Aqui Todos Podem Publicar: Uma Abordagem Escalável para Controle de Acesso Muitos para Muitos em Redes Centradas em Informação

Rafael Hansen da Silva, Weverton Luis da Costa Cordeiro, Luciano Paschoal Gaspary

[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brasil

Resumo. *Um dos principais desafios em Redes Centradas em Informação (ICN) é como prover controle de acesso à publicação e recuperação de conteúdos. Apesar das potencialidades, as soluções existentes geralmente consideram um único usuário agindo como publicador. Ao lidar com múltiplos publicadores, elas podem levar a uma explosão combinatória de chaves criptográficas. As soluções projetadas visando aos múltiplos publicadores, porém, dependem de arquiteturas de rede específicas e/ou de mudanças na mesma para operar. Neste artigo é proposta uma solução, apoiada em criptografia baseada em atributos, para controle de acesso a conteúdos. Nessa solução, o modelo de segurança é voltado a grupos de compartilhamento seguro, nos quais todos os usuários membros podem publicar e consumir conteúdos. Diferente de trabalhos anteriores, a solução proposta mantém o número de chaves proporcional ao de membros nos grupos e pode ser empregada em qualquer arquitetura ICN de forma gradual. A proposta é avaliada quanto ao custo de operação, à quantidade de chaves necessárias, e à eficiência na disseminação de conteúdos. Em comparação às soluções existentes, ela oferece maior flexibilidade no controle de acesso, sem aumentar a complexidade do gerenciamento de chaves e sem causar sobrecustos significativos à rede.*

Abstract. *One of the main challenges in Information Centric Networks (ICN) is providing access control to content publication and retrieval. In spite of the potentialities, existing solutions often consider a single user acting as publisher. When dealing with multiple publishers, they may lead to a combinatorial explosion of cryptographic keys. Those solutions that focus on multiple publishers, on the other hand, rely on specific network architectures and/or changes to operate. In this paper we propose a solution, supported by attribute-based encryption, for content access control. In this solution, the security model is focused on secure content distribution groups, in which any member user can publish to and retrieve from. Unlike previous work, the proposed solution keeps the number of cryptographic keys proportional to the number of group members, and may even be adopted gradually in any ICN architecture. The proposed solution is evaluated with respect to the overhead it imposes, number of required keys, and efficiency of content dissemination. In contrast to existing solutions, it offers higher access control flexibility, without increasing key management process complexity or causing significant network overhead.*

1. Introdução

O paradigma de Redes Centradas em Informação (*Information Centric Networks, ICN*) emergiu como uma direção promissora para a Internet do Futuro [Xylomenos et al. 2014].

Apesar de suas potencialidades – por exemplo, de tornar a distribuição de conteúdos escalável e eficiente, e diminuir o tráfego no núcleo da Internet [Ahlgren et al. 2012], há, ainda, diversos desafios que precisam ser abordados. Um dos mais importantes, e decisivo para o sucesso desse paradigma, está relacionado ao controle de acesso [de Brito et al. 2012, Xylomenos et al. 2014]. Uma vez que os conteúdos passam a ser recuperados a partir de *caches* distribuídas na rede, os mecanismos de segurança precisam garantir que conteúdos publicados de forma protegida (isto é, com restrições de acesso) sejam consumidos apenas por usuários devidamente autorizados.

As soluções existentes geralmente focam em cenários em que grupos de compartilhamento seguro de conteúdo são formados por um publicador e vários consumidores [Misra et al. 2013, Papanis et al. 2014], sendo interessantes para uso por provedores como YouTube, Google Play, iTunes Store e NetFlix. No entanto, elas podem levar a um problema de explosão combinatória de chaves criptográficas, caso adotadas em cenários em que grupos formados por múltiplos publicadores e consumidores são a norma. As soluções focadas em múltiplos publicadores, no entanto, introduzem entidades extras na rede para realizar reencriptação de conteúdos e/ou controle de acesso [Fotiou et al. 2012, Singh et al. 2012]. Embora efetivas, elas são intrusivas e pouco flexíveis para adoção de forma gradual, além de serem vulneráveis ao comportamento malicioso dessas entidades e, em alguns casos, dependentes de arquitetura.

Para lidar com esses problemas, neste artigo, propõe-se um modelo de segurança, apoiado por criptografia baseada em atributos, para controle de acesso a conteúdos em ICN. O modelo utiliza o conceito de participação em grupos de compartilhamento seguro, nos quais apenas usuários membros podem recuperar conteúdos. A publicação pode ser refinada pelo uso de atributos de usuários, de modo a restringir a recuperação a subconjuntos específicos de membros. O modelo proposto concilia suporte a múltiplos publicadores e controle de acesso agnóstico de arquitetura, assim, mantendo o número de chaves proporcional ao de membros nos grupos, e sem depender de entidades centrais. O modelo proposto é avaliado quanto ao suporte a múltiplos publicadores e ao custo de operação. Os resultados alcançados, por meio de avaliações em ambiente experimental controlado, confirmam a efetividade do modelo, o qual introduz um custo marginal para a publicação e a recuperação de conteúdos (em comparação às soluções existentes), ao passo que torna mais robusto e escalável o controle de acesso.

O restante do artigo está organizado como segue. A Seção 2 discute os principais trabalhos relacionados. A Seção 3 descreve em detalhes a solução proposta para controle de acesso a conteúdos em ICN, enquanto que a Seção 4 discute o ambiente experimental utilizado para avaliação da solução e os principais resultados alcançados. Por fim, a Seção 5 conclui o artigo com considerações finais e perspectivas de trabalhos futuros.

2. Trabalhos Relacionados

Criptografia é o mecanismo mais fundamental para se implementar a publicação segura e privativa de conteúdos [Jacobson et al. 2012]. No entanto, os mecanismos de criptografia simétrica e assimétrica não são suficientes se empregados isoladamente em ICN: enquanto a primeira requer algum recurso externo (*ex.* telefone ou *e-mail*) para o processo de distribuição de chaves, a segunda torna inócuas as facilidades de *cache* na rede, uma vez que o conteúdo precisa ser cifrado para cada usuário.

De forma geral, as soluções propostas possuem como objetivos em comum o maior aproveitamento possível do mecanismo de *cache* na rede e a redução da complexidade associada ao controle de acesso. Apesar disso, elas diferem quanto à cardinalidade (na publicação de conteúdos), à intrusividade (isto é, introdução ou modificação de com-

Tabela 1. Propostas para o controle de acesso a conteúdos, organizadas por critérios de cardinalidade, de intrusividade e de proteção ao conteúdo.

Propostas	Cardinalidade		Intrusividade		Proteção do Conteúdo	
	um publicador	vários publicadores	não intrusivas	intrusivas	criptografia simétrica	criptografia assimétrica
Misra et al. [Misra et al. 2013]	x		x		x	
Papanis et al. [Papanis et al. 2014]	x		x		x	
Wood e Uzun [Wood and Uzun 2014]	x			x	x	
Mannes et al. [Mannes et al. 2014]	x		x			x
Singh et al. [Singh et al. 2012]		x		x	nenhum	
Fotiou et al. [Fotiou et al. 2012]		x		x	x	
Hamdane et al. [Hamdane et al. 2013]		x		x	x	
Ghali et al. [Ghali et al. 2015]		x		x	nenhum	

ponentes na rede) e à forma como o conteúdo em si é protegido. A Tabela 1 apresenta uma visão geral das soluções propostas, organizadas segundo esses critérios.

Misra *et al.* [Misra et al. 2013] e Papanis *et al.* [Papanis et al. 2014] propõem que os provedores protejam o conteúdo empregando criptografia simétrica. Enquanto Misra *et al.* empregam o conceito de criptografia em *broadcast* para a distribuição das chaves de acesso ao conteúdo, por sua vez, Papanis *et al.* utilizam o mecanismo CP-ABE (*Ciphertext-Policy Attribute-based Encryption*) [Bethencourt et al. 2007]. Essas soluções tiram bastante proveito do mecanismo de *cache* na rede, por utilizarem criptografia simétrica para proteger o conteúdo. No entanto, elas permitem apenas um publicador no grupo de compartilhamento seguro. Uma vez que cada publicador precisa criar um par de chaves para cada usuário que deve ter acesso aos conteúdos, no cenário em que todos são publicadores, o número de pares de chaves necessárias é proporcional a $\binom{n}{2}$.

Wood e Uzun [Wood and Uzun 2014] e Mannes *et al.* [Mannes et al. 2014] seguem o mesmo modelo baseado em apenas um publicador. No entanto, elas empregam a técnica de reencriptação por *proxy*, proposta orginalmente por Ateniese *et al.* [Ateniese et al. 2006]. Essa técnica utiliza entidades de *proxy* na rede para transformar um conteúdo criptografado, com a chave pública do provedor, em outro conteúdo criptografado, agora com a chave pública do usuário. A principal diferença entre essas soluções reside no critério de intrusividade: enquanto na de Wood e Uzun, depende-se de nodos intermediários para atuar como redistribuidores de chaves de reencriptação, na proposta de Mannes *et al.*, possibilita-se que os próprios publicadores implementem esse papel. Embora menos intrusiva, essa última requer que o publicador do conteúdo esteja permanentemente disponível para criar e distribuir as chaves de reencriptação sempre que o conteúdo for acessado.

As demais soluções propostas avançam no critério de cardinalidade, permitindo vários publicadores no mesmo grupo de compartilhamento seguro, assim, evitando o problema de explosão combinatorial de chaves. Elas dependem, porém, de entidades adicionais para armazenar conteúdos e/ou realizar controle de acesso, o que implica em modificações na arquitetura ICN ou na dependência da disponibilidade dessas entidades. As soluções de Singh *et al.* [Singh et al. 2012] e Ghali *et al.* [Ghali et al. 2015] são particularmente dependentes do comportamento honesto dessas entidades; caso sejam subvertidas, a privacidade dos conteúdos controlados pelas mesmas poderá ser comprometida.

Um aspecto importante que pode ser observado na Tabela 1 é que nenhuma das propostas existentes reúne as características de não intrusividade e de suporte a múltiplos publicadores. Na seção a seguir, apresenta-se um modelo de segurança que satisfaz esses

requisitos, sem dependência de componentes específicos na arquitetura subjacente e sem aumentar a complexidade do processo de gerenciamento de chaves.

3. Habilitando Grupos com Múltiplos Publicadores em ICN

A Figura 1 apresenta uma visão geral do modelo e da arquitetura que o apoia, destacando ainda os atores e componentes envolvidos. O compartilhamento seguro de conteúdos se inicia quando um usuário interage com uma instância da *Aplicação ICN*, executando na sua própria estação local para *criar um grupo*. A aplicação ICN corresponde a um *software* (o equivalente a um navegador *web*) que permite o compartilhamento de conteúdos via paradigma ICN, estendido para suportar o modelo de segurança proposto.

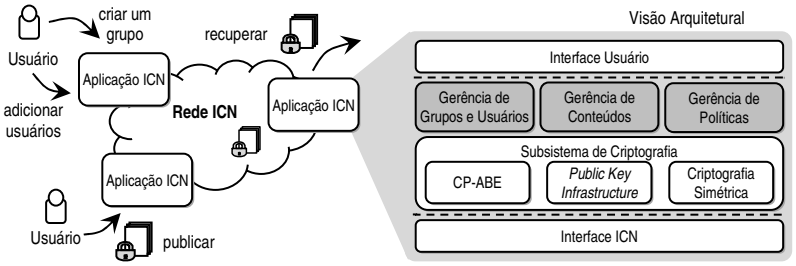


Figura 1. Visão arquitetural da solução proposta.

Apenas o usuário que criou o grupo (denominado de *administrador* no restante do artigo) poderá *adicionar usuários* ao mesmo. Conforme será discutido na próxima subseção, a adição de um usuário consiste na criação de uma credencial de membro (uma chave privada) e na entrega dessa credencial para o usuário. Essa entrega deve ocorrer via compartilhamento seguro, por exemplo, com o uso de criptografia assimétrica. Uma vez habilitado como membro do grupo, o usuário poderá compartilhar conteúdos (isto é, *publicar* e *recuperar* conteúdos) de forma segura com os demais membros.

A visão arquitetural apresentada na parte direita da Figura 1 destaca (em cinza) os componentes que fazem parte da proposta. O componente *Gerência de Grupos e Usuários* reúne as funcionalidades para criação de grupos e adição de membros. O componente *Gerência de Conteúdos* está relacionado com a publicação e recuperação segura de conteúdos. Por fim, o componente *Gerência de Políticas* possibilita o controle fino de acesso aos conteúdos, apoiando, por exemplo, a concessão e a revogação de acesso. Esses componentes são apoiados por um subsistema de criptografia, composto por um mecanismo de criptografia simétrica, uma solução de infraestrutura de chaves públicas (*Public Key Infrastructure, PKI*) e um mecanismo de criptografia baseada em atributos (CP-ABE) [Bethencourt et al. 2007] (doravante referido como *componente CP-ABE*). Observe que os componentes da solução proposta acomodam-se exclusivamente entre as camadas de interface com o usuário e com a rede ICN, sendo restritos portanto ao *software* que executa na estação do usuário.

As Subseções 3.1, 3.2 e 3.3, a seguir, descrevem em detalhes as funcionalidades proporcionadas por cada um dos componentes destacados na visão arquitetural da Figura 1. A Subseção 3.4 encerra a apresentação da proposta, discutindo possíveis estratégias de ataque contra a solução. Para a explicação que segue adota-se um conjunto de notações e convenções sumarizado na Tabela 2.

3.1. Gerência de Grupos e Usuários

A Figura 2 ilustra a dinâmica do processo de manutenção de grupos de compartilhamento seguro, destacando as atividades de criação de grupos e de adição de usuários ao mesmo.

Tabela 2. Glossário de notações relacionadas ao modelo de segurança proposto.

Notação	Definição formal	Descrição
Entidades e conjuntos		
C		Conteúdo original
G		Grupo de compartilhamento seguro
U		Usuário (membro do grupo)
$\mathbb{P}$		Política de acesso
$\mathcal{L}_G$		Conjunto de atributos existentes no grupo G
$\mathcal{L}_{U,G} \subseteq \mathcal{L}_G$		Conjunto de atributos do usuário U no grupo G
Chaves criptográficas		
K_s		Chave de criptografia simétrica
K_U		Chave pública do usuário U
K_U^{-1}		Chave privada do usuário U
K_G		Chave pública do grupo de compartilhamento seguro G
M_G		Chave mestra do grupo de compartilhamento seguro G
$K_{\mathcal{L}_{U,G}}^{-1}$		Chave privada do usuário U no grupo G
Funções criptográficas		
$\{X\}_{K_x}$		Elemento X cifrado usando a chave K_x (simétrica ou assimétrica)
$\{X\}_{(K_G,P)}$		Elemento X cifrado usando a chave do grupo K_G e a política P
Modelo de segurança		
$\widehat{X}$		Identificador do elemento X
C_P	$C_P = \langle \{C\}_{K_s}, \widehat{H_C} \rangle$	Conteúdo C protegido
H_C	$H_C = \langle \{K_s\}_{(K_G,\mathbb{P})}, \widehat{K_G} \rangle$	Bloco habilitador de um conteúdo protegido C_P

Criação de grupo. Como brevemente mencionado anteriormente, o administrador inicia esse processo ao interagir com a aplicação ICN (fluxo 1 na Figura 2). Esse processo compreende basicamente a criação de um par de chaves pública K_G e mestra M_G para o grupo, o que é feito com o apoio do componente CP-ABE. O grupo passa a existir na rede a partir do momento que se dissemina a chave pública K_G na rede, na forma de um objeto, utilizando como identificador o nome do grupo (fluxo 2). A chave mestra M_G é mantida em segredo pelo administrador.

Cada grupo possui um conjunto de atributos $\mathcal{L}_G$, que são utilizados para descrever os usuários membros. Os atributos são cadeias de caracteres de tamanho livre, definidos pelo administrador e existentes somente no escopo daquele grupo. Por exemplo, suponha um grupo composto por integrantes de uma comunidade acadêmica. Alguns atributos possíveis são "professor", "graduando", "mestrando", "doutorando" e "pós-doutorando". Note que não há uma regra geral para a formação dos atributos. Da mesma forma, a semântica dos atributos é dada pelo contexto do grupo. A lista de atributos também deve ser publicada como um objeto na rede (fluxo 3).

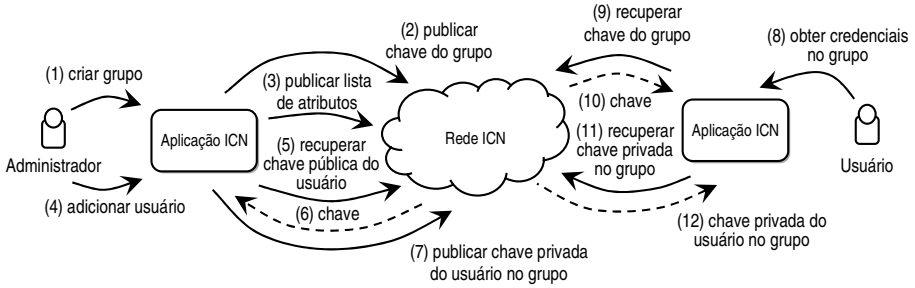


Figura 2. Manutenção de grupos de compartilhamento seguro.

Adição de usuário a um grupo. O administrador inicia esse processo, por intermédio da aplicação ICN (fluxo 4), ao informar os atributos que o novo membro possuirá. Esse processo se desdobra em três passos: (*i*) criar a chave privada do usuário no

grupo $K^{-1}_{\mathcal{L}_{U,G}}$; (*ii*) publicar a chave $K^{-1}_{\mathcal{L}_{U,G}}$ de forma segura na rede, de modo que apenas o usuário adicionado possa recuperá-la; e (*iii*) recuperar a chave $K^{-1}_{\mathcal{L}_{U,G}}$ da rede (esse último passo feito pelo usuário adicionado). Esses passos são descritos em detalhes a seguir.

A chave privada $K^{-1}_{\mathcal{L}_{U,G}}$ é criada com o apoio do componente CP-ABE. Para tal, o administrador deve especificar um conjunto de atributos $\mathcal{L}_{U,G} \subseteq \mathcal{L}_G$ para o usuário. A criação de $K^{-1}_{\mathcal{L}_{U,G}}$ requer também a chave mestra do grupo M_G. Após criada, disponibiliza-se a chave $K^{-1}_{\mathcal{L}_{U,G}}$ (com os atributos $\mathcal{L}_{U,G}$ incorporados) na rede, para que o usuário alvo possa recuperá-la. A entrega deve ocorrer de forma privativa, visto que a posse de $K^{-1}_{\mathcal{L}_{U,G}}$ materializa a participação no grupo. Em outras palavras, $K^{-1}_{\mathcal{L}_{U,G}}$ será empregada para recuperar conteúdos protegidos no grupo (conforme discutido na próxima subseção). Para realizar essa entrega, o administrador precisa recuperar da rede a chave pública K_U do usuário e verificá-la via mecanismo de infraestrutura de chave pública (fluxos 5 e 6). A chave $K^{-1}_{\mathcal{L}_{U,G}}$ é criptografada usando K_U, assim, gerando a chave criptografada $\{K^{-1}_{\mathcal{L}_{U,G}}\}_{K_U}$, a qual é publicada como um objeto na rede (fluxo 7). Por fim, o usuário alvo precisa recuperar as chaves $K^{-1}_{\mathcal{L}_{U,G}}$ e K_G da rede, para poder utilizá-las na publicação e recuperação de conteúdos no grupo. O usuário inicia esse procedimento (fluxo 8) especificando o nome do grupo para recuperar esses objetos. A aplicação recupera, então, a chave pública do grupo K_G (fluxos 9 e 10) e a chave privada do usuário no grupo, criptografada $\{K^{-1}_{\mathcal{L}_{U,G}}\}_{K_U}$ (fluxos 11 e 12). A chave privada no grupo é descriptografada usando a própria chave privada do usuário K^{-1}_U. A partir de então, ele está habilitado para publicar e recuperar conteúdos no grupo. Note que o administrador, caso deseje publicar e recuperar conteúdos do grupo, também precisa criar a sua própria chave $K^{-1}_{\mathcal{L}_{U,G}}$.

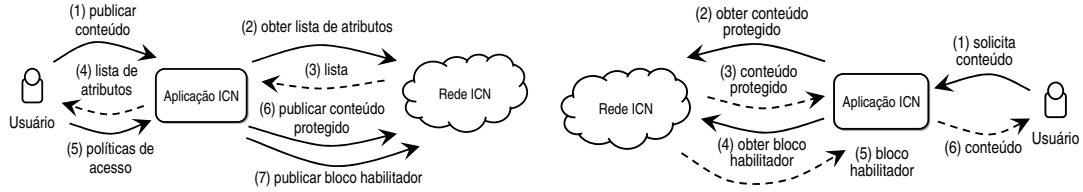
3.2. Gerência de Conteúdos

A gerência de conteúdos reúne todos os procedimentos necessários para a publicação e a recuperação segura de conteúdos na rede. Esses procedimentos se apoiam em dois elementos importantes, o conteúdo protegido e o bloco habilitador.

Conteúdo protegido e bloco habilitador. O primeiro corresponde a um conteúdo cifrado usando criptografia simétrica, enquanto que o segundo contém a chave necessária para decifrar um dado conteúdo. No modelo proposto, um conteúdo protegido possui um (e apenas um) bloco habilitador correspondente. Formalmente, um conteúdo protegido é uma tupla $C_P = \langle \{C\}_{K_s}, \widehat{H_C} \rangle$, onde $\{C\}_{K_s}$ corresponde ao conteúdo original C, cifrado usando uma chave simétrica K_s, e $\widehat{H_C}$ é o identificador do bloco habilitador desse conteúdo protegido. Um bloco habilitador é uma tupla $H_C = \langle \{K_s\}_{(K_G, \mathbb{P})}, \widehat{K_G} \rangle$, onde $\{K_s\}_{(K_G, \mathbb{P})}$ corresponde à chave K_s (usada para cifrar C) cifrada usando (*i*) a chave pública K_G do grupo e (*ii*) uma política de acesso $\mathbb{P}$, e $\widehat{K_G}$ é o identificador da chave pública do grupo. Observe que esse projeto possibilita que vários conteúdos sejam protegidos por um mesmo bloco habilitador. Essa característica pode ser conveniente quando se desejar publicar múltiplos conteúdos usando uma política de acesso única.

O processo para construir um bloco habilitador compreende (*i*) a definição da chave simétrica que será usada para cifrar o conteúdo e (*ii*) a especificação (pelo usuário) da *política de controle de acesso* $\mathbb{P}$. Em relação à chave simétrica, ela pode ser gerada automaticamente, pela aplicação ICN, ou informada pelo usuário. Sobre a política $\mathbb{P}$, ela determinará que usuários do grupo estarão autorizados a decifrar o conteúdo e é feita envolvendo elementos da lista de atributos do grupo $\mathcal{L}_G$.

Para ilustrar o conceito de políticas de acesso, suponha o grupo de compartilha-



(a) Publicação (b) Recuperação

Figura 3. Sequência de passos para publicação e recuperação de conteúdos.

mento de conteúdos acadêmicos nos quais os usuários possuem um (ou mais) dos seguintes atributos: $\mathcal{L}_G = \{\text{professor, graduando, mestrando, doutorando, pos-doutorando}\}$. O usuário pode, por exemplo, especificar uma política $\mathbb{P} = \{\text{professor } \textbf{ou} \text{ graduando}\}$. Nesse caso, a descriptografia baseada em atributos (usando o componente CP-ABE) poderá ser realizada apenas pelos usuários detentores do atributo "professor" ou "graduando" (ou ambos). A metodologia para a formação dessas políticas será discutida mais detalhadamente na Subseção 3.3. Uma vez determinada $\mathbb{P}$, emprega-se o componente CP-ABE para cifrar K_s. Essa cifragem é executada usando a chave pública K_G do grupo e a política $\mathbb{P}$. A chave cifrada $\{K_s\}_{(K_G,\mathbb{P})}$ é, então, encapsulada em H_C.

Após construído o bloco habilitador, o conteúdo protegido pode então ser formado. A sua construção compreende a cifragem do conteúdo original C a ser disseminado na rede, para isso, utilizando-se a chave simétrica K_s encapsulada no bloco habilitador que será associado a esse conteúdo.

Publicação de conteúdos. A Figura 3(a) ilustra a dinâmica do processo de publicação de um conteúdo no grupo. O usuário inicia esse processo ao interagir com a aplicação ICN (fluxo 1 na Figura 3(a)), informando o conteúdo C a ser publicado. Nesse momento, cinco passos são executados. Primeiro, a aplicação recorre à rede para obter a lista atualizada dos atributos do grupo $\mathcal{L}_G$ (fluxos 2 e 3) e disponibiliza-os ao usuário. Em seguida, o usuário elabora a política de acesso $\mathbb{P}$, conforme as restrições de acesso desejadas (fluxos 4 e 5). O terceiro passo, realizado pela aplicação, consiste em criptografar o conteúdo C usando uma chave simétrica K_s. O quarto passo corresponde à construção do bloco habilitador H_C do conteúdo, conforme discutido anteriormente. No último passo, o conteúdo protegido C_P é construído, encapsulando o conteúdo cifrado $\{C\}_{K_s}$ e o identificador para o bloco habilitador $\widehat{H_C}$. Por fim, ambos, conteúdo protegido C_P e bloco habilitador H_C, são publicados na rede (fluxos 6 e 7).

Recuperação de conteúdos. O processo de recuperação, ilustrado na Figura 3(b), inicia-se quando o usuário solicita um conteúdo (fluxo 1). A aplicação solicita à rede o conteúdo protegido C_P correspondente (fluxos 2 e 3), o qual obtém-se da fonte mais próxima. Ao abrir C_P, a aplicação identifica qual bloco habilitador H_C está relacionado a esse conteúdo (por meio do identificador $\widehat{H_C}$ presente na tupla). A aplicação solicita então H_C à rede (fluxos 4 e 5) para recuperar a chave simétrica criptografada $\{K_s\}_{(K_G,\mathbb{P})}$. A chave simétrica $\{K_s\}_{(K_G,\mathbb{P})}$ recuperada é submetida ao componente CP-ABE para decifragem. Para isso, o usuário utiliza a sua chave privada no grupo $K^{-1}_{\mathcal{L}_{U,G}}$. A chave $\{K_s\}_{(K_G,\mathbb{P})}$ é descriptografada *se e somente se* a política de acesso $\mathbb{P}$ usada para cifrá-la for compatível com os atributos utilizados pelo administrador na criação de $K^{-1}_{\mathcal{L}_{U,G}}$ (ao adicionar o usuário no grupo). Caso seja descriptografado com sucesso, o conteúdo é entregue ao usuário (fluxo 6).

Tabela 3. Regras para a definição de políticas de acesso a conteúdos.

⟨política⟩ ::= ⟨atributo⟩ | '(' ⟨política⟩ ')'
| ⟨atributo⟩ e ⟨política⟩ | ⟨atributo⟩ ou ⟨política⟩
| ⟨atributo⟩ = ⟨inteiro⟩ | ⟨atributo⟩ < ⟨inteiro⟩ | ⟨atributo⟩ > ⟨inteiro⟩
| ⟨inteiro⟩ de '(' ⟨coleção⟩ ')'

⟨coleção⟩ ::= ⟨política⟩ ',' ⟨política⟩ | ⟨coleção⟩

3.3. Gerência de Políticas

O modelo de segurança, por meio do componente *Gerência de Políticas*, permite determinar quando e quais usuários podem ter acesso aos conteúdos publicados. Em outras palavras, o modelo reúne mecanismos que permitem conceder, limitar e revogar autorizações de acesso a conteúdos, com base em políticas.

A composição de uma política envolve operadores relacionais ($>$, $<$ e $=$) e lógicos (**e** e **ou**). Com o apoio do componente CP-ABE [Bethencourt et al. 2007], esses operadores permitem determinar quando e quais usuários têm acesso ao conteúdo. A Tabela 3 apresenta o conjunto de regras que regem o processo de construção de políticas de acesso a conteúdo. Nesse conjunto, $<$*atributo*$> \in \mathcal{L}_G$ e $<$*inteiro*$> \in \mathbb{N}$.

Concessão de acesso. Ela consiste basicamente em definir uma política que um determinado conjunto de usuários do grupo deve satisfazer para decifrar um conteúdo. Observe que uma política pode ser formada por apenas um atributo. Nesse caso, para ter acesso ao conteúdo, a chave privada do usuário no grupo $K^{-1}_{\mathcal{L}_{U,G}}$ deve atender à restrição descrita pela política. Por exemplo, suponha dois usuários: *joão* com os atributos $\mathcal{L}_{\text{joão},G} = \{\text{professor, pesquisador}\}$, e *josé* com os atributos $\mathcal{L}_{\text{josé},G} = \{\text{aluno, pesquisador}\}$. Uma política de acesso $\mathbb{P}_1 = \{\text{professor}\}$ permite acesso ao conteúdo apenas para *joão*. A política de acesso $\mathbb{P}_2 = \{\text{pesquisador}\}$, por sua vez, permite o acesso a ambos. As regras não permitem a formação de políticas "coringa", isto é, para acesso universal. Uma forma de alcançar todos os usuários é citar um a um os atributos dos mesmos na política de acesso. Alternativamente, o administrador pode definir um atributo comum aos usuários (ex. "todos"); assim, cada publicador poderá usá-lo em políticas que visem ao acesso universal.

Os atributos (dos usuários e de políticas) podem ainda ser valorados. Eles podem ser criados para indicar, por exemplo, o nível do usuário na hierarquia de uma corporação. Suponha o usuário *joão* com o atributo "nível = 5" e *josé* com o atributo "nível = 2". Caso deseje-se publicar um conteúdo somente para os usuários com nível 3 ou superior (no caso, *joão*), basta definir a política $\mathbb{P} = \{\text{nível} > 2\}$ (assumindo que os níveis de hierarquia são dados por números discretos).

Revogação de acesso. A revogação baseia-se na possibilidade de publicar uma versão mais recente de um bloco habilitador (por exemplo, quando a versão existente expirar na *cache* dos roteadores). Assim, o usuário pode reformular a política daquele bloco para restringir o acesso de algum usuário particular. Há duas estratégias que podem ser empregadas. A primeira é definir um atributo único para cada usuário. Nesse caso, a revogação compreenderia selecionar todos os usuários exceto aquele(s) cujo acesso deve ser revogado. Supondo os usuários *joão*, *josé*, *maria* e *fátima*, e um conteúdo publicado com $\mathbb{P} = \{\text{todos}\}$, revogar o acesso de *joão* a esse conteúdo requer que a política seja reformulada para $\mathbb{P}' = \{1\,\text{de}\,(\text{jose, maria, fatima})\}$. A complexidade de se definir essa restrição para grupos com dezenas de usuários ou mais pode ser trivialmente resolvida na

interface com o usuário, não sendo necessário transportá-la para o modelo.

A segunda forma de implementar revogação é por meio de expiração, usando o mecanismo de comparação de valores de atributos. Para ilustrar, suponha que *joão* possui o atributo "criado = 1435708800" (2015-07-01 00:00:00) e *maria*, "criado = 1446336000" (2015-11-01 00:00:00). A semântica desses atributos corresponde à data e hora (em *timestamp*) que cada um foi adicionado ao grupo. Agora, suponha um conteúdo com a política $\mathbb{P} = \{\text{criado} > 1420070400\}$. Ela garante acesso apenas aos usuários adicionados ao grupo após 1º de janeiro, o que se aplica a *joão* e *maria*. O acesso de *joão* pode ser revogado por expiração, nesse caso, ao se publicar um novo bloco habilitador com $\mathbb{P}' = \{\text{criado} > 1443657600\}$ (1º de outubro). Destaca-se que ambas estratégias podem ser usadas em conjunto, permitindo revogação a curto e longo prazo.

3.4. Possíveis Estratégias de Ataque

O modelo apresentado para compartilhamento seguro de conteúdos foi projetado considerando três premissas básicas: (*i*) o administrador do grupo é confiável; (*ii*) os membros do grupo mantêm em segredo suas respectivas chaves privadas no grupo; e (*iii*) o membro com acesso a um conteúdo protegido não divulga a chave simétrica usada para cifrá-lo.

As implicações das premissas enumeradas acima são descritas a seguir. A primeira estabelece que a concessão de atributos aos usuários membros do grupo é feita de forma confiável. Ou seja, o administrador não deturpará o uso dos atributos ao atribuí-los aos membros, por exemplo, conferindo atributo(s) a um adversário ou mesmo a usuários que não sejam compatíveis com aquele(s) atributo(s). Essa premissa é similar à confiabilidade depositada no gerente de projetos estratégicos e/ou sensíveis, por exemplo, de um *software open-source* (no qual a admissão de um adversário ao time de desenvolvedores pode levar à inclusão de código malicioso no *software* desenvolvido). A segunda premissa está relacionada à segurança dos conteúdos que são acessíveis por determinados usuários. Essa premissa é equivalente à guarda das credenciais de acesso que um usuário possui em um sistema (por exemplo, a chave para um servidor *ssh* ou a senha para um portal de conteúdos pagos). Finalmente, a terceira premissa implica na segurança dos conteúdos protegidos que foram acessados. Nesse caso, o vazamento da chave simétrica seria equivalente ao ato de vazar o próprio conteúdo.

Considerando essas premissas, um atacante pode burlar o modelo de segurança proposto apenas se comprometer (via acesso físico ou remoto) a própria estação do administrador/usuário para subtrair a chave privada do grupo ou as chaves privadas dos usuários. Observe que esse ataque foge ao escopo do artigo, uma vez que a proteção contra o mesmo requer mecanismos que garantam a segurança da própria estação do administrador/usuário. Assumindo a segurança das mesmas, o modelo mantém-se resiliente mesmo que o atacante possua acesso privilegiado a quaisquer elementos da rede ou nela disponíveis (roteadores, blocos habilitadores, chaves públicas, listas de atributos, etc.).

O modelo proposto é robusto a ataques em conluio. Por exemplo, suponha um usuário com o atributo professor e outro com o atributo aluno. Mesmo que esses usuários atuem em conjunto, eles não podem decifrar um conteúdo protegido com a política $\mathbb{P} = \{\text{professor } \mathbf{e} \text{ aluno}\}$, visto que a política requer que o mesmo membro possua ambos os atributos, simultaneamente. Conforme discutido anteriormente, apenas usuários pertencentes ao grupo e que satisfaçam integralmente as políticas de acesso definidas, podem acessar conteúdos publicados. Por fim, o modelo não impede que usuários não pertencentes ao grupo publiquem conteúdos protegidos no mesmo. Isso é possível visto que a publicação requer apenas a chave pública e a lista de atributos do grupo, ambos disponíveis em claro na rede. Os membros do grupo podem evitar o acesso a conteúdos

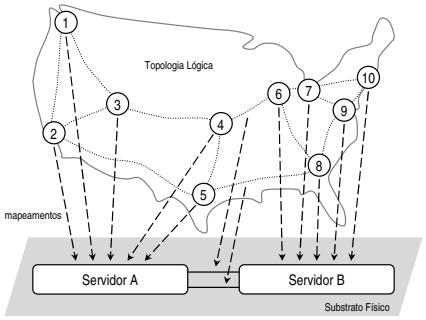


Figura 4. Topologia base da avaliação.

Tabela 4. Cenários avaliados.

Parâmetros	Cenários avaliados	
	A	B
Quantidade de usuários	10	30
Tamanho do arquivo	100MB	100MB
Arquivos publicados	10	30
Capacidade da *cache*	1GB	1GB
Expiração da *cache*	1 hora	1 hora
Tamanho do *chunk*	4KB	4KB
Popularidade dos conteúdos	Zipf $(s = 2.0)$ [1]	Zipf $(s = 2.0)$ [1]

[1] Segundo *Pentikousis et al.* [Pentikousis et al. 2015]

indesejados verificando a origem dos mesmos usando, por exemplo, mecanismos de auto-certificação de conteúdos da própria rede [Jacobson et al. 2012].

4. Avaliação

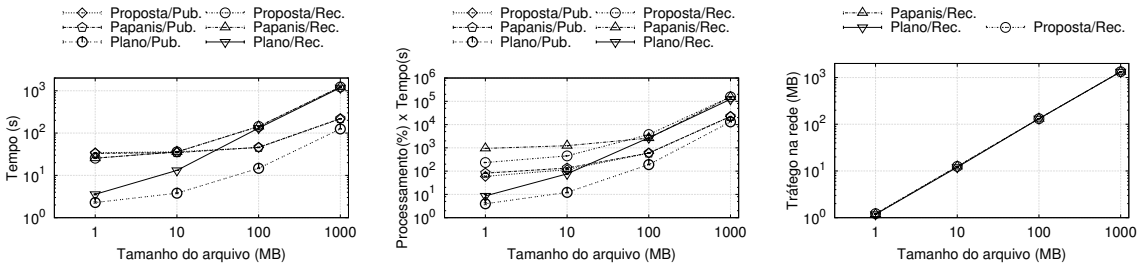
Para aferir a eficácia e eficiência do modelo proposto, uma série de experimentos foi realizada em um ambiente controlado. Os experimentos visaram verificar a escalabilidade do modelo, o custo de operação e o impacto à qualidade de experiência (QoE) dos usuários, em cenários com um número variado de usuários atuando como publicadores e recuperadores. Para comparação, considerou-se a solução de Papanis *et al.* [Papanis et al. 2014] e uma solução de compartilhamento seguro de conteúdos baseada no algoritmo RSA.

4.1. Configuração do Ambiente e Cenários de Avaliação

O modelo proposto foi implementado sobre a arquitetura CCN (*Content Centric Networking*) [Jacobson et al. 2012], usando como base o *software* CCNx 0.8.2 executando sobre a máquina virtual Java SE versão 8. Para o mecanismo de criptografia baseada em atributos, foi utilizado o *software cpabe* 0.11 [Bethencourt et al. 2015]. Visando seguir o padrão para gerenciamento de chaves proposto para arquiteturas ICN [Bian et al. 2013], cada conteúdo protegido é acompanhado de um respectivo metadado, que contém o identificador do bloco habilitador correspondente e a validade do conteúdo, entre outros. Da mesma forma, cada bloco habilitador é acompanhado por um respectivo metadado.

O substrato físico usado nos experimentos compreendeu dois servidores, cada um equipado com 1 processador Intel Xeon E5-2420 (1.9GHz, 12 Threads e 15MB *cache*), 32GB de memória RAM (1333MHz), 1 HD SAS (1TB de capacidade) e 2 interfaces de rede Gigabit Ethernet. Ambos possuem Debian/Linux 7.7 (kernel 3.14.21) e Hipervisor Xen instalados. Os servidores foram conectados diretamente entre si usando dois cabos Ethernet. A topologia lógica usada para a avaliação, um subconjunto da Internet2, é ilustrada na Figura 4. Os mapeamentos dos elementos lógicos para o substrato físico também são apresentados na figura. Cada nodo lógico na topologia corresponde a uma máquina virtual; cada máquina foi instanciada com as seguintes configurações: 2 processadores virtuais, 2 GB de RAM e 40 GB de disco. Os enlaces entre os nodos foram emulados empregando o *software bridge-utils* versão 1.5, todos com velocidade de $\approx$ 98Mbps.

Para a avaliação experimental foram considerados dois cenários, cujos parâmetros mais relevantes são sumarizados na Tabela 4. Por simplificação, todos os conteúdos foram publicados usando uma política de acesso universal (ou seja, qualquer usuário membro do grupo pode decifrá-lo). Essa decisão foi embasada em experimentos preliminares, os quais permitiram observar que a quantidade de atributos não tem efeito relevante sobre custos (tempo de publicação/recuperação, tráfego de rede, etc.) do modelo proposto. Por



(a) Tempo (b) Carga de processamento (c) Tráfego na rede

Figura 5. Custos da solução proposta considerando tempos de publicação e de recuperação, carga de processamento e tráfego gerado na rede.

fim, para cada experimento, foram realizadas 30 execuções e calculado o intervalo de confiança com nível de significância $\alpha = 0.05$.

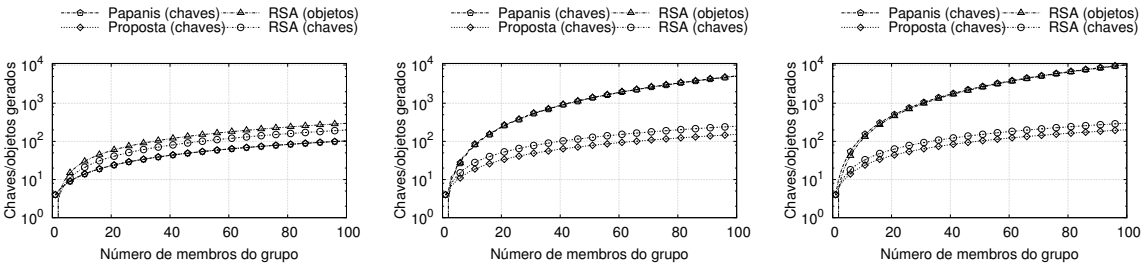
4.2. Custos da Solução Proposta

A primeira parte da avaliação compreende uma análise dos custos da solução em um ambiente isolado, formado por apenas um publicador e um recuperador. Para isso, utilizou-se subconjunto da topologia ilustrada na Figura 4, formada pelos nodos 4 (publicador) e 6 (recuperador). A Figura 5 apresenta uma visão geral dos resultados obtidos para a publicação (curvas "Pub.") e a recuperação (curvas "Rec.") de conteúdos. Para fins de comparação, considerou-se a solução de Papanis *et al.* (curvas "Papanis") e uma solução sem mecanismos de segurança (curvas "Plano"). Por legibilidade, os gráficos são apresentados com o eixo y em escala logarítmica.

A principal conclusão que se pode tirar a partir dos resultados da Figura 5 é a de que o sobrecusto da solução proposta é marginal quando comparado a Papanis *et al.* Focando no tempo médio de disseminação de conteúdos (Figura 5(a)), por exemplo, a solução proposta foi inclusive 0,6% mais eficiente em média na publicação. Em relação aos custos de processamento (Figura 5(b)), esses são ligeiramente maiores na solução proposta (0,5% na publicação e 1,4% na recuperação). Por fim, observa-se que a medição do tráfego gerado na rede (Figura 5(c)) indica desempenhos similares de ambas as soluções.

Quando comparados à solução sem mecanismos de segurança, note que os custos são amortizados de forma proporcional ao tamanho do conteúdo publicado. Esses resultados sugerem que a solução proposta incorre em impacto relativamente pequeno para a qualidade de experiência (QoE) dos usuários. Na publicação, por exemplo, o sobrecusto de tempo diminui de 1.400% (diferença do custo entre a solução proposta e a solução "Plano"), em média (com conteúdos de 1MB) para 72% (1000MB). Nessa comparação, o sobrecusto médio foi de apenas 8% no tempo de recuperação de conteúdos (aspecto de maior importância para a QoE de grande parte dos usuários). Os resultados obtidos para o modelo proposto são inclusive similares ao observado para Papanis *et al.*

É importante mencionar que os custos adicionais de processamento e de tempo devem-se ao uso de criptografia para cifrar/decifrar o conteúdo e as chaves de acesso. Quando não há solução de segurança sendo utilizada, o processamento e o tempo referem-se apenas à publicação/recuperação do conteúdo na rede. Sobre o tráfego gerado na rede (Figura 5(c)), o sobrecusto foi constante e marginal, correspondendo principalmente ao bloco habilitador do conteúdo protegido (que também é disseminado na rede).



(a) 1 publicador (b) $n/2$ publicadores (c) n publicadores

Figura 6. Número de chaves/objetos necessários para a troca de conteúdos.

4.3. Quantidade de Chaves e de Objetos Gerados

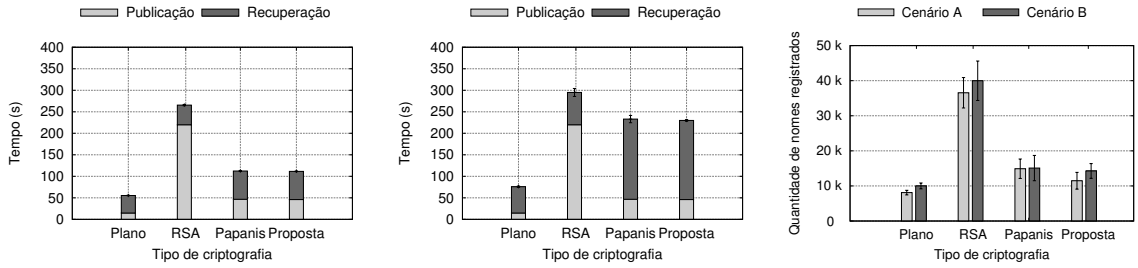
Outro aspecto observado está relacionado à quantidade de chaves/objetos necessários para a disseminação segura de conteúdos, nas situações em que um, metade e todos os usuários atuam como publicadores na rede, respectivamente. Nessa análise, realizada por meio de uma formulação matemática, foram consideradas além da solução proposta: a de Papanis *et al.* [Papanis et al. 2014], e a baseada no RSA. No caso de Papanis *et al.*, ela é instanciada para cada usuário publicador. No modelo baseado no RSA, (*i*) cada usuário possui um par de chaves pública e privada; (*ii*) cada conteúdo é cifrado usando uma chave simétrica única; e (*iii*) a chave do conteúdo é cifrada usando a chave pública de cada usuário alvo.

Os resultados dessa avaliação são apresentados na Figura 6 (o eixo y é apresentado em escala logarítmica). Observa-se que a solução proposta requer o menor número de chaves criptográficas, em comparação com Papanis *et al.* e RSA. Além disso, a solução proposta mantém a proporcionalidade do número das chaves relativas ao número de usuários pertencentes ao grupo, independentemente do número de publicadores. Mais importante, o número de chaves necessárias/objetos publicados aumenta significativamente para as duas últimas. Para Papanis *et al.*, observa-se um aumento de até 9.900%, em contraste com 96% na solução proposta. Em relação a Papanis *et al.*, esse aumento se relaciona ao problema da explosão combinatória de chaves. Embora no cenário usando RSA o número de chaves permaneça relativamente constante, o número de objetos publicados na rede cresce significativamente. O motivo é que, embora a chave simétrica seja única para cada conteúdo, ela precisa ser criptografada individualmente para cada usuário alvo, de modo a garantir que apenas usuários autorizados possam acessar o conteúdo.

4.4. Tempos de Disseminação e Quantidade de Objetos Registrados

O objetivo dessa avaliação, cujos resultados são sumarizados na Figura 7, foi aferir o desempenho da solução proposta, mais especificamente o tempo para disseminação de conteúdos e a sobrecarga à *Forward Information Base* (FIB) dos roteadores, em um ambiente com múltiplos publicadores e consumidores. Essa avaliação usou como base a topologia completa ilustrada na Figura 4 e os cenários sumarizados na Tabela 4. Cada usuário publica 1 e recupera n conteúdos, ou seja, são publicados 10 conteúdos no cenário A e 30 no cenário B. Para comparação, foram empregadas a solução de Papanis *et al.*, uma baseada no algoritmo RSA e outra sem mecanismos de segurança ("Plano").

Observe, nas Figuras 7(a) e 7(b), que a qualidade de experiência (QoE) do usuário (medida pelo tempo necessário para disseminação do conteúdo) é marginalmente afetada na nossa solução, comparado à Papanis *et al.* Mais importante, ela é substancialmente melhor quando comparada à solução baseada no RSA. Esse desempenho é alcançado causando relativamente menos impacto à rede, conforme pode ser observado na Figura 7(c).



(a) Tempos medidos no cenário A (b) Tempos medidos no cenário B (c) FIB nos cenários A e B

Figura 7. Tempo de publicação/recuperação dos conteúdos e quantidade de nomes registrados na FIB, para os cenários A e B.

O tempo relativamente maior de recuperação nas soluções proposta e a de Papanis *et al.* explica-se pelo fato de que a solução baseada no RSA não requer metadados de conteúdo ou de bloco habilitador. Em outras palavras, cada usuário pode localizar diretamente os conteúdos e suas respectivas chaves sem a necessidade de obter os metadados dos mesmos, sendo, portanto, irrelevante publicá-los. Por outro lado, o tempo de publicação é significativamente maior no RSA, visto que n versões criptografadas da chave de um mesmo conteúdo devem ser publicadas na rede, uma para cada usuário alvo. Essa característica se reflete no gráfico da Figura 7(c), com a solução proposta reduzindo em até 68% (no cenário B) a quantidade de nomes registrados na FIB dos roteadores.

5. Considerações Finais

A publicação segura de conteúdos em ICN é uma realidade, com diversas soluções que oferecem os mais variados níveis de controle de acesso. Apesar de promissoras, algumas soluções causam uma sobrecarga significativa na rede ao tornar o processo de gerência (e de distribuição) de chaves combinatorialmente complexo. As soluções que não estão suscetíveis a esse problema, no entanto, são dependentes de arquitetura específica ICN, inserem (ou modificam) componentes na rede e são pouco flexíveis para adoção gradual.

Para suprir essa lacuna, foi apresentada uma nova solução, centrada nos conceitos de grupos de usuários, para o compartilhamento seguro de conteúdos. A partir dos resultados alcançados, foi possível aferir a eficácia e eficiência da solução proposta. Em resumo, esta requer um número comparativamente menor de chaves e objetos na rede (em alguns casos até 97% menos chaves). Esse ganho é alcançado sem degradar a qualidade de experiência do usuário (por exemplo, o tempo necessário para publicar/recuperar conteúdos), ao contrário do que ocorre em outras soluções. Além desses benefícios, a solução proposta pode ser adotada de forma independente e autônoma por um subconjunto de usuários, sem depender de modificações na rede. Por fim, ela permite a publicação e recuperação de conteúdos mesmo que o administrador do grupo (ou o publicador do conteúdo, no caso de recuperação) torne-se indisponível.

Como perspectivas de trabalhos futuros, pretende-se investigar mecanismos para acelerar a disseminação de novas políticas de acesso ao conteúdo na rede, bem como mecanismos para tornar mais simples e eficiente a revogação de acesso a conteúdos.

Referências

Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., and Ohlman, B. (2012). A survey of information-centric networking. *IEEE Communications Magazine*, 50(7):26–36.

Ateniese, G., Fu, K., Green, M., and Hohenberger, S. (2006). Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security*, 9(1):1–30.

Bethencourt, J., Sahai, A., and Waters, B. (2007). Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy (SP 2007)*, pages 321–334.

Bethencourt, J., Sahai, A., and Waters, B. (2015). Advanced crypto software collection. Disponível em: <http://acsc.cs.utexas.edu/cpabe/>. Acesso em: Abril de 2015.

Bian, C., Zhu, Z., Afanasyev, A., Uzun, E., and Zhang, L. (2013). Deploying key management on ndn testbed. Technical report. Disponível em: <http://www.named-data.net/techreport/TR009-publishkey-rev2.pdf>. Acesso em: Junho, 2015.

de Brito, G. M., Velloso, P. B., and Moraes, I. M. (2012). Redes orientadas a conteúdo: Um novo paradigma para a internet. In *Minicursos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2012)*, pages 211–264.

Fotiou, N., Marias, G. F., and Polyzos, G. C. (2012). Access control enforcement delegation for information-centric networking architectures. In *ACM SIGCOMM workshop on Information-centric networking (ICN '12)*, pages 85–90.

Ghali, C., Schlosberg, M. A., Tsudik, G., and Wood, C. A. (2015). Interest-based access control for content centric networks (extended version). *CoRR*, abs/1505.06258.

Hamdane, B., Msahli, M., Serhrouchni, A., and El Fatmi, S. (2013). Data-based access control in named data networking. In *Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom 2013)*, pages 531–536.

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M., Briggs, N., and Braynard, R. (2012). Networking named content. *Commun. ACM*, 55(1):117–124.

Mannes, E., Maziero, C., Lassance, L. C., and Borges, F. (2014). Controle de acesso baseado em reencriptação por proxy em redes centradas em informação. In *Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2014)*.

Misra, S., Tourani, R., and Majd, N. E. (2013). Secure content delivery in information-centric networks: design, implementation, and analyses. In *ACM SIGCOMM workshop on Information-centric networking (ICN '13)*, pages 73–78.

Papanis, J. P., Papapanagiotou, S. I., Mousas, A. S., Lioudakis, G. V., Kaklamani, D. I., and Venieris, I. S. (2014). On the use of attribute-based encryption for multimedia content protection over information-centric networks. *Transactions on Emerging Telecommunications Technologies*, 25(4):422–435.

Pentikousis, K., Ohlman, B., Davies, E., Spirou, S., Boggia, G., and Mahadevan, P. (2015). Information-centric networking: Evaluation methodology draft-irtf-icnrg-evaluation-methodology-03. URL: https://tools.ietf.org/html/draft-irtf-icnrg-evaluation-methodology-03. Acesso em: Outubro de 2015.

Singh, S., Puri, A., Singh, S. S., Vaish, A., and S.Venkatesan (2012). A trust based approach for secure access control in information centric network. *Journal of Information and Network Security*, 1(2):97–104.

Wood, C. and Uzun, E. (2014). Flexible end-to-end content security in ccn. In *11th Consumer Communications and Networking Conference (CCNC 2014)*.

Xylomenos, G., Ververidis, C., Siris, V., Fotiou, N., Tsilopoulos, C., Vasilakos, X., Katsaros, K., and Polyzos, G. (2014). A survey of information-centric networking research. *IEEE Communications Surveys Tutorials*, 16(2):1024–1049.