Gerenciamento de chaves públicas sobrevivente baseado em grupos para MANETs

Eduardo da Silva
Orientador: Luiz Carlos Pessoa Albini
Coorientador: Aldri Luiz dos Santos

09 de julho de 2009

Roteiro

- Introdução
- Ataques em MANETs
- Gerenciamento de chaves
- PGP-Like
- SG-PKM
- Avaliação
- Conclusões

Parte I

Contextualização

Redes ad hoc móveis

- Formadas **dinamicamente**
- Cada nó se comunica diretamente com outros nós
  - que estão dentro do raio de alcance da sua antena
- **Próprios nós** devem agir como **roteadores** das mensagens
- Herdam todos as características das redes sem fio com infraestrutura
- Acrescentam novas características:
  - Autonomia
  - Roteamento multissalto
  - Mobilidade
  - Restrição de energia

Desafios das redes ad hoc móveis I

- Sem infraestrutura:
  - Protocolos utilizados devem ser **completamente distribuídos**
- Sem centralização:
  - **Dificulta** toda a gerência da rede, como detecção de falhas, distribuição de certificados e chaves, e outros
  - Devem ser distribuídas
- Topologia dinâmica:
  - Mudanças na topologia da rede são muito **frequentes** e **imprevisíveis**

Desafios das redes ad hoc móveis II

- Possuem diversos problemas de **segurança**
  - Herdam todos os problemas de segurança das redes com fio e das redes sem fio com infraestrutura
  - **Adicionam** os seus próprios
  - Não é possível a criação de um “ambiente gerenciado”
  - Segurança também deve ser distribuída
- São altamente **vulneráveis** a ataques (passivos e ativos)

Exemplos de tipos de ataques

Camada	Ataque	Descrição
Física	Ruído	interferência no sinal transmitido
Enlace	Colisão	colisões propositais
Rede	*Wormhole*	criação de um canal paralelo de baixa latência
	Blackhole	exclusão dos pacotes para ser roteados
	Grayhole	descarte selectivo de pacotes
Transporte	Inundação de SYN	inundação de pacotes TCP SYN
Várias	Exaustão	retransmissões sucessivas
	DoS Distribuído	vários nós tentando negar/denegrir os serviços
	Egoísmo	**não cooperação nas atividades**
	Sybil	**criação de identidades falsas**

Por que esses ataques?

- Serviços distribuídos dependem da **cooperação** dos nós
- Nós egoístas podem comprometer a **eficiência** desses serviços
- Esquemas de **gerência de chaves** devem ser eficientes mesmo diante de ataques de falta de cooperação (egoísmo)

- Em um ataque Sybil:
  - nó malicioso possui várias identidades
  - compromete a **confiabilidade** de sistemas, como m-commerce e armazenamento distribuído
- Esquemas de gerência de chaves **eficazes** devem conter esse tipo de ataque

Funções do gerenciamento de chaves I

- **Inicializar** os usuários do sistema na rede
- Quanto ao **material criptográfico** (pares de chaves pública e privada, os parâmetros de inicialização e os parâmetros não secretos):
  - gerar, distribuir e instalar
  - armazenar e recuperar
  - controlar o uso
  - fazer a inicialização e manutenção da confiança

Nas MANETs

- Considerar a mobilidade e a topologia dinâmica
- Ser auto-organizado e descentralizado

Classificação dos esquemas de gerenciamento de chaves

- Centralizados
- Parcialmente distribuídos e gerenciados
- Parcialmente distribuídos e auto-organizados
- Distribuídos e gerenciados
- **Distribuídos e auto-organizados**

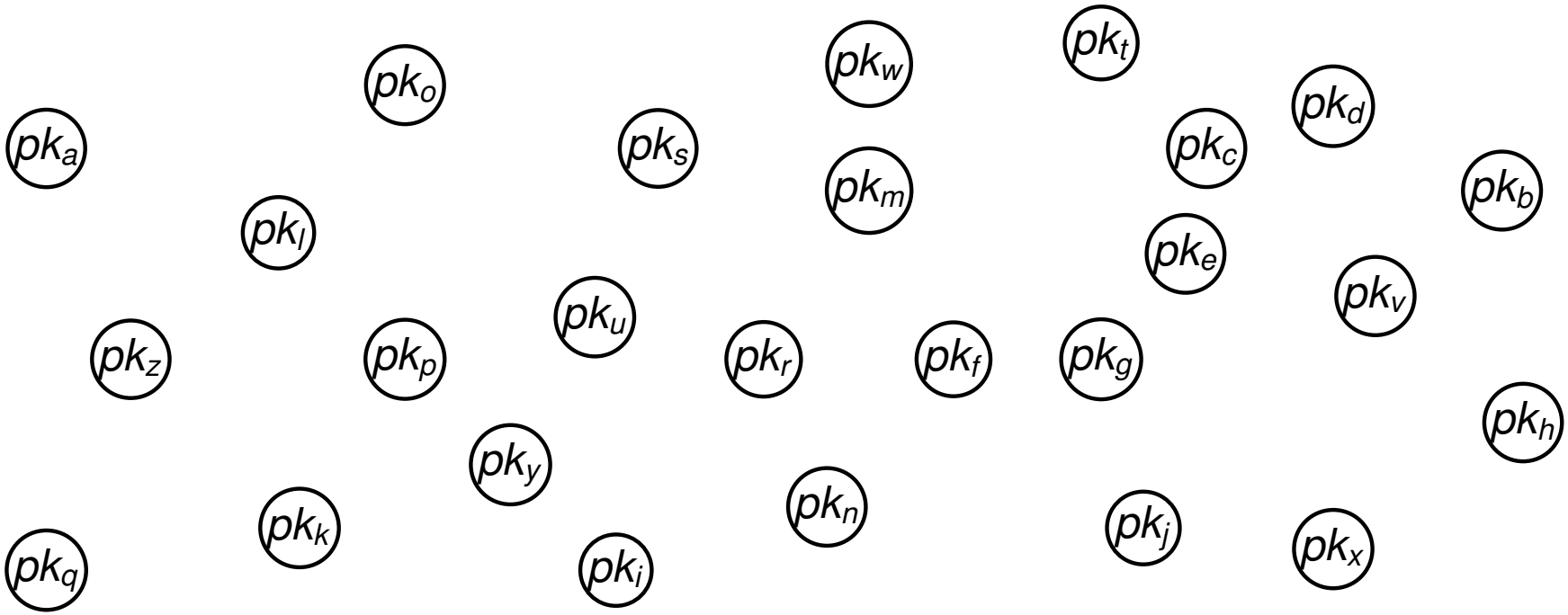
Parte II

Gerenciamento de chaves públicas auto-organizado para MANETs (PGP-Like)

PGP-Like

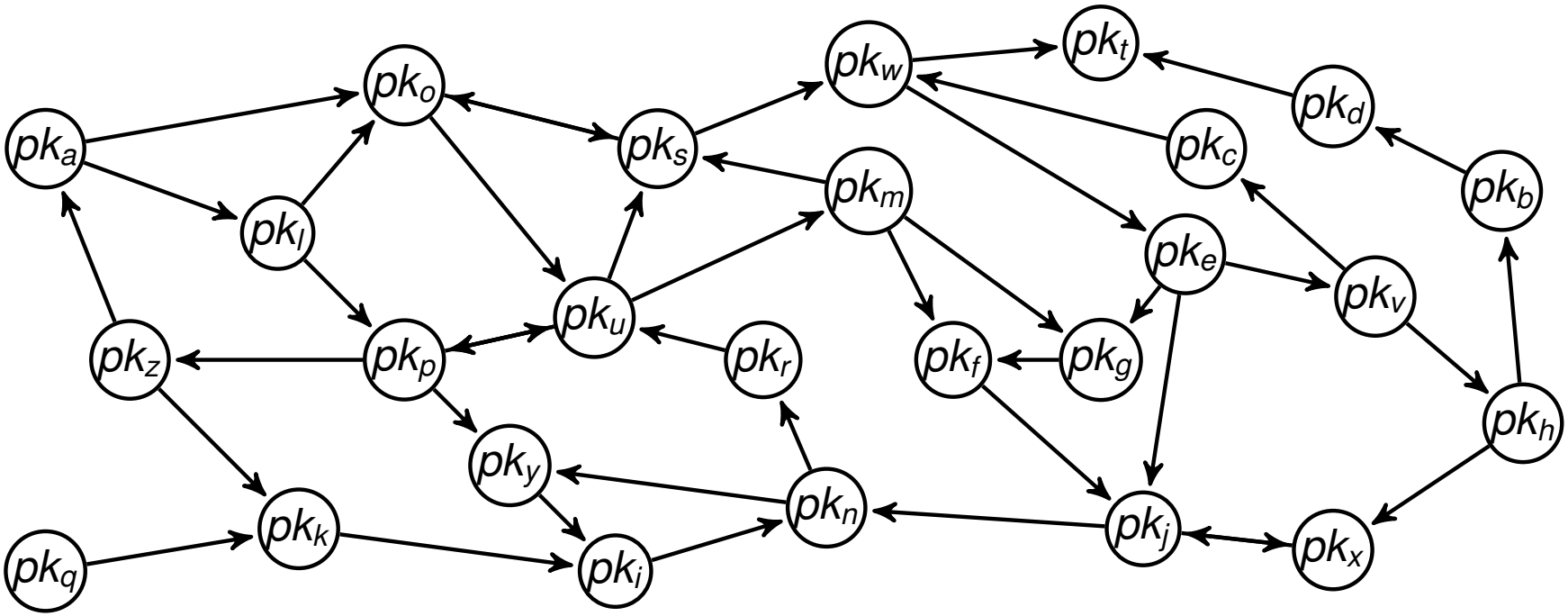
- Inspirado nas **ideias** do PGP
  - PGP foi criado 1991 por Philip Zimmermann
  - É um padrão para a **criptografia** e **proteção** de correio eletrônico na Internet
- Criado em 2003 por integrantes do projeto Terminodes
- Objetivo:
  - fornecer um serviço de gerência de chaves **auto-organizado** e **distribuído** para MANETs

PGP-Like - Funcionamento



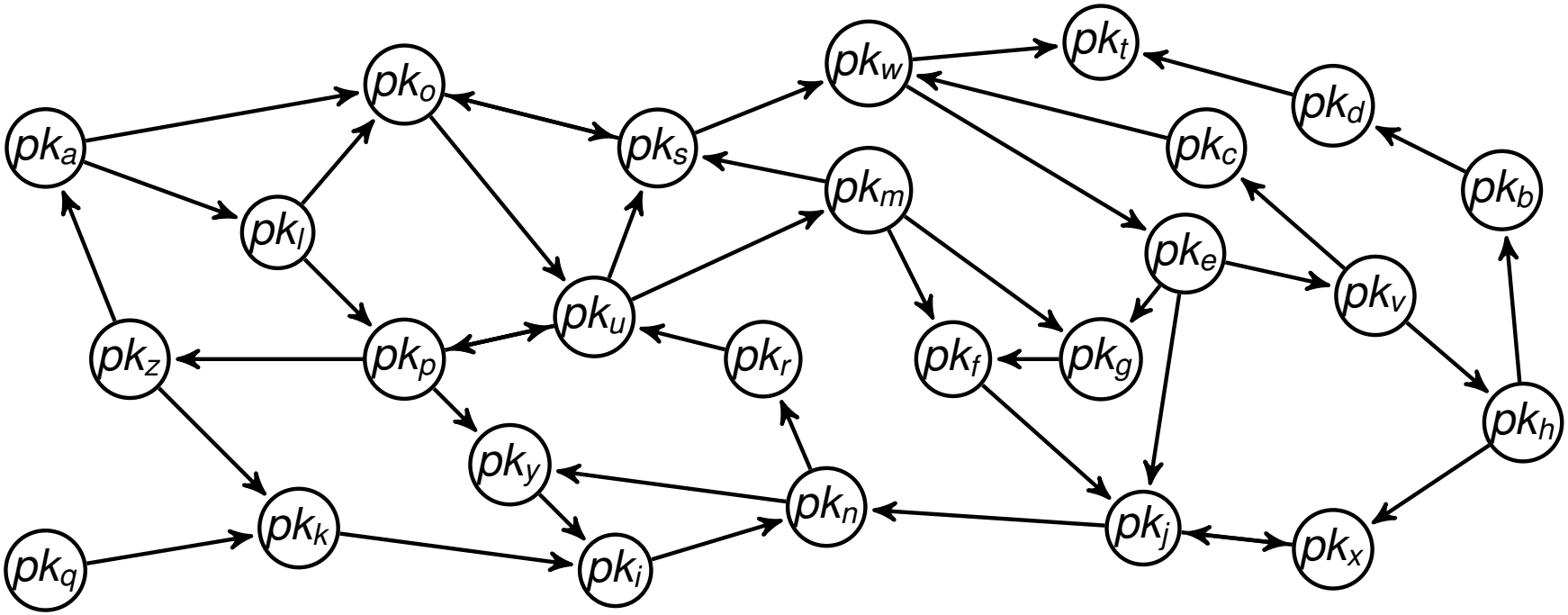
- Baseado nos conceitos do PGP
- Cada nó gera seu próprio par de chaves

PGP-Like - Funcionamento



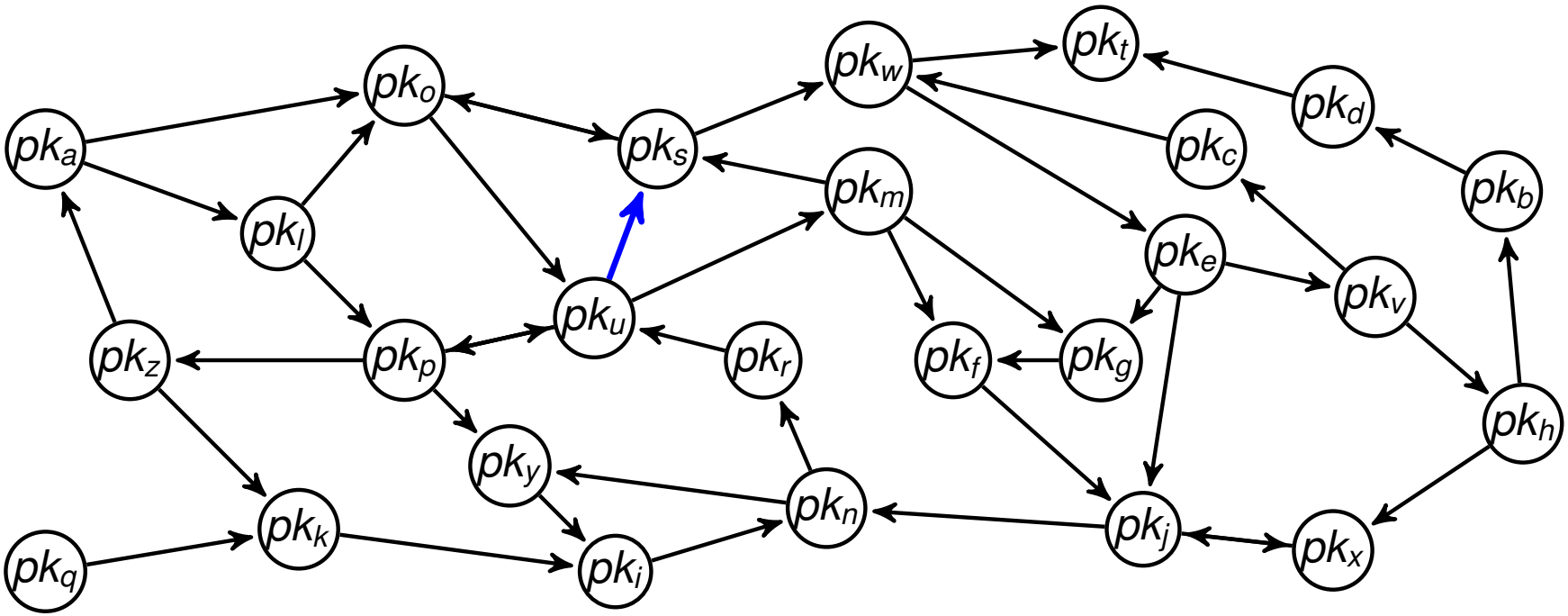
- Baseado nos conceitos do PGP
- Cada nó gera seu próprio par de chaves
- Emitem certificados para os nós que confiam

PGP-Like - Funcionamento



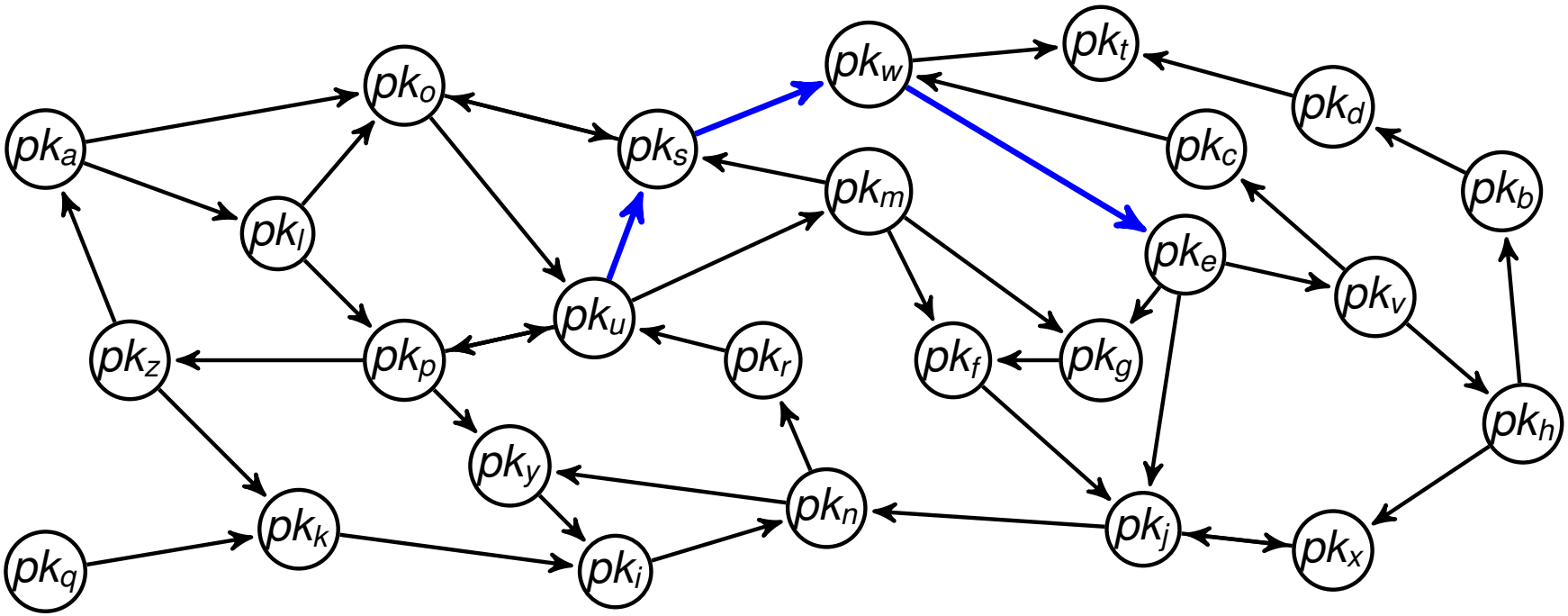
- Chaves públicas e certificados
  - Representados por um grafo direcionado $G = (V, A)$
  - V: Chaves públicas dos nós
  - A: Certificados

PGP-Like - Funcionamento



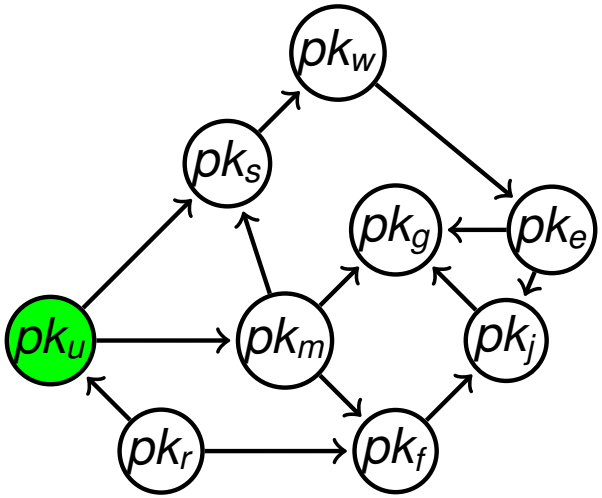
- Aresta direcionada entre dois vértices ($pk_u \rightarrow pk_s$):
  - certificado assinado com SK_u associando pk_s ao nó x_s

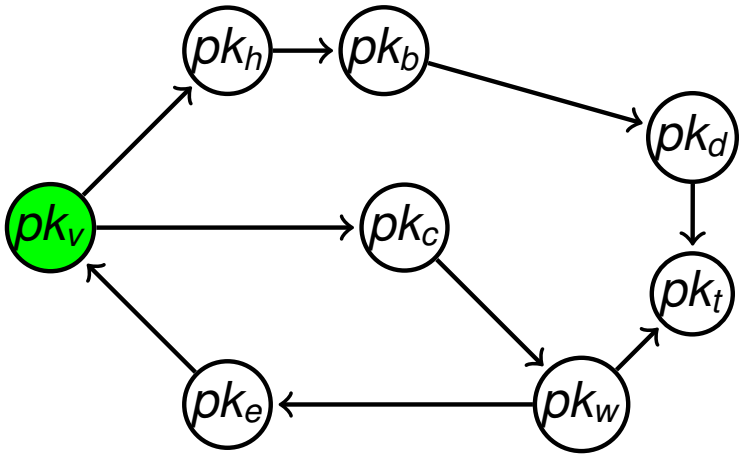
PGP-Like - Funcionamento



- Aresta direcionada entre dois vértices ($pk_u \rightarrow pk_s$):
  - certificado assinado com SK_u associando pk_s ao nó x_s
- Caminho conectando dois vértices ($pk_u \rightsquigarrow pk_e$):
  - cadeia de certificados de pk_u até pk_e

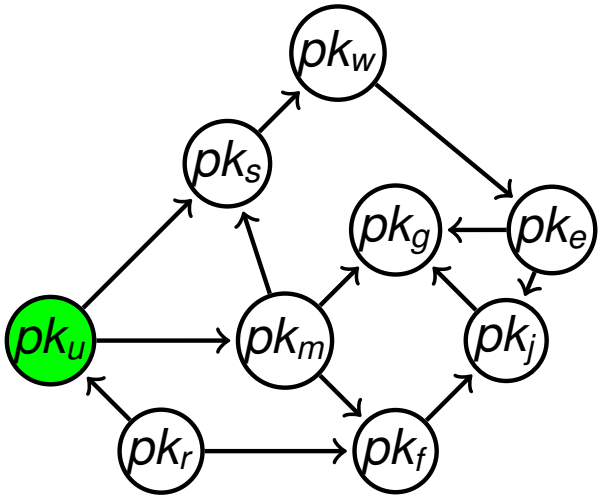
PGP-Like - Autenticação

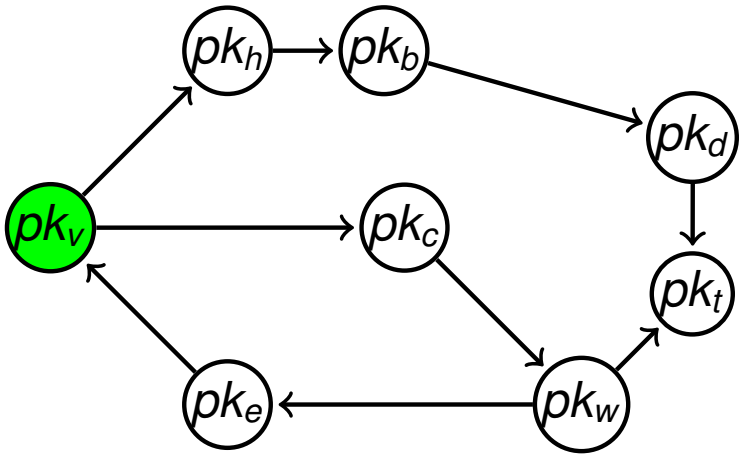




- Cada nó x_u
  - troca certificados com os seus vizinhos
  - possui dois repositórios:
    - repositório de certificados atualizados (G_u)
    - repositório de certificados não-atualizados (G_u^N)

PGP-Like - Autenticação

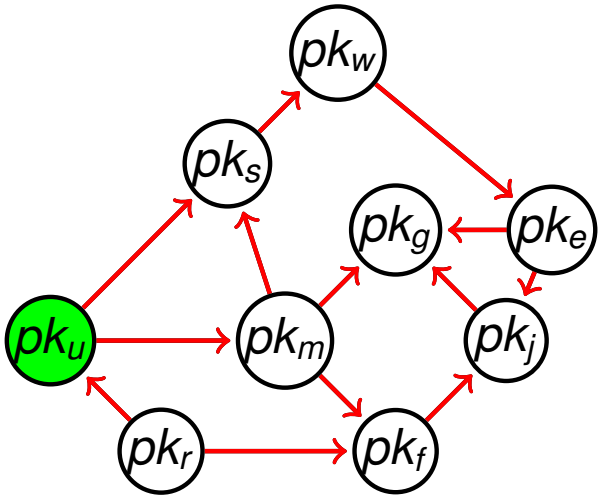


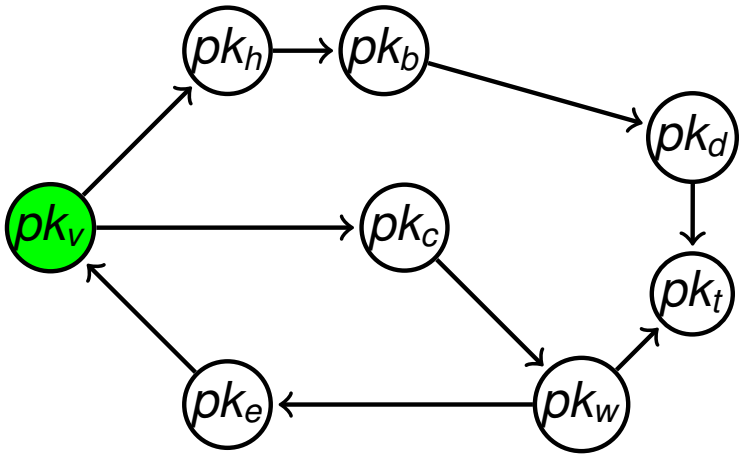


Nó x_u deseja verificar se pk_v pertence ao nó x_v:

- Procura um caminho conectando:
  - pk_u e pk_v em G_u

PGP-Like - Autenticação

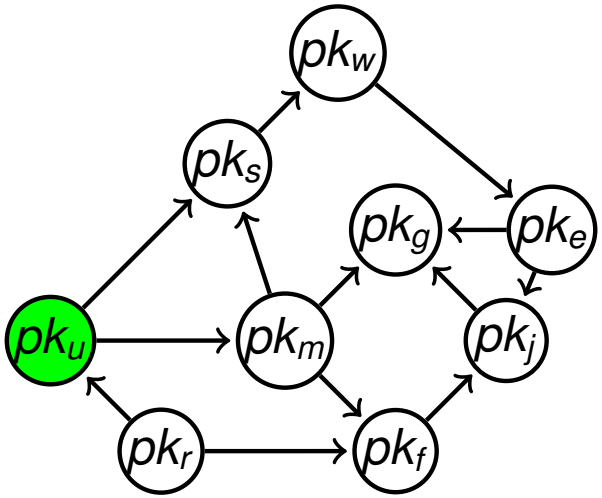


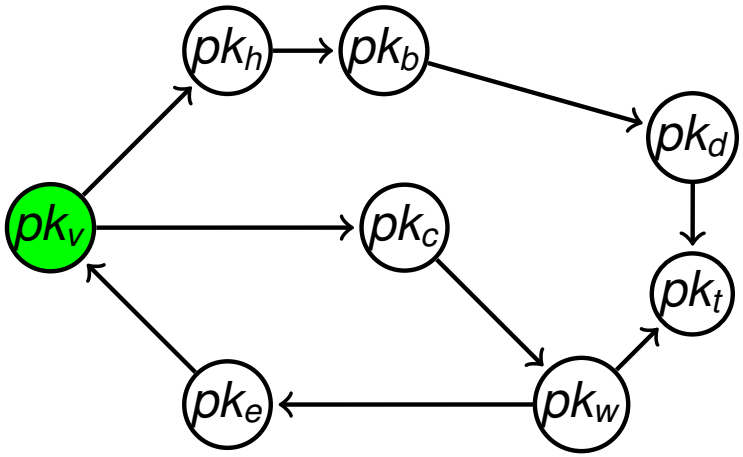


Nó x_u deseja verificar se pk_v pertence ao nó x_v:

- Procura um caminho conectando:
  - pk_u e pk_v em G_u

PGP-Like - Autenticação

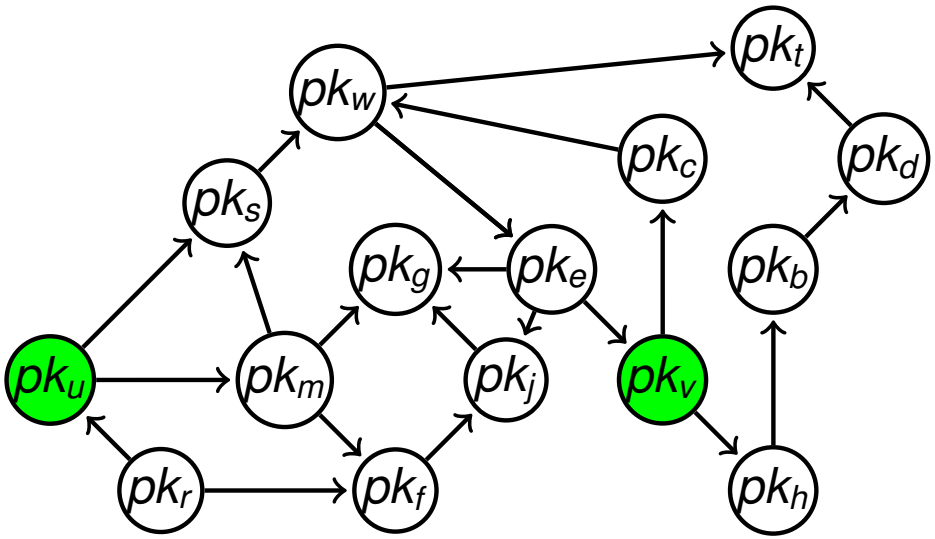




Nó x_u deseja verificar se pk_v pertence ao nó x_v:

- Procura um caminho conectando:
  - pk_u e pk_v em G_u
  - caso não exista, pk_u e pk_v em $(G_u \cup G_v)$

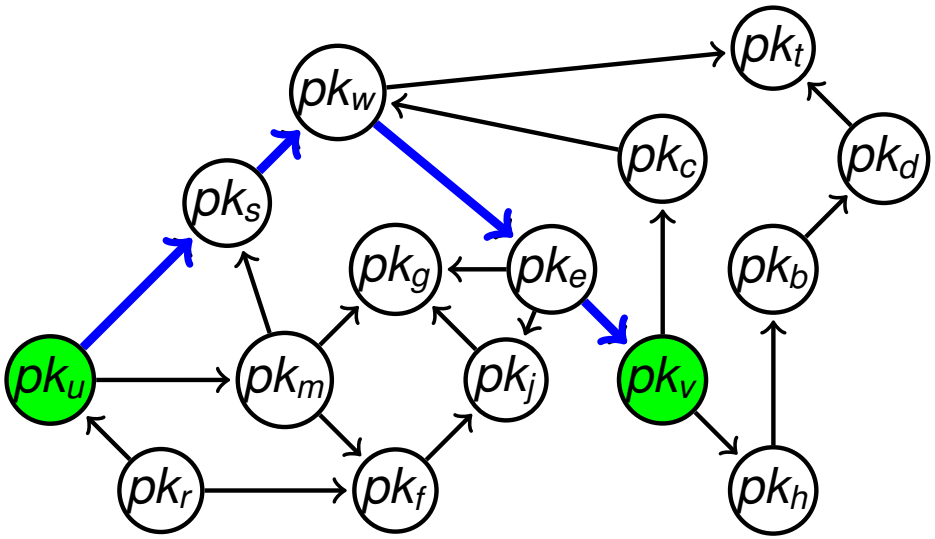
PGP-Like - Autenticação



Nó x_u deseja verificar se pk_v pertence ao nó x_v:

- Procura um caminho conectando:
  - pk_u e pk_v em G_u
  - caso não exista, pk_u e pk_v em $(G_u \cup G_v)$

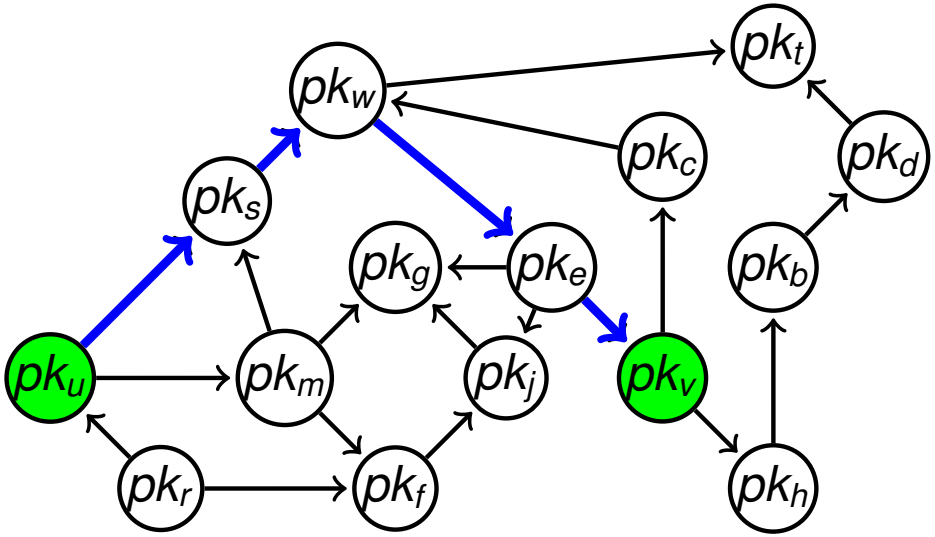
PGP-Like - Autenticação



Nó x_u deseja verificar se pk_v pertence ao nó x_v:

- Procura um caminho conectando:
  - pk_u e pk_v em G_u
  - caso não exista, pk_u e pk_v em $(G_u \cup G_v)$

PGP-Like - Autenticação



Nó x_u deseja verificar se pk_v pertence ao nó x_v:

- Procura um caminho conectando:
  - pk_u e pk_v em G_u
  - caso não exista, pk_u e pk_v em $(G_u \cup G_v)$
  - caso não exista, pk_u e pk_v em $(G_u \cup G_u^N)$
    - verifica os certificados não-atualizados os seus **emissores**

Métricas para a avaliação

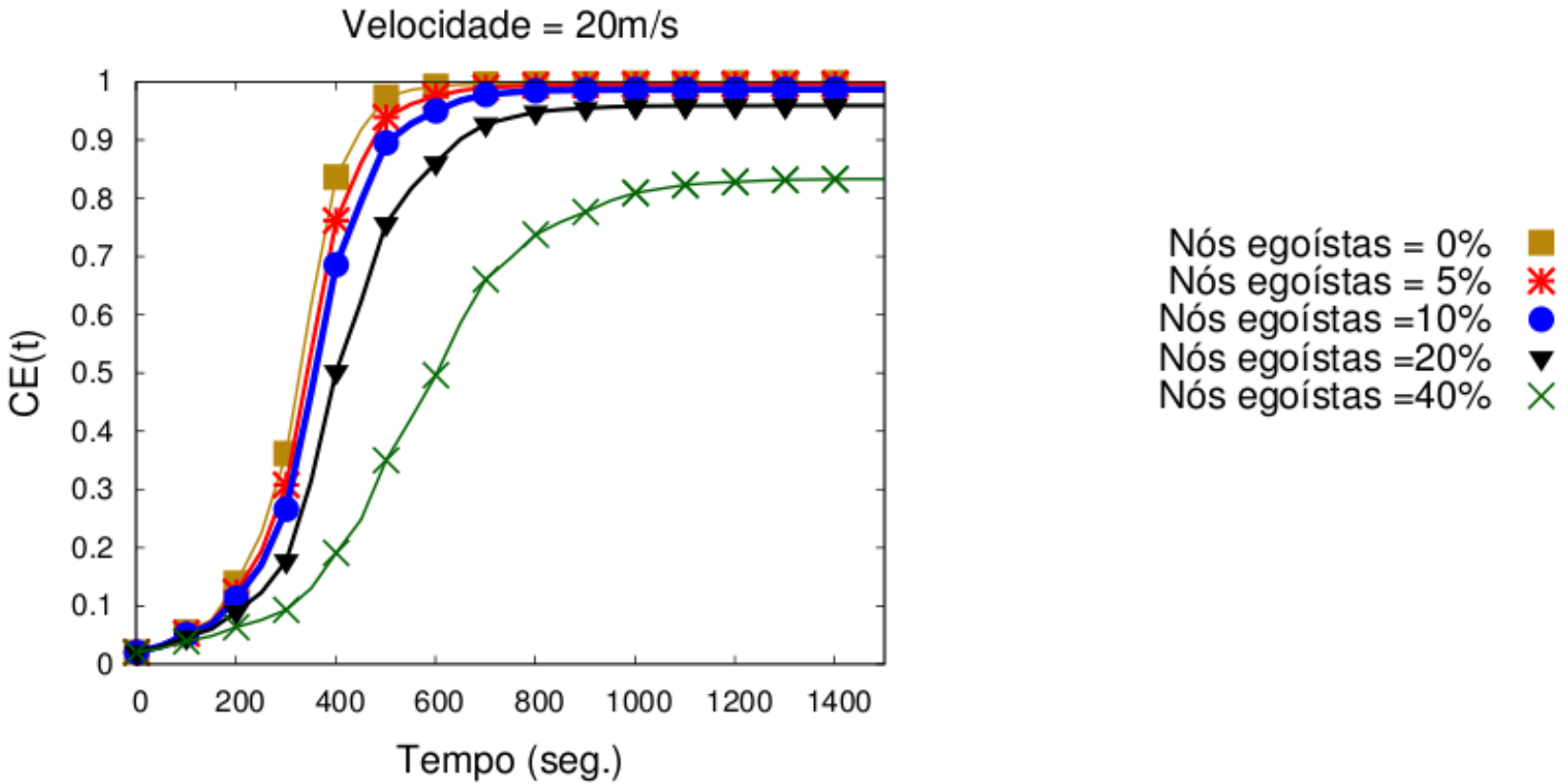
- Convergência das trocas de certificados (CE)
- Alcançabilidade dos nós (UR)

- *Confiabilidade em uma identidade falsa (FIC)*
- *Autenticação indireta de falsas identidades (IA)*
- *Certificados suspeitos por repositório (SC)*

Simulações no NS-2

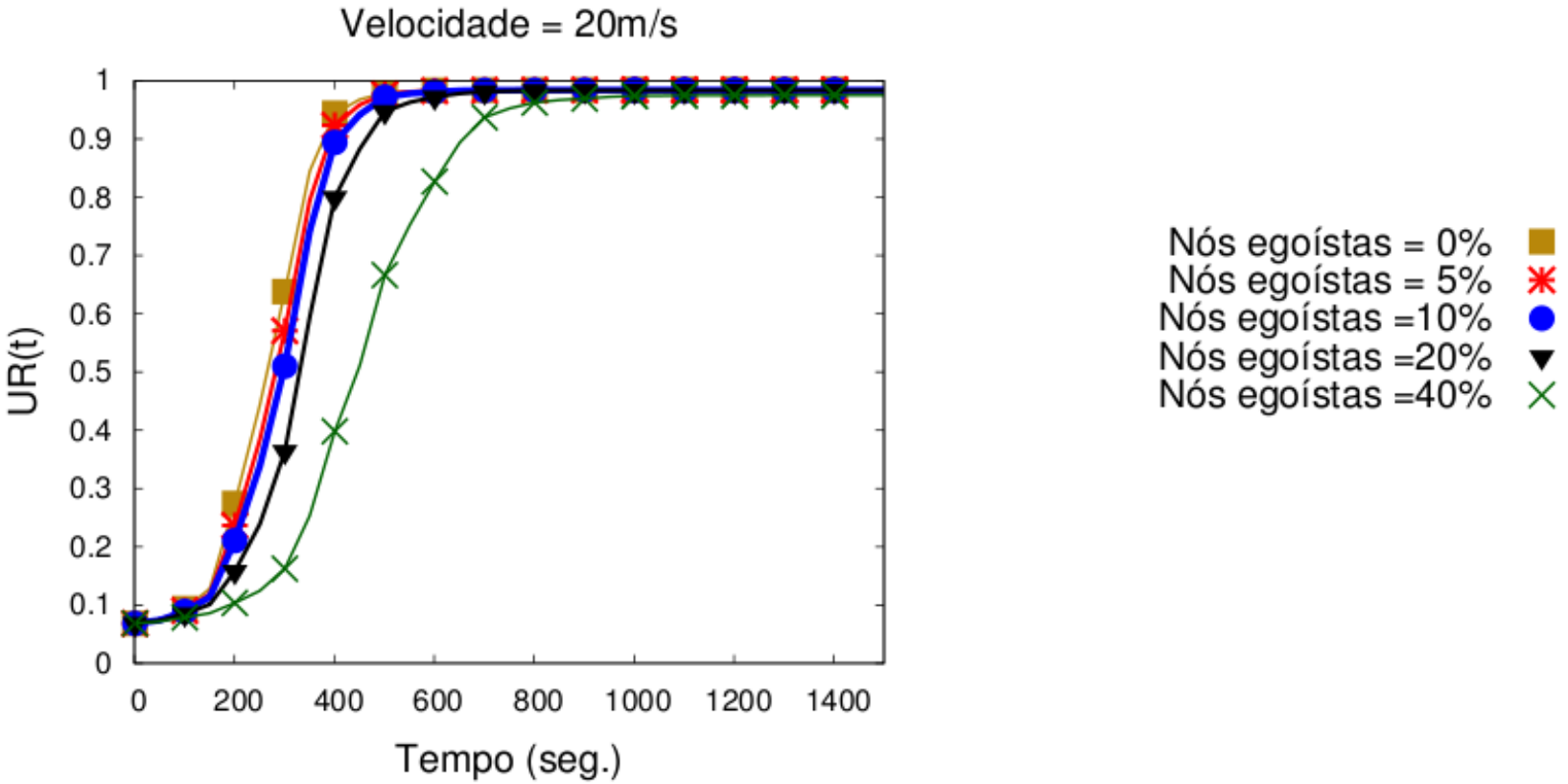
Parâmetro	**Valores utilizados**
Raio de alcance	50 e 120 metros
Quantidade de nós	100 nós
Tamanho do ambiente	1000 x 1000 metros 1500 x 300 metros
Tipo de movimentação	*waypoint* aleatório
Velocidades máximas	5, 10 e 20 m/s
Tempo máximo de pausa	20 segundos
Tempo entre troca de certificados	60 segundos
Quantidade de certificados emitidos	600 certificados
Percentual de atacantes	*5, 10, 20 e 40%*
Tempo de simulação	10000 segundos

Convergência das trocas de certificados



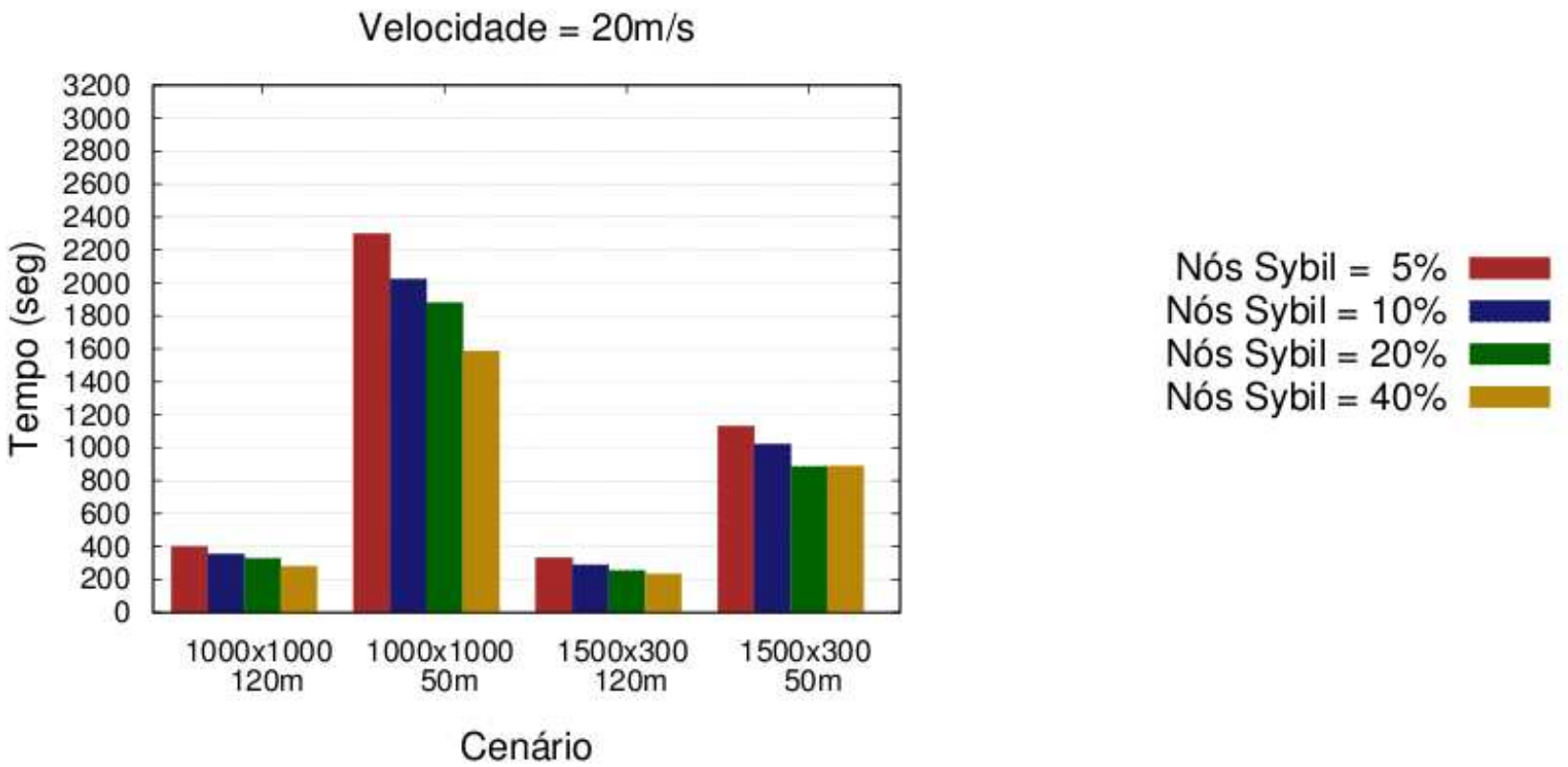
OBS: Apresentados os resultados com velocidade de 20 m/s, raio de alcance de 120 m e tamanho do ambiente do 1000x1000 metros

Alcançabilidade dos nós

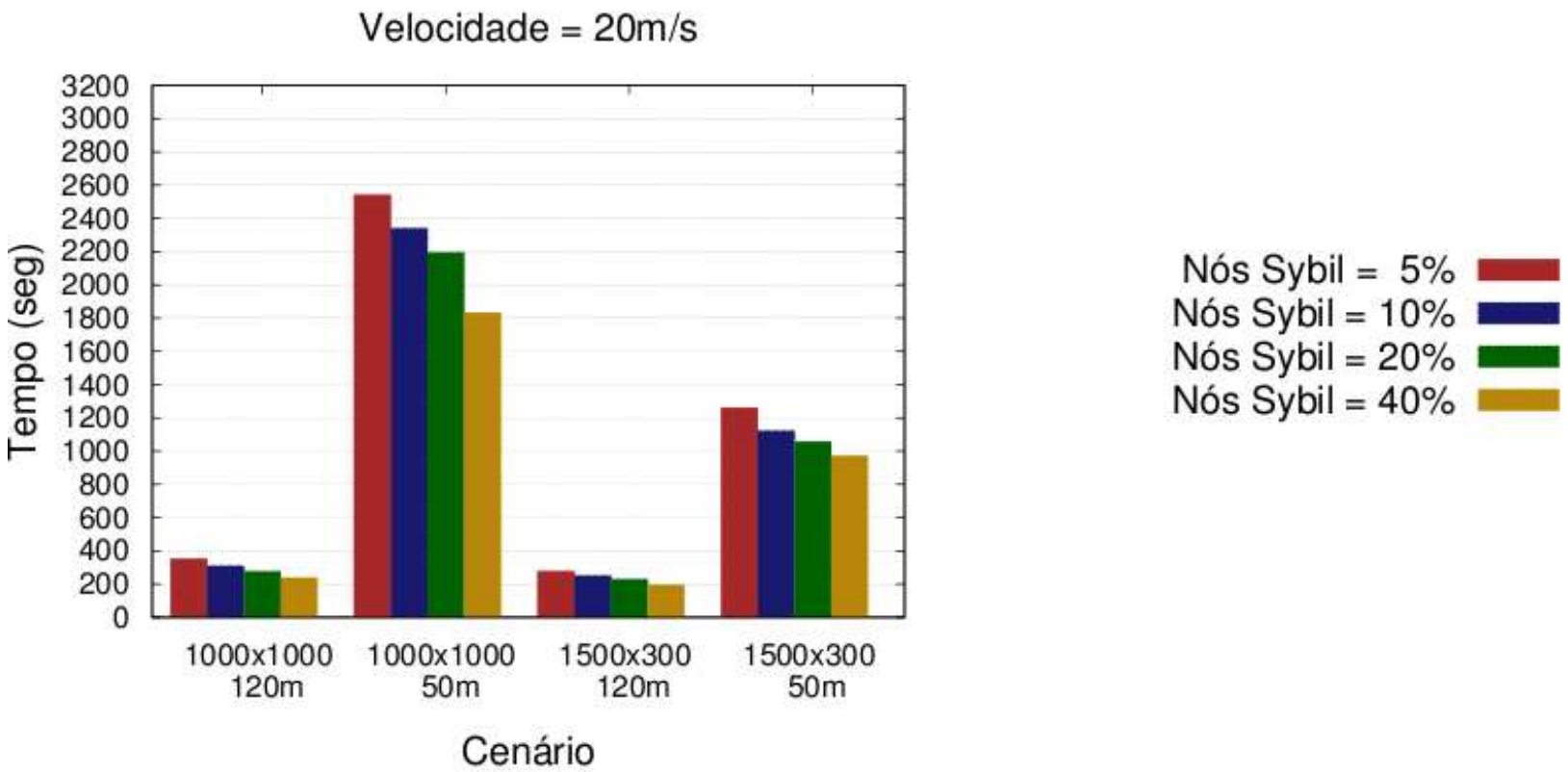


OBS: Apresentados os resultados com velocidade de 20 m/s, raio de alcance de 120 m e tamanho do ambiente do 1000x1000 metros

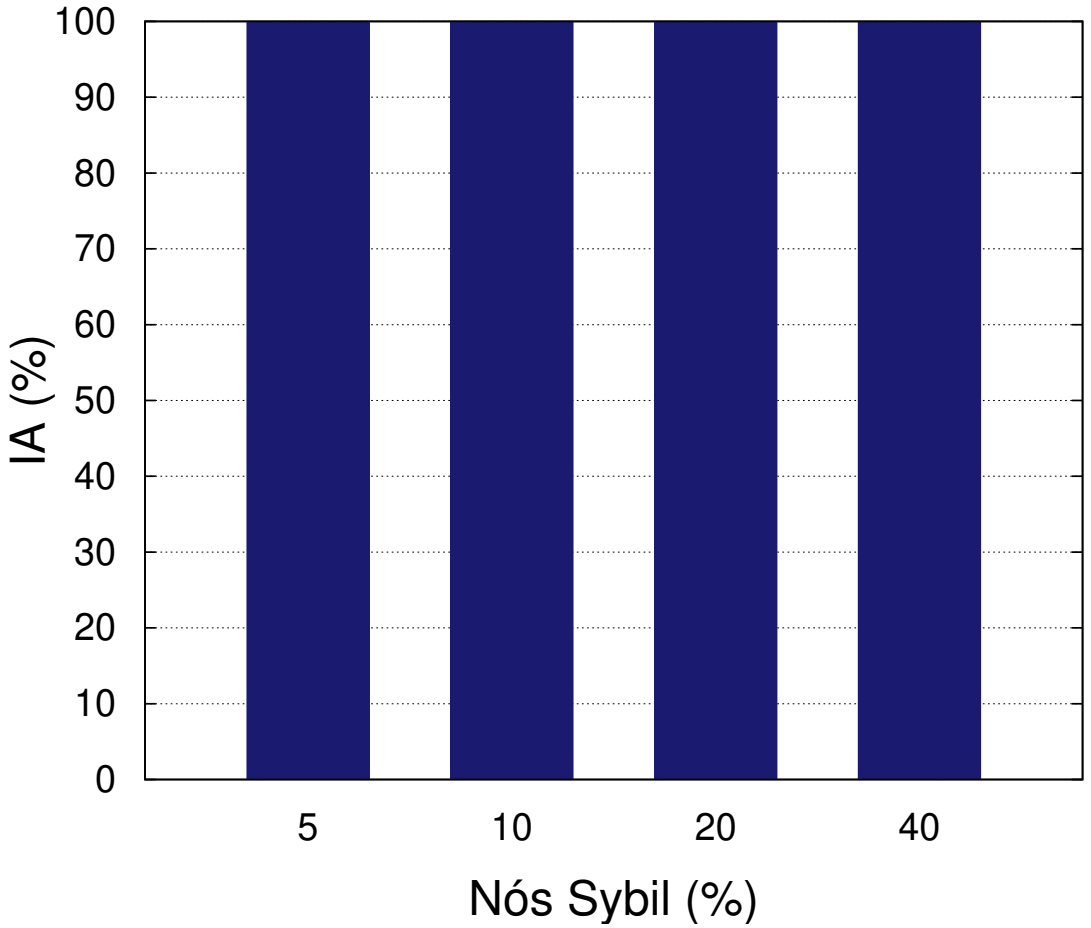
Confiança em identidades falsas – pré-convergência



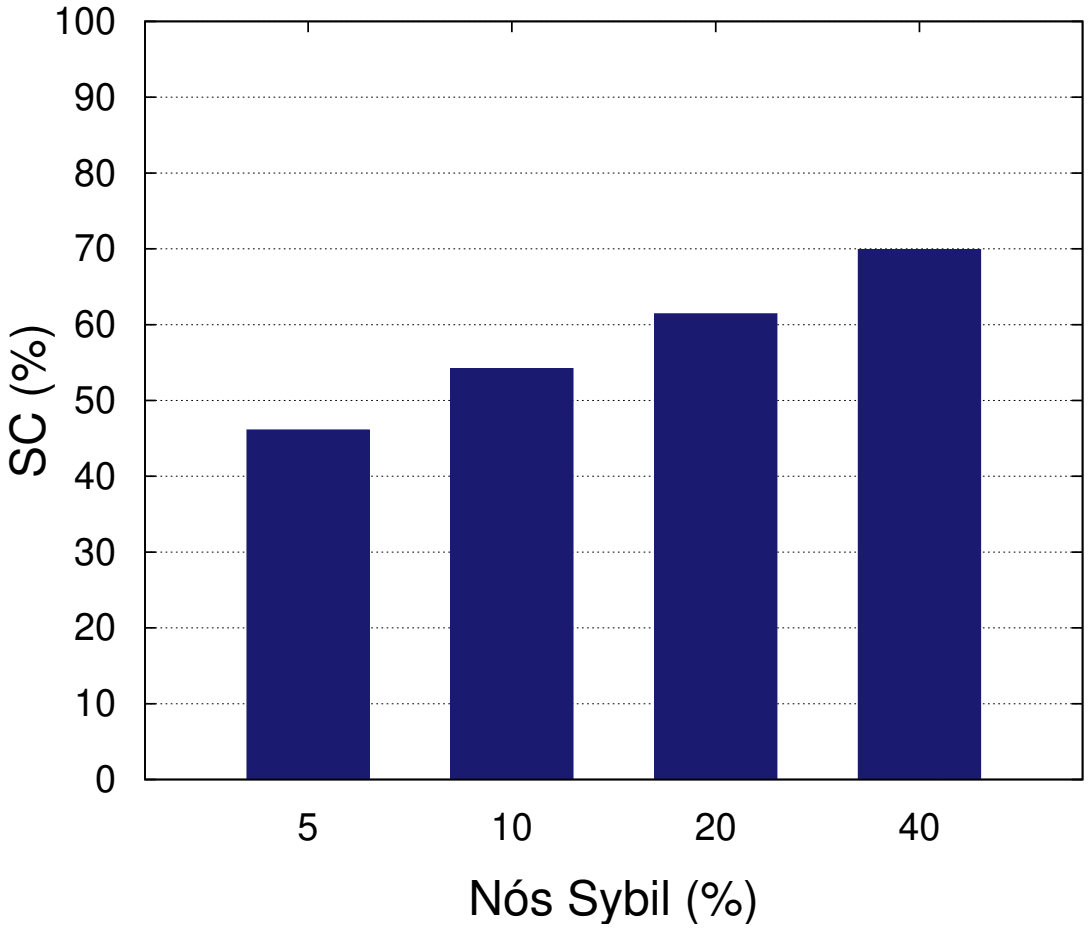
Confiança em identidades falsas – pós-convergência



Autenticação indireta das identidades falsas



Certificados suspeitos nos repositórios locais



Considerações sobre o PGP-Like

Sob ataques de falta de cooperação

- O PGP-Like mantém a sua eficácia
- O número de nós egoístas afeta:
  - quantidade de certificados nos repositórios
  - tempo de convergência

Sob ataques Sybil

- Ele é completamente vulnerável
- Comprometidos mesmo diante de 5% de nós maliciosos

Parte III

Gerenciamento de chaves públicas sobrevivente baseado em grupos para MANETs (SG-PKM)

Objetivos I

Objetivo

- Propor um esquema de gerenciamento de chaves públicas para MANETs baseado em grupos
  - Sobrevivente a ataques
  - Mantenha o seu desempenho diante de ataques de falta de cooperação
  - Seja eficaz diante de ataques *Sybil*

Objetivos II

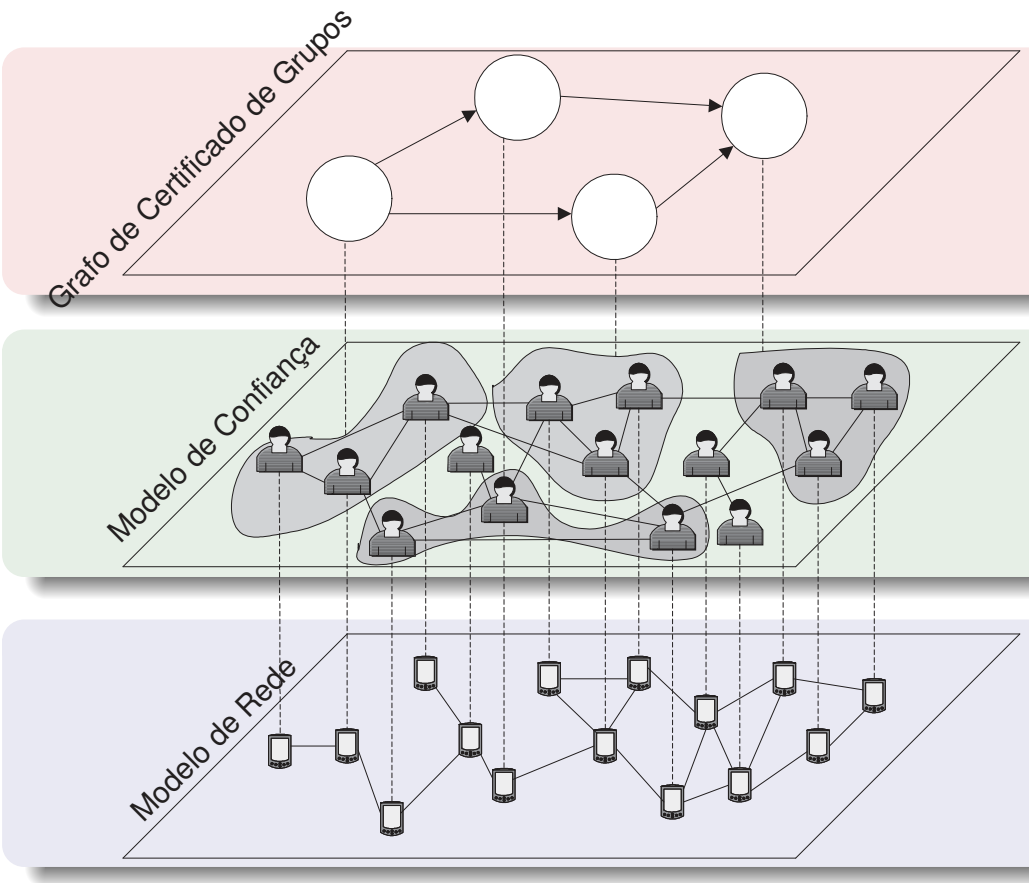
Objetivos específicos

1. *levantar as **fraquezas** e **vulnerabilidades** do PGP-Like*
2. *elaborar **métricas** e quantificar o impacto dos ataques de falta de cooperação e Sybil no PGP-Like*
3. propor um **novo esquema** de gerenciamento de chaves
4. definir métricas para a avaliação desse esquema diante dos ataques de falta de cooperação e Sybil
5. **avaliar** o novo esquema em cenários com ataques de falta de cooperação e Sybil

Objetivos do SG-PKM

- Ser totalmente **distribuído**
- Ser auto-organizado
- Manter o **desempenho** na presença de ataques de falta de cooperação
- Ser **eficaz** diante de ataques Sybil

Visualização em camadas do SG-PKM

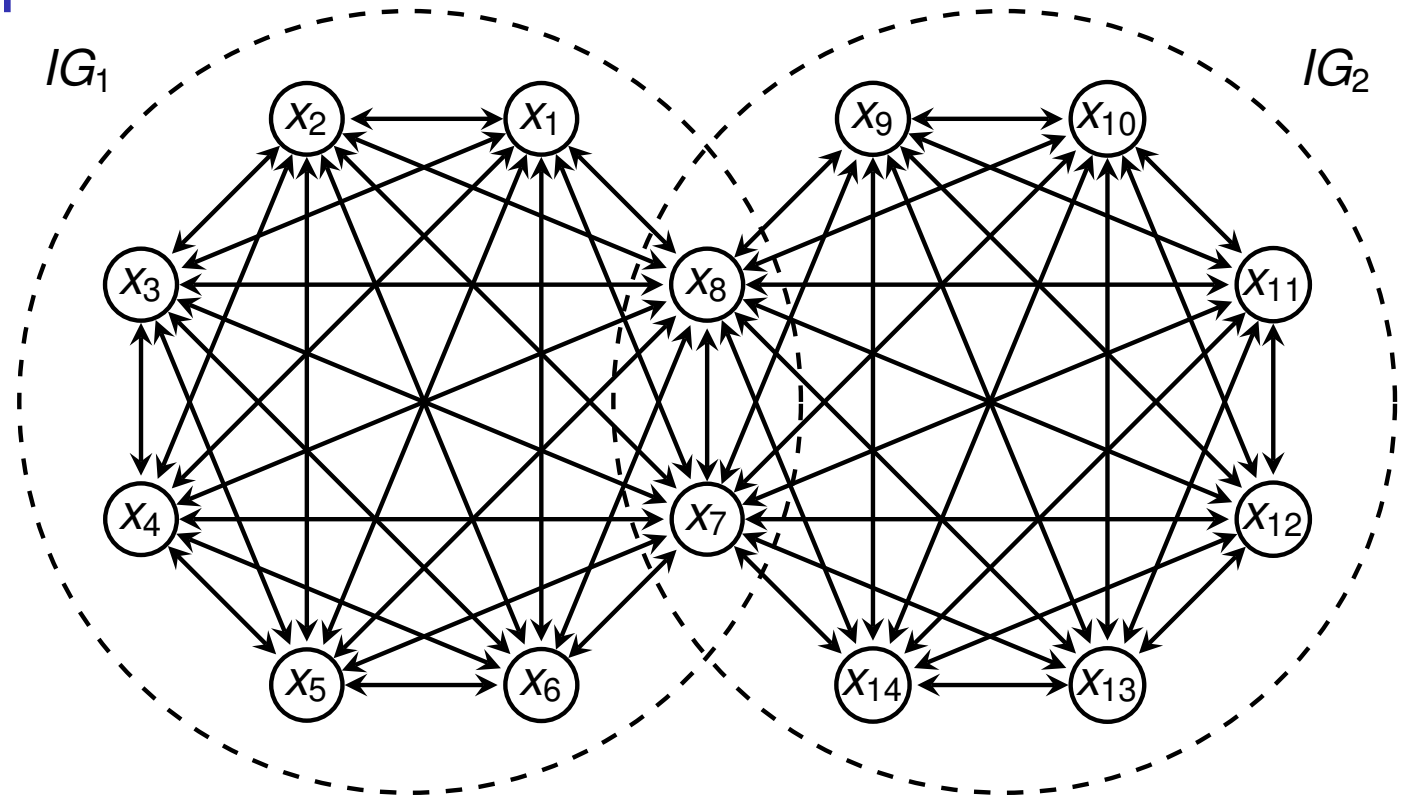


grupos formados pelos nós do sistema

relações de confiança e amizade entre os nós

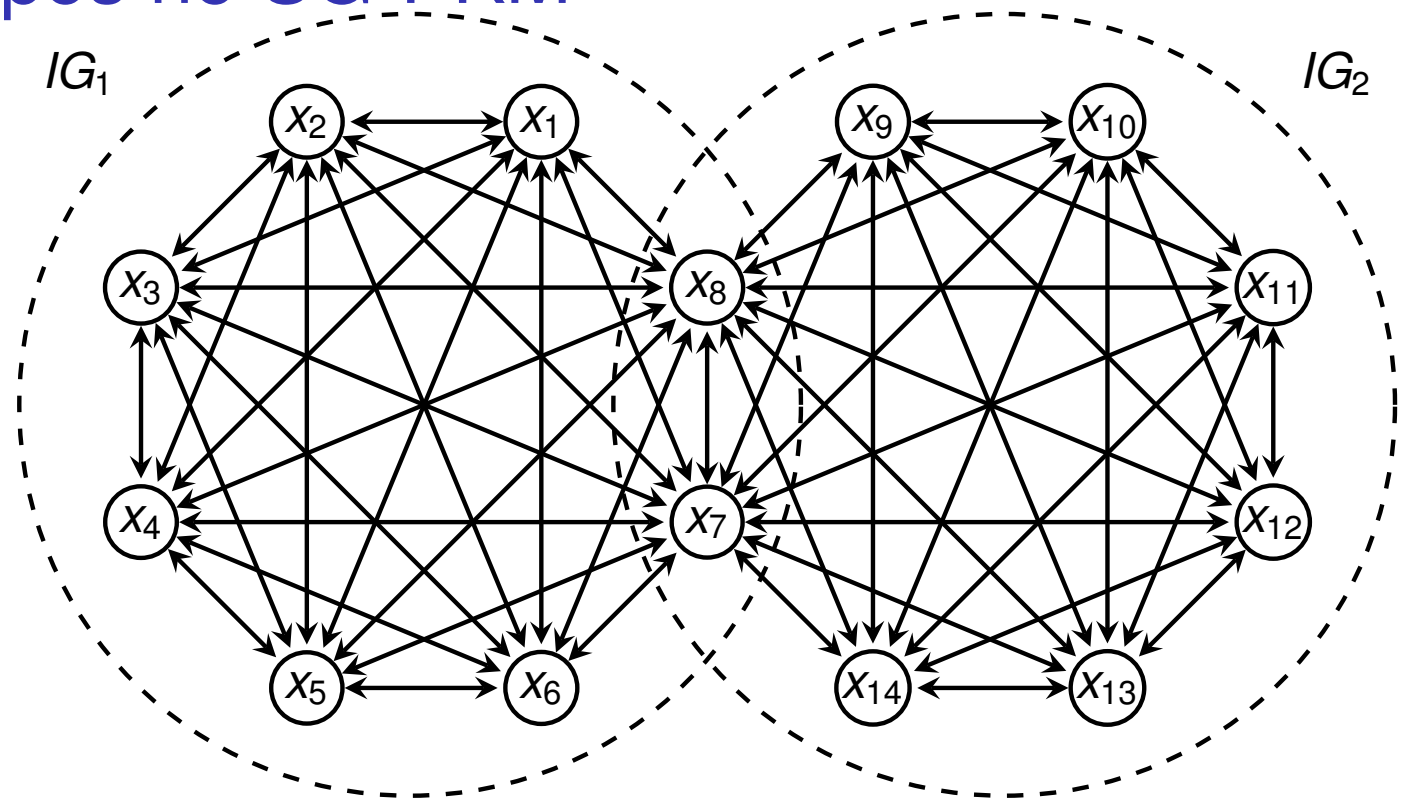
ligações físicas entre dois nós

Os grupos no SG-PKM



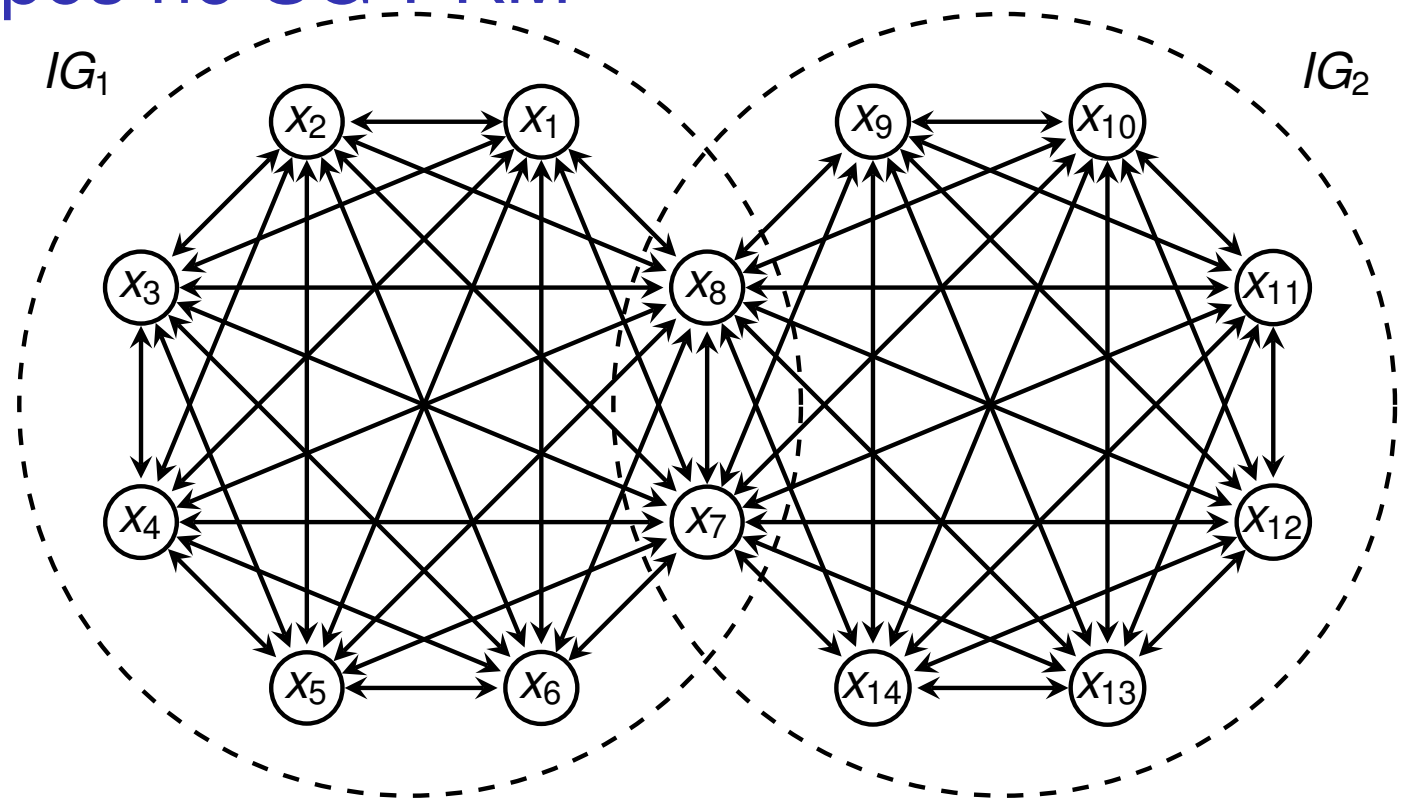
- Nó deseja entrar no sistema
  - Forma um grupo com outros $m - 1$ nós
  - Não é necessário um “líder”

Os grupos no SG-PKM



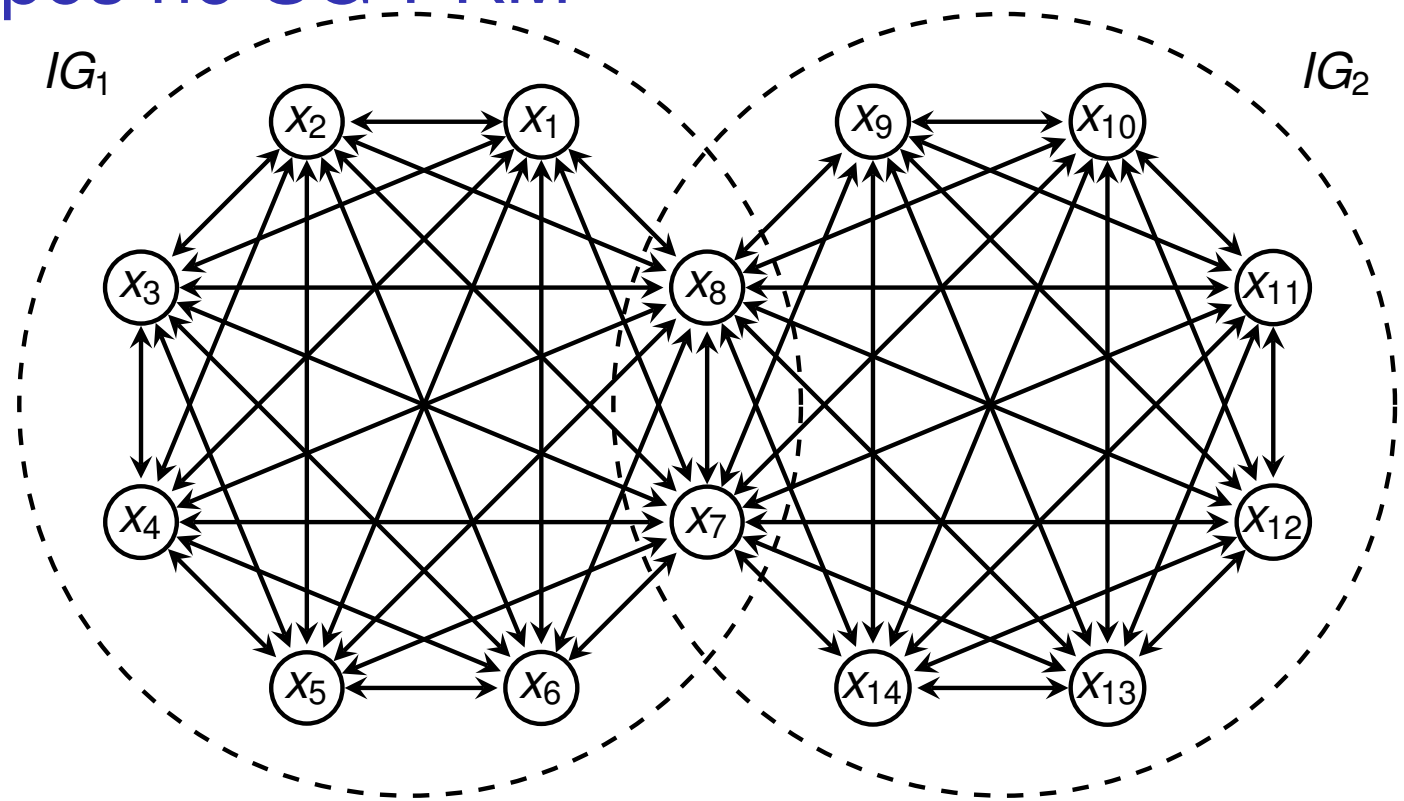
- Nós constroem as chaves pública e privada do grupo
  - Chave pública: disponibilizada a todos
  - Chave privada: distribuída em um esquema de criptografia de limiar (t, m)

Os grupos no SG-PKM



- Identificação do grupo $IG_\alpha = \mathcal{H}(x_1 \| x_2 \| ... \| x_n)$
- Chave pública do grupo $IG_\alpha \Longrightarrow PK_\alpha$
- Chave privada do grupo $IG_\alpha \Longrightarrow SK_\alpha$

Os grupos no SG-PKM



- Cada nó x_u:
  - troca certificados com os seus vizinhos
  - possui dois repositórios:
    - repositório de certificados de grupos atualizados (G_u)
    - repositório de certificados de grupos não-atualizados (G_u^N)

Autenticação

Nó x_u deseja autenticar a chave pública pk_v de x_v

- Nó x_v apresenta um certificado ao x_i
  - certificado $C^{x_v}_{SK_\gamma}$ assinado com a chave privada do grupo IG_γ
- Nó x_u utiliza a chave pública PK_γ para verificar a autenticidade do certificado apresentado
- Mas como saber se a chave pública PK_γ é válida?

Autenticação

Nó x_u deseja autenticar a chave pública pk_v de x_v

- Nó x_v apresenta um certificado ao x_i
  - certificado $C^{x_v}_{SK_\gamma}$ assinado com a chave privada do grupo IG_γ
- Nó x_u utiliza a chave pública PK_γ para verificar a autenticidade do certificado apresentado
- Mas como saber se a chave pública PK_γ é válida?
  - Nó x_u precisa autenticar essa chave pública

Autenticação

Nó x_u deseja autenticar a chave pública pk_v de x_v

- Inicialmente
  - x_u procura $\exists(PK_\alpha \rightrightarrows PK_\gamma) \in G_u : x_u \in IG_\alpha$

Autenticação

Nó x_u deseja autenticar a chave pública pk_v de x_v

- Inicialmente
  - x_u procura $\exists(PK_\alpha \rightrightarrows PK_\gamma) \in G_u : x_u \in IG_\alpha$
- Caso $\nexists(PK_\alpha \rightrightarrows PK_\gamma) \in G_u : x_u \in IG_\alpha$
  - x_u cria $G_1 = G_u \cup G_v$
  - procura $\exists(PK_\alpha \rightrightarrows PK_\gamma) \in G_1 : x_u \in IG_\alpha$

Autenticação

Nó x_u deseja autenticar a chave pública pk_v de x_v

- Inicialmente
  - x_u procura $\exists(PK_\alpha \rightrightarrows PK_\gamma) \in G_u : x_u \in IG_\alpha$
- Caso $\nexists(PK_\alpha \rightrightarrows PK_\gamma) \in G_u : x_u \in IG_\alpha$
  - x_u cria $G_1 = G_u \cup G_v$
  - procura $\exists(PK_\alpha \rightrightarrows PK_\gamma) \in G_1 : x_u \in IG_\alpha$
- Caso $\nexists(PK_\alpha \rightrightarrows PK_\gamma) \in G_u : x_u \in IG_\alpha$
  - x_u cria $G_2 = G_u \cup G_u^N$
  - procura $\exists(PK_\alpha \rightrightarrows PK_\gamma) \in G_2 : x_u \in IG_\alpha$
  - **valida** as associações dos **certificados não-atualizados**

Autenticação

Nó x_u deseja autenticar a chave pública pk_v de x_v

- Inicialmente
  - x_u procura $\exists (PK_\alpha \rightrightarrows PK_\gamma) \in G_u : x_u \in IG_\alpha$
- Caso $\nexists (PK_\alpha \rightrightarrows PK_\gamma) \in G_u : x_u \in IG_\alpha$
  - x_u cria $G_1 = G_u \cup G_v$
  - procura $\exists (PK_\alpha \rightrightarrows PK_\gamma) \in G_1 : x_u \in IG_\alpha$
- Caso $\nexists (PK_\alpha \rightrightarrows PK_\gamma) \in G_u : x_u \in IG_\alpha$
  - x_u cria $G_2 = G_u \cup G_u^N$
  - procura $\exists (PK_\alpha \rightrightarrows PK_\gamma) \in G_2 : x_u \in IG_\alpha$
  - **valida** as associações dos **certificados não-atualizados**
- Caso $\nexists (PK_\alpha \rightrightarrows PK_\gamma) \in G_2 : x_u \in IG_\alpha$
  - x_u não valida PK_γ e não autentica x_v

Validação de um certificado de grupo

Nó x_u deseja validar o certificado $C_{SK_\alpha}^{IG_\beta}$

- x_u envia um pedido de validação (VREQ) a **todos** os membros de IG_α
- Aguarda por no mínimo t respostas de validação (VREP) **válidas** e **positivas**

- Somente se $C_{SK_\alpha}^{IG_\beta}$ ainda é válido
  - os membros de IG_α respondem positivamente ao nó x_u

Outras operações do SG-PKM

Atualização de certificados

- certificados de nós:
  - iniciada pelo próprio nó
  - solicita aos demais membros a atualização do seu certificado

Outras operações do SG-PKM

Atualização de certificados

- certificados de nós:
  - iniciada pelo próprio nó
  - solicita aos demais membros a atualização do seu certificado
- certificados de grupos:
  - um membro do grupo IG_β solicita ao membros de IG_α a atualização de $C_{SK_\alpha}^{IG_\beta}$

Outras operações do SG-PKM

Revogação explícita de certificados

- certificados de nós:
  - iniciada por qualquer membro do grupo IG_α
  - precisa da **aprovação** de no mínimo t membros do grupo
  - **após a revogação**, todos os grupos que emitiram um certificado para IG_α são informados

A revogação implítica é baseada no **tempo de validade** dos certificados

Outras operações do SG-PKM

Revogação explícita de certificados

- certificados de nós:
  - iniciada por qualquer membro do grupo IG_α
  - precisa da **aprovação** de no mínimo t membros do grupo
  - **após a revogação**, todos os grupos que emitiram um certificado para IG_α são informados
- certificados de grupos:
  - qualquer nó do grupo IG_α pode iniciar a revogação do $C_{SK_\alpha}^{IG_\beta}$
  - precisa da **aprovação** de no mínimo t membros do grupo IG_α
  - **após a revogação**, os nós que solicitaram a **validação** do certificado revogado são **informados**

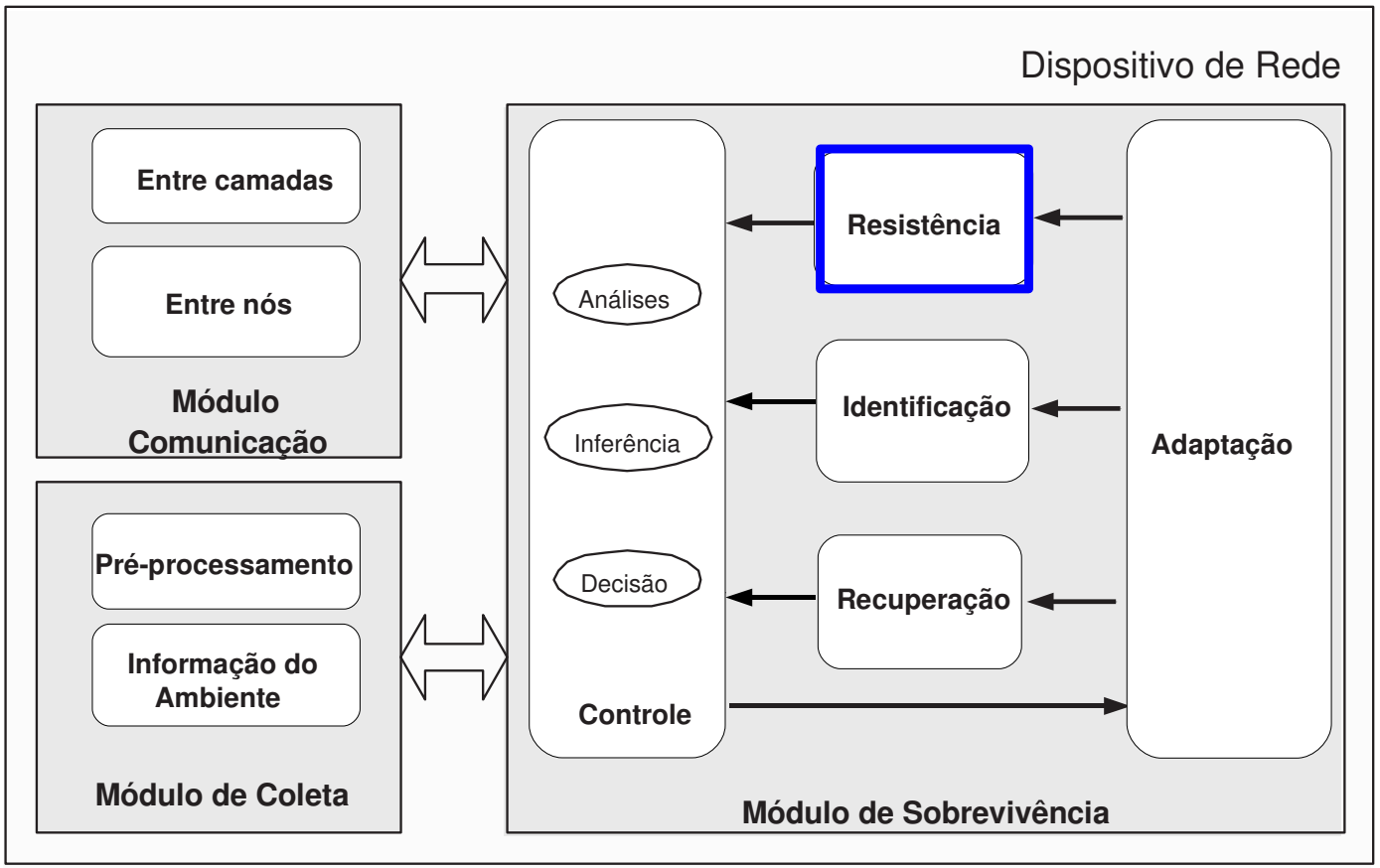
A revogação implítica é baseada no **tempo de validade** dos certificados

Arquitutura para suporte

- O SG-PKM é totalmente **independente** de arquitetura
- Qualquer **arquitetura** com essas características pode ser aplicada
  - flexível
  - sobrevivente a ataques
  - integrada com esquemas de reputação e prevenção
- Foi utilizada a SAMNAR (*Survivable Ad hoc and Mesh Architecture*)
  - possui três linhas de defesa: **preventiva**, **reativa** e **tolerância**
  - criada em 2008, parte da tese de doutorado de Michele Nogueira Lima (LIP6 – Paris – França)
  - visa aumentar a capacidade da rede **fornecer** serviços mesmo na presença de ataques

Uso da arquitetura SAMNAR

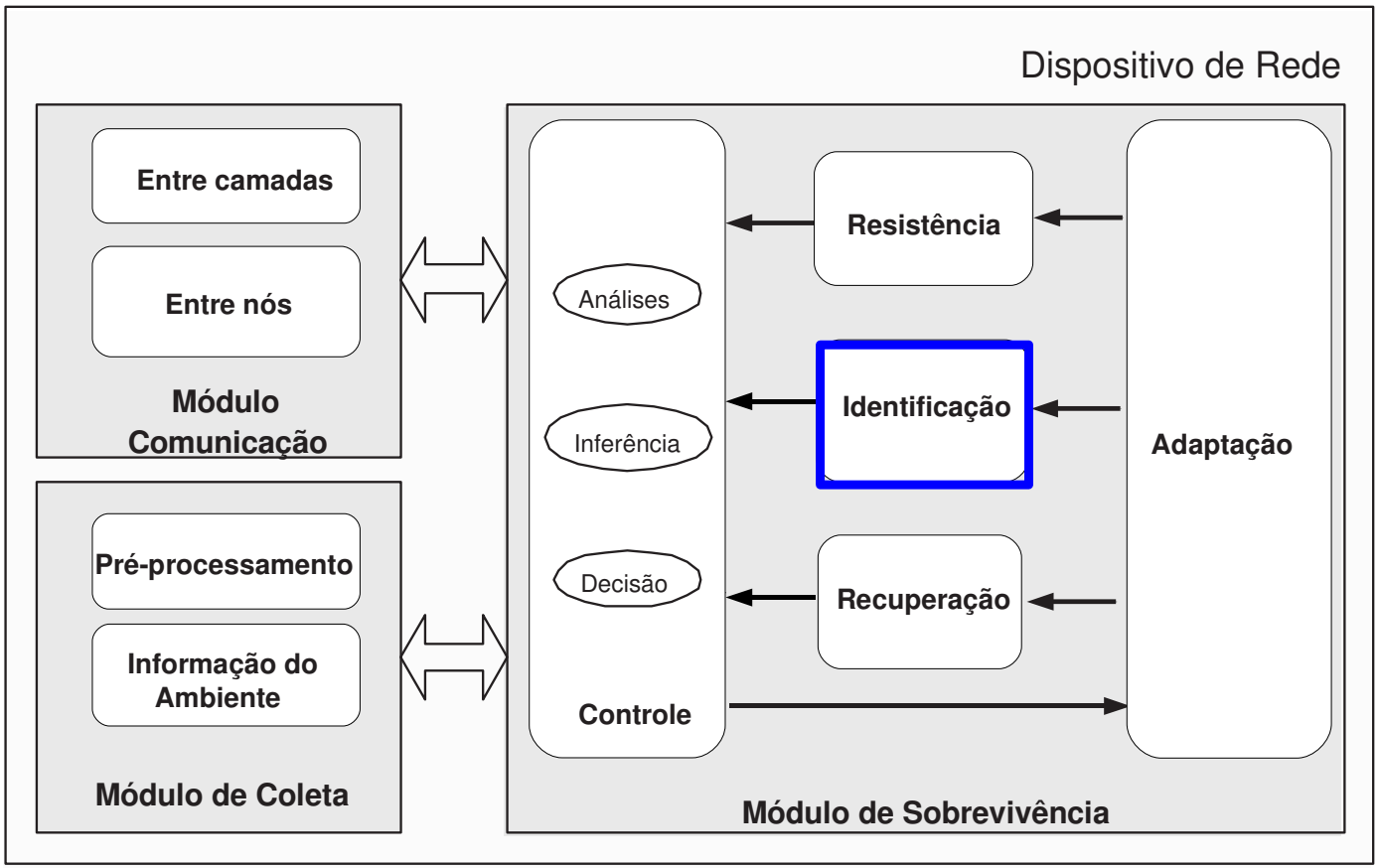
Componente de resistência



- operações criptográficas como: assinaturas digitais e código de autenticação de mensagens

Uso da arquitetura SAMNAR

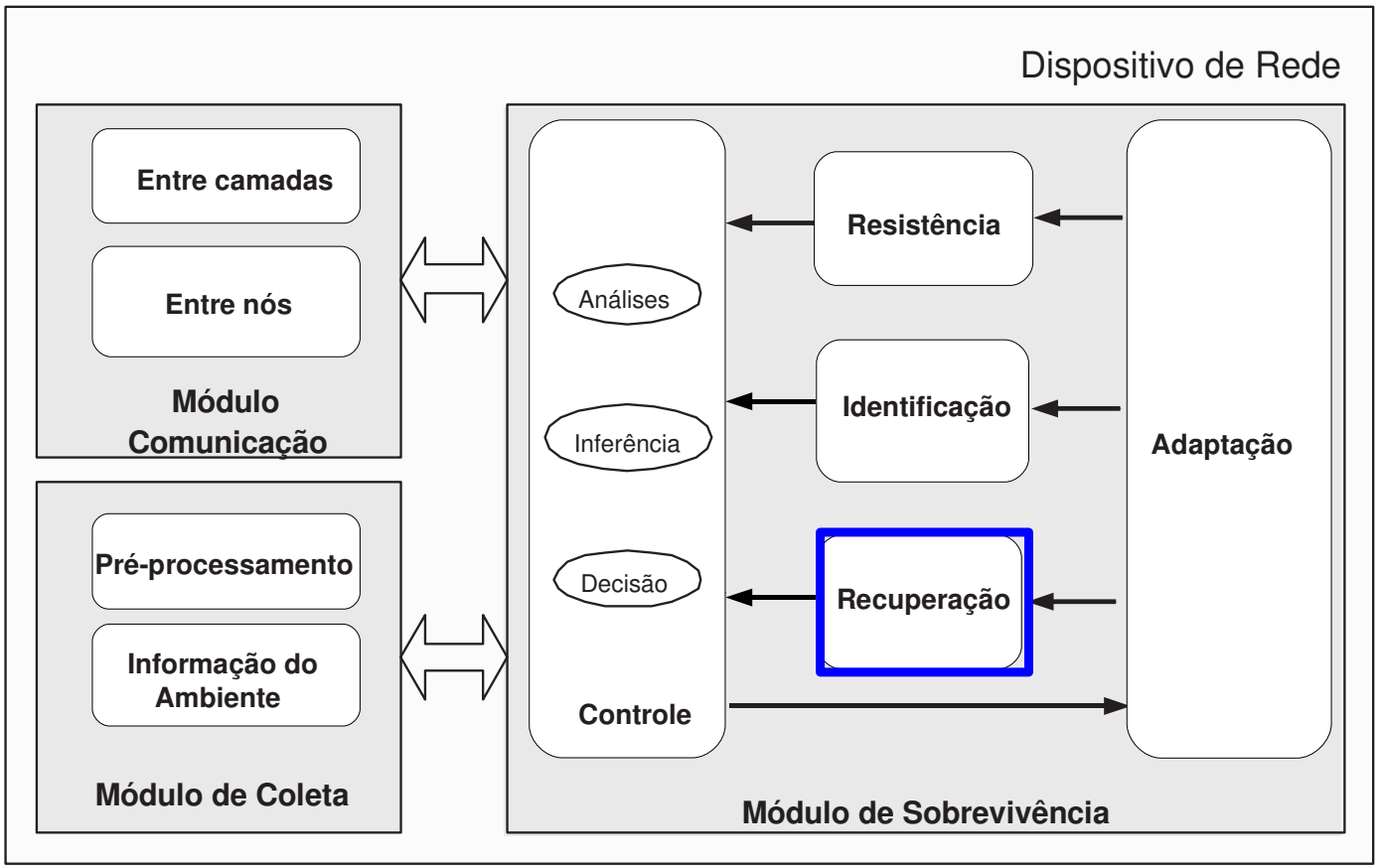
Componente de identificação



- entradas de um sistema de reputação

Uso da arquitetura SAMNAR

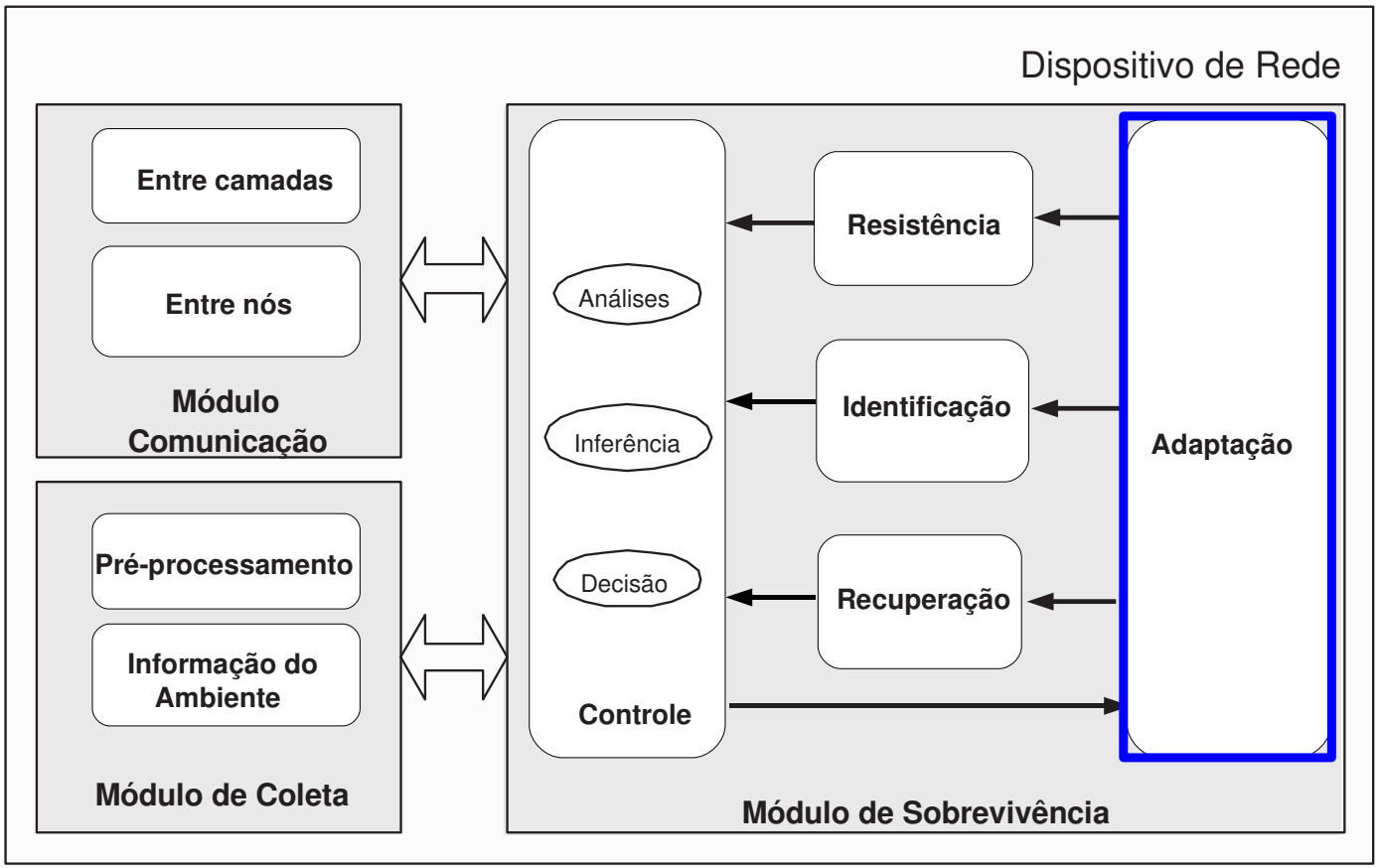
Componente de recuperação



- formação de grupos: servem como testemunhas das trocas de chaves
- cadeias de certificados disjuntas na autenticação

Uso da arquitetura SAMNAR

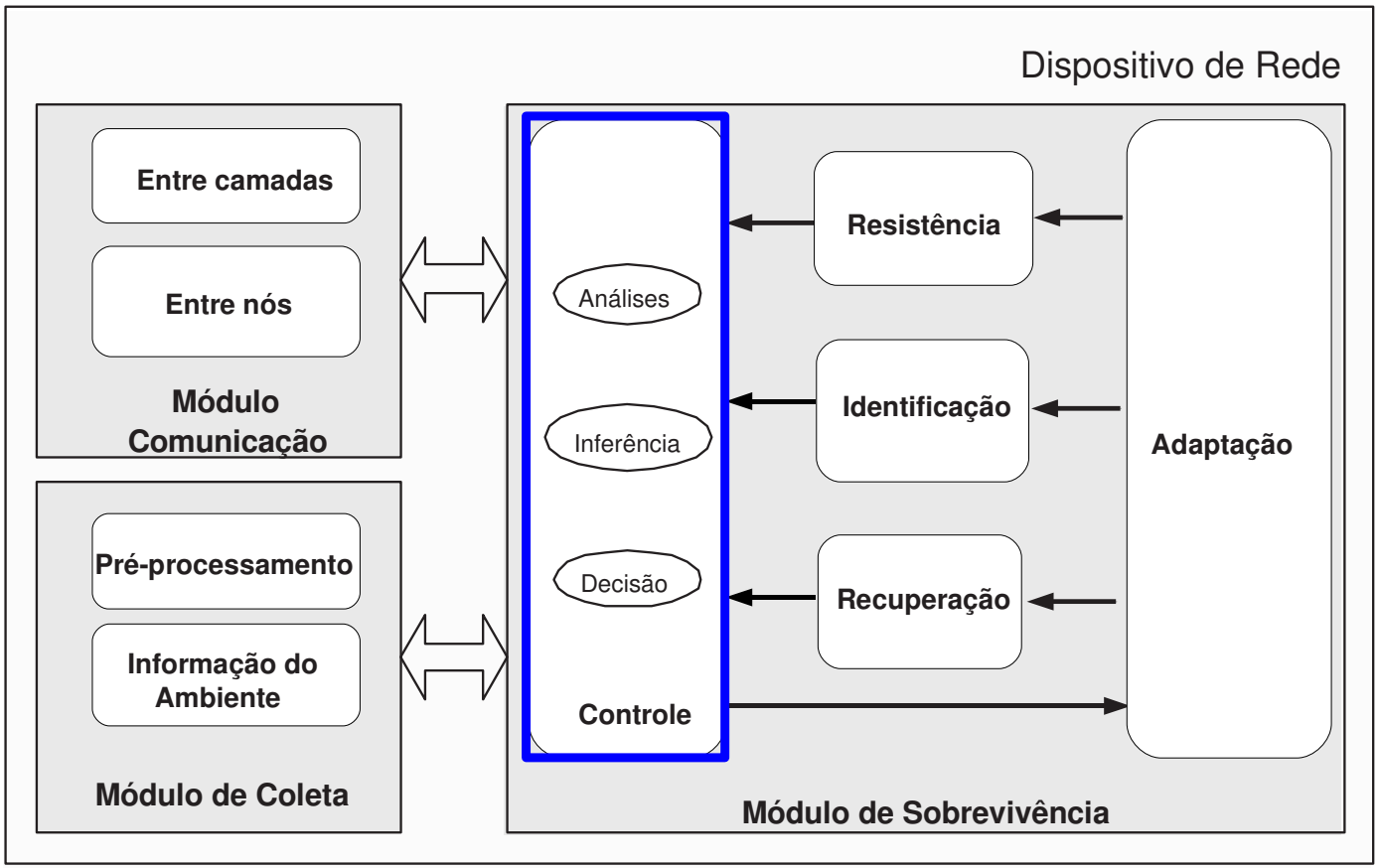
Componente de adaptação



- alteração dos parâmetros de redundância e valores de limiares

Uso da arquitetura SAMNAR

Componente de controle



- analisa os valores recebidos de outros componentes
- envia valores ao módulo de adaptação

Métricas para a avaliação

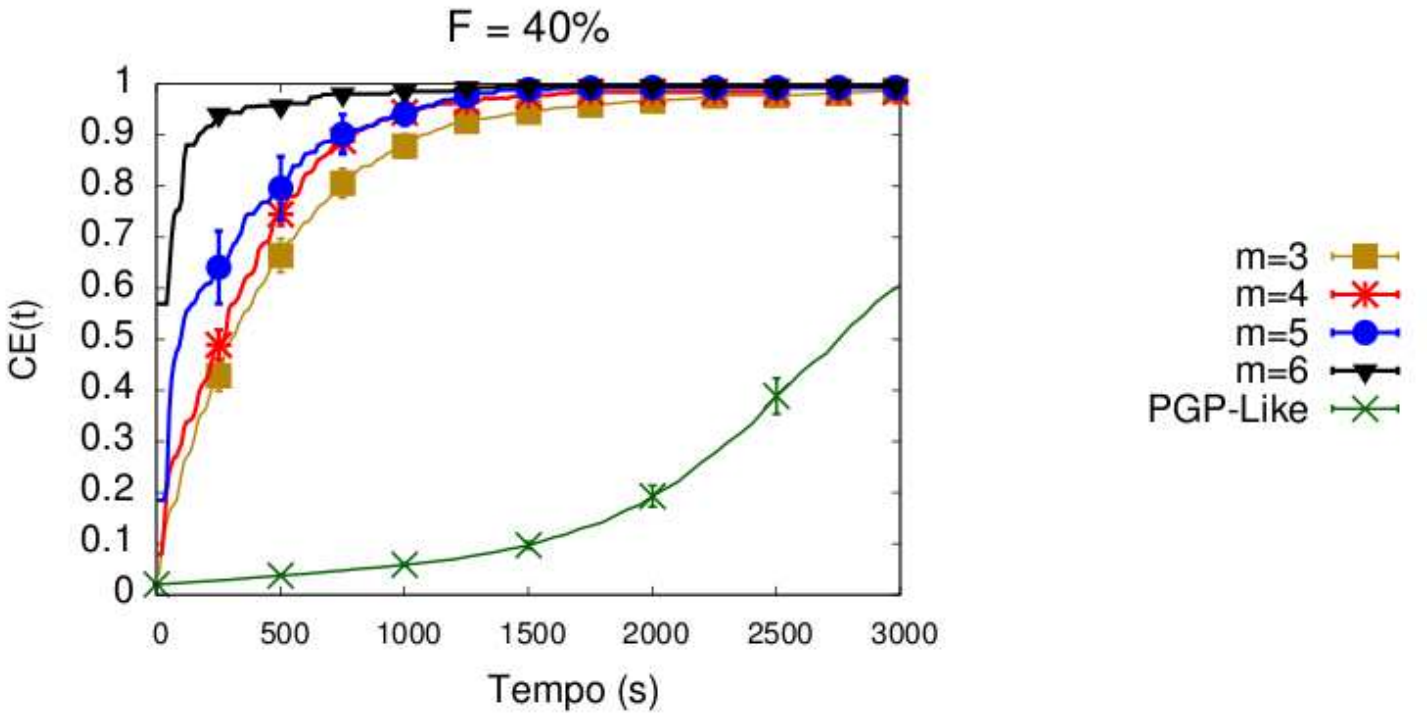
- *Convergência das trocas de certificados (CE)*
- *Autenticabilidade dos usuários (UA)*
- Alcançabilidade dos grupos (GR)

- Grupos não comprometidos (NCG)
- Autenticações não comprometidas (NCA)

Simulações no NS-2

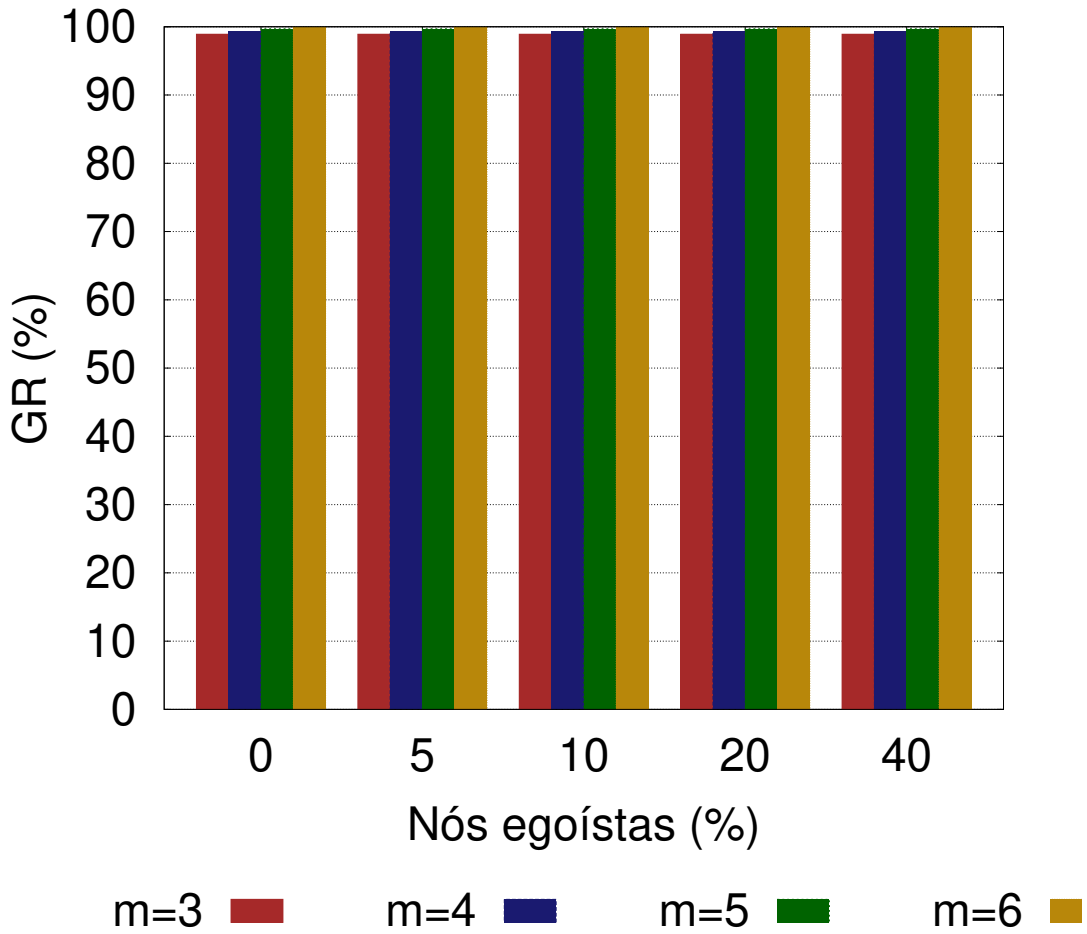
Parâmetro	**Valores utilizados**
Raio de alcance	50 e 120 metros
Quantidade de nós	100 nós
Velocidades máximas	5, 10 e 20 m/s
Tamanho dos grupos	3, 4, 5 e 6
Tamanho do ambiente	1000 x 1000 metros 1500 x 300 metros
Tipo de movimentação	*waypoint* aleatório
Tempo máximo de pausa	20 segundos
Tempo entre troca de certificados	60 segundos
Quantidade de certificados emitidos	600 certificados
Tempo de simulação	10000 segundos
Percentual de atacantes	5, 10, 20 e 40%

Convergência das trocas de certificados

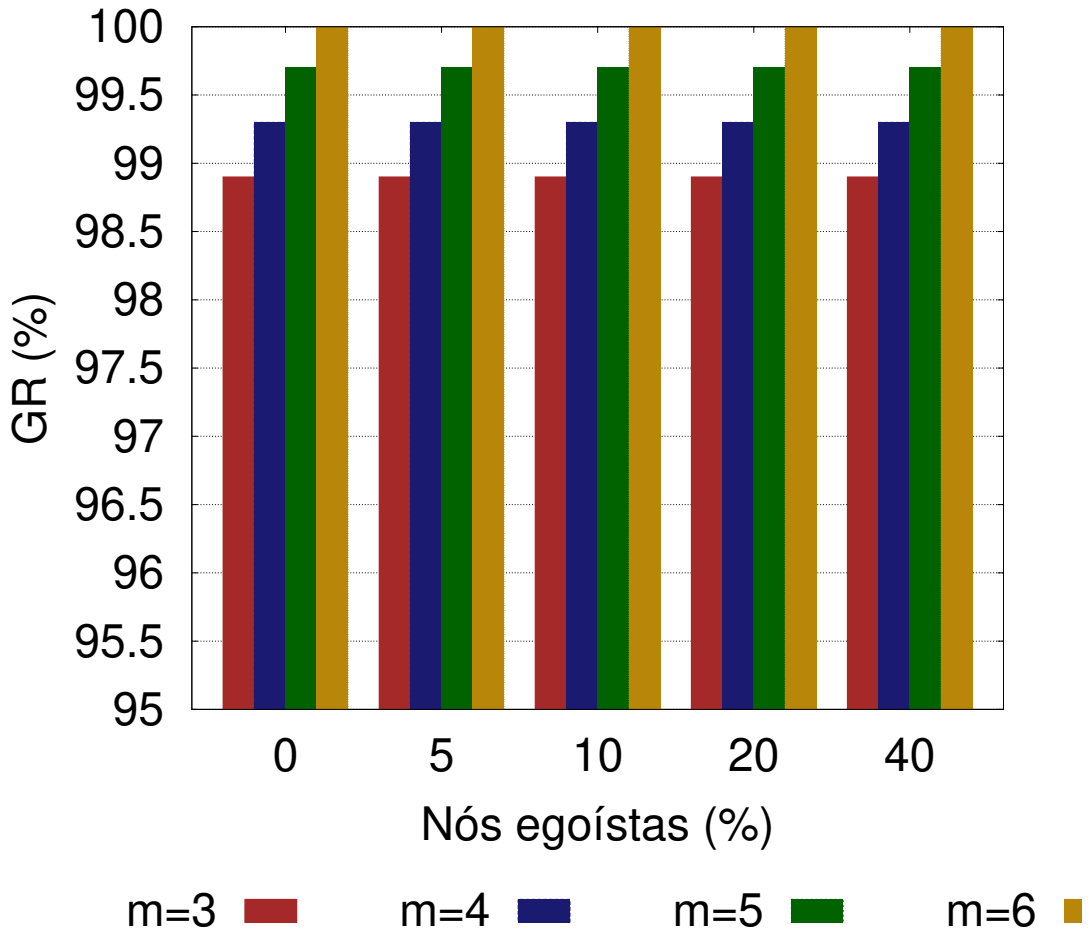


OBS: Resultados com velocidade de 20 m/s, raio de alcance de **50 m**, tamanho do ambiente do 1000x1000 metros e 40% de atacantes

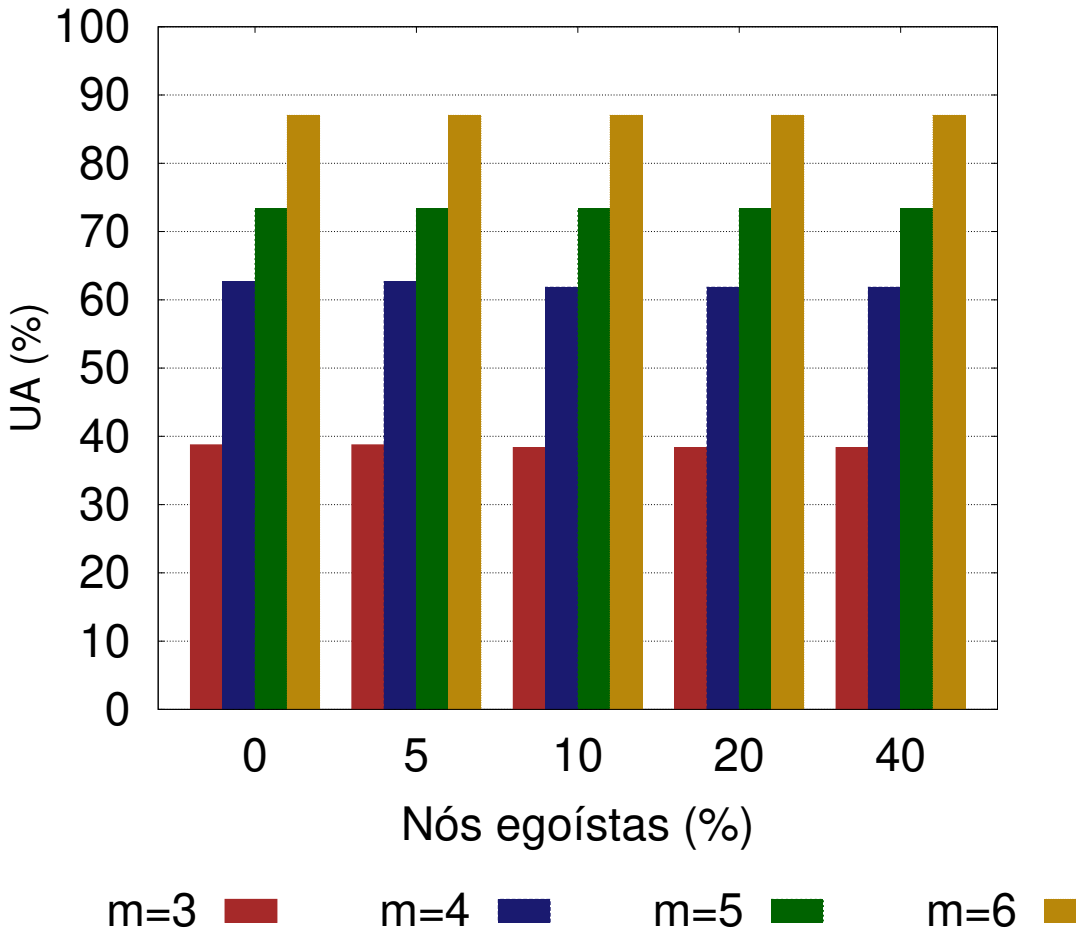
Alcançabilidade dos grupos



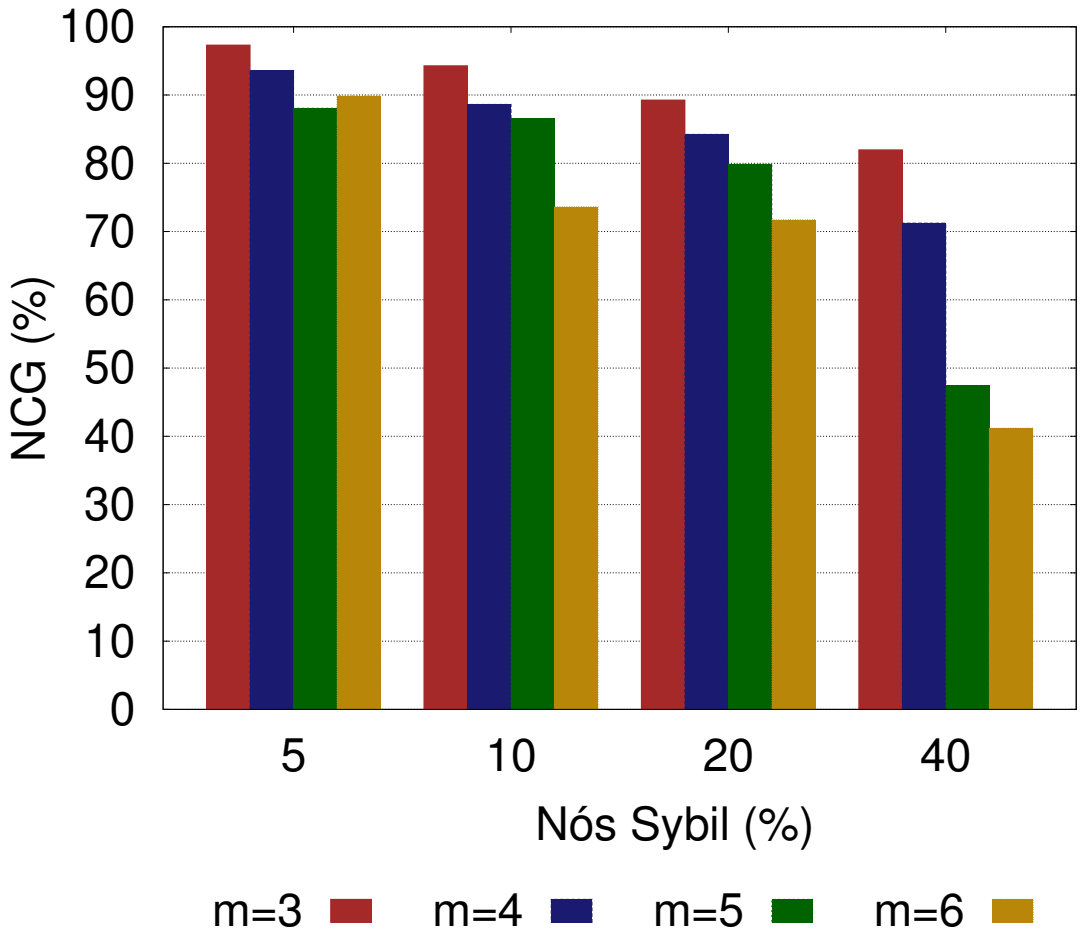
Alcançabilidade dos grupos



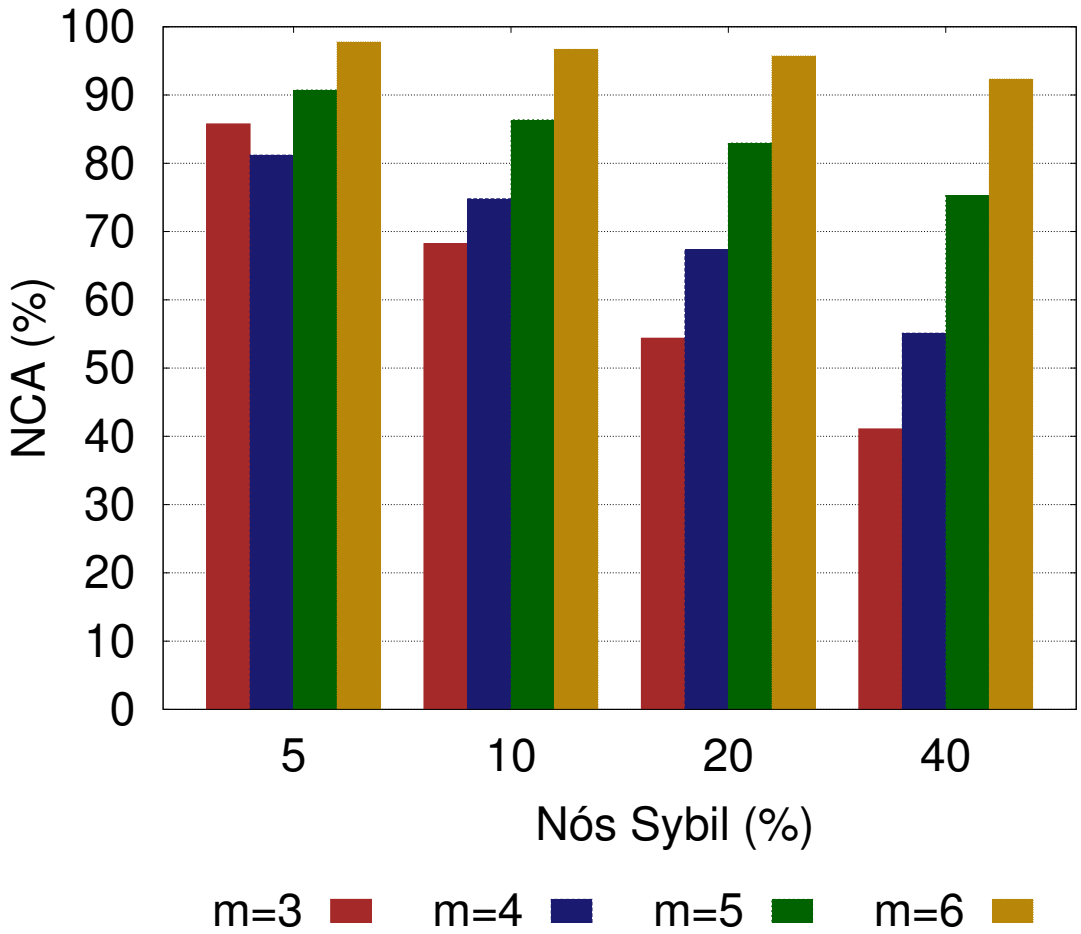
Autenticabilidade dos usuários



Grupos não-comprometidos



Autenticações não-comprometidas



Considerações sobre o SG-PKM

Sob ataques de falta de cooperação

- O SG-PKM mantém a sua eficácia
- O número de nós egoístas afeta:
  - tempo de convergência

Sob ataques Sybil

- Resiste a esse ataque melhor que PGP-Like
- Principalmente em cenários com grupos de 5 e 6 membros
- O esquema é sobrevivente aos ataques Sybil

Parte IV

Conclusões

Considerações finais I

- As **características** das MANETs:
  - as tornam altamente vulneráveis a ataques
  - dificultam a implementação de esquemas de gerenciamento de chaves **eficazes** e **seguros**
- O PGP-Like é:
  - **considerado** um dos melhores esquemas para MANETs
  - suceptível a ataques maliciosos
  - totalmente **vulnerável** a ataques Sybil

Considerações finais II

- Este trabalho propôs um novo esquema, o SG-PKM
  - nós formam grupos baseados em **relações de amizades**
  - nesses grupos, os nós:
    - **trocam** as suas chaves públicas
    - **emitem** certificados
  - membros de um grupo podem emitir certificados para **outros grupos**
  - exige a formação de cadeias de certificados **disjuntas** na autenticação

Considerações finais III

- Os resultados mostraram que o SG-PKM:
  - conseguiu **resistir** aos ataques de falta de cooperação
    - convergências das trocas de certificados → antes que o PGP-Like
  - resistiu aos ataques Sybil:
    - na maioria dos casos, as identidades falsas não foram **autenticadas** pelos nós **não-comprometidos**
  - **autenticação dos nós** → desempenho menor que o PGP-Like
    - consequência da exigência das cadeias disjuntas de certificados

- Todos os objetivos foram alcançados

Considerações finais IV

- Limitações do SG-PKM:
  - assume-se que usuários formam grupos baseados em suas relações de amizades
  - troca de chaves por um canal fora da banda
  - todos os grupos possuem o mesmo tamanho
  - os grupos possuem tamanhos fixos

Trabalhos futuros

- Avaliar a eficácia do SG-PKM em cenários com outros tipos de ataques
- Avaliar a praticabilidade do SG-PKM considerando outras características das redes sociais
- Analisar o impacto no desempenho e eficácia contra ataques se forem utilizadas mais cadeias disjuntas de certificados na autenticação
- Realizar simulações utilizando grafos de redes sociais verdadeiras

Publicações realizadas I

1. Identity-based key management in mobile ad hoc networks: Techniques and applications. *IEEE Wireless Communications Magazine*, IEEE Communications Society, New York, NY, USA, v. 15, Oct 2008. ISSN 1536-1284.
2. Quantifying misbehaviour attacks against the self-organized public key management on manets. In: *Proceedings of the International Conference on Security and Cryptography (SECRYPT '08)*. Porto, Portugal: INSTCC Press, 2008. p. 128–135. ISSN 978-989-8111-59-3. **Na lista dos best-papers da conferência**
3. Segurança em redes ad hoc. In: *Anais do XXVI Simpósio Brasileiro de Telecomunicações (SBRT '08)*. Rio de Janeiro, RJ, Brasil: SBrT - Sociedade Brasileira de Telecomunicaçõs, 2008. p. 19–20. ISBN 978-85-89748-05-6.
4. Survivable Keying for Wireless Ad Hoc Networks. In: *11th IFIP/IEEE International Symposium on Integrated Network Management (IM 2009)*, New York, June, 2009. p. 606-613. ISSN 978-1-4244-3487-9.
5. Resisting Impersonation Attacks in Chaining-Based Public-Key Management on MANETs: the Virtual Public-Key Management. In: *Proceedings of the International Conference on Security and Cryptography (SECRYPT '09)*. Milan, Italy: INSTCC Press, 2009. (to appear)
6. Chapter: Analyzing the Effectiveness of Self-Organized Public Key Management on MANETs under Lack of Cooperation and Impersonation attacks. In: *E*-Business and Telecommunication Networks. (Springer) 2009 (to appear).

OBRIGADO!

Métricas para a avaliação

- Convergência das trocas de certificados (CE)

$$CE(t) = \frac{\sum_{x_i \in S} CE_i(t)}{|S|} \qquad \text{em que}$$

$$CE_i(t) = \frac{\sum_{x_a, x_b \in S} (pk_a \rightarrow pk_b) \in (G_i \cup G_i^N)}{\sum_{x_x, x_y \in S} (pk_x \rightarrow pk_y) \in G}$$

Métricas para a avaliação

- Convergência das trocas de certificados (CE)
- Alcançabilidade dos nós (UR)

$$UR(t) = \frac{\sum_{x_i \in S} UR_i(t)}{|S|} \qquad \text{em que}$$

$$UR_i = \frac{\sum_{x_a \in S} (pk_i \rightsquigarrow pk_a) \in (G_i \cup G_i^N)}{|S|}$$

Métricas para a avaliação

- Convergência das trocas de certificados (CE)
- Alcançabilidade dos nós (UR)
- Confiabilidade em uma identidade falsa (FIC)

$$FIC = \frac{\sum_{x_i \in NC} FIC_i}{|NC|} \qquad \text{em que}$$

$$FIC_i = \begin{cases} 1 & \text{caso} \quad \exists\, x_f \in (G_i \cup G_i^N) \text{ sendo que } \; x_f \in (S \cap NC) \\ 0 & \text{caso contrário} \end{cases}$$

Métricas para a avaliação

- Convergência das trocas de certificados (CE)
- Alcançabilidade dos nós (UR)
- Confiabilidade em uma identidade falsa (FIC)
- Autenticação indireta de falsas identidades (IA)

$$IA = \frac{\sum_{x_i \in NC} IA_i}{|NC|} \qquad \text{em que}$$

$$IA_i = \begin{cases} 1 & \text{caso} \quad \exists (pk_i \rightsquigarrow pk_f) \in (G_i \cup G_f) \ \text{ sendo que } \ x_f \in (S \cap NC) \\ 0 & \text{caso contrário} \end{cases}$$

Métricas para a avaliação

- Convergência das trocas de certificados (CE)
- Alcançabilidade dos nós (UR)
- Confiabilidade em uma identidade falsa (FIC)
- Autenticação indireta de falsas identidades (IA)
- Certificados suspeitos por repositório (SC)

$$SC = \frac{\sum_{x_i \in NC} SC_i}{|NC|} \qquad \text{em que}$$

$$SC_i = \frac{\sum_{x_z \in G_i} \sum_{x_f \in F} (pk_z \rightarrow pk_f) \in G_i}{|G_i|}$$

Métricas para a avaliação

- Convergência das trocas de certificados (CE)

$$CE(t) = \frac{\sum_{i \in X} CE_i(t)}{|X|} \quad \text{em que}$$

$$CE_i(t) = \frac{\sum_{IG_\alpha, IG_\beta \in IG} (PK_\alpha \rightarrow PK_\beta) \in (G_i \cup G_i^N)}{\sum_{IG_\gamma, IG_\delta \in IG} (PK_\gamma \rightarrow PK_\delta) \in G} \quad (1)$$

Métricas para a avaliação

- Convergência das trocas de certificados (CE)
- Autenticabilidade dos usuários (UA)

$$UA = \frac{\sum_{i \in X} UA_i}{|X|} \quad \text{em que}$$

$$UA_i = \sum_{j \in X} (x_i \rightsquigarrow x_j) \in (G_i \cup G_j \cup \ G_i^N) \tag{1}$$

Métricas para a avaliação

- Convergência das trocas de certificados (CE)
- Autenticabilidade dos usuários (UA)
- Alcançabilidade dos grupos (GR)

$$GR(t) = \frac{\sum_{i \in X} GR_i(t)}{|X|} \quad \text{em que}$$

$$GR_i(t) = \sum_{\substack{IG_\alpha \in IG_{x_i} \\ IG_\beta \in IG}} (PK_\alpha \rightsquigarrow PK_\beta) \in (G_i \cup G_i^N) \qquad (1)$$

Métricas para a avaliação

- Convergência das trocas de certificados (CE)
- Autenticabilidade dos usuários (UA)
- Alcançabilidade dos grupos (GR)
- Grupos não comprometidos (NCG)

$$NCG = \frac{\sum_{IG_\alpha \in IG} NCG_\alpha}{|IG|} \quad \text{em que}$$

$$NCG_\alpha = \begin{cases} 1 & \text{se} \quad \nexists\, f \in IG_\alpha : f \text{ é uma identidade falsa} \\ 0 & \text{caso contrário} \end{cases} \tag{1}$$

Métricas para a avaliação

- Convergência das trocas de certificados (CE)
- Autenticabilidade dos usuários (UA)
- Alcançabilidade dos grupos (GR)
- Grupos não comprometidos (NCG)
- Autenticações não comprometidas (NCA)

$$NCA = \frac{\sum_{i \in X} NCA_i}{|X|} \qquad \text{em que}$$

$$NCA_i = \begin{cases} 1 & \text{se} \quad \nexists\, (pk_i \rightsquigarrow pk_f) \quad \forall f \in F \\ 0 & \text{caso contrário} \end{cases} \tag{1}$$