Gerenciamento de chaves públicas sobrevivente baseado em grupos para MANETs

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

20 de julho de 2010

UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

NR2

Roteiro

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

Redes ad hoc móveis

- São formadas **dinamica** e **espontaneamente**
- Sem infraestrutura e sem centralização:
  - Protocolos utilizados devem ser **completamente distribuídos**
  - **Dificulta** a implementação de serviços gerência da rede
- Topologia dinâmica
- 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

- **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

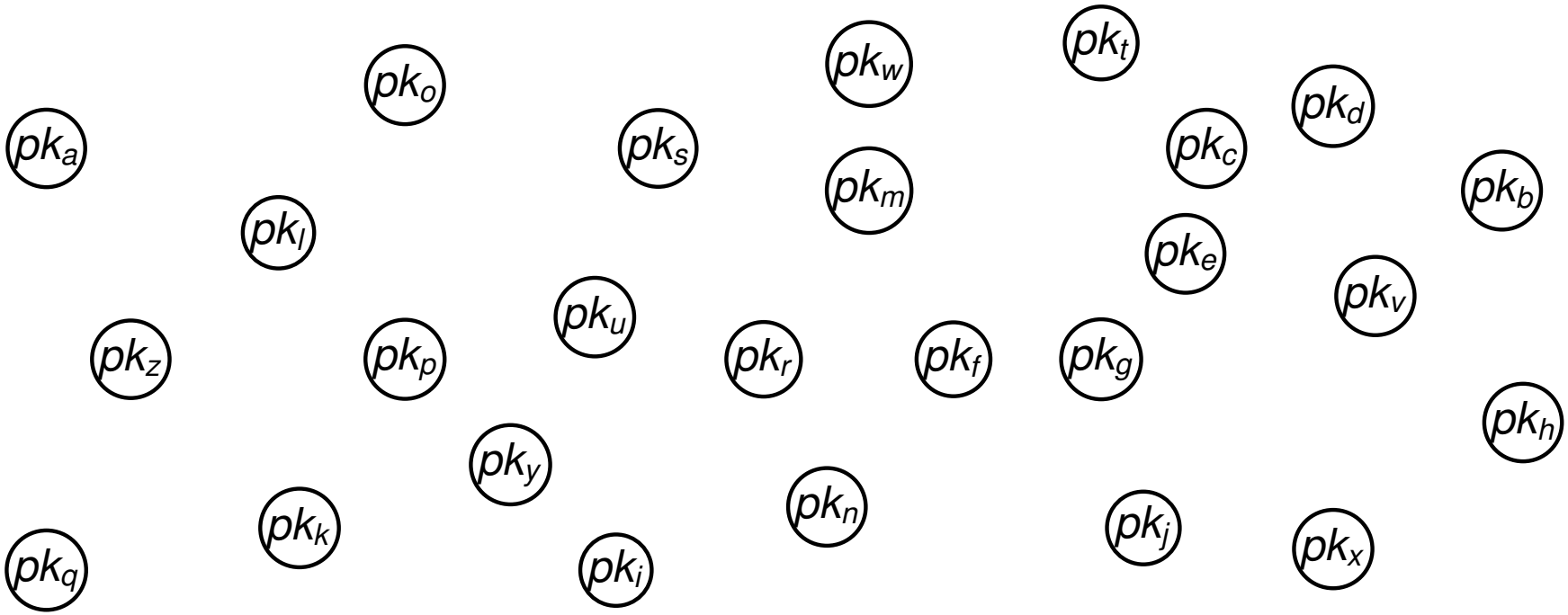
Nas MANETs

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

PGP-Like

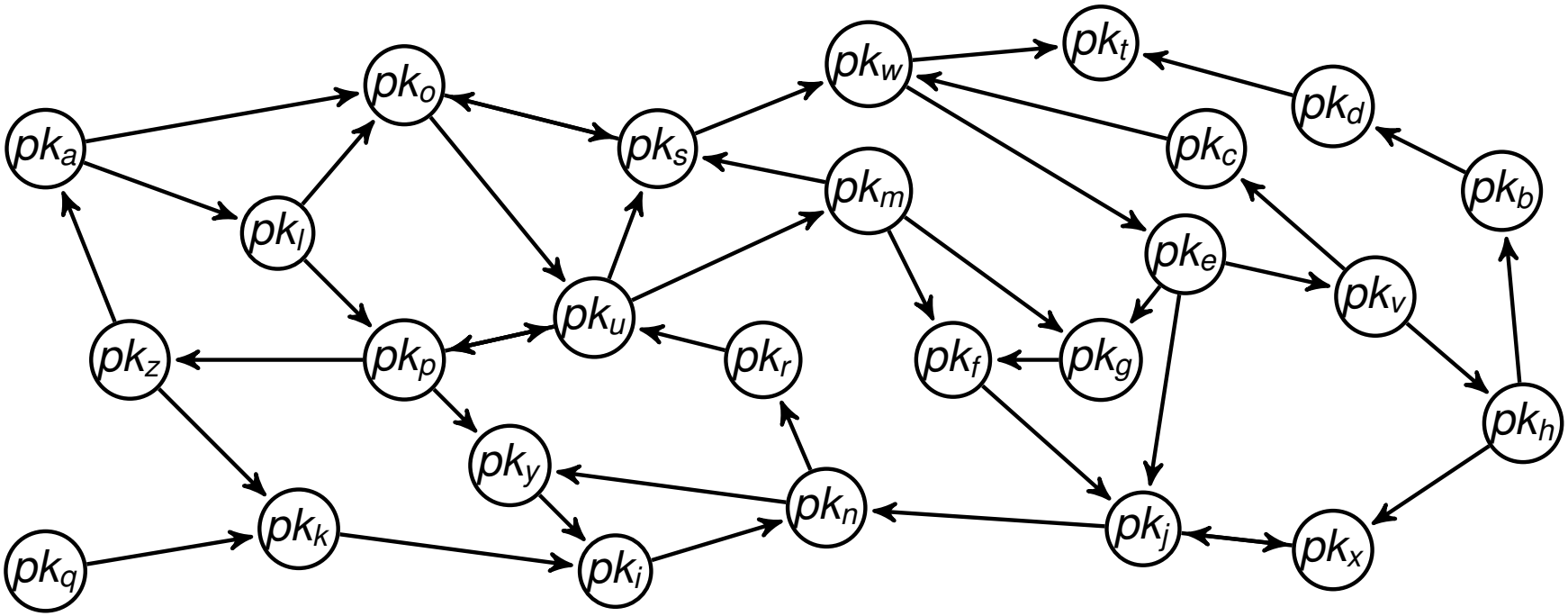
- Inspirado nas **ideias** do PGP
  - PGP foi criado 1991 por Philip Zimmermann
  - É um padrão para a **criptografia** e **proteção** de correio eletrônico na Internet
- Criado em 2003 por integrantes do projeto Terminodes
- Objetivo:
  - fornecer um serviço de gerência de chaves **auto-organizado**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

PGP-Like - Funcionamento



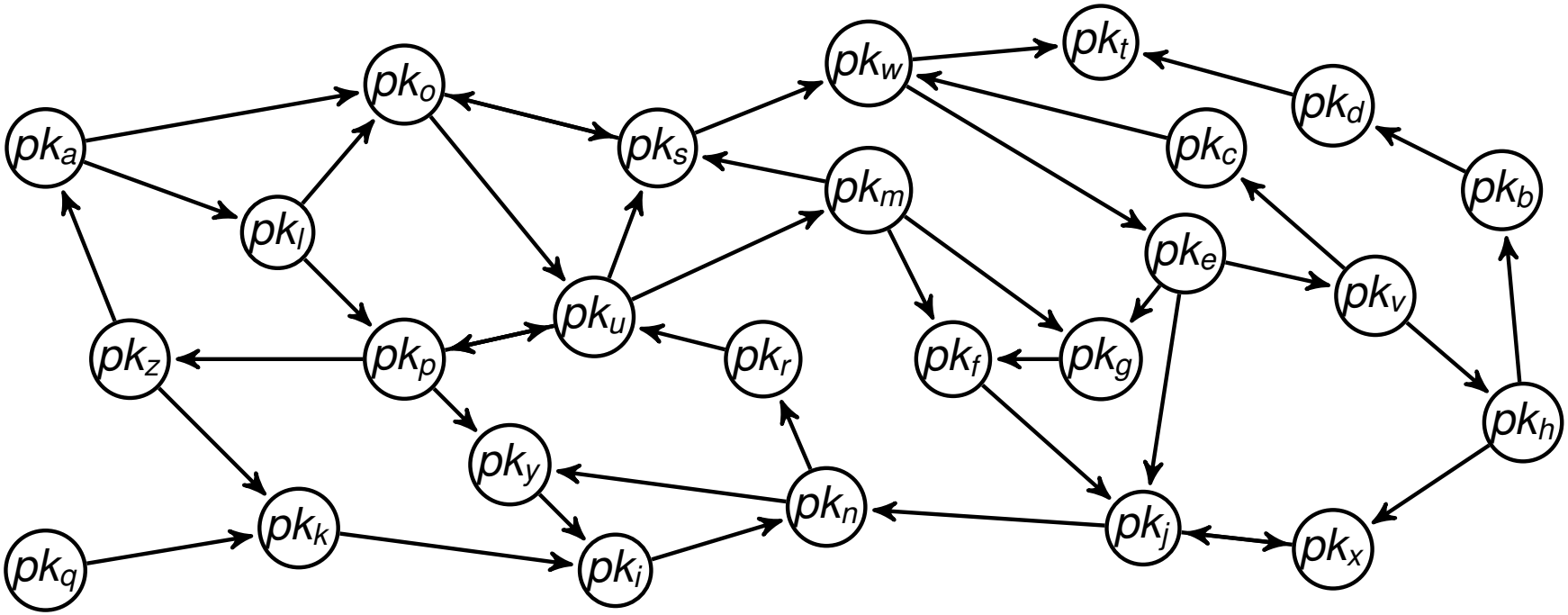
- Baseado nos conceitos do PGP
- Cada nó gera seu próprio par de chaves

PGP-Like - Funcionamento



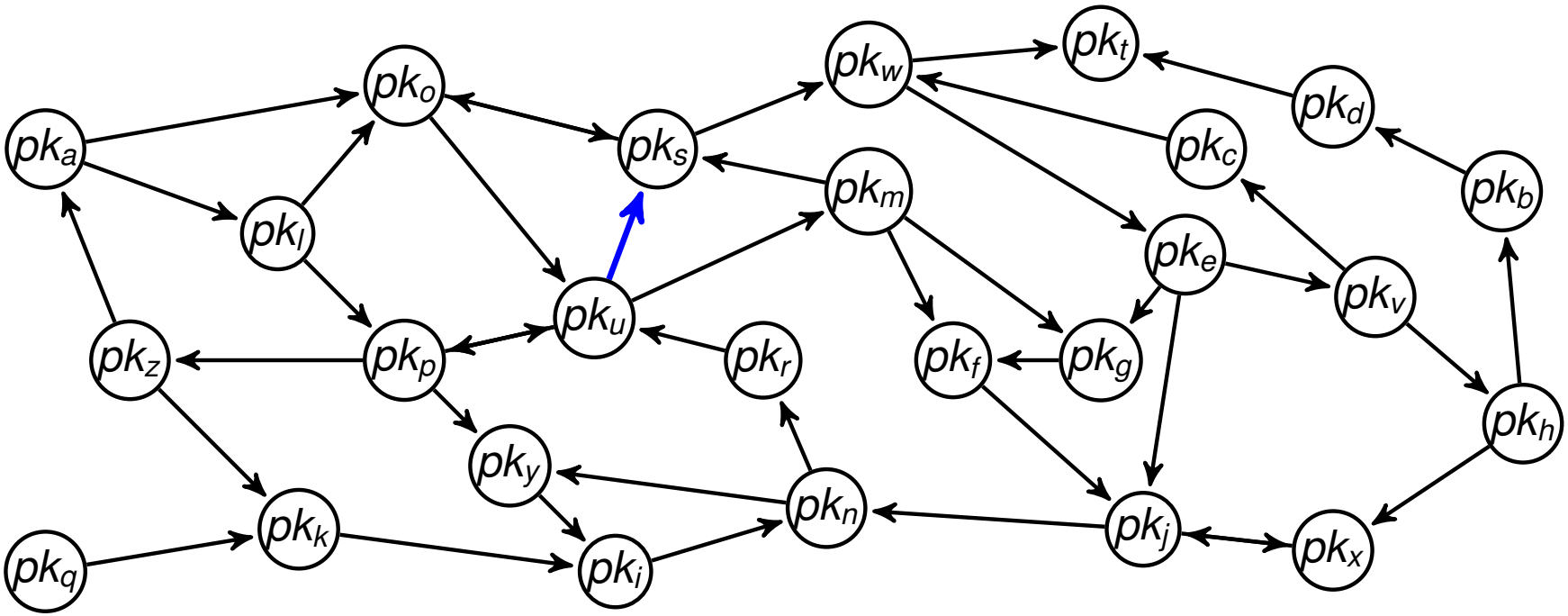
- Baseado nos conceitos do PGP
- Cada nó gera seu próprio par de chaves
- Emitem certificados para os nós que confiam

PGP-Like - Funcionamento



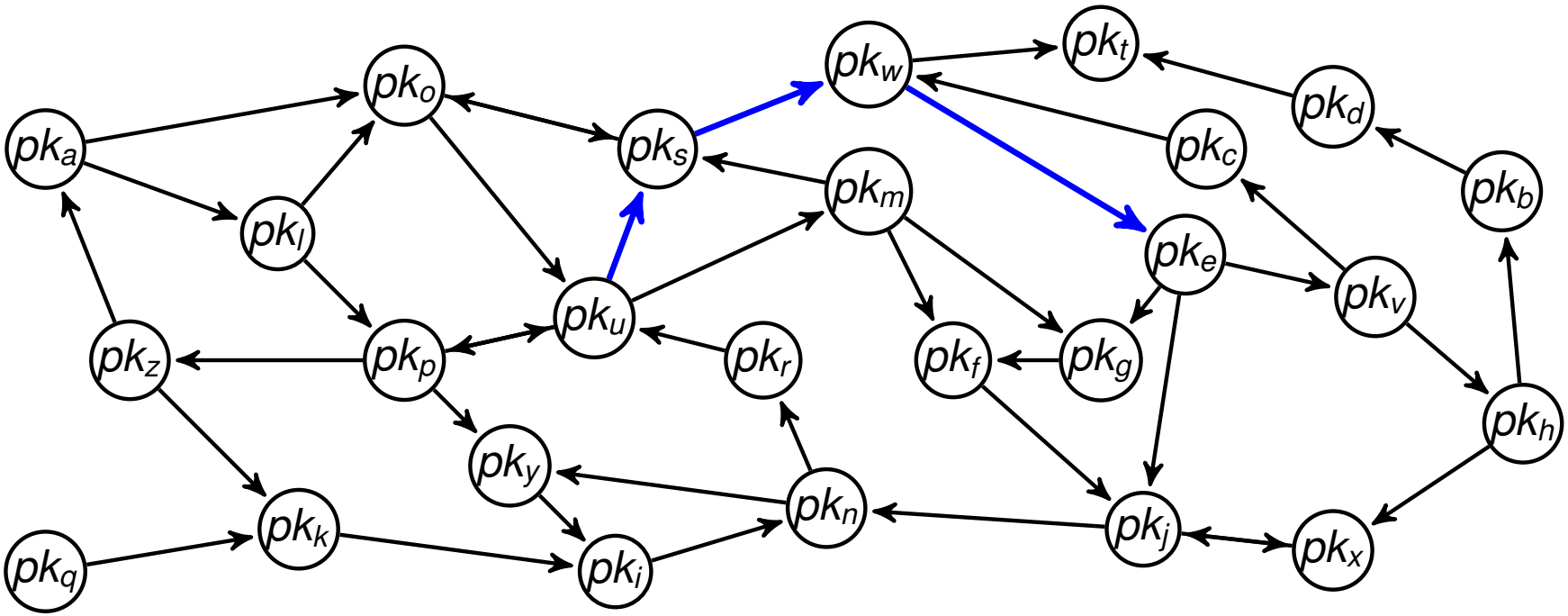
- Chaves públicas e certificados
  - Representados por um grafo direcionado $G = (V, A)$
  - V: Chaves públicas dos nós
  - A: Certificados

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

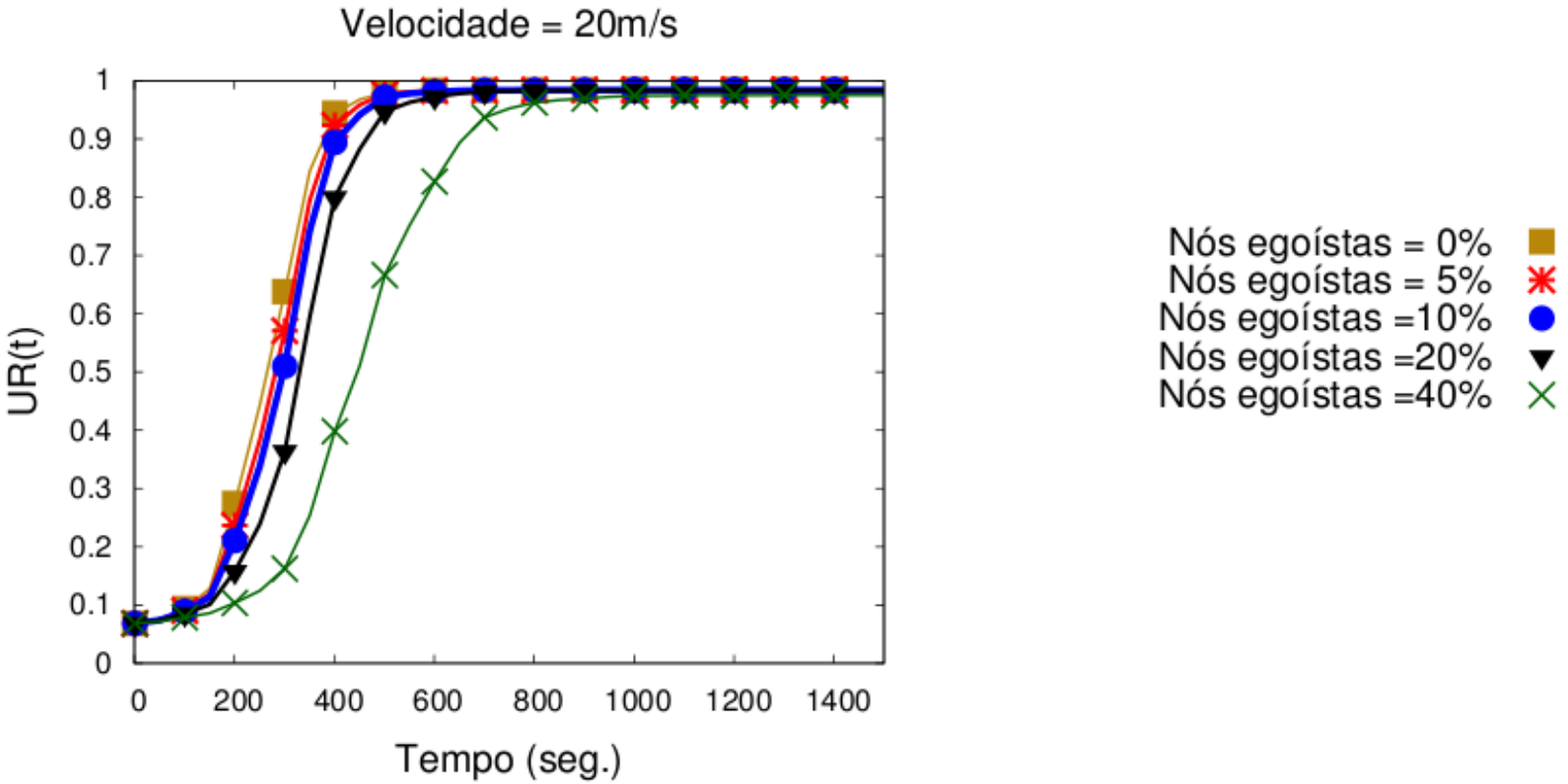


- Aresta direcionada entre dois vértices ($pk_u \rightarrow pk_s$):
  - certificado assinado com SK_u associando pk_s ao nó x_s
- Caminho conectando dois vértices ($pk_u \rightsquigarrow pk_e$):
  - cadeia de certificados de pk_u até pk_e

Simulações no NS-2

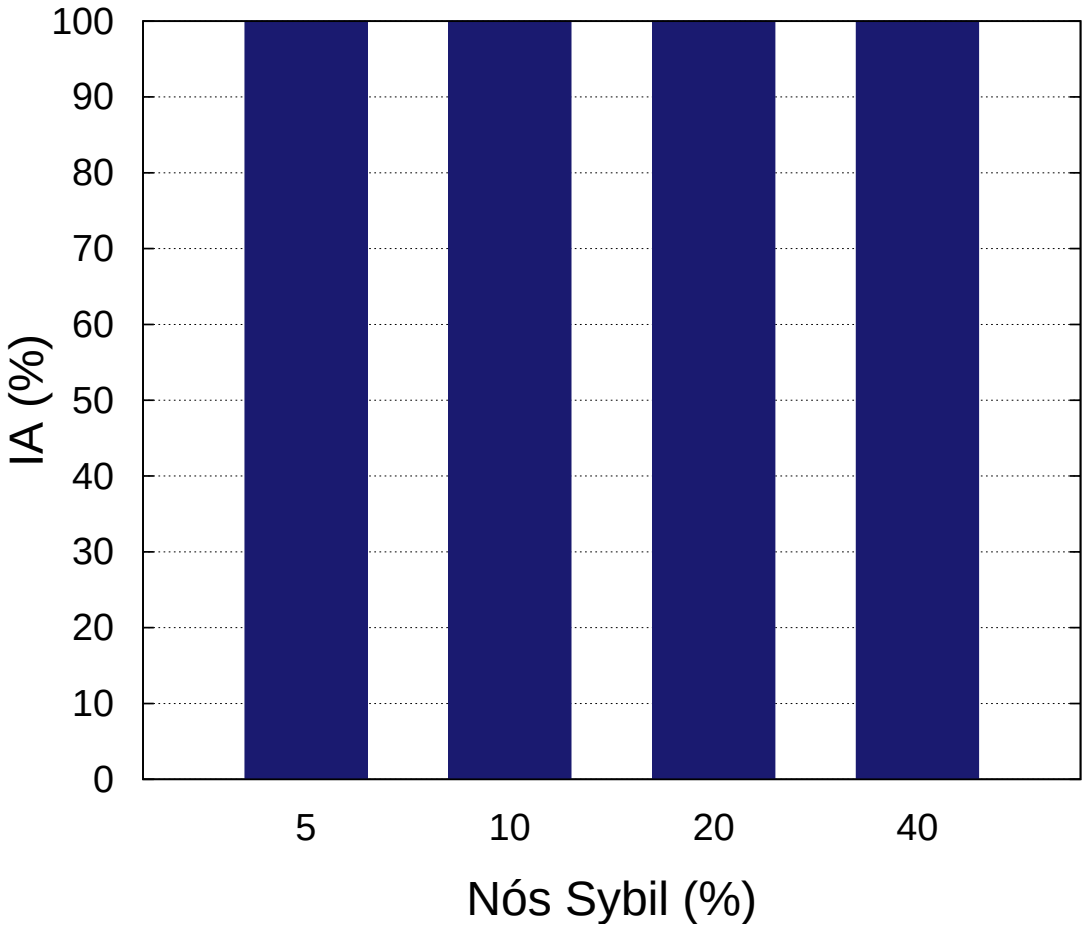
Parâmetro	**Valores utilizados**
Raio de alcance	50 e 120 metros
Quantidade de nós	100 nós
Tamanho do ambiente	1000 x 1000 metros 1500 x 300 metros
Tipo de movimentação	*waypoint* aleatório
Velocidades máximas	5, 10 e 20 m/s
Tempo máximo de pausa	20 segundos
Tempo entre troca de certificados	60 segundos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

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

Autenticação indireta das identidades falsas

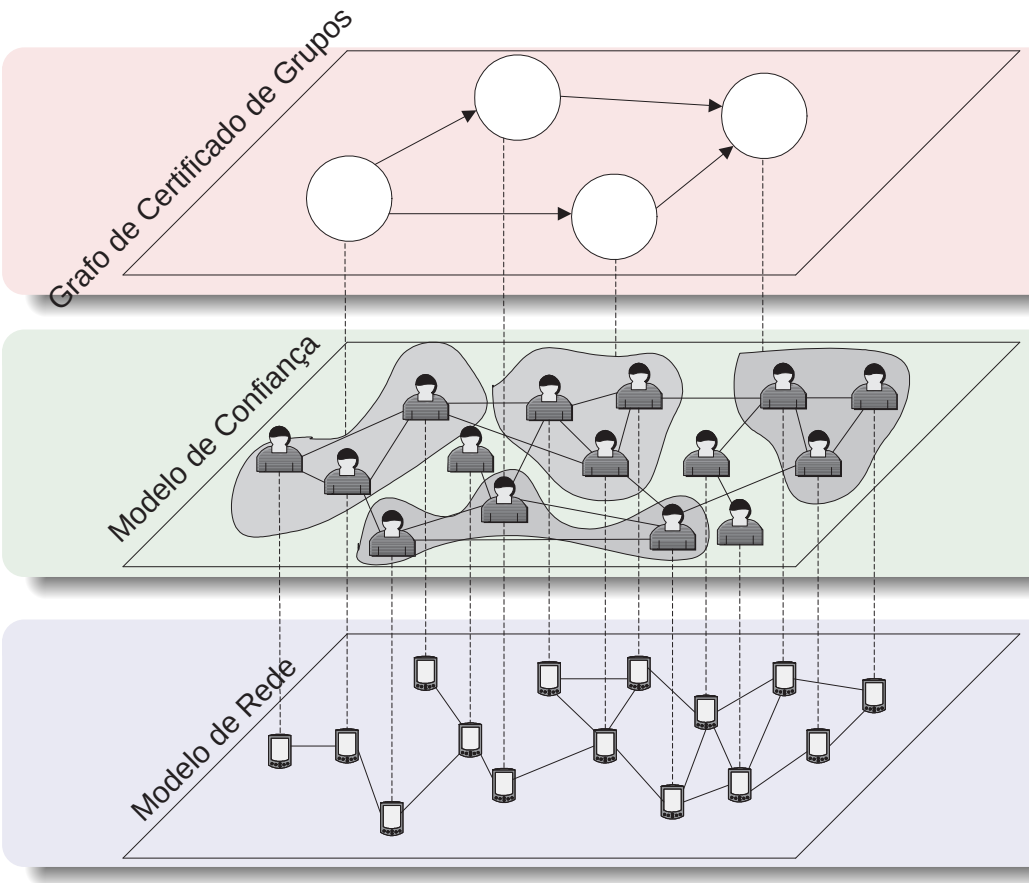


OBS: Ele é completamente vulnerável, mesmo diante de 5% de nós maliciosos

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

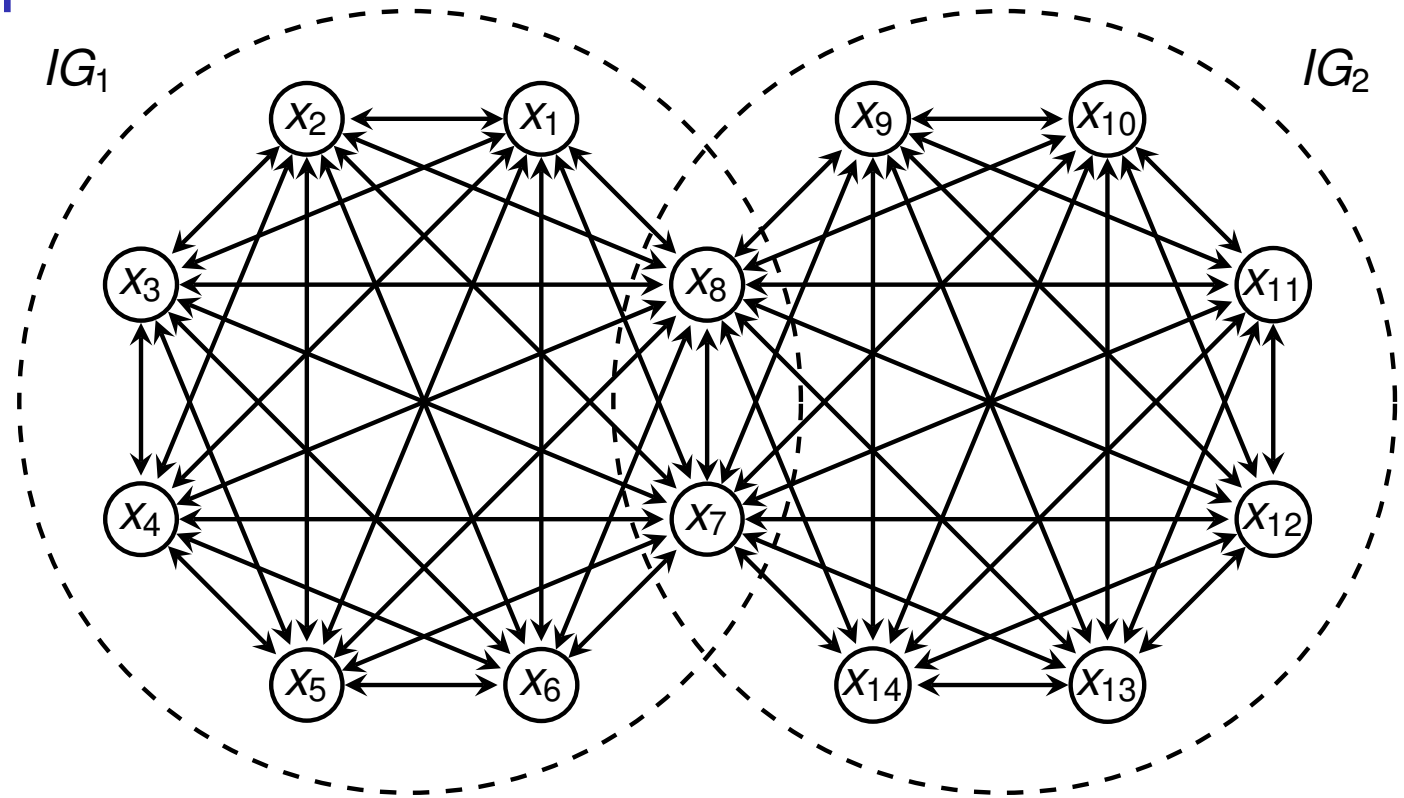


grupos formados pelos nós do sistema

relações de confiança e amizade entre os nós

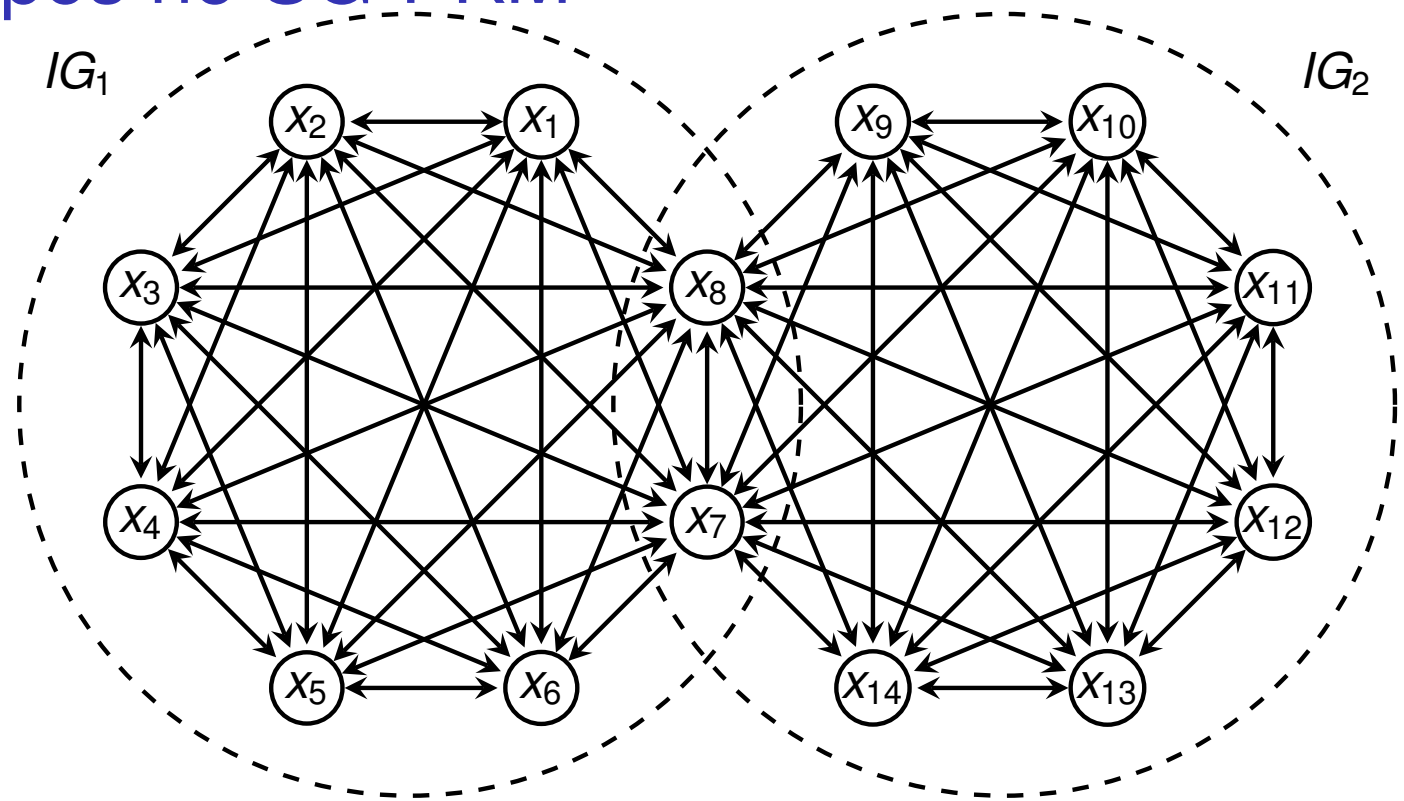
ligações físicas entre dois nós

Os grupos no SG-PKM



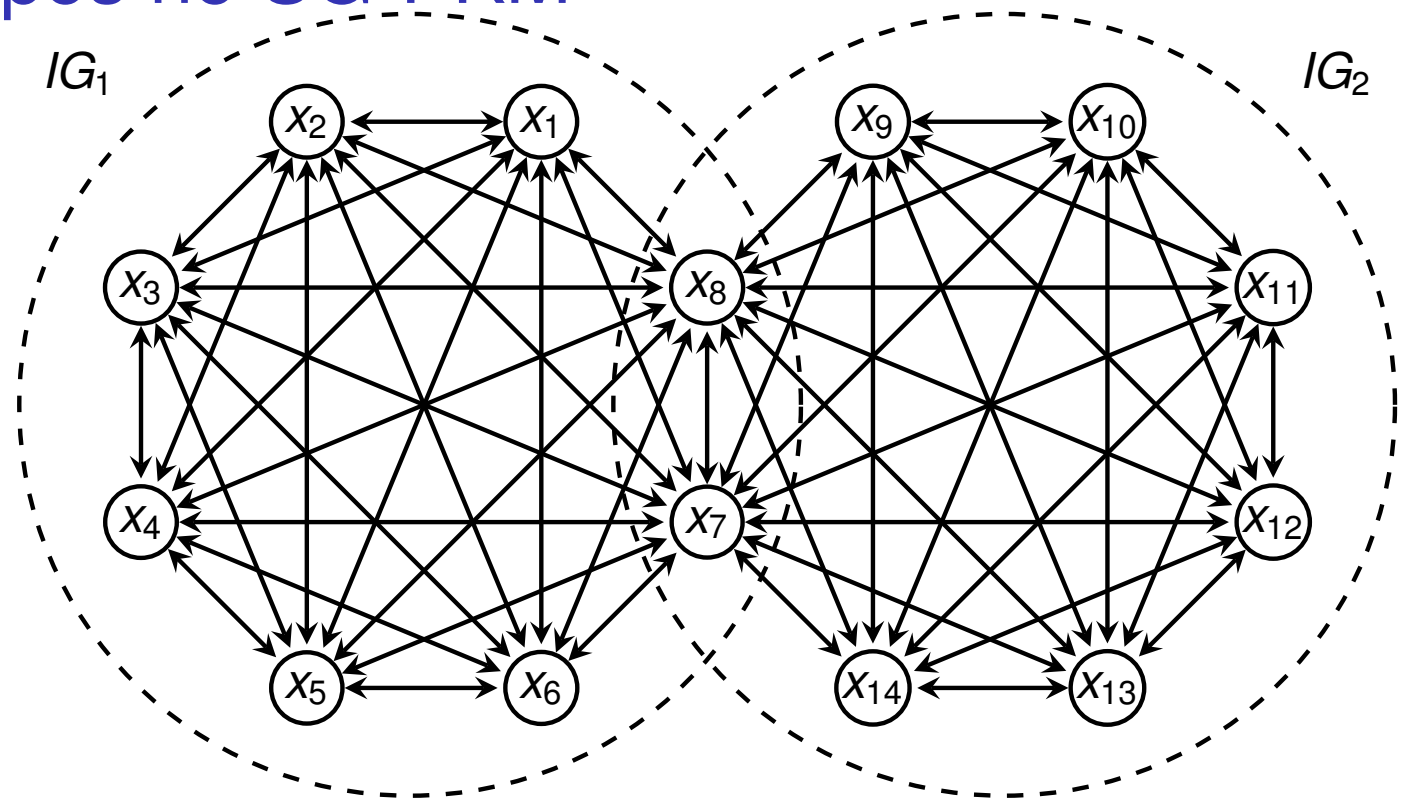
- Nó deseja entrar no sistema
  - Forma um grupo com outros $m - 1$ nós
  - Não é necessário um “líder”

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



- 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_u
  - 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_u
  - certificado $C_{SK_\gamma}^{x_v}$ 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

Outras operações do SG-PKM

- Atualização
  - certificados de nós:
  - certificados de grupos:
- Revogação **explícita**
  - certificados de nós:
  - certificados de grupos:
- Revogação **implítica**
  - baseada no **tempo de validade** dos certificados

Métricas para a avaliação

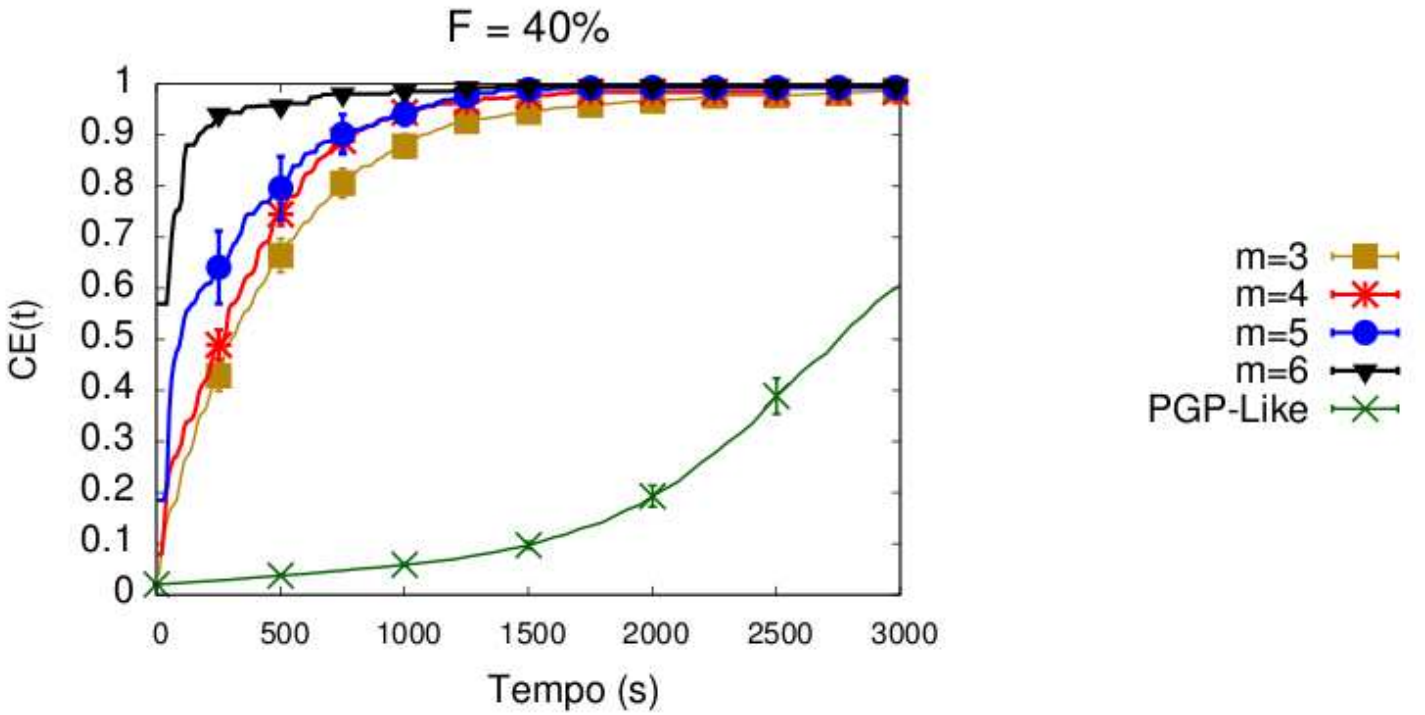
- *Convergência das trocas de certificados (CE)*
- *Autenticabilidade dos usuários (UA)*
- Alcançabilidade dos grupos (GR)

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

Simulações no NS-2

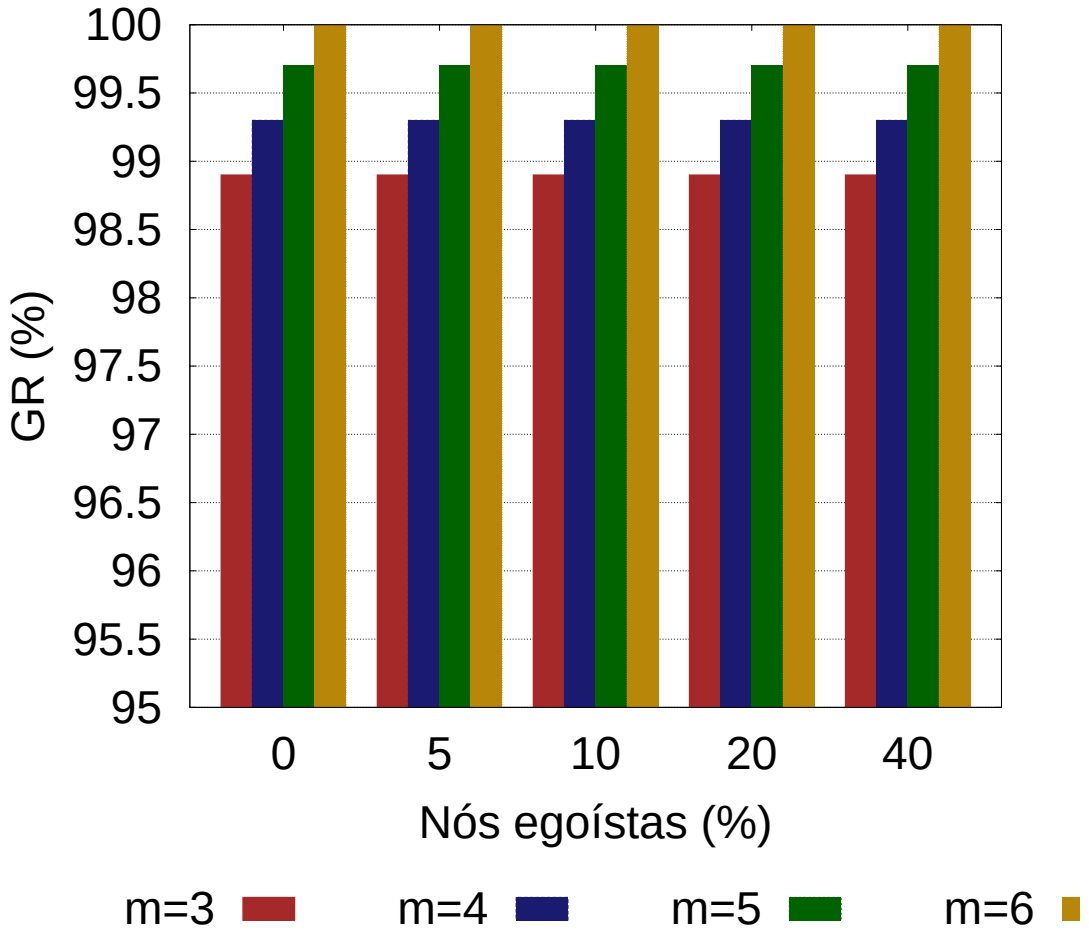
Parâmetro	**Valores utilizados**
Raio de alcance	50 e 120 metros
Quantidade de nós	100 nós
Velocidades máximas	5, 10 e 20 m/s
Tamanho dos grupos	**3, 4, 5 e 6**
Tamanho do ambiente	1000 x 1000 metros 1500 x 300 metros
Tipo de movimentação	*waypoint* aleatório
Tempo máximo de pausa	20 segundos
Tempo entre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

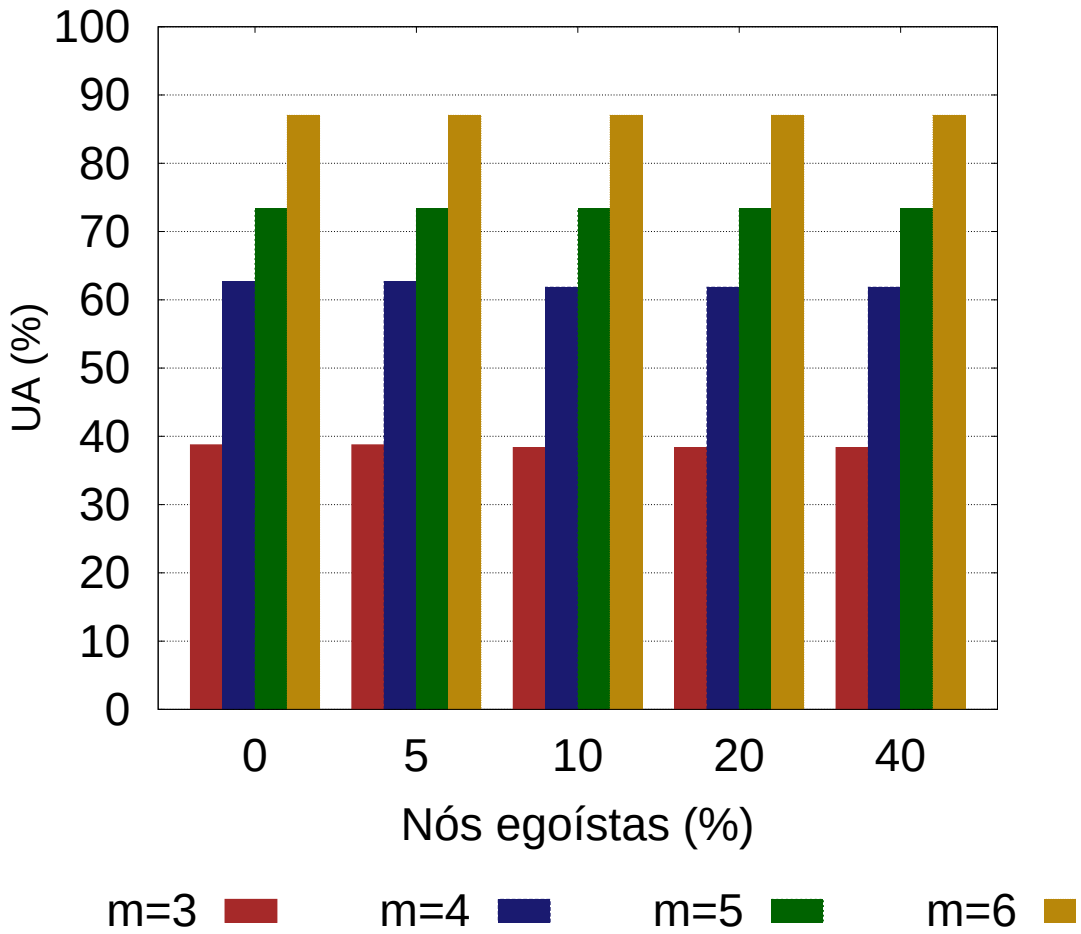


OBS: Resultados com velocidade de 20 m/s, raio de alcance de **50 m**, tamanho do ambiente do 1000x1000 metros e 40% de atacantes

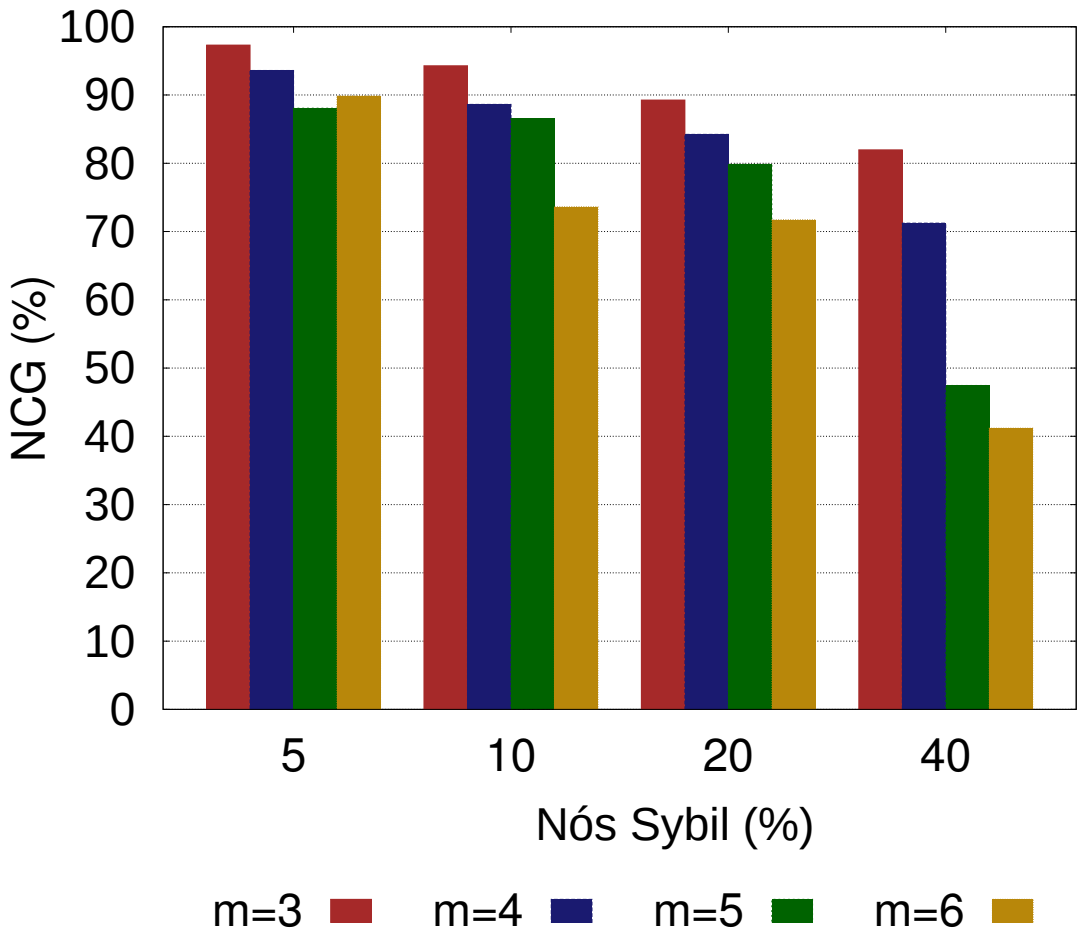
Alcançabilidade dos grupos



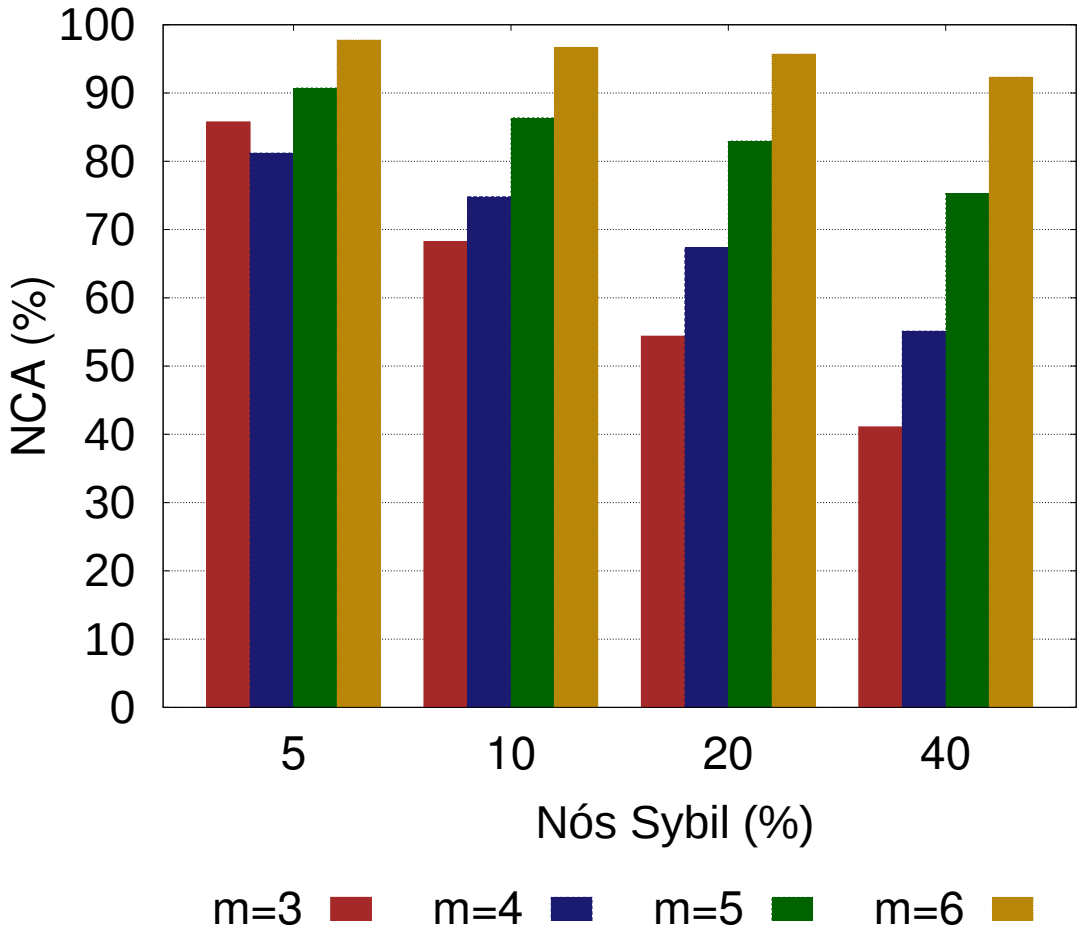
Autenticabilidade dos usuários



Grupos não-comprometidos



Autenticações não-comprometidas



Considerações finais

- As **características** das MANETs:
  - as tornam altamente vulneráveis a ataques
  - dificultam a implementação de serviços **eficazes** e **seguros**
- O PGP-Like é:
  - **considerado** um dos melhores esquemas para MANETs
  - totalmente **vulnerável** a ataques Sybil
- Este trabalho propôs um novo esquema, o SG-PKM
  - nós formam grupos baseados em **relações de amizades**
  - exige cadeias de certificados **disjuntas** na autenticação
- Os resultados mostraram que o SG-PKM:
  - conseguiu **resistir** aos ataques Sybil:
    - na maioria dos casos, as identidades falsas não foram **autenticadas** pelos nós **não-comprometidos**

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

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!