Universidade Tecnológica Federal do Paraná- Câmpus de Pato Branco
Departamento Acadêmico de Informática
Curso de Engenharia de Computação

Controle de acesso baseado em reencriptação por proxy em Redes Centradas em Informação

Autores: Elisa Mannes,
Carlos Maziero,
Luiz Carlos Lassance,
Fabio Borges

Sumário

- Introdução
- Controle de acesso em ICN
- Reencriptação por *proxy*
- Controle de acesso usando reencriptação
- Avaliação
- Conclusão

Introdução

- Redes Centradas em Informação (ICN - Information-centric Networks)
- Nomear, rotear e encaminhar conteúdo na rede ao invés de endereços de maquina permite a implementação de cache nos dispositivos da rede.
- O paradigma de ICN também modifica os aspectos relacionados à segurança de redes.

Introdução

- 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.
- Existem soluções de controle de acesso desenvolvidas especialmente para uso em arquiteturas de ICN.

Introdução

- Proposta de solução:
  - o conteúdo pode ser armazenado em qualquer dispositivo e recuperado por qualquer usuário;
  - os usuários que acessam o conteúdo não podem decifrá-lo, a menos que sejam autorizados pelo provedor de conteúdo;
  - não há a adição de novas entidades na rede para a aplicação ou a validação de políticas de acesso;

Controle de acesso em ICN

- Cópias em cache podem ser acessadas por qualquer usuário.
- Ações de roteamento e de encaminhamento são realizadas diretamente pelo nome do conteúdo.
- Encriptação do conteúdo.

Reencriptação por *proxy*

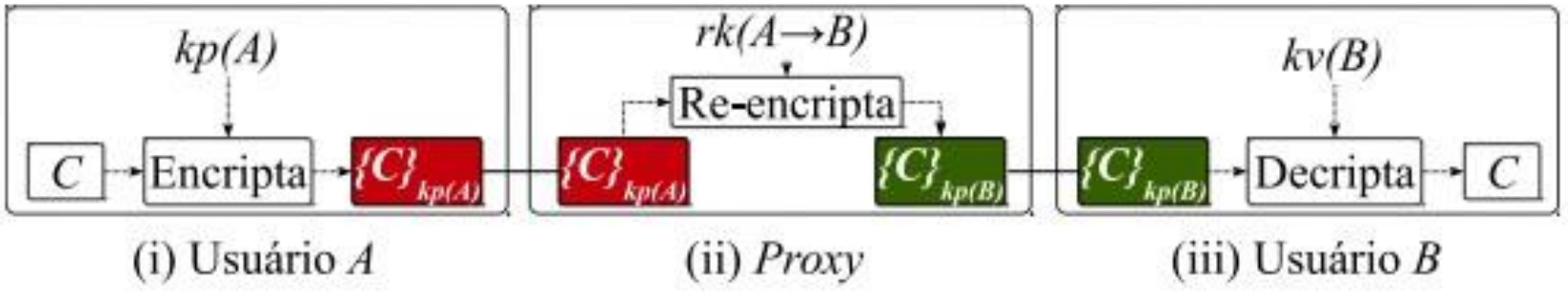

Figura 1. Visão geral do esquema de reencriptação por *proxy*

O usuário **A** encripta um conteúdo **C** com a sua chave pública **kp(A)**, gerando **{C}kp(A)**. Caso o usuário **A** queira permitir que o usuário **B** acesse o conteúdo **C**, ele envia ao proxy o conteúdo **{C}kp(A)** e uma chave de reencriptação **rkA->B**, calculada com base na chave pública **kp(B)** do usuário B. O proxy então utiliza a chave de reencriptação enviada por **A** para reencriptar o conteúdo para **B**, gerando **{C}kp(B)**. O proxy envia o conteúdo **{C}kp(B)** para o usuário **B**, que o decripta utilizando a sua chave privada **kv(B)**.

Reencriptação por *proxy*

- Garantem:
  - o proxy não pode ser capaz de acessar o conteúdo da mensagem que reencripta.
  - de posse da mensagem encriptada e da chave de reencriptação, não pode recuperar as chaves privadas de A ou B.

Reencriptação por *proxy*

- Algoritmos que compõem um esquema de reencriptação por *proxy*:

CONFIGURAÇÃO: recebe como entrada um parâmetro de segurança k e tem como saída uma tupla de parâmetros globais PARAM.

GERAÇÃO DE CHAVES: gera pares de chaves pública-privada (kp, kv).

ENCRIPTAÇÃO: ao receber $kp(A)$ e uma mensagem m, gera uma mensagem encriptada $\{m\}_{kp(A)}$.

DECRIPTAÇÃO: ao receber $kv(A)$ e $\{m\}_{kp(A)}$, gera como saída a mensagem m.

GERAÇÃO DE CHAVE DE REENCRIPTAÇÃO: tem como entrada a chave privada $kv(A)$ e a chave pública $kp(B)$ e como saída uma chave de reencriptação $rk_{A \to B}$.

REENCRIPTAÇÃO: ao entrar a chave de reencriptação $rk_{A \to B}$ e o texto encriptado $\{m\}_{kp(A)}$, tem como saída $\{m\}_{kp(B)}$.

Reencriptação por *proxy*

- Para fundamentar a solução proposta, são necessárias três propriedades fundamentais dos esquemas de reencriptação por *proxy*:

- *Unidirecionalidade*: a delegação de direitos de decriptar de $A \rightarrow B$ não implica na delegação de $B \rightarrow A$;
- *Salto único*: somente mensagens originais podem ser reencriptadas;
- *Segurança contra conluio*: o usuário B e o *proxy* em conluio não conseguem recuperar a chave privada de A.

Controle de acesso usando reencriptação

- Modelo de rede:
  - Arquitetura NDN *(Named-Data Network),* infraestrutura composta por Provedores de conteúdo, Roteadores e Usuários.

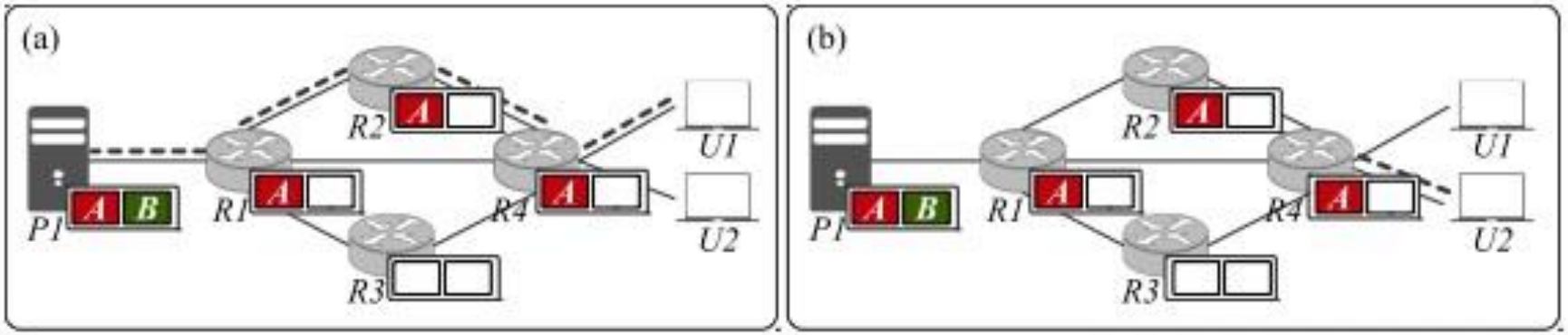

Figura 2. Infraestrutura da arquitetura NDN

Controle de acesso usando reencriptação

- Modelo de ameaças:
  - Considera-se que entidades maliciosas (A) são usuários ilegítimos que não têm acesso ao conteúdo do provedor, ou ainda usuários legítimos que tentam acessar conteúdo ao qual não têm autorização.
  - Eles podem explorar o conteúdo protegido na rede pelas seguintes formas:

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

Controle de acesso usando reencriptação

- Solução proposta dividida em três domínios:
  - Domínio do provedor de conteúdo (encriptação de conteúdo e geração de chaves de reencriptação para usuários)
  - Domínio da rede (roteamento e ao encaminhamento de conteúdo na rede seguindo o paradigma de ICN)
  - Domínio do usuário (composto pela aplicação do provedor de conteúdo e pelas operações de reencriptação e decriptação do conteúdo.)

Controle de acesso usando reencriptação

A seguir, são detalhadas as ações realizadas pelo provedor de conteúdo e pelos usuários para acessar um conteúdo protegido na ICN.

Controle de acesso usando reencriptação

- Encriptação e distribuição de conteúdos (Fig.3a):
- Geração e distribuição da chave de reencriptação (Fig.3b):

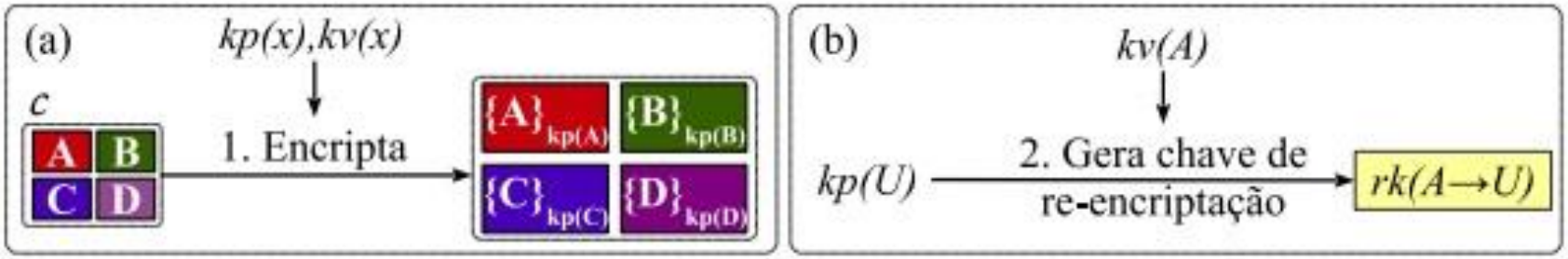

Figura 3. Domínio da fonte: (a) encriptação e (b) geração de chave de reencriptação

Controle de acesso usando reencriptação

- Reencriptação e decriptação de conteúdo:

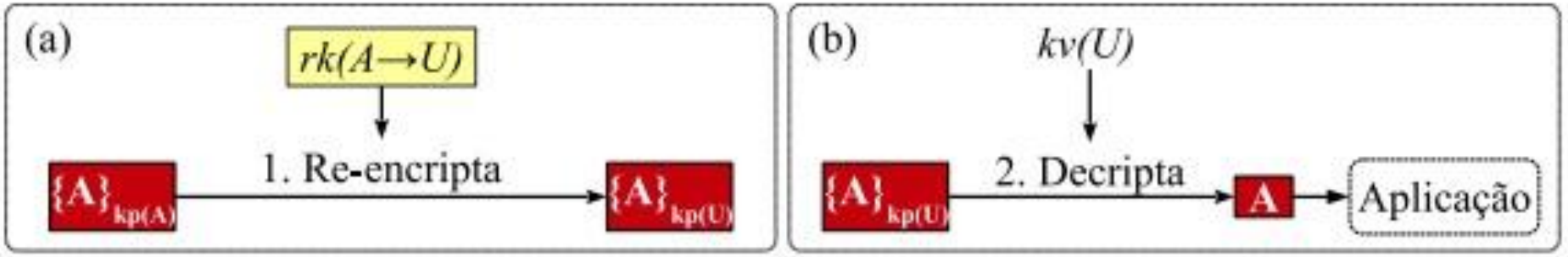

Figura 4. Domínio do usuário: (a) reencriptação e (b) decriptação

Controle de acesso usando reencriptação

- Invalidação da chave de reencriptação:
- uma vez que o usuário U possua a chave de reencriptação rkA→U para o conteúdo A, ele e capaz de decriptar o conteúdo A sempre que desejar.
- qualquer conteúdo que tenha sido encriptado pelo provedor de conteúdo com a mesma chave pública utilizada para encriptar o conteúdo A, kp(A), kv(A) pode ser decriptado por U com a chave rkA→U.

Avaliação

- Para avaliar a viabilidade computacional foi implementado em Python os seis algoritmos do esquema. A métricas adotadas foram o tempo para encriptar e gerar as chaves de reencriptação, que são ações desempenhadas pela fonte, e o tempo para reencriptar e decriptar o conteúdo, ações desempenhadas pelo usuário

Tabela 1. Parâmetros utilizados na avaliação da solução

Parâmetro	Valor	Parâmetro	Valor
Tamanho da chave (k)	1024, 2048 bits	Funções de *hash* H_1, H_3, H_4	mod q
Tamanho da mensagem (ℓ_0)	0.5, 1, 2, 4, 8, 16, 32 Kb	Função de *hash* H_2	mod $2^{(\ell_0+\ell_1)}$
Parâmetro de segurança (ℓ_1)	160 *bits*		

Avaliação

- A Figura 5 apresenta os resultados obtidos com as operações desempenhadas pelo provedor de conteúdo: ENCRIPTAÇÃO e GERAÇÃO DE CHAVES DE REENCRIPTAÇÃO .

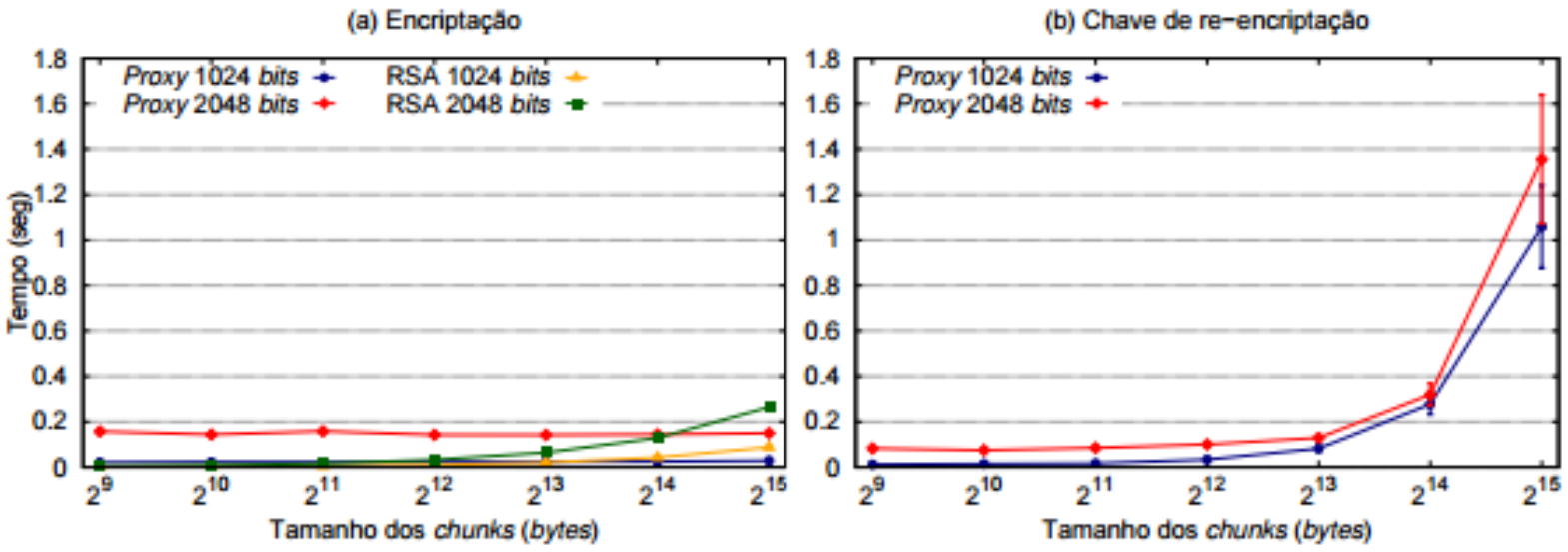

Figura 5. Avaliação da encriptação e da geração de chave de reencriptação

Avaliação

- A Figura 6 apresenta os resultados obtidos com as operações desempenhadas pelo usuário: REENCRIPTAÇÃO e DECRIPTAÇÃO .

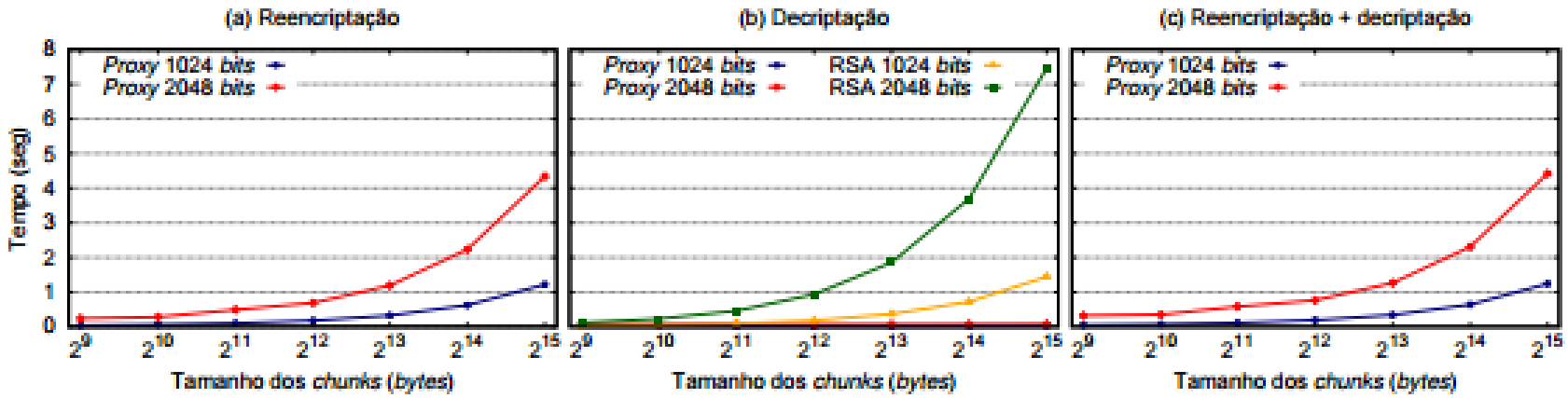

Figura 6. Avaliação da reencriptação e decriptação

Conclusão

- Este trabalho propôs uma solução de controle de acesso baseada em reencriptação por proxy que permite que somente usuários autorizados possam acessar conte údos em uma arquitetura de ICN, mesmo na presença de entidades maliciosas. Além disso, a solução proposta garante os benefícios do uso do cache e não introduz mudanças significativas nos provedores e na rede.

Universidade Tecnológica Federal do Paraná- Câmpus de Pato Branco
Departamento Acadêmico de Informática
Curso de Engenharia de Computação

Controle de acesso baseado em reencriptação por proxy em Redes Centradas em Informação

Autores: Elisa Mannes,
Carlos Maziero,
Luiz Carlos Lassance,
Fabio Borges