6	1.8	1.7	1.8	1.8
21	0.5	0.5	1.6	1.9	1.7	1.8	1.5	1.8	1.7	1.7	1.8	1.8
22	0.4	0.4	1.8	1.6	1.8	1.9	1.8	1.7	1.7	1.8	1.9	1.8
23	0.5	0.8	1.5	1.8	1.8	1.8	1.9	1.8	1.7	1.8	1.9	1.8
24	0.5	0.5	0.8	1.8	1.7	1.8	1.5	1.9	1.8	1.8	1.9	1.8
25	0.8	0.7	1.8	1.7	1.8	1.9	1.5	1.5	1.8	1.8	1.6	1.7
26	0.5	0.5	1.8	1.9	1.8	1.8	1.5	1.8	1.8	1.8	1.6	1.8
27	0.6	0.5	1.8	1.8	1.7	1.8	1.9	1.8	1.7	1.8	1.5	1.9
28	0.5	0.5	1.5	1.8	1.7	1.8	1.8	1.8	1.8	1.8	1.8	1.7
29	0.5	0.5	1.5	1.9	1.7	1.7	1.8	1.7	1.7	1.8	1.8	1.8
30	0.5	0.5	1.7	1.6	1.7	1.8	1.6	1.8	1.7	1.8	1.9	1.8
31	0.5	0.5	1.4	1.6	1.8	1.8	1.8	1.8	1.8	1.8	1.5	1.5
32	1.5	1.8	1.5	1.5	1.8	1.9	1.6	1.7	1.7	1.8	1.8	1.9
33	0.5	0.5	1.5	1.9	1.8	1.8	1.6	1.8	1.8	1.7	1.7	1.8
34	1.4	1.7	1.8	1.6	1.8	1.8	1.9	1.8	1.7	1.8	1.8	1.8
35	1.7	1.7	1.5	1.9	1.8	1.8	1.5	1.7	1.8	1.7	1.9	1.7
36	0.5	0.5	1.8	1.8	1.8	1.8	1.9	1.7	1.7	1.8	1.5	1.5
37	0.5	0.5	1.8	1.6	1.8	1.8	1.9	1.9	1.8	1.8	1.8	1.8
38	0.7	0.7	1.5	1.9	1.8	1.9	1.6	1.8	1.8	1.8	1.9	1.8
39	0.5	0.5	1.8	1.6	1.7	1.9	1.9	1.7	1.8	1.8	1.9	1.8
40	0.5	0.5	1.5	1.5	1.8	1.8	1.9	1.8	1.7	1.8	1.5	1.6
41	0.5	0.5	1.8	1.9	1.8	1.8	1.6	1.8	1.8	1.8	1.7	1.9
42	0.5	0.5	1.8	1.6	1.7	1.8	1.9	1.8	1.8	1.7	1.6	1.8
43	0.5	0.7	1.5	1.8	1.7	1.7	1.8	1.8	1.8	1.8	1.7	1.9
44	0.7	0.6	1.7	1.7	1.7	1.8	1.9	1.7	1.7	1.8	1.7	1.9
45	0.5	0.5	1.8	1.8	1.7	1.8	1.6	1.8	1.7	1.8	1.8	1.9
46	0.5	0.5	1.5	1.9	1.6	1.8	1.5	1.7	1.8	1.8	1.9	1.9
47	1.7	1.7	1.5	1.7	1.7	1.8	1.6	1.9	1.8	1.8	1.7	1.9
48	0.5	0.5	1.8	1.8	1.7	1.8	1.8	1.9	1.7	1.8	1.6	1.8
49	2.0	1.8	1.5	1.8	1.7	1.8	1.8	1.8	1.7	1.7	1.9	1.8
50	0.8	0.7	1.8	1.9	1.8	1.8	1.6	1.7	1.7	1.8	1.8	1.8

Tabela 5.4: Cálculo de Confiança do nó 3 nos tempos 500 e 1500 do Cenário 2 do Teste 3

5.2.3 Cenário 3

O terceiro cenário testado é contituído de uma área de 1000 x 1000, com 50 nós sendo 5 maliciosos, 125 m de raio.



(a) Teste 1

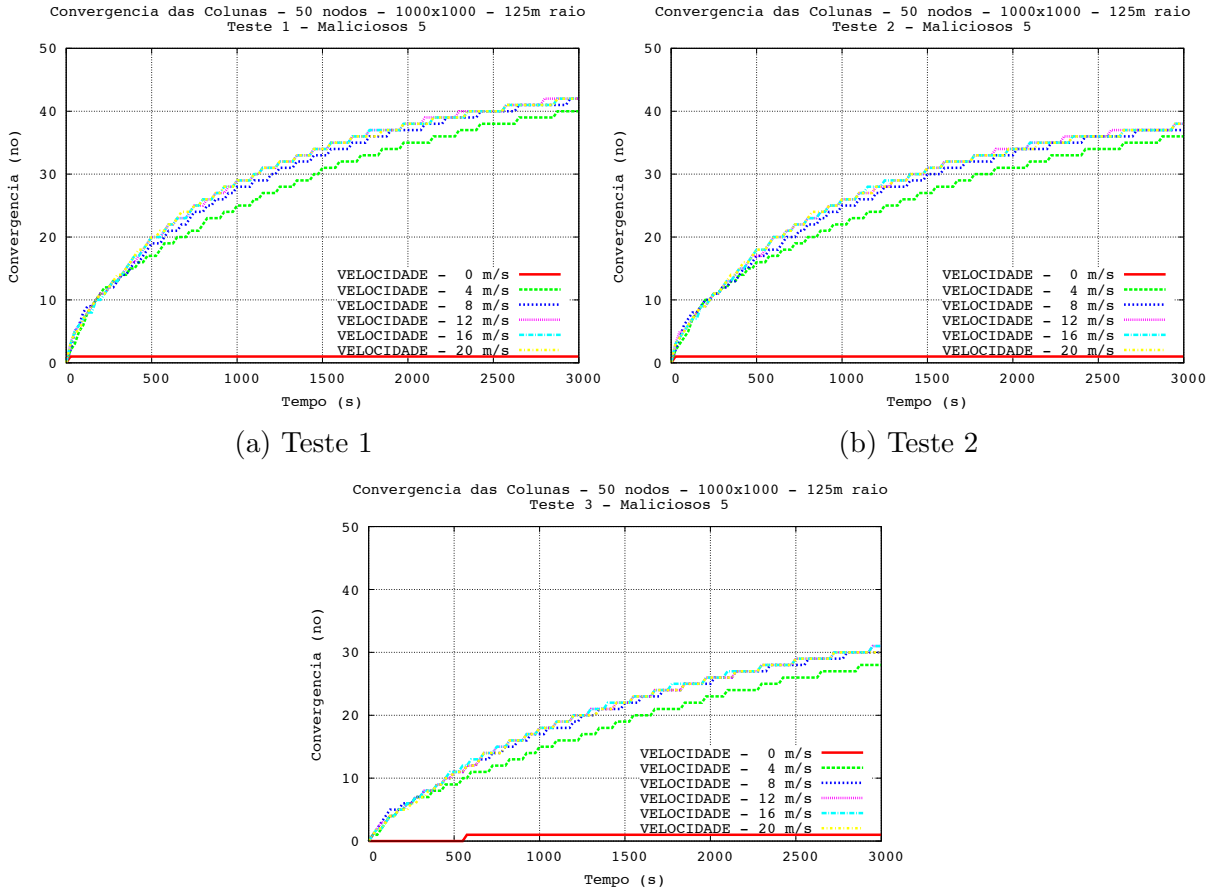
(b) Teste 2

(c) Teste 3

Figura 5.7: Simulações de convergência da rede com cenário de 50 nós, sendo 5 nós maliciosos, dimensão de 1000 x 1000 e raio de 125.

Pode-se notar inicialmente que a convergência neste cenário é diferente do cenário 1, isto por que no cenário 3 o raio de cobertura é igual a 125m, diferente do cenário 1 que o raio é 250m. Através da Figura 5.7 é possível verificar as convergências de rede dos três testes no Cenário 3. Como são poucos os nós maliciosos, 5 no total, a convergência entre o Teste 1 e o Teste 2 são próximas, 85% e 80%, isto por que a rejeição de dados é baixa. Neste caso, o Teste 3 tem uma convergência menor, visto que o modelo seleciona os dados que serão trocados de acordo com o Status de Confiança.

Ainda, é possível observar que na velocidade 0 m/s a convergência nem aparece nos gráficos. Isso é decorrência do cenário proposto. Como a área é maior e o raio de cobertura dos nós é menor, muitos nós ficam isolados inicialmente e, por isso, as trocas de informações se tornam quase nulas. Isso também acarreta que os testes não atingem os 100% de convergência.



(a) Teste 1

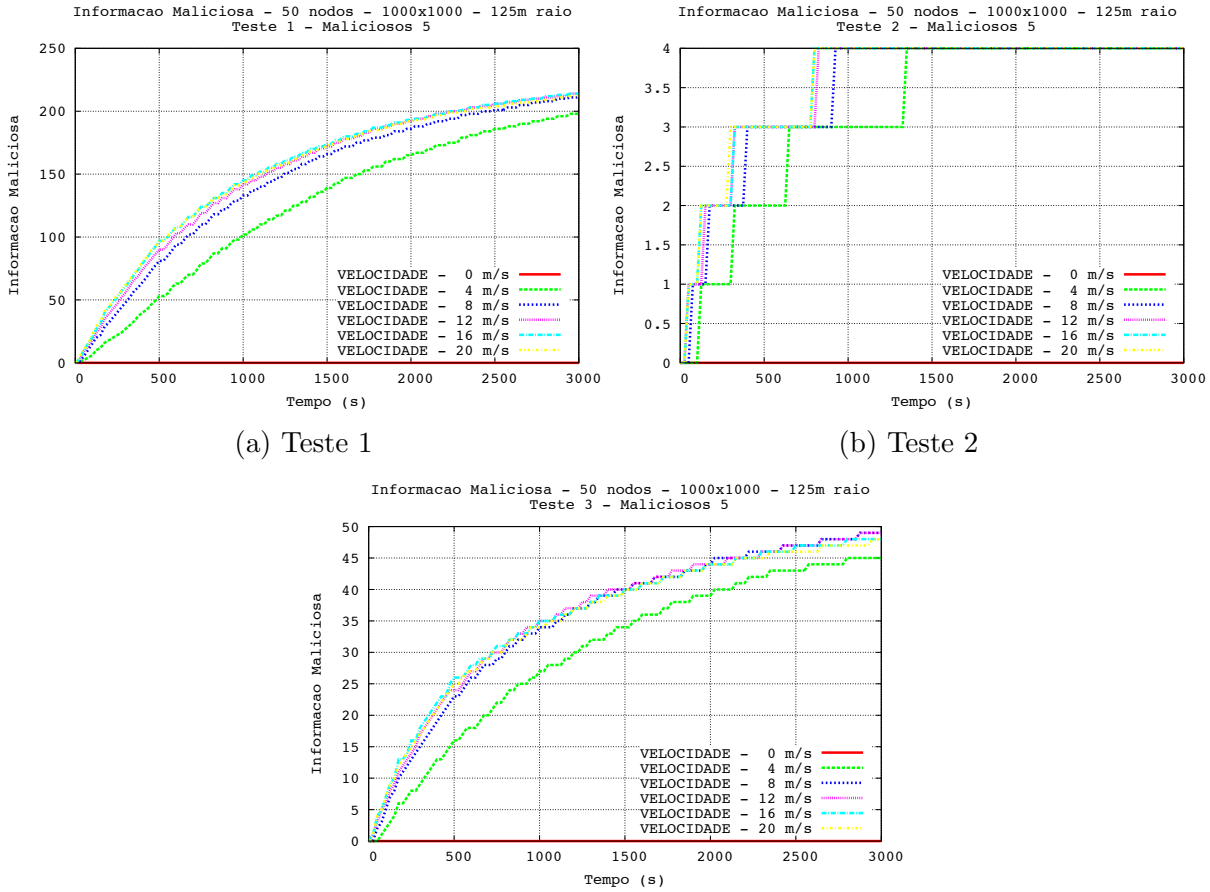
(b) Teste 2

(c) Teste 3

Figura 5.8: Simulações de convergência de cada nó com cenário de 50 nós, sendo 5 nós maliciosos, dimensão de 1000 x 1000 e raio de 125.

Na Figura 5.8 é possível analisar a convergência de cada nó dos três testes no Cenário 3. Inicialmente, é possível verificar que na velocidade 0 m/s a convergência atinge apenas 1 nó, ilustrando a afirmativa passada anteriormente, sobre as características do Cenário 3.

Com relação às diferentes velocidades testadas, somente a velocidade 0 m/s é que não apresenta resultados satisfatórios. As demais velocidades têm resultados semelhantes, porém quanto maior a velocidade, mais rápida é a convergência. Esses resultados demostram quão importante é a mobilidade para o TrustUm.



(a) Teste 1

(b) Teste 2

(c) Teste 3

Figura 5.9: Simulações de propagação de informação maliciosa com cenário de 50 nós, sendo 5 nós maliciosos, dimensão de 1000 x 1000 e raio de 125.

Através da Figura 5.9 é possível verificar a propagação de informação maliciosa no Cenário 3. Analisando as Figuras 5.9a e 5.9c, a redução de informação maliciosa é de 76%. Tal valor é decorrente da utilização do modelo na escolha das informações que são trocadas. Contudo, a convergência de rede foi 25% menor no Teste 3. Proporcionalmente, o valor esperado com essa redução no Teste 1 seria de aproximadamente 150 informações maliciosas, todavia com o Teste 3 o valor ficou em aproximadamente 50 informações maliciosas.

O Teste 3 demostra que, apesar da perda na convergência da rede, os resultados apresentados sobre a propagação de informação maliciosa são vantajosos. Vale ressaltar que o TrustUm prevê que um nó confiável tende a receber mais informações confiáveis, e com isso, selecionar melhor os nós que irão receber suas informações.

Através da Tabela 5.4 é possível verificar a Matriz de Confiança do nó 1 nos tempos

	Velocidade 0		Velocidade 4		Velocidade 8		Velocidade 12		Velocidade 16		Velocidade 20	
	500	1500	500	1500	500	1500	500	1500	500	1500	500	1500
1	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
2	0.5	0.5	-0.5	-1.2	-0.5	-1.3	-0.5	-1.8	-1.6	-1.7	-1.7	-1.5
3	0.5	0.5	1.6	1.8	1.5	1.8	1.5	1.5	0.6	1.8	1.8	1.7
4	0.5	0.5	-0.2	-1.7	-1.6	-1.7	-1.6	-1.7	-1.6	-1.5	-1.4	-1.6
5	0.5	0.5	1.7	1.7	1.9	1.7	1.7	1.6	1.6	1.5	1.5	1.8
6	0.5	0.5	-1.2	-1.7	-1.7	-1.6	-0.6	-1.6	-0.5	-0.5	-0.7	-1.5
7	0.5	0.5	1.6	1.7	1.7	1.7	0.5	1.8	1.7	1.8	1.8	1.7
8	0.5	0.5	-0.6	-1.6	-0.5	-1.7	-0.7	-0.7	-0.7	-0.5	0.5	-1.7
9	0.7	0.7	0.8	1.6	1.6	1.7	1.8	1.8	1.6	1.6	0.7	0.7
10	0.5	0.5	-0.5	-1.5	-0.7	-0.7	-1.6	-1.6	-1.7	-1.8	-1.6	-1.7
11	0.5	0.7	0.8	1.8	1.8	1.7	1.9	1.6	1.7	1.6	1.7	1.7
12	0.5	0.5	0.7	1.8	0.7	1.7	1.5	1.9	1.7	1.6	0.8	1.7
13	0.5	0.5	0.8	1.7	0.8	0.6	1.8	1.7	1.5	1.5	1.6	1.6
14	0.5	0.5	1.5	2.0	0.7	1.8	1.6	1.6	0.6	1.5	1.7	1.7
15	0.5	0.5	1.5	1.5	1.5	1.8	1.7	1.7	0.5	1.5	1.8	1.7
16	0.5	0.5	1.5	1.8	1.5	1.8	1.6	1.7	1.7	1.6	1.5	1.8
17	0.5	0.5	1.5	1.5	1.8	1.7	1.5	1.8	1.7	1.8	1.6	1.7
18	0.5	0.5	0.5	1.7	1.5	1.5	1.5	1.6	1.7	1.8	1.8	1.6
19	0.5	0.5	1.5	1.8	1.5	1.5	1.9	1.7	0.7	0.8	1.5	1.8
20	0.5	0.5	1.7	1.7	0.8	1.8	1.5	1.9	0.7	0.8	0.8	1.7
21	0.5	0.5	1.7	1.6	1.9	1.8	1.7	1.7	1.7	1.8	1.8	1.7
22	1.9	1.6	1.8	1.6	1.8	1.8	1.8	1.8	1.7	1.6	1.6	1.8
23	1.5	2.0	1.7	1.5	1.9	1.7	1.9	1.8	0.5	0.5	1.7	1.6
24	0.5	0.5	0.5	0.7	1.6	1.5	1.7	1.7	1.7	1.6	1.7	1.6
25	0.5	0.5	0.8	1.6	0.6	1.6	0.9	0.6	0.5	0.5	1.7	1.7
26	0.5	0.5	1.7	1.7	0.8	1.7	1.5	1.9	1.5	1.5	0.5	0.7
27	0.5	0.5	1.7	1.6	0.7	1.7	1.7	1.7	1.7	1.5	1.7	1.6
28	0.5	0.5	1.6	1.5	1.8	1.7	1.7	1.7	1.5	1.8	1.8	1.7
29	0.5	0.5	0.6	1.5	0.7	1.7	1.8	1.7	1.5	1.8	1.6	1.7
30	0.7	0.5	0.9	1.7	0.9	1.7	1.5	1.8	0.5	0.8	0.5	1.6
31	0.5	0.5	1.6	1.5	0.5	1.8	1.9	1.7	0.8	1.8	1.6	1.5
32	0.5	0.5	0.6	1.7	1.8	1.6	1.5	1.9	1.8	1.8	1.5	1.8
33	0.5	0.5	1.9	1.6	0.5	0.8	0.5	1.8	1.6	1.7	0.8	1.8
34	0.5	0.5	1.8	1.5	1.6	1.7	1.8	1.7	1.7	1.6	1.9	1.7
35	0.5	0.5	1.8	1.5	0.5	1.8	1.6	1.7	1.5	1.5	1.7	1.7
36	0.5	0.5	1.5	1.7	1.7	1.7	1.7	1.8	0.7	1.7	0.7	1.7
37	0.5	0.5	0.9	1.7	1.7	1.8	0.5	1.9	1.7	1.6	0.5	0.7
38	0.5	0.5	0.6	1.8	1.9	1.8	1.7	1.7	0.7	0.7	1.6	1.6
39	0.5	0.5	0.7	0.8	0.7	0.7	1.9	1.7	1.4	1.8	1.8	1.6
40	0.5	0.5	1.7	1.6	1.5	1.5	0.8	0.7	1.6	1.7	1.7	1.7
41	0.5	0.5	0.7	0.6	1.7	1.8	1.9	1.7	0.7	1.8	1.7	1.6
42	2.0	2.0	1.6	1.7	1.8	1.7	1.8	1.8	1.7	1.8	1.8	1.7
43	0.5	0.5	0.5	0.8	1.9	1.7	1.7	1.7	1.7	1.8	1.7	1.7
44	0.5	0.5	0.8	1.6	1.7	1.6	0.6	1.7	1.6	1.6	1.7	1.7
45	0.5	0.5	1.5	1.8	1.7	1.7	1.8	1.7	1.7	1.8	1.5	1.6
46	0.5	0.5	0.7	0.8	1.5	1.8	0.6	1.6	1.6	1.5	1.6	1.7
47	0.5	0.5	1.8	1.8	1.7	1.7	0.7	0.7	1.6	1.5	1.8	1.7
48	0.5	0.5	0.7	0.7	0.8	1.8	0.4	1.7	1.8	1.8	0.8	1.7
49	0.5	0.5	0.7	1.8	0.9	1.6	1.7	1.7	0.5	1.5	0.8	0.7
50	0.5	0.5	1.9	1.5	0.8	1.6	1.6	1.7	1.7	1.8	0.7	1.7

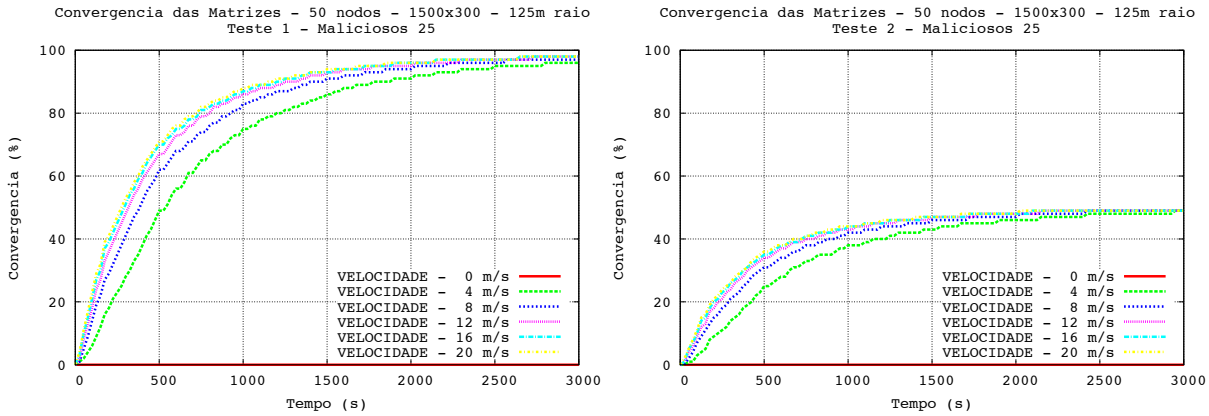
Tabela 5.5: Cálculo de Confiança do nó 1 nos tempos 500 e 1500 do Cenário 3 do Teste 3

500 e 1500. Neste cenário, são 5 os nós maliciosos, os Nós 2, 4, 6, 8 e 10. Nos tempos analisados, a velocidade 0 m/s não apresenta resultado algum. Nas demais velocidades a diferença entre os tempos 500 e 1500 é significativa. Alguns oscilam pra cima, outros pra baixo revelando tendências de confiança.

Outro detalhe aparente é que, devido às características do Cenário 3, mesmo no tempo 1500 alguns nós não tem as informações definidas sobre os demais. Na Tabela 5.5 por exemplo, o Nó 1 não tem informações sobre o Nó 25 na velocidade 16 m/s nos tempos 500 e 1500. Tal constatação tem impacto nos resultados dos demais, uma vez que os nós que se comunicam com o Nó 25 não recebem informações, e por consequência, a convergência se torna mais lenta.

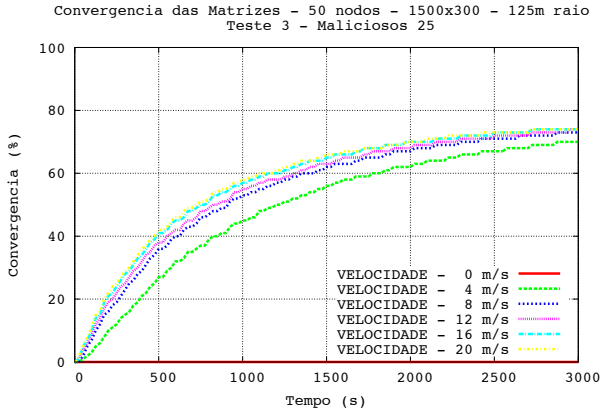
5.2.4 Cenário 4

O quarto cenário testado contém uma área de 1500 x 300, com 50 nós sendo 25 maliciosos, 125 de raio.



(a) Teste 1

(b) Teste 2

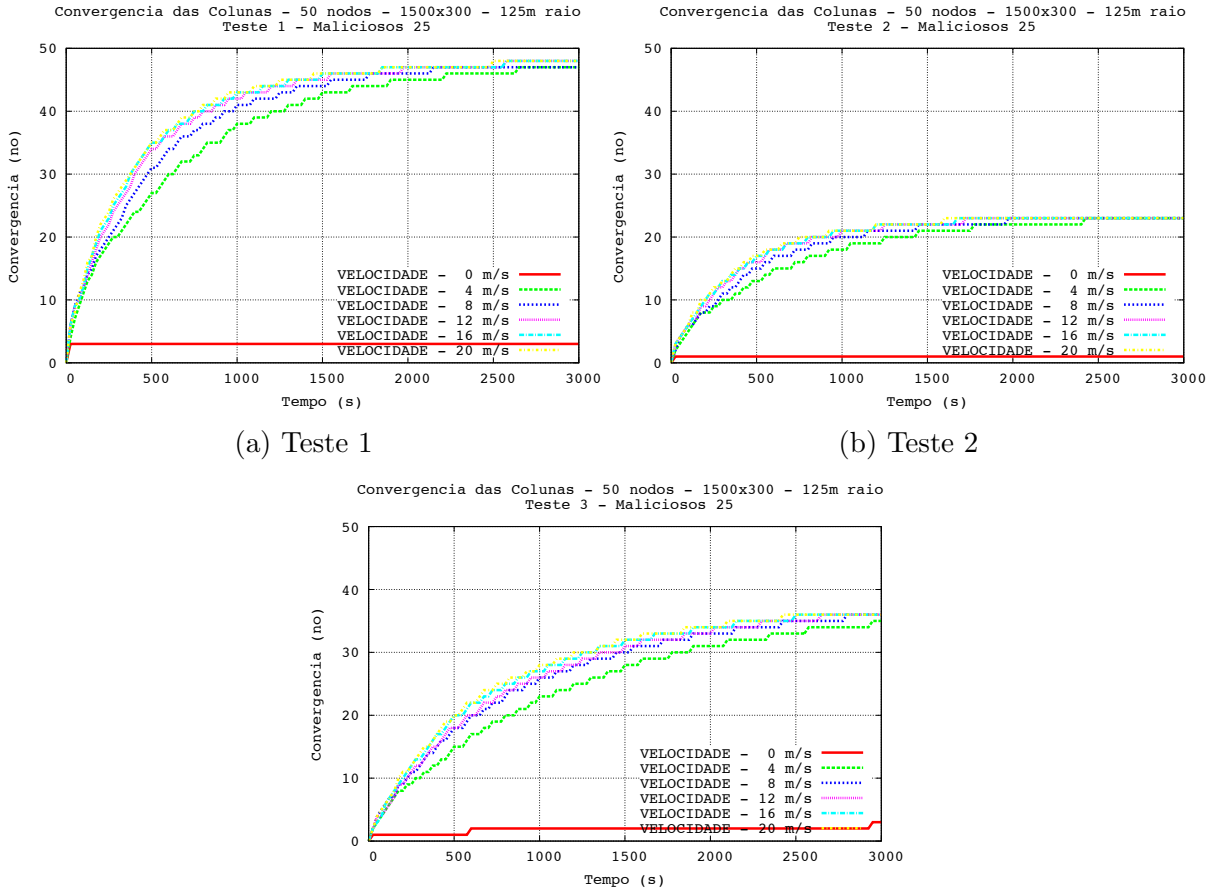


(c) Teste 3

Figura 5.10: Simulações de convergência da rede com cenário de 50 nós, sendo 25 nós maliciosos, dimensão de 1500 x 300 e raio de 125.

Através da Figura 5.10 é possível verificar as convergências de rede dos três testes no Cenário 4. O Teste 1 teve a convergência de aproximadamente 100%. Do mesmo modo que aconteceu no Cenário 3, o raio de 125 prejudica a troca de informações na velocidade 0 m/s, cujos nós ficam isolados uns dos outros.

A diferença de o Teste 1 (Figura 5.10a) e o Teste 3 (Figura 5.10c) é de 25%. Essa diferença é aceitável perto da quantidade de informação maliciosa, que chega a 50%.



(a) Teste 1

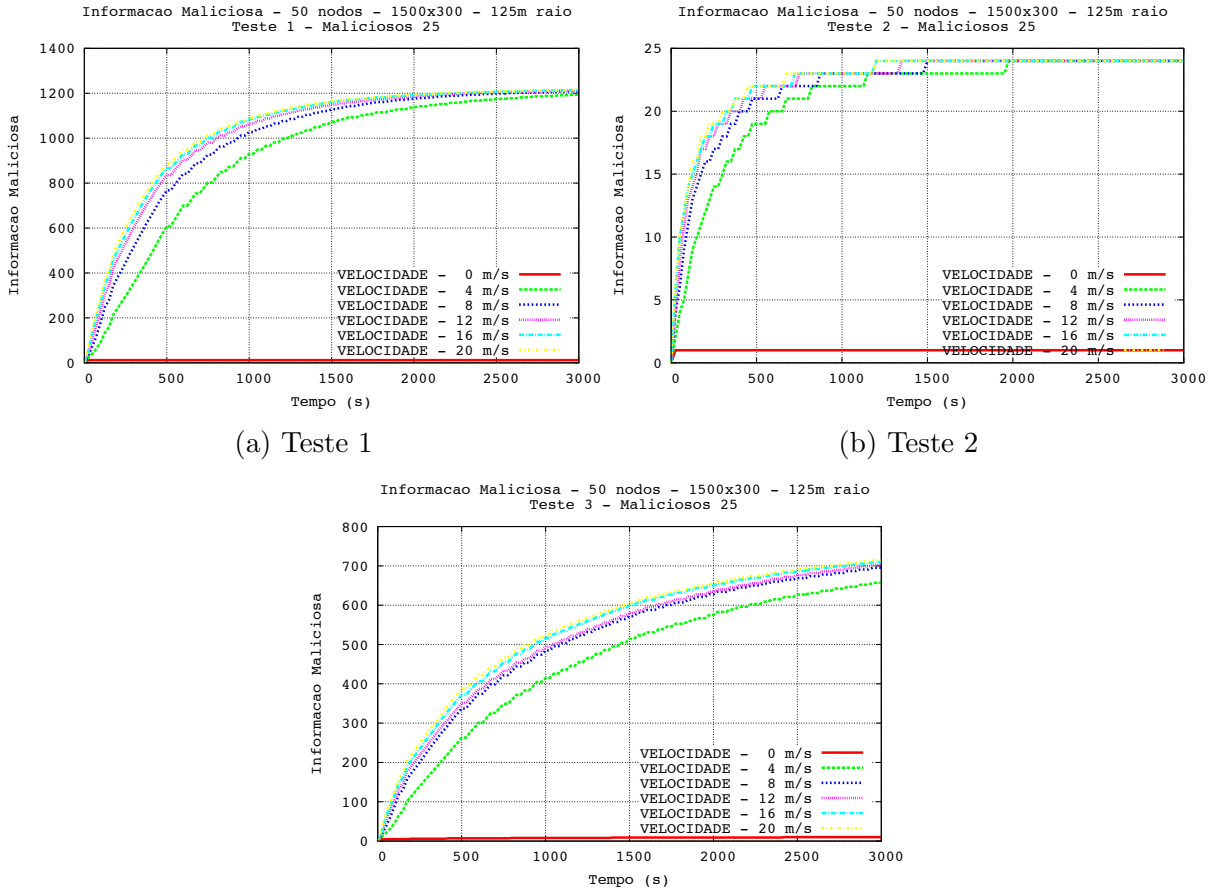
(b) Teste 2

(c) Teste 3

Figura 5.11: Simulações de convergência de cada nó com cenário de 50 nós, sendo 25 nós maliciosos, dimensão de 1500 x 300 e raio de 125.

Na Figura 5.11 é possível evidenciar que a convergência no Teste 2 é igual a quantidade de nós confiáveis da rede. Isso somente se existir mobilidade na rede. Também, na velocidade 0 m/s o TrustUm no Teste 3 faz com que troquem informações a fim de extrair o máximo de informações confiáveis de nós maliciosos.

Os resultados apresentados na Figura 5.11c demonstram que, mesmo nós maliciosos atingem a convergência. Todavia essas informações não são aproveitadas pelos demais. Por mais confiável que um nó seja, são as avaliações dos demais nós que garantem isso, além de quantificar as informações que serão trocadas.



(a) Teste 1

(b) Teste 2

(c) Teste 3

Figura 5.12: Simulações de propagação de informação maliciosa com cenário de 50 nós, sendo 5 nós maliciosos, dimensão de 1000 x 1000 e raio de 125.

A propagação de informação maliciosa apresentada na Figura 5.12 demostra a redução que o Teste 3 apresentou em relação o Teste 1. Tal diferença chega a 41% no final do teste.

Através da Tabela 5.6 é possível observar algumas características do Cálculo da Confiança. No exemplo, os nós maliciosos são os nós pares. Primeiramente os valores calculados para a Velocidade 0 são mais imprecisos que nas demais velocidades, todavia o Nó 5 conseguiu identificar alguns nós maliciosos, como os nós 26 e 30, por exemplo. Nas demais velocidades, a detecção é total, pois a convergência propicia isso.

	Velocidade 0		Velocidade 4		Velocidade 8		Velocidade 12		Velocidade 16		Velocidade 20	
	500	1500	500	1500	500	1500	500	1500	500	1500	500	1500
1	0.5	0.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5
2	0.5	0.5	-0.5	-1.7	-1.5	-1.6	-0.5	-1.6	-1.4	-1.5	-0.8	-1.6
3	0.5	0.5	1.8	1.5	0.4	1.5	1.3	1.3	1.5	1.5	1.6	1.7
4	0.5	0.5	-0.5	-0.5	-1.3	-1.4	-0.5	-1.7	-1.5	-1.5	-1.4	-1.3
5	1.1	1.2	1.0	1.8	1.5	1.5	1.0	1.5	1.5	1.6	1.4	1.5
6	0.5	0.5	-0.5	-0.5	-1.4	-1.4	-1.4	-1.3	-1.5	-1.5	-1.6	-1.4
7	0.5	0.5	1.5	1.5	1.3	1.5	1.4	1.5	1.5	1.4	1.3	1.6
8	0.5	0.5	-1.6	-1.6	-1.3	-1.4	-1.6	-1.6	-1.4	-1.4	-1.6	-1.5
9	0.5	0.5	1.8	1.8	1.4	1.5	1.3	1.5	1.6	1.6	1.4	1.6
10	0.5	0.5	-1.7	-1.7	-1.3	-1.5	-0.5	-1.6	-1.4	-1.5	-1.5	-1.5
11	0.5	0.5	1.8	1.7	0.5	1.5	1.5	1.5	1.6	1.5	1.8	1.7
12	0.5	0.5	0.5	-0.5	-1.3	-1.5	-1.5	-1.6	-1.5	-1.5	-1.4	-1.5
13	0.5	0.5	1.5	1.5	0.8	1.7	1.5	1.3	1.5	1.7	0.7	1.4
14	0.5	0.5	-1.5	-1.4	-1.4	-1.5	-1.3	-1.5	-1.6	-1.6	-0.5	-1.5
15	0.5	0.5	1.5	1.5	0.5	1.6	1.5	1.7	1.5	1.5	0.7	1.7
16	0.5	0.5	-0.6	-1.5	-1.4	-1.4	-1.4	-1.5	-1.4	-1.5	-1.8	-1.6
17	0.5	0.5	1.5	1.5	1.4	1.4	1.5	1.7	1.6	1.5	1.8	1.7
18	0.5	0.5	-0.5	-1.6	-1.4	-1.4	-1.5	-1.6	-0.5	-1.6	-0.5	-1.7
19	0.5	0.5	1.5	1.5	1.6	1.6	1.7	1.6	1.4	1.5	1.5	1.5
20	0.5	0.5	-1.1	-1.5	-1.3	-1.4	-1.5	-1.4	-1.5	-1.6	-1.5	-1.3
21	0.5	0.5	1.6	1.4	1.5	1.5	1.5	1.5	1.6	1.6	1.5	1.5
22	0.5	0.5	-1.7	-1.5	-1.3	-1.6	-1.5	-1.5	-1.4	-1.4	-1.5	-1.5
23	0.5	0.5	1.5	1.8	1.4	1.6	1.5	1.5	1.6	1.6	1.6	1.6
24	0.5	0.5	-1.7	-1.7	-1.5	-1.6	-0.6	-1.4	-1.5	-1.6	-1.8	-1.7
25	0.5	0.5	1.8	1.7	1.5	1.5	0.4	1.5	1.5	1.6	1.3	1.5
26	-1.0	-1.0	-1.5	-1.5	-1.4	-1.5	-1.4	-1.3	-0.5	-1.5	-0.4	-1.4
27	0.5	0.5	0.5	1.6	0.4	0.5	1.2	1.6	1.7	1.7	1.6	1.4
28	0.5	0.5	-0.5	-1.5	-1.4	-1.6	-1.2	-1.4	-1.4	-1.5	-1.4	-1.5
29	0.5	0.5	1.5	1.4	1.6	1.6	1.4	1.4	0.5	1.6	1.7	1.6
30	-0.6	-0.7	-0.5	-1.6	-1.4	-1.4	-1.7	-1.6	-1.5	-1.6	-1.4	-1.6
31	0.5	0.5	1.5	1.7	1.4	1.5	1.4	1.5	1.6	1.6	1.9	1.7
32	0.5	0.5	-1.5	-1.5	-0.3	-1.6	-0.5	-1.6	-0.4	-1.6	-1.7	-1.6
33	0.5	0.5	1.8	1.6	1.3	1.6	1.5	1.5	1.5	1.5	1.7	1.6
34	0.5	0.5	-0.5	-1.4	-1.4	-1.6	-0.5	-1.6	-1.5	-1.5	-1.4	-1.4
35	0.5	0.5	1.5	1.5	1.4	1.7	1.3	1.5	1.5	1.5	1.7	1.7
36	0.5	0.5	0.5	-1.8	-1.4	-1.5	-1.4	-1.4	-1.4	-1.5	-1.6	-1.6
37	0.5	0.5	1.4	1.3	1.4	1.6	0.5	1.6	1.5	1.6	1.4	1.5
38	0.5	0.5	-0.5	-1.5	-1.6	-1.6	-0.5	-1.6	-0.5	-1.6	-1.3	-1.6
39	0.5	0.5	1.2	1.6	0.8	1.5	1.5	1.5	1.3	1.5	1.7	1.7
40	-0.1	-0.0	-0.5	-1.6	-1.5	-1.7	-0.5	-1.2	-0.4	-1.5	-1.8	-1.7
41	1.2	1.2	1.5	1.5	1.7	1.7	1.4	1.5	1.5	1.5	1.6	1.6
42	-1.0	-1.0	-1.0	-1.7	-1.3	-1.6	-1.3	-1.4	-1.5	-1.6	-1.4	-1.4
43	0.5	0.5	1.5	1.5	1.4	1.5	1.3	1.5	1.6	1.6	1.3	1.6
44	0.5	0.5	-1.7	-1.4	-1.4	-1.4	-1.2	-1.5	-1.3	-1.5	-1.4	-1.6
45	0.5	0.5	1.5	1.7	1.5	1.5	1.6	1.8	1.5	1.6	1.7	1.5
46	-1.0	-1.1	-1.7	-1.5	-0.4	-1.6	-0.4	-1.4	-1.5	-1.5	-1.4	-1.4
47	0.5	0.5	1.5	1.5	0.5	1.6	1.5	1.5	1.7	1.7	1.6	1.4
48	0.5	0.5	-1.5	-1.3	-1.4	-1.5	-0.5	-1.5	-1.5	-1.5	-1.6	-1.4
49	0.5	0.5	1.5	1.4	0.4	0.4	0.4	0.4	1.6	1.6	1.5	1.5
50	0.5	0.5	-1.5	-1.4	-1.4	-1.5	-1.4	-1.4	-1.6	-1.6	-0.5	-1.7

Tabela 5.6: Cálculo de Confiança do nó 5 nos tempos 500 e 1500 do Cenário 4 do Teste 3

5.2.5 Exemplo do Cálculo de Confiança no Cenário 4

Este exemplo consiste no Cálculo de Confiança do nó 5 sobre o nó 11 na Velocidade 12 m/s no tempo 1500s. Através da Tabela 6.1, presente no Apêndice A, tem-se a Matriz de Confiança do nó 5 no tempo 1500s do Cenário 4. Os valores dos pesos p_1 e p_2 utilizados são 1 (um). Inicialmente é necessário calcular as informações atribuídas pelos demais nós ao nó 11. Para isso, utiliza-se a primeira parte da Fórmula 4.5.

Através da varredura da coluna 11, aplicando o somatório a cada resultado gerado, multiplicando a confiança ao tempo relativo, tem-se o valor de 0.5.

Para a segunda parte da Fórmula 4.5 basta multiplicar a informação do nó 5 sobre o nó 11 com o peso p_2. Esta informação está na Tabela 6.1 linha 5 coluna 11. O valor gerado é 1.0.

Para finalizar, faz-se a soma dos valores gerados para chegar ao resultado final. O

valor final do Cálculo de Confiança do nó 4 sobre o nó 11 é 1.5. Caso o nó calculado fosse não confiável o valor de confiança tenderia a valores negativos.

O valor gerado será enviado a aplicação que solicitou o cálculo e cabe a ela considerar ou não a informação como confiável. É a aplicação que determina o nível de corte entre confiável e não confiável e varia de acordo com cada aplicação. Para o modelo, um resultado positivo é considerado confiável e um valor negativo é considerado como não confiável.

5.2.6 Análise

Os cenários foram construídos para modelar situações extremas onde os testes poderiam apresentar resultados incoerentes ou falhos. As dimensões, quantidade de nós, quantidade de nós maliciosos, raios de cobertura e as velocidades foram escolhidos uma vez que, além de serem comuns na maioria das simulações em diversos outros estudos, maximizam as possibilidades de resultados, sejam pela mobilidade e alcance de informações maliciosas.

Analisando os resultados apresentados pelos três testes, conclui-se que o Teste 3 tem o melhor resultado: convergência da rede X propagação de informação maliciosa. No cenário 1 a diferença entre o Teste 1 e o Teste 3 foi de 33%, no cenário 2 a diferença foi de 64%, no cenário 3 a diferença foi de 76% e no cenário 4 a diferença foi de 41%. Esse resultado reforça o comprometimento do modelo em selecionar as informações de acordo com o Status de Confiança de cada nó. Ainda, os resultados apresentados pelas Matrizes de Confiança confirmam que o Cálculo de Confiança atinge o objetivo em qualquer nó da rede, tendo pelo menos um contato com o nó desejado, seja esse contato por qualquer nó conhecido.

Também é necessário observar que os testes não simularam a inclusão e remoção de nós da rede. Tal modificação não impacta no desempenho do modelo, e também não impacta a formação dos valores do Cálculo de Confiança.

CAPÍTULO 6

CONCLUSÃO

O Modelo de Confiança proposto tem o objetivo de calcular a confiança entre quaisquer dois nós em uma rede Ad Hoc. Para isso basta somente um nó trocar informações com outro que teve contato com o nó desejado. Com isso, é possível detectar nós maliciosos, e por consequência, gerar uma confiabilidade na rede.

O modelo esta dividido em três etapas: Monitoramento de Vizinhos, Troca de Informações e Cálculo de Confiança. O Monitoramento de Vizinhos é responsável pela avaliação de um nó em seu vizinho. Através de testes realizados é possível identificar se o vizinho é confiável ou não, atribuindo um valor de 1 (um) para confiável e -1 (menos um) para não confiável.

A segunda etapa é responsável pela troca de informações coletadas de acordo com o tempo e a mobilidade. Nesta etapa utiliza-se a Teoria de Jogos para gerenciar as trocas. Através do Jogo do Ultimato os nós utilizam seus Status de Confianças, e através do resultado trocam a quantidade relativa à porcentagem gerada. As informações enviadas são escolhidas aleatoriamente, respeitando as quantidades previstas. Um nó com Status de Confiança alto comparado ao outro, receberá menos informação, uma vez que suas informações são mais confiáveis que as do outro. O contrário também acontece.

O Cálculo de Confiança utiliza de todas as informações coletadas na Matriz de Confiança ao longo de um intervalo de tempo, bem como os pesos atribuídos a informação própria e aos tempos, gerando o valor de confiança desejado. Esse cálculo leva em consideração os tempos em que as informações foram trocadas como também leva em conta de quem é a informação. Os resultados são gerados em valor absoluto, porém é possível normalizá-lo no intervalo [-1,1].

Os resultados obtidos mostram que a utilização do TrustUm acarreta uma diminuição entre 30% e 70% nas informações maliciosas trocadas entre nós dependendo do cenário e

das características de cada rede. Esses resultados demonstram um grande passo na criação de um ambiente livre de nós maliciosos, uma vez que se tornou possível identificá-los e quantificar essa confiança, e com isso é possível fazer um isolamento, ou uma quarentena até que o comportamento volte ao normal.

BIBLIOGRAFIA

[1] W.J. Adams e IV Davis, N.J. Toward a decentralized trust-based access control system for dynamic collaboration. *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics*, páginas 317–324, junho de 2005.

[2] Omer Alper e Ron Nickel. Nash bargaining as a military decision tool: An example from base closure. *Military Operations Research*, 16(2):19–30, 2011.

[3] R Axelrod e WD Hamilton. The evolution of cooperation. *Science*, 211(4489):1390–1396, 1981.

[4] Nicholas Bardsley. Dictator game giving: altruism or artefact? *Experimental Economics*, 11(2):122–133, 2007.

[5] Vittorio Bilò, Michele Flammini, Giovanna Melideo, e Luca Moscardelli. On nash equilibria for multicast transmissions in ad-hoc wireless networks. Rudolf Fleischer e Gerhard Trippen, editors, *Algorithms and Computation*, volume 3341 of *Lecture Notes in Computer Science*, páginas 755–770. Springer Berlin / Heidelberg, 2005.

[6] Gary E. Bolton, Elena Katok, e Rami Zwick. Dictator game giving: Rules of fairness versus acts of kindness. *International Journal of Game Theory*, 27:269–299, 1998. 10.1007/s001820050072.

[7] Phillip Bonacich. Power and centrality: A family of measures. *American Journal of Sociology*, 92(5):1170–1182, março de 1987.

[8] Gary Bornstein e Ilan Yaniv. Individual and group behavior in the ultimatum game: Are groups more rational players. *Experimental Economics*, 1(1):101–108, junho de 1998.

[9] Sonja Buchegger e Jean-Yves Le Boudec. Performance analysis of the confidant protocol. *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, MobiHoc '02, páginas 226–236. ACM, New York, NY, USA, 2002.

[10] Jin-Hee Cho, A. Swami, e Ing-Ray Chen. A survey on trust management for mobile ad hoc networks. *Communications Surveys Tutorials, IEEE*, 13(abril):562–583, quarter de 2011.

[11] Marco Conti, Silvia Giordano, Enrico Gregori, e Stephan Olariu. Equilibrium analysis of packet forwarding strategies in wireless ad hoc networks - the static case. *Personal Wireless Communications*, volume 2775 of *Lecture Notes in Computer Science*, páginas 776–789. Springer Berlin / Heidelberg, 2003.

[12] Rachel Croson e Nancy Buchan. Gender and culture: International experimental evidence from trust games. *The American Economic Review*, 89(2):386–391, maio de 1999.

[13] Bolton Gary E. e Zwick Rami. Anonymity versus punishment in ultimatum bargaining. *Games and Economic Behavior*, 10(1):95–121, julho de 1995.

[14] Mark Felegyhazi, Jean-Pierre Hubaux, e Levente Buttyan. Nash equilibria of packet forwarding strategies in wireless ad hoc networks. *IEEE Transactions on Mobile Computing*, 5(5):463–476, maio de 2006.

[15] D. Fudenberg e J. Tirole. *Game Theory*, volume 1 of *MIT Press Books*. MIT Press, 1991.

[16] John Gale, Kenneth G. Binmore, e Larry Samuelson. Learning to be imperfect: The ultimatum game. *Games and Economic Behavior*, 8(1):56–90, 1995.

[17] Katarina Gospic, Erik Mohlin, Peter Fransson, Predrag Petrovic, Magnus Johannesson, e Martin Ingvar. Limbic justice - amygdala involvement in immediate rejection in the ultimatum game. *PLoS Biology*, 9(5):e1001054, maio de 2011.

[18] Werner Guth, Rolf Schmittberger, e Bernd Schwarze. An experimental analysis of ultimatum bargaining. *Journal of Economic Behavior & Organization*, 3(4):367–388, dezembro de 1982.

[19] Russell Hardin. The Street-Level Epistemology of Trust. *Politics & Society*, 21(4):505–529, dezembro de 1993.

[20] John C. Harsanyi. Games with incomplete information played by bayesian players, i-iii. *Management Science*, 50:1804–1817, dezembro de 2004.

[21] Shaun Hargreaves Heap e Yanis. Varoufakis. *Game theory : a critical text / Shaun P. Hargreaves Heap & Yanis Varoufakis.* Routledge, New York :, 2nd ed. edition, 2004.

[22] Dirk Helbing e Sergi Lozano. Phase transitions to cooperation in the prisoner's dilemma. *Physical Review E*, 81:057102, maio de 2010.

[23] Juan José Jaramillo e R. Srikant. A game theory based reputation mechanism to incentivize cooperation in wireless ad hoc networks. *Ad Hoc Networks*, 8(4):416–429, junho de 2010.

[24] Catholijn Jonker e Jan Treur. Formal analysis of models for the dynamics of trust based on experiences. Francisco Garijo e Magnus Boman, editors, *Multi-Agent System Engineering*, volume 1647 of *Lecture Notes in Computer Science*, páginas 221–231. Springer Berlin / Heidelberg, 1999.

[25] Harvey S. James Jr. The trust paradox: a survey of economic inquiries into the nature of trust and trustworthiness. *Journal of Economic Behavior & Organization*, 47(3):291–307, 2002.

[26] John F. Nash Jr. Equilibrium Points in n-Person Games. *PNAS. Proceedings of the National Academy of Sciences of the USA*, 36(1):48–49, janeiro de 1950.

[27] K. Komathy e P. Narayanasamy. Trust-based evolutionary game model assisting aodv routing against selfishness. *Journal of Network and Computer Application*, 31(4):446–471, 2008.

[28] Ruidong Li, Jie Li, Peng Liu, e Hsiao-Hwa Chen. An objective trust management framework for mobile ad hoc networks. *Vehicular Technology Conference*, páginas 56–60, abril de 2007.

[29] Yu Liu, Cristina Comaniciu, e Hong Man. A bayesian game approach for intrusion detection in wireless ad hoc networks. *Proceeding from the 2006 workshop on Game theory for communications and networks*, GameNets '06, New York, NY, USA, 2006. ACM.

[30] Carlos Andrey Maia, Ricardo Luders, Rafael Santos Mendes, e Laurent Hardouin. Estratégias de controle por modelo de referência de sistemas a eventos discretos max-plus lineares. *Revista Controle & Automação*, 16:263–278, setembro de 2005.

[31] Antonella Marchetti, Ilaria Castelli, Katia M. Harlé, e Alan G. Sanfey. Expectations and outcome: The role of proposer features in the ultimatum game. *Journal of Economic Psychology*, 32(3):446–449, junho de 2011.

[32] Sergio Marti e Hector Garcia-Molina. Taxonomy of trust: Categorizing p2p reputation systems. *Computer Networks*, 50(4):472–484, 2006.

[33] D. Harrison McKnight e Norman L. Chervany. What is trust ? a conceptual analysis and an interdisciplinary model. *Proceedings of the 2000 Americas Conference on Information Systems*, volume 346, agosto de 2000.

[34] Marcela Mejia, Néstor Peña, Jose L. Muñoz, Oscar Esparza, e Marco a. Alzate. A game theoretic trust model for on-line distributed evolution of cooperation in manets. *Journal of Network and Computer Applications*, 34(1):39–51, janeiro de 2011.

[35] Pietro Michiardi e Refik Molva. Game theoretic analysis of security in mobile ad hoc networks. Relatório Técnico EURECOM+981, Eurecom, abril de 2002.

[36] Roger B Myerson. *Game Theory: Analysis of Conflict*. Harvard University Press, 1991.

[37] John F Nash. The bargaining problem. *Econometrica*, 18(2):155–162, abril de 1950.

[38] Martin A. Nowak, Karen M. Page, e Karl Sigmund. Fairness versus reason in the ultimatum game. *Science*, 289(5485):1773–1775, 2000.

[39] The network simulator ns-2. http://www.isi.edu/nsnam/ns/, 1995.

[40] Simon Parsons e Michael Wooldridge. Game theory and decision theory in multi-agent systems. *Autonomous Agents and Multi-Agent Systems*, 5:243–254, 2002. 10.1023/A:1015575522401.

[41] Matja Perc e Attila Szolnoki. Social diversity and promotion of cooperation in the spatial prisoner's dilemma game. *Physical Review E*, 77:011904, janeiro de 2008.

[42] Charles E. Perkins. *Ad Hoc Networking*. Addison-Wesley Professional, 1 edition, 2008.

[43] Emmanuel M. Pothos, Gavin Perry, Philip J. Corr, Mervin R. Matthew, e Jerome R. Busemeyer. Understanding cooperation in the prisoner's dilemma game. *Personality and Individual Differences*, 51(3):210–215, 2011.

[44] Y. Qiu e P. Marbach. Bandwidth allocation in ad hoc networks: a price-based approach. *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 2, páginas 797–807, março de 2003.

[45] Eric Rasmusen. *Readings in Games and Information*. Wiley-Blackwell, 2001.

[46] Mary Rigdon, Keiko Ishii, Motoki Watabe, e Shinobu Kitayama. Minimal social cues in the dictator game. *Journal of Economic Psychology*, 30(3):358–367, 2009.

[47] Julian B. Rotter. Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, 35:1–7, 1980.

[48] Alan G. Sanfey, James K. Rilling, Jessica A. Aronson, Leigh E. Nystrom, e Jonathan D. Cohen. The neural basis of economic decision-making in the ultimatum game. *Science*, 300(5626):1755–1758, 2003.

[49] Roberto da Silva e Gustavo Adolfo Kellerman. Analyzing the payoff of a heterogeneous population in the ultimatum game. *Brazilian Journal of Physics*, 37:1206–1211, dezembro de 2007.

[50] Vikram Srinivasan, Pavan Nuggehalli, C.F. Chiasserini, e R.R. Rao. Cooperation in wireless ad hoc networks. *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 2, páginas 808–817. IEEE, março de 2003.

[51] V. Srivastava, J. Neel, A.B. Mackenzie, R. Menon, L.A. Dasilva, J.E. Hicks, J.H. Reed, e R.P. Gilles. Using game theory to analyze wireless ad hoc networks. *Communications Surveys and Tutorials, IEEE*, 7(4):46–56, quarter de 2005.

[52] Richard H. Thaler. Anomalies: The ultimatum game. *The Journal of Economic Perspectives*, 2(abril):195–206, 1988.

[53] A. Urpi, M. Bonuccelli, e Silvia Giordano. Modelling cooperation in mobile ad hoc networks: a formal description of selfishness. *WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, páginas 10, Sophia Antipolis, France, 2003.

[54] J Von Neumann e O Morgenstern. *Theory of games and economic behavior*, volume 37. Princeton University Press, 1947.

[55] Paul J. Zak, Robert Kurzban, Sheila Ahmadi, Ronald S. Swerdloff, Jang Park, Levan Efremidze, Karen Redwine, Karla Morgan, e William Matzner. Testosterone administration decreases generosity in the ultimatum game. *PLoS ONE*, 4(12):e8330, dezembro de 2009.

[56] Guopeng Zhang, Kun Yang, e Hsiao-Hwa Chen. Resource allocation for wireless cooperative networks: a unified cooperative bargaining game theoretic framework. *Wireless Communications, IEEE*, 19(2):38–43, abril de 2012.

[57] Yongguang Zhang e Wenke Lee. Intrusion detection in wireless ad-hoc networks. *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, páginas 275–283, New York, NY, USA, 2000. ACM.

[58] Zhaoyang Zhang, Jing Shi, Hsiao-Hwa Chen, M. Guizani, e Peiliang Qiu. A cooperation strategy based on nash bargaining solution in cooperative relay networks. *Vehicular Technology, IEEE Transactions on*, 57(4):2570–2577, julho de 2008.

[59] Shanshan Zheng, Tao Jiang, e John S. Baras. Exploiting trust relations for nash equilibrium efficiency in ad hoc networks. *IEEE International Conference on Communications (ICC), 2011*, páginas 1–5, junho de 2011.

[60] Charikleia Zouridaki, Brian L. Mark, Marek Hejmo, e Roshan K. Thomas. Robust cooperative trust establishment for manets. *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, SASN '06, páginas 23–34, New York, NY, USA, 2006. ACM.

APÊNDICE A

Este apêndice apresenta a Matriz de Confiança do nó 5 no tempo 1500s do Cenário 4. Essa tabela é necessária para o Cálculo da Confiança, uma vez que serve de consulta para cada etapa do modelo.

Na Tabela 6.1, cada campo contém uma tupla com o valor da confiança adquirido pela Troca de Informações e o tempo em que essa troca foi realizada.

	1		2		3		4		5		6		7		8		9		10		11		12		13
1	1	0.00	0	903.00	1	903.00	-1	903.00	0	210.03	0	0.00	1	903.00	-1	903.00	1	903.00	-1	903.00	0	210.03	1	210.03	1	210.03
2	0	0.00	1	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
3	0	0.00	0	136.00	1	0.00	0	136.00	1	1225.03	0	0.00	1	1225.03	-1	1225.03	1	136.00	0	0.00	0	136.00	0	136.00	0	136.00
4	0	0.00	0	0.00	0	0.00	1	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
5	1	0.00	-1	0.00	1	0.00	-1	0.00	1	0.00	-1	0.00	0	0.00	-1	0.00	1	0.00	-1	0.00	1	0.00	1	0.00	1	0.00
6	0	0.00	0	0.00	0	0.00	0	0.00	0	378.04	1	0.00	0	0.00	0	36.04	0	36.04	0	0.00	0	36.04	0	0.00	0	36.04
7	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
8	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	28.02	0	28.02	1	28.02	0	28.02	0	28.02	0	28.02	0	0.00	0	28.02
9	0	0.00	-1	171.01	0	0.00	-1	171.01	1	171.01	0	0.00	0	0.00	0	0.00	1	0.00	0	0.00	1	171.01	0	171.01	0	171.01
10	0	0.00	0	406.03	0	0.00	0	0.00	0	406.03	0	0.00	0	0.00	0	120.02	0	120.02	1	0.00	0	120.02	0	0.00	0	120.02
11	0	0.00	-1	231.04	0	0.00	0	231.04	0	231.04	0	0.00	0	231.04	0	0.00	1	231.04	0	0.00	1	231.04	1	231.04	1	231.04
12	0	0.00	0	0.00	0	10.01	0	0.00	1	10.01	0	10.01	0	10.01	0	10.01	0	10.01	0	10.01	0	10.01	1	0.00	0	10.01
13	0	0.00	0	0.00	0	120.02	0	0.00	1	120.02	-1	120.02	0	120.02	-1	120.02	0	120.02	0	120.02	1	120.02	0	0.00	1	120.02
14	0	0.00	-1	1431.01	0	120.02	0	0.00	0	120.02	-1	1431.01	1	1431.01	0	120.02	1	120.02	0	1431.01	1	120.02	1	1431.01	0	120.02
15	0	0.00	-1	1081.03	1	1081.03	-1	1081.03	1	406.03	0	36.03	1	1081.03	-1	1081.03	1	1081.03	0	1081.03	1	406.03	1	406.03	1	666.01
16	0	0.00	0	780.04	1	780.04	-1	780.04	0	105.00	0	105.00	1	780.04	-1	780.04	1	780.04	-1	780.04	1	105.00	0	0.00	0	105.00
17	0	0.00	-1	780.01	1	780.01	-1	780.01	0	0.00	0	0.00	1	780.01	0	780.01	1	780.01	-1	780.01	0	0.00	0	0.00	0	741.04
18	0	0.00	-1	946.02	1	946.02	0	946.02	1	300.03	0	105.03	1	946.02	-1	946.02	1	946.02	0	946.02	1	300.03	1	300.03	1	595.03
19	0	0.00	-1	210.04	0	0.00	0	210.04	0	210.04	0	0.00	1	210.04	0	0.00	1	210.04	0	0.00	1	210.04	0	210.04	0	210.04
20	0	0.00	-1	561.00	1	561.00	0	0.00	0	120.02	0	120.02	1	120.02	0	120.02	1	120.02	0	120.02	1	120.02	0	0.00	1	561.00
21	0	0.00	0	0.00	0	0.00	0	0.00	0	105.03	-1	105.03	0	105.03	0	105.03	1	105.03	0	105.03	1	105.03	0	0.00	1	105.03
22	0	0.00	0	136.00	0	0.00	0	136.00	1	1326.02	0	0.00	1	1326.02	-1	1326.02	1	136.00	0	0.00	1	136.00	0	136.00	0	136.00
23	0	0.00	-1	561.04	1	561.04	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	561.04
24	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
25	0	0.00	-1	1081.03	1	1081.03	-1	1081.03	1	91.00	0	91.00	1	1081.03	-1	1081.03	1	1081.03	0	1081.03	1	91.00	0	0.00	0	91.00
26	0	0.00	0	378.04	0	105.03	-1	378.04	1	1128.00	0	105.03	1	1128.00	-1	1128.00	0	378.04	-1	105.03	1	378.04	1	378.04	1	378.04
27	0	0.00	-1	903.00	0	903.00	-1	903.00	0	0.00	0	0.00	1	903.00	-1	903.00	1	903.00	-1	903.00	0	0.00	0	0.00	0	0.00
28	0	0.00	0	0.00	0	91.02	0	0.00	0	91.02	0	91.02	0	91.02	0	91.02	1	91.02	0	91.02	1	91.02	0	0.00	0	91.02
29	0	0.00	-1	561.04	1	561.04	0	406.02	1	1128.02	0	0.00	1	1128.02	-1	1128.02	0	406.02	-1	1128.02	1	406.02	1	406.02	0	561.04
30	0	0.00	-1	666.01	0	666.01	-1	378.00	0	378.00	0	0.00	1	378.00	0	0.00	0	378.00	0	0.00	1	378.00	0	378.00	1	666.01
31	0	0.00	0	741.04	1	741.04	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	741.04
32	0	0.00	-1	820.00	1	820.00	-1	820.00	0	0.00	0	0.00	1	820.00	-1	820.00	0	820.00	-1	820.00	0	0.00	0	0.00	0	741.03
33	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
34	0	0.00	-1	561.03	1	561.03	-1	406.04	1	406.04	0	45.04	1	406.04	-1	406.04	1	406.04	-1	45.04	1	406.04	0	406.04	1	406.04
35	0	0.00	-1	741.04	1	741.04	0	0.00	1	105.03	0	105.03	0	105.03	-1	105.03	0	105.03	0	105.03	0	105.03	0	0.00	0	105.03
36	0	0.00	0	0.00	0	0.00	0	0.00	1	1326.02	0	0.00	1	1326.02	-1	1326.02	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
37	0	0.00	-1	946.02	1	946.02	-1	946.02	0	0.00	0	0.00	1	946.02	-1	946.02	1	946.02	-1	946.02	0	0.00	0	0.00	1	561.00
38	0	0.00	0	666.02	0	666.02	-1	406.03	1	406.03	-1	66.03	1	406.03	-1	406.03	1	406.03	0	66.03	1	406.03	0	406.03	0	666.02
39	0	0.00	-1	946.01	1	946.01	-1	946.01	0	120.03	0	120.03	1	946.01	-1	946.01	1	946.01	-1	946.01	0	120.03	0	0.00	0	435.01
40	0	0.00	-1	1431.00	0	0.00	0	190.02	0	190.02	-1	1431.00	1	1431.00	0	0.00	1	190.02	-1	1431.00	1	190.02	0	1431.00	0	190.02
41	0	0.00	-1	820.00	1	820.00	-1	820.00	1	1378.01	-1	36.03	1	1378.01	-1	1378.01	1	820.00	0	820.00	0	36.03	0	0.00	1	741.03
42	0	0.00	0	0.00	0	105.00	0	0.00	1	105.00	0	105.00	0	105.00	-1	105.00	0	105.00	0	105.00	0	105.00	0	0.00	1	105.00
43	0	0.00	0	171.02	0	0.00	0	171.02	0	171.02	0	0.00	1	171.02	0	0.00	0	171.02	0	0.00	0	171.02	0	171.02	0	171.02
44	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
45	0	0.00	-1	861.00	1	861.00	-1	861.00	0	0.00	0	0.00	1	861.00	-1	861.00	1	861.00	-1	861.00	0	0.00	0	0.00	0	0.00
46	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
47	0	0.00	-1	528.01	0	528.01	0	0.00	1	1225.02	-1	36.03	1	1225.02	-1	1225.02	0	36.03	0	36.03	0	36.03	0	0.00	0	36.03
48	0	0.00	0	276.02	0	0.00	-1	276.02	0	276.02	0	0.00	1	276.02	0	0.00	1	276.02	0	0.00	1	276.02	1	276.02	0	276.02
49	0	0.00	-1	903.01	1	903.01	-1	903.01	0	300.03	0	0.00	1	903.01	-1	903.01	0	903.01	-1	903.01	1	300.03	0	300.03	0	300.03
50	0	0.00	-1	990.01	0	990.01	-1	990.01	0	120.02	0	120.02	1	990.01	-1	990.01	0	990.01	-1	990.01	0	120.02	0	0.00	1	120.02

Tabela 6.1: Matriz de Confiança do nó 5 no tempo 1500 do Cenário 4

		14		15		16		17		18		19		20		21		22		23		24		25		26
1	1	903.00	1	903.00	0	210.03	1	210.03	1	903.00	0	903.00	1	903.00	0	210.03	0	903.00	0	903.00	1	210.03	0	210.03	0	0.00
2	0	0.00	0	0.00	0	300.04	0	0.00	0	0.00	0	1081.03	0	0.00	0	300.04	0	300.04	0	0.00	0	0.00	0	0.00	0	0.00
3	1	1225.03	1	1225.03	1	136.00	1	136.00	1	1225.03	0	136.00	1	1225.03	1	1225.03	1	1225.03	0	0.00	1	1225.03	1	1225.03	1	1225.03
4	0	0.00	0	0.00	0	0.00	0	0.00	0	1176.02	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
5	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00	0	0.00	1	0.00	1	0.00
6	0	0.00	0	0.00	0	378.04	0	0.00	0	1225.02	0	36.04	0	0.00	0	378.04	0	1225.02	0	0.00	0	1225.02	0	36.04	0	0.00
7	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
8	0	0.00	0	28.02	0	406.00	0	0.00	0	0.00	0	946.02	0	0.00	0	406.00	0	406.00	0	28.02	0	0.00	0	28.02	0	0.00
9	0	0.00	0	0.00	1	171.01	1	171.01	0	0.00	1	171.01	0	0.00	1	171.01	1	171.01	0	0.00	0	0.00	0	171.01	0	0.00
10	0	0.00	0	0.00	0	406.03	0	0.00	0	0.00	0	120.02	0	435.01	0	406.03	0	435.01	0	435.01	0	0.00	0	120.02	0	435.01
11	0	0.00	0	0.00	1	231.04	1	231.04	0	0.00	1	231.04	1	231.04	1	231.04	1	231.04	0	0.00	1	231.04	1	231.04	0	0.00
12	0	0.00	1	10.01	0	10.01	0	0.00	0	0.00	0	10.01	0	0.00	0	10.01	0	10.01	0	10.01	0	10.01	0	10.01	0	0.00
13	0	0.00	1	120.02	1	120.02	0	0.00	0	0.00	0	120.02	0	0.00	1	120.02	0	120.02	0	120.02	0	120.02	0	120.02	0	0.00
14	1	1431.01	1	120.02	1	120.02	1	1431.01	1	1431.01	0	120.02	1	1431.01	1	1431.01	1	1431.01	1	1431.01	1	120.02	0	120.02	0	0.00
15	1	1081.03	1	1081.03	1	666.01	1	406.03	1	1081.03	1	1081.03	1	1081.03	1	666.01	1	1081.03	1	1081.03	1	666.01	0	666.01	0	666.01
16	1	780.04	1	780.04	1	105.00	0	0.00	1	780.04	1	780.04	1	780.04	0	105.00	1	780.04	1	780.04	1	105.00	0	105.00	0	0.00
17	1	780.01	1	780.01	1	741.04	1	0.00	1	780.01	1	780.01	1	780.01	1	741.04	1	780.01	1	780.01	1	741.04	1	741.04	1	741.04
18	1	946.02	1	946.02	1	595.03	1	300.03	1	946.02	1	946.02	1	946.02	1	595.03	1	946.02	1	946.02	0	595.03	1	595.03	1	595.03
19	0	0.00	0	0.00	1	210.04	0	210.04	0	0.00	1	210.04	0	210.04	1	210.04	1	210.04	0	0.00	1	210.04	1	210.04	0	0.00
20	0	0.00	1	120.02	1	561.00	0	0.00	0	0.00	0	561.00	1	561.00	0	561.00	1	561.00	1	561.00	1	561.00	0	561.00	1	561.00
21	0	0.00	0	105.03	0	105.03	0	0.00	0	0.00	0	105.03	0	0.00	1	105.03	1	105.03	0	105.03	0	105.03	1	105.03	0	0.00
22	1	1326.02	1	1326.02	0	136.00	0	136.00	1	1326.02	0	136.00	1	1326.02	1	136.00	1	1326.02	0	0.00	1	1326.02	1	1326.02	1	1326.02
23	0	0.00	0	0.00	1	561.04	0	0.00	0	0.00	1	561.04	1	561.04	0	561.04	1	561.04	1	561.04	1	561.04	0	561.04	0	561.04
24	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	0.00	0	0.00	0	0.00
25	0	1081.03	0	1081.03	0	91.00	0	0.00	1	1081.03	1	1081.03	1	1081.03	1	91.00	1	1081.03	1	1081.03	1	91.00	1	91.00	0	0.00
26	1	1128.00	1	1128.00	1	378.04	1	378.04	1	1128.00	0	378.04	1	1128.00	1	1128.00	1	1128.00	0	105.03	1	1128.00	0	1128.00	1	1128.00
27	1	903.00	1	903.00	1	630.01	0	0.00	1	903.00	1	903.00	1	903.00	1	630.01	1	903.00	1	903.00	1	630.01	1	630.01	1	630.01
28	0	0.00	1	91.02	1	91.02	0	0.00	0	0.00	1	91.02	0	0.00	0	91.02	0	91.02	1	91.02	1	91.02	0	91.02	0	0.00
29	1	1128.02	1	1128.02	1	561.04	1	406.02	1	1128.02	0	561.04	1	1128.02	0	1128.02	1	1128.02	0	561.04	1	1128.02	1	1128.02	0	1128.02
30	0	0.00	0	0.00	0	666.01	1	378.00	0	0.00	1	666.01	0	666.01	1	666.01	1	666.01	1	666.01	1	666.01	1	666.01	1	666.01
31	0	0.00	0	0.00	1	741.04	0	0.00	0	0.00	0	741.04	1	741.04	1	741.04	1	741.04	1	741.04	1	741.04	0	741.04	1	741.04
32	0	820.00	1	820.00	1	741.03	0	0.00	1	820.00	0	820.00	1	820.00	1	741.03	1	820.00	1	820.00	1	741.03	0	741.03	1	741.03
33	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
34	0	0.00	1	45.04	0	561.03	1	406.04	0	0.00	1	561.03	1	561.03	1	561.03	1	561.03	1	561.03	1	561.03	1	561.03	1	561.03
35	0	0.00	0	105.03	1	741.04	0	0.00	0	0.00	1	741.04	1	741.04	1	741.04	1	741.04	1	741.04	1	741.04	1	741.04	1	741.04
36	1	1326.02	1	1326.02	0	0.00	0	0.00	1	1326.02	0	0.00	0	1326.02	1	1326.02	1	1326.02	0	0.00	1	1326.02	0	1326.02	1	1326.02
37	1	946.02	1	946.02	1	561.00	0	0.00	0	946.02	1	946.02	1	946.02	1	561.00	1	946.02	1	946.02	1	561.00	0	561.00	1	561.00
38	0	0.00	1	66.03	0	666.02	1	406.03	0	0.00	1	666.02	1	666.02	1	666.02	0	666.02	1	666.02	1	666.02	0	666.02	0	666.02
39	1	946.01	1	946.01	1	435.01	0	0.00	1	946.01	1	946.01	1	946.01	1	435.01	0	946.01	1	946.01	1	435.01	1	435.01	1	435.01
40	1	1431.00	0	0.00	1	190.02	1	1431.00	1	1431.00	1	190.02	1	1431.00	1	1431.00	1	1431.00	1	1431.00	1	190.02	1	190.02	0	0.00
41	1	1378.01	1	1378.01	1	741.03	0	0.00	1	1378.01	0	820.00	1	1378.01	1	1378.01	1	1378.01	1	820.00	1	1378.01	1	1378.01	1	1378.01
42	0	0.00	1	105.00	0	105.00	0	0.00	0	0.00	1	105.00	0	0.00	0	105.00	1	105.00	1	105.00	0	105.00	1	105.00	0	0.00
43	0	0.00	0	0.00	1	171.02	1	171.02	0	0.00	0	171.02	0	171.02	1	171.02	0	171.02	0	0.00	0	0.00	0	171.02	0	0.00
44	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
45	1	861.00	0	861.00	0	0.00	0	0.00	1	861.00	1	861.00	1	861.00	0	0.00	1	861.00	1	861.00	0	0.00	0	0.00	0	0.00
46	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
47	1	1225.02	1	1225.02	1	528.01	0	0.00	1	1225.02	0	528.01	0	528.01	1	528.01	1	1225.02	1	528.01	1	1225.02	1	1225.02	1	1225.02
48	0	0.00	0	0.00	1	276.02	1	276.02	0	0.00	0	276.02	0	276.02	1	276.02	0	276.02	0	0.00	1	276.02	0	276.02	0	0.00
49	1	903.01	1	903.01	1	300.03	1	300.03	1	903.01	1	903.01	0	903.01	0	300.03	0	903.01	1	903.01	1	300.03	1	300.03	0	0.00
50	1	990.01	1	990.01	0	120.02	0	0.00	1	990.01	1	990.01	1	990.01	0	120.02	0	990.01	1	990.01	1	120.02	0	120.02	0	0.00

		27		28		29		30		31		32		33		34		35		36		37		38		39
1	1	903.00	0	210.03	1	210.03	1	903.00	0	0.00	0	0.00	0	0.00	1	903.00	0	210.03	1	903.00	0	903.00	1	903.00	1	210.03
2	0	0.00	0	0.00	0	0.00	0	1081.03	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
3	0	0.00	1	1225.03	1	136.00	0	1225.03	1	1225.03	0	0.00	0	0.00	1	1225.03	1	1225.03	1	136.00	1	1225.03	0	0.00	1	1225.03
4	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	1176.02	0	0.00	0	0.00
5	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00	0	0.00	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00
6	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	36.04	0	0.00	0	0.00	0	0.00	0	1225.02	0	0.00	0	1225.02
7	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
8	0	0.00	0	0.00	0	0.00	0	946.02	0	28.02	0	0.00	0	28.02	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
9	0	0.00	1	171.01	0	171.01	0	171.01	0	0.00	0	0.00	0	0.00	0	171.01	0	171.01	1	171.01	0	0.00	0	0.00	0	171.01
10	0	435.01	0	0.00	0	0.00	0	435.01	0	0.00	0	0.00	0	120.02	0	435.01	0	406.03	0	0.00	0	0.00	0	0.00	0	0.00
11	0	0.00	1	231.04	1	231.04	1	231.04	0	0.00	0	0.00	0	0.00	1	231.04	0	231.04	0	231.04	0	0.00	0	0.00	0	231.04
12	0	0.00	0	0.00	0	0.00	0	0.00	0	10.01	0	0.00	0	10.01	0	10.01	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
13	0	0.00	0	0.00	0	0.00	0	0.00	0	120.02	0	0.00	0	120.02	0	36.03	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
14	1	1431.01	1	1431.01	0	0.00	0	0.00	1	1431.01	0	0.00	1	1431.01	1	120.02	1	1431.01	0	0.00	1	1431.01	0	0.00	0	0.00
15	1	1081.03	1	406.03	1	406.03	1	1081.03	1	666.01	0	0.00	1	666.01	1	1081.03	1	406.03	1	1081.03	1	1081.03	1	1081.03	0	666.01
16	0	0.00	0	0.00	0	0.00	1	780.04	0	105.00	0	0.00	1	105.00	0	780.04	0	0.00	1	780.04	1	780.04	0	780.04	0	0.00
17	1	780.01	0	0.00	0	0.00	0	780.01	1	741.04	0	0.00	1	741.04	1	780.01	0	0.00	1	780.01	1	780.01	1	780.01	1	741.04
18	0	946.02	1	300.03	0	300.03	1	946.02	0	595.03	0	0.00	1	595.03	1	946.02	1	300.03	1	946.02	0	946.02	1	946.02	1	595.03
19	0	0.00	1	210.04	0	210.04	1	210.04	0	0.00	0	0.00	0	0.00	1	210.04	0	210.04	1	210.04	0	0.00	0	0.00	0	210.04
20	1	561.00	0	0.00	0	0.00	0	561.00	1	561.00	0	0.00	1	561.00	1	561.00	0	0.00	0	561.00	1	561.00	0	0.00	1	561.00
21	0	0.00	0	0.00	0	0.00	0	0.00	1	105.03	0	0.00	0	105.03	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
22	0	0.00	1	1326.02	0	136.00	1	1326.02	1	1326.02	0	0.00	0	0.00	1	1326.02	1	1326.02	0	136.00	1	1326.02	0	0.00	1	1326.02
23	1	561.04	0	0.00	0	0.00	0	561.04	1	561.04	0	0.00	1	561.04	1	561.04	0	0.00	1	561.04	0	561.04	0	0.00	1	561.04
24	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
25	1	1081.03	0	0.00	0	0.00	1	1081.03	0	91.00	0	0.00	0	91.00	1	1081.03	0	0.00	0	1081.03	0	1081.03	1	1081.03	0	0.00
26	0	0.00	1	1128.00	0	378.04	1	1128.00	1	1128.00	0	0.00	0	105.03	1	1128.00	1	1128.00	1	378.04	1	1128.00	0	0.00	1	1128.00
27	1	630.01	0	0.00	0	0.00	1	903.00	0	630.01	0	0.00	1	630.01	1	903.00	0	0.00	1	903.00	1	903.00	1	903.00	1	630.01
28	0	0.00	1	0.00	0	0.00	0	0.00	0	91.02	0	0.00	1	91.02	1	91.02	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
29	1	561.04	1	1128.02	1	406.02	1	1128.02	1	1128.02	0	0.00	1	561.04	1	1128.02	1	1128.02	1	561.04	1	1128.02	0	0.00	1	1128.02
30	1	666.01	1	378.00	1	378.00	1	666.01	1	666.01	0	0.00	1	666.01	1	666.01	1	378.00	1	666.01	1	666.01	0	0.00	1	666.01
31	0	741.04	0	0.00	0	0.00	1	741.04	1	741.04	0	0.00	1	741.04	1	741.04	0	0.00	1	741.04	1	741.04	0	0.00	1	741.04
32	1	820.00	0	0.00	0	0.00	0	820.00	0	741.03	1	0.00	1	741.03	1	820.00	0	0.00	0	820.00	0	820.00	0	820.00	1	741.03
33	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
34	1	561.03	1	406.04	1	406.04	1	561.03	1	561.03	0	0.00	1	561.03	1	561.03	0	406.04	0	561.03	1	561.03	0	0.00	1	561.03
35	1	741.04	0	0.00	0	0.00	1	741.04	1	741.04	0	0.00	0	741.04	0	741.04	1	0.00	0	741.04	1	741.04	0	0.00	1	741.04
36	0	0.00	1	1326.02	0	0.00	1	1326.02	1	1326.02	0	0.00	0	0.00	1	1326.02	0	1326.02	1	0.00	1	1326.02	0	0.00	1	1326.02
37	1	946.02	0	0.00	0	0.00	1	946.02	1	561.00	0	0.00	1	561.00	1	946.02	0	0.00	1	946.02	1	946.02	1	946.02	1	561.00
38	1	666.02	1	406.03	0	406.03	0	666.02	1	666.02	0	0.00	1	666.02	1	666.02	1	406.03	1	666.02	1	666.02	1	0.00	1	666.02
39	1	946.01	0	0.00	0	0.00	1	946.01	1	435.01	0	0.00	1	435.01	1	946.01	0	0.00	1	946.01	0	946.01	1	946.01	1	435.01
40	0	1431.00	1	1431.00	0	190.02	0	190.02	1	1431.00	0	0.00	1	1431.00	0	190.02	0	1431.00	1	190.02	1	1431.00	0	0.00	0	190.02
41	1	820.00	1	1378.01	0	0.00	0	1378.01	1	1378.01	0	0.00	1	741.03	1	1378.01	1	1378.01	0	820.00	1	1378.01	0	820.00	1	1378.01
42	0	0.00	0	0.00	0	0.00	0	0.00	1	105.00	0	0.00	1	105.00	0	105.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
43	0	0.00	0	171.02	1	171.02	1	171.02	0	0.00	0	0.00	0	0.00	1	171.02	0	171.02	0	171.02	0	0.00	0	0.00	0	171.02
44	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
45	0	0.00	0	0.00	0	0.00	1	861.00	0	0.00	0	0.00	0	0.00	1	861.00	0	0.00	0	861.00	1	861.00	0	861.00	0	0.00
46	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
47	1	528.01	1	1225.02	0	0.00	1	1225.02	1	1225.02	0	0.00	0	528.01	1	1225.02	0	1225.02	1	528.01	1	1225.02	0	0.00	0	1225.02
48	0	0.00	1	276.02	1	276.02	0	276.02	0	0.00	0	0.00	0	0.00	0	276.02	0	276.02	1	276.02	0	0.00	0	0.00	0	276.02
49	1	903.01	1	300.03	1	300.03	1	903.01	0	0.00	0	0.00	0	0.00	1	903.01	1	300.03	1	903.01	1	903.01	0	903.01	0	300.03
50	1	990.01	0	0.00	0	0.00	1	990.01	0	120.02	0	0.00	1	120.02	1	990.01	0	0.00	1	990.01	1	990.01	0	990.01	0	0.00

		40		41		42		43		44		45		46		47		48		49		50
1	0	903.00	1	903.00	0	0.00	0	903.00	0	0.00	1	903.00	1	903.00	1	210.03	0	0.00	1	903.00	1	903.00
2	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	300.04	0	300.04	0	0.00	0	0.00	0	0.00
3	1	1225.03	0	136.00	1	1225.03	0	0.00	1	1225.03	1	1225.03	1	136.00	0	1225.03	1	1225.03	1	1225.03	0	0.00
4	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
5	1	0.00	1	0.00	1	0.00	1	0.00	0	0.00	1	0.00	0	0.00	1	0.00	1	0.00	1	0.00	1	0.00
6	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	378.04	0	378.04	0	0.00	0	1225.02	0	0.00
7	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
8	0	0.00	0	0.00	0	0.00	0	28.02	0	0.00	0	0.00	0	406.00	0	406.00	0	0.00	0	0.00	0	0.00
9	0	0.00	1	171.01	0	0.00	0	0.00	0	0.00	0	0.00	1	171.01	1	171.01	0	0.00	0	0.00	0	0.00
10	0	0.00	0	406.03	0	0.00	0	0.00	0	0.00	0	435.01	0	435.01	0	406.03	0	0.00	0	0.00	0	0.00
11	0	0.00	0	231.04	0	0.00	0	0.00	0	0.00	0	0.00	0	231.04	0	231.04	0	0.00	0	0.00	0	0.00
12	0	0.00	0	0.00	0	0.00	0	10.01	0	10.01	0	0.00	0	10.01	0	10.01	0	0.00	0	10.01	0	0.00
13	0	0.00	0	0.00	0	0.00	0	120.02	0	120.02	0	0.00	0	120.02	0	120.02	0	0.00	0	36.03	0	0.00
14	0	0.00	1	1431.01	0	0.00	1	1431.01	1	1431.01	1	1431.01	1	1431.01	0	120.02	1	1431.01	1	1431.01	1	1431.01
15	0	1081.03	1	1081.03	1	666.01	1	1081.03	0	36.03	1	1081.03	1	1081.03	1	406.03	0	666.01	1	1081.03	1	1081.03
16	1	780.04	0	780.04	0	0.00	1	780.04	0	105.00	1	780.04	1	780.04	0	105.00	0	0.00	1	780.04	1	780.04
17	1	780.01	1	780.01	1	741.04	1	780.01	0	0.00	1	780.01	1	780.01	0	0.00	1	741.04	1	780.01	1	780.01
18	1	946.02	1	946.02	1	595.03	0	946.02	0	105.03	1	946.02	1	946.02	1	300.03	1	595.03	1	946.02	1	946.02
19	0	0.00	0	210.04	0	0.00	0	0.00	0	0.00	0	0.00	0	210.04	0	210.04	0	0.00	0	0.00	0	0.00
20	0	0.00	1	561.00	1	561.00	0	120.02	0	120.02	1	561.00	1	561.00	1	120.02	1	561.00	0	561.00	1	561.00
21	0	0.00	0	0.00	0	0.00	1	105.03	0	105.03	0	0.00	0	105.03	1	105.03	0	0.00	0	0.00	0	0.00
22	1	1326.02	1	136.00	1	1326.02	0	0.00	0	1326.02	1	1326.02	0	136.00	1	1326.02	1	1326.02	0	1326.02	0	0.00
23	0	0.00	1	561.04	1	561.04	0	0.00	0	0.00	1	561.04	1	561.04	0	0.00	1	561.04	1	561.04	1	561.04
24	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
25	1	1081.03	1	1081.03	0	0.00	1	1081.03	0	91.00	1	1081.03	1	1081.03	1	91.00	0	0.00	1	1081.03	1	1081.03
26	1	1128.00	1	378.04	1	1128.00	0	105.03	1	1128.00	1	1128.00	1	378.04	1	1128.00	0	1128.00	1	1128.00	0	0.00
27	0	903.00	1	903.00	0	0.00	1	903.00	0	0.00	1	903.00	1	903.00	0	0.00	1	630.01	1	903.00	1	903.00
28	0	0.00	0	0.00	0	0.00	0	91.02	0	91.02	0	0.00	0	91.02	0	91.02	0	0.00	1	91.02	0	0.00
29	1	1128.02	1	561.04	1	1128.02	0	0.00	1	1128.02	1	1128.02	1	561.04	1	1128.02	1	1128.02	1	1128.02	0	561.04
30	0	0.00	0	666.01	1	666.01	0	0.00	0	0.00	1	666.01	1	666.01	1	378.00	0	666.01	1	666.01	1	666.01
31	0	0.00	0	741.04	1	741.04	0	0.00	0	0.00	1	741.04	1	741.04	0	0.00	1	741.04	1	741.04	1	741.04
32	1	820.00	1	820.00	1	741.03	1	820.00	0	0.00	1	820.00	1	820.00	0	0.00	1	741.03	1	820.00	1	820.00
33	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
34	0	0.00	1	561.03	1	561.03	0	45.04	1	45.04	1	561.03	1	561.03	1	406.04	1	561.03	1	561.03	1	561.03
35	0	0.00	1	741.04	0	0.00	0	105.03	1	105.03	1	741.04	1	741.04	0	105.03	0	741.04	1	741.04	0	741.04
36	1	1326.02	0	0.00	0	1326.02	0	0.00	0	1326.02	0	1326.02	0	0.00	1	1326.02	1	1326.02	1	1326.02	0	0.00
37	1	946.02	1	946.02	1	561.00	1	946.02	0	0.00	1	946.02	1	946.02	0	0.00	1	561.00	1	946.02	1	946.02
38	0	0.00	0	666.02	1	666.02	0	66.03	0	66.03	0	666.02	1	666.02	0	406.03	0	666.02	0	666.02	0	666.02
39	0	946.01	1	946.01	1	435.01	1	946.01	0	120.03	1	946.01	1	946.01	0	120.03	0	435.01	1	946.01	1	946.01
40	1	0.00	1	1431.00	0	0.00	1	1431.00	1	1431.00	0	1431.00	0	1431.00	0	190.02	1	1431.00	1	1431.00	1	1431.00
41	1	1378.01	1	820.00	1	1378.01	0	820.00	1	1378.01	1	1378.01	1	820.00	1	1378.01	0	1378.01	1	1378.01	1	820.00
42	0	0.00	0	0.00	1	0.00	0	105.00	1	105.00	0	0.00	0	105.00	0	105.00	0	0.00	0	105.00	0	0.00
43	0	0.00	0	171.02	0	0.00	1	0.00	0	0.00	0	0.00	1	171.02	1	171.02	0	0.00	0	0.00	0	0.00
44	0	0.00	0	0.00	0	0.00	0	0.00	1	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
45	0	861.00	1	861.00	0	0.00	1	861.00	0	0.00	1	861.00	1	861.00	0	0.00	0	0.00	1	861.00	1	861.00
46	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	0.00	0	0.00	0	0.00	0	0.00	0	0.00
47	1	1225.02	1	528.01	1	1225.02	0	36.03	0	1225.02	1	1225.02	1	528.01	1	1225.02	1	1225.02	1	1225.02	1	528.01
48	0	0.00	0	276.02	0	0.00	0	0.00	0	0.00	0	0.00	0	276.02	1	276.02	1	0.00	0	0.00	0	0.00
49	1	903.01	1	903.01	0	0.00	1	903.01	0	0.00	1	903.01	1	903.01	1	300.03	0	0.00	1	903.01	1	903.01
50	0	990.01	1	990.01	0	0.00	1	990.01	0	120.02	1	990.01	1	990.01	0	120.02	0	0.00	1	990.01	1	990.01

CAIO RUAN NICHELE

MODELO DE CONFIANÇA PARA REDES AD HOC BASEADO EM TEORIA DE JOGOS

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.
Orientador: Prof. Dr. Luiz Carlos Pessoa Albini
Coorientador: Prof. Dr. André L. Vignatti

CURITIBA

2012