Universidade Federal do Paraná

Elisa Mannes

Controle de acesso baseado em criptografia para a distribuição segura de conteúdo multimídia em Redes Centradas em Informação

Curitiba PR
2016

Elisa Mannes

Controle de acesso baseado em criptografia para a distribuição segura de conteúdo multimídia em Redes Centradas em Informação

Tese apresentada como requisito parcial à obtenção do grau de Doutora em Informática no Programa de Pós-Graduação em Informática, setor de Ciências Exatas, da Universidade Federal do Paraná.

Área de concentração: *Ciência da Computação.*

Orientador: Carlos Alberto Maziero.

Curitiba PR
2016

Mannes, Elisa
Controle de acesso baseado em criptografia para a distribuição segura de conteúdo multimídia em redes centradas de informação / Elisa Mannes. – Curitiba, 2016
93 f. : il.; tabs.

Tese (doutorado) – Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-Graduação em Informática.
Orientador: Carlos Alberto Maziero

1. Criptografia de dados (Computação). 2. Redes de computado - res. 3. Controle de acesso. I. Maziero, Carlos Alberto. II. Título

CDD 005.8

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
Setor CIÊNCIAS EXATAS
Programa de Pós Graduação em INFORMÁTICA
Código CAPES: 40001016034P5

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em INFORMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da Tese de Doutorado de **ELISA MANNES**, intitulada: "**Controle de acesso baseado em criptografia para a distribuição segura de conteúdo multimídia em Redes Centradas em Informação**", após terem inquirido a aluna e realizado a avaliação do trabalho, são de parecer pela sua aprovação.

Curitiba, 17 de Junho de 2016.

Prof CARLOS ALBERTO MAZIERO
Presidente da Banca Examinadora (UFPR)

Prof ELIAS PROCÓPIO DUARTE JUNIOR
Avaliador Interno (UFPR)

Prof LUIZ CARLOS PESSOA ALBINI
Avaliador Interno (UFPR)

Prof ANELISE MUNARETTO FONSECA
Avaliador Externo (UTFPR)

Prof IGOR MONTEIRO MORAES
Avaliador Externo (UFF)

À comunidade acadêmica.

Agradecimentos

Ao meu orientador, professor Carlos Maziero, que com a sua excelência em pesquisa conduziu de forma brilhante os meus estudos. Obrigada por aceitar me orientar, por confiar e aceitar o meu interesse pelo tema da pesquisa, pelos conselhos, pelo apoio com os artigos e pelo exemplo de como ser um ótimo orientador.

Ao meu noivo, Luiz Carlos, que além de me auxiliar em todos os aspectos envolvidos em um doutorado, me auxiliou com a sua inteligência e seu conhecimento em programação. Obrigada pelas discussões e ideias, pelos ensinamentos na programação necessária para a execução dos testes e pelas correções no texto.

Ao Dr. Fábio Borges agradeço a disponibilidade, a paciência e a atenção comigo e minha pesquisa. Obrigada por dedicar seu tempo, mesmo no meio do seu doutorado, para me auxiliar com as minhas dúvidas. Obrigada por ir apresentar nosso artigo no Chipre, pelas sugestões e correções nos textos.

À minha irmã Mariana, que mesmo com muito trabalho dedicou seu tempo para corrigir todo o texto desta tese. Não poderia ter recebido correção melhor! Ao meu irmão Elton e aos meus pais Marisa e Orlando, obrigada por todo o apoio. Obrigada também à Marie pelas risadas proporcionadas durante a escrita desta tese.

Às minhas amigas doutoras Cinara e Rebeca, que desde o começo do doutorado me apoiam, me auxiliam e deixaram esses quatro anos de estudos mais doces e divertidos. Obrigada pelas viagens, pelas risadas, pelos cafés, pela paciência e por acreditar em mim mais que eu.

Aos professores da banca examinadora, Igor Moraes, Anelise Munaretto, Elias Duarte e Luiz Albini, obrigada pela disponibilidade, pela correção e pelas ótimas sugestões. Aos professores Luiz Albini, André Vignatti e Renato Carmo, obrigada pelos ensinamentos em suas respectivas disciplinas. Obrigada aos funcionários do departamento de informática por todo o apoio durante os quatro anos de doutorado.

Resumo

O uso cada vez maior da Internet destaca o seu grande sucesso, mas também revela as deficiências de uma arquitetura que sustenta uma rede de distribuição de conteúdo com um modelo inicialmente planejado para a comunicação ponto a ponto. As redes centradas em informação (*Information-Centric Network* - ICN) representam uma abordagem promissora ao abordar esse problema com um modelo mais adequado para a distribuição de conteúdo, no qual o conteúdo é a entidade principal da camada de rede. Para isso, o roteamento e o encaminhamento são realizados pelo nome dos conteúdos ao invés de endereços de máquina, e os conteúdos podem ser armazenados em *caches* na rede. Essa mudança traz diversos benefícios para a rede, principalmente para conteúdos muito acessados, como músicas e vídeos, mas gera preocupações com relação ao acesso não autorizado a conteúdos protegidos, pois os provedores não são consultados em requisições que são atendidas pelos *caches*. As soluções propostas para o controle de acesso em ICN geralmente limitam os benefícios trazidos pelos *caches* ou não garantem um nível de segurança adequado. Assim, este trabalho propõe uma solução para controle de acesso que permita que o conteúdo seja armazenado nos *caches*, que seja segura contra o acesso não autorizado e que não interfira no funcionamento das arquiteturas de ICN. Para isso, a solução proposta utiliza o esquema de recifragem por *proxy*, em que um conteúdo cifrado com uma chave pública $pk_{(u1)}$ pode ser transformado em um conteúdo cifrado com uma chave pública $pk_{(u2)}$, sem expor o conteúdo original nem as chaves privadas correspondentes. Essa transformação é tradicionalmente feita por uma entidade semi-confiável denominada *proxy*, usando uma *chave de recifragem* definida e criada por $u1$ a partir da sua chave privada e da chave pública de $u2$. Na solução proposta, a recifragem por *proxy* é adaptada ao transferir as funções do *proxy* para o próprio usuário, que recebe a chave de recifragem diretamente do provedor de conteúdo. Desta forma, o provedor distribui seus conteúdos cifrados e cada usuário, ao acessar um conteúdo, solicita uma chave de recifragem correspondente para o provedor. A chave de recifragem enviada é exclusiva do usuário para determinado conteúdo e só funciona com o conhecimento da chave privada do usuário que solicitou o acesso. Assim, ao receber uma requisição para a chave de recifragem de um conteúdo, o provedor pode aplicar as políticas de controle de acesso necessárias, impedindo que usuários não autorizados possam decifrar os conteúdos recuperados dos *caches*. A solução proposta é analisada em quatro aspectos: desempenho de uma arquitetura de ICN na distribuição de conteúdos multimídia, desempenho do esquema de recifragem por *proxy*, desempenho da solução proposta nos provedores e nos usuários e comparação com outras soluções criptográficas. Os resultados confirmam os benefícios da ICN na distribuição de conteúdo multimídia, e revelam que enquanto o esquema de recifragem por *proxy* tem desempenho adequado no domínio do provedor, a operação de decifragem no domínio do usuário se mostra inadequada para o fluxo de conteúdos maiores que 1GB por hora. Assim, é proposta uma otimização que diminui o tempo da operação de decifragem em até 96%, tornando o esquema atrativo para o controle de acesso de conteúdos em ICN. Em comparação com outras soluções, a solução proposta é mais segura, mais eficiente e faz o melhor uso dos *caches* na rede.

Palavras-chave: recifragem por *proxy*, controle de acesso, redes centradas em informação.

Abstract

The increasing use of the Internet by the users in their daily routines highlights the Internet great success whilst reveals the shortcomings of an architecture that supports a content distribution network with an architectural model originally designed for point to point communication. In this context, the Information-Centric Network (ICN) paradigm is a promising approach to address the current shortcomings of the Internet with an architecture more suitable for content distribution. In ICN, the content is the main entity on the network layer, thus routing and forwarding are performed on named content rather than host addresses, and content can be stored on in-network caches. This change brings many benefits to the network, especially for popular contents such as music and video, but also raises concerns about unauthorized access, since the provider does not interact with users which have their requests satisfied by caches. Existing solutions for access control in ICN often limit the benefits of caches or do not guarantee an adequate level of security. Thus, this work proposes an access control solution for ICN that allows content to be stored in caches and recovered by any user, is safe against unauthorized access, and does not interfere on ICN functioning. The proposed solution employs a proxy reencryption scheme, in which a content encrypted with a public key $pk_{(u1)}$ can be transformed into a content encrypted with a public key $pk_{(u2)}$, without exposing the original content nor the corresponding private keys. This transformation is traditionally done by a semi-trusted entity called the proxy, using a *reencryption key* defined and created by $u1$ from its private key and $u2$ public key. In the proposed solution, the proxy reencryption is adapted to transfer proxy functions to the user himself, who receives the reencryption key directly from the content provider. Thus, the content provider distributes encrypted content, and each user requests a reencryption key for each content they wish to access. The reencryption key sent by the content provider is exclusive to that user and to the requested content; consequently, it works only with the corresponding public-private key pair of the user requesting the content. Therefore, before issuing a reencryption key, the content provider can apply access control policies, preventing malicious users to decrypt the contents retrieved from in-network caches. The proposed solution is evaluated in four aspects: ICN performance on multimedia distribution, performance of proxy reencryption, performance of the proposed solution on content providers and users, and a comparative analysis with two distinct cryptographic solutions. Results confirm the benefits of ICN on multimedia content distribution, and reveals that while the proxy reencryption scheme is adequate for the content provider domain, the decryption operation on the user's domain is inadequate for content flows bigger than 1GB per hour. Thus, we propose an optimization on reencryption and decryption operations, leading to a reduction of up to 96% the decryption time on users, making the scheme attractive and suitable for content access control in ICN. Compared to other cryptographic access control solutions, the proposed solution is safer, more efficient and makes the best use of in-network caches.

Keywords: proxy reencryption, access control, information-centric networks.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Acrônimos

ACL	*Access Control List*
ABE	*Attribute-Based Encryption*
ADSL	*Asymmetric Digital Subscriber Line*
AES	*Advanced Encryption Standard*
ARP	*Address Resolution Protocol*
AS	*Autonomous System*
BE	*Broadcast Encryption*
CCA	*Chosen Ciphertext Attack*
CCN	*Content-Centric Network*
CCN-AC	*Content-Centric Network Access Control*
CDN	*Content Distribution Network*
CP	*Ciphertext-Policy*
CS	*Content Store*
DASH	*Dynamic Adaptive Streaming over HTTP*
DES	*Data Encryption Standard*
DHCP	*Dynamic Host Configuration Protocol*
DHT	*Distributed Hash Table*
DNS	*Domain Name System*
DONA	*Data-Oriented Network Architecture*
DRM	*Digital Rights Management*
DTN	*Delay Tolerant Networks*
EB	*Enabling Block*
EU-RE	*Efficient Unidirectional Re-Encryption*
EU-PRE	*Efficient Unidirectional Proxy Re-Encryption*
FIB	*Forwarding Information Base*
FIFO	*First In First Out*
FTP	*File Transfer Protocol*
GB	*Gigabyte*
GHz	*Gigahertz*
GSM	*Global System for Mobile Communications*
HBC	*Honest But Curious*
HD	*High Definition*
HTTP	*Hypertext Transfer Protocol*
IBAC	*Interest-Based Access Control*
IBE	*Identity-Based Encryption*
ICN	*Information Centric Network*
ICN-RG	*ICN Research Group*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*

ISP	*Internet Service Provider*
KB	*Kilobyte*
KP	*Key-Policy*
kbps	*Kilobits Per Second*
MAC	*Medium Access Control*
MANETs	*Mobile Ad Hoc Networks*
MB	*Megabyte*
MCAC	*Mandatory Content Access Control*
MTU	*Maximum Transmission Unit*
NACK	*Non Acknowledgement*
NDN	*Named-Data Network*
ndnSim	*Named-Data Network Simulator*
NDO	*Named Data Object*
NetInf	*NETwork of INFormation*
NRS	*Name Resolution Service*
NS-3	*Network Simulator*
P2P	*Peer-to-peer*
PARC	*Palo Alto Research Center*
PHR	*Personal Health Records*
PIT	*Pending Interest Table*
PRE	*Proxy Re-Encryption*
PURSUIT	*Pursuing a Pub/Sub Internet*
RAM	*Random Access Memory*
RH	*Resolution Handler*
RSA	*Rivest-Shamir-Adleman*
RTT	*Round Trip Time*
SSH	*Secure Shell*
SHA	*Secure Hash Algorithm*
TCP	*Transmission Control Protocol*
TOR	*The Onion Project*
UCLA	*University of California, Los Angeles*
UDP	*User Datagram Protocol*
URL	*Unified Resource Locator*

Lista de Símbolos

R	Roteador
u	Usuário do sistema
$/ <> / <>$	Nome do conteúdo
$p1, p2$	Provedores
$rk_{u1 \to u2}$	Chave de recifragem do usuário $u1$ para o usuário $u2$
m	Mensagem original
m'	Mensagem encriptada
m''	Mensagem recifrada
$pkx_{(u)}$	Chave pública x do usuário u
$skx_{(u)}$	Chave privada x do usuário u
k	Chave secreta
$\{c\}_{pkx_{(u)}}$	Mensagem c cifrada com a chave pública x do usuário u
κ	Tamanho das chaves
$\mathcal{C}$	Conjunto de conteúdos
ℓ_0	Tamanho das mensagens
ℓ_1	Parâmetro de segurança
α	Popularidade relativa da distribuição Zipf
ω	Conjunto de atributos

Capítulo 1

Introdução

A distribuição de conteúdo destaca-se como o serviço mais utilizado atualmente na Internet. De fato, as aplicações que geram conteúdo em tempo real, tais como *Netflix*, *YouTube* e *Spotify*, representam a categoria com maior tráfego mundial na Internet, ultrapassando 50% do total do tráfego mensal na América do Norte [Sandvine, 2015]. Embora esse novo cenário reforce o sucesso da Internet, ele também revela as suas fraquezas para acomodar, de forma eficiente e segura, o novo padrão de tráfego que a distribuição de conteúdo impõe. Ao considerar conteúdos populares, por exemplo, várias cópias idênticas são transmitidas pelos mesmos canais, o que pode ocasionar congestionamento nos canais de comunicação, alta latência e custos extras para os provedores [Perino e Varvello, 2011]. A necessidade de contornar essas deficiências e tornar a Internet uma arquitetura mais adequada para a distribuição de conteúdo tem sido uma preocupação há algum tempo. As redes par-a-par (*peer-to-peer* - P2P) [Schollmeier, 2001] e as redes de distribuição de conteúdo (*Content Distribution Network* - CDN) [Kangasharju et al., 2002], por exemplo, são estruturas que visam criar um ambiente mais adequado para estes cenários. No entanto, essas soluções são camadas específicas sobre a rede tradicional, herdando as suas limitações e servindo apenas para conteúdos específicos [Bari et al., 2012].

A principal razão pela qual a arquitetura da Internet não é nativamente adequada para a distribuição de conteúdo vem do fato de que a camada de rede é fundamentada no protocolo IP (*Internet Protocol*), que é *centrado em máquinas* [Jacobson et al., 2012]. O protocolo IP identifica cada interface de rede por um endereço IP. Para acessar um conteúdo, primeiramente é necessário encontrar o endereço IP da máquina que contém o conteúdo, estabelecer uma conexão com a máquina e então solicitar o conteúdo. Neste sentido, o protocolo IP é apontado como inerentemente ineficiente para a disseminação de conteúdo, uma vez que o modelo exige a localização e a conexão entre máquinas, quando o interesse principal é no conteúdo, independente de sua localização [Ahlgren et al., 2012]. Portanto, quando aplicado para a distribuição de conteúdo, o protocolo IP impossibilita a adoção de diversos mecanismos atrativos, como por exemplo, o aproveitamento de cópias em máquinas próximas do usuário, o que diminuiria a latência ou atraso no recebimento do conteúdo, e a otimização do tráfego quando muitos usuários solicitam conteúdos idênticos, como em fluxos de mídia ao vivo. Desta forma, o descompasso entre o protocolo IP e as atuais exigências impostas para a arquitetura da Internet representa uma enorme motivação para uma arquitetura mais dinâmica, modular e adaptável, adequada para acomodar os novos padrões de uso, principalmente com relação à distribuição de conteúdo.

1.1 Contextualização

As redes centradas em informação (*Information-centric Network* - ICN) [Ahlgren et al., 2012] ganharam atenção considerável da academia e da indústria ao propor superar as deficiências atuais da Internet, modificando a principal entidade da camada de rede de máquinas para *conteúdos*. Ao modificar o foco da camada de rede, a ICN muda substancialmente a maneira como os dados fluem na Internet, pois a requisição, o roteamento e o encaminhamento são realizados a partir do *nome do conteúdo*. Como consequência, a rede pode armazenar cópias do conteúdo e usá-las para responder às requisições dos usuários, criando *caches* diretamente na rede. Um mecanismo de *cache* na rede potencializa um melhor desempenho na entrega do conteúdo e torna a arquitetura mais adequada para os atuais padrões de tráfego. Além disso, a nomeação de conteúdo na camada de rede permite que os roteadores conheçam o que está sendo solicitado em cada interface e, desta forma, podem realizar a agregação de tráfego, contribuindo para que somente uma cópia da requisição e da resposta trafegue pela rede.

Entretanto, a mudança imposta pelo paradigma de ICN na camada de rede também modifica vários aspectos relacionados à segurança. A nomeação de conteúdos na camada de rede, por exemplo, modifica o foco da segurança para a proteção do conteúdo em si, ao invés de proteger máquinas ou conexões. Assim, o conteúdo deve prover mecanismos para que os usuários sejam capazes de aferir sua integridade e autenticidade diretamente a partir do próprio conteúdo [AbdAllah et al., 2015a]. Além disso, embora o *cache* traga benefícios óbvios, ele também impõe novos desafios relacionados à privacidade e ao controle de acesso. Os dispositivos que possuem *caches*, por exemplo, não avaliam se o usuário que requisitou o conteúdo é autorizado a acessá-lo. Já a privacidade é agravada pela presença de conteúdo nomeado na rede, pois se tradicionalmente a rede tem conhecimento de um endereço de máquina para realizar o roteamento, na ICN a rede tem conhecimento do nome dos conteúdos que estão sendo acessados, o que pode ser usado para fins de monitoramento e censura. Desta forma, torna-se claro que a ICN abre caminho para potenciais ameaças de segurança que estão ausentes na Internet atual e, desta forma, a segurança deve ser aplicada de um modo diferente das redes tradicionais. Consequentemente, os aspectos de segurança em ICN precisam de atenção especial, a fim de assegurar que a arquitetura seja robusta, tanto com relação ao desempenho quanto à segurança, para suportar as exigências atuais e futuras da Internet.

1.2 Problema

A possibilidade de armazenamento de conteúdo em *caches* nos dispositivos da rede gera uma grande preocupação com relação ao controle de acesso dos conteúdos, pois as cópias em *cache* podem ser acessadas por qualquer usuário, inclusive aqueles que não têm autorização. O provedor de conteúdo, por exemplo, não tem controle sobre os dispositivos que possuem seus conteúdos em *cache* e nem interage com os usuários que têm suas requisições atendidas pelos *caches* na rede, dificultando a execução de políticas de acesso. O problema do controle de acesso em ICN se destaca principalmente ao considerar a distribuição de conteúdos multimídia protegidos, em que fica ainda mais evidente a necessidade de assegurar que o provedor possa validar políticas de acesso para o conteúdo armazenado em *cache*. Tais serviços geralmente requerem um rigoroso controle das contas de usuários, do número de reproduções do conteúdo e da quantidade de dispositivos autorizados, por exemplo. Assim, esse tipo de aplicação requer uma solução de controle

de acesso que seja parte do próprio conteúdo, de outra forma, é pouco provável que a arquitetura de ICN seja adotada para a distribuição de conteúdos multimídia, que justamente compõem a categoria que teria o maior benefício com a adoção da ICN.

As soluções tradicionais para controle de acesso na distribuição de conteúdo, apesar de serem transferíveis para ICN, geralmente inviabilizam a proposta do uso de *cache* na rede, principalmente porque exigem a manutenção de uma comunicação segura entre máquinas. Por outro lado, a maioria das soluções de controle de acesso desenvolvidas especialmente para uso em ICN emprega o uso de criptografia simétrica e garante que somente usuários autorizados tenham acesso à chave utilizada. Essa estratégia, apesar de eficiente, pode representar um problema caso a chave seja divulgada, pois é a mesma para todos os usuários. Além disso, muitas soluções acrescentam entidades terceiras na rede ou exigem que os próprios roteadores validem as políticas de acesso, antes de enviar uma cópia em *cache*. Além de adicionar um passo extra na recuperação de conteúdo ao utilizar entidades terceiras, utilizar os próprios roteadores para essa validação exige um grande desempenho do núcleo da rede, o que pode representar atrasos na recuperação do conteúdo e sobrecarga nos roteadores. Desta forma, ainda não há uma abordagem de controle de acesso que seja adequada e que preserve todos os benefícios introduzidos pela ICN.

1.3 Objetivos

Este trabalho tem como objetivo propor uma solução de controle de acesso para ICN, que englobe três aspectos principais: (i) o conteúdo pode ser armazenado em qualquer dispositivo e recuperado por qualquer usuário, fazendo uso eficiente dos *caches* previstos no paradigma de ICN; (ii) os usuários que possuem o conteúdo devem ser autorizados pelo provedor de conteúdo para acessá-lo; (iii) não há adição de novas entidades na rede para a aplicação ou validação de políticas de acesso. Neste trabalho, considera-se como *controle de acesso* na distribuição de conteúdo em ICN a garantia de que o provedor de conteúdo possa impor as *regras de controle de acesso* desejadas, decidindo quem pode acessar o conteúdo que ele disponibiliza na rede. Essa decisão é tomada a partir de uma *política de controle de acesso* que define regras, como por exemplo, o pagamento de mensalidades, se o conteúdo está de acordo com o serviço contratado, com o tipo de inscrição ou com a idade do usuário.

Primeiramente, busca-se um estudo dos desafios de segurança nas principais áreas de ICN, propondo uma organização para a área e aprofundando o estudo das deficiências das soluções de controle de acesso existentes. A partir deste estudo, propõe-se uma solução de controle de acesso adequada para uso em ICN, por meio da adaptação do esquema criptográfico de recifragem por *proxy* [Chow et al., 2010]. A recifragem por *proxy* prevê que um conteúdo cifrado com uma chave pública $pk_{(u1)}$ do usuário $u1$ pode ser transformado em um conteúdo cifrado com uma chave pública $pk_{(u2)}$, do usuário $u2$, sem expor o conteúdo original nem as chaves privadas correspondentes. Essa transformação é tradicionalmente feita por uma entidade semi-confiável denominada *proxy*, usando uma *chave de recifragem* definida e criada por $u1$ a partir da sua chave privada e da chave pública de $u2$. Na solução proposta, a recifragem por *proxy* é adaptada para atingir os objetivos buscados, sendo que a entidade do *proxy* é retirada do processo, e as suas funções são alocadas diretamente no usuário. Desta forma, somente os provedores e os usuários estão envolvidos com as funções de controle de acesso, e a rede é livre para entregar o conteúdo de maneira mais eficiente.

Por fim, investiga-se o desempenho da solução proposta nos domínios do provedor e do usuário na distribuição de música e vídeo, e propõe-se uma otimização dos algoritmos de

recifragem e decifragem no domínio do usuário, a fim de otimizar os tempos de decifragem e possibilitar o uso da solução proposta em dispositivos com poucos recursos. Além disso, busca-se realizar uma análise comparativa da solução proposta com outras soluções de controle de acesso criptográficas para ICN, identificando aspectos de adequação à ICN, de desempenho e de segurança de cada uma delas.

1.4 Estrutura do documento

Esta tese está dividida em 8 capítulos. O Capítulo 2 introduz os fundamentos do paradigma de ICN e descreve a escolha pela arquitetura *Named-Data Network* (NDN). O Capítulo 3 apresenta uma visão detalhada dos problemas de segurança em ICN e especifica o problema do acesso não autorizado. O Capítulo 4 introduz os conceitos da recifragem por *proxy* e detalha o *Efficient Unidirectional Proxy Re-Encryption*, que fundamenta a solução proposta. O Capítulo 5 apresenta a solução proposta, enfatizando a adaptação do esquema de recifragem por *proxy* e o funcionamento da solução no provedor de conteúdos e no dispositivo do usuário. O Capítulo 6 valida as características da arquitetura NDN na distribuição de conteúdo multimídia e avalia a solução proposta em dois aspectos: desempenho do esquema de recifragem por *proxy* e o desempenho dos provedores e usuários ao realizar as operações criptográficas em arquivos de música e vídeo. O Capítulo 7 detalha e avalia a proposta de otimização nos algoritmos de recifragem e decifragem do esquema de recifragem por *proxy*, além de apresentar uma análise comparativa da solução proposta com outras duas soluções de controle de acesso criptográficas. Por fim, o Capítulo 8 apresenta as contribuições deste trabalho e lista as oportunidades de trabalhos futuros.

Capítulo 2

Redes Centradas em Informação

Este capítulo apresenta o paradigma das redes centradas em informação (*Information-centric Network* - ICN) como uma arquitetura para a Internet do Futuro, adequada às demandas de distribuição de conteúdo. Ele está dividido em duas seções. A Seção 2.1 introduz os principais componentes da arquitetura do paradigma de ICN e expõe os benefícios da sua adoção. A Seção 2.2 detalha as escolhas de projeto específicas da arquitetura de referência utilizada neste trabalho, a *Named-Data Network* (NDN), e apresenta uma visão geral de outras três arquiteturas relevantes do paradigma de ICN.

2.1 Fundamentos de redes centradas em informação

A perspectiva de evoluir e adequar a arquitetura da Internet para a distribuição de conteúdo constitui a principal razão para a proposta do paradigma de redes centradas em informação (ICN) [Brito et al., 2012]. Neste sentido, a ICN propõe explorar o conteúdo como a principal entidade da camada de rede ao nomear, rotear, encaminhar e prover segurança no conteúdo ao invés de realizar essas atividades em enlaces de comunicação e sessões de aplicações entre dispositivos, tornando a arquitetura mais natural para o fluxo de conteúdo na rede. Em comparação com as redes IP (*Internet Protocol*), a ICN se diferencia em duas questões principais: *o que* a rede roteia e *como* esse roteamento é realizado. Os roteadores atuais tradicionalmente roteiam endereços IP que indicam o dispositivo que contém o conteúdo requisitado. Já os roteadores na ICN devem rotear nomes de conteúdos em direção a uma cópia disponível deste conteúdo. Assim, o protocolo IP endereça dispositivos enquanto a ICN endereça conteúdo. Para rotear uma requisição do usuário até o provedor, os roteadores IP são apoiados pela hierarquia dos endereços IP. Já o paradigma de ICN roteia o conteúdo nomeado em direção ao provedor do conteúdo, contudo, ela permite que os roteadores armazenem conteúdos em *cache* e, desta forma, caso o roteador possua o conteúdo armazenado localmente, ele pode satisfazer essa requisição sem a necessidade de solicitar o conteúdo ao provedor. Esse cenário é bastante atraente para a distribuição de conteúdos, principalmente os populares, em que vários usuários estão interessados, como no caso de transmissões ao vivo.

A ICN também traz diversos novos benefícios como consequência da nomeação de conteúdos diretamente na camada de rede. O benefício mais evidente é a redução de tráfego nos canais de comunicação e a consequente diminuição no atraso de entrega de conteúdo. Isso é possível por dois motivos: a agregação de requisições para o mesmo conteúdo nos roteadores e a possibilidade de *cache* na rede. As requisições recebidas de usuários diferentes para o mesmo conteúdo podem ser agregadas nos roteadores,

fazendo com que somente uma cópia trafegue na rede até o roteador mais próximo do usuário. Já a possibilidade de armazenar os conteúdos oportunisticamente em *caches* na rede dá ao roteador a oportunidade de priorizar locais que apresentem menor atraso de comunicação, por exemplo. Outra característica da ICN é o suporte a cenários desafiadores, como redes móveis *ad hoc* (*Mobile Ad hoc NETworks - MANET*) [Toh, 2001] e redes tolerantes a desconexões (*Delay Tolerant Network - DTN*) [Fall, 2003]. Estes cenários são beneficiados pela descentralização dos conteúdos na rede, o que permite que o conteúdo possa ser recuperado de qualquer local disponível, sem a necessidade de uma conexão fim a fim (cliente-servidor) persistente. Além disso, a ICN transfere o foco da segurança, tradicionalmente focada na proteção dos enlaces de comunicação, para o conteúdo, o que elimina a necessidade de confiança em dispositivos específicos para a recuperação de conteúdo.

A Figura 2.1 ilustra um exemplo simples do funcionamento do paradigma de ICN. Neste exemplo, a rede é composta pelo provedor do conteúdo, quatro roteadores, $R1$, $R2$, $R3$ e $R4$ e três usuários, $u1$, $u2$ e $u3$. Neste exemplo, o provedor disponibiliza os conteúdos a, b e c para os usuários. O nome do conteúdo é anunciado aos usuários com a concatenação do nome do provedor e do nome do conteúdo; os usuários aprendem os nomes desses conteúdos, $/p1/a$, $/p1/b$ e $/p1/c$, através de aplicações ou mecanismos de buscas. A ICN fornece um modelo de requisição/resposta em que as requisições são enviadas pelo usuário em direção à rede, que roteia essa requisição com base no nome do conteúdo. Na Figura 2.1(a) o usuário $u1$ envia uma requisição para o conteúdo $/p1/a$ ao seu roteador de borda, $R4$. O roteador $R4$, por sua vez, roteia a requisição em direção ao provedor, já que não possui o conteúdo $/p1/a$ em seu *cache*. A requisição segue o caminho até o provedor, sendo que a resposta contendo o conteúdo $/p1/a$ segue o caminho reverso, em direção ao usuário, como mostra a Figura 2.1(b). Cada roteador no caminho armazena uma cópia de $/p1/a$ em seu *cache*, possibilitando que em requisições futuras para esse mesmo conteúdo a rede possa usufruir de redução de tráfego nos canais e diminuição da latência na rede. Por exemplo, na Figura 2.1(c) o usuário $u2$ solicita o conteúdo $/p1/a$ para o seu roteador de borda, $R4$. O roteador $R4$ possui o conteúdo $/p1/a$ armazenado em seu *cache* e prontamente responde a requisição de $u2$. Esse comportamento também se repete no exemplo apresentado na Figura 2.1(d), em que o usuário $u3$ solicita o conteúdo $/p1/a$ para $R3$, que roteia a requisição em direção ao provedor. Contudo, o roteador $R1$ possui o conteúdo $/p1/a$ em seu *cache* e, portanto, responde à requisição sem necessitar consultar o provedor. O roteador $R3$ recebe o conteúdo de $R1$, armazena uma cópia em seu *cache* e encaminha o conteúdo para $u3$.

Em comparação com a arquitetura IP, a ICN se diferencia em três aspectos principais: a *nomeação de conteúdo* na camada de rede, o *roteamento e encaminhamento* e o *cache na rede*. A decisão de projeto de como cada um desses aspectos é tratado depende do projeto de cada arquitetura que utiliza o paradigma de ICN. Contudo, existem propriedades que são intrínsecas ao modelo de ICN que devem ser seguidas pelas arquiteturas. Nas próximas subseções essas três áreas são descritas com mais detalhes.

2.1.1 Nomeação de conteúdo

A forma como um conteúdo é nomeado no paradigma de ICN implica na garantia de três propriedades principais: unicidade, persistência e certificação. O esquema de nomeação deve identificar de forma inequívoca cada um dos conteúdos disponíveis na rede, a fim de garantir a unicidade, ao mesmo tempo que permite aos roteadores rotear e

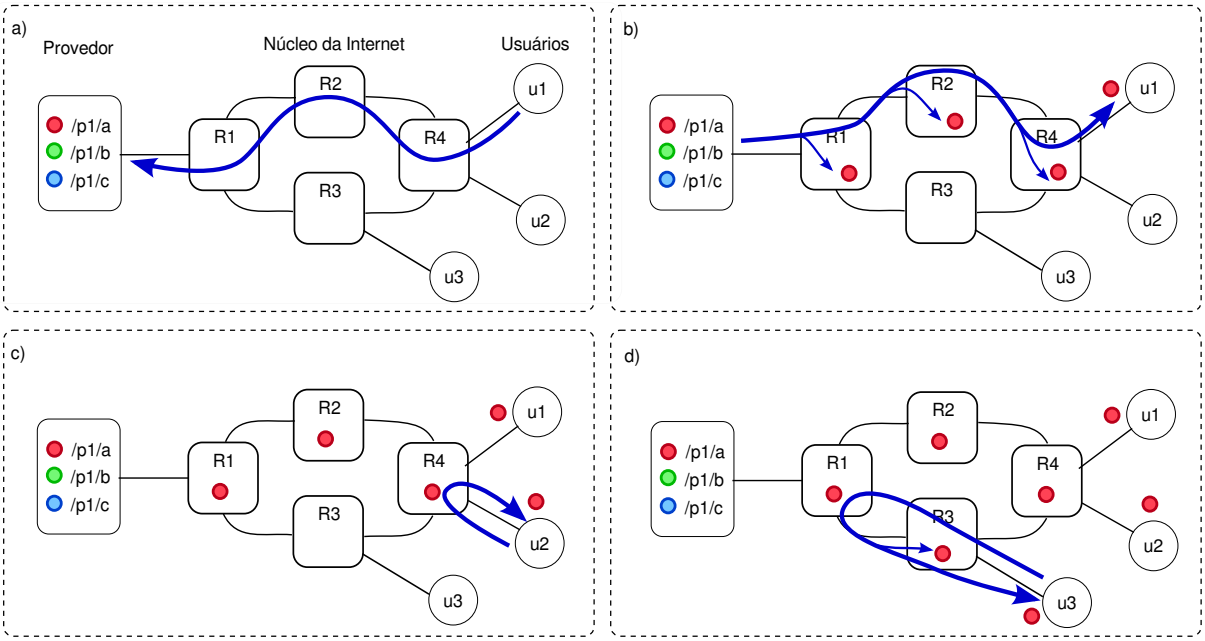

Figura 2.1: Modelo de funcionamento do paradigma de redes centradas em informação.

encaminhar os conteúdos com um bom desempenho. Além disso, o esquema de nomeação deve permitir que o conteúdo possa ser realocado sem a mudança do seu nome, garantindo a persistência do conteúdo na rede. Já a certificação do nome do conteúdo é necessária para que os usuários possam aferir a integridade e a autenticidade do conteúdo ao recebê-lo, já que é possível recuperar o conteúdo de outros locais além do provedor do conteúdo.

Atualmente, os principais esquemas de nomes explorados em ICN são divididos em dois tipos: *nomes planos* e *nomes hierárquicos*. O esquema de nomes planos explora uma estrutura de nomes de tamanhos fixos compostos por *bits* de aparência aleatória, como os gerados por funções de *hash*, por exemplo. Eles garantem a unicidade do nome, já que ele é gerado a partir de cada conteúdo, e a persistência, pois o nome reflete apenas o seu vínculo com o conteúdo em si, independente da localização ou provedor. A certificação se dá pelo próprio nome, que representa o resumo da função de *hash* do conteúdo. A Figura 2.2(a) ilustra a composição de um nome de conteúdo utilizando o esquema de nomeação plana [Dannewitz et al., 2013]. Neste esquema, o nome do conteúdo é composto de duas partes: a identificação da função de *hash* utilizada para gerar o nome do conteúdo e o resumo da função de *hash* aplicada ao conteúdo.

Em contrapartida, os esquemas de nomes hierárquicos propõem uma estrutura hierárquica para nomear os conteúdos, com a agregação de componentes significativos ao nome do conteúdo, similar à forma como as páginas *web* são nomeadas. Esse esquema de nomeação garante a unicidade dos nomes por aceitar uma grande diversidade de concatenações. Contudo, isso pode dificultar a realocação de conteúdo, já que o nome do conteúdo pode estar ligado à sua localização ou ao identificador do provedor. A certificação no esquema de nomes hierárquicos é realizada através da assinatura da relação entre o conteúdo e o seu nome, feita com a chave pública do provedor. A Figura 2.2(b) exemplifica o nome de um conteúdo no esquema de nomeação hierárquica. Neste modelo, o nome é composto pelo caminho hierárquico de armazenamento do conteúdo no provedor. Este complemento deve identificar sem equívoco o conteúdo dentro do domínio do provedor, por isso deve ser único.

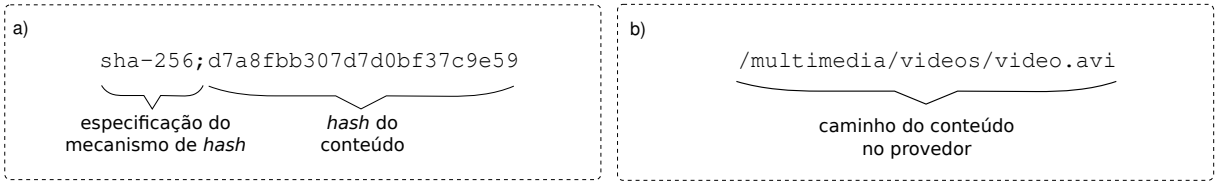

Figura 2.2: Modelos de (a) nomeação plana e (b) nomeação hierárquica.

2.1.2 Roteamento e encaminhamento de conteúdo nomeado

O roteamento é responsável por direcionar as requisições dos usuários até uma cópia do conteúdo, armazenada no provedor ou em um *cache* na rede, e encaminhar esse conteúdo ao usuário que o requisitou. Nas ICNs, os roteadores realizam três funções básicas considerando o nome do conteúdo: preencher e manter suas tabelas de roteamento com informações de localização dos conteúdos, rotear as requisições que chegam dos usuários até uma cópia do conteúdo e manter um *cache* para a otimização do tráfego. O armazenamento das informações de roteamento representa um grande desafio por conta da escalabilidade, ao considerar a grande quantidade de páginas indexadas na Internet. Além disso, a maneira como os roteadores roteiam e encaminham os conteúdos na rede deve ser rápida e eficiente, o que pode depender do esquema de nomeação utilizado e das políticas de *cache* adotadas.

Dois esquemas de roteamento têm sido considerados nas arquiteturas de ICN: o *roteamento baseado em nomes* e o *roteamento baseado em nomes com auxílio de um serviço de resolução de nomes* (*Name Resolution Service* - NRS). No esquema de roteamento baseado em nomes, os roteadores roteiam o conteúdo diretamente pelo nome. As tabelas de roteamento são preenchidas com informações de prefixos hierárquicos e a interface de rede para a qual o roteador deve encaminhar requisições com o prefixo. Os roteadores armazenam informações do estado das requisições conforme elas são enviadas e, quando atendidas, as informações do estado da requisição são consumidas. Desta forma, o encaminhamento do conteúdo até o usuário é realizado pelo caminho inverso da requisição. A Figura 2.3(a) apresenta um exemplo simples do roteamento baseado em nomes, em que os roteadores $R1$ e $R2$ possuem entradas em suas tabelas para os conteúdos dos provedores $p1$ e $p2$. O roteador $R1$, por exemplo, deve rotear os pedidos para os conteúdos de $p2$ através da interface de rede 2.

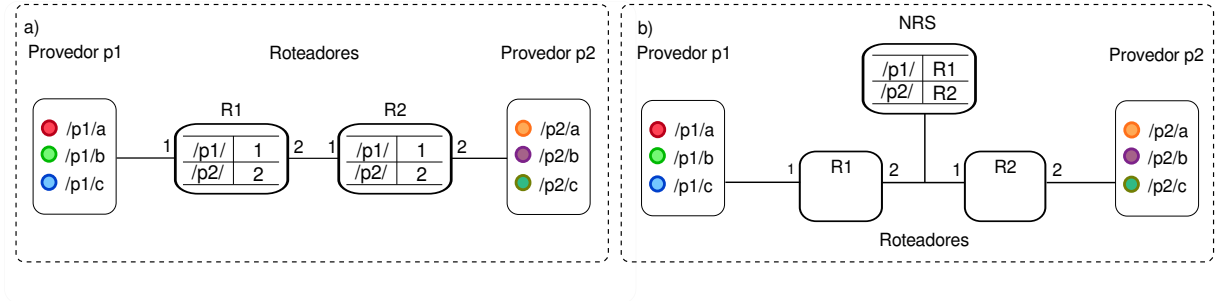

Figura 2.3: Modelos de (a) roteamento baseado em nomes e (b) roteamento com auxílio de um serviço de resolução de nomes.

O roteamento com auxílio de um serviço baseado em nomes funciona de forma semelhante ao DNS tradicional. Nesse esquema de roteamento, o NRS mapeia nomes de conteúdos e um conjunto de localização desses conteúdos, na forma de dicas de roteamento.

Ao receber uma requisição, os roteadores consultam o NRS para recuperar essas dicas de roteamento para o conteúdo, que é então roteado por um protocolo de roteamento tradicional até o local indicado pelo NRS, que pode ser o provedor de conteúdo original ou um *cache*. O encaminhamento do conteúdo até o usuário pode seguir um caminho diferente e é estabelecido pelo protocolo de roteamento. A Figura 2.3(b) ilustra o roteamento com NRS. Os roteadores $R1$ e $R2$ consultam o NRS sempre que recebem uma requisição. O roteador $R1$, por exemplo, ao receber uma requisição para algum conteúdo de $p2$, consulta o NRS e recebe como dica que o próximo salto para a melhor cópia disponível é o roteador $R2$. Então, com o auxílio das tabelas internas de roteamento, o roteador $R1$ sabe que deve encaminhar essa requisição para a interface de rede 2.

2.1.3 *Cache* de conteúdo na rede

A possibilidade de armazenamento de conteúdos em *caches* na rede enriquece a ICN com diversas vantagens, sendo a principal delas o melhor desempenho na entrega de conteúdo, tanto para os usuários como para os provedores de conteúdos. O paradigma de ICN não impõe questões como políticas de *cache*, exclusão de conteúdos do *cache* ou tipo de *cache*, porém a existência do *cache* é primordial para o sucesso de qualquer arquitetura que utiliza o paradigma de ICN como premissa. Na literatura, destacam-se três soluções de *cache* para as ICNs: o *cache na rede*, o *cache fora da rede* e o *cache par-a-par*. A Figura 2.4 ilustra os cenários de cada um dos tipos de *cache*, discutidos a seguir.

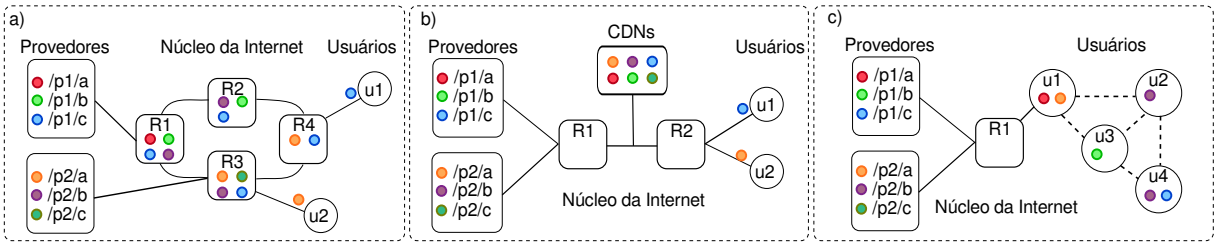

Figura 2.4: Modelos de (a) *cache* na rede, (b) *cache* fora da rede e (c) *cache* par-a-par.

O *cache* na rede explora oportunisticamente a popularidade dos conteúdos através do tráfego de requisições que passam nos roteadores. Tradicionalmente, o *cache* na rede é realizado pelos próprios roteadores, visto a sua posição privilegiada para aferir a popularidade dos conteúdos, como mostra a Figura 2.4(a), além do melhor desempenho proporcionado por *caches* diretamente associados aos roteadores da rede. Já o *cache* fora da rede é realizado por servidores dedicados, similar ao funcionamento das CDNs atuais. Ele é considerado fora da rede por não estar inserido diretamente no núcleo da rede, mas sim nas bordas como cópias dos provedores de conteúdo, como ilustra a Figura 2.4(b). O esquema de *cache* par-a-par é utilizado em redes móveis, por exemplo, em que os dispositivos dos usuários podem ser utilizados para armazenar conteúdo e melhorar a disponibilidade de conteúdo na região. A Figura 2.4(c) apresenta um exemplo deste esquema. Em conjunto com o modelo de *cache* escolhido pela arquitetura de ICN, a arquitetura também deve balancear os critérios de escolha relacionados à manipulação de conteúdos em *cache*, tais como qual conteúdo armazenar, como substituir e quando retirar os conteúdos do *cache*.

2.2 A arquitetura *Named-Data Network*

A nomeação, o roteamento e o *cache* são as áreas principais do paradigma de ICN, contudo, cada arquitetura que instancia esse paradigma defende escolhas de projeto diferentes para cada uma dessas áreas. Neste trabalho, consideramos como referência a arquitetura NDN (*Named-Data Network*) [Jacobson et al., 2009], que é a arquitetura mais consolidada e com um grande número de trabalhos relevantes. A arquitetura NDN foi proposta inicialmente como *Content-centric Network* (CCN) [Jacobson et al., 2009]. Apesar de agora serem tratadas como duas arquiteturas distintas por questões de direitos autorais, elas compartilham todo o fundamento para a construção da arquitetura baseada no paradigma de ICN até 2012, quando cada arquitetura seguiu com grupos de pesquisas distintos. Enquanto a arquitetura CCN é mantida exclusivamente pelo PARC (*Palo Alto Research Center*) com restrições aos códigos fonte, a arquitetura NDN é mantida por acadêmicos de diversas partes do mundo com o objetivo de manter a arquitetura aberta e disponível, assim como acontece com os protocolos da Internet atual. Assim, a proposta da arquitetura NDN é a mais avançada entre as que empregam o paradigma de ICN, sendo apoiada e financiada por grandes indústrias e governos ao redor do mundo [Consortium, 2014] e com uma literatura bastante consolidada com trabalhos que a exploram em diversos aspectos.

A arquitetura NDN utiliza como parâmetro o modelo ampulheta da arquitetura da Internet atual, conforme ilustra a Figura 2.5. O sucesso da Internet tem como base este modelo, pois a adoção de uma camada de rede universal baseada no protocolo IP (Figura 2.5(a)) permitiu a evolução independente das demais camadas, facilitando o crescimento e a popularização da Internet. Por conta dessa experiência, a arquitetura NDN adequa o modelo ampulheta para o paradigma de ICN, eliminando as camadas de transporte e enlace e propondo a adoção de duas outras camadas: segurança e estratégia (Figura 2.5(b)). Enquanto a camada de segurança é específica de cada aplicação e deve conter ações para garantir a segurança do conteúdo, a camada de estratégia trata das escolhas de parâmetros para a transmissão dos conteúdos entre enlaces físicos, possivelmente simultaneamente entre vários enlaces disponíveis [Zhang et al., 2014]. Com isso, a NDN permite que não somente pontos finais sejam nomeados, mas também conteúdos e comandos para alguma ação (acender a luz, por exemplo), enriquecendo a camada de rede ao mesmo tempo que a simplifica e a transforma em um modelo mais adequado para a distribuição de conteúdos.

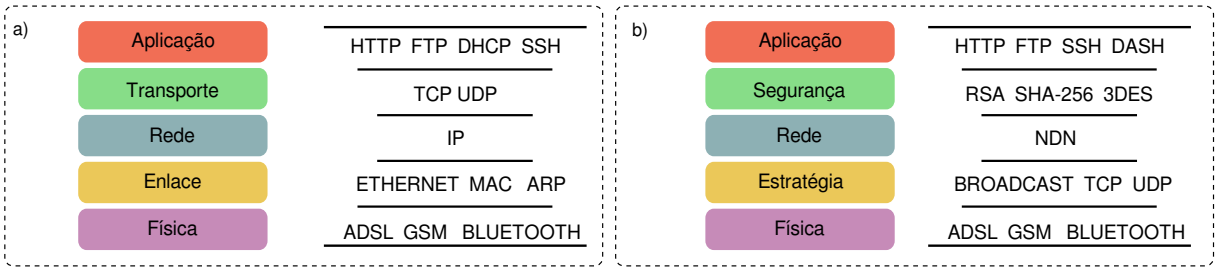

Figura 2.5: Comparação do modelo de camadas das arquiteturas (a) TCP/IP e (b) NDN.

O fluxo de conteúdos na NDN acontece com o envio e o recebimento de dois tipos de pacotes: o pacote de *Interesse* e o pacote de *Dado* [Shilton et al., 2014]. O pacote de *Interesse* é enviado pelo usuário para expressar seu desejo em receber um conteúdo específico na rede. Para isso, ele deve incluir no pacote de *Interesse* o nome do conteúdo desejado. Como resposta, um pacote de *Dado* é enviado para o usuário,

contendo o nome, o conteúdo e uma assinatura que relaciona o nome com o conteúdo para que seja possível verificar a sua integridade. Desta forma, a NDN introduz o conceito de comunicação orientada ao usuário, já que um usuário só recebe um conteúdo se ele enviou um *Interesse* anteriormente. Na arquitetura NDN, os conteúdos são previamente fragmentados em pedaços de tamanhos padrão, chamados de *chunks*. Eles são unicamente nomeados, roteados e seguros. Um conteúdo é recebido por completo por um usuário após o recebimento de todos os *chunks* que o compõem, sendo que *chunks* diferentes de um mesmo conteúdo podem ser recuperados de lugares distintos (provedor ou *cache*).

A arquitetura NDN emprega um esquema de nomeação hierárquica, inspirada na simplicidade da hierarquia dos endereços IP. A arquitetura NDN considera que os provedores de conteúdos são responsáveis pela nomeação do conteúdo e pela administração da hierarquia de nomes, sendo que a rede não impõe restrições quanto à forma do nome do conteúdo, permitindo que eles explorem da melhor forma o esquema de nomes. Contudo, o prefixo dos nomes deve ser globalmente único, o que traz a necessidade de uma entidade global que gerencie os prefixos roteáveis globalmente, similar ao gerenciamento da delegação de endereços IP na Internet atual. Os nomes dos conteúdos na NDN são compostos pela combinação de componentes, similar a como uma URL (*Unified Resource Locator*) é formada. Por exemplo, o nome de conteúdo */exemplo.com/video.avi* pode ser o nome de um vídeo no domínio *exemplo.com*. Além disso, os nomes de conteúdos podem conter informações extras que sejam relevantes para a aplicação, como versão ou índice do segmento do conteúdo. Por exemplo, o conteúdo */exemplo.com/multimidia/videos/video.avi*/1/3 pode representar o segmento 3 da versão 1 do conteúdo */exemplo.com/multimidia/videos/video.avi*. Para a nomeação de conteúdos dinâmicos, como fluxo de conteúdos de uma videoconferência, a NDN propõe duas alternativas: que os usuários e provedores sejam capazes de construir, independentemente, os nomes dos conteúdos com base em informações que ambos possuem de antemão ou o uso de campos específicos dos pacotes de *Interesse*, que permite a descoberta e a recuperação do conteúdo após algumas interações com o provedor.

Assim como as demais arquiteturas que adotam o paradigma de ICN, a arquitetura NDN transfere a segurança para o próprio conteúdo. Com a possibilidade de receber conteúdos de *caches*, por exemplo, é necessário que os usuários possam aferir a integridade e a autenticidade dos conteúdos recebidos. Para verificar a integridade do conteúdo, a arquitetura NDN adota a assinatura do mapeamento entre o conteúdo e o nome do conteúdo. Por exemplo, ao publicar um conteúdo, o provedor cria uma tupla de mapeamento $M(n, p, c) =< n, c, sign_p(n, c) >$, em que n é o nome do conteúdo, p é o provedor do conteúdo, c é o conteúdo e $sign_p(n, c)$ é a assinatura, relacionando o conteúdo com o seu nome. Ao receber o conteúdo, o usuário precisa recuperar a chave pública do provedor para verificar a assinatura e, assim, aferir a integridade do conteúdo recebido [Smetters e Jacobson, 2009]. Além disso, os pacotes de *Interesse* permitem que os usuários possam escolher receber conteúdos de provedores confiáveis através das assinaturas, evitando o recebimento de conteúdos falsos ou de provedores não confiáveis. A definição de esquemas para determinar quais provedores são confiáveis ou em quais chaves confiar ainda é um problema em aberto no paradigma de ICN, inclusive na arquitetura NDN.

Os roteadores na arquitetura NDN são compostos por três entidades principais: a base de informação de roteamento (*Forwarding Information Base* - FIB), a tabela de interesses pendentes (*Pending Interest Table* - PIT) e o armazenamento de conteúdo (*Content Store* - CS). A FIB mantém os registros das interfaces de saída para os nomes globalmente roteáveis contidos na tabela de roteamento e é responsável por rotear as requisições de conteúdo até uma cópia disponível. Qualquer esquema de roteamento

disponível pode ser empregado para o preenchimento das entradas de roteamento da FIB. Já a PIT armazena as informações de requisições de conteúdos pendentes, que são compostas pelo nome do conteúdo solicitado e pela interface de entrada. As entradas da PIT são consumidas no momento em que uma resposta para uma determinada requisição é recebida e encaminhada para a interface de entrada. No caso de o roteador não receber uma resposta para uma requisição dentro de um tempo limite, por conta de perda de pacotes, por exemplo, a entrada da PIT correspondente expira.

Além disso, entradas na PIT para o mesmo conteúdo, mesmo que vindas de interfaces distintas, são agregadas para melhoria da escalabilidade e desempenho da rede. Assim, somente a primeira requisição recebida por um roteador é enviada adiante, o que resulta em um balanceamento de fluxo, já que cada *Dado* recebido corresponde a um *Interesse* enviado. Além disso, por conta do uso de conteúdos nomeados na camada de rede, um pacote de *Dado* pode ser útil para mais de um usuário na rede, o que permite que os roteadores armazenem os conteúdos em *cache* e os utilizem para satisfazer requisições futuras. O CS armazena os conteúdos de acordo com as políticas de *cache* adotadas pelo roteador. Cada roteador é capaz de armazenar conteúdos com base nas requisições que trafegam por ele, desta forma, os provedores de conteúdo não precisam ser contatados em todas as requisições de seus conteúdos; a rede pode fornecer uma cópia disponível em *cache*. Quanto mais perto do usuário a cópia do conteúdo é acessada, mais rápida e eficiente é a entrega desse conteúdo.

A Figura 2.6 apresenta o funcionamento básico de um roteador na NDN. Ao receber um pacote de *Interesse* para o conteúdo $/p2/c$, primeiramente o roteador verifica a CS. Se o conteúdo estiver no *cache*, ele é prontamente enviado para a interface de entrada (interface 1). De outra forma, o roteador verifica se existe uma entrada na PIT para esse conteúdo. Se houver, ele acrescenta a interface de entrada da requisição nesse registro da PIT, caso contrário, ele adiciona uma nova entrada na PIT para essa requisição e verifica as entradas da FIB para encontrar a interface em que deve enviar a requisição em busca do conteúdo (interface 2). A requisição segue esse procedimento em todos os roteadores, até que o conteúdo seja satisfeito por um *cache* em algum roteador no caminho ou que o provedor do conteúdo seja consultado. Essas atividades estão ilustradas na Figura 2.6(a). Um pacote de *Dado* contendo o conteúdo solicitado trafega até o usuário pelo caminho inverso do envio do pacote de *Interesse*. A Figura 2.6(b) ilustra esse encaminhamento. Ao receber um pacote de *Dado*, primeiramente o roteador verifica se há uma entrada na PIT para esse conteúdo. Se não houver uma entrada que corresponda ao conteúdo recebido, ele é descartado, já que é um conteúdo não solicitado. De outra forma, o roteador armazena o conteúdo em seu *cache* de acordo com as políticas locais de *cache*, e então envia o conteúdo para as interfaces que estão aguardando.

No caso de uma requisição que não pode ser completada, seja pela falta de entradas na FIB ou por falhas nos enlaces, o roteador envia um $NACK$ (*non acknowledgement*) para a interface de entrada, que pode reenviar a requisição por um caminho alternativo. Como a arquitetura NDN não possui uma camada de transporte, as funções que tradicionalmente seriam dessa camada, como entrega confiável e controle de congestionamento, são realizadas e gerenciadas diretamente pelas aplicações e pela camada de estratégia do modelo da NDN, que tem a intenção de englobar os serviços da camada de transporte tradicional.

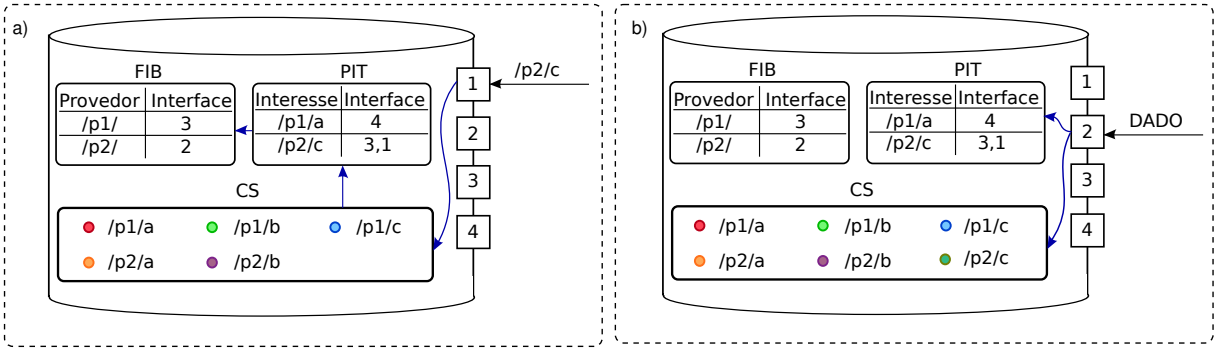

Figura 2.6: Esquema de um roteador na arquitetura NDN.

2.2.1 Outras arquiteturas

Além da arquitetura NDN, existem outras que também propõem o uso do paradigma de ICN para uma melhor distribuição de conteúdo, como a *Data-Oriented Network Architecture* (DONA) [Koponen et al., 2007], a *Network of Information* (NetInf) [Dannewitz et al., 2013] e a *Pursuing a Pub/Sub Internet* (PURSUIT) [Trossen e Parisis, 2012]. Todas elas compartilham os mesmos componentes básicos do paradigma de ICN, isto é, conteúdo nomeado, roteamento e encaminhamento pelo nome do conteúdo e *cache* na rede. Entretanto, cada uma tem suas peculiaridades com relação à implementação de tais funções, resumidas a seguir.

A arquitetura *Data-Oriented Network Architecture* (DONA) [Koponen et al., 2007] é uma das precursoras a propor o uso do paradigma de ICN na Internet. Como a pioneira, ela propõe a adoção do paradigma de ICN como uma camada sobre o protocolo IP e, desta forma, não provê todos os benefícios que a ICN oferece, visto que as deficiências do protocolo IP continuam presentes. Nesse modelo os conteúdos são nomeados pelo provedor do conteúdo, no formato $P : L$, em que P é o *hash* da chave pública do provedor e L é um nome arbitrário escolhido para identificar o conteúdo. Um usuário, ao requisitar um conteúdo, receberá uma tupla composta por <conteúdo, chave pública, assinatura>, permitindo que o usuário possa aferir a integridade ao comparar a assinatura do conteúdo e a chave pública do provedor. O roteamento é realizado pelos protocolos tradicionais de roteamento com o suporte de manipuladores de resolução (*Resolution Handlers* - RH), similar ao DNS utilizado tradicionalmente. Os RHs são organizados de forma hierárquica e a sua função é manter os registros de localização dos conteúdos. Cada entidade que queira oferecer um conteúdo o registra em seu RH local. Os usuários enviam as requisições para o seu RH local, que por sua vez, encontra a cópia mais próxima por meio dos seus registros. A partir de então, tanto a requisição quanto a resposta são enviadas pelos roteadores utilizando os protocolos de roteamento padrão. Se um RH tem interesse em armazenar em *cache* o conteúdo correspondente a uma requisição, ele deve modificar o endereço de requisição para que esse conteúdo específico chegue até ele antes de ser encaminhado ao usuário original. Desta forma, o RH pode armazenar o conteúdo em seu *cache* de acordo com a popularidade, por exemplo.

Já a arquitetura *Network of Information* (NetInf) [Dannewitz et al., 2013] referencia seus conteúdos como objetos de dados nomeados (*Named Data Object* - NDO). Cada NDO é nomeado de acordo com o esquema de nomeação plana [Farrell et al., 2013]. Desta forma, o NetInf garante a unicidade dos nomes dos NDOs. A integridade dos NDOs é realizada ao checar o valor de *hash* recebido no nome do NDO com o cálculo do *hash* do conteúdo recebido. A arquitetura NetInf emprega o roteamento baseado em nomes

com auxílio de um serviço de resolução de nomes (NRS). O serviço de resolução de nomes complementa o roteamento baseado em nomes, ao prover formas de localizar os NDOs na rede através de dicas de roteamento, que indicam onde encontrar diretamente o NDO ou o próximo salto em direção ao NDO. Para disponibilizar um NDO na rede, o provedor do conteúdo deve enviar uma mensagem para o NRS, contendo o nome do NDO e as dicas de roteamento correspondentes. Para solicitar um NDO, o usuário deve primeiramente buscar as dicas de roteamento. O NRS responde com uma lista de NDOs que correspondem à pesquisa, juntamente com as dicas de roteamento. Para encaminhar o NDO para o usuário solicitante, a arquitetura NetInf permite o uso de duas estratégias: os roteadores podem manter os estados das requisições e, desta forma, o NDO segue o mesmo caminho da requisição, ou as requisições podem ser rotuladas com informações de rede, assim, essas informações guiam o NDO até o usuário.

A arquitetura PURSUIT (*Pursuing a Pub/Sub Internet*) [Trossen e Parisis, 2012] incorpora o modelo *publish/subscribe* [Eugster et al., 2003] no paradigma de redes centradas em informação. Na arquitetura PURSUIT, os *publicadores* são provedores que fornecem conteúdo para a rede e os *assinantes* são usuários que expressam seus interesses em determinados conteúdos. Ao utilizar esse modelo, a arquitetura PURSUIT se diferencia das demais arquiteturas principalmente com relação ao roteamento e a forma como os provedores anunciam seus conteúdos. A arquitetura PURSUIT adota um esquema de nomeação plana, com a assistência de uma árvore de informação hierárquica organizada e gerenciada pelos *rendezvous nodes* (que correspondem aos roteadores no modelo tradicional), que organizam os conteúdos em *escopos* [Fotiou et al., 2012]. Para publicar conteúdos na rede, os publicadores criam os escopos e anunciam para o *rendezvous*. Cada domínio tem um *rendezvous node* interconectado globalmente por uma DHT (*Distributed Hash Table*) hierárquica, responsável por mediar as requisições de publicação e assinatura de conteúdos. Os *rendezvous nodes* locais anunciam seus escopos para a infraestrutura DHT para que seus conteúdos sejam vistos globalmente. Os usuários acessam os conteúdos enviando uma requisição para o *rendezvous node* responsável pelo conteúdo, que por sua vez relaciona a requisição com um conteúdo previamente publicado. Qualquer nó que encaminha conteúdo na rede pode manter cópias de conteúdos em seus *caches*, desta forma se tornando um publicador para esse conteúdo específico.

2.3 Considerações finais

Este capítulo apresentou o paradigma das redes centradas em informação e detalhou os seus três componentes básicos: nomeação, roteamento e *cache* na rede. Também descreveu com detalhes as particularidades de projeto da arquitetura NDN, como a nomeação hierárquica, o roteamento pelo nome do conteúdo e o *cache* refletindo o padrão de acesso dos usuários. Apesar do potencial das ICNs na melhoria da distribuição de conteúdos na rede, este novo paradigma também apresenta diversos desafios, principalmente com relação à segurança. O próximo capítulo apresenta uma visão detalhada e organizada das vulnerabilidades e ataques de segurança do paradigma de ICN, destacando o problema do acesso não autorizado aos conteúdos armazenados em *cache* na rede.

Capítulo 3

Desafios de segurança em ICN

Este capítulo apresenta alguns dos principais desafios de segurança das redes centradas em informação e propõe uma organização da literatura para os ataques de segurança. O capítulo está dividido em duas seções: a Seção 3.1 lista os principais ataques e vulnerabilidades de segurança na nomeação, no roteamento e no *cache* do paradigma de ICN. A Seção 3.2 discute as implicações inerentes do modelo de comunicação da ICN no acesso controlado ao conteúdo, classificando as soluções de controle de acesso e analisando os benefícios e limitações de cada classe.

3.1 Ataques e vulnerabilidades em ICN

Apesar dos grandes benefícios na adoção do paradigma de ICN para a distribuição de conteúdos, a mudança profunda que ela representa na camada de rede invariavelmente leva a novos desafios de segurança [Brito et al., 2012, AbdAllah et al., 2015a]. Na nomeação de conteúdos, por exemplo, é consenso entre as arquiteturas de ICN que se forneça algum tipo de mecanismo de verificação de integridade e autenticidade para o conteúdo, de preferência embutido no próprio nome, permitindo que os usuários possam verificar se ele foi modificado e decidir se confiam no conteúdo recebido. No roteamento, a preocupação é com relação à robustez diante de ataques de negação de serviço, já que a quantidade de conteúdos nomeados representa muito mais entradas nas tabelas de roteamento do que endereços IP tradicionais; desta forma, a arquitetura deve oferecer meios de proteger as tabelas de roteamento de serem exploradas com o registro de entradas inválidas, por exemplo. Já os mecanismos de *cache* introduzidos pela ICN também podem ser alvos de entidades maliciosas; desta forma, são necessárias medidas de segurança que evitem ataques amplamente conhecidos, como poluição e espionagem de *cache*.

Para entender melhor as vulnerabilidades do paradigma de ICN e como os ataques prejudicam o funcionamento das arquiteturas, os ataques de segurança são organizados em três domínios principais: segurança no conteúdo, no roteamento e no *cache*. Cada um desses domínios é classificado em três classes. A segurança no conteúdo engloba ameaças na integridade, privacidade e acesso não autorizado. A segurança no roteamento inclui os ataques que visam a exaustão de recursos dos roteadores, a indisponibilidade dos provedores e o esgotamento de rotas para os conteúdos. Já a segurança no mecanismo de *cache* apresenta as ameaças de espionagem, poluição e envenenamento. A análise apresentada vai além de [Ribeiro et al., 2012, AbdAllah et al., 2015a] ao analisar o paradigma de ICN como um todo, sem focar em uma arquitetura específica. A Figura 3.1 ilustra cada um

desses domínios e suas respectivas classes de ataques, bem como as entidades maliciosas que são mais propensas a explorar cada vulnerabilidade.

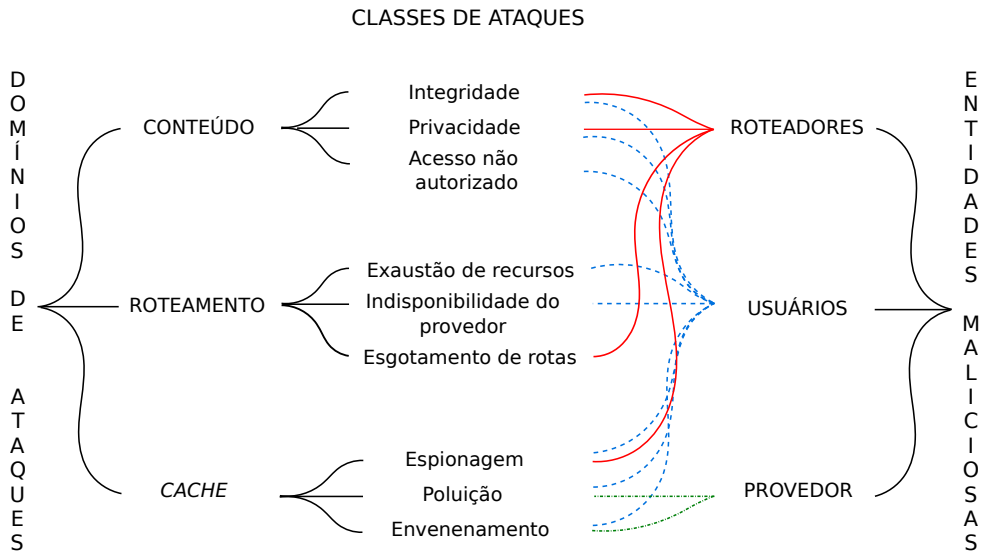

Figura 3.1: Organização dos ataques de segurança em ICN.

Em geral, os ataques nas arquiteturas de ICN podem ser iniciados por qualquer entidade da rede: usuários, provedores de conteúdo, roteadores e entidades que armazenam conteúdos em *cache*. Neste trabalho, denomina-se maliciosa qualquer uma dessas entidades que utiliza a rede de forma incorreta, com o objetivo de explorar as vulnerabilidades da arquitetura de ICN para interromper os serviços da rede, comprometer a privacidade dos usuários ou dos provedores de conteúdo e obter acesso indevido a recursos protegidos. Tais entidades maliciosas podem agir sozinhas ou em conluio para aumentar o efeito do ataque. Também considera-se que as entidades maliciosas podem se apresentar com recursos limitados, como usuários com computadores domésticos, por exemplo, ou ainda entidades maliciosas que possuem um grande poder computacional disponível para os ataques, tais como roteadores, provedores de conteúdo e agências de governos.

Segurança no conteúdo

A nomeação de conteúdo é uma das áreas que mais precisam de atenção em relação à segurança, uma vez que é o núcleo de qualquer arquitetura de ICN. Tão importante quanto a proteção do nome atribuído ao conteúdo é a proteção do próprio conteúdo. Devido à possibilidade de desacoplar o conteúdo da sua localização e armazená-lo em entidades terceiras, o conteúdo é suscetível a ameaças relacionadas à integridade, à privacidade e ao acesso não autorizado. A Figura 3.2 apresenta um exemplo de cada uma dessas classes (entidades da cor preta são maliciosas).

A integridade dos conteúdos pode ser ameaçada por usuários maliciosos que adulteram os conteúdos, renomeando ou corrompendo, já que eles têm fácil acesso aos mesmos através dos *caches* [Hamdane et al., 2012, Ribeiro et al., 2014], conforme ilustra a Figura 3.2(a), em que o roteador $R2$ modifica o conteúdo de uma cópia em *cache* e responde a requisição de $u2$ com a cópia adulterada. Esses ataques comprometem a integridade dos conteúdos pois fazem com que os usuários recebam conteúdos corrompidos ou que não correspondam à requisição feita. Portanto, mecanismos para garantia da integridade e da autenticidade do conteúdo têm sido considerados desde a concepção

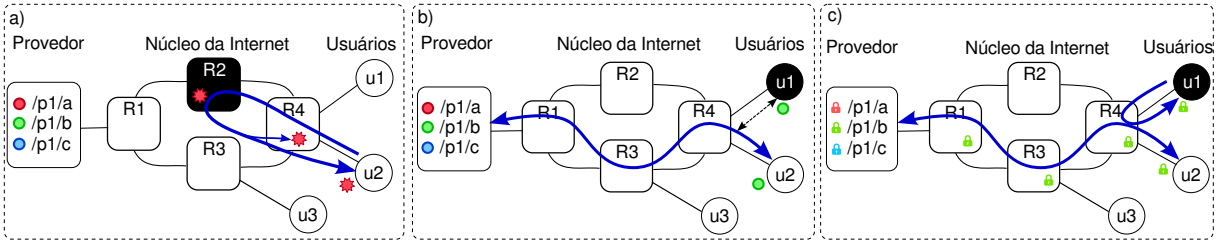

Figura 3.2: Funcionamento básico das classes de ataques no conteúdo: (a) integridade, (b) privacidade e (c) acesso não autorizado.

dos esquemas de nomeação, através da adoção de assinaturas digitais para fornecer garantias sobre a proveniência e a integridade do conteúdo [Smetters e Jacobson, 2009, Dannewitz et al., 2010, Baugher et al., 2012, Goldman et al., 2014]. Alternativamente, esquemas de criptografia baseada em identidade (*Identity-Based Encryption* - IBE) também são propostos para aferir a integridade e a autenticidade do conteúdo [Zhang et al., 2011, Hamdane et al., 2012, Vieira e Poll, 2013, Hamdane et al., 2014]. Neste caso, os próprios nomes dos conteúdos podem servir como a chave pública do provedor.

Outro aspecto derivado das soluções para integridade e autenticidade é a gerência de confiança das chaves dos provedores de conteúdos, já que para verificar a integridade e a autenticidade de um conteúdo, deve-se confiar na chave que o assina. Apesar de nenhum mecanismo de gerência de confiança específico ser adotado pelas arquiteturas de ICN, diversas alternativas aos esquemas tradicionais já foram propostas, principalmente explorando mecanismos distribuídos e descentralizados [Jeong et al., 2010, Wong e Nikander, 2010, Arianfar et al., 2011, Wong e Magalhães, 2012, Lu et al., 2013, Khan et al., 2013, Mauri e Verticale, 2013, Chaabane et al., 2013, Massawe et al., 2013, Acs et al., 2013, Khan et al., 2014, Mahadevan et al., 2014].

A privacidade dos usuários e dos provedores também é afetada pela forma como a ICN funciona [Compagno et al., 2015], pois os roteadores e detentores de *caches* têm ciência do nome do conteúdo que trafega na rede, sendo possível que entidades maliciosas explorem esta característica para monitorar, filtrar e bloquear requisições específicas de usuários ou provedores de conteúdos, com base nos nomes [Arianfar et al., 2011, Massawe et al., 2013, Acs et al., 2013]. A Figura 3.2(b) ilustra um exemplo em que o usuário $u1$ monitora o canal e descobre o que $u2$ está acessando, pelo nome do conteúdo. Embora seja difícil identificar o usuário específico que está solicitando determinado conteúdo, este ataque poderia ser construído para negar serviço ou censurar certos conteúdos para alvos específicos. O principal mecanismo para prover privacidade em ICN é ocultar ou mascarar o conteúdo em requisições para a rede [Bonomi et al., 2006, Fotiou et al., 2014, Cui et al., 2016]. Apesar da cifragem da requisição ser uma solução que permita sigilo perfeito para o usuário, ela exige a colaboração do provedor, além de influenciar no desempenho dos mecanismos de *cache* [Tourani et al., 2015]. Esse problema também surge nas soluções que se baseiam na cifragem da requisição para um circuito específico de roteadores ou usuários, semelhante ao TOR (*The Onion Router*) [DiBenedetto et al., 2011, Tsudik et al., 2014, Seo et al., 2014].

Já a possibilidade de que as requisições dos usuários sejam satisfeitas por cópias armazenadas em entidades não controladas pelos provedores de conteúdo traz a preocupação com a garantia da aplicação de políticas de controle de acesso dos conteúdos [Ion et al., 2013, Loo e Aiash, 2015]. A Figura 3.2(c) apresenta um exemplo simples de acesso não autorizado, em que o usuário $u1$ descobre o nome de um conteúdo protegido e o solicita diretamente ao *cache*, que atende à requisição. Caso esse conteúdo não esteja

protegido, ele pode ser utilizado pelo usuário $u1$ sem que o provedor tenha conhecimento desse acesso. As soluções existentes para o controle de acesso aos conteúdos em *cache* serão detalhadas na próxima seção.

Segurança no roteamento

Os roteadores são, sem dúvidas, as entidades mais importantes de uma rede. Eles são responsáveis por encontrar o conteúdo na rede, encaminhá-lo ao usuário e gerenciar e atualizar todas as informações de roteamento em suas tabelas. Com a adoção do paradigma de ICN, há uma mudança substancial em como os roteadores desempenham essas funções, modificando a forma e o impacto de ataques conhecidos, como os ataques de exaustão de recursos, os que visam a indisponibilidade do provedor e os de esgotamento de rota. A Figura 3.3 ilustra essas três classes de ataques.

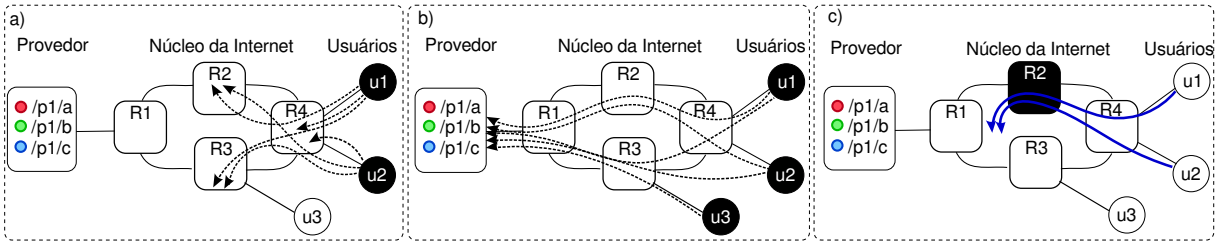

Figura 3.3: Funcionamento básico das classes de ataques no roteamento: (a) exaustão de recursos, (b) indisponibilidade do provedor e (c) esgotamento de rotas.

Os ataques de exaustão de recursos exploram o fato que os roteadores mantêm o registro das requisições recebidas dos usuários para cada interface de rede, que serve para que o conteúdo seja encaminhado para o usuário no caminho reverso da sua requisição. Este mecanismo é apontado como potencialmente vulnerável a ataques de negação de serviço, através do recebimento de inúmeras requisições maliciosas, conforme mostra a Figura 3.3(a). Porém tais ataques necessitam de uma preparação especial por parte dos usuários maliciosos, pois as entradas de requisições para o mesmo conteúdo são agregadas por questões de desempenho. Os usuários maliciosos podem, por exemplo, requisitar conteúdos aleatórios de prefixos diferentes, que exijam entradas distintas na tabela [Gasti et al., 2012, Goergen et al., 2012, Choi et al., 2013, Dai et al., 2013, Afanasyev et al., 2013, Compagno et al., 2013, Virgilio et al., 2013, Wählisch et al., 2013b, Elechi et al., 2014, Karami e Guerrero-Zapata, 2015] ou ainda agir em conluio com um provedor malicioso que não responde às requisições [Lauinger, 2010, Wang et al., 2013, Wählisch et al., 2013a].

Outro ataque no roteamento é realizado ao concentrar as requisições maliciosas em um único provedor ou prefixo específico, o que pode interromper o fornecimento de serviços por parte do provedor de conteúdo atacado [Lauinger, 2010, Gasti et al., 2012]. A Figura 3.3(b) ilustra um ataque em que usuários maliciosos enviam requisições diretamente para uma única vítima. No entanto, os usuários maliciosos precisam se certificar que os conteúdos solicitados não sejam satisfeitos por *caches* no caminho até o provedor, anexando nomes de conteúdos inexistentes ao prefixo do provedor, induzindo o mecanismo de roteamento a encaminhar a requisição diretamente para o provedor do prefixo [Lauinger, 2010, Gasti et al., 2012, Wang et al., 2012, Afanasyev et al., 2013, Compagno et al., 2013, Dai et al., 2013].

As primeiras tentativas de mitigar os ataques de exaustão de recursos e prevenir a indisponibilidade de provedores têm como método principal o monitoramento e a identificação de grandes quantidades de requisições nos roteadores [Nguyen et al., 2015, AbdAllah et al., 2015b, Al-Sheikh et al., 2015]. As métricas para o monitoramento podem ser a taxa de requisições não satisfeitas [Fotiou et al., 2010, Gasti et al., 2012, Goergen et al., 2012, Karami, 2013, Alzahrani et al., 2013c, Alzahrani et al., 2013b, Alzahrani et al., 2013a, Wang et al., 2014a, Karami e Guerrero-Zapata, 2014, Karami e Guerrero-Zapata, 2015], a quantidade de espaço de armazenamento utilizado pelas entradas da PIT [Compagno et al., 2013], ou ainda a quantidade de requisições por interface do roteador [Afanasyev et al., 2013, Nguyen et al., 2015]. Assim, caso os roteadores detectem quantidades anormais de conteúdos distintos requisitados em uma mesma interface, por exemplo, eles podem limitar as requisições de tal interface, ou responder à interface maliciosa com conteúdos vazios que satisfazem essas solicitações suspeitas, limpando as entradas dos roteadores [Dai et al., 2013].

O ataque de exaustão de rota, apresentado na Figura 3.3(c), explora as entradas das tabelas de roteamento, registrando rotas falsas ou maliciosas [Goergen et al., 2012, Wählisch et al., 2013a]. Alternativamente, um roteador malicioso pode registrar rotas para conteúdos válidos em que ele se coloca como parte da rota com o objetivo de descartar ou atrasar as respostas das requisições [Gasti et al., 2012, Wählisch et al., 2013b]. Este ataque pode ser ainda mais agressivo quando se considera uma rede de colaboração, tais como as redes móveis *ad hoc*, em que os usuários assumem naturalmente o papel de roteadores para encaminhar pacotes. Neste caso, entidades maliciosas podem modificar as informações de roteamento ou desviar o tráfego para roteadores maliciosos que servem conteúdos maliciosos [Loo e Aiash, 2015]. Para evitar tais ameaças, as arquiteturas de ICN preveem que o anúncio de rotas entre os roteadores seja assinado, portanto, passíveis de verificação, evitando que usuários maliciosos registrem rotas falsas [Gasti et al., 2012, Wählisch et al., 2013a].

Segurança no *cache*

A existência de *cache* na rede é uma das características mais proeminentes das arquiteturas de ICN. Ele tem como função melhorar a distribuição de conteúdo na rede, posicionando cópias dos conteúdos mais perto dos usuários. Contudo, os mecanismos de *caching* não são novidade e, portanto, há um conjunto bem conhecido de ameaças contra os sistemas de *cache* em redes tradicionais, como espionagem, poluição e envenenamento, que consequentemente ameaçam o paradigma de ICN, como mostra a Figura 3.4.

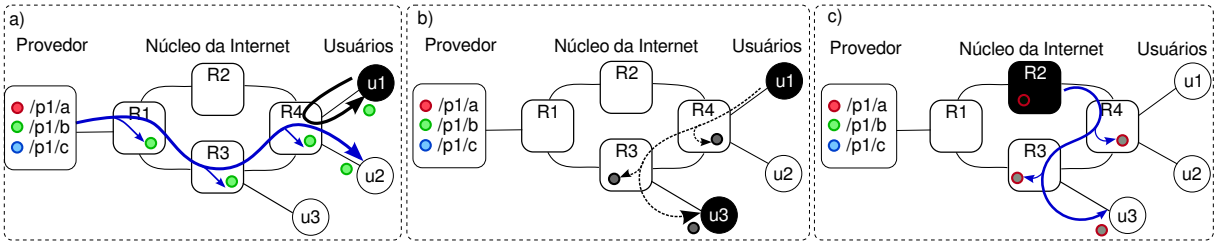

Figura 3.4: Funcionamento básico das classes de ataques no conteúdo: (a) espionagem, (b) poluição e (c) envenenamento.

Uma das políticas de *cache* mais interessantes para ser adotada pelas arquiteturas de ICN é o armazenamento de cópias de conteúdos de acordo com o padrão de acesso dos usuários. Porém, essa política faz com que o *cache*, involuntariamente, represente o comportamento dos usuários na Internet, que pode ser explorado a fim de obter informações confidenciais sobre um usuário ou um grupo de usuários [Mauri e Verticale, 2014] através da espionagem, como ilustrado na Figura 3.4(a). Para espionar os conteúdos em *cache* um usuário malicioso pode, por exemplo, listar os conteúdos de seu *cache* imediato para verificar em quais conteúdos os usuários estão mais interessados [Lauinger, 2010, Lauinger et al., 2011, Ntuli e Han, 2012] ou pela diferença do tempo entre respostas obtidas do *cache* e do provedor de conteúdo [Lauinger, 2010, Mohaisen et al., 2012, Chaabane et al., 2013, Acs et al., 2013]. Contudo, embora estes ataques sejam viáveis e representem uma ameaça contra a privacidade dos usuários, é consenso geral que correlacionar um usuário específico com um conteúdo em *cache* não é trivial e pode exigir informações adicionais por parte das entidades maliciosas. Além disso, os usuários maliciosos podem influenciar o *cache* ao solicitar uma grande quantidade de conteúdo impopular, a fim de interromper a relevância local do conteúdo e degradar a eficiência do *cache* [Lauinger, 2010, Xie et al., 2012, Conti et al., 2013, Gouge et al., 2016]. Isso pode fazer com que todo o ganho com o uso de *caches* na rede seja perdido, pois quanto menos cópias relevantes nos *caches*, mais requisições são encaminhadas diretamente para o provedor de conteúdo [Cieza et al., 2015, Pires e Moraes, 2015].

O uso de um sistema de monitoramento é a contramedida mais indicada para evitar os ataques de espionagem, pois verificam e contabilizam altas taxas de requisições enviadas para o *cache* em um curto período de tempo e a taxa de sucesso de requisições encontradas no *cache* local [Ntuli e Han, 2012]. Já para lidar com ataques que utilizam as informações de tempo de resposta, a estratégia mais utilizada é o adiamento das respostas enviadas pelos *caches*, a fim de igualar os tempos de resposta do *cache* com o tempo do provedor do conteúdo [Lauinger, 2010, Mohaisen et al., 2012, Chaabane et al., 2013, Mohaisen et al., 2015, Ding et al., 2014]. O uso de *caches* colaborativos também pode ser usado como contramedida para esses ataques, pois aumenta o conjunto de locais em que o conteúdo pode estar armazenado, desafiando o usuário malicioso a descobrir se o conteúdo estava em *cache* ou não [Chaabane et al., 2013].

Os ataques de poluição e de envenenamento de *cache* são parecidos em sua forma de ataque, porém distintos nas consequências para a rede e os usuários. A Figura 3.4(b) exemplifica um ataque de poluição realizado por dois usuários maliciosos; um solicita conteúdo irrelevante e outro atende a essas requisições, poluindo os *caches* no caminho entre os dois. Neste ataque, os benefícios do *cache* na rede são comprometidos, pois os conteúdos em *cache* não são de interesse dos usuários. Já os ataques de envenenamento de *cache* são facilitados pelo uso de conteúdos nomeados na camada de rede, pois usuários maliciosos podem antecipar a nomeação de um conteúdo relevante e anunciá-lo na rede, porém o conteúdo é ilegal ou não corresponde ao nome atribuído ao conteúdo [Fotiou et al., 2010], conforme ilustra a Figura 3.4(c), em que um roteador malicioso popula os *caches* de antemão com conteúdos de interesse, porém, forjados. Quando o conteúdo verdadeiro se tornar disponível, os *caches* irão satisfazer as requisições com o conteúdo falso que eles armazenaram anteriormente [Gasti et al., 2012, Ghali et al., 2014b, Loo e Aiash, 2015].

O monitoramento dos conteúdos armazenados em *caches* também é a principal estratégia utilizada para evitar o armazenamento de conteúdos irrelevantes [Goergen et al., 2012, Karami e Guerrero-Zapata, 2015, Xu et al., 2015]. Além disso, com o apoio desses mecanismos de monitoramento, pode-se aplicar estratégias probabilís-

ticas para decidir se um conteúdo deve ser armazenado em *cache* [Xie et al., 2012, Conti et al., 2013]. Considerando o ataque de envenenamento, o paradigma de ICN não oferece meios de evitar naturalmente a distribuição de conteúdo falso, pois a saída dos conteúdos do *cache* depende do modelo de substituição de conteúdo adotado pelo *cache*, ou pela exclusão explícita de determinados conteúdos indesejados indicados através de campos específicos das requisições dos usuários [Ghali et al., 2014b]. A abordagem básica contra esses ataques é a verificação da proveniência do conteúdo, o que pode ser feito através da verificação das assinaturas dos conteúdos antes que sejam armazenados em *cache* [Gasti et al., 2012, Ghali et al., 2014c, Ghali et al., 2014a, Ribeiro et al., 2014, Ghali et al., 2015a, Hyung Kim et al., 2015].

3.2 O desafio do controle de acesso

A infraestrutura de armazenamento em *cache* na rede, introduzida pelo paradigma de ICN, representa um grande desafio para a proteção dos conteúdos contra acesso não autorizado, pois já não é obrigatória a conexão com um servidor específico para um usuário recuperar um conteúdo. Os provedores, por exemplo, não têm controle sobre os dispositivos que armazenam em *cache* seus conteúdos, nem interagem com os usuários que têm suas requisições satisfeitas por *caches* na rede, naturalmente prejudicando o controle e a execução de políticas de acesso. Além disso, o conteúdo pode ser armazenado em *caches* ao longo do caminho por entidades não confiáveis, tais como roteadores, dispositivos móveis ou servidores terceirizados (como em uma CDN), facilitando a distribuição não autorizada de conteúdos protegidos [Ion et al., 2013, Loo e Aiash, 2015].

Neste trabalho, considera-se como *controle de acesso* na distribuição de conteúdo em ICN a garantia de que o provedor de conteúdo possa impor as *regras de controle de acesso* desejadas, decidindo quem pode acessar o conteúdo que ele disponibiliza na rede. Essa decisão é tomada a partir de uma *política de controle de acesso* que define regras, como por exemplo, o pagamento de mensalidades, se o conteúdo está de acordo com o serviço contratado, com o tipo de inscrição ou com a idade do usuário. A dificuldade de aplicar políticas de acesso aos conteúdos em *cache* pode ser dividida em três pilares principais: (1) os *caches* podem ser acessados por qualquer usuário; (2) os roteadores não aplicam políticas de controle de acesso antes de satisfazer a uma requisição; e (3) enquanto a manutenção de um conteúdo específico em *cache* seja benéfico para a rede, os roteadores podem não seguir as regras de substituição de conteúdos do *cache* e servir conteúdo obsoleto aos usuários.

O problema do controle de acesso em ICN destaca-se especialmente quando se considera a distribuição de conteúdos protegidos ou com direitos autorais, como filmes, músicas e *softwares*. Para serviços que oferecem esse tipo de conteúdo, tais como *Netflix*, *Hulu*, *Amazon*, *Apple Store*, *Play Store* e *Steam*, o controle de acesso faz parte do negócio, pois o acesso geralmente requer um rigoroso controle das contas de usuários, do número de reproduções do conteúdo e da quantidade de dispositivos autorizados, por exemplo, exigindo a conformidade do usuário com regras estritas do provedor. Assim, divulgar esse tipo de conteúdo na Internet sem a possibilidade de aplicar políticas de controle de acesso seria prejudicial para os provedores de conteúdo. As soluções atuais para controle de acesso na distribuição de conteúdo, apesar de serem transferíveis para ICN, geralmente inviabilizam a proposta do uso de *cache* na rede, pois exigem a cifragem do fluxo fim a fim, por exemplo. Desse modo, há uma necessidade óbvia em reforçar o controle de acesso

no conteúdo recuperado a partir de *caches*, ao mesmo tempo permitindo que o *cache* seja amplamente utilizado.

Restringir o conhecimento do nome do conteúdo somente para os usuários autorizados não é suficiente para o controle de acesso em ICN, já que as ações de roteamento e de encaminhamento são realizadas diretamente pelo nome do conteúdo e, desta forma, os nomes podem ser facilmente descobertos por ataques de espionagem, por exemplo [Lauinger, 2010, Massawe et al., 2013, Chaabane et al., 2013]. A cifragem do conteúdo é a solução pioneira em ICN para garantia que somente usuários autorizados, que possuam uma chave válida, possam acessá-lo (s2) [Jacobson et al., 2012]. Contudo, a cifragem de um mesmo conteúdo para usuários diferentes não é conveniente, pois o conteúdo cifrado para um usuário específico não pode ser acessado por outro e, portanto, as cópias armazenadas em *cache* não são aproveitadas.

Diversas soluções para controle de acesso foram propostas considerando as especificações das diferentes arquiteturas de ICN. Para uma melhor compreensão do estado da arte, as soluções de controle de acesso para ICN são divididas em quatro grupos: baseadas em criptografia, baseadas em infraestrutura, híbridas e outras. As soluções baseadas em criptografia utilizam algum esquema criptográfico para proteger o acesso ao conteúdo, independente do local em que o conteúdo for recuperado. Já as soluções baseadas em infraestrutura introduzem o uso de servidores dedicados ou utilizam os recursos da própria infraestrutura de ICN para validar políticas de acesso aos conteúdos antes de enviá-los para um usuário. As soluções híbridas trabalham com esquemas criptográficos em conjunto com alguma infraestrutura de validação de acesso, enquanto que a categoria outros apresenta os trabalhos que não se encaixam nas categorias acima, como controlar quais entidades podem armazenar certos conteúdos em *cache* para evitar a divulgação não autorizada deles. A seguir apresenta-se uma revisão da literatura em cada uma das categorias propostas.

3.2.1 Soluções baseadas em criptografia

Em geral, as soluções baseadas em criptografia utilizam uma chave secreta para cifrar os conteúdos, enquanto a chave secreta é distribuída cifrada com algum esquema de criptografia assimétrica [Zhu et al., 2011, Yu et al., 2015]. Diversos esquemas criptográficos alternativos têm sido empregados para a distribuição de chaves secretas para os usuários autorizados, visando o aproveitamento do conteúdo por um conjunto de usuários, tais como a criptografia de *broadcast* (*Broadcast Encryption* - BE) (s6) [**?**], a criptografia baseada em atributos (*Attribute-based Encryption* - ABE) (s7, s10) [**?**, **?**], a recifragem por *proxy* [Ateniese et al., 2006] e chaves de sessão. O uso da BE [Misra et al., 2013, Posch et al., 2013] permite que a chave secreta seja distribuída cifrada com a chave do grupo de *broadcast*. Cada usuário autorizado pertencente ao grupo recebe uma chave individual, no momento do seu registro no provedor, que é utilizada para decifrar as mensagens cifradas com a chave do grupo. Com o ABE, cada usuário tem sua chave representando seus atributos perante o provedor, sendo que a chave secreta é cifrada com os atributos permitidos a acessá-la, garantindo que somente os usuários cujas chaves reflitam os atributos necessários possam recuperar a chave secreta e acessar o conteúdo [Papanis et al., 2013, Li et al., 2014]. Na recifragem por *proxy*, além de receber a chave secreta cifrada, cada usuário recebe também uma chave de recifragem, que permite a transformação da cifra recebida em uma mensagem que pode ser decifrada com a chave privada do próprio usuário (s12) [Wood e Uzun, 2014]. Por fim, as chaves de sessão são

chaves efêmeras utilizadas para o envio da chave secreta do conteúdo para o usuário [Wang et al., 2014b] (s9).

Visando a evolução das soluções criptográficas para o controle de acesso em ICN, [Kurihara et al., 2015] propõem um *framework* de controle de acesso, chamado CCN-AC (*CCN Access Control*) que pode ser utilizado em conjunto com qualquer solução baseada em criptografia (s17). Para isso, são utilizados os pacotes de manifestos introduzidos pela última versão da arquitetura CCN. Os manifestos são pacotes especiais que contém uma lista do nome de todos os *chunks* que compõem um conteúdo. Os manifestos de conteúdos protegidos contam com campos especiais para a divulgação dos nomes das chaves criptográficas necessárias para decifrar o conteúdo. A ideia é que o provedor cifre os conteúdos com uma chave secreta e que essa chave seja protegida por um esquema criptográfico, fazendo com que ela seja divulgada somente para usuários autorizados.

Uma solução mais elaborada propõe o uso de duas camadas de criptografia simétrica para garantir o uso dos *caches* por um grupo grande de usuários (s13). Cada conteúdo é dividido em blocos, que são divididos em *chunks*. Os *chunks* de cada bloco são cifrados com uma chave secreta, e carregam consigo um pedaço dessa chave. Para recuperar a chave secreta, é necessário que o usuário recupere todo o bloco. Além disso, uma segunda camada de cifragem é acrescentada aos *chunks*, utilizando uma técnica de regressão de chaves. Cada *chunk* é cifrado com uma derivação da chave principal, que é enviada ao usuário diretamente pelo provedor através da autenticação do usuário. Ao receber todo o bloco, o usuário realiza a regressão das chaves e retira a segunda camada de cifragem, revelando os *chunks* cifrados com a primeira camada. Combinando os pedaços da chave secreta, presentes em cada *chunk* que compõe o bloco, o usuário é capaz de decifrar o conteúdo [Mangili et al., 2015].

3.2.2 Soluções baseadas em infraestrutura

As soluções de controle de acesso infraestruturadas geralmente assumem a existência de servidores de autenticação, ou ainda que os roteadores ou *caches* verifiquem políticas de segurança antes de encaminhar um conteúdo para um usuário. A primeira solução infraestruturada explorada considera a arquitetura NetInf em seu primeiro estágio, em que os NRSs validam o acesso dos usuários aos conteúdos, com base em chaves públicas autorizadas contidas em um metadado associado ao conteúdo solicitado. Se a chave pública do usuário está listada nas informações do metadado, o NRS considera que o provedor reconhece o usuário como legítimo para acessar o conteúdo em questão (s1) [Renault et al., 2009]. Embora essa solução utilize a informação das chaves públicas dos usuários, ela não considera a cifragem dos conteúdos. Outra solução nessa mesma linha é proposta para a arquitetura PURSUIT e assume que os provedores criam as políticas de acesso aos seus conteúdos e as distribuem para os roteadores, que são responsáveis por validá-las com as credenciais do usuário que requisita o conteúdo, antes de enviá-lo como resposta caso o conteúdo seja servido pelo *cache* (s3) [Singh et al., 2012].

Alguns trabalhos argumentam que é inviável para os roteadores ou *caches* validarem políticas de acesso de todos os conteúdos, e então propõem uma infraestrutura separada de servidores de validação de políticas de acesso, também na arquitetura PURSUIT [Fotiou et al., 2012]. Nessa solução os produtores criam as políticas de acesso e enviam para os servidores de validação (s4). Antes de enviar um conteúdo para o usuário, o *cache* deve verificar com um servidor de validação se a credencial do usuário satisfaz a política de acesso para aquele conteúdo. Outra solução infraestruturada, para a arquitetura

NetInf, considera que os usuários devem se registrar em um NRS, que envia um *token* autenticando o usuário. De posse do *token*, o usuário contata o provedor para recuperar o conteúdo. O provedor verifica com o NRS se o *token* é válido, compara os atributos do *token* com os atributos do conteúdo solicitado e se o usuário for autorizado a acessar o conteúdo requisitado, o provedor o cifra com a chave pública do usuário e o envia (s15) [Aiash e Loo, 2015a, Aiash e Loo, 2015b].

3.2.3 Soluções híbridas

As soluções híbridas em geral consideram o uso de criptografia aliada a uma infraestrutura de verificação de acesso. Por exemplo, [Golle e Smetters, 2010, Hamdane et al., 2013] propõem que cada servidor raiz de hierarquia de nomes tenha um servidor de controle de acesso associado. Além de validar as políticas de acesso através de uma lista de controle de acesso (*Access Control List* - ACL), o servidor também tem como função distribuir a chave secreta para os usuários autorizados (s5). Mais tarde, [Hamdane e El Fatmi, 2015] estendem essa proposta para controlar também a escrita em servidores protegidos, compartilhando a chave privada do provedor para que usuários autorizados possam criar novos conteúdos no servidor (s14, s20).

Os filtros de Bloom [Bonomi et al., 2006] também são explorados para o controle de acesso, pois permitem que entidades verifiquem se uma informação pertence a um conjunto sem revelar a informação. Assim, [Chen et al., 2014] propõem uma solução simples ao cifrar os conteúdos com uma chave secreta e enviá-la cifrada com a chave pública de cada usuário individualmente, inovando ao propor que os provedores distribuam aos roteadores listas com filtros de Bloom das chaves públicas dos usuários autorizados a acessar cada conteúdo. Desta forma, de posse de tais listas, os roteadores verificam se o usuário está contido no conjunto de usuários autorizados a acessar um conteúdo, evitando que as requisições de usuários não autorizados sejam encaminhadas adiante na rede ou que sejam satisfeitas por um conteúdo em *cache* (s11).

Já a solução proposta por [Zheng et al., 2015] baseia-se nos princípios da recifragem por *proxy*, que permite que uma mensagem cifrada com a chave pública de um usuário $u1$ seja decifrada com a chave privada de outro usuário, $u2$. Essa solução considera a existência de uma infraestrutura de servidores na borda da rede que funciona como um *proxy* na recuperação de conteúdos protegidos na rede. Os provedores de conteúdo cifram o conteúdo com sua chave pública e uma chave aleatória $k1$ e o distribuem para a rede conforme a demanda. Para um usuário acessar esse conteúdo, ele deve solicitar para o servidor de borda, que recupera esse conteúdo de qualquer lugar da rede e o recifra com uma nova chave, $k2$, única para cada usuário. O servidor de borda envia essa chave para o provedor que autentica o usuário e gera uma chave de recifragem com base nas chaves $k1$ e $k2$ e envia para o usuário, que a utiliza para decifrar o conteúdo (s16).

Outra ideia para o controle de acesso, chamada IBAC (*Interest-Based Access Control*), explora a imprevisibilidade dos nomes dos conteúdos através de técnicas de ofuscação, como *hashes*, fazendo com que usuários não autorizados não consigam solicitar os conteúdos. Além disso, os roteadores validam a entrega de conteúdos em *cache* através de uma assinatura contida no pacote de *Interesse*. Se a assinatura do usuário que enviou o *Interesse* estiver na lista de usuários autorizados nos roteadores, o roteador envia o conteúdo do *cache*, se disponível (s19, s18) [Ghali et al., 2015b].

3.2.4 Outras

Em [Tan et al., 2014] é proposto um esquema de controle de acesso em que um conteúdo é dividido em duas partes pelo provedor: um pequeno pedaço é distribuído individualmente para cada usuário autorizado enquanto o restante é distribuído normalmente pela rede. Para ter acesso ao conteúdo, é necessário que o usuário recupere a pequena parte, diretamente do provedor, e o restante do conteúdo de qualquer local disponível (s8). Uma visão diferente para o controle de acesso aos conteúdos, proposta em [Li et al., 2015], introduz uma solução que valida quais entidades podem armazenar conteúdos em *caches* na rede, chamada de MCAC (*Mandatory Content Access Control*) (s21). Isso é feito através de etiquetas nos conteúdos expressando sua permissão de armazenamento em *cache* e da utilização de roteadores específicos para realizar a verificação das políticas dos conteúdos. A princípio, esse controle pode ser somente garantido pelo roteador de borda do provedor, mas pode ser estendido para outros roteadores a partir de uma rede de confiança.

3.2.5 Discussão

A Tabela 3.1 apresenta uma compilação das soluções de controle de acesso propostas para ICN, divididas pelo tipo da solução, o tipo de conteúdo que protege, a facilidade da descoberta e do vazamento da chave criptográfica utilizada para proteger o conteúdo e o ano da proposta. Com esse levantamento, observa-se que o interesse no controle de acesso aos conteúdos em ICN tem aumentado a cada ano, e que as soluções propostas tendem igualmente para soluções criptográficas, infraestruturadas e híbridas.

Nas soluções criptográficas, o uso de chaves secretas, amplamente utilizada pela sua eficiência computacional, tem a desvantagem de ser facilmente repassada para usuários não autorizados, que podem obter acesso a todo o conteúdo a partir dos *caches*. Por isso, nessas soluções o vazamento das chaves se torna fácil, e a revogação do acesso é difícil porque envolve a substituição do conteúdo nos *caches*, a cifragem com uma nova chave secreta e a distribuição da nova chave para os usuários ainda autorizados. As soluções infraestruturadas e híbridas procuram dificultar que as chaves secretas sejam divulgadas introduzindo etapas extras de comunicação para a validação, autenticação ou recuperação de chaves e atributos, o que pode ser bastante difícil de garantir no ambiente da Internet. No entanto, essas soluções geralmente tornam a revogação de acesso mais fácil, já que existem servidores que detém o conhecimento atualizado das permissões de acesso dos usuários. No mais, soluções infraestruturadas geralmente pressupõem a existência de uma infraestrutura específica para validação de políticas de acesso, o que pode ir contra a ideia da distribuição de conteúdo de forma eficiente, direta e simples que a ICN propõe.

A partir desses esforços, observa-se que o fornecimento de uma solução eficiente para controlar o acesso aos conteúdos, mantendo as características benéficas da ICN, não é uma tarefa trivial e exige o alinhamento de vários objetivos, principalmente com relação à eficiência na garantia de políticas de controle de acesso em conjunto com um bom desempenho na entrega de conteúdo através dos *caches*. Assim, a solução de controle de acesso ideal precisa manter as características da ICN, permitindo que os conteúdos sejam armazenados em *cache* ao longo da rede ao mesmo tempo que não permite o acesso não autorizado desses conteúdos, sem sobrecarregar a rede ou introduzir etapas extras para a recuperação de conteúdo.

Tabela 3.1: Classificação das soluções para controle de acesso em ICN.

Id	Solução	Tipo	Aplicação	Descoberta da chave	Revogação do acesso	Ano
s1	Políticas de acesso no conteúdo	Infraestruturada	Geral	—	Fácil	2009
s2	Criptografia simétrica/assimétrica	Criptográfica	Conferência	Fácil	Fácil	2011
s3	Políticas de acesso nos roteadores	Infraestruturada	Livros, música, filmes	—	Fácil	2012
s4	Políticas de acesso em servidores	Infraestruturada	Geral	—	Fácil	2012
s5	Criptografia simétrica/assimétrica	Híbrida	Geral	Fácil	Fácil	2013
s6	Criptografia de *broadcast*	Criptográfica	Multimídia	Fácil	Difícil	2013
s7	Criptografia baseada em atributos	Criptográfica	Multimídia	Fácil	Difícil	2013
s8	Divisão do conteúdo	Outros	Multimídia	—	Difícil	2014
s9	Chaves de sessão	Criptográfica	*Web*	Fácil	Fácil	2014
s10	Criptografia baseada em atributos no nome	Híbrida	Conteúdos privados	Fácil	Fácil	2014
s11	Criptografia baseada em atributos e filtros de Bloom	Híbrida	Multimídia	Fácil	Fácil	2014
s12	Recifragem por *proxy*	Criptográfica	Multimídia	Fácil	Difícil	2014
s13	Criptografia simétrica e regressão de chaves	Criptográfica	Geral	Fácil	Difícil	2015
s14	Criptografia assimétrica	Híbrida	Geral	Fácil	Fácil	2015
s15	Políticas de acesso no NRS	Infraestruturada	Geral	—	Fácil	2015
s16	*One-time key* e recifragem	Híbrida	Geral	Difícil	Fácil	2015
s17	*Framework* de controle de acesso	Criptográfica	Geral	Fácil	Fácil	2015
s18	Baseado em nome	Criptográfica	Geral	Fácil	Fácil	2015
s19	Baseado em interesse	Híbrida	Geral	Fácil	Fácil	2015
s20	Criptografia simétrica	Híbrida	Ambientes controlados	Difícil	Fácil	2015
s21	Restrição de conteúdos protegidos no *cache*	Outros	Conteúdos sigilosos	—	Fácil	2015

3.3 Considerações finais

Este capítulo apresentou uma visão geral dos desafios de segurança do paradigma de ICN, especialmente do problema do acesso não autorizado aos conteúdos armazenados em *cache* na rede. Apesar de existirem diversas soluções para a aplicação de políticas de acesso, as soluções existentes não podem ser consideradas inteiramente adequadas para o ambiente de ICN. Enquanto algumas permitem que os conteúdos sejam facilmente acessados através da divulgação da chave secreta que o protege, outras exigem que a própria infraestrutura de rede valide e autentique os usuários. Portanto, o paradigma de ICN necessita de uma solução de controle de acesso que atenda às suas particularidades. O próximo capítulo apresenta uma visão detalhada do esquema criptográfico de recifragem por *proxy*, que fundamenta a solução de controle de acesso proposta neste trabalho.

Capítulo 4

Recifragem por *Proxy*

Este capítulo descreve detalhadamente a recifragem por *proxy* (*Proxy Re-Encryption* - PRE), um esquema criptográfico que permite a transformação de uma mensagem cifrada com a chave pública de um usuário $u1$ em uma mensagem que possa ser decifrada com a chave privada de outro usuário, $u2$. O capítulo está dividido em duas seções: a Seção 4.1 apresenta os fundamentos da recifragem por *proxy*, a classifica em diversos modelos e discute as suas aplicações na literatura. A Seção 4.2 detalha os algoritmos do EU-PRE (*Efficient Unidirectional Proxy Re-Encryption*), um esquema de recifragem por *proxy*, e discute o seu potencial para uma solução de controle de acesso alinhada às características de ICN.

4.1 Fundamentos da recifragem por *proxy*

A recifragem por *proxy* (*Proxy Re-Encryption* - PRE) [Blaze et al., 1998] é um esquema criptográfico utilizado como uma alternativa mais segura e eficiente para a criptografia assimétrica tradicional em cenários que os usuários desejam delegar direitos de acesso às suas mensagens cifradas. Na criptografia assimétrica, cada usuário possui um par de chaves, sendo uma chave privada (sk) e uma chave pública (pk). A chave privada deve ser mantida em segredo pelo dono da chave, enquanto a chave pública deve ser divulgada para os interessados. Tradicionalmente, se uma mensagem é cifrada com a chave privada do usuário, ela pode ser decifrada por qualquer usuário que tenha conhecimento da respectiva chave pública; já uma mensagem cifrada com a chave pública somente pode ser decifrada pela chave privada associada, ou seja, pelo dono da chave. Em cenários em que um usuário, $u1$, deseja permitir que um outro usuário, $u2$, acesse as mensagens originalmente cifradas com a chave pública de $u1$, a forma usual de realizar essa delegação é através da entrega da chave privada do usuário $u1$ ao usuário $u2$ [Ma e Ao, 2009a, Ma e Ao, 2009b]. Assim, o usuário $u2$ utiliza diretamente a chave privada de $u1$ para decifrar e acessar as mensagens de $u1$. Contudo, esse modelo simples apresenta diversas desvantagens que impossibilitam seu uso em algumas aplicações. Primeiramente, o usuário $u2$ tem acesso à chave privada de $u1$ e ao texto aberto de todas as suas mensagens, portanto, deve ser uma entidade confiável para o usuário $u1$ [Libert e Vergnaud, 2011]. Além disso, o usuário $u1$ pode querer interromper o acesso de $u2$ às suas mensagens, o que se torna difícil de garantir uma vez que a chave privada foi divulgada.

Desta forma, a recifragem por *proxy* explora adaptações nos modelos de criptografia assimétrica tradicionais introduzindo uma entidade terceira, o *proxy*, que intermedeia a delegação de decifragem dos usuários $u1$ e $u2$. Para isso, ao invés de entregar sua

própria chave privada, como anteriormente, o usuário $u1$ autoriza o *proxy* a transformar as mensagens cifradas com a sua chave pública para o usuário $u2$ através de uma chave de recifragem, $rk_{u1 \to u2}$, que funciona somente para o usuário $u2$. Assim, o *proxy* recifra a mensagem de $u1$ para $u2$, sem acessar o texto aberto, e o usuário $u2$ acessa as mensagens normalmente utilizando a sua chave privada, como se fossem enviadas a ele originalmente.

A Figura 4.1 ilustra o funcionamento de um esquema básico de recifragem por *proxy*, composto pelos usuários $u1$ e $u2$ e por um *proxy* (neste trabalho segue-se a notação padrão da literatura de PRE). Neste exemplo, o usuário $u1$ cifra uma mensagem m com a sua chave pública, que tradicionalmente só pode ser decifrada com a chave privada de $u1$ (o usuário $u1$ pode, alternativamente, receber a mensagem m' de outro usuário). Para permitir que o usuário $u2$ acesse a mensagem original m através da recifragem, o usuário $u1$ envia ao *proxy* a mensagem cifrada m' e uma chave de recifragem $rk_{u1 \to u2}$, calculada com base na chave pública do usuário $u2$. O *proxy* utiliza a chave de recifragem enviada por $u1$ para recifrar o conteúdo para $u2$, gerando m''. Na recifragem, o *proxy* não tem acesso à mensagem m, nem à chave privada de $u1$. O *proxy* então envia a mensagem m'' para o usuário $u2$, que utiliza a sua chave privada para recuperar a mensagem original m.

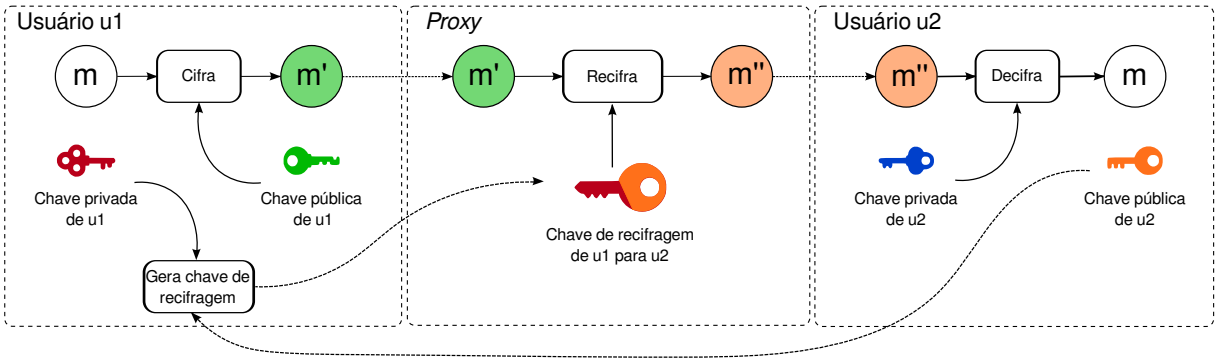

Figura 4.1: Modelo básico de um esquema tradicional de recifragem por *proxy*.

Em comparação com os esquemas tradicionais de criptografia assimétrica, como o RSA (*Rivest-Shamir-Adleman*) [Rivest et al., 1978], compostos pelas operações de configuração do sistema, geração de chaves, cifragem e decifragem, a recifragem por *proxy* tem as funções extras de calcular as chaves de recifragem para cada delegação entre usuários e de recifrar as mensagens. A função de calcular a chave de recifragem é realizada geralmente pelo usuário que delega o direito de decifrar suas mensagens ou por servidores em uma infraestrutura terceirizada, pois essa operação depende do conhecimento da chave privada do usuário que delega. Já a função de recifragem fica sob responsabilidade de um *proxy* semi-confiável. As premissas abaixo definem as operações padrão dos esquemas de recifragem por *proxy*, sendo que a implementação é dependente do tipo de recifragem por *proxy* [Ateniese et al., 2006, Chow et al., 2010]:

Configuração: recebe como entrada um parâmetro de segurança κ e tem como saída uma tupla de parâmetros globais.

Geração de chaves: gera os pares de chaves pública, pk, e privada, sk.

Cifragem: recebe $pk_{(u1)}$ e uma mensagem m, gera uma mensagem $\{m\}_{pk_{(u1)}}$.

Geração de chave de recifragem: tem como entrada a chave privada $sk_{(u1)}$ e a chave pública $pk_{(u2)}$ e como saída uma chave de recifragem $rk_{u1 \to u2}$.

Recifragem: recebe a chave de recifragem $rk_{u1 \to u2}$ e o texto cifrado $\{m\}_{pk_{(u1)}}$, tem como saída $\{m\}_{pk_{(u2)}}$.

Decifragem: utilizando $sk_{(u2)}$ e $\{m\}_{pk_{(u2)}}$, gera como saída a mensagem m.

A corretude dos esquemas de recifragem por *proxy* requer que, para quaisquer parâmetros e mensagens m, as seguintes equações sejam verdadeiras [Ateniese et al., 2009]:

$$Decifra(sk_{(u1)}, Cifra(pk_{(u1)}, m)) = m,$$
$$Decifra(sk_{(u2)}, Recifra(rk_{u1 \to u2}, Cifra(pk_{(u1)}, m))) = m$$

Os esquemas de recifragem por *proxy* têm sido explorados em diversas aplicações na literatura, sendo o controle de acesso uma aplicação natural desses esquemas. Devido às suas características, a recifragem por *proxy* se mostra uma alternativa promissora aos esquemas de criptografia assimétrica também no controle do acesso aos conteúdos em *cache* em uma rede centrada em informação, pois permite que vários usuários acessem uma mesma mensagem cifrada através da delegação de chaves de recifragem, permitindo o *cache* na rede sem prejudicar o controle de acesso. A próxima subseção detalha e discute o uso de esquemas de recifragem por *proxy* e suas aplicações.

4.1.1 Aplicação dos esquemas de PRE

A aplicação motivadora para a proposta inicial de um esquema de recifragem por *proxy* foi o encaminhamento temporário de *e-mails* cifrados de um usuário para outro [Ateniese et al., 2009]. Por exemplo, um usuário $u1$ sai de férias e deseja que seu colega $u2$ possa acessar seus *e-mails* enquanto estiver fora. Para isso, o usuário $u1$ envia uma chave de recifragem para o servidor de *e-mails*, autorizando-o a recifrar seus *e-mails* para o usuário $u2$. Desta forma, o servidor de *e-mails* não tem conhecimento do conteúdo dos *e-mails* de $u1$, sendo mais eficiente e seguro do que o usuário $u1$ simplesmente entregar sua chave privada para o servidor de *e-mails* [Jakobsson, 1999, Zhou et al., 2005]. Outra utilidade dos esquemas de PRE é em listas de *e-mails*, pois os usuários da lista podem trocar *e-mails* de forma segura ao cifrá-los com uma chave pública comum ao grupo. O servidor de *e-mails* então recifra e encaminha os *e-mails* para cada usuário, que os decifram utilizando suas respectivas chaves privadas [Khurana et al., 2006].

O uso da recifragem por *proxy* para o controle de acesso a conteúdos tem sido bastante explorado, principalmente no contexto de controle de acesso a conteúdos na nuvem. Por exemplo, diversas soluções utilizam esquemas de PRE para que um usuário possa armazenar seus dados cifrados em uma nuvem e autorizar o acesso a eles através da criação de uma chave de recifragem, que é entregue ao servidor na nuvem. Assim, o usuário não precisa confiar na nuvem para liberar o acesso aos usuários autorizados, pois os dados estão cifrados e somente o usuário relacionado à chave de recifragem pode decifrar as mensagens recifradas pela nuvem [Ateniese et al., 2006, Yu et al., 2010, Ma et al., 2011, Xu et al., 2012, Zhang e Chen, 2012, Xiong et al., 2012, Tysowski e Hasan, 2013, Kissel e Wang, 2013, Tian et al., 2013, Liu et al., 2014]. O PRE se torna interessante para soluções de controle de acesso principalmente ao considerar tipos de conteúdos específicos, como conteúdos protegidos por direitos autorais, e dados sensíveis, como dados de saúde. Algumas soluções já foram propostas nestes contextos, em que o PRE é utilizado na gerência de direitos digitais de conteúdos multimídia (*Digital*

Rights Management - DRM), delegando e controlando o acesso para diferentes dispositivos acessarem o mesmo conteúdo protegido [Taban et al., 2006, Ma et al., 2011] e na proteção de dados pessoais de saúde (*Personal Health Records* - PHR), permitindo que o usuário armazene seus dados cifrados e libere o acesso para médicos e enfermeiros através da recifragem por *proxy*, limitando a possibilidade de vazamento das informações particulares de saúde do usuário [Ibraimi et al., 2008, Do et al., 2011, He et al., 2011].

Apesar dessas soluções terem semelhança com o problema do controle de acesso em ICN, elas consideram que os provedores de conteúdo têm controle sobre o conteúdo, podendo revogar o acesso ou invalidar a chave de recifragem a qualquer momento. Isso pode ser um problema ao aplicá-los no ambiente de ICN, já que o conteúdo pode estar em um *cache* não controlado pelo provedor, por exemplo. Para explorar o esquema de PRE no controle de acesso de conteúdos em ICN, a próxima subseção apresenta uma organização dos diversos esquemas de recifragem por *proxy* propostos na literatura, bem como identifica e classifica as várias propriedades desses esquemas. Além disso, são definidos os requisitos e as propriedades desejáveis em um esquema de recifragem por *proxy* para o controle de acesso na distribuição de conteúdo em ICN.

4.1.2 Propriedades dos esquemas de PRE

A introdução dos esquemas de recifragem por *proxy* despertou um grande interesse na comunidade acadêmica, sendo que diversos esquemas foram propostos com o objetivo de incorporar propriedades diferentes ou torná-los mais seguros. Em geral, os esquemas de recifragem por *proxy* devem garantir três asserções básicas: (1) o *proxy* não pode ser capaz de acessar o conteúdo da mensagem que recifra; (2) o usuário $u2$ não pode obter o conteúdo da mensagem sem a intervenção da função de recifragem; e (3) de posse da mensagem cifrada e da chave de recifragem, o *proxy* não pode recuperar as chaves privadas de $u1$ e $u2$ [Matsuo, 2007, Zhu et al., 2010]. Essas três asserções são as bases que garantem que um sistema de PRE seja seguro para uso, evitando que o *proxy* consiga recuperar as mensagens de $u1$ ou sua chave privada, depositando apenas o mínimo de confiança necessária no *proxy* para a revogação da delegação de acesso [Ateniese et al., 2009]. Partindo dessas asserções, que são comuns a todos os esquemas de PRE, foram identificadas cinco propriedades segundo as quais podem ser classificados os esquemas de PRE: direção da delegação, número de saltos de recifragem, transitividade da chave de recifragem, necessidade de interação com o usuário e robustez contra conluio [Ivan e Dodis, 2003]. Essas propriedades e os valores que podem ser atribuídos a cada uma são resumidas na Tabela 4.1.

Os esquemas de PRE existentes geralmente apresentam um conjunto específico de valores dessas propriedades. Por exemplo, um esquema de PRE não pode sustentar ambos os valores de unidirecionalidade e bidirecionalidade para a propriedade direção da delegação. Além dessas propriedades, os esquemas de PRE podem apresentar características especiais, adicionadas para atender demandas de aplicações específicas. Por exemplo, para as aplicações em que é necessário gerar delegações de um para muitos, foram propostos esquemas de PRE que adaptam os esquemas tradicionais de criptografia baseada em atributos [Tang, 2008, Weng et al., 2009a, Weng et al., 2009b, Zhao et al., 2010, Fang et al., 2011, Liu et al., 2012, Liang et al., 2013a, Liang et al., 2013b] e a criptografia de *broadcast* [Chu et al., 2009]. Nesses modelos, o PRE cria chaves de recifragem que são utilizadas pelo *proxy* para recifrar mensagens para todos os usuários que possuem determinados atributos ou que possuem uma chave de um grupo de *broadcast*. A criptografia baseada em identidade também é utilizada por esquemas de PRE, mas neste

Tabela 4.1: Propriedades dos esquemas de recifragem por *proxy*.

Propriedade	**Valores**	**Descrição**
Direção da delegação	Unidirecional	a delegação $u1 \rightarrow u2$ **não** implica na delegação de $u2 \rightarrow u1$
	Bidirecional	a delegação $u1 \rightarrow u2$ implica na delegação de $u2 \rightarrow u1$
Número de saltos de recifragem	Único salto	somente mensagens originais podem ser recifradas
	Múltiplos saltos	uma mensagem recifrada de $u1 \rightarrow u2$ pode ser novamente recifrada de $u2 \rightarrow u3$
Transitividade da chave de recifragem	Transitivo	o *proxy* pode, a partir de $rk_{u1 \rightarrow u2}$ e $rk_{u2 \rightarrow u3}$, produzir $rk_{u1 \rightarrow u3}$
	Intransitivo	o *proxy* **não** pode, a partir de $rk_{u1 \rightarrow u2}$ e $rk_{u2 \rightarrow u3}$, produzir $rk_{u1 \rightarrow u3}$
Necessidade de interação com o usuário	Interativo	as chaves de recifragem são geradas por $u1$ **com** a necessidade de interações com $u2$
	Não interativo	as chaves de recifragem são geradas por $u1$ **sem** a necessidade de interações com $u2$
Robustez contra conluio	Robusto	o usuário $u2$ e o *proxy* em conluio **não** conseguem recuperar a chave privada de $u1$
	Não robusto	o usuário $u2$ e o *proxy* em conluio conseguem recuperar a chave privada de $u1$

modelo a chave de recifragem serve somente para um usuário, com determinada identidade [Wang e Yang, 2009, Singh et al., 2013, Qiu et al., 2015].

Outra característica incorporada aos esquemas de PRE é a delegação com base na busca por palavra-chave nas mensagens antes da recifragem [Dong et al., 2008, Wang e Cao, 2009, Chen e Li, 2011, Shao et al., 2011, Yau et al., 2011, Fang et al., 2012]. Nesse modelo, o *proxy* só realiza a recifragem se a mensagem possuir certas palavras-chave determinadas pelo usuário $u1$. A temporização da delegação de direitos de recifragem também é explorada [Liang et al., 2013b], delimitando o tempo que o *proxy* é autorizado a realizar a recifragem. No término do tempo concedido, o *proxy* deve consultar o usuário $u1$ para renovar ou suspender a delegação, sendo que a corretude desse modelo é baseada no bom comportamento do *proxy* que segue os tempos delimitados para a delegação. A invisibilidade do *proxy* [Jia et al., 2010, Seo et al., 2013] e a recifragem anônima [Shao et al., 2012, Kawai e Takashima, 2013, Zheng et al., 2014] também são características utilizadas nos esquemas de PRE. Em esquemas com invisibilidade do *proxy*, os usuários não têm ciência da presença de um *proxy* intermediando a comunicação. Já nos esquemas de PRE anônimos, entidades terceiras que analisam a mensagem recifrada não conseguem distinguir os usuários envolvidos na comunicação. Atualmente, muitas pesquisas envolvendo os esquemas de recifragem por *proxy* têm como foco a melhoria da segurança dos esquemas já propostos [Canetti e Hohenberger, 2007, Deng et al., 2008, Guoan et al., 2010, Canard et al., 2011, Vivek et al., 2011, Cai e Liu, 2014, Khan et al., 2014]. A Tabela 4.2 resume os principais esquemas de PRE, suas propriedades e a primitiva criptográfica sobre a qual cada um está construído.

Para utilizar um esquema de recifragem por *proxy* como solução de controle de acesso aos conteúdos em ICN, é ideal que ele sustente cinco propriedades, detalhadas

Tabela 4.2: Comparação das propriedades dos modelos de recifragem por *proxy*.

Solução/Ano	**Unidirecional**	**Bidirecional**	**Único salto**	**Múltiplus saltos**	**Transitiva**	**Intransitiva**	**Interativa**	**Não-interativa**	**Robusto contra conluio**	**Primitiva criptográfica**
Criptografia por *proxy* atômica [Blaze et al., 1998]		✓		✓	✓		✓			El Gamal
PRE controlado por quóruns [Jakobsson, 1999]	✓		✓		✓			✓		El Gamal
Baseado em identidade [Matsuo, 2007]	✓		✓		✓			✓		IBE
Baseado em atributos [Ma e Ao, 2009a]	✓		✓		✓			✓	✓	ABE
Baseado em *broadcast* [Wang e Cao, 2009]	✓		✓		✓			✓	✓	BE
Unidirecional eficiente [Chow et al., 2010]	✓		✓			✓	✓		✓	El Gamal
Proxy invisível [Jia et al., 2010]	✓		✓			✓	✓		✓	Chaves assimétricas
Palavra-chave [Yau et al., 2011]	✓		✓		✓		✓		✓	El Gamal
Anônimo [Shao et al., 2012]	✓		✓			✓	✓		✓	El Gamal

abaixo. Considerando um cenário de distribuição de conteúdo em ICN, em que o provedor de conteúdos $u1$ cifra e distribui seus conteúdos na rede, e que um usuário $u2$ acessa esses conteúdos, o esquema deve ser:

Unidirecional: a unidirecionalidade evita que a chave de recifragem $u1 \rightarrow u2$, criada para um usuário $u2$, também dê acesso a $u1$ aos conteúdos cifrados por $u2$.

Único salto: o salto único garante que um conteúdo recifrado não possa ser cifrado novamente para outro usuário, dando acesso a um usuário que normalmente não poderia acessar.

Intransitivo: a intransitividade garante que um *proxy* não seja capaz de criar novas chaves de recifragem para outros usuários além daqueles que o usuário $u1$ delegou acesso através das chaves de recifragem.

Interativo: a interatividade garante que o usuário $u2$ se comunique com o provedor antes de acessar um conteúdo, a fim de que uma chave de recifragem seja criada para ele.

Robusto contra conluio: o esquema deve fornecer segurança contra conluio para que o *proxy* ou o usuário, de posse do conteúdo recifrado e da chave de recifragem, não consiga descobrir a chave privada do provedor e comprometer os conteúdos.

Entre os trabalhos estudados, três esquemas de PRE contemplam essas propriedades: o esquema unidirecional eficiente [Chow et al., 2010], o esquema de *proxy* invisível [Jia et al., 2010] e o esquema de *proxy* anônimo [Shao et al., 2012]. Dentre eles, o esquema *Efficient Unidirectional Proxy Re-Encryption* (EU-PRE) [Chow et al., 2010] se mostra mais simples e eficiente, pois não implementa as funções de invisibilidade do *proxy* e anonimato das mensagens cifradas, como os outros dois esquemas. Ainda, essas funções não são relevantes para uma solução de controle de acesso para ICN. Além de possuir as propriedades desejadas para a aplicação em ICN, o esquema EU-PRE é seguro contra ataques de texto cifrado escolhido (*Chosen-Ciphertext Attack* - CCA) na asserção da dificuldade de se resolver o problema de um logaritmo discreto. Ele também é aprovado por outros trabalhos [Yang et al., 2011, Canard et al., 2011] e garante que uma entidade terceira com acesso à função de recifragem não aprenda nada além do que aprenderia ao interagir normalmente com o *proxy* [Hohenberger et al., 2007]. A próxima seção detalha o funcionamento do EU-PRE.

4.2 *Efficient Unidirectional Proxy Re-Encryption*

O EU-PRE se diferencia dos demais esquemas de recifragem por *proxy* por cifras menores e eficiência computacional. Para tal, o EU-PRE não depende de emparelhamentos como a maioria dos esquemas de PRE, pois tem como base o esquema criptográfico El Gamal [El Gamal, 1985] e as assinaturas de Schnorr [Schnorr, 1991]. Isso faz com que ele seja mais eficiente, já que os emparelhamentos são custosos computacionalmente [Chow et al., 2010]. O EU-PRE é composto por seis algoritmos: *configuração*, *geração de chaves*, *cifragem*, *geração de chave de recifragem*, *recifragem* e *decifragem*. Tradicionalmente, existem quatro entidades envolvidas em um esquema de recifragem por *proxy*: uma infraestrutura terceirizada, o usuário que delega, o *proxy* e o usuário que recebe a delegação. Os algoritmos de configuração e geração de chaves dos usuários são executados na infraestrutura terceirizada (opcionalmente pode ser executada no próprio usuário que delega), enquanto a cifragem e a geração das chaves de recifragem são realizadas pelo usuário que delega os direitos de recifragem. A recifragem é responsabilidade de um *proxy* e a decifragem ocorre no dispositivo do usuário que recebe a mensagem recifrada. A seguir, os seis algoritmos do EU-PRE são detalhados.

Configuração: escolher dois números primos p e q tal que $q \mid p-1$ (q deve ser divisor de $(p-1)$), o parâmetro ℓ_0 para o tamanho da mensagem, o parâmetro de segurança ℓ_1 e um gerador g do grupo $\mathbb{G}$ (subgrupo de $\mathbb{Z}_p^*$ de ordem q). Além desses parâmetros, o sistema utiliza quatro funções de *hash*: $H_1 : \{0,1\}^{\ell_0} \times \{0,1\}^{\ell_1} \rightarrow \mathbb{Z}_q^*$, $H_2 : \mathbb{G} \rightarrow \{0,1\}^{\ell_0+\ell_1}$, $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ e $H_4 : \mathbb{G} \rightarrow \mathbb{Z}_q^*$. Os parâmetros públicos do sistema são: $(q, \mathbb{G}, g, H_1, H_2, H_3, H_4, \ell_0, \ell_1)$.

Geração de chaves: o conjunto de chaves do esquema EU-PRE é composto por dois pares de chaves públicas-privadas para cada usuário do sistema. Essa característica é introduzida por [Chow et al., 2010] para garantir que a chave privada de um usuário $u1$ não seja divulgada caso o *proxy* e o usuário troquem informações. Considerando um usuário $u1$, as chaves privadas $sk1_{(u1)}$ e $sk2_{(u1)}$ são escolhidas aleatoriamente em $\mathbb{Z}_q^*$ e as chaves públicas são calculadas por g^{sk}, assim $pk1_{(u1)} = g^{sk1_{(u1)}} \bmod p$ e $pk2_{(u1)} = g^{sk2_{(u1)}} \bmod p$.

Cifragem: uma mensagem m é cifrada pelo usuário $u1$ com as suas chaves públicas $pk1_{(u1)}$ e $pk2_{(u1)}$. Escolher t a partir de $\mathbb{Z}_q^*$ e ω de tamanho ℓ_1 e calcular $r = H_1(m, \omega)$ e D, E e F como segue:

$$D = (pk1_{(u1)}^{H_4(pk2_{(u1)})} \cdot pk2_{(u1)})^t \bmod p \tag{4.1}$$

$$E = (pk1_{(u1)}^{H_4(pk2_{(u1)})} \cdot pk2_{(u1)})^r \bmod p \tag{4.2}$$

$$F = H_2(g^r \bmod p) \oplus (m||\omega) \tag{4.3}$$

Calcular também $s = t + r \cdot H_3(D, E, F) \bmod q$. A saída é ($D$,$E$,$F$,$s$).

Geração da chave de recifragem: para gerar uma chave de recifragem de $u1$ para $u2$, são necessárias as chaves privadas de $u1$ e uma das chaves públicas de $u2$, $pk2_{(u2)}$. Deve-se escolher aleatoriamente h de tamanho ℓ_0 e π de tamanho ℓ_1 e calcular $v = H_1(h \times \pi)$. Calcular também $V = pk2_{(u2)}^v \bmod p$ e $W = H_2(g^v \bmod p) \oplus (h||\pi)$. A chave de recifragem é:

$$rk_{u1 \to u2} = h\left(\left(sk1_{(u1)} \cdot H_4(pk2_{(u1)}) + sk2_{(u1)}\right)^{-1} \bmod p - 1\right) \tag{4.4}$$

A saída é $(rk_{u1 \to u2}, V, W)$.

Recifragem: primeiramente, o *proxy* deve validar

$$(pk1_{(u1)}^{H_4(pk2_{(u1)})} \cdot pk2_{(u1)} \bmod p)^s \bmod p = D \cdot (E^{H_3(D,E,F)} \bmod p) \bmod p \tag{4.5}$$

se a igualdade for verdadeira, calcular

$$E' = E^{rk_{u1 \to u2}} \bmod p \tag{4.6}$$

a saída é (E', F, V, W).

Decifragem: A mensagem m é decifrada por $u2$ mediante sua chave privada $sk2_{(u2)}$. Primeiramente, o usuário $u2$ recupera $(h||\pi)$ e $(m||\omega)$ ao calcular

$$(h||\pi) = W \oplus H_2(V^{sk2_{(u2)}^{-1} \bmod p-1} \bmod p) \tag{4.7}$$

$$(m||\omega) = F \oplus H_2(E'^{h^{-1} \bmod p-1} \bmod p) \tag{4.8}$$

A saída é a mensagem m se $V = pk2_{(u2)}^{H_1(h,\pi)} \bmod p$ e $E' = g^{H_1(m,\omega) \cdot h} \bmod p$.

A Figura 4.2 resume o funcionamento do esquema EU-PRE. Primeiramente, uma infraestrutura de chave pública computa e distribui as chaves aos usuários (setas 1 e 2). Do lado do usuário $u1$, que delega a decifragem das suas mensagens cifradas para outro usuário, estão as funções de cifragem e geração de chaves de recifragem. Para a cifragem, são necessárias ambas as chaves públicas de $u1$, $pk1_{(u1)}$ e $pk2_{(u1)}$, e a mensagem a ser cifrada m (seta 3). A saída é (D, E, F, s), em que E e F contêm a mensagem. Para gerar a chave de recifragem para o usuário $u2$ são necessárias as chaves privadas de $u1$, $sk1_{(u1)}$ e

$sk2_{(u1)}$, a chave pública $pk1_{(u1)}$ e a chave pública $pk2_{(u2)}$ do usuário $u2$ (seta 4). A saída é a chave de recifragem $rk_{u1 \to u2}$ e as variáveis V e W. Para recifrar a mensagem, o *proxy* recebe de $u1$ as variáveis (D, E, F, s) e $rk_{u1 \to u2}, V, W$ (setas 5 e 6). A saída da recifragem é (E', F, V, W), em que E' e F contêm a mensagem. Para decifrar a mensagem recebida do *proxy* (seta 7), o usuário $u2$ precisa somente da sua chave privada $sk2_{(u2)}$, recuperando a mensagem m original (seta 8).

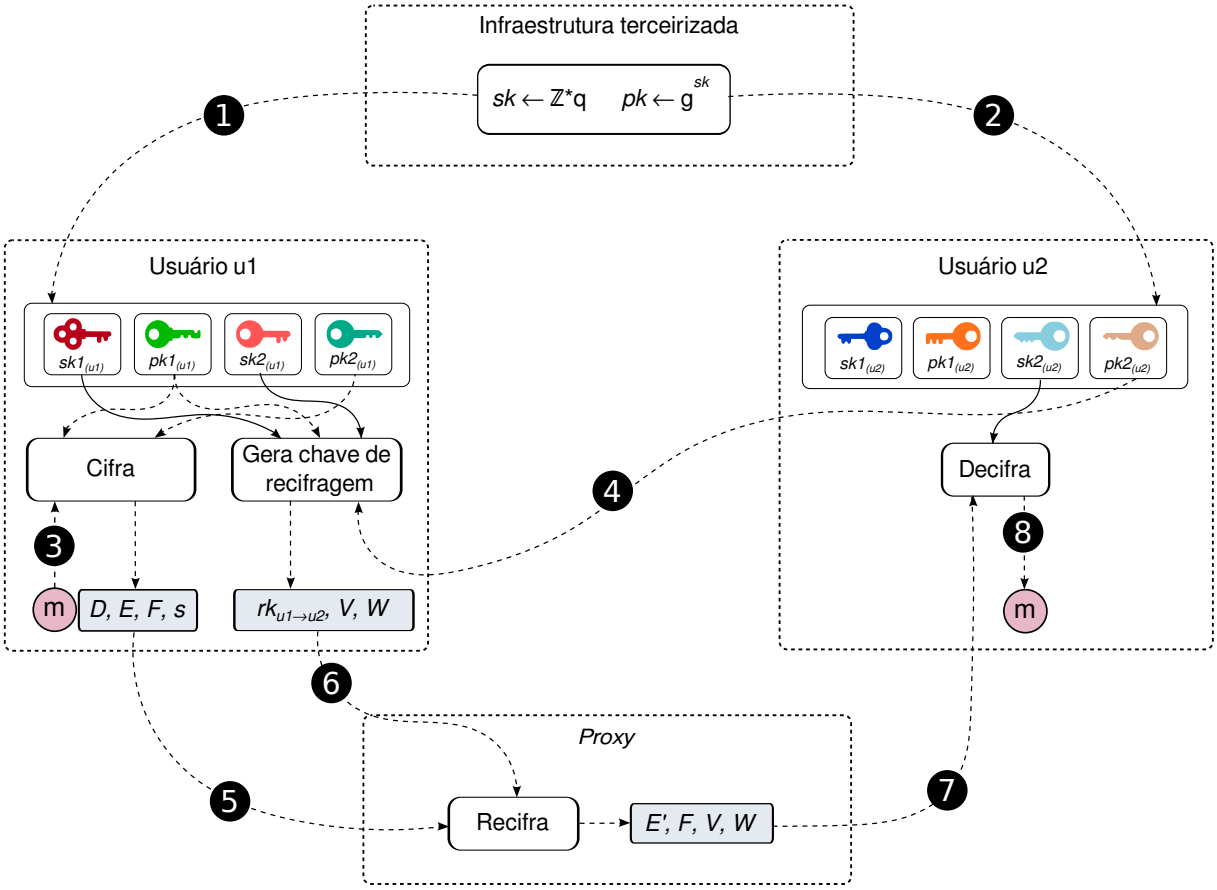

Figura 4.2: Resumo do funcionamento do esquema de recifragem por *proxy* EU-PRE.

4.3 Considerações finais

Este capítulo explorou o esquema criptográfico de recifragem por *proxy*, em que uma mensagem cifrada para um usuário $u1$ pode ser transformada em uma mensagem cifrada para $u2$, através de uma chave de recifragem $rk_{u1 \to u2}$. Foram identificadas as propriedades ideais para um esquema de PRE ser aplicado em um serviço de controle de acesso e apresentadas as diversas aplicações dos esquemas de PRE na literatura, apontando que o PRE é um modelo natural para o controle de acesso de conteúdos. Dentre os esquemas de PRE existentes, o EU-PRE é o esquema que melhor se adapta às necessidades de uma solução de controle de acesso para ICN. O próximo capítulo apresenta e detalha a proposta de uma solução para o controle de acesso de conteúdos multimídia em ICN, utilizando o esquema de recifragem por *proxy* como fundamento.

Capítulo 5

Controle de acesso em ICN utilizando recifragem por *proxy*

Este capítulo detalha a proposta de uma solução de controle de acesso para a distribuição de conteúdos multimídia em ICN, baseada no esquema criptográfico de recifragem por *proxy* EU-PRE. O capítulo está dividido em quatro seções. A Seção 5.1 apresenta uma visão geral da solução proposta e as asserções relacionadas aos modelos de rede, de distribuição de conteúdo e de ameaças. A Seção 5.2 detalha as etapas da solução proposta, dividida em dois domínios: domínio do provedor e domínio do usuário. A Seção 5.3 compara a solução proposta com outras soluções propostas, ressaltando as diferenças. Por fim, a Seção 5.4 discute os benefícios e as limitações da solução proposta.

5.1 Visão geral da proposta

Diferente das soluções de controle de acesso criptográficas existentes para ICN, apresentadas no Capítulo 3, a solução proposta visa ser completamente alinhada aos requisitos do paradigma, mantendo simples o processo de requisição e entrega do conteúdo. Para isso, a solução proposta é modelada para evitar o uso de entidades terceiras para a validação de políticas de acesso, que representam etapas extras na recuperação do conteúdo, e utilizar o esquema criptográfico de recifragem por *proxy* EU-PRE para agregar segurança contra o acesso não autorizado aos conteúdos. A recifragem por *proxy* tem a vantagem de dificultar o vazamento de chaves criptográficas que dão acesso aos conteúdos, quando comparada ao uso de chaves secretas únicas. Isso acontece porque no esquema de recifragem por *proxy* cada usuário deve obter uma chave de recifragem única e exclusiva, que só pode ser utilizada em conjunto com a chave privada do usuário.

Contudo, para a aplicação do EU-PRE em uma solução de controle de acesso que atenda às necessidades das ICNs, é importante atentar à sobrecarga da existência de um *proxy* na intermediação da recuperação de um conteúdo, além do espaço de armazenamento para as chaves públicas-privadas e de recifragem. A intermediação do *proxy* pode afetar o tempo para recuperação de um conteúdo pelo usuário, influenciando negativamente principalmente a execução de conteúdos multimídia, muitas vezes sensível às variações da rede. O armazenamento das chaves também pode ser um problema, principalmente pela grande quantidade de usuários de aplicações multimídia e pelo fato de que o esquema EU-PRE utiliza dois pares de chaves pública-privada para cada usuário. Outra característica que deve ser considerada é o fato de uma chave de recifragem poder ser utilizada para recifrar todos os conteúdos cifrados com a chave pública correspondente, o que pode ser

um problema para o provedor caso ele cifre todos os seus conteúdos com a mesma chave e a chave de recifragem seja divulgada para a rede, por exemplo.

A solução proposta é modelada na camada de segurança da arquitetura NDN, garantindo a independência das camadas de aplicação e de rede. Desta forma, a solução proposta pode ser utilizada por qualquer tipo de conteúdo, em qualquer arquitetura de ICN. Contudo, a solução proposta é otimizada para conteúdos em que muitos usuários estão interessados, como é o caso de conteúdos multimídia. A solução proposta tem como objetivo atender três condições principais:

1. o conteúdo pode ser armazenado em qualquer dispositivo e recuperado por qualquer usuário;

2. não há a adição de novas entidades na rede para a aplicação ou a validação de políticas de acesso;

3. os usuários que acessam o conteúdo não podem decifrá-lo, a menos que sejam explicitamente autorizados pelo provedor de conteúdo.

Para que a solução de controle de acesso proposta esteja alinhada a esses objetivos, o esquema de recifragem por *proxy* EU-PRE é adaptado para que a entidade do *proxy* não participe do processo de recifragem, sendo eliminada do modelo (a solução de controle de acesso de [Wood e Uzun, 2014], proposta paralelamente à nossa, também adota essa estratégia, porém difere da nossa proposta ao utilizar uma chave secreta única para cifrar os conteúdos). Assim, as propriedades do esquema EU-PRE, se tornam importantes para a garantia da segurança da solução proposta. A unidirecionalidade, por exemplo, garante que o provedor não possa acessar mensagens cifradas pelo usuário. O salto único garante que os usuários não possam recifrar o conteúdo para outro usuário, enquanto a intransitividade garante que os usuários não possam criar chaves de recifragem para outros. A interatividade é importante porque exige que os usuários se comuniquem com o provedor para a criação da chave de recifragem, e por fim, o EU-PRE é seguro contra conluio, garantindo que os usuários não consigam descobrir as chaves privadas do provedor, mesmo tendo acesso à mensagem recifrada e à chave de recifragem. A subseção a seguir detalha a incorporação das funções do *proxy* no usuário.

5.1.1 Junção do *proxy* com o usuário

Na solução proposta, a função de recifragem, tradicionalmente executada por um *proxy*, é alocada diretamente no usuário que recebe a delegação de acesso, que passa a executar as funções de recifragem e decifragem do conteúdo. Desta forma, não há a necessidade da presença de uma entidade *proxy*, pois o provedor envia a chave de recifragem diretamente para os usuários. Além disso, é importante ressaltar que essa modificação não introduz perda de segurança, desde que o esquema de recifragem por *proxy* utilizado garanta que uma mesma entidade possa ter conhecimento de ambas as funções, sem acarretar no descobrimento da chave privada do usuário que delega o acesso. O esquema EU-PRE garante essa asserção [Chow et al., 2010].

O provedor de conteúdo, que delega direitos de decifragem para os usuários autorizados, deve utilizar um par de chaves pública-privada distinto para cada conteúdo. Assim, o provedor pode controlar individualmente o acesso a cada um dos conteúdos, pois é necessário que o provedor crie chaves de recifragem diferentes para cada conteúdo e para

cada usuário que deseja acessá-lo. Esse controle é realizado no momento em que o usuário solicita a chave de recifragem para o conteúdo.

A Figura 5.1 ilustra o funcionamento geral da solução proposta, considerando as três entidades envolvidas na recuperação de conteúdo: (a) o provedor, (b) a ICN e (c) o usuário. Os conteúdos são devidamente cifrados pelo provedor, neste exemplo representados pelo conteúdo c, com uma chave pública exclusiva do conteúdo ($pk_{(c)}$), e individualmente nomeados de acordo com o esquema de nomeação adotado. Ele também os disponibiliza para acesso através da sua aplicação. O usuário que deseja acessar um conteúdo fornecido pelo provedor deve requisitá-lo para a rede (seta 2), que roteia as requisições conforme as especificações da arquitetura de ICN. A rede pode satisfazer a requisição do usuário com um conteúdo recuperado diretamente do provedor do conteúdo, assim como de um *cache* na rede (seta 3).

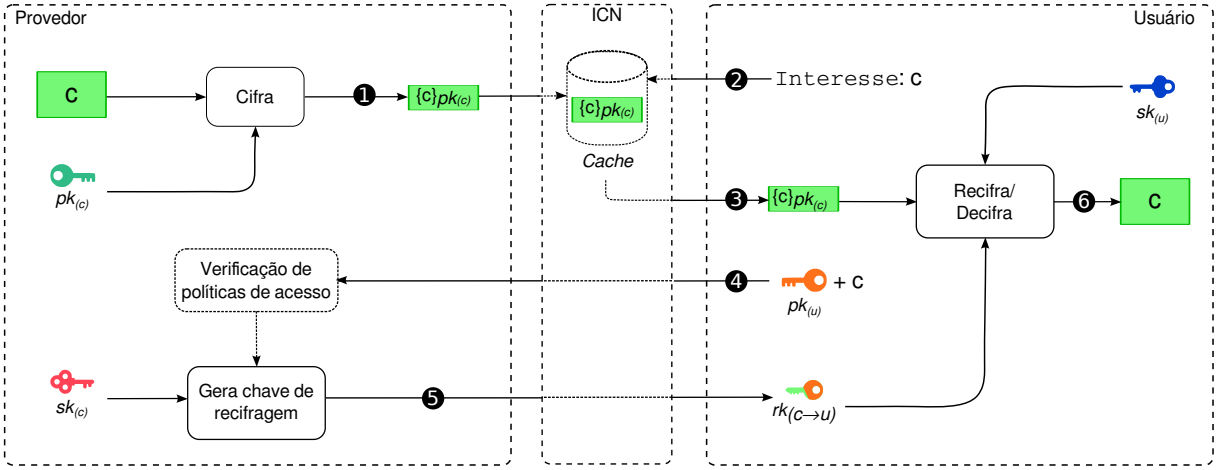

Figura 5.1: Visão geral da solução proposta para o controle de acesso de conteúdos.

Ao receber o conteúdo, o usuário ainda não é capaz de decifrá-lo; para isso, é necessário que ele solicite ao provedor uma chave de recifragem, $rk_{c \to u}$, informando o nome do conteúdo que deseja acessar (c) e a sua chave pública ($pk_{(u)}$) (seta 4). Como o provedor precisa da chave pública do usuário para gerar a chave de recifragem, ele pode solicitar a chave quando o usuário se autentica pela primeira vez na aplicação e armazenar para consultas futuras. Nessa etapa, o provedor tem a oportunidade de validar e aplicar as políticas de acesso apropriadas, de acordo com o usuário e o conteúdo ao qual ele deseja obter acesso.

Caso o usuário não seja habilitado para acessar o conteúdo, o provedor simplesmente nega a entrega de uma chave de recifragem para o usuário. Por outro lado, se o usuário é um usuário legítimo e com credenciais para acessar o conteúdo, o provedor calcula a chave de recifragem (seta 5), vinculada à chave pública do usuário que solicitou. Dessa forma, a chave de recifragem é exclusiva do usuário para aquele conteúdo, e só tem validade se utilizada em conjunto com a sua chave privada. Ao receber a chave de recifragem, o usuário a combina com a sua chave privada (sk_u), decifrando apropriadamente o conteúdo (seta 6). Vale ressaltar que, apesar da chave de recifragem ser única para cada conteúdo, o usuário tem apenas um par de chaves pública-privada para acessar a todos os conteúdos. As asserções consideradas na modelagem da solução proposta são organizadas em um modelo de três dimensões, composto pelos modelos de rede, de distribuição de conteúdos e de ameaças. Esses modelos são detalhados nas próximas subseções.

5.1.2 Modelo de rede

O modelo de rede segue as escolhas de projeto da arquitetura NDN [Jacobson et al., 2012]). Contudo, a solução proposta pode ser aplicada a qualquer arquitetura, pois não implica em mudanças no paradigma de ICN. Como a arquitetura NDN já foi detalhada na Seção 2.2, essa subseção apresenta um resumo do seu funcionamento, destacando as operações principais. A infraestrutura da NDN é composta por provedores de conteúdo, roteadores e usuários. Os provedores de conteúdo anunciam os seus conteúdos na rede, sendo que o conteúdo é dividido em *chunks* de 4KB [Salsano et al., 2012], individualmente nomeados e assinados. Os roteadores são responsáveis por rotear e encaminhar as requisições de conteúdo, assim como armazenar, opcionalmente, os *chunks* em *caches* internos, de acordo com a política de *cache* adotada. Para requisitar um *chunk* na rede, o usuário deve enviar um pacote de *Interesse* e, em resposta, recebe um pacote de *Dado* com o *chunk* solicitado, recuperado diretamente do provedor ou de algum *cache* próximo.

5.1.3 Modelo de distribuição de conteúdo

Ainda que o controle de acesso seja desejável para a maioria dos conteúdos na Internet, este trabalho considera as características de distribuição de conteúdos populares, em que um grande conjunto de usuários esteja interessado no mesmo conteúdo. Nesse cenário, o mecanismo de *cache* é utilizado em seu potencial máximo e os benefícios da ICN surgem de forma mais substancial. Esse modelo pode ser representado por conteúdos tais como vídeos, *e-books*, *streaming* e atualizações de *software*. Entretanto, a solução de controle de acesso proposta é aplicável a outros tipos de conteúdo.

O modelo de distribuição de conteúdo inicia com a disponibilização dos conteúdos pelo provedor por meio de uma aplicação específica, fornecida pelo próprio provedor. Os usuários navegam pelo catálogo de conteúdos através dessa aplicação, que pode ser previamente carregada nos dispositivos ou estar disponível para instalação sob demanda. Os provedores oferecem o acesso aos seus conteúdos por meio de uma assinatura do serviço, exigindo que os usuários sejam registrados e autenticados apropriadamente na aplicação para ter acesso ao catálogo de conteúdo.

Os conteúdos são armazenados nos próprios provedores ou em uma infraestrutura terceirizada, como uma CDN por exemplo, ou ainda em *caches* pela rede. Para acessar aos conteúdos, o usuário deve utilizar a aplicação do provedor com as suas credenciais. Além disso, o provedor deve validar o usuário (sua identidade e chave pública) para certificar-se de que o usuário é legítimo para o serviço e aplicar as políticas de acesso de acordo com o usuário. As chaves do usuário e as chaves de recifragem dos conteúdos acessados pelo usuário são armazenadas na aplicação, e em condições normais não são acessíveis por outras aplicações no dispositivo do usuário.

5.1.4 Modelo de ameaças

No modelo de ameaças assume-se que o provedor de conteúdo se comporta corretamente, ou seja, não distribui conteúdo protegido ou direitos de acesso a usuários não autorizados. Os roteadores seguem o comportamento *honesto porém curioso* (*Honest But Curious* - HBC) [Paverd et al., 2014]. No modelo HBC, as entidades seguem corretamente o protocolo, mas podem acessar as informações que transitam entre as entidades. Assim, considera-se que os roteadores desempenham corretamente suas funções (roteamento, encaminhamento e armazenamento de conteúdo em *cache*), porém podem ser curiosos e

tentar acessar o conteúdo que estão roteando. Também assume-se que os usuários não divulgam as suas chaves privadas, nem adulteram a aplicação fornecida pelo provedor para acesso aos conteúdos.

Considera-se que entidades maliciosas são usuários ilegítimos que não têm acesso ao conteúdo do provedor, ou ainda usuários legítimos que tentam acessar conteúdo ao qual não têm autorização. A intenção dessas entidades maliciosas é obter acesso ao conteúdo protegido sem ter as obrigações inerentes dos usuários autorizados, tais como pagamento, verificação de idade ou ainda tipos de acesso diferenciados, como contas básicas e avançadas. Eles podem explorar o conteúdo protegido na rede de três formas:

1. aprender ou descobrir o nome do conteúdo e requisitá-lo na rede;
2. espionar os canais de comunicação ou interferir em pontos de acesso;
3. examinar ou sondar *caches* próximos, ou acessar diretamente o seu próprio *cache*.

Além disso, assume-se que qualquer usuário da rede, incluindo as entidades maliciosas, podem recuperar as chaves de recifragem a partir dos *caches*, da mesma forma que podem solicitar conteúdo protegido na rede. Por fim, como os usuários têm acesso ao conteúdo oferecido pelo provedor através de uma aplicação específica, não há necessidade de descobrir o nome do conteúdo de antemão ou por meios não confiáveis.

5.2 Funcionamento da solução proposta

A solução de controle de acesso proposta é estruturada em três domínios: *domínio do provedor de conteúdo*, *domínio da rede* e *domínio do usuário*. O domínio do provedor de conteúdo engloba a cifragem do conteúdo e a geração de chaves de recifragem para os usuários, sob demanda. O domínio da rede refere-se ao roteamento e ao encaminhamento de conteúdo seguindo o paradigma de ICN. O domínio do usuário é composto pela aplicação do provedor de conteúdo e pelas operações de recifragem/decifragem do conteúdo. Tanto o provedor quanto uma infraestrutura terceirizada podem ser responsáveis por distribuir as chaves pública-privada aos usuários. A seguir, são detalhadas as ações realizadas pelo provedor de conteúdo e pelos usuários (o domínio da rede é abordado com detalhes na Seção 2.2 e novamente resumido na Seção 5.1.2).

5.2.1 Domínio do provedor: cifragem e geração de chaves de recifragem

A primeira medida do provedor na preparação dos conteúdos para a distribuição aos usuários é a criação de um conjunto de pares de chaves públicas-privadas, que serão utilizadas para a cifragem dos seus conteúdos (opcionalmente o provedor pode receber as chaves de uma infraestrutura terceirizada). Além das chaves, o provedor também possui um conjunto $\mathcal{C}$ de conteúdos que deseja disponibilizar para seus usuários. Cada conteúdo $c_i \in \mathcal{C}$ possui um par de chaves pública-privada exclusivo, $\{sk_{(c_i)}, pk_{(c_i)}\}$. Os conteúdos são segmentados em *chunks* e cada *chunk* é individualmente cifrado com a chave pública $pk_{(c_i)}$, sendo que todos os *chunks* pertencentes ao mesmo conteúdo são cifrados com a mesma chave. A chave privada correspondente ($sk_{(c_i)}$) é guardada em segredo pelo provedor de conteúdo.

O conteúdo é distribuído conforme as requisições dos usuários, sendo armazenado em *cache* na rede, de acordo com as políticas de *cache* adotadas. Neste estágio, o conteúdo pode estar em qualquer lugar na rede; porém, como a chave privada correspondente ao conteúdo é conhecida somente pelo provedor, nenhum usuário, legítimo ou malicioso, é capaz de decifrá-lo. A Figura 5.2(a) detalha o funcionamento dessas operações. O provedor possui um conjunto de conteúdos, $\mathcal{C} = \{a, b, c, d, e, f\}$ e os cifra com os seus respectivos pares de chaves, gerando os conteúdos cifrados $\{a\}_{pk_{(a)}}$, $\{b\}_{pk_{(b)}}$, $\{c\}_{pk_{(c)}}$, $\{d\}_{pk_{(d)}}$, $\{e\}_{pk_{(e)}}$ e $\{f\}_{pk_{(f)}}$, que são disponibilizados para os usuários.

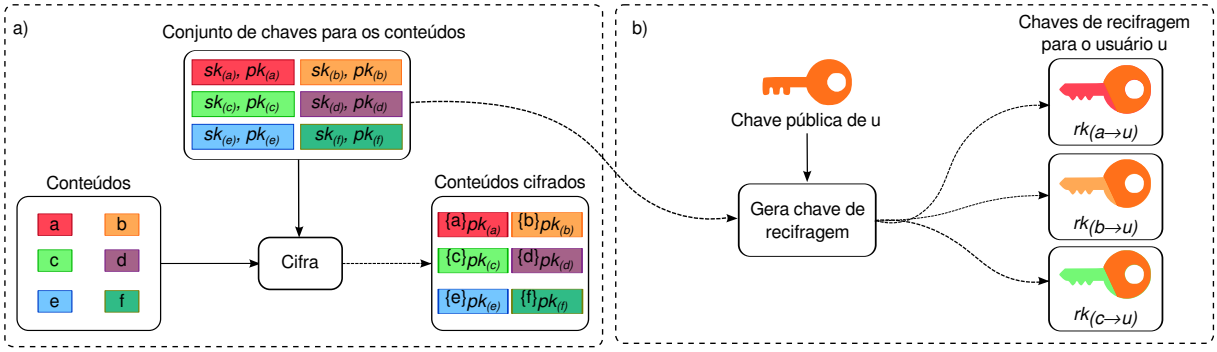

Figura 5.2: Domínio do provedor: (a) cifragem e (b) geração de chaves de recifragem.

Antes que a aplicação no usuário possa consumir o conteúdo, ele deve ser decifrado. Para isso, um usuário u que deseja decifrar um conteúdo c_i solicita uma chave de recifragem $rk_{c_i \to u}$ para o provedor. Essa mensagem representa um pacote de *Interesse* comum, válido no contexto da aplicação e roteado pela ICN até o provedor da aplicação. O provedor verifica se o usuário é autorizado a acessar o conteúdo c_i, identifica a chave privada utilizada para cifrar o conteúdo, $sk_{(c_i)}$, e então calcula a chave de recifragem $rk_{c_i \to u}$, que envolve a chave pública do usuário, $pk_{(u)}$, e a envia para o usuário. Isso significa que o usuário u é o único habilitado a utilizar a chave de recifragem $rk_{c_i \to u}$ para decifrar o conteúdo c_i, já que esse procedimento requer a chave privada de u (ao menos que o usuário u divulgue sua chave privada). É inútil para uma entidade maliciosa requisitar o conteúdo e interceptar uma chave de recifragem: ela pode ser capaz de recifrar o conteúdo, mas a mensagem cifrada resultante só poderá ser decifrada pelo usuário que possuir a chave privada correspondente à chave de recifragem. A Figura 5.2(b) detalha a operação de geração da chave de recifragem para os conteúdos a, b e c, que só podem ser utilizadas exclusivamente pelo usuário u.

Uma vez que o usuário u possua a chave de recifragem $rk_{c_i \to u}$ para o conteúdo c_i, ele é capaz de decifrar o conteúdo c_i sempre que desejar. Além disso, qualquer conteúdo c_j que tenha sido cifrado pelo provedor de conteúdo com a mesma chave pública utilizada para cifrar o conteúdo c_i, pode ser decifrado por u com a chave $rk_{c_i \to u}$. Essa é a principal razão pela qual é fortemente recomendado que cada conteúdo tenha um par distinto de chaves pública-privada.

Apesar de considerar que as chaves de recifragem sejam armazenadas dentro da aplicação, e que o usuário, em condições normais, não tenha acesso direto a elas, ainda é importante lidar com a revogação dessas chaves. Uma forma natural de invalidar as chaves de recifragem é renovando periodicamente a cifragem dos conteúdos com chaves públicas diferentes. Desta forma, os conteúdos teriam chaves de recifragem diferentes, forçando os usuários a solicitarem as novas chaves sempre que desejarem acessar novamente um conteúdo e suas chaves de recifragem forem inválidas. Contudo, essa solução pode

apresentar problemas com as políticas de substituição de conteúdo nos *caches*, já que os roteadores não tem a obrigação de retirar um conteúdo do *cache*, mesmo que expirado, caso o armazenamento desse conteúdo represente um ganho representativo de desempenho para esse roteador. Embora seja um desafio importante, a revogação de chaves não é explorada com detalhes neste trabalho.

5.2.2 Domínio do usuário: decifragem e uso do conteúdo

Quando um usuário deseja acessar um conteúdo, c_i por exemplo, ele deve solicitar a chave de recifragem $rk_{c_i \to u}$ para o provedor. Utilizando essa chave de recifragem e a sua chave privada, o usuário decifra os *chunks*, sob demanda da aplicação. As chaves de recifragem são exclusivas de cada usuário e de cada conteúdo, portanto, a cada conteúdo acessado, o usuário deve requisitar a respectiva chave de recifragem para o provedor de conteúdo (a chave de recifragem é a mesma para todos os *chunks* que compõem um conteúdo). Desta forma, o provedor pode negar o envio de chaves de recifragem para usuários que não cumpram os requisitos impostos.

A Figura 5.3 ilustra o recebimento e a decifragem dos conteúdos $\{a\}_{pk_{(a)}}$, $\{b\}_{pk_{(b)}}$ e $\{c\}_{pk_{(c)}}$. A decifragem envolve as operações de recifragem e decifragem. Após a decifragem do *chunk* recebido, a aplicação pode utilizá-lo ou armazená-lo em um *buffer*, conforme a necessidade. O usuário que já acessou um conteúdo e foi autorizado pelo provedor com a respectiva chave de recifragem, pode recuperá-la de um *cache* na rede, se disponível.

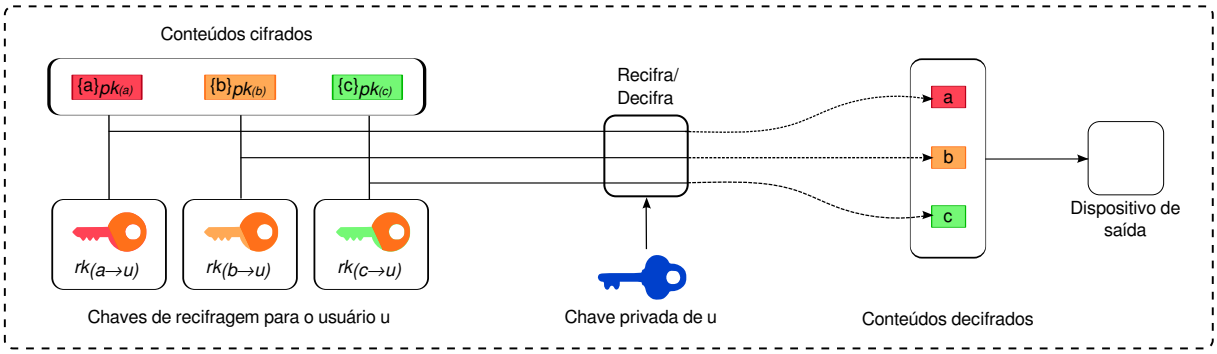

Figura 5.3: Domínio do usuário: decifragem e uso do conteúdo.

5.3 Trabalhos correlatos

Dentre as soluções de controle de acesso criptográficas para ICN, destacam-se a criptografia de *broadcast* e a criptografia baseada em atributos, que são exploradas em diversos trabalhos já discutidos na Seção 3.2. Em comparação com essas duas soluções, a solução proposta é mais segura, pois utiliza uma chave diferente para cada conteúdo enquanto a criptografia de *broadcast* e a criptografia baseada em atributos são utilizadas para a distribuição de uma chave secreta única para todos os usuários. Além disso, a solução proposta também faz o melhor uso dos *caches* na rede ao garantir que um mesmo conteúdo satisfaça as requisições de todos os usuários para esse conteúdo. A criptografia baseada em atributos, por exemplo, pode dividir o acesso ao conteúdo em diferentes atributos para viabilizar as operações criptográficas de cifragem e decifragem, o que faz com que um conteúdo não sirva para todos os usuários. Ainda que a criptografia de

broadcast divida o acesso em vários grupos de usuários, todos têm acesso à mesma chave, o que pode prejudicar ainda mais a segurança dos conteúdos.

A solução proposta por [Wood e Uzun, 2014], que também aplica a recifragem por *proxy* para o controle de acesso, tem os mesmos problemas que as soluções anteriores. Apesar do *proxy* também ser acoplado ao usuário, os autores concluem que o modelo de recifragem por *proxy* não é eficiente para a cifragem dos conteúdos, sendo utilizado então para a distribuição de uma chave secreta, assim como as soluções de criptografia de *broadcast* e baseada em atributos. Assim, cada usuário recebe uma chave de recifragem para extrair a chave secreta, que é a mesma para todos os usuários.

5.4 Benefícios e limitações

O principal objetivo da solução proposta é fornecer uma forma para os provedores de conteúdos controlarem o acesso aos seus conteúdos em uma rede ICN. Os principais obstáculos para alcançar tal propriedade vêm de duas características intrínsecas ao paradigma de ICN: a implementação de conteúdo nomeado e o *cache* ubíquo de tais conteúdos. Enquanto o conteúdo nomeado facilita às entidades maliciosas identificar e recuperar conteúdo protegido na rede, o *cache* descentraliza a distribuição do conteúdo, sendo que os usuários não precisam necessariamente se comunicar com o provedor para recuperar um conteúdo; no lugar, um *cache* na rede pode fornecer o conteúdo para o usuário.

A solução proposta lida com o segundo problema apontado, ao distribuir o conteúdo cifrado e utilizar uma versão modificada do esquema criptográfico de recifragem por *proxy*. Com a solução proposta, somente usuários autorizados podem decifrar conteúdos protegidos, independente do local em que forem recuperados. A seguir, apresenta-se uma discussão da solução proposta acerca dos benefícios e limitações do seu uso com relação ao desempenho, à segurança e à adequação ao paradigma de ICN.

Desempenho

Da perspectiva do domínio do provedor de conteúdo, existe o ônus de cifrar todos os conteúdos com um par de chaves distinto, gerar as chaves de recifragem sob demanda para seus usuários e armazenar os pares de chaves de todos os conteúdos. A quantidade de usuários e conteúdos pode influenciar negativamente o desempenho do provedor de conteúdo, uma vez que estão intimamente relacionados à quantidade de chaves que ele gerencia. Além do mais, é necessário que pelo menos um servidor esteja sempre ativo para atender às requisições de chaves de recifragem dos usuários. De qualquer forma, pode-se assumir que os provedores podem superar eventuais problemas de desempenho ao adotar estratégias de distribuição e balanceamento de carga, por exemplo. No domínio do usuário, a questão é a tarefa extra de recifrar o conteúdo antes de decifrá-lo, em comparação aos métodos tradicionais de criptografia assimétrica.

Além disso, esquemas de criptografia assimétrica em geral são computacionalmente mais caros que a utilização de chaves secretas, o que justifica o uso de um esquema de criptografia assimétrica somente para cifrar as chaves secretas, que são pequenas e não causam sobrecarga para a cifragem e decifragem. Na solução proposta, o desempenho das operações criptográficas é dependente das configurações do dispositivo que as executa, assim como a quantidade de armazenamento exigido para as chaves criptográficas depende da quantidade de conteúdos distintos. O desempenho do esquema proposto é discutido exaustivamente no próximo capítulo.

Um outro ponto importante com relação ao desempenho está relacionado à recifragem periódica do conteúdo com chaves diferentes, para realizar a revogação de acesso. Uma das questões que apoiam esse processo é um dos problemas abertos em ICN, apontado no documento do grupo de pesquisas de ICN do IETF (*Internet Engineering Task Force*), o ICN-RG (*ICN Research Group*) [Kutscher et al., 2016]. Neste documento, levanta-se uma preocupação com relação à robustez das chaves públicas dos provedores de conteúdos contra ataques de força bruta, já que entidades maliciosas podem recuperar um conjunto relativamente grande de conteúdos criptografados com a mesma chave. Desta forma, a recifragem periódica dos conteúdos pode ser relevante para evitar tais problemas. Ainda assim, a cifragem periódica dos conteúdos com chaves diferentes pode ocasionar uma carga não negligenciável aos provedores de conteúdo.

Segurança

Ao utilizar um esquema de criptografia assimétrica ao invés de chaves secretas, como tradicionalmente proposto para controle de acesso em ICN, a solução proposta melhora a segurança geral da distribuição de conteúdo, tornando mais difícil que usuários não autorizados acessem conteúdos protegidos. Por exemplo, em soluções que empregam chaves secretas, é suficiente que uma entidade maliciosa divulgue a chave para violar o conteúdo protegido. Na solução proposta, é necessário que um usuário legítimo divulgue ambas as suas chaves privada e de recifragem. Mesmo assim, somente o conteúdo relacionado àquela chave estaria corrompido. Além disso, o provedor de conteúdo pode simultaneamente implementar medidas que restrinjam a um determinado número o uso concomitante de aplicações por um mesmo usuário, tornando ainda menos provável que os usuários divulguem suas chaves privadas e de recifragem, sob o risco de serem penalizados.

Embora os esquemas de recifragem por *proxy* considerem os *proxies* entidades confiáveis, na solução proposta a confiabilidade de entidades terceiras não demanda preocupação, pois a função de recifragem é transferida para o usuário e executada através das aplicações. Desta forma, o usuário não tem incentivos para agir maliciosamente ao realizar as funções de *proxy*.

Adequação à ICN

Um dos principais objetivos da solução proposta é a adequação ao paradigma de ICN. Neste sentido, a solução não implica mudanças em qualquer arquitetura de ICN, já que somente provedores de conteúdo e usuários estão envolvidos nas ações de cifragem e decifragem do conteúdo. Como a rede não é afetada pela solução, ela fica livre para rotear e encaminhar os conteúdos para quem os requisite, na sua melhor forma. Além disso, nenhuma função de segurança é transferida para as entidades da rede: os roteadores não precisam verificar chaves ou validar políticas de acesso. Contudo, é necessário que os provedores de conteúdo estejam sempre disponíveis para a geração de chaves de recifragem para seus usuários, que ocorre sob demanda.

Além do mais, o processo de revogação de chaves ainda implica em pelo menos uma desvantagem: por uma janela de tempo, o conteúdo antigo pode ser acessado por usuários que possuam a chave de recifragem correspondente, caso o conteúdo antigo ainda esteja em algum *cache*. Além disso, para renovar o conteúdo disponível na rede, é necessário que o armazenamento de conteúdo nos *caches* tenha um tempo de vida limitado; de outra forma, os usuários continuam requisitando o conteúdo antigo e os *caches* nunca seriam renovados. De qualquer forma, o paradigma de ICN já prevê um tempo de vida para os

conteúdos em *cache* [Zhang et al., 2014]. Uma alternativa seria incorporar um carimbo de tempo no nome do conteúdo e configurar a aplicação para que requisite o conteúdo com o carimbo de tempo apropriado. Contudo, a questão da revogação de chaves necessita de uma investigação mais profunda, fora do escopo do presente trabalho.

5.5 Considerações finais

Este capítulo apresentou uma solução de controle de acesso utilizando o esquema de recifragem por *proxy* EU-PRE. Para atender às necessidades das ICNs, a entidade *proxy* é eliminada do processo e as suas funções são alocadas diretamente no usuário, que realiza a recifragem e a decifragem do conteúdo. Cada conteúdo é cifrado pelo provedor com uma chave pública exclusiva; para acessá-lo, os usuários devem requisitar uma chave de recifragem para o provedor, que pode negar o envio de acordo com suas políticas de acesso para o conteúdo e o usuário. A solução proposta permite que os conteúdos possam ser armazenados nos *caches* na rede sem prejudicar o controle de acesso pelo provedor de conteúdo, garantindo os benefícios do uso do *cache* sem introduzir mudanças significativas nos provedores de conteúdos e na rede. O próximo capítulo avalia o desempenho computacional da solução e apresenta uma avaliação do seu funcionamento em uma ICN.

Capítulo 6

Avaliação de desempenho da solução de controle de acesso em ICN

Este capítulo apresenta uma análise de desempenho da solução de controle de acesso proposta para a distribuição de conteúdos multimídia em uma rede centrada em informação. Ele está dividido em três seções. A Seção 6.1 apresenta os cenários e discute os resultados obtidos com a análise do desempenho da arquitetura NDN na distribuição de conteúdos populares. A Seção 6.2 descreve os cenários e os resultados obtidos com a aferição do desempenho dos algoritmos do EU-PRE e a Seção 6.3 apresentam os cenários e resultados da avaliação de desempenho da solução proposta em dois domínios: o domínio do provedor e o domínio do usuário.

6.1 Desempenho da arquitetura NDN

Apesar dos conceitos de ICN serem propícios para a distribuição de conteúdo, existem poucos estudos que analisam o impacto do tráfego de aplicações reais no paradigma de ICN, inclusive na distribuição de conteúdo multimídia. Optou-se por realizar simulações para a análise devido à dificuldade de acesso a implantações reais de ICN. As simulações foram realizadas na arquitetura NDN, utilizando o simulador ndnSIM (*Named-data Network Simulator*) versão 2.0 [Mastorakis et al., 2015], implementado e mantido pela comunidade de ICN com a gerência da UCLA (*University of California, Los Angeles*). O ndnSIM é baseado no simulador NS-3 (*Network Simulator*), amplamente utilizado para simulações de redes, e implementa as funções básicas da arquitetura NDN. Contudo, o ndnSIM ainda é um simulador novo e em constante aperfeiçoamento.

Seguindo a tendência da comunidade de pesquisadores em ICN, utilizou-se um dos cenários disponibilizados pela iniciativa Rocketfuel [Spring et al., 2004] para a topologia da rede. Esses cenários representam a topologia dos provedores de serviços da Internet (*Internet Service Providers* - ISPs) e possuem dados que se aproximam da infraestrutura atual da Internet em relação a quantidade de roteadores, de usuários e de *backbones*. Atualmente, estão disponíveis as topologias de dez sistemas autônomos (*Autonomous System* - AS) da Europa, Austrália, Estados Unidos e Índia. Dentre eles, foi escolhido o cenário da Tiscali (Europa), com 75 roteadores, ilustrado na Figura 6.1. Esse cenário foi escolhido por representar o maior cenário disponível compatível com os experimentos desejados. A largura de banda dos enlaces variam entre 9,7Mbps e 94,4Mbps e o atraso entre 5.019μs e 9.983μs. Os pontos verdes representam os roteadores do *backbone* e os pontos azuis, *gateways*.

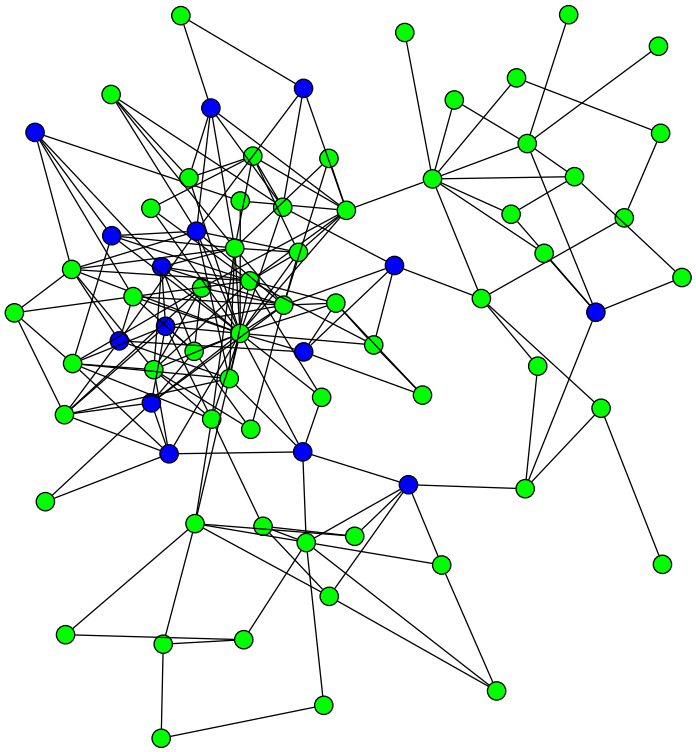

Figura 6.1: Topologia da Tiscali na iniciativa Rocketfuel.

Apesar de a avaliação considerar somente o núcleo da rede (roteadores e *gateways*), assume-se que os roteadores recebem aleatoriamente as requisições dos seus usuários e as encaminham em direção ao roteador do provedor solicitado, sendo que os *caches* no caminho também podem satisfazer as requisições. São considerados três cenários distintos para o *cache* na rede: sem *cache*[1], *cache* de 100 *chunks* e *cache* ilimitado. Tais cenários representam impactos diferentes na recuperação de dados na ICN: o cenário sem *cache* apresenta o comportamento da Internet tradicional; o modelo de *cache* com 100 *chunks* deve lidar com políticas de *cache* e de substituição de conteúdos em *cache*, pois o espaço de armazenamento é limitado; e por fim, o cenário com *cache* ilimitado modela uma ICN sem a interferência de políticas de *cache*. A política de *cache* em todos os cenários é a FIFO (*First In First Out*), em que os *chunks* mais antigos são retirados dos *caches* primeiro.

Consideram-se também dois cenários distintos em que 10% e 30% dos roteadores são conectados diretamente aos provedores de conteúdo, o que representa uma variação na quantidade de servidores na rede. Todos os servidores pertencem ao mesmo provedor, e oferecem o mesmo catálogo de conteúdos, funcionando como uma CDN. Os provedores mantêm um catálogo de 100 conteúdos de 1GB cada, que são individualmente nomeados e divididos em *chunks* de 4KB, o padrão para a arquitetura NDN. Para modelar a quantidade de requisições de conteúdos na rede segue-se uma distribuição Zipf, que se assemelha com o comportamento de requisições de conteúdos populares na Internet. Nessa distribuição, o acesso ao total de conteúdos disponíveis está dividido em muitos acessos a alguns poucos conteúdos (conteúdos de grande interesse dos usuários, como filmes recém lançados) e

[1]Nos experimentos, utilizou-se um *cache* com capacidade para 1 *chunk*, que é o valor mínimo permitido pelo simulador ndnSIM.

poucos acessos à maioria dos conteúdos (conteúdos com interesses de alguns usuários). A distribuição de acesso aos conteúdos na rede, considerando um catálogo de 100 conteúdos, é representada na Figura 6.2. O parâmetro α determina a concentração de requisições aos conteúdos mais acessados pelos usuários dentre os 100 conteúdos disponíveis no catálogo.

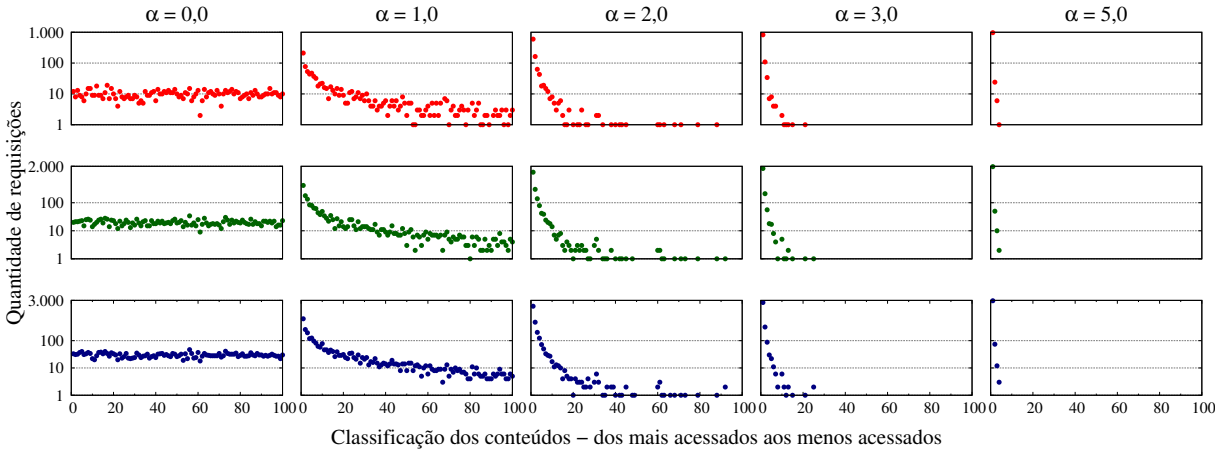

Figura 6.2: Distribuição Zipf de requisições aos conteúdos do catálogo com diferentes valores para α.

Para as requisições de conteúdo pelos usuários, foram considerados cenários com 1.000, 2.000 e 3.000 requisições, com o parâmetro α variando entre 0 e 5. Os diferentes valores para as requisições representam a quantidade de usuários interessados simultaneamente nos conteúdos, o que pode influenciar o comportamento dos *caches*, principalmente ao considerar diferentes valores para α. Os resultados apresentados são a média de 35 simulações, realizadas em um servidor Linux Mint 17 Qiana 64 *bits*, processador AMD Opteron 6136 2,4GHz, com 86GB RAM e um servidor Debian Wheezy 64 *bits*, processador Intel Xeon E312xx 2,0GHz, com 16GB RAM, alternadamente. O intervalo de confiança é de 95%. A Tabela 6.1 apresenta um resumo dos parâmetros utilizados nas simulações.

Tabela 6.1: Parâmetros utilizados na avaliação da distribuição de conteúdo na NDN.

Parâmetro	**Valor**
Quantidade de requisições	1.000, 2.000 e 3.000
Quantidade de servidores	8 (10%) e 23 (30%)
Quantidade de roteadores	75
Topologia	Tiscali (Europa)
Tamanho do catálogo de conteúdos	100 conteúdos
Tamanho dos conteúdos	1GB
Modelos de *cache*	sem *cache*, *cache* com 100 *chunks*, *cache* ilimitado
Zipf α	0, 1, 2, 3 e 5

Na análise da eficiência da arquitetura NDN na distribuição de conteúdos multimídia são computados os tempos para a rede entregar um *chunk* para o usuário e o *cache hit*, que é a porcentagem de requisições satisfeitas pelos *caches* na rede.

6.1.1 Resultados

Uma das principais vantagens na adoção das ICNs é a presença de *cache* na rede, que beneficia diretamente a entrega de conteúdos para os usuários. Assim, a primeira métrica analisada é o tempo para a entrega de um *chunk* para o usuário, com a influência de diferentes configurações de *caches*. A Figura 6.3 apresenta os resultados obtidos, comparando-os ao cenário sem *cache*, incluso nos gráficos como referência. Como esperado, a presença de *cache* na rede representa um ganho substancial, comparado a um cenário sem *caches*, pois os *chunks* podem ser obtidos diretamente de um *cache* próximo, se disponível. Esse comportamento é observado em ambos os cenários com *cache*, exceto para α=0 e 1 com 10% e 30% de servidores no cenário com *cache* ilimitado, ilustrado nas Figuras 6.3(b) e (d). Isso acontece por conta da expiração dos *Interesses* nas PITs dos roteadores. Os cenários com *cache* ilimitado exigem que os roteadores armazenem todos os *chunks* que passam por eles, levando mais tempo para encontrar uma ocorrência de *chunk* nos *caches*, resultando na expiração das entradas das PITs antes do encaminhamento do *chunk*. Conforme uma maior quantidade de requisições dos usuários se concentram em menos conteúdos na rede ($\alpha > 1$), menos conteúdos são armazenados em *cache*, otimizando a procura e, consequentemente, a entrega aos usuários.

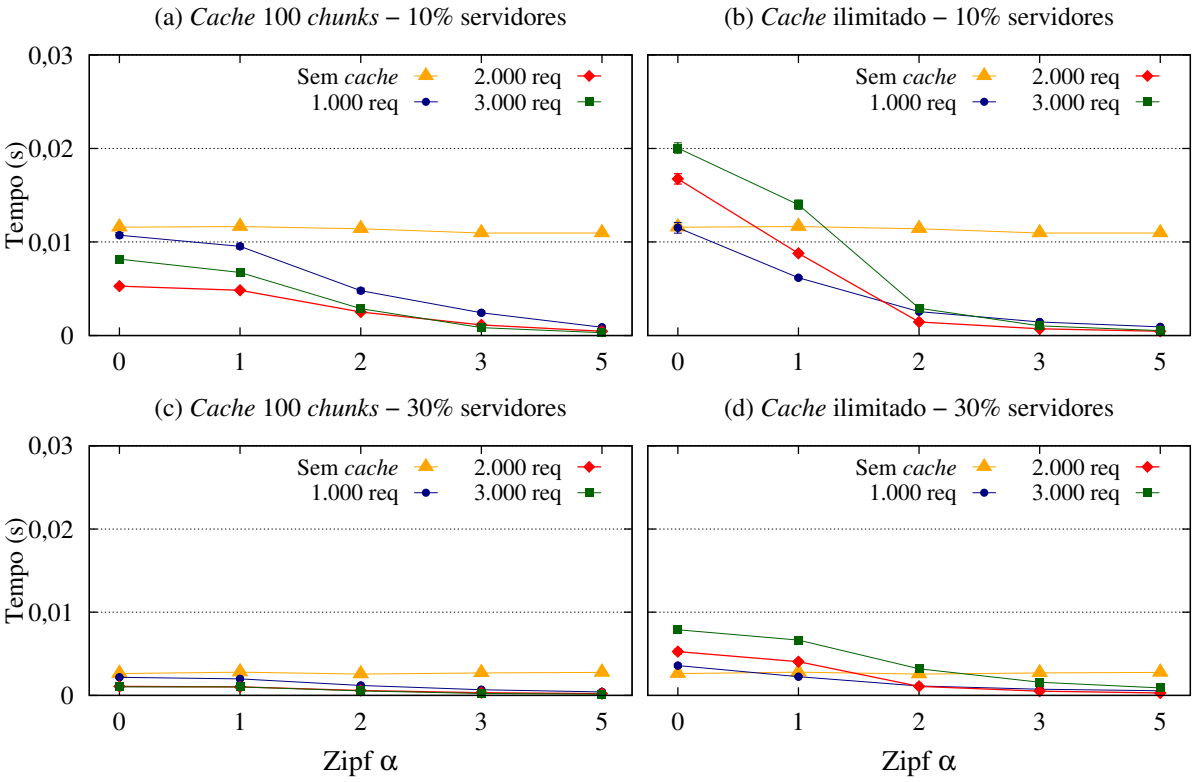

Figura 6.3: Tempo para requisição e recebimento dos *chunks*.

Além disso, observa-se que a presença de mais servidores na rede implica em menos tempo para a recuperação de um *chunk*. Apesar de esperado, o resultado é interessante pois mostra que o uso de servidores extras, ou de CDNs, pode ser diminuído com a adoção da ICN, mas não totalmente dispensado. Ao mesmo tempo que a carga da entrega dos conteúdos pode ser dividida com a rede nos casos de conteúdos populares, a existência de servidores próximos aos usuários significa a certeza de que o conteúdo pode ser encontrado nesses servidores, ao contrário dos *caches* próximos, em que não há a certeza de existir

o conteúdo requisitado. Contudo, quanto mais usuários estão interessados no mesmo conteúdo, mais eficiente é a arquitetura de ICN, independente da quantidade de servidores na rede, pois a probabilidade de encontrar o conteúdo em *cache* também aumenta.

Já o desempenho do *cache*, como esperado, está relacionado com o tamanho dos *caches* e a quantidade de servidores, conforme apresentado na Figura 6.4. Observa-se, por exemplo, que o tamanho do *cache* possui uma pequena influência na porcentagem de *cache hit* obtido, aproximadamente 20% nos cenários com α=0, 1 e 2, e 10% nos cenários com α=3 e 5, comparando o cenário com *cache* de 100 *chunks* (Figura 6.4(a)) e o cenário com *cache* infinito ((Figura 6.4(b)), ambos com 10% de servidores.

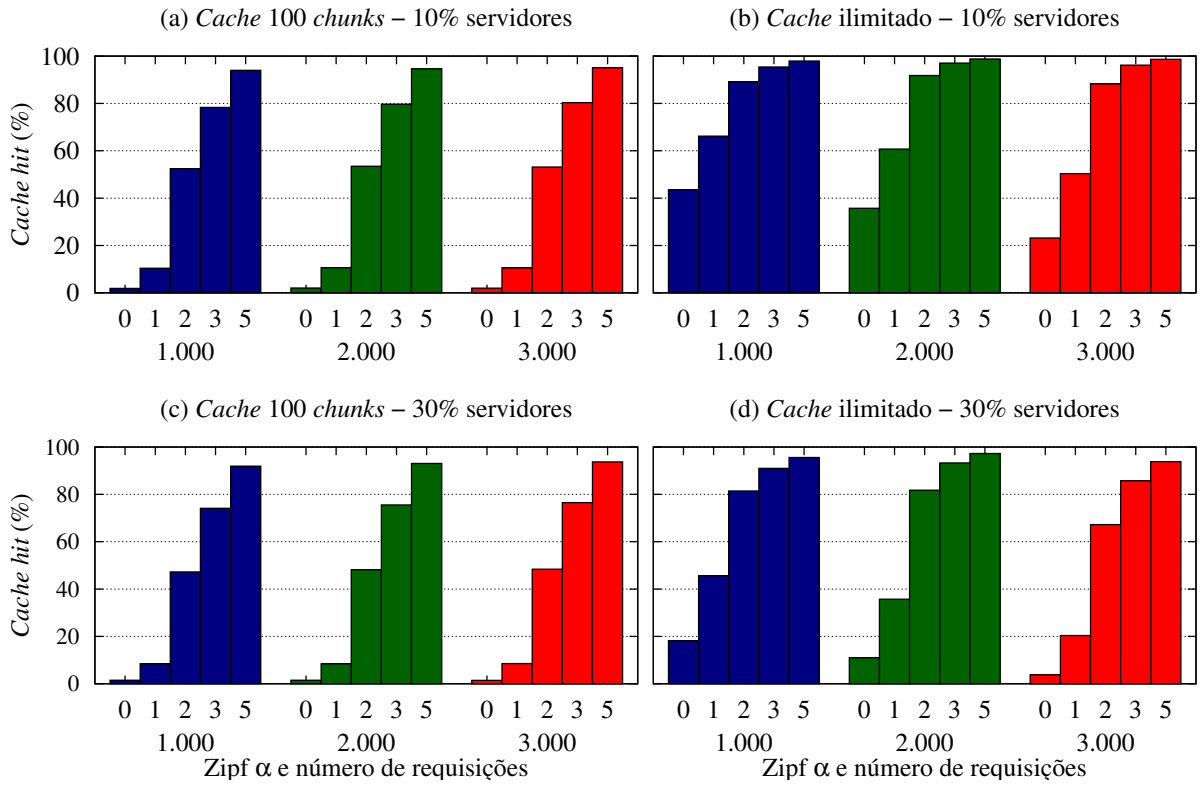

Figura 6.4: *Cache hit* nas requisições dos *chunks*.

Apesar do aumento do tamanho dos *caches* melhorar a probabilidade de *cache hits*, a quantidade de requisições concentradas em menos conteúdos (representada pelo parâmetro α) tem um impacto maior na taxa de *cache hits*. Assim, confirma-se a hipótese de que o paradigma de ICN tem um impacto mais significativo em conteúdos populares, em que um grande número de usuários está interessado. Este fenômeno está presente no acesso a conteúdos multimídia, como vídeos e músicas. Essa tendência é extrapolada nos cenários com $\alpha = 5$ (as requisições dos usuários estão concentradas em 5 de 100 conteúdos disponíveis).

Contudo, também foi observado um comportamento inesperado: a presença de um maior número de servidores na rede afeta negativamente o desempenho dos *caches*, ilustrado nas Figuras 6.4(c) e (d), comparado aos resultados das Figuras 6.4(a) e (b). Esse comportamento pode ser explicado pelo fato de que a existência de mais servidores na rede resulta em uma maior quantidade de caminhos disjuntos que a requisição pode percorrer até encontrar uma cópia do conteúdo, seja em um servidor ou em um *cache*. Consequentemente, o *cache* fica disperso na rede, fazendo com que o conteúdo tenha menos chance de ser encontrado em *cache* e maior chance de ser encaminhado até um servidor.

Entretanto, esse comportamento não é observado em α maiores, já que a maior quantidade de requisições enviadas para esses conteúdos populares aumenta a chance de um conteúdo ser armazenado em *cache*. A Figura 6.5 reforça essa conclusão ao apresentar a carga de requisições atendidas pelos servidores, em que a presença de uma quantidade maior de servidores na rede resulta em mais requisições sendo atendidas por eles.

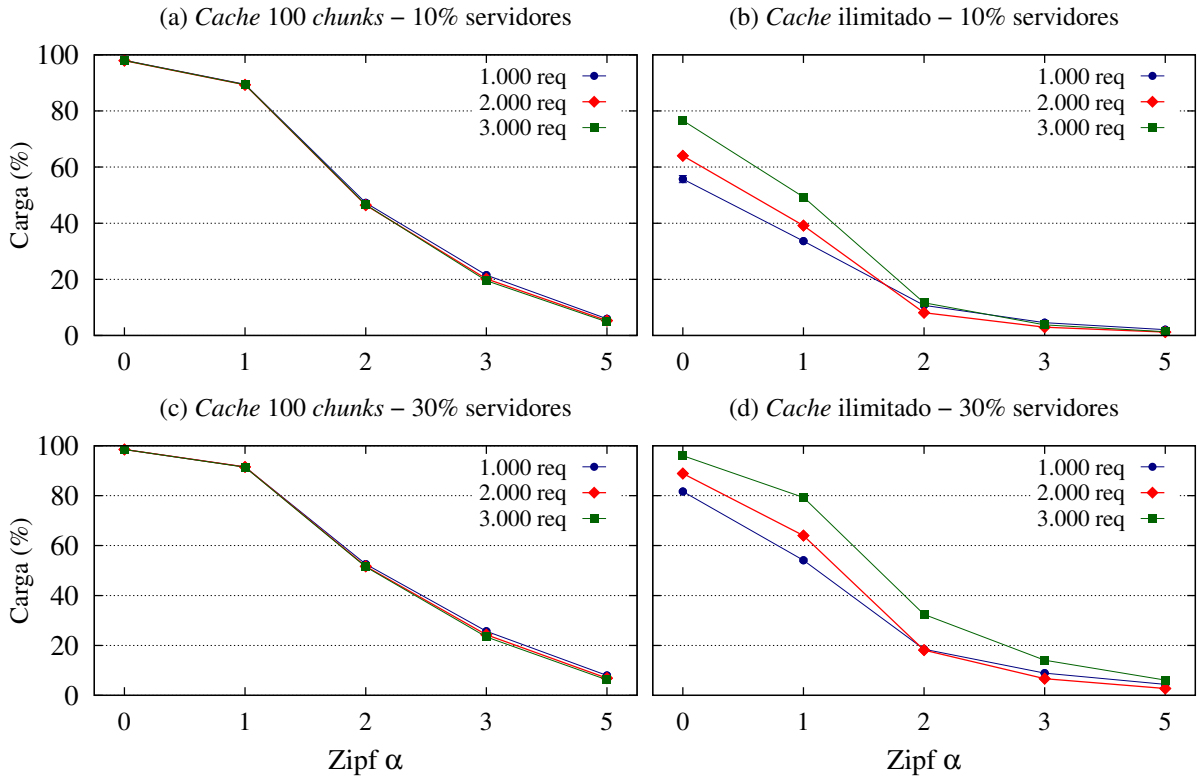

Figura 6.5: Quantidade de *Interesses* satisfeitos diretamente pelos provedores.

Neste contexto, fica claro o potencial de uma ICN bem ajustada na melhora da entrega de conteúdo multimídia, tanto para os usuários quanto para os provedores e ISPs. Primeiramente, o *cache* na rede aproxima o conteúdo do usuário interessado, fazendo uma entrega mais rápida com a diminuição do RTT (*Round Trip Time*) entre a requisição do conteúdo e o seu recebimento. Consequentemente, a quantidade de dados que trafegam pela infraestrutura de rede dos ISPs diminui, sendo localizada mais próxima ao usuário, evitando o uso de enlaces de outros provedores e diminuindo custos de comunicação. Além disso, a infraestrutura de armazenamento e processamento dos provedores de conteúdo para atender aos usuários é distribuída parcialmente entre os *caches* na rede, o que permite que os provedores atendam mais usuários sem precisar investir em aparelhos específicos para cada aplicação, assim como o Netflix faz atualmente ao instalar servidores próprios diretamente nos ISPs, gerando maiores investimentos em equipamentos, funcionários especializados e atualizações de conteúdo entre todos os servidores.

6.2 Desempenho do EU-PRE

O objetivo da avaliação do EU-PRE é validar o desempenho computacional dos seus algoritmos. Esse esquema não possuía uma implementação ou avaliação do seu desempenho quando este trabalho foi iniciado, portanto, é fundamental avaliar a sua

viabilidade computacional. Para isso, implementou-se os seis algoritmos do esquema EU-PRE utilizando a linguagem Python, versão 2.7: *configuração*, *geração de chaves*, *cifragem*, *geração de chaves de recifragem*, *recifragem* e *decifragem*. O desempenho do esquema EU-PRE é comparado a um esquema de criptografia assimétrica tradicional, o RSA. A implementação do RSA avaliada nesse trabalho é a implementada na biblioteca `PyCrypto`, disponível para Python[2].

Para ter uma noção clara do comportamento do EU-PRE, a avaliação é realizada com diferentes tamanhos de mensagens. Contudo, o tamanho da mensagem de interesse é 4KB, o tamanho padrão de um *chunk* na arquitetura NDN. Além disso, as mensagens são cifradas com diferentes tamanhos de chaves: 1.024, 2.048 e 3.072 *bits*. A avaliação do EU-PRE é realizada em dois ambientes distintos, representados pela capacidade de processamento dos dispositivos utilizados, com o objetivo de representar o poder computacional de um provedor de conteúdo e de um dispositivo de usuário final. Identifica-se pelo *cenário A* o lado do provedor de conteúdo e o *cenário B* o lado do usuário. O cenário A é avaliado em um servidor Linux Mint 17 Qiana 64 *bits*, processador AMD Opteron 6136 2,4GHz, com 86GB RAM. Já o cenário B foi avaliado em um *notebook* ASUS, processador Intel Core i5, 1,60GHz, 8GB de RAM e sistema operacional Ubuntu 14.04 64 *bits*.

Os resultados apresentados também são a média de 35 execuções, com um intervalo de confiança de 95%. Os algoritmos de *configuração* e de *geração de chaves* podem opcionalmente serem executados em uma infraestrutura terceirizada e, portanto, não são considerados os custos computacionais dos mesmos. Contudo, assume-se que os provedores de conteúdos e os usuários conheçam de antemão suas respectivas chaves públicas-privadas e os parâmetros do sistema. A Tabela 6.2 resume os parâmetros utilizados para a validação do EU-PRE. Neste estágio, escolheu-se funções de *hash* simples apenas para a validação dos algoritmos, portanto, a segurança das mesmas não é aferida.

Tabela 6.2: Parâmetros utilizados na avaliação do esquema EU-PRE.

Parâmetro	**Valor**
Tamanho da chave	1.024, 2.048, 3.072 *bits*
Tamanho das mensagens (ℓ_0)	0,5, 1, 2, 4, 8, 16, 32, 64 KB
Parâmetro de segurança exigido pelo esquema (ℓ_1)	160 *bits*
Funções de *hash* (H_1, H_3, H_4)	x mod q
Função de *hash* H_2	x mod $2^{(\ell_0+\ell_1)}$

Para a avaliação computacional do EU-PRE são analisados os tempos de cifragem e geração de chaves de recifragem, considerando o cenário A, e os tempos de recifragem e decifragem, considerando o cenário B. Observa-se que as escalas do eixo Y são diferentes entre os gráficos, para uma melhor visualização dos comportamentos e valores obtidos.

6.2.1 Resultados

A análise de desempenho do EU-PRE inicia com a discussão dos tempos para as operações de cifragem e geração de chaves de recifragem, funções do provedor. A Figura 6.6 apresenta os resultados obtidos com essas operações. Os resultados apontam

[2]A implementação dos algoritmos do EU-PRE está disponível em *http://www.inf.ufpr.br/elisam/proxy*.

que o desempenho do esquema é adequado. Por exemplo, a operação de cifragem das mensagens de 0.5 a 64KB, apresentada na Figura 6.6(a), é realizada em menos de 70ms, sendo que a cifragem do *chunk* padrão da NDN, 4KB, acontece em 18ms com uma chave de 2.048 *bits*. Também é importante ressaltar a variância do crescimento do tempo em relação ao tamanho da mensagem; a média de crescimento do tempo entre os vários tamanhos de *chunks* é de 19,61%, 4,51% e 1,70% para chaves de 1.024, 2.048 e 3.072 *bits*, respectivamente.

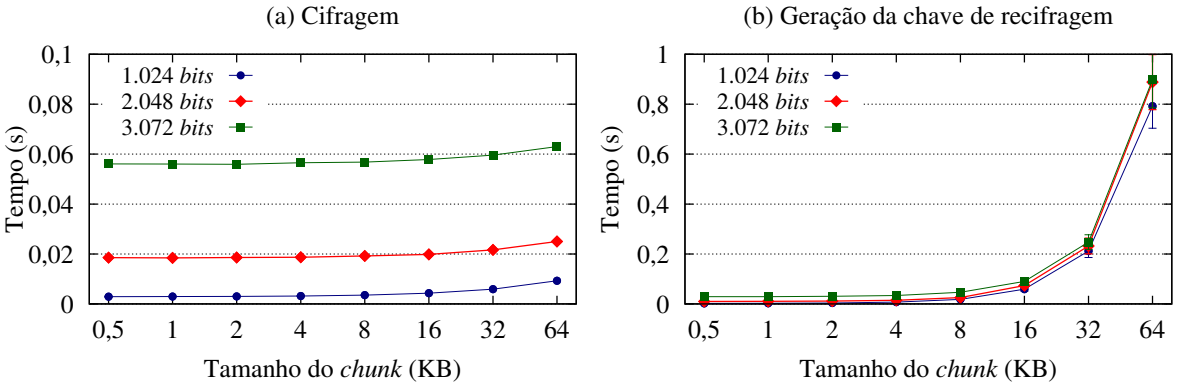

Figura 6.6: Tempo de execução das operações de cifragem e geração de chave de recifragem no esquema EU-PRE - cenário A.

Apesar do tempo necessário para gerar uma chave de recifragem para mensagens de 4KB ser menor que 40ms, mesmo para chaves de 3.072 *bits*, o tempo de processamento aumenta com o tamanho das mensagens em uma taxa muito maior, conforme ilustra a Figura 6.6(b), se aproximando de 1 segundo para mensagens de 64KB. Como o tamanho padrão das mensagens (*chunks*) nas arquiteturas de ICN é de 4KB, isso não representa um impedimento. Contudo, pode ser um problema caso adote-se tamanhos de *chunks* maiores. Porém, ressalta-se que o custo da geração de chaves de recifragem deve-se à geração da variável h, que tem o tamanho da mensagem, na Equação 4.4 (Seção 4.2). Caso essa execução seja otimizada, utilizando por exemplo a criptografia simétrica para a geração do número pseudo-aleatório h [Borges et al., 2012], os tempos para geração da chave de recifragem podem ser menores.

Comparado ao RSA, o esquema EU-PRE se apresenta mais escalável (dentro do intervalo considerado), pois o RSA tem uma taxa de crescimento maior ao aumentar o tamanho da mensagem, conforme ilustra a Figura 6.7(b). Esse comportamento é evidenciado no caso de mensagens de 64KB e uma chave de 3.072 *bits*, em que o RSA tem desempenho inferior ao esquema de recifragem por *proxy* adotado, executando a operação em aproximadamente 130ms enquanto o EU-PRE executa em aproximadamente 70ms. Contudo, vale ressaltar que, para mensagens de 4KB, tanto o EU-PRE quanto o RSA tem desempenho abaixo de 60ms, sendo que o RSA executa a cifragem de 4KB em aproximadamente 8ms para chaves de 3.072 *bits*.

Já os resultados obtidos com as operações de recifragem e decifragem do EU-PRE, apresentados na Figura 6.8, mostram que o tempo para o processamento da recifragem é dependente do tamanho da mensagem, sendo que a recifragem de mensagens de 4KB leva 90,47ms com uma chave de 2.048 *bits*, como mostra a Figura 6.8(a). Ressalta-se que, na solução proposta, o usuário deve também executar a operação de decifragem, apresentada na Figura 6.8(b). A decifragem apresenta um bom desempenho, sendo que o tempo necessário para decifrar é menor que 40ms, independente do tamanho da mensagem

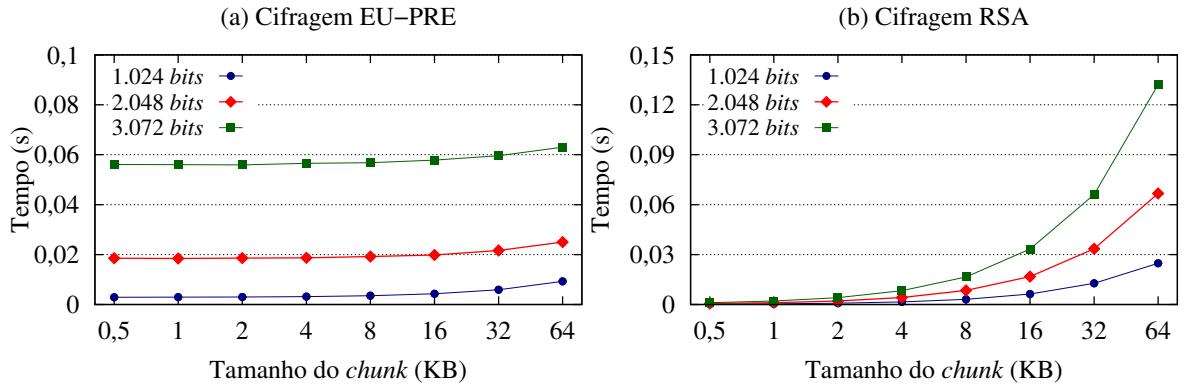

Figura 6.7: Comparação do tempo de execução da operação de cifragem do EU-PRE e RSA - cenário A.

ou do tamanho da chave. Um bom desempenho nas operações de recifragem e decifragem é primordial para o desempenho da solução proposta, pois considera-se que os dispositivos dos usuários devam recifrar e decifrar os *chunks* recebidos a uma velocidade que permita o uso do conteúdo sem pausas, o que é importante principalmente para conteúdos multimídia.

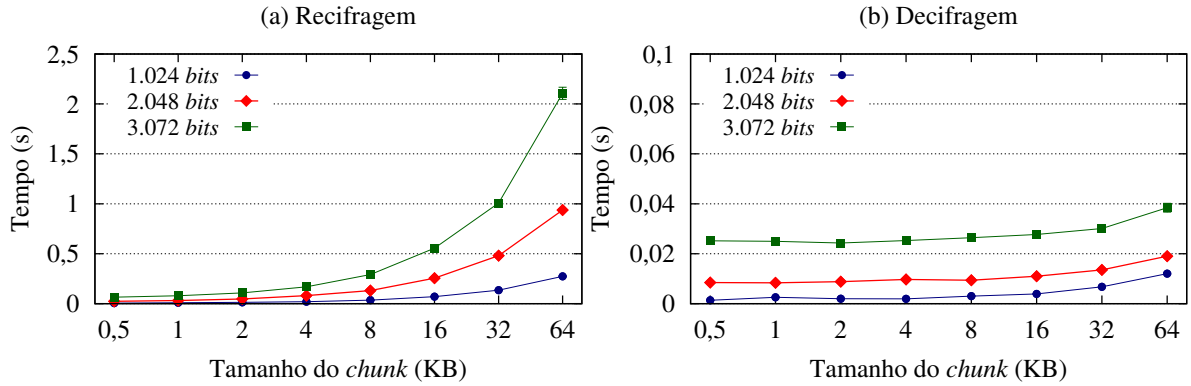

Figura 6.8: Tempo de execução das operações de recifragem e decifragem no esquema EU-PRE - cenário B.

Comparando a soma dos tempos das operações de recifragem e decifragem do EU-PRE com o RSA, Figura 6.9(a) e (b), observa-se que o EU-PRE é mais escalável quando há o aumento do tamanho das mensagens, mesmo considerando as duas operações juntas. Por exemplo, a decifragem do RSA é extremamente lenta, levando aproximadamente 55 segundos para decifrar uma mensagem de 64KB com uma chave de 3.072 *bits*, enquanto a recifragem + decifragem do EU-PRE leva aproximadamente 2 segundos. Também vale ressaltar que os tempos de processamento podem variar de acordo com o *hardware* utilizado e otimizações na implementação dos códigos.

A partir dos tempos obtidos na aferição dos algoritmos do EU-PRE, pode-se observar que as operações de cifragem e decifragem são mais escaláveis que o RSA, já que o crescimento do tempo de processamento ao aumentar o tamanho das mensagens é menor do que os resultados obtidos com o RSA. Contudo, há a operação extra de cálculo de chaves de recifragem para o provedor e a recifragem no usuário, que pode acarretar uma sobrecarga não negligenciável, principalmente para o usuário. Por isso, a próxima subseção discute o impacto do EU-PRE na solução proposta.

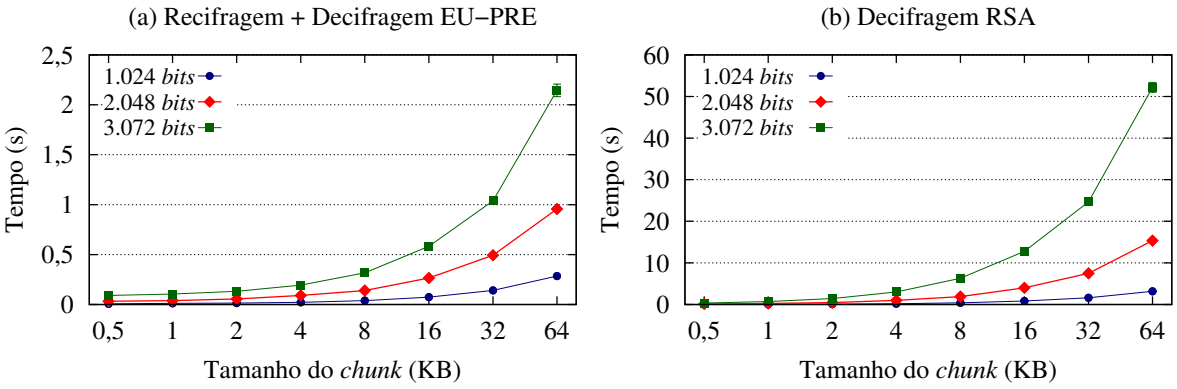

Figura 6.9: Comparação do tempo de execução da operação de decifragem do EU-PRE e RSA - cenário B.

6.3 Desempenho do provedor e do usuário

Para compreender melhor a relevância dos tempos de cifragem, recebimento e decifragem dos *chunks* no fluxo de conteúdos nos provedores e nos usuários, são analisados os tempos totais para cifragem e decifragem de conteúdos inteiros. Para isso, são caracterizadas duas aplicações de recuperação de conteúdo: *streaming* de música, como no serviço Spotify, e *streaming* de vídeos, como no serviço Netflix. No *streaming* de músicas, o tamanho de um conteúdo depende da qualidade do áudio que a aplicação oferece. Para áudios com uma taxa de 96kbps, que é uma qualidade baixa e geralmente utilizada para dispositivos móveis, são recuperados aproximadamente 720KB de dados por minuto; para uma qualidade média de 160kbps, são necessários aproximadamente 1,5MB de dados por minuto, e para uma qualidade alta de áudio, com uma taxa de 320kbps, são recuperados aproximadamente 2,4MB de dados por minuto. Para o *streaming* de vídeos, considerou-se o comportamento para vídeos de qualidade padrão e de alta definição. Para vídeos de qualidade padrão, são necessários aproximadamente 1GB de dados por hora, e para a recuperação de vídeos de alta definição, são necessários aproximadamente 3GB de dados por hora.

Ambas as aplicações são analisadas com diferentes quantidades de operações paralelas, representadas pela quantidade de núcleos de processadores nos dispositivos dos provedores e dos usuários. Para a cifragem do conteúdo no provedor são considerados arquivos de áudio de 1,4, 3, 4,8 e 6MB, representando aproximadamente dois minutos de música para cada conteúdo, e para a cifragem de arquivos de vídeo são considerados arquivos de 1, 1,6, 2 e 6GB, representando aproximadamente duas horas de vídeo para cada conteúdo. Para a recuperação e decifragem dos conteúdos no dispositivo do usuário, são considerados os fluxos esperados em um minuto para músicas e em uma hora para vídeos, o que representa metade do tamanho dos arquivos cifrados. A Tabela 6.3 resume os parâmetros utilizados na análise.

Para a avaliação do domínio do provedor é analisado o tempo para os provedores de conteúdo cifrarem um conteúdo inteiro com qualidades diferentes de áudio e vídeo, assim como o tempo para cifragem de todo um catálogo de conteúdos. Para a análise do domínio do usuário, são computados o tempo que o usuário aguarda para receber uma chave de recifragem e a quantidade de armazenamento necessária para guardar as chaves de recifragem recebidas, além dos tempos para o recebimento, recifragem e decifragem de um *chunk*, resultando no tempo que o usuário aguarda para que um *chunk* esteja pronto

Tabela 6.3: Parâmetros utilizados na avaliação do provedor e do usuário.

Parâmetro	Valor
Arquivos de música (cifragem)	1,4, 3, 4,8 e 6MB
Arquivos de filmes (cifragem)	1, 1,6, 2 e 6GB
Quantidade de núcleos do provedor	16, 18, 24, 32 e 48
Arquivos de música (decifragem por minuto)	720KB, 1,5MB, 2,4MB e 3MB
Arquivos de filmes (decifragem por hora)	500MB, 800MB, 1GB e 3GB
Quantidade de núcleos do usuário	2, 4, 6, 8 e 10

para enviar ao dispositivo de saída. Devido à diferença dos tamanhos de arquivos de música e vídeo, a análise para arquivos de música é realizada em segundos e minutos, enquanto a análise dos vídeos é realizada em horas.

6.3.1 Resultados

Ao adotar uma solução criptográfica para o controle de acesso, é esperada uma sobrecarga nos provedores para a cifragem de todo o seu catálogo de conteúdos e para o cálculo de distribuição de chaves de recifragem. Essa sobrecarga pode afetar negativamente a qualidade de serviço para o usuário, mesmo que os provedores dividam a carga da distribuição de conteúdo com a rede. Contudo, se a segurança das chaves dos conteúdos não for comprometida, essa operação é realizada somente uma vez para o catálogo. Para analisar essas questões, primeiramente investiga-se o tempo necessário para o provedor cifrar um conteúdo inteiro em dois casos: arquivos de música e arquivos de vídeo. Os tempos são comparados utilizando diferentes quantidades de operações paralelas. Também é analisado o tempo para a cifragem de todo o catálogo de conteúdos do provedor. Os resultados apresentados consideram o uso de uma chave de 2.048 *bits*.

A Figura 6.10 apresenta os resultados obtidos com a cifragem de arquivos inteiros de música e de vídeo, com diferentes qualidades. Considerando a cifragem dos arquivos de música, em que o tamanho máximo é de 6MB, apresentado na Figura 6.10(a), a cifragem é executada em menos de 2 segundos, mesmo com o menor número de operações paralelas. Já com 32 e 48 operações paralelas, a operação de cifragem para todos os tamanhos de arquivos ocorre em menos de 1 segundo. A cifragem de arquivos de vídeo, apresentada na Figura 6.10(b), segue o mesmo comportamento, contudo, em uma grandeza de tempo maior. Por exemplo, considerando 16 operações paralelas, os arquivos são cifrados em menos de 30 minutos, enquanto com 48 operações paralelas esse tempo é reduzido para menos de 10 minutos, considerando um arquivo de vídeo de alta definição de 6GB.

Obviamente, esses valores têm uma influência direta no tempo para a cifragem do catálogo inteiro, como mostra a Figura 6.11. Para a cifragem de um catálogo de 100 músicas, o provedor leva menos de 3 minutos, utilizando 16 operações paralelas, como ilustra a Figura 6.11(a). Já para a cifragem de um catálogo de vídeos, o servidor com a mesma quantidade de operações paralelas leva aproximadamente 50 horas para arquivos de alta definição (6GB). Obviamente esses tempos são menores ao considerar mais operações paralelas. Por exemplo, a cifragem de um catálogo de vídeos de qualidade padrão, 2GB, leva menos de 20 horas, como apresenta a Figura 6.11(b). É esperado que os provedores cifrem os conteúdos de antemão e adicionem conteúdos esporadicamente ao seu catálogo, diluindo a carga computacional no tempo. Além disso, é esperado que o catálogo de

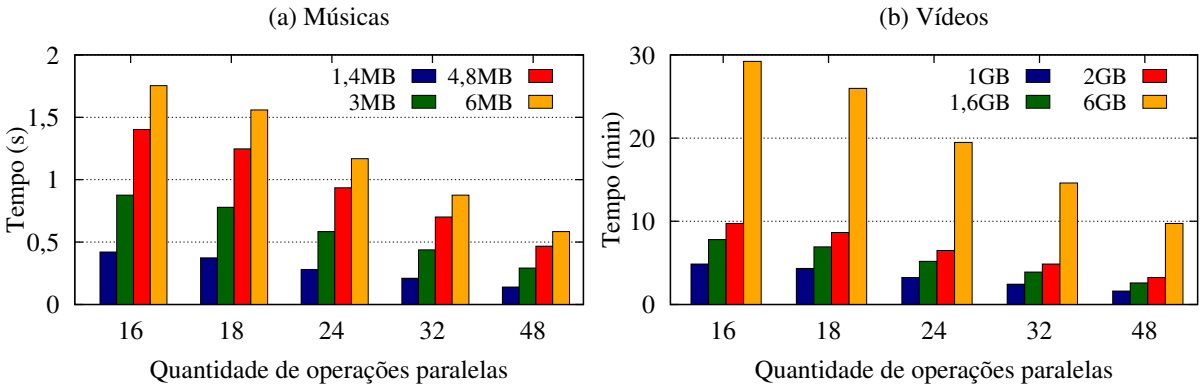

Figura 6.10: Tempo estimado para cifragem de músicas e de vídeos.

conteúdos do provedor seja composto por um conjunto de conteúdos com vários tipos de qualidade, seja de música ou de vídeo, para servir usuários com recursos distintos. Mais ainda, esses tempos consideram apenas um servidor cifrando todo o catálogo, sendo que o tempo para cifrar todo o catálogo de conteúdo pode ser diminuído à medida em que mais servidores participam dessa operação. Além disso, essas operações são realizadas internamente pelos servidores, e não dependem da rede ou dos usuários para completá-la.

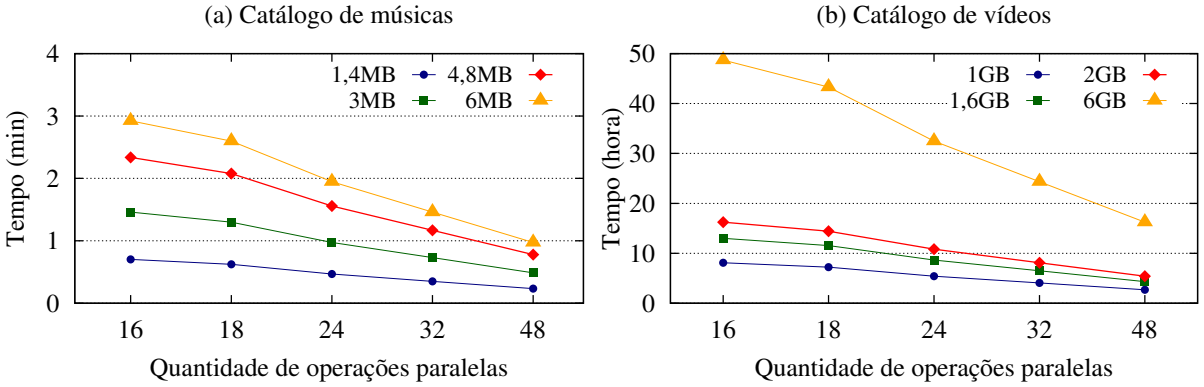

Figura 6.11: Tempo estimado para cifragem de um catálogo inteiro de 100 conteúdos de músicas e de vídeos.

Da perspectiva do usuário, é esperado que o dispositivo receba, recifre e decifre o conteúdo em uma taxa que permita o consumo do conteúdo sem interrupções. A Figura 6.12 ilustra o tempo médio entre a requisição de um *chunk* de 4KB e a sua recifragem/decifragem, estando pronto para uso. São apresentados os resultados referentes à soma dos tempos de recebimento dos *chunks* no cenário com 2.000 requisições, 10% de servidores, *cache* de 100 *chunks* e $\alpha = 3$ (Figura 6.3(a)), com a soma dos tempos do EU-PRE para recifragem e decifragem no dispositivo do usuário. Observa-se que a eficiência da rede resulta em um pequeno impacto no tempo final para o uso do conteúdo pelo usuário, sendo as funções de recifragem e decifragem determinantes no tempo para o consumo do conteúdo.

Para compreender melhor a relevância dos tempos de recebimento, recifragem e decifragem dos *chunks* no fluxo de conteúdos no usuário, estimou-se os tempos totais para recebimento e finalização da decifragem considerando um minuto de execução de arquivos de música e uma hora de execução de arquivos de vídeo. O esperado é que o usuário consiga receber e decifrar o fluxo em menos de um minuto para os arquivos de

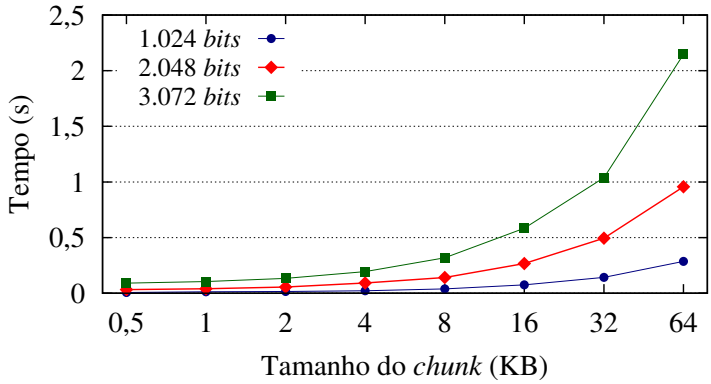

Figura 6.12: Tempo estimado para recuperação, recifragem e decifragem de um *chunk*.

música e em menos de uma hora para os arquivos de vídeo. A Figura 6.13 apresenta os resultados obtidos considerando diversos valores de operações paralelas, desta vez, refletindo um dispositivo de usuário (cenário B). Para os arquivos de música, apresentados na Figura 6.13(a), os resultados mostram que o tempo decorrido desde a requisição do primeiro *chunk* do conteúdo até a recifragem/decifragem do último *chunk* é menor que um minuto, ou seja, o usuário recebe, recifra e decifra a quantidade de dados necessários para a execução de um minuto de música em menos de um minuto, mesmo considerando apenas duas execuções paralelas e arquivos de áudio de alta qualidade (2,4MB).

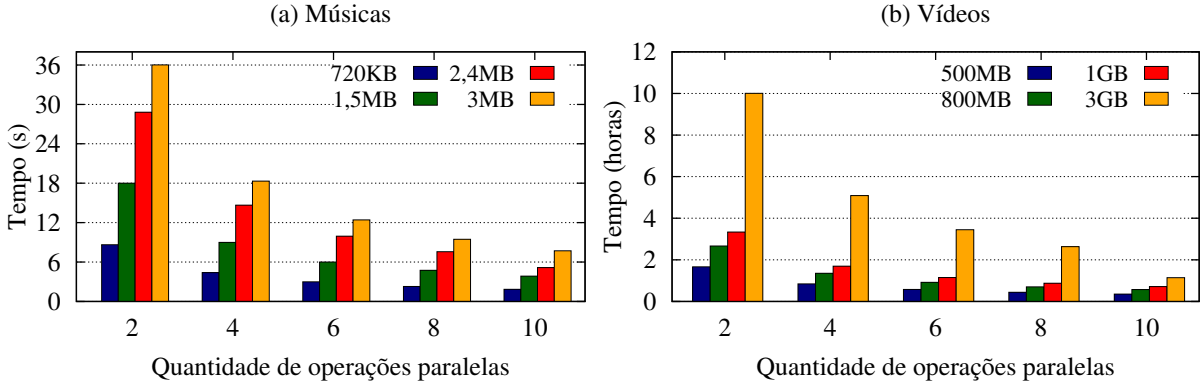

Figura 6.13: Tempo estimado para recuperação, recifragem e decifragem de arquivos de músicas e vídeos.

Contudo, para a recifragem/decifragem de arquivos de vídeo, apresentados na Figura 6.13(b), exige-se uma carga de processamento muito maior do usuário, sendo que apenas a partir de seis operações paralelas os arquivos de qualidade padrão são recebidos, recifrados e decifrados em menos de uma hora, o que é necessário para que a aplicação não sofra com a falta de conteúdo em *buffer* e prejudique a experiência do usuário. Portanto, o tempo de recuperação e decifragem ultrapassa o tempo esperado de execução do vídeo, sendo que o tempo de *download* do conteúdo é responsável por apenas 1,75% do tempo total. Arquivos de alta definição (3GB) ultrapassam uma hora para recebimento, recifragem e decifragem, mesmo extrapolando a quantidade de operações paralelas para dez, o que significa que são necessárias mais de uma hora de computação de recifragem/decifragem para o usuário usufruir de uma hora de vídeos de alta definição. Assim, as operações de recifragem e decifragem representam uma grande carga computacional no dispositivo do usuário, revelando que há margens para otimizações.

Além do custo computacional das operações do esquema EU-PRE, também foi aferido o tamanho das chaves de recifragem criadas pelo provedor de conteúdo, conforme ilustra a Figura 6.14. O objetivo é verificar o custo de comunicação no envio das chaves de recifragem, além do espaço para armazenamento das chaves de recifragem no usuário, já que para cada conteúdo acessado, o usuário deve solicitar e receber uma chave de recifragem diferente. Com base nos resultados obtidos, observou-se que o tamanho de uma chave de recifragem para um conteúdo é dependente do tamanho do *chunk*, somado a uma pequena sobrecarga. Isso mostra que o custo para a recuperação de uma chave de recifragem para cada conteúdo, considerando o MTU (*Maximum Transmission Unit*) padrão de 1.500 *bytes* e *chunks* de tamanho 4KB, é de aproximadamente 3 RTTs. Contudo, uma mesma chave de recifragem é utilizada para todos os *chunks* pertencentes ao mesmo conteúdo, sendo que para recifrar um conteúdo inteiro só é necessário uma chave de recifragem.

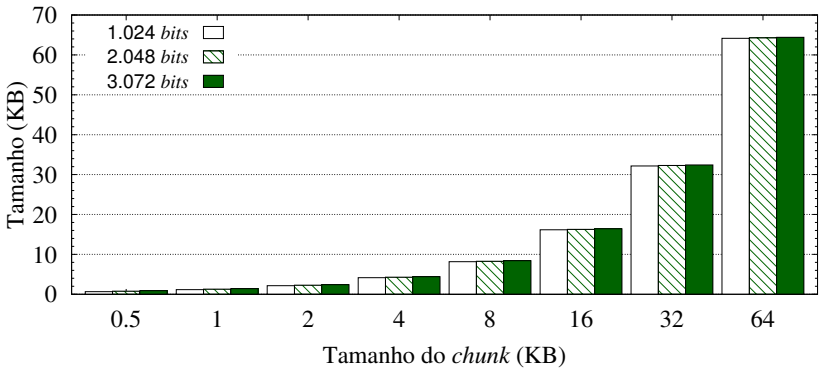

Figura 6.14: Tamanho das chaves de recifragem do esquema EU-PRE.

De acordo com a solução proposta, é esperado que as requisições pela chave de recifragem sejam roteadas até um servidor de aplicação disponível, que por sua vez responde ao usuário com a chave de recifragem correspondente ao conteúdo que ele deseja acessar. Apesar da possibilidade de armazenar as chaves de recifragem em *cache*, esse comportamento não é vantajoso para o usuário nem para a rede, pois a chave de recifragem serve para todos os *chunks* de um conteúdo e só seria útil resgatá-la de um *cache* caso o usuário acesse novamente o mesmo conteúdo antes que as políticas de *cache* retirem naturalmente a chave de recifragem do *cache*, o que é pouco provável.

Desta forma, a Figura 6.15 apresenta uma análise do tempo necessário para um usuário obter uma chave de recifragem do provedor, considerando o tempo desde a requisição, cálculo da chave pelo provedor e envio da chave ao usuário. Como esperado, o tamanho da chave utilizada na solução de controle de acesso é o fator determinante do tempo que o usuário aguarda para o recebimento da chave. Contudo, mesmo com chaves de 3.072 *bits*, o tempo total para o recebimento das chaves de recifragem é menor que 50ms. Observa-se também que quanto mais servidores de aplicação disponíveis na rede, menor o tempo para o recebimento da chave de recifragem. Esse comportamento é esperado, pois como o *cache* na rede não influencia no tempo das requisições das chaves de recifragem, a presença de mais provedores de conteúdo significa uma maior probabilidade dos seus servidores estarem mais próximos dos usuários, diminuindo o tempo da requisição.

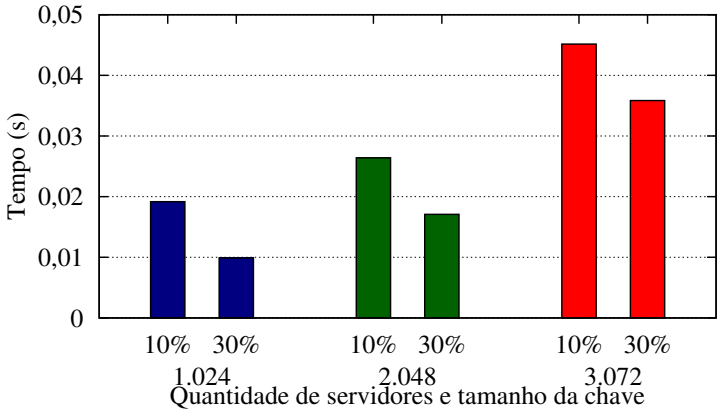

Figura 6.15: Tempo para requisição, cálculo e recebimento da chave de recifragem com relação ao tamanho das chaves utilizadas no esquema EU-PRE.

6.4 Considerações finais

Este capítulo apresentou uma avaliação da eficiência da NDN na distribuição de conteúdo, do desempenho computacional dos algoritmos do EU-PRE e do desempenho da solução de controle de acesso proposta na recuperação de músicas e vídeos. Os resultados mostram que as aplicações multimídia se beneficiam do paradigma de ICN, principalmente considerando conteúdos muito populares e *caches* com capacidade de armazenamento limitado, porém suficiente para acomodar uma parcela considerável dos conteúdos populares. Também foram validados os algoritmos do EU-PRE, e, enquanto arquivos de músicas são recebidos e decifrados em um tempo suficiente para uma ótima reprodução no dispositivo do usuário, a solução proposta exige maior desempenho computacional dos dispositivos dos usuários para executar as operações criptográficas de recifragem/decifragem para o consumo de vídeos de alta definição. O próximo capítulo apresenta uma proposta e avaliação de uma otimização dos algoritmos de recifragem e decifragem do EU-PRE, além de uma análise comparativa de outras duas soluções de controle de acesso criptográficas para ICN: criptografia de *broadcast* e criptografia baseada em atributos.

Capítulo 7

Otimização do EU-PRE e comparação com outras soluções

Este capítulo apresenta uma proposta de otimização dos algoritmos de recifragem e decifragem do esquema EU-PRE e compara seu desempenho com outras duas soluções de controle de acesso para ICN. Ele está dividido em duas seções: a Seção 7.1 detalha a otimização proposta, apresenta as equações otimizadas e compara a otimização com o esquema EU-PRE original. A Seção 7.2 compara a solução proposta, agora otimizada, com outras duas soluções criptográficas para o controle de acesso em ICN: a criptografia de *broadcast* e a criptografia baseada em atributos.

7.1 Proposta

Com a alocação das funções do *proxy* no domínio do usuário, é possível realizar a junção das operações de recifragem e decifragem, o que pode resultar em uma execução mais rápida dessas funções no dispositivo do usuário. A incorporação dessas operações é justificável, pois são operações dependentes e sempre são executadas em conjunto pelo usuário. As propriedades do esquema EU-PRE garantem que o usuário, de posse do conteúdo cifrado e da chave de recifragem, não pode descobrir a chave privada do provedor e a otimização proposta não introduz vulnerabilidades no funcionamento do esquema.

A otimização envolve as Equações 4.6 (recifragem) e 4.8 (decifragem), descritas na Seção 4.2 e reapresentadas abaixo para maior clareza. No modelo do EU-PRE original, o *proxy* recebe do provedor as variáveis (D, E, F, s) e a chave de recifragem $(rk_{c\to u}, V, W)$, do conteúdo c para o usuário u. Após realizar as validações com as variáveis D e E, o *proxy* calcula a mensagem recifrada para enviar ao usuário, utilizando a chave de recifragem desse usuário, conforme Equação 7.1.

$$E' = E^{rk_{c\to u}} \bmod p \tag{7.1}$$

O *proxy* envia para o usuário as variáveis (E', F, V, W). Para recuperar o conteúdo c, o usuário deve executar a Equação 7.2, em que a variável E', calculada anteriormente pelo *proxy*, é utilizada em conjunto com F e h (recuperado anteriormente pela Equação 4.7).

$$(m||\omega) = F \oplus H_2(E'^{h^{-1} \bmod p-1} \bmod p) \tag{7.2}$$

Na solução proposta, essas duas operações são realizadas na mesma entidade (o usuário), o que permite a simplificação da operação de recifragem diretamente na função

de decifragem, aplicando a variável E diretamente na Equação 7.2. O usuário agora recebe diretamente do provedor de conteúdo as variáveis (D, E, F, s). Como o usuário já está de posse da variável E, pode-se eliminar a Equação 7.1 ao substituir o E', antes recebido do *proxy*, por E, agora recebido do provedor, e aplicando o expoente $rk_{c\to u}$ diretamente na Equação 7.2, conforme Equação 7.3.

$$\begin{aligned}(m||\omega) &= F \oplus H_2((E^{rk_{c\to u}} \bmod p)^{\frac{1}{h} \bmod p-1} \bmod p) \\ &= F \oplus H_2(E^{rk_{c\to u}\cdot\frac{1}{h} \bmod p-1} \bmod p) \\ &= F \oplus H_2(E^{\frac{rk_{c\to u}}{h} \bmod p-1} \bmod p)\end{aligned} \tag{7.3}$$

O esquema EU-PRE garante que o esquema não é vulnerável ao conluio do *proxy* com o usuário, assim, assume-se que qualquer informação conhecida pelo *proxy* e pelo usuário juntos não interferem na segurança da solução otimizada.

No restante deste capítulo, refere-se ao EU-PRE como o esquema de recifragem por *proxy* original proposto por [Chow et al., 2010] e ao EU-RE (*Efficient Unidirectional Re-encryption*) como o esquema otimizado utilizado na solução proposta, enfatizando a ausência do *proxy*.

7.1.1 Avaliação da otimização

A validação do esquema otimizado, EU-RE, tem o objetivo de aferir o ganho de desempenho em comparação com o esquema original, EU-PRE. Os parâmetros de simulação são idênticos aos resumidos na Tabela 6.2 (Seção **??**), e as métricas são o tempo de computação das operações de recifragem e decifragem. Os resultados obtidos com o esquema otimizado são comparados ao esquema EU-PRE original, sendo que os resultados apresentados são a soma do tempo das operações de recifragem e decifragem para ambos os esquemas [1]. Vale ressaltar que as operações de cifragem e geração de chaves de recifragem, ambas executadas nos provedores, não sofreram alterações com a otimização proposta e não são reavaliadas nessa seção.

A Figura 7.1 apresenta os resultados obtidos com o esquema otimizado, comparados aos resultados obtidos com o esquema original, já apresentados na Seção **??**. Observa-se que a otimização proposta resulta em um ganho expressivo nos tempos de recifragem e decifragem somados no usuário, sendo que o impacto é maior para as mensagens maiores, obtendo uma redução de até 96%, com chaves de 3.072 *bits* e *chunks* de 64KB. Contudo, o impacto para as mensagens menores também é expressivo, sendo que para *chunks* de 4KB a média do ganho de desempenho é de 75%. O menor ganho ocorre com *chunks* de 0,5KB, 43%. O desempenho da versão otimizada é melhor porque na versão original, o expoente da Equação 7.1 é dependente do tamanho da mensagem, assim como o seu tempo de processamento. Na versão otimizada, essa equação é eliminada e o novo expoente é menor.

Além da melhoria no desempenho, observa-se que no esquema original há uma inversão em h (Equação 7.1) que depende do tamanho da mensagem; já no esquema otimizado, essa inversão é realizada em $rk_{c\to u}/h$ (Equação 7.3). Consequentemente, no esquema otimizado, o tempo para computar essas operações tem uma variação menor com o aumento do tamanho das mensagens, apresentada com maiores detalhes na Tabela 7.1. Por exemplo, considerando chaves de 2.048 *bits*, a diferença de tempo entre a

[1] A implementação do código otimizado está disponível em *http://www.inf.ufpr.br/elisam/proxy*.

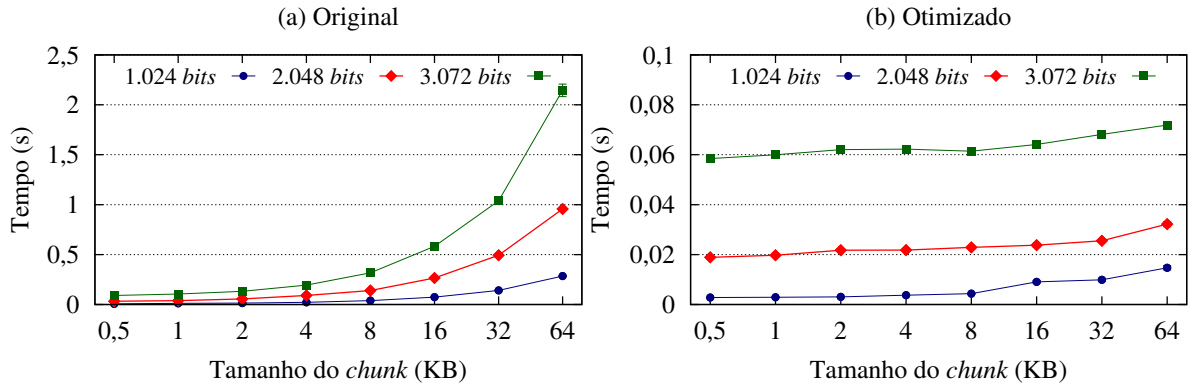

Figura 7.1: Comparação de desempenho do esquema de recifragem por *proxy* original (EU-PRE) e otimizado (EU-RE).

recifragem/decifragem de um *chunk* de 0,5KB para um *chunk* de 64KB é de 14403,58ms na versão original, e 153,7ms na versão otimizada. Esse comportamento é interessante caso as arquiteturas de ICN vierem a adotar *chunks* de tamanhos maiores. A Tabela 7.1 também apresenta a porcentagem de otimização do tempo de recifragem/decifragem e os resultados obtidos com a recifragem/decifragem de um *chunk* de 1MB, enfatizando o ganho de desempenho em *chunks* de tamanho maiores.

Tabela 7.1: Comparação dos tempos de processamento das funções de recifragem + decifragem do esquema original e otimizado no cenário B (ms).

Chunk **(KB)**	**1.024 *bits***			**2.048 *bits***			**3.072 *bits***		
	EU-PRE	EU-RE	%	EU-PRE	EU-RE	%	EU-PRE	EU-RE	%
0,5	6,10	2,81	53,93	31,87	18,92	40,63	90,29	58,46	35,25
1	11,54	2,92	74,70	39,00	19,75	49,36	104,24	59,95	42,49
2	14,72	3,04	79,35	55,28	21,77	60,62	132,10	62,03	53,04
4	21,71	3,72	82,87	90,47	21,78	75,93	193,60	62,27	67,84
8	38,60	4,33	88,78	140,01	22,89	83,65	317,14	61,42	80,63
16	73,88	9,06	87,74	265,45	23,77	91,05	582,53	64,10	89,00
32	141,31	9,91	92,99	493,87	25,51	94,83	1037,77	68,14	93,43
64	285,23	14,73	94,84	956,40	32,19	96,63	2145,15	71,88	96,65
1.024	4179,24	153,31	96,33	14435,45	172,62	98,80	30898,34	216,01	99,30

Para verificar o impacto da otimização proposta no dispositivo do usuário, a Figura 7.2 compara os tempos para o recebimento, recifragem e decifragem de arquivos de música e vídeo utilizando o esquema original e o otimizado. Para os arquivos de música foram contabilizados os tempos de processamento para arquivos de qualidade média (1,5MB) e alta (2,4MB). A versão original já satisfazia os critérios de tempo para o fluxo ($<$ 1 minuto), sendo que o esquema otimizado recebe, recifra e decifra em menos de 7 segundos, mesmo considerando o cenário com apenas duas operações paralelas e arquivos de qualidade alta. Esse ganho de desempenho é interessante para a utilização da solução proposta em dispositivos com recursos escassos, como *smartphones*.

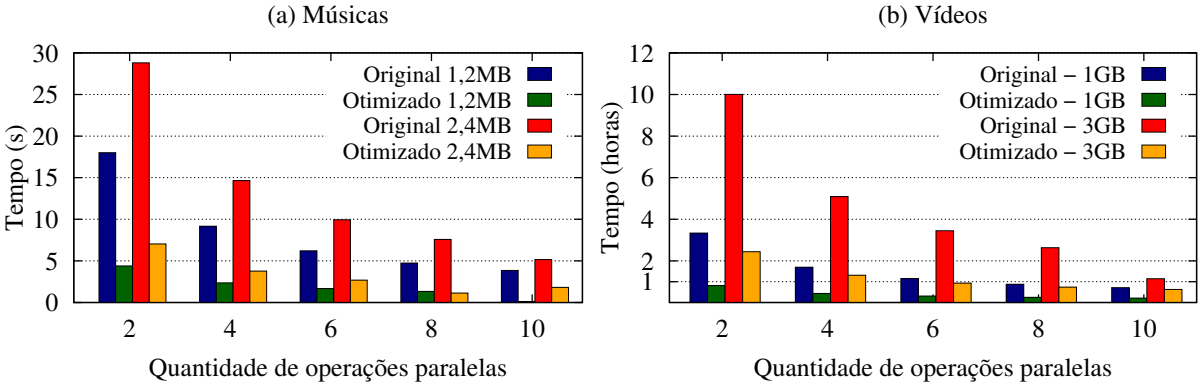

Figura 7.2: Comparação da recifragem + decifragem do esquema original e otimizado.

Já para o recebimento de vídeos, a otimização proposta se mostra ainda mais eficaz. Na versão original, nem mesmo ao considerar dez operações paralelas o dispositivo do usuário é capaz de recifrar/decifrar um vídeo de alta definição (3GB) em menos de uma hora. Com a otimização, é possível executar um vídeo de alta definição a partir de seis operações paralelas. Além disso, na versão original, a recifragem/decifragem representa aproximadamente 98% do tempo total de recebimento e decifragem, e na versão otimizada, 92%. O desempenho alcançado ainda não é ideal para o uso da solução proposta em dispositivos com recursos escassos, porém, a execução de vídeos de alta definição de longa duração é mais usual em dispositivos como *notebooks* e vídeo *games*, que possuem uma melhor configuração de *hardware* e fonte de energia abundante.

7.2 Comparação de soluções de controle de acesso

A fim de validar as características da solução otimizada em comparação com outras soluções de controle de acesso criptográficas propostas para ICN, foram escolhidas duas soluções que têm o potencial de satisfazer dois objetivos: (1) o conteúdo em *cache* pode servir o maior conjunto de usuários possível e (2) os provedores podem ativamente controlar quem acessa o conteúdo, independentemente do local em que o conteúdo é recuperado. Assim, foram escolhidas a criptografia de *broadcast* e a criptografia baseada em atributos. Como as soluções de controle de acesso baseadas em criptografia têm características distintas, elas podem ser adequadas para aplicações diferentes.

A criptografia de *broadcast* (BE) [Boneh et al., 2005] compreende uma entidade central que cifra as mensagens com uma chave secreta única para um grupo de usuários. Essa chave secreta é cifrada com a chave pública do grupo, e cada usuário pode extrair a chave secreta individualmente usando sua própria chave privada. A chave secreta é distribuída em um *enabling block* (EB) na forma de um conteúdo, que pode ser compartilhado entre todos os usuários. O BE tem sido efetivamente usado em vários contextos em que um conjunto de usuários precisa decifrar o mesmo arquivo, como a proteção de discos Blu-ray e serviços de assinatura de TV [Boneh et al., 2005].

A possibilidade de que um grande grupo de usuários possa acessar o mesmo conteúdo cifrado com a mesma chave secreta faz do BE uma solução interessante para uso em ICN, já que permite que os *caches* na rede trabalhem com todo o seu potencial. A Figura 7.3(a) ilustra um exemplo do uso do BE para controle de acesso em ICN, como proposto em [Misra et al., 2013]. Os provedores de conteúdo devem cifrar o conteúdo com

uma chave secreta e cifrar essa chave secreta com a chave pública do grupo de *broadcast*, gerando o EB $/p1/EB$. Em seguida, o provedor calcula e distribui diferentes chaves privadas para cada usuário autorizado no grupo. Para decifrar o conteúdo, o usuário deve recuperar e extrair a chave secreta do EB, utilizando a sua chave privada dada pelo provedor. Por exemplo, as requisições do usuário $u1$ para o conteúdo $/p1/a$ e para o EB são satisfeitas pelo *cache* do roteador $R4$. De posse do conteúdo, do EB e da sua chave privada, o usuário $u1$ é capaz de decifrar o conteúdo com êxito, bem como $u2$, que também possui uma chave do grupo e pode recuperar o mesmo conteúdo dos *caches* na rede.

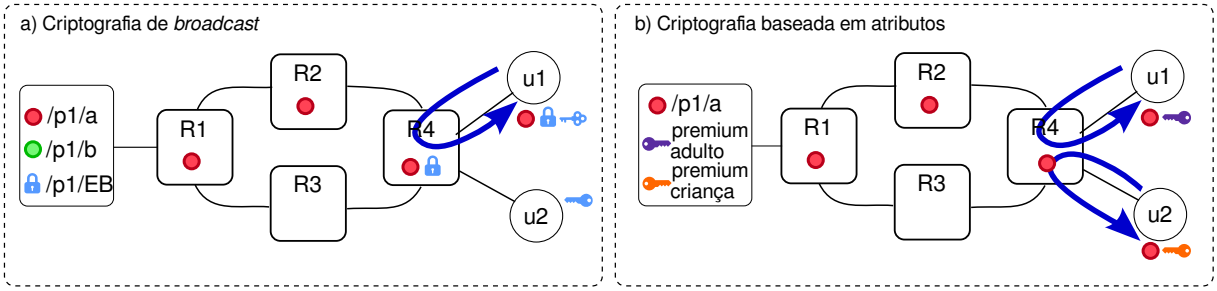

Figura 7.3: Modelos de controle de acesso com (a) criptografia de *broadcast* e (b) criptografia baseada em atributos.

Já a criptografia baseada em atributos (ABE) [Bethencourt et al., 2007, Lewko et al., 2010] considera um conjunto de atributos dos usuários para conceder acesso a um conteúdo cifrado. Existem duas variantes dos esquemas de ABE: *Key-Policy* (KP) e *Ciphertext-Policy* (CP). No esquema KP, os atributos são incorporados no texto cifrado e a chave contém as políticas que determinam quais atributos o usuário deve ter para decifrá-lo, enquanto que no esquema CP os atributos são incorporados na chave e as políticas são aplicadas no conteúdo cifrado. Assim, no esquema KP-ABE, quem emite as chaves tem controle sobre quem decifra o conteúdo, enquanto no CP-ABE quem cifra o conteúdo tem o controle sobre quem o decifra.

Os esquemas de ABE têm sido bastante explorados no contexto de controle de acesso em ICN [Ion et al., 2013, Papanis et al., 2013, Li et al., 2014], principalmente porque permitem que apenas usuários que satisfaçam os atributos, através da chave privada, possam decifrar o conteúdo, não importa de onde o conteúdo foi recuperado. Além disso, ele não exige que os provedores estejam ativos para a verificação das políticas de acesso. Ambos os modelos KP-ABE e CP-ABE são explorados, devido à flexibilidade na criação de políticas e pelo controle do provedor sobre os atributos para decifragem.

A Figura 7.3(b) ilustra uma solução de controle de acesso baseada em ABE para ICN, como proposto em [Papanis et al., 2013]. O provedor cifra o conteúdo $/p1/a$ com os atributos permitidos, *premium* e *adulto* neste exemplo. Qualquer usuário que possuir uma chave com tais atributos está autorizado a decifrá-lo. Em seguida, o conteúdo é disponibilizado para os usuários e pode ser armazenado em *cache* nos roteadores. No caso de uma cópia em *cache* satisfazer uma requisição de conteúdo, não há a necessidade de o usuário entrar em contato com o provedor para decifrá-lo; uma chave previamente entregue (com os atributos necessários para decifrar o conteúdo) é suficiente para que o usuário o decifre. Por exemplo, o usuário $u1$ recebe uma cópia em *cache* do conteúdo $/p1/a$ e a política é satisfeita pelos atributos presentes em sua chave. Por outro lado, o usuário $u2$ não tem os atributos necessários para satisfazer as políticas incorporadas no conteúdo, assim, mesmo que ele não se comunique com o provedor de conteúdo, o controle de acesso é eficaz pois $u2$ não pode decifrar o conteúdo, já que seus atributos são *premium* e *criança*.

7.2.1 Cenário

Para comparar as características das soluções de controle de acesso criptográficas para a distribuição de conteúdo multimídia no paradigma de ICN, foram escolhidas as soluções de [Misra et al., 2013] para a criptografia de *broadcast*, a solução de [Papanis et al., 2013] para a criptografia baseada em atributos e a solução proposta neste trabalho para a recifragem por *proxy*. Essas soluções foram escolhidas devido à relevância e potencial de adesão aos princípios da ICN, além da disponibilidade do código para simulação. Para a criptografia de *broadcast*, foi utilizada a implementação dos algoritmos de [Boneh et al., 2005], com grupos de 512, 2.048, 8.192, 32.768 e 131.072 usuários. Para a solução baseada em ABE, considerou-se tanto a versão KP quanto a versão CP. Foram aferidos os algoritmos de [Bethencourt et al., 2007, Lewko et al., 2010], com um conjunto de 10, 20, 30, 40 e 50 atributos. Para a recifragem por *proxy* utiliza-se a versão otimizada EU-RE e tamanhos de chaves de 1.024, 2.048 e 3.072 *bits* [2]. A Tabela 7.2 resume os parâmetros utilizados nas simulações.

Tabela 7.2: Parâmetros utilizados na avaliação do BE, ABE e EU-RE.

Parâmetros	**Valor**
Tamanho do grupo BE	512, 2.048, 8.192, 32.768 e 131.072
Quantidade de atributos do ABE	10 a 50 (incrementos de 10)
Tamanho das chaves no EU-RE	1.024, 2.048 e 3.072
Parâmetros de segurança (*bits*)	BE 201, ABE 512, EU-RE 160

A análise busca comparar os tempos das operações criptográficas para a geração de chaves e cifragem, no domínio do provedor de conteúdo, e de decifragem, no domínio do usuário. Também é analisado o tempo para recebimento e decifragem de fluxos de música e de vídeo, em cada uma das soluções. As simulações foram realizadas em um *notebook* ASUS, processador Intel Core i5 1,60GHz, 8GB de RAM e sistema operacional Ubuntu 14.04 LTS 64-bit. Todos os resultados apresentados são a média de 35 execuções, com um intervalo de confiança de 95%.

7.2.2 Resultados

A Figura 7.4 apresenta o desempenho computacional do BE para as operações de geração de chaves, cifragem da chave secreta e decifragem, com diferentes tamanhos de grupos. A geração de chaves do BE, Figura 7.4(a), está diretamente relacionada ao tamanho do grupo de *broadcast* que o provedor deseja que seja capaz de decifrar um conteúdo com a mesma chave secreta. Assim, o custo para criar as chaves para todos os usuários no grupo pode ser proibitivo para grupos com muitos usuários, especialmente se os provedores de conteúdo lidarem também com um grande número de grupos distintos. Por exemplo, um grupo com um pouco mais de 131.000 usuários exige aproximadamente 30 minutos para a geração das chaves. Além disso, a inclusão de novos membros no grupo pode exigir a geração de novas chaves para todos os usuários do grupo, pois o grupo precisa ser refeito para adicionar mais usuários além da quantidade inicial para a qual foi

[2] A implementação da solução de criptografia de *broadcast* está disponível em *crypto.stanford.edu/pbc/bce/* e da solução de criptografia baseada em atributos está disponível em *code.google.com/p/libfenc/*.

criado. Por outro lado, as operações de cifragem e decifragem são rápidas, como ilustra a Figura 7.4(b), pois compreendem somente a cifragem e decifragem da chave secreta usada na cifragem dos conteúdos. Vale lembrar que o provedor de conteúdo deve ainda cifrar os conteúdos com a chave secreta utilizando algum mecanismo de criptografia simétrica, como o AES (*Advanced Encryption Standard*) (essa operação não está contabilizada).

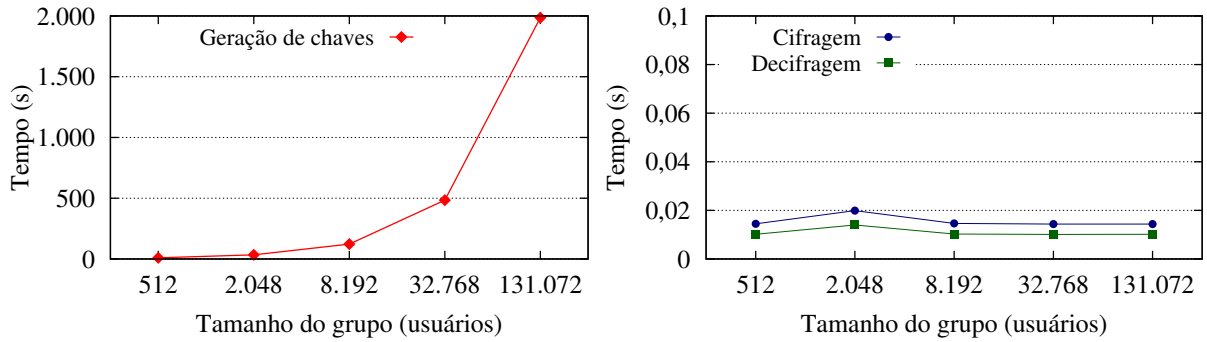

Figura 7.4: Desempenho do BE na geração de chaves, cifragem e decifragem.

Já o ABE, apresentado na Figura 7.5, é influenciado pela quantidade de atributos utilizados. Quanto mais atributos, maior o tempo de computação.

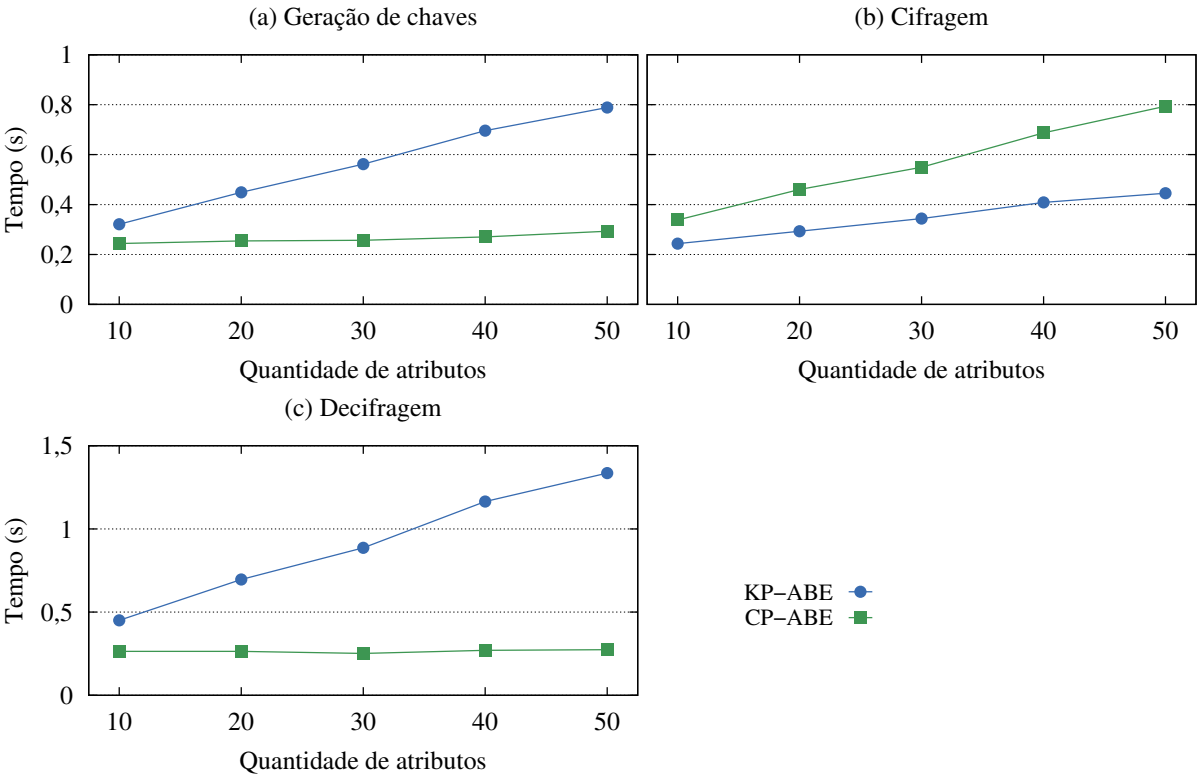

Figura 7.5: Desempenho do ABE na geração de chaves, cifragem e decifragem.

Porém, mais atributos significam um melhor controle no acesso ao conteúdo. Como esperado, a geração de chaves do KP-ABE é mais demorada do que o CP-ABE, conforme ilustra a Figura 7.5(a), bem como a cifragem com o CP-ABE consome mais tempo do que o KP-ABE (Figura 7.5(b)). Isso ocorre porque o CP-ABE incorpora os atributos diretamente no texto cifrado enquanto o KP-ABE incorpora os atributos na própria chave.

Como o número de atributos pode crescer à medida que o controle de acesso é ajustado, pode ser necessário cifrar o mesmo conteúdo para diferentes grupos de atributos a fim de evitar a sobrecarga da grande quantidade de atributos na geração de chaves e cifragem. A operação de decifragem também reflete essas características: o CP-ABE apresenta uma menor sobrecarga quando comparado ao KP-ABE, pois no KP-ABE as políticas de acesso são reforçadas no momento da decifragem, conforme a chave do usuário. Os resultados são apresentados na Figura 7.5 (c).

A Figura 7.6 apresenta o tempo estimado entre a requisição de um *chunk* pelo usuário e a completa decifragem, estando pronto para a reprodução. O resultados apresentados consideram a soma dos tempos de recebimento de *chunks* de 4KB no cenário com 2000 requisições, 10% de servidores e $\alpha = 3$ (Figura 6.3(a)), somados aos tempos de decifragem das três soluções consideradas. Observa-se que todas as soluções de controle de acesso levam menos de um segundo para que o *chunk* esteja pronto para a reprodução, embora o BE e o EU-RE apresentem a menor sobrecarga, aproximadamente 10 e 30ms por *chunk*, respectivamente. O KP-ABE leva mais de 80ms, compensando o menor tempo de processamento nas operações de cifragem; como as políticas de acesso estão na chave, ele leva mais tempo na decifragem do conteúdo. Por outro lado, o CP-ABE realiza as operações de decifragem mais rápido, pois as políticas já foram incorporadas no conteúdo através da operação de cifragem.

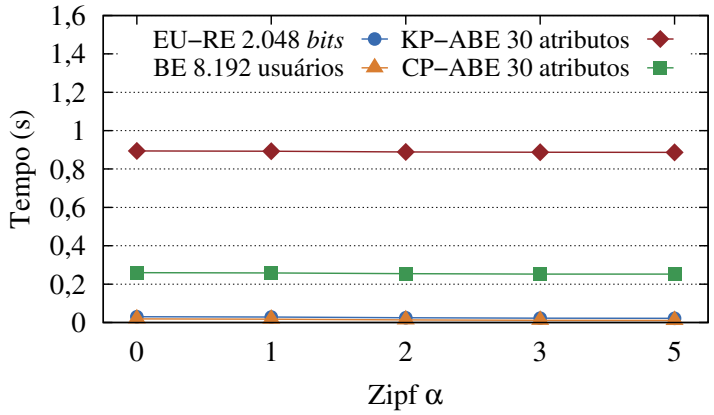

Figura 7.6: Comparação dos esquemas BE, ABE e EU-RE no tempo de recebimento e decifragem de *chunks* de 4KB.

A Figura 7.7 mostra o tempo decorrido desde a requisição do primeiro *chunk* até a decifragem do último *chunk* que compõe o conteúdo, finalizando a decifragem de todo o conteúdo, para os quatro modelos de controle de acesso: BE, KP-ABE, CP-ABE e EU-RE. A simulação com o BE foi realizada com o AES e uma chave de 256 *bits*, e os resultados correspondentes consideram a decifragem dos *chunks* mais a decifragem do EB para a extração da chave secreta, que acontece somente uma vez por conteúdo. Para o KP-ABE e CP-ABE são considerados 30 atributos e para o EU-RE, chaves de 2.048 *bits*.

Entre as soluções, o BE se destaca pelo uso de criptografia simétrica, que é reconhecidamente mais eficiente que os modelos de criptografia assimétrica. As Figuras 7.7(a) e (b) mostram que para decifrar conteúdos de música, o BE leva menos de 1 segundo, mesmo considerando arquivos de áudio de qualidade alta (> 2,4MB) e apenas duas operações paralelas. Para arquivos de vídeo, o BE leva aproximadamente 16 minutos para a decifragem completa de um arquivo de alta definição (3GB) com duas operações paralelas. Comparado aos outros modelos, o BE se apresenta como o mais eficiente, sendo

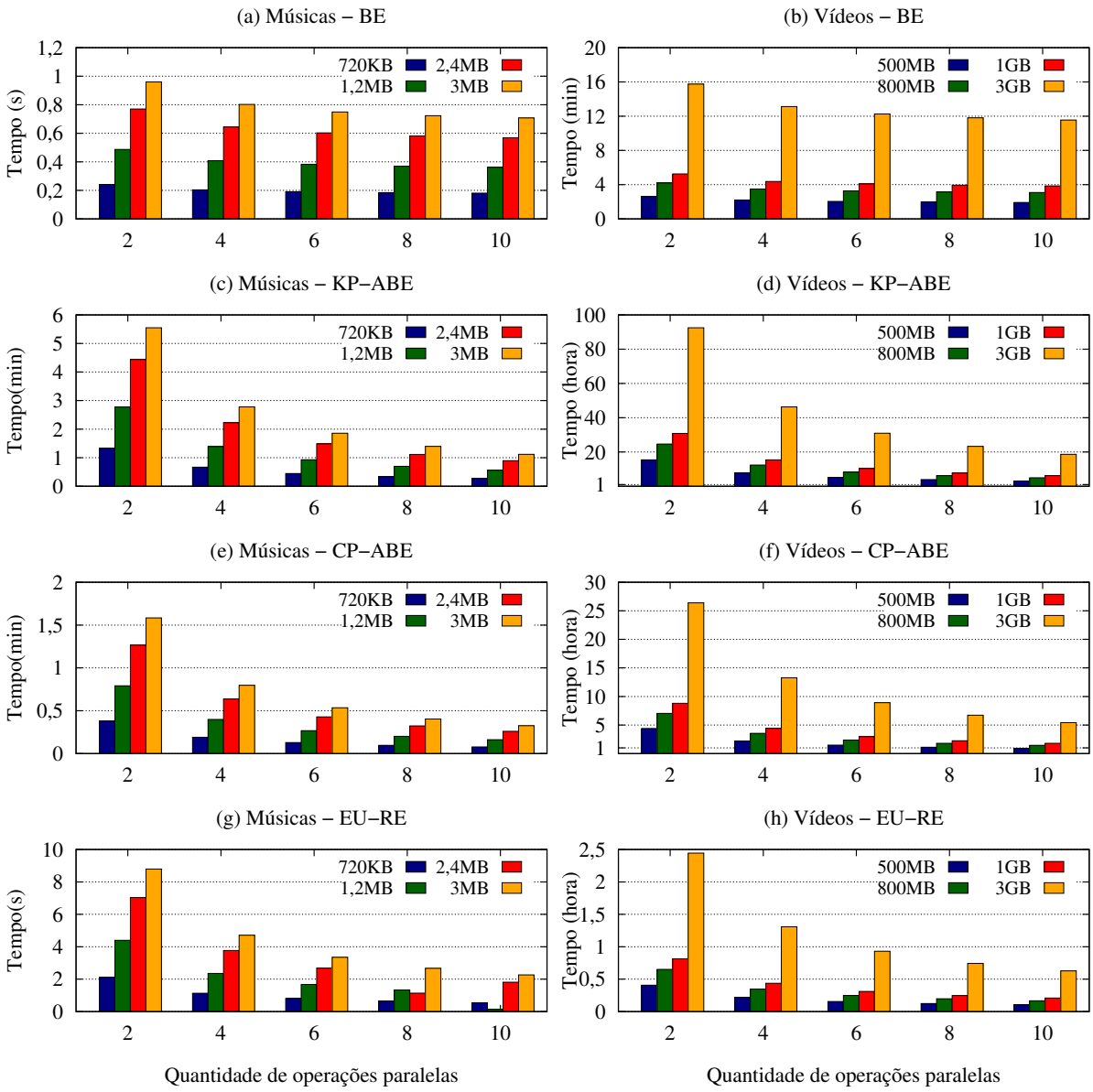

Figura 7.7: Comparação dos esquemas BE, ABE e EU-RE no tempo de recebimento e decifragem de arquivos de música e vídeo.

que aproximadamente 66% do tempo total é para o recebimento do conteúdo e o restante para as operações criptográficas. Contudo, ao considerar a utilização do ABE ou EU-RE para a distribuição de uma chave secreta e a criptografia simétrica para a cifragem do conteúdo, esses modelos também terão desempenho semelhante.

Para o ABE, em ambos os modelos KP-ABE e CP-ABE, o tempo para o recebimento e decifragem dos *chunks* supera o de um minuto para músicas (Figuras 7.7(c) e (e)) e uma hora para vídeos (Figuras 7.7(d) e (f)). O KP-ABE, por exemplo, mesmo considerando dez operações paralelas, não é capaz de decifrar um fluxo de áudio de alta qualidade em um minuto. Para vídeos, a eficiência do KP-ABE é ainda pior, pois nem mesmo com o menor arquivo considerado, 500MB, é possível decifrar em menos de uma hora. O CP-ABE, como já discutido, tem uma maior carga no provedor de conteúdo com a cifragem, pois as políticas estão incorporadas na própria cifra. Portanto, a decifragem é mais eficiente que o KP-ABE, mas ainda assim a decifragem de arquivos de vídeo em

menos de uma hora só é possível a partir de dez operações paralelas, e somente para arquivos com 500MB. Já as músicas podem ser decifradas em menos de um minuto a partir de quatro operações paralelas para arquivos com 2,4MB e 3MB.

O EU-RE não tem o desempenho do BE, mas para uma solução de criptografia assimétrica, se mostra mais eficiente do que o ABE. Além disso, ele vem com a vantagem da não utilização de uma chave secreta única para todos os usuários, o que representa um ganho de segurança para o sistema, em comparação com o BE. O desempenho do EU-RE para a decifragem de arquivos de músicas, como ilustra a Figura 7.7(g), está dentro do esperado para a aplicação. Já para os arquivos de vídeo, com exceção dos fluxos de 3GB com duas e quatro operações paralelas, o desempenho também é adequado para que a experiência do usuário não seja prejudicada, como mostra a Figura 7.7(h).

Discussão

Todos os três esquemas de criptografia avaliados são adequados para o controle de acesso em ICN do ponto de vista da abrangência de um conteúdo em *cache*, embora tenham características que os tornam mais adequados em casos específicos. O modelo de BE, por exemplo, exige pouco do provedor para a cifragem e dos usuários para a decifragem, fazendo com que os provedores de conteúdo possam lidar eficientemente com uma grande quantidade de conteúdo e que os usuários usufruam de um fluxo rápido de conteúdo, mesmo para dispositivos com recursos limitados. Isso se deve ao uso da criptografia simétrica para cifrar os conteúdos, que é rápida para a cifragem e decifragem. No entanto, o uso de chaves secretas para o controle de acesso em ICN pode não garantir a proteção desejada. Por exemplo, se um usuário no grupo de *broadcast* extrai a chave secreta do EB, ele pode facilmente divulgá-la para os usuários não autorizados. Embora qualquer esquema de criptografia permita essa prática, as características da ICN fazem com que a divulgação de uma chave secreta seja atraente, uma vez que usuários não autorizados que a possuem podem recuperar o conteúdo diretamente de *caches* na rede e a utilizar para decifrá-los.

Além do mais, enquanto os conteúdos estiverem armazenados em *cache* e os usuários possuírem a chave secreta, qualquer usuário do grupo de *broadcast* é capaz de decifrar o conteúdo. Mesmo que o provedor de conteúdo descubra que houve o vazamento da chave secreta e recrie o grupo de *broadcast* com novas chaves, essa operação é extremamente cara e pode não resolver o problema caso os roteadores não retirem os conteúdos obsoletos dos seus *caches*. No entanto, para amenizar o problema do tamanho do grupo na computação das chaves dos usuários, o provedor de conteúdo pode optar por criar grupos menores com diferentes EBs, que possuem a mesma chave secreta. Assim, todos os usuários dos grupos de *broadcast* podem recuperar o mesmo conteúdo dos *caches*, usufruindo das vantagens das ICNs.

O ABE, por outro lado, permite que os provedores de conteúdo controlem o acesso de uma forma mais eficaz através dos atributos. Por exemplo, ao incorporar as políticas de acesso diretamente nas chaves ou nos textos cifrados, o provedor garante que mesmo que ele não esteja ativo, somente os usuários que possuem os atributos necessários possam decifrar os conteúdos, mesmo que servidos pelos *caches*. No entanto, quanto mais atributos são incorporados, maior é a carga computacional para a geração de chaves e cifragem. Assim, as soluções de controle de acesso utilizando o ABE muitas vezes sugerem que a quantidade de atributos não seja muito grande. Contudo, cifrar o mesmo conteúdo para diferentes grupos de atributos pode interferir no funcionamento dos *caches*, já que um conteúdo pode não atender a todos os usuários.

Além disso, as soluções de ABE implicam uma maior carga computacional no usuário para a decifragem, quando comparado com o BE e EU-RE; assim, o ABE não é adequado para aplicações de *streaming*, pelo menos na sua proposta original. Além disso, embora os provedores de conteúdo tenham um melhor controle sobre quem pode decifrar cada um dos seus conteúdos, uma vez que um usuário tenha acesso legítimo a uma chave de decifragem refletindo seus atributos, ele pode distribuí-la para usuários não autorizados. Renovar as chaves de decifragem para os usuários pode implicar na necessidade de recifrar todo o catálogo de conteúdos, o que adiciona uma carga extra nos provedores de conteúdo.

A solução proposta neste trabalho, com sua otimização, tem uma menor sobrecarga nos usuários, comparado aos modelos de ABE. Contudo, a solução proposta evita o uso das chaves secretas para o compartilhamento de conteúdos devido à fraca segurança agregada a esse modelo, por isso a sobrecarga é justificável quando comparado ao BE. Para os provedores de conteúdo, o EU-RE tem a tarefa extra de calcular chaves de recifragem sob demanda para cada usuário, além de calcular os pares de chaves pública-privada para cada usuário, que pode ser realizada por uma infraestrutura terceirizada, assim como nas outras soluções. Uma solução de controle de acesso baseada no EU-RE garante o acesso aos conteúdos através da chave de recifragem, que pode ser negada pelo provedor caso o usuário não satisfaça as políticas de acesso. Além disso, um usuário não autorizado não consegue utilizar a chave de recifragem de outro usuário, pois também é necessária a chave privada do usuário original para a decifragem. Desta forma, o EU-RE é mais seguro do que as outras soluções, já que, para um usuário não autorizado ter acesso a um conteúdo protegido, é necessário que ele recupere um conteúdo protegido, a chave de recifragem correspondente ao conteúdo e a chave privada do usuário correspondente à chave de recifragem. Além disso, a proposta do EU-RE faz o melhor uso dos *caches*, pois somente uma cópia do conteúdo é distribuída e serve a todos os usuários, já que o controle de acesso é realizado através da entrega de uma chave de recifragem correspondente para os usuários autorizados.

A revogação de chaves é um problema para todas as soluções discutidas, pois uma vez entregue, as chaves estão no controle dos dispositivos dos usuários. Revogar usuários no BE é difícil, pois é necessário recifrar os conteúdos com uma nova chave, e certificar-se que o usuário revogado não receba a nova chave. No ABE, os provedores de conteúdo podem adicionar marcas de tempo como atributos nas chaves e recifrar e redistribuir o conteúdo com as novas marcas de tempo, assim, os usuários que possuem as marcas de tempo antigas não são mais autorizados a acessar os novos conteúdos. Mesmo assim, ainda pode ser necessário calcular e distribuir novas chaves de decifragem para os usuários autorizados, caso as marcas de tempo das suas chaves não estejam dentro do limite permitido. No esquema EU-RE, a revogação pode ser realizada com a recifragem de todo o catálogo de conteúdo com novos pares de chaves, o que exige que os usuários solicitem novas chaves de recifragem para continuar acessando os conteúdos. Contudo, esse modelo introduz uma grande sobrecarga nos provedores de conteúdo para a cifragem do catálogo periodicamente. Além disso, a revogação de chaves em todas as soluções é prejudicada pelo armazenamento dos conteúdos em *caches*, uma vez que o conteúdo pode ser armazenado por um longo tempo nos *caches* na rede. Por exemplo, os roteadores podem ignorar os tempos de expiração ou políticas de retirada de conteúdos em *caches* caso a sua manutenção no *cache* esteja beneficiando a rede como um todo.

7.3 Considerações finais

Este capítulo apresentou uma otimização para as funções de recifragem e decifragem do esquema de recifragem por *proxy* EU-PRE e a validação da otimização mostrou que houve uma redução nos tempos de recifragem/decifragem de até 96%. O ganho de desempenho com a otimização é fundamental para a aplicação da solução proposta nos dispositivos do usuário. O esquema otimizado foi comparado a outras duas soluções de controle de acesso criptográficas, sendo que (1) a solução proposta apresenta um melhor aproveitamento do *cache*, pois o mesmo conteúdo serve qualquer usuário; (2) oferece uma maior segurança contra a divulgação da chave de acesso, já que é necessário divulgar também a chave privada do usuário; e (3) apresenta menor sobrecarga computacional nos dispositivos dos usuários, comparado à criptografia baseada em atributos. Entretanto, a revogação de acesso ainda é um desafio para as soluções de controle de acesso em geral, principalmente devido ao *cache* na rede.

Capítulo 8

Conclusão

O paradigma das redes centradas em informação visa criar uma Internet alinhada à distribuição de conteúdo, que é responsável pela maior quantidade de tráfego na Internet atualmente. As ICNs propõem uma arquitetura mais natural, nomeando e roteando conteúdos ao invés de endereços de máquina, sendo que os usuários não precisam se conectar a uma máquina específica a fim de acessar um conteúdo. Em vez disso, os usuários solicitam o conteúdo para a rede e a própria rede satisfaz essa requisição com a cópia disponível mais adequada, permitindo que ele possa ser armazenado em *caches* para a melhoria do desempenho da rede em geral. Essas características fazem das ICNs um ambiente ideal para a distribuição de conteúdos multimídia, principalmente os que muitos usuários estão interessados simultaneamente. Nesses cenários, os *caches* na rede aproximam o conteúdo do usuário final, diminuindo a latência da rede na entrega do conteúdo e melhorando a experiência do usuário.

No entanto, do ponto de vista da segurança, o paradigma de ICN apresenta grandes desafios. Em primeiro lugar, o foco da segurança passa a ser o conteúdo em si, que deve carregar consigo informações suficientes para que os usuários possam aferir a integridade e a autenticidade do conteúdo. Além disso, as mudanças consequentes do roteamento de conteúdos nomeados e da implementação de *caches* na rede representam novas ameaças de segurança, como o controle de acesso aos conteúdos. Garantir a execução de políticas de controle de acesso nos conteúdos armazenados em *caches* é um desafio importante, pois muitas aplicações devem controlar quem acessa seus conteúdos. Como os roteadores na rede não tem a obrigação de verificar quais usuários têm acesso aos conteúdos, as cópias em *cache* podem ser acessadas por usuários não autorizados. Esse problema é ainda mais preocupante para aplicações que distribuem conteúdos protegidos, que são acessados mediante pagamentos de assinaturas, por exemplo, e que é o caso da grande maioria de aplicações que distribuem conteúdos multimídia. Neste caso, é ainda mais importante que os provedores de conteúdos possam ter o controle da execução de políticas de acesso dos seus conteúdos, inclusive os que são recuperados dos *caches*.

Neste contexto, este trabalho propôs uma solução para a garantia de controle de acesso aos conteúdos em ICN, com especial atenção aos conteúdos multimídia. Para isso, a solução proposta emprega o esquema criptográfico de recifragem por *proxy*, que permite que o provedor delegue direitos de decifragem dos seus conteúdos para um usuário, mediante o envio de uma chave de recifragem para o usuário. Assim, o provedor de conteúdo cifra o conteúdo com uma chave pública exclusiva, gerando um conteúdo único que pode ser armazenado em *cache* e utilizado para atender às requisições de qualquer usuário. Entretanto, para o usuário decifrar o conteúdo, ele deve requisitar uma chave

de recifragem diretamente para o provedor. Deste modo, o provedor de conteúdo tem a oportunidade de executar as políticas de acesso nos seus conteúdos, mesmo que eles tenham sido recuperados dos *caches*.

A solução proposta foi avaliada através de simulações em três aspectos: rede, provedor e usuário. Os resultados mostraram que a solução proposta não interfere no funcionamento da rede, usufruindo de todo o ganho proporcionado pelos *caches*, e que as funções do provedor de conteúdo, cifragem e geração de chaves de recifragem, não são impeditivos para o uso da solução. Contudo, as funções do usuário, recifragem e decifragem, apresentam um desempenho inferior para a recuperação de conteúdos de alta definição, por exemplo. Por isso, foi proposta uma otimização nas funções de recifragem e decifragem, que resultou em uma diminuição de até 96% no tempo de execução dessas operações e tornou o esquema viável e interessante para o uso, inclusive em dispositivos com menos recursos computacionais. Comparada a outras duas soluções de controle de acesso criptográficas para ICN, a solução proposta tem melhor desempenho, é mais segura e faz o melhor uso dos *caches*.

8.1 Contribuições

As contribuições deste trabalho são as seguintes:

1. Visão geral da área de segurança em ICN e proposta de organização taxonômica dos ataques e contramedidas, em particular o desafio do controle de acesssa, descrita em detalhes no Capítulo 3;

2. Proposta de uma solução de controle de acesso baseada em recifragem por *proxy* para conteúdo multimídia em ICN, apresentada no Capítulo 5;

3. Implementação e aferição do desempenho de um esquema de recifragem por *proxy*, avaliado no Capítulo 6;

4. Análise de desempenho da solução proposta na distribuição e no acesso a conteúdos multimídia, discutida no Capítulo 6;

5. Proposta de otimização do esquema de recifragem por *proxy* e validação da modificação, detalhada no Capítulo 7;

6. Análise comparativa da solução proposta com outras duas soluções de controle de acesso criptográficas para ICN, abordada no Capítulo 7.

As pesquisas realizadas durante este trabalho resultaram nas seguintes publicações:

1. MANNES, Elisa; MAZIERO, Carlos; LASSANCE, Luiz; BORGES, Fábio. *Controle de acesso baseado em reencriptação por proxy em Redes Centradas em Informação*. Anais do XIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg), páginas 2-15, Belo Horizonte, MG, 2014. [Mannes et al., 2014]

2. MANNES, Elisa; MAZIERO, Carlos; LASSANCE, Luiz; BORGES, Fábio. *Optimized Access Control Enforcement over Encrypted Content in Information-Centric Networks*. IEEE Symposium on Computer and Communications (ISCC), páginas 924-929, Larnaca, Chipre, 2015. [Mannes et al., 2015]

3. MANNES, Elisa; MAZIERO, Carlos; LASSANCE, Luiz; BORGES, Fábio. *Assessing the Impact of Cryptographic Access Control Solutions on Multimedia Delivery in Information-Centric Networks.* IEEE/IFIP Network Operations and Management Symposium (NOMS), páginas 427-435, Istambul, Turquia, 2016. [Mannes et al., 2016]

4. MANNES, Elisa; MAZIERO, Carlos. *Naming content on the Network Layer: a security analysis of the Information-Centric Network model.* Computer Networks. Elsevier. *Aguardando resultado.*

8.2 Trabalhos futuros

Para trabalhos futuros foram identificadas as seguintes oportunidades:

- Investigar a reutilização da variável h na decifragem dos *chunks* no dispositivo do usuário, o que pode melhorar ainda mais o desempenho da operação de decifragem;
- Refinar o esquema de revogação de chaves de recifragem, evitando que usuários que não são mais autorizados a acessar o conteúdo continuem utilizando as chaves de recifragem previamente recebidas;
- Estudar o impacto da solução proposta diante da distribuição de um mesmo conteúdo com codificações diferentes, para se adaptar a diferentes condições de tráfego e de recursos computacionais do dispositivo do usuário;
- Explorar modelos de distribuição de chaves criptográficas adequadas a ICN, de forma que provedores e usuários possam aferir a confiança nas chaves criptográficas recebidas da rede.

Referências Bibliográficas

[AbdAllah et al., 2015a] AbdAllah, E., Hassanein, H. e Zulkernine, M. (2015a). A Survey of Security Attacks in Information-Centric Networking. *IEEE Communications Surveys and Tutorials*, 17(3):1–14.

[AbdAllah et al., 2015b] AbdAllah, E., Zulkernine, M. e Hassanein, H. (2015b). Detection and Prevention of Malicious Requests in ICN Routing and Caching. Em *IEEE International Conference on Computer and Information Technology (ICCIT'15)*, páginas 1741–1748.

[Acs et al., 2013] Acs, G., Conti, M., Gasti, P., Ghali, C. e Tsudik, G. (2013). Cache Privacy in Named-Data Networking. Em *33rd International Conference on Distributed Computing Systems (ICDCS'13)*, páginas 41–51.

[Afanasyev et al., 2013] Afanasyev, A., Mahadevan, P., Moiseenko, I., Uzun, E. e Zhang, L. (2013). Interest Flooding Attack and Countermeasures in Named Data Networking. Em *International Conference on Networking (Networking'13)*, páginas 1–9.

[Ahlgren et al., 2012] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D. e Ohlman, B. (2012). A Survey of Information-Centric Networking. *IEEE Communications Magazine*, 50(7):26–36.

[Aiash e Loo, 2015a] Aiash, M. e Loo, J. (2015a). A Formally Verified Access Control Mechanism for Information Centric Networks. Em *International Conference on Security and Cryptography (SECRYPT'15)*, páginas 377–383.

[Aiash e Loo, 2015b] Aiash, M. e Loo, J. (2015b). An Integrated Authentication and Authorization Approach for the Network of Information Architecture. *Journal of Network and Computer Applications*, 50(C):73–79.

[Al-Sheikh et al., 2015] Al-Sheikh, S., Wählisch, M. e Schmidt, T. C. (2015). Revisiting Countermeasures Against NDN Interest Flooding. Em *2nd ACM Conference on Information-Centric Networking (ICN'15)*, páginas 0–3.

[Alzahrani et al., 2013a] Alzahrani, B., Vassilakis, V. e Reed, M. (2013a). Key Management in Information Centric Networking. *International Journal of Computer Networks and Communications*, 5(6):153–166.

[Alzahrani et al., 2013b] Alzahrani, B., Vassilakis, V. e Reed, M. (2013b). Mitigating Brute-force Attacks on Bloom-filter based Forwarding. Em *Conference on Future Internet Communications (CFIC'13)*, páginas 1–7.

[Alzahrani et al., 2013c] Alzahrani, B., Vassilakis, V. e Reed, M. (2013c). Securing the Forwarding plane in Information Centric Networks. Em *5th Computer Science and Electronic Engineering Conference (CEEC'13)*, páginas 174–178.

[Arianfar et al., 2011] Arianfar, S., Koponen, T., Raghavan, B. e Shenker, S. (2011). On Preserving Privacy in Content-oriented Networks. Em *ACM SIGCOMM Workshop on Information-centric Networking (ICN'11)*, páginas 19–24.

[Ateniese et al., 2009] Ateniese, G., Benson, K. e Hohenberger, S. (2009). Key-Private Proxy Re-encryption. Em *The RSA Conference on Topics in Cryptology (CT-RSA'09)*, páginas 279–294.

[Ateniese et al., 2006] Ateniese, G., Fu, K., Green, M. e Hohenberger, S. (2006). Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage. *ACM Transactions on Information System Security*, 9(1):1–30.

[Bari et al., 2012] Bari, M., Chowdhury, S., Ahmed, R., Boutaba, R. e Mathieu, B. (2012). A Survey of Naming and Routing in Information-Centric Networks. *Communications Magazine, IEEE*, 50(12):44–53.

[Baugher et al., 2012] Baugher, M., Davie, B., Narayanan, A. e Oran, D. (2012). Self-verifying Names for Read-only Named Data. Em *IEEE Conference on Computer Communications Workshops (INFOCOM'12)*, páginas 274–279.

[Bethencourt et al., 2007] Bethencourt, J., Sahai, A. e Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. Em *Symposium on Security and Privacy (S & P'07)*, páginas 321–334.

[Blaze et al., 1998] Blaze, M., Bleumer, G. e Strauss, M. (1998). Divertible Protocols and Atomic Proxy Cryptography. Em *International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'98)*, páginas 127–144.

[Boneh et al., 2005] Boneh, D., Gentry, C. e Waters, B. (2005). Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys. Em *International Conference on Advances in Cryptology (CRYPTO'05)*, páginas 258–275.

[Bonomi et al., 2006] Bonomi, F., Mitzenmacher, M., Panigrahy, R., Singh, S. e Varghese, G. (2006). An Improved Construction for Counting Bloom Filters. Em *14th Conference on Annual European Symposium (ESA'06)*, páginas 684–695.

[Borges et al., 2012] Borges, F., Petzoldt, A. e Portugal, R. (2012). Small Private Keys for Systems of Multivariate Quadratic Equations Using Symmetric Cryptography. Em *34th Congresso Nacional de Matemática Aplicada à Computação (CNMAC'12)*, páginas 1085–1091.

[Brito et al., 2012] Brito, G. M. d., Velloso, P. B. e Moraes, I. M. (2012). *Redes Orientadas a Conteúdo: Um Novo Paradigma para a Internet*, capítulo: 5, páginas 211–264. Minicursos do XXX Simpósio Brasileiro de Redes de Computadores de Sistemas Distribuídos.

[Cai e Liu, 2014] Cai, Y. e Liu, X. (2014). A Multi-use CCA-Secure Proxy Re-encryption Scheme. Em *12th International Conference on Dependable, Autonomic and Secure Computing (DASC'14)*, páginas 39–44.

[Canard et al., 2011] Canard, S., Devigne, J. e Laguillaumie, F. (2011). Improving the Security of an Efficient Unidirectional Proxy Re-encryption Scheme. *Journal of Internet Services and Information Security*, 1(2):140–160.

[Canetti e Hohenberger, 2007] Canetti, R. e Hohenberger, S. (2007). Chosen-ciphertext Secure Proxy Re-encryption. Em *14th ACM Conference on Computer and Communications Security (CCS'07)*, páginas 185–194.

[Chaabane et al., 2013] Chaabane, A., De Cristofaro, E., Kaafar, M. A. e Uzun, E. (2013). Privacy in Content-oriented Networking: Threats and Countermeasures. *SIGCOMM Computer Communications Review*, 43(3):25–33.

[Chen et al., 2014] Chen, T., Lei, K. e Xu, K. (2014). An Encryption and Probability based Access Control Model for Named Data Networking. Em *International Performance Computing and Communications Conference (IPCCC'14)*, páginas 1–8.

[Chen e Li, 2011] Chen, X. e Li, Y. (2011). Efficient Proxy Re-encryption with Private Keyword Searching in Untrusted Storage. *International Journal on Computer Network and Information Security*, 3(2):50–56.

[Choi et al., 2013] Choi, S., Kim, K., Kim, S. e hee Roh, B. (2013). Threat of DoS by Interest Flooding Attack in Content-centric Networking. Em *International Conference on Information Networking (ICOIN'13)*, páginas 315–319.

[Chow et al., 2010] Chow, S. S. M., Weng, J., Yang, Y. e Deng, R. H. (2010). Efficient Unidirectional Proxy Re-encryption. Em *3rd International Conference on Cryptology in Africa (AFRICACRYPT'10)*, páginas 316–332.

[Chu et al., 2009] Chu, C.-K., Weng, J., Chow, S. S. M., Zhou, J. e Deng, R. H. (2009). Conditional Proxy Broadcast Re-Encryption. Em *14th Australasian Conference on Information Security and Privacy (ACISP'09)*, páginas 327–342.

[Cieza et al., 2015] Cieza, E. G., Moraes, I. M. e Velloso, P. B. (2015). Uma Análise do Impacto do Ataque de Poluição de Cache em Redes Orientadas a Conteúdo Sem-Fio. Em *Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg'15)*, páginas 1–14.

[Compagno et al., 2015] Compagno, A., Conti, M., Gasti, P., Mancini, L. e Tsudik, G. (2015). Violating Consumer Anonymity: Geo-locating Nodes in Named Data Networking. Em *13th International Conference on Applied Cryptography and Network Security (ACNS'15)*, páginas 1–25.

[Compagno et al., 2013] Compagno, A., Conti, M., Gasti, P. e Tsudik, G. (2013). Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking. *38th IEEE Conference on Local Computer Networks (LCN'13)*, páginas 630–638.

[Consortium, 2014] Consortium (2014). UCLA, Cisco and more join forces to replace TCP/IP. http://www.networkworld.com/article/2602109/lan-wan/ucla-cisco-more-join-forces-to-replace-tcpip.html. Último acesso: 06 de março de 2016.

[Conti et al., 2013] Conti, M., Gasti, P. e Teoli, M. (2013). A Lightweight Mechanism for Detection of Cache Pollution Attacks in Named Data Networking. *Computer Networks*, 57(16):3178–3191.

[Cui et al., 2016] Cui, X., Tsang, Y. H., Hui, L. C. K., Yiu, S. M. e Luo, B. (2016). Defend Against Internet Censorship in Named Data Networking. Em *18th International Conference on Advanced Communication Technology (ICACT'16)*, páginas 300–305.

[Dai et al., 2013] Dai, H., Wang, Y., Fan, J. e Liu, B. (2013). Mitigate DDoS Attacks in NDN by Interest Traceback. Em *2nd IEEE International Workshop on Emerging Design Choices in Name-Oriented Networking (NOMEN'13)*, páginas 381–386.

[D'Ambrosio et al., 2011] D'Ambrosio, M., Dannewitz, C., Karl, H. e Vercellone, V. (2011). MDHT: A Hierarchical Name Resolution Service for Information-centric Networks. Em *SIGCOMM Workshop on Information-centric Networking (ICN'11)*, páginas 7–12.

[Dannewitz et al., 2010] Dannewitz, C., Golić, J., Ohlman, B. e Ahlgren, B. (2010). Secure Naming for a Network of Information. Em *IEEE Conference on Computer Communications Workshops (INFOCOM'10)*, páginas 1–6.

[Dannewitz et al., 2013] Dannewitz, C., Kutscher, D., Ohlman, B., Farrell, S., Ahlgren, B. e Karl, H. (2013). Network of Information (NetInf) - An Information-centric Networking Architecture. *Computer Communications*, 36(7):721–735.

[Deng et al., 2008] Deng, R. H., Weng, J., Liu, S. e Chen, K. (2008). Chosen-Ciphertext Secure Proxy Re-encryption without Pairings. Em *7th International Conference in Cryptology and Network Security (CANS'08)*, páginas 1–17.

[DiBenedetto et al., 2011] DiBenedetto, S., Gasti, P., Tsudik, G. e Uzun, E. (2011). ANDaNA: Anonymous Named Data Networking Application. Em *19th Annual Network and Distributed System Security Symposium (NDSS'12)*, páginas 1–18.

[Ding et al., 2014] Ding, K., Liu, Y., Cho, H.-H., Chao, H.-C. e Shih, T. K. (2014). Cooperative Detection and Protection for Interest Flooding Attacks in Named Data Networking. *International Journal of Communication Systems*, 29(5):1–10.

[Do et al., 2011] Do, J. M., Song, Y. J. e Park, N. (2011). Attribute Based Proxy Re-encryption for Data Confidentiality in Cloud Computing Environments. Em *1st International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI'11)*, páginas 248–251.

[Dong et al., 2008] Dong, C., Russello, G. e Dulay, N. (2008). Shared and Searchable Encrypted Data for Untrusted Servers. Em *22nd Working Conference on Data and Applications Security (DBSEC'08)*, páginas 127–143.

[El Gamal, 1985] El Gamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. Em *Proceedings of Advances in Cryptology (CRYPTO'85)*, páginas 10–18.

[Elechi et al., 2014] Elechi, O. O., Igwe, J. S. e Eze, E. C. (2014). Denial of Service in Internet Protocol Network and Information Centric Network: An Impediment to Network Quality of Service. *Journal of Information Engineering and Applications*, 4:14–24.

[Eugster et al., 2003] Eugster, P. T., Felber, P. A., Guerraoui, R. e Kermarrec, A.-M. (2003). The Many Faces of Publish/Subscribe. *ACM Computing Surveys*, 35(2):114–131.

[Fall, 2003] Fall, K. (2003). A delay-tolerant network architecture for challenged internets. Em *Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'03)*, páginas 27–34.

[Fang et al., 2011] Fang, L., Susilo, W., Ge, C. e Wang, J. (2011). Interactive Conditional Proxy Re-encryption with Fine Grain Policy. *Jornal of System Software*, 84(12):2293–2302.

[Fang et al., 2012] Fang, L., Susilo, W., Ge, C. e Wang, J. (2012). Chosen-ciphertext Secure Anonymous Conditional Proxy Re-encryption with Keyword Search. *Theoretical Computer Science*, 462(1):39–58.

[Farrell et al., 2013] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keränen, A. e Hallam-Baker, P. (2013). Naming Things with Hashes. RFC 6920.

[Fotiou et al., 2010] Fotiou, N., Marias, G. F. e Polyzos, G. C. (2010). Towards a Secure Rendezvous Network for Future Publish/Subscribe Architectures. Em *3rd Future Internet Symposium (FIS'10)*, páginas 49–56.

[Fotiou et al., 2012] Fotiou, N., Marias, G. F. e Polyzos, G. C. (2012). Access control Enforcement Delegation for Information-centric Networking Architectures. Em *2nd ACM SIGCOMM Workshop on Information-centric Networking (ICN'12)*, páginas 85–90.

[Fotiou et al., 2014] Fotiou, N., Trossen, D., Marias, G., Kostopoulos, A. e Polyzos, G. (2014). Enhancing Information Lookup Privacy Through Homomorphic Encryption. *Journal of Security and Communication Networks*, 7(12):2804–2814.

[Gasti et al., 2012] Gasti, P., Tsudik, G., Uzun, E. e Zhang, L. (2012). DoS and DDoS in Named-Data Networking. Em *22nd International Conference on Computer Communications and Networks (ICCCN'13)*, páginas 1–7.

[Ghali et al., 2015a] Ghali, C., Narayanan, A., Oran, D., Tsudik, G. e Wood, C. A. (2015a). Secure Fragmentation for Content-centric Networks. Em *14th International Symposium on Network Computing and Applications (NCA'15)*, páginas 47–56.

[Ghali et al., 2015b] Ghali, C., Schlosberg, M. A., Tsudik, G. e Wood, C. A. (2015b). Interest-Based Access Control for Content Centric Networks. Em *2nd ACM Conference on Information-centric Networking (ICN'15)*, páginas 1–10.

[Ghali et al., 2014a] Ghali, C., Tsudik, G. e Uzun, E. (2014a). Elements of Trust in Named-Data and Content-Centric Networking. *ACM SIGCOMM Computer Communication Review*, 44(5):1–10.

[Ghali et al., 2014b] Ghali, C., Tsudik, G. e Uzun, E. (2014b). Needle in a Haystack: Mitigating Content Poisoning in Named-Data Networking. Em *NDSS Workshop on Security of Emerging Networking Technologies (SENT'14)*, páginas 1–10.

[Ghali et al., 2014c] Ghali, C., Tsudik, G. e Uzun, E. (2014c). Network-Layer Trust in Named-Data Networking. *ACM SIGCOMM Computer Commununication Review*, 44(5):12–19.

[Goergen et al., 2012] Goergen, D., Cholez, T., François, J. e Engel, T. (2012). Security Monitoring for Content-Centric Networking. Em *7th International Workshop on Data Privacy Management (DPM'12)*, páginas 274–286.

[Goldman et al., 2014] Goldman, A. D., Uluagac, A. S. e Copeland, J. A. (2014). Cryptographically-Curated File System (CCFS): Secure, Inter-operable, and Easily Implementable Information-Centric Networking. Em *39th Conference on Local Computer Networks (LCN'14)*, páginas 142–149.

[Golle e Smetters, 2010] Golle, J. T. P. e Smetters, D. (2010). CCNx Access Control Specifications. Technical report, PARC.

[Gouge et al., 2016] Gouge, J., Seetharam, A. e Roy, S. (2016). On the Scalability and Effectiveness of a Cache Pollution based DoS Attack in Information Centric Networks. Em *International Conference on Computing, Networking and Communications (ICNC'16)*, páginas 1–5.

[Guoan et al., 2010] Guoan, Z., Liming, F., Jiandong, W., Chunpeng, G. e Yongjun, R. (2010). Improved Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption. Em *IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS'10)*, páginas 476–480.

[Hamdane e El Fatmi, 2015] Hamdane, B. e El Fatmi, S. (2015). A Credential and Encryption Based Access Control Solution for Named Data Networking. Em *International Symposium on Integrated Network Management (IM'15)*, páginas 1234–1237.

[Hamdane et al., 2014] Hamdane, B., Fatmi, S. G. E. e Serhrouchni, A. (2014). A Novel Name-Based Security Mechanism for Information-Centric Networking. Em *Wireless Communication and Networking Conference (WCNC'14)*, páginas 1–5.

[Hamdane et al., 2013] Hamdane, B., Msahli, M., Serhrouchni, A. e Fatmi, S. G. E. (2013). Data-based Access Control in Named Data Networking. Em *9th International Conference on Collaborative Computing: Networking, Applications and Worksharing (COLABORATECOM'13)*, páginas 531–536.

[Hamdane et al., 2012] Hamdane, B., Serhrouchni, A., Fadlallah, A. e Fatmi, S. E. (2012). Named-Data Security Scheme for Named Data Networking. Em *3rd International Conference on the Network of the Future (NOF'12)*, páginas 1–6.

[He et al., 2011] He, Y. J., Hui, L. C. K. e Yiu, S. M. (2011). Avoid Illegal Encrypted DRM Content Sharing with Non-transferable Re-encryption. Em *13th International Conference on Communication Technology (ICCT'11)*, páginas 703–708.

[Hohenberger et al., 2007] Hohenberger, S., Rothblum, G. N., Shelat, A. e Vaikuntanathan, V. (2007). Securely Obfuscating Re-encryption. Em *4th Conference on Theory of Cryptography (TCC'07)*, páginas 233–252.

[Hyung Kim et al., 2015] Hyung Kim, D., Nam, S., Bi, J. e Yeom, I. (2015). Efficient Content Verification in Named Data Networking. Em *ACM Conference on Information-centric Network (ICN'15)*, páginas 109–116.

[Ibraimi et al., 2008] Ibraimi, L., Tang, Q., Hartel, P. e Jonker, W. (2008). A Type-and-Identity-based Proxy Re-encryption Scheme and its Application in Healthcare. Em *Secure Data Management*, páginas 185–198. Springer.

[Ion et al., 2013] Ion, M., Zhang, J. e Schooler, E. (2013). Toward Content-centric Privacy in ICN: Attribute-based Encryption and Routing. Em *3rd ACM SIGCOMM Workshop on Information-centric networking (ICN'13)*, páginas 39–40.

[Ivan e Dodis, 2003] Ivan, A. e Dodis, Y. (2003). Proxy Cryptography Revisited. Em *Network and Distributed System Security Symposium (NDSS'03)*, páginas 01–20.

[Jacobson et al., 2012] Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M., Briggs, N. e Braynard, R. (2012). Networking Named Content. *Communications of the ACM*, 55(1):117–124.

[Jacobson et al., 2009] Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H. e Braynard, R. L. (2009). Networking Named Content. Em *5th international conference on Emerging networking experiments and technologies (CoNEXT'09)*, páginas 1–12.

[Jakobsson, 1999] Jakobsson, M. (1999). On Quorum Controlled Asymmetric Proxy Re-encryption. Em *2nd International Workshop on Practice and Theory in Public Key Cryptography (PKC'99)*, páginas 112–121.

[Jeong et al., 2010] Jeong, J., Kwon, T. T. e Choi, Y. (2010). Host-oblivious Security for Content-based Nnetworks. Em *5th International Conference on Future Internet Technologies (CFI'10)*, páginas 35–40.

[Jia et al., 2010] Jia, X., Shao, J., Jing, J. e Liu, P. (2010). CCA-Secure Type-based Proxy Re-encryption with Invisible Proxy. Em *10th International Conference on Computer and Information Technology (CIT'10)*, páginas 1299–1305.

[Kangasharju et al., 2002] Kangasharju, J., Roberts, J. e Ross, K. W. (2002). Object Replication Strategies in Content Distribution Networks. *Computer Communications*, 25(4):376–383.

[Karami, 2013] Karami, A. (2013). Data Clustering for Anomaly Detection in Content-Centric Networks. *International Journal of Computer Applications*, 81(7):1–8.

[Karami e Guerrero-Zapata, 2014] Karami, A. e Guerrero-Zapata, M. (2014). A Fuzzy Anomaly Detection System based on Hybrid PSO-K Means Algorithm in Content-centric Networks. *Neurocomputing*, 149(1):1253–1269.

[Karami e Guerrero-Zapata, 2015] Karami, A. e Guerrero-Zapata, M. (2015). A Hybrid Multiobjective RBF-PSO Method for Mitigating DoS Attacks in Named Data Networking. *Neurocomputing*, 151(0):1262–1282.

[Kawai e Takashima, 2013] Kawai, Y. e Takashima, K. (2013). Fully-Anonymous Functional Proxy-Re-Encryption. *IACR Cryptology ePrint Archive*, 2013:1–73.

[Khan et al., 2014] Khan, A. N., Kiah, M. L., Madani, S. A., Ali, M., Khan, A. U. e Shamshirband, S. (2014). Incremental Proxy Re-encryption Scheme for Mobile Cloud Computing Environment. *Journal of Supercomputing*, 68(2):624–651.

[Khan et al., 2013] Khan, S. U., Cholez, T., Engel, T. e Lavagno, L. (2013). A Key Management Scheme for Content Centric Networking. Em *International Symposium on Integrated Network Management (IM'13)*, páginas 828–831.

[Khurana et al., 2006] Khurana, H., Heo, J. e Pant, M. (2006). From Proxy Encryption Primitives to a Deployable Secure-Mailing-List Solution. Em *8th International Conference on Information and Communications Security (ICICS'06)*, páginas 260–281.

[Kissel e Wang, 2013] Kissel, Z. e Wang, J. (2013). Access Control for Untrusted Content Distribution Clouds Using Unidirectional Re-encryption. Em *International Conference on High Performance Computing and Simulation (HPCS'13)*, páginas 49–56.

[Koponen et al., 2007] Koponen, T., Chawla, M., Chun, B.-G., Ermolinskiy, A., Kim, K. H., Shenker, S. e Stoica, I. (2007). A Data-oriented (and beyond) Network Architecture. *SIGCOMM Computer Communications Review*, 37(4):181–192.

[Kurihara et al., 2015] Kurihara, J., Wood, C. e Uzun, E. (2015). An Encryption-Based Access Control Framework for Content-Centric Networking. Em *IFIP Networking (Networking'15)*, páginas 1–9.

[Kutscher et al., 2016] Kutscher, D., Pentikousis, K., Psaras, I., Corujo, D., Saucez, D., Schmidt, T. e Waehlisch, M. (2016). ICN Research Challenges. https://tools.ietf.org/pdf/draft-irtf-icnrg-challenges-06.pdf. Último acesso: 12 de abril de 2016.

[Lauinger, 2010] Lauinger, T. (2010). Security and Scalability of Content-Centric Networking. Dissertação de Mestrado, Eurecom, Sophia-Antipolis, França e Technische Universität Darmstadt, Alemanha.

[Lauinger et al., 2011] Lauinger, T., Strufe, T., Laoutaris, N., Biersack, E., Rodriguez, P. e Kirda, E. (2011). Privacy Implications of Ubiquitous Caching in Named Data Networking Architectures. Relatório técnico, Technische Universität Darmstadt. TR-iSecLab-0812-001.

[Lewko et al., 2010] Lewko, A., Sahai, A. e Waters, B. (2010). Revocation Systems with Very Small Private Keys. Em *Symposium on Security and Privacy (S & P'10)*, páginas 273–285.

[Li et al., 2014] Li, B., Verleker, A. P., Huang, D., Wang, Z. e Zhu, Y. (2014). Attribute-based Access Control for ICN Naming Scheme. Em *IEEE Conference on Communications and Network Security (CNS'14)*, páginas 391–399.

[Li et al., 2015] Li, Q., Sandhu, R., Zhang, X. e Xu, M. (2015). Mandatory Content Access Control for Privacy Protection in Information Centric Networks. *IEEE Transactions on Dependable and Secure Computing*, 1(99):1–13.

[Liang et al., 2013a] Liang, K., Fang, L., Susilo, W. e Wong, D. S. (2013a). A Ciphertext-Policy Attribute-Based Proxy Re-encryption with Chosen-Ciphertext Security. Em *5th International Conference on Intelligent Networking and Collaborative Systems (INCoS'13)*, páginas 552–559.

[Liang et al., 2013b] Liang, K., Huang, Q., Schlegel, R., Wong, D. S. e Tang, C. (2013b). A Conditional Proxy Broadcast Re-encryption Scheme Supporting Timed-Release. Em *9th Information Security Practice and Experience (ISPEC'13)*, páginas 132–146.

[Libert e Vergnaud, 2011] Libert, B. e Vergnaud, D. (2011). Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption. *IEEE Transactions on Information Theory*, 57(3):1786–1802.

[Liu et al., 2012] Liu, Q., Wang, G. e Wu, J. (2012). Clock-Based Proxy Re-encryption Scheme in Unreliable Clouds. Em *41st International Conference on Parallel Processing Workshops (ICPPW'12)*, páginas 304–305.

[Liu et al., 2014] Liu, Q., Wang, G. e Wu, J. (2014). Time-based Proxy Re-encryption Scheme for Secure Data Sharing in a Cloud Environment. *Information Science*, 258:355–370.

[Loo e Aiash, 2015] Loo, J. e Aiash, M. (2015). Challenges and Solutions for Secure Information Centric Networks: A Case Study of the NetInf Architecture. *Journal of Network and Computer Applications*, 50(0):64–72.

[Lu et al., 2013] Lu, Y., Wang, Z., Yu, Y.-T., Fan, R. e Gerla, M. (2013). Social Network Based Security Scheme in Mobile Information-Centric Network. Em *12th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net'13)*, páginas 1–7.

[Ma e Ao, 2009a] Ma, C. e Ao, J. (2009a). Group-Based Proxy Re-encryption Scheme. Em *5th International Conference on Intelligent Computing (ICIC'09)*, páginas 1025–1034.

[Ma e Ao, 2009b] Ma, C. e Ao, J. (2009b). Group-based Proxy Re-encryption Scheme Secure Against Chosen Ciphertext Attack. *International Journal on Network Security*, 8(3):266–270.

[Ma et al., 2011] Ma, G., Pei, Q., Wang, Y. e Jiang, X. (2011). A General Sharing Model Based on Proxy Re-encryption. Em *7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'11)*, páginas 248–251.

[Mahadevan et al., 2014] Mahadevan, P., Uzun, E., Sevilla, S. e Garcia-Luna-Aceves, J. (2014). CCN-KRS: A Key Resolution Service for CCN. Em *1st International Conference on Information-centric Networking (ICN'14)*, páginas 97–106.

[Mangili et al., 2015] Mangili, M., Martignon, F. e Paraboschi, S. (2015). A Cache-aware Mechanism to Enforce Confidentiality, Trackability and Access Policy Evolution in Content-Centric Networks. *Computer Networks*, 76(0):126–145.

[Mannes et al., 2014] Mannes, E., Maziero, C., Lassance, L. C. e Borges, F. (2014). Controle de Acesso Baseado em Reencriptação por Proxy em Redes Centradas em Informação. Em *XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg'14)*, páginas 2–15.

[Mannes et al., 2015] Mannes, E., Maziero, C., Lassance, L. C. e Borges, F. (2015). Optimized Access Control Enforcement over Encrypted Content in Information-centric Networks. Em *20th IEEE Symposium on Computers and Communications (ISCC'15)*, páginas 924–929.

[Mannes et al., 2016] Mannes, E., Maziero, C., Lassance, L. C. e Borges, F. (2016). Assessing the Impact of Cryptographic Access Control Solutions on Multimedia Delivery in Information-centric Networks. Em *15th IEEE/IFIP Network Operations and Management Symposium (NOMS'16)*, páginas 1–6.

[Massawe et al., 2013] Massawe, E. A., Du, S. e Zhu, H. (2013). A Scalable and Privacy-Preserving Named Data Networking Architecture Based on Bloom Filters. Em *33rd International Conference on Distributed Computing Systems Workshops (ICDCSW'13)*, páginas 22–26.

[Mastorakis et al., 2015] Mastorakis, S., Afanasyev, A., Moiseenko, I. e Zhang, L. (2015). ndnSIM 2.0: A new version of the NDN simulator for NS-3. Technical Report NDN-0028, NDN.

[Matsuo, 2007] Matsuo, T. (2007). Proxy Re-encryption Systems for Identity-Based Encryption. Em *1st International Conference Pairing-Based Cryptography (ICPBC'07)*, páginas 247–267.

[Mauri e Verticale, 2013] Mauri, G. e Verticale, G. (2013). Distributing Key Revocation Status in Named Data Networking. Em *19th Conference on Information and Communications Technologies (EUNICE'13)*, páginas 310–313.

[Mauri e Verticale, 2014] Mauri, G. e Verticale, G. (2014). On the Tradeoff between Performance and User Privacy in Information Centric Networking. Em *6th International Conference on New Technologies, Mobility and Security (NTMS'14)*, páginas 1–5.

[Misra et al., 2013] Misra, S., Tourani, R. e Majd, N. E. (2013). Secure Content Delivery in Information-centric Networks: Design, Implementation, and Analyses. Em *3rd ACM SIGCOMM Workshop on Information-centric networking (ICN'13)*, páginas 73–78.

[Mohaisen et al., 2015] Mohaisen, A., Mekky, H., Zhang, X., Xie, H. e Kim, Y. (2015). Timing Attacks on Access Privacy in Information Centric Networks and Countermeasures. *IEEE Transactions on Dependable and Secure Computing*, 12(6):675–687.

[Mohaisen et al., 2012] Mohaisen, A., Zhang, X., Schuchard, M., Xie, H. e Kim, Y. (2012). Protecting Access Privacy of Cached Contents in Information Centric Networks. Em *ACM Conference on Computer and Communications Security (CCS'12)*, páginas 1001–1003.

[Nguyen et al., 2015] Nguyen, T., Cogranne, R., Doyen, G. e Retraint, F. (2015). Detection of Interest Flooding Attacks in Named Data Networking using Hypothesis Testing. Em *International Workshop on Information Forensics and Security (WIFS'15)*, páginas 1–6.

[Ntuli e Han, 2012] Ntuli, N. e Han, S. (2012). Detecting Router Cache Snooping in Named Data Networking. Em *International Conference on ICT Convergence (ICTC'12)*, páginas 714–718.

[Papanis et al., 2013] Papanis, J. P., Papapanagiotou, S. I., Mousas, A. S., Lioudakis, G. V., Kaklamani, D. I. e Venieris, I. S. (2013). On the Use of Attribute-Based Encryption for Multimedia Content Protection over Information-Centric Networks. *Transactions on Emerging Telecommunications Technologies*, 25(4):422–435.

[Paverd et al., 2014] Paverd, A., Martin, A. e Brown, I. (2014). Modelling and Automatically Analysing Privacy Properties for Honest-but-Curious Adversaries. Technical report, University of Oxford.

[Perino e Varvello, 2011] Perino, D. e Varvello, M. (2011). A Reality Check for Content Centric Networking. Em *ACM SIGCOMM Workshop on Information-centric Networking (ICN '11)*, páginas 44–49.

[Pires e Moraes, 2015] Pires, A. L. N. e Moraes, I. M. (2015). Uma Avaliação do Ataque de Negação de Serviço em Conluio Consumidor-Produtor em Redes Orientadas a Conteúdo. Em *XXXIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC'15)*, páginas 1–14.

[Posch et al., 2013] Posch, D., Hellwagner, H. e Schartner, P. (2013). On-demand Video Streaming based on Dynamic Adaptive Encrypted Content Chunks. Em *IEEE International Conference on Network Protocols (ICNP'13)*, páginas 1–6.

[Qiu et al., 2015] Qiu, J., Jo, J. e Lee, H. (2015). Collusion-Resistant Identity-Based Proxy Re-Encryption Without Random Oracles. *International Journal of Security and Its Applications*, 9(9):337–344.

[Renault et al., 2009] Renault, E., Ahmad, A. e Abid, M. (2009). Toward a Security Model for the Future Network of Information. Em *4th International Conference on Ubiquitous Information Technologies Applications (ICUT'09)*, páginas 1–6.

[Ribeiro et al., 2014] Ribeiro, I., Rocha, A., Albuquerque, C. e Guimarães, F. (2014). On the Possibility of Mitigating Content Pollution in Content-Centric Networking. Em *39th Conference on Local Computer Networks (LCN'14)*, páginas 498–501.

[Ribeiro et al., 2012] Ribeiro, I. C. G., Guimarães, F. Q., Kazienko, J., Rocha, A., Velloso, P., Moraes, I. e de Albuquerque, C. V. N. (2012). *Segurança em Redes Centradas em Conteúdo: Vulnerabilidades, Ataques e Contramedidas*, capítulo: 3, páginas 101–150. Minicursos do XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais.

[Rivest et al., 1978] Rivest, R. L., Shamir, A. e Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of ACM*, 21(2):120–126.

[Salsano et al., 2012] Salsano, S., Detti, A., Cancellieri, M., Pomposini, M. e Blefari-Melazzi, N. (2012). Transport-layer Issues in Information Centric Networks. Em *2nd ACM SIGCOMM Workshop on Information-centric Networking (ICN'12)*, páginas 19–24.

[Sandvine, 2015] Sandvine (2015). Global Internet Phenomena Report: 1H 2015. https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/global-internet-phenomena-report-latin-america-and-north-america.pdf. Último acesso: 17 de abril de 2016.

[Schnorr, 1991] Schnorr, C. P. (1991). Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, 4(3):161–174.

[Schollmeier, 2001] Schollmeier, R. (2001). A Definition of peer-to-peer Networking for the Classification of peer-to-peer Architectures and Applications. Em *1st International Conference on Peer-to-Peer Computing (P2P'01)*, páginas 101–102.

[Seo et al., 2013] Seo, J. W., Yum, D. H. e Lee, P. J. (2013). Proxy-invisible CCA-secure Type-based Proxy Re-encryption Without Random Oracles. *Theoretical Computer Science*, 491(0):83 –93.

[Seo et al., 2014] Seo, S. C., Kim, T. e Jang, M. (2014). A Privacy-preserving Approach in Content Centric Network. Em *11th Consumer Communications and Networking Conference (CCNC'14)*, páginas 866–871.

[Shao et al., 2011] Shao, J., Liu, P., Cao, Z. e Wei, G. (2011). Multi-Use Unidirectional Proxy Re-Encryption. Em *IEEE International Conference on Communications (ICC'11)*, páginas 1–5.

[Shao et al., 2012] Shao, J., Liu, P., Wei, G. e Ling, Y. (2012). Anonymous Proxy Re-encryption. *Security and Communication Networks*, 5(5):439–449.

[Shilton et al., 2014] Shilton, K., Burke, J., Claffy, K., Duan, C. e Zhang, L. (2014). A World on NDN: Affordances and Implications of the Named Data Networking Future Internet Architecture. Technical Report NDN-0018, University of California, Los Angeles.

[Singh et al., 2013] Singh, K., Pandu Rangan, C. e Banerjee, A. (2013). Lattice based Identity Based Proxy Re-encryption Scheme. *Journal of Internet Services and Information Security*, 3(3/4):38–51.

[Singh et al., 2012] Singh, S., Puri, A., Singh, S. S., Vaish, A. e Venkatesan, S. (2012). A Trust Based Approach For Secure Access Control In Information Centric Network. *International Journal of Information and Network Security*, 1(2):97–104.

[Smetters e Jacobson, 2009] Smetters, D. e Jacobson, V. (2009). Securing network content. Relatório Técnico TR-2009-1, PARC.

[Spring et al., 2004] Spring, N., Mahajan, R., Wetherall, D. e Anderson, T. (2004). Measuring ISP Topologies with Rocketfuel. *IEEE/ACM Transactions on Networking*, 12(1):2–16.

[Taban et al., 2006] Taban, G., Cárdenas, A. A. e Gligor, V. D. (2006). Towards a Secure and Interoperable DRM Architecture. Em *ACM Workshop on Digital Rights Management (DRM'06)*, páginas 69–78.

[Tan et al., 2014] Tan, X., Zhou, Z., Zou, C., Niu, Y. e Chen, X. (2014). Copyright Protection in Named Data Networking. Em *6th Intel Conference on Wireless Communications and Signal Processing (WCSP'14)*, páginas 1–6.

[Tang, 2008] Tang, Q. (2008). Type-Based Proxy Re-encryption and Its Construction. Em *9th International Conference on Cryptology in India (INDOCRYPT'08)*, páginas 130–144.

[Tian et al., 2013] Tian, X., Wang, X. e Zhou, A. (2013). DSP Re-encryption Based Access Control Enforcement Management Mechanism in DaaS. *International Journal of Network Security*, 15(1):28–41.

[Toh, 2001] Toh, C. (2001). *Ad Hoc Wireless Networks: Protocols and Systems*. Prentice Hall, 1st edition.

[Tourani et al., 2015] Tourani, R., Misra, S., Kliewer, J., Ortegel, S. e Mick, T. (2015). Catch Me If You Can: A Practical Framework to Evade Censorship in Information-Centric Networks. Em *2nd ACM Conference on Information-Centric Networking (ICN'15)*, páginas 1–10.

[Trossen e Parisis, 2012] Trossen, D. e Parisis, G. (2012). Designing and Realizing an Information-centric Internet. *IEEE Communications Magazine*, 50(7):60–67.

[Tsudik et al., 2014] Tsudik, G., Uzun, E. e Wood, C. A. (2014). AC3N: An API and Service for Anonymous Communication in Content-Centric Networking. Em *Consumer Communications and Networking Conference (CCNC'14)*, páginas 858–865.

[Tysowski e Hasan, 2013] Tysowski, P. K. e Hasan, M. A. (2013). Hybrid Attribute-based Encryption and Re-encryption for Scalable Mobile Applications in Clouds. *Centre for Applied Cryptographic Research (CACR), University of Waterloo, Tech. Rep*, 13.

[Vieira e Poll, 2013] Vieira, B. e Poll, E. (2013). A Security Protocol for Information-Centric Networking in Smart Grids. Em *Smart Energy Grid Security Workshop (SEGS'13)*, páginas 1–10.

[Virgilio et al., 2013] Virgilio, M., Marchetto, G. e Sisto, R. (2013). PIT Overload Analysis in Content Centric Networks. Em *3rd ACM SIGCOMM Workshop on Information-centric Networking (ICN'13)*, páginas 67–72.

[Vivek et al., 2011] Vivek, S. S., Sharmila Deva Selvi, S., Radhakishan, V. e Pandu Rangan, C. (2011). Conditional Proxy Re-Encryption - A More Efficient Construction. Em *4th International Conference on Advances in Network Security and Applications (NSA'11)*, páginas 502–512.

[Wählisch et al., 2013a] Wählisch, M., Schmidt, T. C. e Vahlenkamp, M. (2013a). Backscatter from the Data Plane – Threats to Stability and Security in Information-Centric Network Infrastructure. *Computer Networks*, 57(16):3192–3206.

[Wählisch et al., 2013b] Wählisch, M., Schmidt, T. C. e Vahlenkamp, M. (2013b). Lessons from the Past: Why Data-driven States Harm Future Information-Centric Networking. Em *International Conference on Networking (Networking'13)*, páginas 1–9.

[Wang e Cao, 2009] Wang, H. e Cao, Z. (2009). A Fully Secure Unidirectional and Multi-use Proxy Re-encryption Scheme. Em *16th Conference on Computer and Communications Security (CCS'09)*, páginas 1–3.

[Wang et al., 2012] Wang, K., Chen, J., Zhou, H. e Qin, Y. (2012). Content-Centric Networking: Effect of Content Caching on Mitigating DoS Attack. *International Journal of Computer Science Issues*, 9(6):43–52.

[Wang et al., 2013] Wang, K., Chen, J., Zhou, H., Qin, Y. e Zhang, H. (2013). Modeling Denial-of-service Against Pending Interest Table in Named Data Networking. *International Journal of Communication Systems*, 26:1–14.

[Wang et al., 2014a] Wang, K., Zhou, H., Qin, Y. e Zhang, H. (2014a). Cooperative-Filter: Countering Interest Flooding Attacks in Named Data Networking. *Software Computing*, 18(9):1803–1813.

[Wang e Yang, 2009] Wang, X. e Yang, X. (2009). Identity-based Broadcast Encryption based on One to Many Identity based Proxy Re-encryption. Em *2nd International Conference on Computer Science and Information Technology (ICCSIT'09)*, páginas 47–50.

[Wang et al., 2014b] Wang, Y., Xu, M., Feng, Z., Li, Q. e Li, Q. (2014b). Session-based Access Control in Information-centric Networks: Design and Analyses. Em *International Performance Computing and Communications Conference (IPCCC'14)*, páginas 1–8.

[Weng et al., 2009a] Weng, J., Deng, R. H., Ding, X., Chu, C.-K. e Lai, J. (2009a). Conditional Proxy Re-encryption Secure Against Chosen-ciphertext Attack. Em *4th International Symposium on Information, Computer, and Communications Security (ASIACCS'09)*, páginas 322–332.

[Weng et al., 2009b] Weng, J., Yang, Y., Tang, Q., Deng, R. H. e Bao, F. (2009b). Efficient Conditional Proxy Re-encryption with Chosen-Ciphertext Security. Em *12th International Conference on Information Security (ISC'09)*, páginas 151–166.

[Wong e Magalhães, 2012] Wong, W. e Magalhães, M. F. (2012). Security Approaches for Information-Centric Networking. Em *Applied Cryptography and Network Security*, capítulo: 5, páginas 76–98. InTech.

[Wong e Nikander, 2010] Wong, W. e Nikander, P. (2010). Secure Naming in Information-centric Networks. Em *Re-Architecting the Internet Workshop (ReARCH'10)*, páginas 1–6.

[Wood e Uzun, 2014] Wood, C. e Uzun, E. (2014). Flexible End-to-End Content Security in CCN. Em *Consumer Communications and Networking Conference (CCNC'14)*, páginas 1–8.

[Xie et al., 2012] Xie, M., Widjaja, I. e Wang, H. (2012). Enhancing Cache Robustness for Content-centric Networking. Em *International Conference on Computer Communications (INFOCOM'12)*, páginas 2426–2434.

[Xiong et al., 2012] Xiong, H., Zhang, X., Zhu, W. e Yao, D. (2012). CloudSeal: End-to-End Content Protection in Cloud-Based Storage and Delivery Services. 96:491–500.

[Xu et al., 2012] Xu, L., Wu, X. e Zhang, X. (2012). CL-PRE: A Certificateless Proxy Re-encryption Scheme for Secure Data Sharing with Public Cloud. Em *7th ACM Symposium on Information, Computer and Communications Security (ASIACCS'12)*, páginas 87–88.

[Xu et al., 2015] Xu, Z., Chen, B., Wang, N., Zhang, Y. e Li, Z. (2015). ELDA: Towards Efficient and Lightweight Detection of Cache Pollution Attacks in NDN. Em *IEEE Conference on Local Computer Networks (LCN'15)*, páginas 1–9.

[Yang et al., 2011] Yang, Y., Gu, L. e Bao, F. (2011). Addressing Leakage of Re-encryption Key in Proxy Re-encryption Using Trusted Computing. Em *2nd International Conference on Trusted Systems (InTrust'11)*, páginas 189–199.

[Yau et al., 2011] Yau, W.-C., Heng, S.-H. e Goi, B.-M. (2011). Proxy Re-encryption with Keyword Search: New Definitions and Algorithms with Proofs. *International Journal of Security and Its Applications*, 5(2):75–90.

[Yu et al., 2010] Yu, S., Wang, C., Ren, K. e Lou, W. (2010). Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. Em *29th IEEE Conference on Computer Communications (INFOCOM'10)*, páginas 1–9.

[Yu et al., 2015] Yu, Y., Afanasyev, A. e Zhang, L. (2015). Name-Based Access Control. Relatório Técnico TR NDN-0034, University of California, Los Angeles, Los Angeles.

[Zhang et al., 2014] Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Claffy, K., Crowley, P., Papadopoulos, C., Wang, L. e Zhang, B. (2014). Named Data Networking. *ACM SIGCOMM Computer Communication Review*, 44(3):66–73.

[Zhang e Chen, 2012] Zhang, R. e Chen, P. (2012). A Dynamic Cryptographic Access Control Scheme in Cloud Storage Services. Em *8th International Conference on Computing and Networking Technology (ICCNT'12)*, páginas 50–55.

[Zhang et al., 2011] Zhang, X., Chang, K., Xiong, H., Wen, Y., Shi, G. e Wang, G. (2011). Towards Name-based Trust and Security for Content-centric Network. Em *19th International Conference on Network Protocols (ICNP'11)*, páginas 1–6.

[Zhao et al., 2010] Zhao, J., Feng, D. e Zhang, Z. (2010). Attribute-Based Conditional Proxy Re-Encryption with Chosen-Ciphertext Security. Em *Global Telecommunications Conference (GLOBECOM'10)*, páginas 1–6.

[Zheng et al., 2015] Zheng, Q., Wang, G., Ravindran, R. e Azgin, A. (2015). Achieving Secure and Scalable Data Access Control in Information-centric Networking. Em *International Conference on Communications (ICC'15)*, páginas 5367–5373.

[Zheng et al., 2014] Zheng, Q., Zhu, W., Zhu, J. e Zhang, X. (2014). Improved Anonymous Proxy Re-encryption with CCA Security. Em *9th ACM Symposium on Information, Computer and Communications Security (CCS'14)*, páginas 249–258.

[Zhou et al., 2005] Zhou, L., Marsh, M. A., Schneider, F. B. e Redz, A. (2005). Distributed Blinding for Distributed ElGamal Re-Encryption. Em *25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, páginas 824–824.

[Zhu et al., 2010] Zhu, J., Zhang, F. e Song, X. (2010). A New Certificateless Proxy Re-encryption Scheme. Em *International Conference on Web Information Systems and Mining (WISM'10)*, páginas 53–58.

[Zhu et al., 2011] Zhu, Z., Burke, J., Zhang, L., Gasti, P., Lu, Y. e Jacobson, V. (2011). A New Approach to Securing Audio Conference Tools. Em *7th Asian Internet Engineering Conference (AINTEC'11)*, páginas 120–123.