Gerenciamento de chaves públicas sobrevivente baseado em grupos para MANETs

Eduardo da Silva, Aldri L. dos Santos, Luiz Carlos P. Albini[1]

[1]NR2 – Programa de Pós-Graduação em Informática
Universidade Federal do Paraná – Curitiba – PR – Brasil

{eduardos,aldri,albini}@inf.ufpr.br

Resumo. *Dentre os diversos sistemas de gerenciamento de chaves propostos para as MANETs, o Sistema de Gerenciamento de Chaves Públicas Auto-organizado tem sido o mais indicado, por ser completamente distribuído e auto-organizável. Contudo, ele é totalmente vulnerável a ataques Sybil. Este trabalho apresenta um sistema de gerenciamento de chaves públicas sobrevivente a tais ataques, chamado de SG-PKM. Nesse sistema, os nós formam grupos a partir das suas relações de amizade e emitem certificados entre os membros do grupo. Além disso, os grupos emitem certificados entre si para garantir a autenticidade das suas chaves públicas. Para autenticarem-se, dois nós sem uma relação direta devem formam no mínimo duas cadeias de certificados ligando os grupos a que pertencem. Resultados obtidos via simulações mostram a sobrevivência do sistema diante de ataques Sybil, garantindo mais de 70% de autenticações não comprometidas para grupos com cinco ou seis membros diante de 40% de nós maliciosos.*

1. Introdução

As redes ad hoc móveis (MANETs) são estabelecidas dinamicamente sem depender de uma infraestrutura fixa ou administração centralizada e o seu funcionamento é mantido pelos próprios nós de uma forma auto-organizada [Papadimitratos and Haas 2005]. Um dos grandes desafios dessas redes é prover segurança para as aplicações, pois elas herdam os problemas de segurança das redes sem fio convencionais e agregam novos, devido às suas características particulares. Portanto, as MANETs são altamente susceptíveis a diversos tipos de ataques [Bannack et al. 2008, Wu et al. 2006].

Diferentes tipos de ataques podem ter uma grande efeito sobre um sistema de gerenciamento de chaves. Dentre eles, destacam-se os ataques de falta de cooperação e Sybil [Bannack et al. 2008]. O ataque de falta de cooperação consiste em um nó não colaborando com a rede para economizar recursos. O ataque Sybil consiste em um nó criando múltiplas identidades falsas utilizando um único dispositivo físico. Essas identidades adicionais podem ser fabricadas ou roubadas de nós legítimos.

Criptografia é a principal técnica usada para garantir a segurança das redes. As técnicas criptográficas dependem de chaves, que são informações relacionadas aos nós comunicantes e são usadas em conjunto com os algoritmos criptográficos. O gerenciamento de chaves consiste na administração segura dessas chaves. Contudo, fornecer uma entidade confiável para esse gerenciamento nas MANETs é uma tarefa difícil [Buttyán and Hubaux 2002]. Assim, o gerenciamento de chaves nas MANETs deve considerar características como a topologia dinâmica, ser auto-organizado e descentralizado [da Silva et al. 2008a, van der Merwe et al. 2007].

Entre os diversos esquemas propostos para as MANETs, um dos principais é o *Sistema de Gerenciamento de Chaves Públicas Auto-Organizado* [Čapkun et al. 2003],

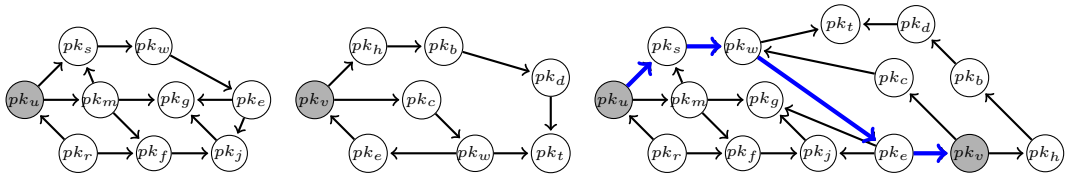
chamado neste trabalho de PGP-*Like*. No entanto, esse sistema não foi projetado considerando a existência de ataques de má-conduta, oferecendo apenas um mecanismo de detecção de certificados conflitantes. Neste trabalho, a eficácia do PGP-*Like* foi avaliada diante de ataques de falta de cooperação e *Sybil*, e os resultados mostram que ele é totalmente vulnerável a ataques *Sybil*.

Para solucionar essa vulnerabilidade, este trabalho propõe um sistema de gerenciamento de chaves públicas totalmente distribuído e auto-organizado para MANETs, chamado de *Sistema de Gerenciamento de Chaves Públicas Sobrevivente baseado em Grupos* (SG-PKM). Ele tem como objetivo manter o seu desempenho e eficácia diante de ataques de falta de cooperação e *Sybil*. No SG-PKM, os nós formam grupos baseados em relações de amizade. Além disso, as operações básicas baseiam-se na redundância de informações, sendo assim necessário mais de um nó para a confirmação de uma operação.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta as características do PGP-*Like* e o impacto dos ataques de má-conduta sobre ele. A Seção 3 descreve o SG-PKM, suas características e operações. A Seção 4 discute a avaliação do SG-PKM em cenários com ataques. Por fim, a Seção 5 contém as conclusões.

2. O sistema de gerenciamento de chaves públicas auto-organizado

No *Sistema de Gerenciamento de Chaves Públicas Auto-Organizado* (PGP-*Like*), os nós criam as suas chaves públicas e privadas e emitem certificados para os nós que eles confiam [Čapkun et al. 2003]. Esses certificados são armazenados e distribuídos pelos nós de uma forma auto-organizada e distribuída. Para isso, cada nó x_u mantém dois repositórios, o de certificados atualizados (G_u) e o de certificados não-atualizados (G_u^N). As Figuras 1(a) e 1(b) ilustram os repositórios G_u e G_v dos nós x_u e x_v. A Tabela 1 contém a notação utilizada na descrição dos sistemas de gerenciamento de chaves deste trabalho.



(a) Repositório G_u (b) Repositório G_v (c) $G_u \cup G_v$ e os caminhos de certificados

Figura 1. Repositórios de certificados atualizados dos nós x_u e x_v

Quando o nó x_u deseja verificar a autenticidade da chave pública pk_v do nó x_v, ele busca um caminho do vértice pk_u até pk_v $(pk_u \rightsquigarrow pk_v) \in G_u$. Caso $\nexists (pk_u \rightsquigarrow pk_v) \in G_u$, x_u cria $G_1 = G_u \cup G_v$ (Figura 1(c)). Nesse caso, a cadeia $(pk_u \rightarrow pk_s \rightarrow pk_w \rightarrow pk_e \rightarrow pk_v)$ pode ser utilizada. Caso $\nexists (pk_u \rightsquigarrow pk_v) \in G_1$, então ele usa informações de G_u^N. Se $\exists (pk_u \rightsquigarrow pk_v) \in G_u \cup G_u^N$, x_u precisa atualizar todos os certificados expirados ou não-atualizados junto aos seus respectivos emissores. Por fim, $\nexists (pk_u \rightsquigarrow pk_v) \in G_u \cup G_u^N$, x_u não realiza a autenticação de pk_v.

Tabela 1. Notação usada na descrição dos sistemas de gerenciamento de chaves

Notação	Descrição
x_u	Identidade do nó u
pk_u / sk_u	Chave pública/privada de x_u
$pk_u \rightsquigarrow pk_v$	Cadeia de certificados entre pk_u e pk_v
S	Conjunto de nós do sistema
G	Grafo de certificados do sistema

Notação	Descrição
IG_α	Identidade do grupo α
PK_α / SK_α	Chave pública/privada de IG_α
$pk_u \rightarrow pk_v$	Certificado de pk_v emitido por n_u
NC	Nós não-comprometidos no sistema
F	Conjunto de nós Sybil no sistema

O PGP-*Like* oferece um mecanismo de troca periódica de certificados, no qual cada nó solicita os repositórios dos seus vizinhos. Após sucessivas trocas, os certificados emitidos podem estar armazenados por todos os nós. Essa característica, no entanto, tornam o PGP-*Like* vulnerável a ataques *Sybil*, pois um nó malicioso não precisa comprometer outros nós para iniciar um ataque. O mecanismo de detecção de certificados conflitantes do PGP-*Like* não impede que um atacante crie uma identidade falsa, emita um certificado para ela e convença um usuário correto de que esse certificado é válido[da Silva et al. 2008b].

2.1. Avaliação do funcionamento do PGP-Like diante de ataques

Na avaliação do PGP-*Like* sob ataques de falta de cooperação e *Sybil*, foi utilizado o simulador NS 2.30. Os cenários possuem 100 nós, com raio de alcance de 50 e 120 metros, em um ambiente de 1000 x 1000 e 1500 x 300 metros. A movimentação segue o padrão *waypoint* aleatório, com velocidades máximas de 5, 10 e 20 m/s e tempo de pausa máximo de 20s. São emitidos 600 certificados aleatórios durante a formação da rede e as trocas de certificados ocorrem a cada 60 segundos. São considerados 5%, 10%, 20% e 40% de atacantes. Os resultados são médias de 35 simulações com intervalo de confiança de 95%. A Tabela 2 resume as métricas utilizadas nesta avaliação: Convergência nas Trocas de Certificados (CE), Alcançabilidade dos Nós (UR), Confiabilidade em Identidades Falsas (FIC), Autenticação Indireta de Identidades Falsas (IA) e Certificados Suspeitos (SC).

Tabela 2. Métrica utilizadas na avaliação do PGP-Like

Métrica	Representação		Descrição
CE	$\frac{\sum_{x_i \in S} CE_i(t)}{\lvert S \rvert}$	$CE_i(t) = \frac{\sum_{x_a, x_b \in S} (pk_a \rightarrow pk_b) \in (G_i \cup G_i^N)}{\sum_{x_x, x_y \in S} (pk_x \rightarrow pk_y) \in G}$	Tempo para que os certificados alcancem todos os nós
UR	$\frac{\sum_{x_i \in S} UR_i(t)}{\lvert S \rvert}$	$UR_i = \frac{\sum_{x_a \in S} (pk_i \rightsquigarrow pk_a) \in (G_i \cup G_i^N)}{\lvert S \rvert}$	Eficácia das trocas de certificados para a autenticação das chaves
FIC	$\frac{\sum_{x_i \in NC} FIC_i}{\lvert NC \rvert}$	$FIC_i = \begin{cases} 1 & \text{caso} \quad \exists\, x_f \in (G_i \cup G_i^N) \\ 0 & \text{caso contrário} \end{cases}$	Tempo para que uma identidade falsa se torne parte dos repositórios dos nós
IA	$\frac{\sum_{x_i \in NC} IA_i}{\lvert NC \rvert}$	$IA_i = \begin{cases} 1 & \text{caso} \quad \exists (pk_i \rightsquigarrow pk_f) \in (G_i \cup G_f) \\ 0 & \text{caso contrário} \end{cases}$	Percentual de identidades falsas autenticadas por nós não-comprometidos
SC	$\frac{\sum_{x_i \in NC} SC_i}{\lvert NC \rvert}$	$SC_i = \frac{\sum_{x_z \in G_i} \sum_{x_f \in F} (pk_z \rightarrow pk_f) \in G_i}{\lvert G_i \rvert}$	Certificados emitidos por um nó *Sybil* armazenados por nós não-comprometidos

Inicialmente, o PGP-*Like* foi avaliado em cenários com ataques de falta de cooperação, considerando as métricas CE e UR. Esses resultados foram omitidos e estão disponíveis na versão completa da dissertação[1].

Diante de ataques *Sybil*, foram consideradas as métricas FIC, IA e SC na avaliação do PGP-*Like*. O gráfico FIC da Figura 2 mostra que quanto maior a quantidade de nós maliciosos, menos tempo é necessário para que as identidades falsas sejam propagadas. Nessas simulações, os nós *Sybil* emitem certificados falsos desde a formação da rede. O gráfico IA da Figura 2 indica que, independente do número de nós maliciosos, as autenticações de identidades falsas via junção dos repositórios de certificados é sempre 100%. Por fim, o gráfico SC da Figura 2 mostra que a quantidade de certificados suspeitos nos repositórios dos nós aumenta com o número de nós maliciosos no sistema.

3. Gerenciamento de chaves públicas sobrevivente baseado em grupos

Esta seção apresenta o esquema de gerenciamento de chaves distribuído e auto-organizado proposto, chamado de *Sistema de Gerenciamento de Chaves Públicas Sobrevivente ba-*

[1]Em `http://www.nr2.ufpr.br/eduardo/publications/dissertacao.pdf`

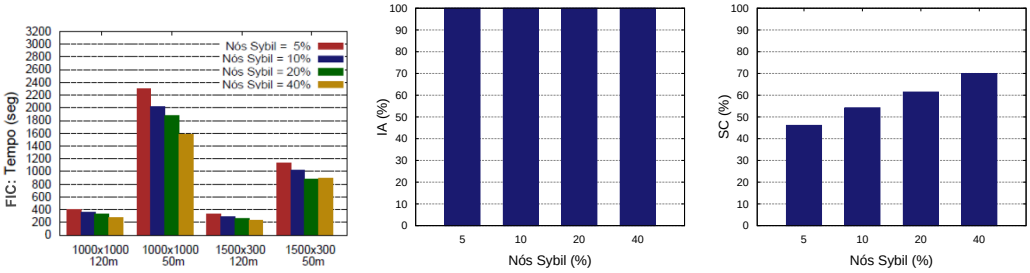


Figura 2. Avaliação do PGP-Like diante de ataques Sybil

seado em Grupos para MANET (SG-PKM). O SG-PKM tem como objetivo manter o seu desempenho e eficácia diante de ataques de falta de cooperação e *Sybil*. Nele os nós formam grupos baseados em relações de amizades. Baseado em [Zhang et al. 2008], assume-se uma confiabilidade bidirecional, em que, se x_i confia em x_j, então x_j confia em x_i. Os nós de um grupo servem como testemunhas na emissão de certificados para os demais nós do grupo. Além disso, os grupos podem se inter-relacionar, emitindo certificados mutuamente. Esse inter-relacionamento forma um grafo de certificados de grupos.

O SG-PKM pode ser abstraído em três camadas (Figura 3): o **modelo de rede** representa as ligações físicas entre os nós; o **modelo de confiança** representa as relações de confiança e amizade existentes; o **modelo de grupo** representa os grupos formados. Este último é denotado por um grafo $G = (IG, E)$, no qual IG representa o conjunto dos grupos e E os certificados emitidos entre os grupos. Cada nó cria seu par de chaves pública e privada e, para participar do sistema, precisa formar um grupo com outros $(m-1)$ nós. Nesses pequenos grupos de tamanho m, todos os nós possuem o mesmo papel e não é necessária a presença de um líder. A Figura 4 ilustra dois grupos, IG_1 e IG_2.

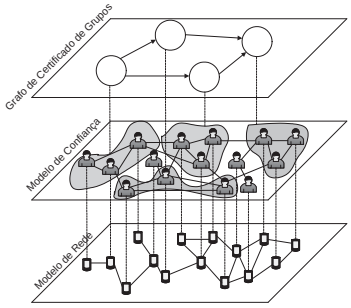


Figura 3. Camadas do SG-PKM

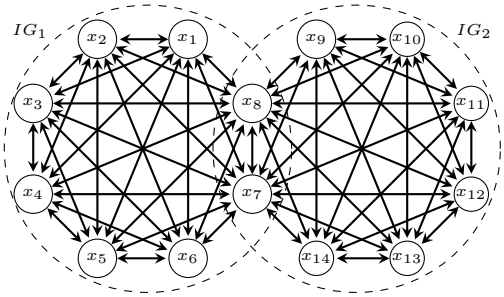


Figura 4. Inter-relacionamento dos grupos

Na formação de um grupo IG_α, os nós constroem colaborativamente as chaves pública (PK_α) e privada (SK_α) do grupo. Essas chaves podem ser construídas utilizando qualquer esquema de acordo de chaves distribuído e sem a existência de uma terceira entidade confiável [Pedersen 1991]. Em seguida, a chave pública do grupo é diponibilizada a todos os nós da rede e a chave privada é distribuída entre os m nós do grupo seguindo um esquema de criptografia de limiar [Shamir 1979]. Além disso, são emitidos *certificados de nós* assinados com SK_α, associando a chave pública de cada nó com a sua identidade.

Em uma segunda etapa, os grupos emitem *certificados de grupos* entre si, associando a chave pública de um grupo com a sua identidade. Assim, se os membros de um dado grupo IG_α acreditam que a chave pública PK_β pertence ao grupo IG_β, eles emitem um certificado assinado com a chave privada SK_α, associando a identidade IG_β

com a chave pública PK_β. Esse certificado é armazenado por todos os membro de IG_α e IG_β. Para obterem mais informações sobre os certificados emitidos no sistema, os nós periodicamente trocam os seus certificados com os vizinhos.

Para armazenar os certificados, cada nó x_i possui um repositório de certificados atualizados de grupos (G_i) e um de certificados não-atualizados de grupos (G_i^N). Quando um nó x_u, membro de IG_α, deseja autenticar a chave pública do nó x_v, membro de IG_β, ele obtém o certificado de x_v com a identificação de IG_β. Para autenticar o certificado apresentado, x_u deve obter no mínimo duas cadeias disjuntas de certificados válidos de grupos ligando PK_α a PK_β em G_u ou em $G_u \cup G_v$. Por fim, o SG-PKM também permite operações de atualização e a revogação dos certificados de nós e de grupos.

O detalhamento das operações e do funcionamento do SG-PKM encontram-se na versão completa da dissertação. São detalhadas as etapas para a emissão dos certificados de nós e a construção colaborativa dos certificados de grupos, assim como o formato desses certificados. Também estão descritos os algoritmos de trocas de certificados e autenticação, validação, atualização, revogação e auto-revogação de certificados e as equações criadas para o entendimento do sistema proposto.

4. Avaliação do SG-PKM

A avaliação do SG-PKM consiste na análise da formação dos grupos, da sobrecarga de comunicação e a sua eficácia diante de ataques de falta de cooperação e *Sybil*.

4.1. Análise da formação dos grupos

A formação dos grupos é um requisito para um nó participar do sistema. Assim, a possibilidade da existência de tais grupos em uma rede de amigos foi analisada empiricamente. Para isso, foi aplicada a metodologia e as métricas propostas em [Latapy et al. 2008] sobre uma rede social de amigos real, uma sub-rede do PGP[2]. Essa base de dados é denotada por um grafo direcionado, formado por 956 vértices e 14647 arestas. Nesse caso, o conjunto de vértices representa os usuários do PGP, enquanto o conjunto de arestas, as relações de confiança entre eles.

Na avaliação, essa base de dados foi transformada em um grafo simétrico, do qual foram extraídos os cliques máximos. No SG-PKM, os cliques representam os grupos e indicam que todos os nós trocaram simetricamente as suas chaves públicas. A Tabela 3 resume as estatísticas sobre os cliques no grafo analisado. O número de cliques com um tamanho igual a 4, 5 ou 6 é maior do que os outros. Esses resultados confirmam a possibilidade das formações de grupos, necessários para o funcionamento do sistema.

Tabela 3. Estátisticas dos cliques para o grafo do PGP

Tamanho dos cliques	1	2	3	4	5	6
# de cliques	956	14647	47661	78016	77160	49150
# de cliques máximo	9	1921	4460	6599	6395	4893

4.2. Sobrecarga de comunicação

A sobrecarga de comunicação do SG-PKM foi calculada considerando: (i) Δh é a média do número de saltos entre os nós do sistema; (ii) L é o conjunto dos nós que solicitaram

[2]Disponível em `http://keyring.debian.org/`

uma validação do certificado de grupo que está sendo atualizado ou revogado. Os custos apresentados na Tabela 4 são quantidades de mensagens trocadas na operação. É importante ressaltar que, após a convergência das trocas de certificados, a maioria das operações de autenticação são realizadas localmente, não gerando sobrecarga na comunicação.

Tabela 4. Custo de comunicação das operações

Operação	Notação	Custo de comunicação
Autenticação	$ACO(C_{SK_\beta}^{x_v})$	$(URREQ + m.URREP)\ .\ \Delta h$
Validação	$VCO(C_{SK_\delta}^{IG_\omega})$	$(m.VREQ + m.VREP)\ .\ \Delta h$
Revogação de nó	$RCO(C_{SK_\alpha}^{x_j})$	$(3(\lvert IG_\alpha - x_i\rvert) + \lvert IG_\beta : IG_\beta \rightarrow IG_\alpha \in G\rvert + \lvert L\rvert)\ .\ \Delta h$
Revogação de grupo	$RCO(C_{SK_\alpha}^{IG_\beta})$	$(3(\lvert IG_\alpha - x_i\rvert) + \lvert L\rvert)\ .\ \Delta h$
Atualização de nó	$UCO(C_{SK_\alpha}^{x_i})$	$(3\lvert IG_\alpha - x_i\rvert)\ .\ \Delta h$
Atualização de grupo	$UCO(C_{SK_\alpha}^{IG_\beta})$	$(3\lvert IG_\alpha - x_i\rvert + \lvert IG_\beta - IG_\alpha\rvert + \lvert L\rvert)\ .\ \Delta h$

4.3. Análise da eficácia diante de ataques

A avaliação do SG-PKM diante de ataques de falta de cooperação e *Sybil* considera os mesmos parâmetros usados na avaliação do PGP-*Like*. A criação das chaves públicas e privadas e a emissão dos certificados de nós e de grupos acontecem durante a formação dos grupos. O tamanho dos grupos varia entre 3 e 6 membros. Por limitação de espaço, são apresentados apenas os cenários de 1000x1000m e 20 m/s de velocidade máxima. Os resultados dos demais cenários encontram-se na versão completa da dissertação. A Tabela 5 resume as métricas utilizadas nesta avaliação: Convergência das Trocas de Certificados (CE), Alcançabilidade dos Grupos (GR), Autenticabilidade dos Nós (UA), Grupos Não-Comprometidos (NCG) e Autenticações Não-Comprometidas (NCA).

Tabela 5. Métrica utilizadas na avaliação do SG-PKM

Métrica	Representação		Descrição
CE	$\frac{\sum_{i \in X} CE_i(t)}{\lvert X\rvert}$	$CE_i(t) = \frac{\sum_{IG_\alpha, IG_\beta \in IG\ (PK_\alpha \rightarrow PK_\beta) \in (G_i \cup G_i^N)}}{\sum_{IG_\gamma, IG_\delta \in IG\ (PK_\gamma \rightarrow PK_\delta) \in G}}$	Tempo para os nós terem todos os certificados em seus repositórios
GR	$\frac{\sum_{i \in X} GR_i(t)}{\lvert X\rvert}$	$GR_i(t) = \sum_{\substack{IG_\alpha \in IG_{x_i} \\ IG_\beta \in IG}} (PK_\alpha \rightsquigarrow PK_\beta) \in (G_i \cup G_i^N)$	Percentagem de grupos encontrados nos repositórios dos nós
UA	$\frac{\sum_{i \in X} UA_i}{\lvert X\rvert}$	$UA_i = \sum_{j \in X} (x_i \rightsquigarrow x_j) \in (G_i \cup G_j \cup G_i^N)$	Percentagem de autenticações dos usuários
NCG	$\frac{\sum_{IG_\alpha \in IG} NCG_\alpha}{\lvert IG\rvert}$	$NCG_\alpha = \begin{cases} 1 & \text{se} \quad \nexists\, f \in IG_\alpha \\ 0 & \text{caso contrário} \end{cases}$	Taxa de grupos não comprometidos diante de nós desonestos
NCA	$\frac{\sum_{i \in X} NCA_i}{\lvert X\rvert}$	$NCA_i = \begin{cases} 1 & \text{se} \quad \nexists\, (pk_i \rightsquigarrow pk_f) \quad \forall f \in F \\ 0 & \text{caso contrário} \end{cases}$	Taxa de autenticações de grupos não comprometidas por atacantes

Inicialmente, foi comparada a eficácia do SG-PKM com o PGP-*Like* diante de ataques de falta de cooperação, considerando a métrica CE. Nesse caso, devido à similaridade de comportamento, são apresentados apenas os resultados em cenários com 40% de atacantes. Como ilustrado no gráfico CE da Figura 5, ele sempre alcança 100%. Além disso, em todos os casos, o SG-PKM converge antes que o PGP-*Like*.

O gráfico GR da Figura 5 indica que, independente da percentagem de atacantes, a alcançabilidade dos grupos é praticamente 100%. Mesmo quando esse valor não alcança 100%, ele fica acima dos 99%. Porém isso não significa que todos os nós podem autenticar-se mutuamente, pois é preciso formar no mínimo duas cadeias disjuntas de certificados de grupos. O gráfico UA da Figura 5 mostra que a autenticabilidade dos nós sempre apresenta os mesmos valores, independente da quantidade de atacantes. Isso mostra a sobrevivência do SG-PKM. Além disso, UA aumenta na medida em que aumenta o tamanho dos grupos. Quando $m = 6$, ele alcança mais que 85%, e quando $m = 3$, cerca

de 40%. Isso ocorre porque com grupos pequenos é mais difícil criar redundâncias entre eles e, consequentemente, formar as cadeias disjuntas de certificados.

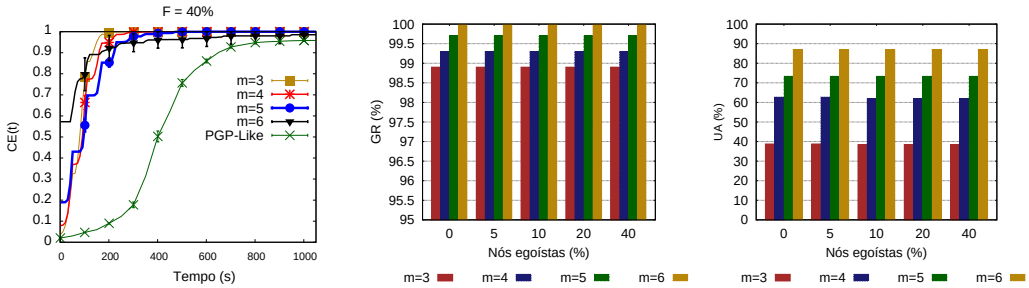


Figura 5. Avaliação do SG-PKM diante de ataques de falta de cooperação

O SG-PKM também foi avaliado na presença de nós *Sybil*, que criam identidades falsas, formam grupos com essas identidades e tentam comprometer nós autênticos para emitirem certificados para esses grupos falsos. O gráfico NCG da Figura 6 mostra que diminuindo o tamanho dos grupos, aumenta-se o impacto dos ataques *Sybil*. Contudo, mesmo com 20% de atacantes, o percentual de grupos não afetados é maior que 70%.

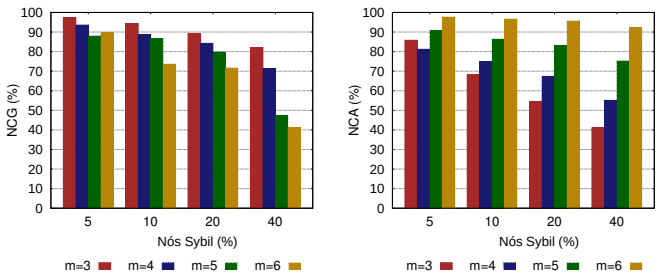


Figura 6. Avaliação do SG-PKM diante de ataques Sybil

Finalmente, o gráfico NCA da Figura 6 apresenta o impacto dos ataques *Sybil* nas autenticações do SG-PKM. Os resultados mostram que quanto maior os grupos, maior é a resistência ao ataque *Sybil*. Mesmo diante de 40% de nós maliciosos, esse ataque não compromete o sistema. Com $m = 5$, NCA é maior do que 75% e com $m = 6$ ele é cerca de 92%. Esses resultados mostram que o SG-PKM é altamente sobrevivente a esses ataques, pois mesmo que os nós maliciosos consigam participar dos grupos, eles geralmente não conseguem ser autenticados pelos nós não-comprometidos. Isso ocorre devido à exigência de cadeias disjuntas de certificados de grupos nas autenticações.

5. Conclusões

Este trabalho propôs um novo esquema de gerência de chaves para MANETs, chamado de SG-PKM, que tem como objetivo manter o seu desempenho e eficácia diante de ataques de falta de cooperação e Sybil. O sistema de gerência de chaves atualmente mais indicado para as MANETs, PGP-*Like*, é totalmente vulnerável a ataques do tipo *Sybil*. No SG-PKM, os nós formam grupos baseados em relações de amizade. Nesses grupos, eles trocam suas chaves públicas e emitem certificados mutuamente. Um grupo também pode emitir certificados para outros grupos.

Os resultados mostram que o SG-PKM conseguiu manter o mesmo desempenho que o PGP-Like diante de ataque de falta do cooperação. Já sob ataques *Sybil*, o SG-PKM é muito mais eficaz. Na maioria dos casos, as identidades falsas não conseguiram comprometer a quantidade necessária de nós para participarem dos grupos e, mesmo

quando conseguiram participar, na maioria das vezes não foram autenticadas pelos nós não-comprometidos. Concluindo, o SG-PKM apresenta uma boa robustez contra ataques de falta de cooperação e *Sybil*, apresentando uma alta sobrevivência a esses ataques.

O desenvolvimento deste trabalho proporcionou as seguintes contribuições: levantamento das fraquezas e vulnerabilidades do PGP-*Like*; criação de métricas para a quantificação do impacto dos ataques de falta de cooperação e *Sybil*; avaliação do PGP-*Like* diante desses ataques; apresentação do esquema de gerenciamento de chaves SG-PKM; análise da possibilidade das formações de grupos e dos relacionamentos entre os grupos; avaliação do SG-PKM diante de ataques de falta de cooperação e *Sybil*. Essas contribuições possibilitaram as seguintes publicações: [da Silva et al. 2008a, da Silva et al. 2008b, Bannack et al. 2008, Nogueira et al. 2009, da Silva et al. 2009, e Silva et al. 2009].

Referências

Bannack, A., da Silva, E., Lima, M. N., dos Santos, A. L., and Albini, L. C. P. (2008). Segurança em redes ad hoc. In *Anais do XXVI Simpósio Brasileiro de Telecomunicações (SBRT '08)*, pages 19–20.

Buttyán, L. and Hubaux, J.-P. (2002). Report on a working session on security in wireless ad hoc networks. In *Mobile Computing and Communications Review*, volume 6.

Čapkun, S., Buttyán, L., and Hubaux, J.-P. (2003). Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 2(1):52–64.

da Silva, E., Lima, M. N., dos Santos, A. L., and Albini, L. C. P. (2008a). Identity-based key management in mobile ad hoc networks: Techniques and applications. *IEEE Wireless Communications Magazine*, 15:46–52.

da Silva, E., Lima, M. N., dos Santos, A. L., and Albini, L. C. P. (2008b). Quantifying misbehaviour attacks against the self-organized public key management on manets. In *Proceedings of the International Conference on Security and Cryptography (SECRYPT '08)*, pages 128–135.

da Silva, E., Lima, M. N., dos Santos, A. L., and Albini, L. C. P. (2009). *Analyzing the Effectiveness of the Self-organized Public-Key Management System on MANETs under the Lack of Cooperation and the Impersonation Attacks*, volume 48 of *Springer CCIS*, pages 166–179. Springer.

e Silva, R. F., da Silva, E., and Albini, L. C. P. (2009). 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 2009)*, pages 155–158.

Latapy, M., Magnien, C., and Vecchio, N. D. (2008). Basic notions for the analysis of large two-mode networks. *Social Networks*, 30(1):31–48.

Nogueira, M., Pujolle, G., da Silva, E., dos Santos, A., and Albini, L. C. P. (2009). Survivable keying for wireless ad hoc networks. In *Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management (IM '09)*, pages 606–613.

Papadimitratos, P. and Haas, Z. J. (2005). *Securing mobile ad hoc networks*, chapter 21, pages 457–481. CRC Press - Auerbach Publications, Boca Raton, Florida, USA.

Pedersen, T. P. (1991). A threshold cryptosystem without a trusted party. In *Proceedings of Advances in Cryptology (EuroCrypt '91)*, volume 547 of *LNCS*, pages 522–526, London, UK. Springer.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11):612–613.

van der Merwe, J., Dawoud, D., and McDonald, S. (2007). A survey on peer-to-peer key management for mobile ad hoc networks. *ACM Computing Survey*, 39(1):1.

Wu, B., Chen, J., Wu, J., and Cardei, M. (2006). *A survey on attacks and countermeasures in mobile ad hoc networks*, chapter 12, pages 103–136. Springer-Verlag, New York, NY, USA.

Zhang, C., Song, Y., and Fang, Y. (2008). Modeling secure connectivity of self-organized wireless ad hoc networks. In *Proceedings of the 27th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '08)*, pages 251–255.