Uma Avaliação do Esquema de Gerenciamento de Chave Baseado em Identidade *Identity Key Management*

Murilo W. S. Lima [1]
Eduardo da Silva [1 2]
Luiz Carlos Pessoa Albini [1]

Resumo: A segurança é um dos principais desafios nas Redes Ad Hoc Móveis (MANETs - Mobile Ad Hoc Networks). As características naturais das MANETs tornam essas redes altamente vulneráveisaà muitos ataques, desde a camada física até a camada de aplicação. Existem diversos algoritmos e protocolos para tratar com essas ameaças. Todos esses algoritmos têm um elemento comum: o uso da criptografia. Entre os sistemas criptográficos encontrados na literatura, os baseados em identidade parecem melhor se adaptar ao paradigma das MANETs. Suas principais vantagens são o baixo custo computacional e a sobrecarga reduzida. Este trabalho apresenta uma avaliação do principal esquema criptográfico baseado em identidade para as MANETs, o Identity Key Management (IKM). A avaliação foi realizada considerando a renovação e revogação de chaves e a presença de ataques de falsa acusação. Os resultados mostram que o IKM é vulnerável a esse ataque e o particionamento da rede pode levá-lo a um estado instável.

Abstract: Security is one of the main issues in Mobile Ad Hoc Networks (MANETs). MANETs natural features make them highly vulnerable to several attacks ranging from the physical up to the application layer. There are several algorithms and protocols to deal with these threats. All of them have a common element, the use of cryptography. Among the cryptographic systems found in the literature, the identity based ones seem to best fit the MANETs paradigm. Their main advantages are the low computational cost and the reduced overhead. This work presents an evaluation of the main identity based cryptographic scheme for MANETs, the Identity Key Management (IKM). The evaluation was performed considering the key renovation, the key revocation and the presence of false accusation attacks. Results show that the IKM is vulnerable to this attack, and the partition of the network might lead it to an unstable state.

[1]NR2 – Departamento de Informatica, UFPR
{mwsl06;eduardos;albini}@inf.ufpr.br
[2]IFC – Instituto Federal Catarinense
eduardo@ifc-araquari.edu.br

1 Introdução

Com o desenvolvimento das tecnologias de comunicação sem fio e dos dispositivos móveis, como telefones móveis, smartphones, PDAs e tablets, as redes ad hoc móveis (MANETs - *Mobile Ad Hoc Networks*) têm ganhado muita atenção tanto da academia como das empresas. Essas redes não possuem infraestrutura e o seu funcionamento deve ser mantido pelos próprios nós, de forma autônoma, adaptativa e auto-organizada [5]. Devido às suas características e flexibilidade, essas redes são alternativas atrativas para ambientes em que a infraestrutura de rede é muito cara ou possa estar comprometida. MANETs estão em uso atualmente em ambientes militares, redes veiculares, redes espaciais e vêm ganhando cada vez mais atenção no campo das telecomunicações. Estudos indicam que a próxima geração da comunicação sem fio unirá os conceitos e tecnologias das redes sem fio convencionais com as rede sem fio sem infraestrutura [12].

Entretanto, as MANETs são suscetíveis a diversos tipos de ataques [9] provenientes da comunicação sem fio, que é sujeita a interferências e interceptações, ou pela ação de nós maliciosos. Por serem dinâmicas e abertas, essas redes podem sofrer particionamentos e desconexões. Além disso, a mobilidade obriga que os mecanismos de segurança sejam distribuídos, facilitando ataques como de falsa acusação e personificação [18].

Técnicas de criptografia têm sido amplamente utilizadas para proteger as comunicações de dados. Por meio dessas técnicas, os dados são cifrados de forma que podem ser lidos somente pelo destinatário da mensagem. Os dados cifrados são protegidos contra o acesso, a leitura e a modificação não autorizadas [16]. Todas as operações criptográficas dependem de chaves de criptografia. A manutenção das chaves e de todo o material criptográfico relacionado é conhecida como gerenciamento de chaves. Esquemas de gerenciamento de chaves devem considerar a geração, armazenamento, distribuição, proteção e revogação das chaves, bem como devem garantir que elas estejam disponíveis aos nós autênticos. Nas MANETs, esquemas de gerenciamento de chaves devem ser distribuídos e auto-organizados [10].

Os sistemas de criptografia, ou criptossistemas, podem ser classificados em simétricos e assimétricos, dependendo da forma com a qual as chaves criptográficas são criadas, mantidas e utilizadas. A criptografia simétrica utiliza uma única chave secreta para cifrar e decifrar mensagens. Há duas abordagens de criptografia simétrica para MANETs. A primeira distribui uma única chave para todos os nós na inicialização da rede. Essa solução é inviável visto que qualquer nó, ao ser atacado, representa uma ameaça à rede inteira. A segunda abordagem distribui para cada par de nós, uma chave simétrica conhecida apenas pelos dois nós. Essa técnica, embora mais segura que a primeira, apresenta duas desvantagens: falta de escalabilidade, requer o uso de N^2 chaves; e sobrecarga de armazenamento, pois cada nó precisa armazenar $N-1$ chaves. Além disso, a criptografia simétrica não suporta assinaturas

digitais [5].

A criptografia assimétrica, também conhecida como criptografia de chaves públicas, utiliza um par de chaves para cada nó: uma chave pública e outra privada. A chave pública é distribuída livremente na rede, enquanto a chave privada é conhecida apenas pelo seu proprietário. Uma mensagem cifrada com a chave pública pode ser decifrada somente com a sua respectiva chave privada e vice-versa. Essa técnica criptográfica garante a confidencialidade das mensagens trafegadas, como também a autenticidade do emissor e receptor [13].

Os esquemas de criptografia assimétrica podem ou não ser baseados em certificados. Nos esquemas baseados em certificados, as chaves públicas dos nós são autenticadas por meio de certificados assinados por uma entidade confiável, centralizada ou distribuída, que associa a chave pública com o seu respectivo proprietário. Nas MANETs, os certificados emitidos podem ser distribuídos durante a inicialização da rede ou sob demanda, usando uma entidade confiável para a emissão e autenticação desses certificados. Contudo, estabelecer uma entidade confiável é um grande desafio nessas redes, devido à sua descentralização e à ausência de um modelo de confiança [19]. Existem diversos estudos sobre a aplicação da criptografia assimétrica baseada em certificados para MANETs [19, 21, 1].

Os esquemas de criptografia assimétrica sem certificados não requerem a emissão e, consequentemente, o gerenciamento dos certificados de chaves públicas. Uma classe de criptossistemas sem certificados é conhecida como Criptografia Baseada em Identidade (IBC - *Identity Based Cryptography*) [17]. Nesse tipo de criptografia, a chave pública de um nó é identificada por uma cadeia de caracteres única e amplamente conhecida, como um endereço de IP, endereço MAC ou e-mail, e a chave privada é derivada diretamente dessa cadeia. Esses esquemas requerem um gerenciamento de chaves mais simples e possuem um custo computacional e de armazenamento menor que os criptossistemas baseados em certificados, sendo atrativos para as MANETs [6]. Recentemente, diversos estudos têm sido realizados aplicando IBCs em MANETs [14, 8, 2, 11, 20].

Dentre os esquemas de gerenciamento de chaves baseados em identidades para MANETs, o IKM (*Identity Key Management for MANETs*) [20] é o mais importante. O IKM é o único que fornece revogação e atualização de chaves em operações totalmente distribuídas. Contudo, esse esquema não foi avaliado diante de ataques de mal comportamento. Apenas um estudo inicial foi realizado em [7]. Dessa forma, este trabalho estende [7], apresentando uma avaliação do IKM em cenários com particionamento e ataques de falsa acusação, conhecidos como *bad mouthing*. Os resultados mostram que o IKM é vulnerável aos ataques de falsa acusação e que suas funcionalidades podem ser comprometidas pelo particionamento da rede. Além disso, este trabalho apresenta um estudo do custo de comunicação nas operações de revogação e atualização de chaves e o atraso encontrado nessas atualizações.

O restante deste trabalho está organizado da seguinte forma: a Seção 2 apresenta os

principais esquemas de gerenciamento de chaves baseados em identidade para MANETs; a Seção 3 discute o funcionamento do IKM, com suas características e vulnerabilidades; a Seção 4 descreve a avaliação do IKM e apresenta a discussão dos resultados encontrados; por fim, a Seção 5 contém as conclusões e considerações finais.

2 Criptografia baseada em identidade para MANETs

A criptografia baseada em identidade (IBC - *Identity Based Criptograpy*) [17] é uma alternativa aos métodos baseados em certificados, possuindo um gerenciamento de chaves mais simples e um custo menor de armazenamento. Esse tipo de criptografia permite que as chaves públicas sejam derivadas diretamente da identidade dos nós, enquanto que as chaves privadas são geralmente geradas por uma entidade chamada Gerador de Chave Privada (PKG - *Private Key Generator*) [3]. O PKG pode ser uma entidade externa ou interna à rede. Cada nó é capaz de descobrir a chave pública de outro nó sem trocar nenhuma mensagem.

O uso de criptografia baseada em identidade tem seu maior impacto no gerenciamento das chaves, podendo afetar diretamente seu desempenho e segurança. A maioria dos esquemas de gerenciamentos de chaves baseados em identidade para MANETs utilizam técnicas de criptografia de limiar, associadas a uma entidade segura para distribuição de chaves privadas. Existem diversos esquemas de gerência de chaves baseados em identidades para MANETs. Os principais são apresentados a seguir e um estudo mais abrangente sobre a aplicação destes esquemas pode ser encontrado em [6].

Khalili-Katz-Arbaugh O gerenciamento de chaves proposto em [14] combina técnicas de criptografia de limiar com criptografia baseada em identidade. Todos os nós que inicializam a rede formam um PKG distribuído, chamado PKG de limiar. O PKG de limiar possui uma chave privada mestre, que é distribuída entre os n nós da rede usando um esquema de criptografia de limiar t-sobre-n. A chave pública mestre é distribuída a todos os nós.

Para receber sua chave privada, um nó X apresenta a identidade para pelo menos t nós do PKG de limiar. Cada um desses nós calcula uma parte da chave privada e a envia ao nó solicitante. Recebendo t partes, o nó X monta sua chave privada. O esquema assume que as identidades são gravadas em hardware e não podem ser alteradas. Além disso, o esquema não prevê revogações ou atualizações de chaves.

Deng-Mukherjee-Agrawal O esquema proposto em [8] possui dois componentes: a geração de chaves distribuída e a autenticação baseada em identidade. A geração de chaves fornece a chave mestre da rede e o par de chaves pública/privada de cada nó. O mecanismo de autenticação baseado em identidade fornece autenticação e confidencialidade fim-a-fim entre os nós.

O par de chaves pública/privada mestre é computado e distribuído da mesma maneira que no esquema proposto por Khalili-Katz-Arbaugh. A segurança na transmissão das t partes das chaves privadas é garantida utilizando chaves públicas temporárias. Cada nó do PKG envia sua respectiva parte da chave privada assinada com a chave pública temporária do nó. Esse esquema não prevê revogações ou atualizações de chaves.

Bohio-Miri O esquema de Bohio-Miri [2] assume que os nós são inicializados antes da formação da rede, obtendo seus parâmetros públicos e suas chaves privadas de um PKG externo. Quando dois nós querem se comunicar, eles calculam uma chave simétrica usando uma função *hash*, de forma não interativa e sem o envolvimento do PKG. Esse procedimento é chamado "acordo de chaves", e gera uma sobrecarga na rede, pois usa mensagens de *broadcast*. Para reduzir esta sobrecarga, os autores propõem o uso de chaves simétricas por grupo, eliminando a necessidade de acordos entre os nós do grupo.

Como as chaves do nó e de *broadcast* são simétricas, o esquema não garante a irretratabilidade das operações e não impede ataques de personificação. Além disso, o esquema de Bohio-Miri também não prevê revogação ou atualização de chaves e requer estruturas de suporte e servidores online, violando os princípios dos IBCs [4].

Identity-Based Authentication and Key Exchange O *Identity-Based Authentication and Key Exchange* (IDAKE) [11] consiste em duas versões: MANET-IDAKE básico e MANET-IDAKE totalmente distribuído. O IDAKE usa chaves simétricas e assimétricas em ambas as técnicas. Na versão básica, existe uma fase de inicialização, com acesso ao PKG. Após a inicialização, acontece a fase de execução, na qual são realizadas as operações de criação de chaves simétricas, atualização e revogação de chaves. A fase de execução não requer o uso de um PKG. Para isso, o PKG deve inicializar todos os nós que entram na rede após a sua formação.

Na versão totalmente distribuída, todas as tarefas são realizadas pelos próprios nós da rede, sem nenhum PKG externo. O PKG externo é emulado utilizando um esquema de limiar t-sobre-n. Contudo, não é especificado como as chaves são distribuídas aos nós.

A Tabela 1 sumariza as principais características dos esquemas apresentados anteriormente. É importante notar que o Bohio-Miri e o IDAKE-Básico usam PKG externos. Os esquemas Khalili-Katz-Arbaugh e Deng-Mukherjee-Agrawal não tratam revogação e renovação de chaves. Além disso, apenas o esquema Deng-Mukherjee-Agrawal especifica uma maneira de distribuição das chaves após a formação da rede.

Tabela 1. Comparativo dos esquemas de gerenciamento de chaves baseados em identidade

	Khalili-Katz-Arbaugh	**Deng-Mukherjee-Agrawal**	**Bohio-Miri**	**IDAKE Básico**	**IDAKE Distribuído**
Limiar	Sim	Sim	Não	Não	Sim
PKG	Interno	Interno	Externo	Externo	Interno
Revogação	Não	Não	Sim	Sim	Sim
Renovação	Não	Não	Sim	Sim	Sim
Chaves assimétricas	Sim	Sim	Não	Sim	Sim
Distribuição das chaves privadas	Canal seguro	Chaves temporárias	Antes da inicialização	Antes da inicialização	Não especificada

3 Esquema *Identity Key Management* (IKM)

Esta seção apresenta as características e o funcionamento do *Identity Key Management* (IKM) [20]. No IKM, cada nó possui um par de chaves pública/privada que são utilizadas nas operações de autenticação, acordo de chaves, cifração e assinatura digital. O algoritmo do IKM é descrito em três fases: pré-distribuição, atualização e revogação de chaves.

3.1 Pré-distribuição de chaves

A pré-distribuição ocorre na inicialização da rede. Nela, o PKG externo equipa cada nó com o material criptográfico necessário para o funcionamento da rede. Ele gera os parâmetros das funções criptográficas, monta e distribui o segredo compartilhado, gera as chaves de todos os nós e os parâmetros de atualização de chaves. Dentre os parâmetros gerados, está a função *hash H*, usada para a construção das chaves das próximas fases da rede. O PKG também distribui as tarefas administrativas da rede a alguns nós, a fim de habilitar atualizações e revogações de chaves. Ele ainda distribui as funcionalidades do próprio PKG a n nós da rede utilizando um esquema de criptografia de limiar t-sobre-n. Os n nós escolhidos formam o conjunto Ω, chamado D-PKG.

O PKG também gera também dois números aleatórios K_{p1} e K_{p2} , que são os segredos da rede. K_{p1} não é inserido na rede e é de conhecimento apenas do PKG. Cada nó $V \in$ D-PKG armazena uma parte distinta de K_{p2}, em um esquema de criptografia de limiar. Assim, um nó do D-PKG precisa da colaboração de outros $t - 1$ nós do D-PKG para formar K_{p2}. Além disso, todos os nós da rede devem conhecer quem são os membros do D-PKG.

O IKM é composto por fases de atualização de chaves, denotadas por p_i em que $1 \leq i \leq M$, sendo M o maior índice de fase. Cada fase p_i é denotada por uma cadeia binária $salt_i$. O par de chaves pública/privada de cada nó contém um elemento específico do nó e um

elemento específico da fase. O par de chaves pública/privada do nó A para a fase i é denotado pela tupla $< K_{A,p_i}, K^{-1}_{A,p_i} >$, na qual K_{A,p_i} é a chave pública na fase p_i, K^{-1}_{A,p_i} é a chave privada para a fase p_i e -1 indica que o elemento é uma chave privada. Esses elementos são atualizados a cada mudança de fase. K_A e K_A^{-1} formam o elemento específico do nó A e, portanto, não mudam no decorrer da rede. Essas informações são enviadas do PKG para os nós na inicialização da rede. Além disso, o PKG também inicializa o par de chaves da primeira fase.

3.2 Revogação das chaves

A revogação de chaves no IKM é formada por três subprocessos: notificação de mal comportamento, geração da revogação e verificação da revogação.

Notificação de mal comportamento Uma vez que um nó A detecta o mal comportamento de um outro nó B, o nó A gera uma mensagem de acusação assinada com K^{-1}_{A,p_i} contra o nó B. Essa mensagem é enviada a todos os nós do D-PKG via *unicast*, pois se o nó B recebê-la, pode apresentar um comportamento correto temporariamente. Além disso, um nó do D-PKG considera que um nó B se comporta inadequadamente somente após receber γ acusações durante uma janela de tempo pré-determinada.

Na inicialização da rede, o PKG inicializa todos os nós com uma função F relacionando cada nó com um conjunto de nós do D-PKG. Essa função de mapeamento é definida como: $F(ID_B) = ID_{X_j} | 1 \leq j \leq \beta, X_j \in \Omega, X_j \neq \beta$, em que β representa o número de nós do D-PKG. Essa função define os nós do D-PKG que devem receber as acusações contra o nó B. Nota-se que β representa um *trade-off* entre a resiliência do sistema contra ataques e a sobrecarga de rede gerada no processo de notificação. No caso em que $\beta = 1$, um nodo em $F(ID_B)$ pode ter um comportamento inadequado e escapar da revogação. No outro extremo, $\beta = n$, há uma ótima resiliência, porém a sobrecarga de comunicação é muito maior.

Geração da revogação Ao receber uma acusação, o D-PKG irá descartá-la caso a acusação seja contra o próprio nó de origem. Ao atingir o limiar γ, um nó do D-PKG gera uma revogação parcial e a publica para toda a rede. Essa revogação parcial será usada em conjunto com outras revogações parciais para gerar uma revogação completa contra um nó mal comportado.

Cada nó possui um líder associado a ele no D-PKG. que deve coletar as revogações parciais dos outros nós do D-PKG. A coleta é dividida em dois casos: $\beta \geq t$ e $\beta < t$. Se $\beta \geq t$, o líder coleta t revogações parciais. Se $\beta < t$, o líder coleta as revogações parciais e envia elas aos outros $t - \beta$ nós do D-PKG escolhidos aleatoriamente. Esses nós podem responder ao líder com revogações parciais, completando as t revogações parciais. O IKM prevê o caso em que um ou mais nós do D-PKG possuam mal comportamento. Neste caso, a

revogação é realizada de forma similar a $\beta < t$.

Verificação da revogação Uma vez que o líder gera uma revogação contra o nó B, essa revogação é enviada a todos os nós por meio de uma inundação. Os nós, ao receberem uma revogação, devem verificar sua autenticidade e armazená-la. O IKM prevê mecanismos de troca de revogações entre vizinhos.

3.3 Atualização de chaves

O IKM descreve um mecanismo de atualização de chaves para prevenir ataques de criptoanálises e limitar potenciais danos causados por chaves inválidas. Esta atualização pode ocorrer periodicamente ou quando um limite de nós revogados é atingido. Um nó A pode atualizar sua chave pública seguindo: $K_{A,p_{i+1}} = (H(ID_A), H(salt_{i+1}))$.

Para a geração da chave privada, é necessária a colaboração de t nós de Ω. A atualização ocorre quando um nó em Ω inicia uma nova fase. Esse nó deve escolher aleatoriamente outros $t-1$ nós do D-PKG e enviar uma requisição de chaves parciais para eles. Após juntar as $t-1$ partes, o nó constrói a chave privada comum a todos os nós da rede. Por fim, ele envia uma mensagem a todos os nós não revogados contendo a chave gerada. Para isso, utiliza uma variante do esquema descrito em [15], que possibilita que os nós com chaves de fases anteriores consigam atualizá-las.

4 Avaliação do IKM

Inicialmente, apresenta-se uma avaliação analítica considerando as características das MANETs. Em seguida, apresenta-se os resultados das simulações avaliando a eficácia do IKM em cenários com ataques de falsa acusação.

4.1 Avaliação Analítica

PKG Externo Quando um nó X deseja entrar na rede, ele deve contatar um PKG externo para receber o seu material criptográfico. Em seguida, ele deve contatar os nós do D-PKG e solicitar o seu par de chaves específicos da fase. Contudo, manter um PKG externo e confiável pode ser difícil nas MANETs. Além disso, a ausência de um PKG externo após a inicialização da rede pode dificultar a entrada de novos nós no sistema.

Particionamento da Rede O IKM considera $t = n/2$. Porém, por questões de segurança contra falhas e ataques maliciosos, os esquemas baseados na criptografia de limiares requerem $t > n/2$. Assumindo $t = n/2$, o IKM torna-se vulnerável a ataques de mal com-

portamento e ao particionamento da rede. A Figura 1a ilustra um cenário em que o IKM é configurado para usar um esquema 3-sobre-6. Após a inicialização da rede, os nós se movimentam livremente e a rede é dividida em duas, com três nós do D-PKG em cada parte (Figura 1b). Os nós das duas partições são capazes de contatar um D-PKG funcional e as atualizações e revogações de chaves são válidas em ambas, podendo levar a estados inconsistentes.

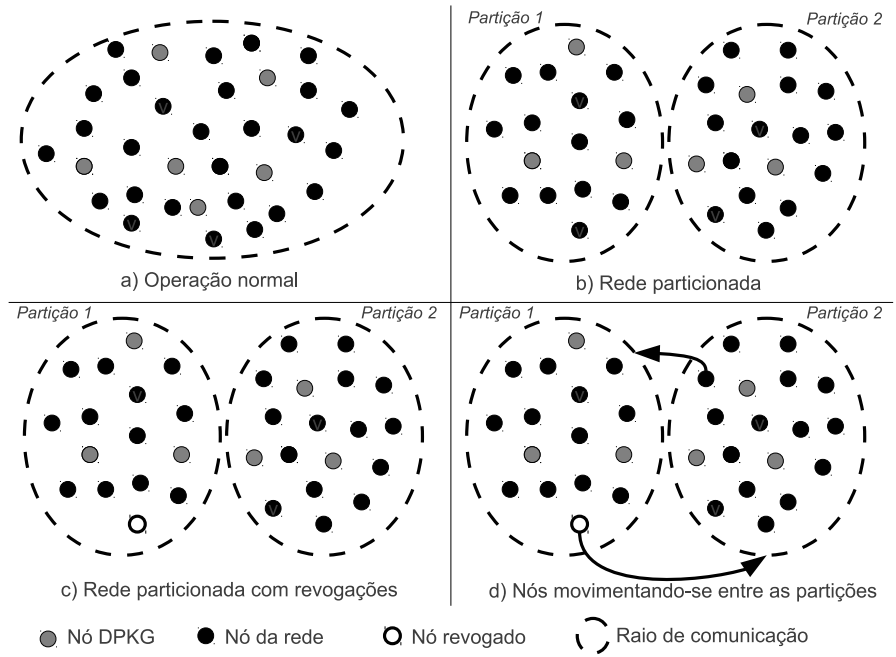

Figura 1. Particionamento da rede com segredo compartilhado 3-sobre-6

No exemplo da Figura 1c, os nós da primeira partição da rede podem revogar a chave privada de um nó comprometido. Como a rede está particionada, os nós na outra partição não serão informados sobre a revogação, causando inconsistência entre as informações dos nós D-PKGs. Caso o nó comprometido se mova para a outra partição, ele pode usar suas chaves normalmente (Figura 1d). Se as chaves do nó comprometido forem de outra fase, ele só precisa esperar pela próxima fase para receber a atualização de sua chave privada.

4.2 Resultados das simulações

O IKM foi avaliado por meio de simulações utilizando o *Network Simulator* 2.31, considerando os mesmos cenários usados originalmente no IKM [20]. Os ambientes simu-

lados possuem 50 nós distribuídos em uma área quadrada de 700 x 700 m. O protocolo de acesso ao meio é o IEEE 802.11 e o modelo de propagação é o de reflexão no solo de dois raios. A Tabela 2 descreve todos os parâmetros considerados nas simulações. Os resultados apresentados são médias de 35 simulações com um intervalo de confiança de 95%.

Tabela 2. Parâmetros considerados nas simulações

Parâmetro	**Valor usado**
Dimensão da rede	700 x 700 m
Raio de transmissão	250 m
Quantidade de nós	50 nós
Modelo de mobilidade	*waypoint* aleatório
Modelo de propagação	Reflexão no solo em dois raios
Velocidade máxima	5, 10 e 20 m/s
Tempo máximo de pausa	5 segundo
(n, t)	(10, 5) e (20, 10)
Atacantes	De 1 a 10 nós
Acusações requiridas	Igual a t
Atacantes em conluio	$t + 5$ nós

Eficácia da Revogação Inicialmente, o IKM foi avaliado em cenários sem a presença de nós maliciosos e com $\beta = t$. Em teoria, quando $\beta = t$, o IKM apresenta um comportamento mais seguro sob ataques de falsa acusação. Nestas simulações, o número de acusadores varia entre t e $t + 5$. Dessa forma, com $n = 10$ e $t = 5$, o número de acusadores varia de cinco a dez nós e, com $n = 20$ e $t = 10$, o número de acusadores varia de 10 a 15 nós.

A Figura 2 ilustra o percentual de revogações de chaves não realizadas. Os resultados mostram que com $n = 20$ e $\beta = t = 10$, a porcentagem de revogações não realizadas chega a 100%. Dessa forma, o IKM não foi capaz de revogar chaves de nós comprometidos, não sendo eficaz em ambientes hostis. Em cenários com $n = 10$ e $\beta = t = 5$, a revogação se mostra mais eficiente. Mesmo assim, no melhor caso, quando o número de acusadores é igual a quatorze nós, a porcentagem de revogações não realizadas foi maior que 60%. Esses resultados mostram que o sistema pode ser vulnerável devido à dificuldade de revogar chaves mesmo com várias acusações.

O IKM também foi avaliado em cenários sob ataques de falsa acusação, com $1 \leq \beta \leq 3$. Neste tipo de ataque, os nós maliciosos atuam em conluio enviando acusações falsas contra um nó a fim de revogá-lo e removê-lo da rede. A simulação sob tais ataques é feita com cada nó malicioso enviando acusações contra o nó X ao D-PKG. As Figuras 3a e 3b mostram o impacto desses ataques no IKM. Nessas simulações, considera-se $\gamma = t$. Assim, quando $t = 5$, são necessárias cinco acusações distintas para revogar uma chave.

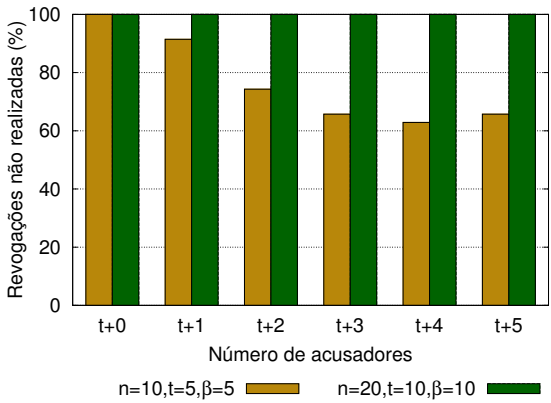

Figura 2. Revogações não realizadas em cenários sem ataques

A Figura 3a apresenta os resultados com $n = 10$, $t = 5$, $1 \leq \beta \leq 3$ e o número de atacantes (δ) variando entre cinco e dez ($5 \leq \delta \leq 10$). Quando $\beta = 1$ e $\delta = 5$, a porcentagem de ataques bem sucedidos é de quase 60% e alcança quase 95% de sucesso com $\beta = 1$ e $\delta = 10$. Além disso, aumentando o valor de β, reduz-se o impacto das falsas acusações, embora quando $\beta = 3$ e $\delta = 9$, ela ainda é maior que 60%.

A Figura 3b apresenta o impacto dos ataques de falsa acusação em cenários com $n = 20$, $t = 10$, $1 \leq \beta \leq 3$ e $5 \leq \delta \leq 10$. Nos cenários com $\beta = 1$ e $\delta = 10$, a porcentagem de ataques bem sucedidos é quase 40% e alcança quase 98% quando $\delta = 15$. Além disso, o aumento de β reduz o impacto do ataque, embora quando $\beta = 3$ e $\delta = 15$, ela ainda é quase 40%.

Esses resultados mostram a importância de uma boa escolha nos parâmetros n, t e β. Nos cenários sem atacantes, valores baixos para esses parâmetros funcionam melhor. Porém, isso pode causar a sobrecarga de poucos nós do sistema, pois reduz o tamanho do D-PKG. Por outro lado, ao mesmo tempo em que valores altos de n e t podem reduzir a sobrecarga do sistema, dividindo a tarefa de gerenciamento de chaves entre mais nós, eles tornam muito mais difícil a revogação de chaves comprometidas.

Já os resultados em cenário com atacantes mostram que é necessário usar β com valores altos para aumentar a segurança do IKM contra falsas acusações. Porém, valores elevados de β podem desabilitar completamente o mecanismo de revogação de chaves. Por isso, a escolha correta de β tem um grande impacto no comportamento do IKM. Um valor alto diminui a vulnerabilidade mas torna mais difícil realizar revogações corretas, incluindo revogações de nós maliciosos. Um valor baixo permite o funcionamento correto das revogações,

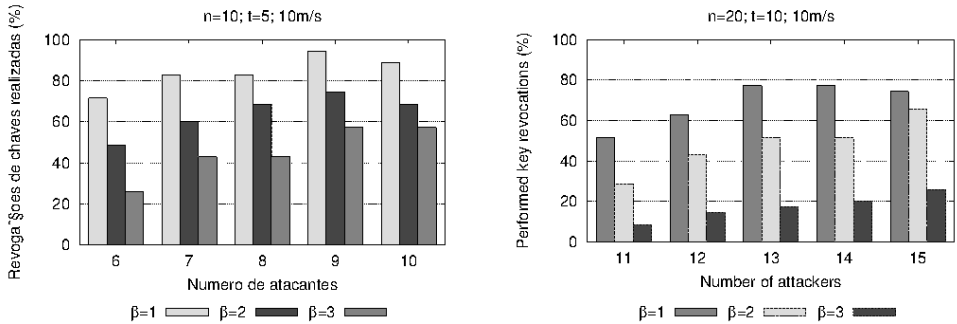

Figura 3. Impacto dos ataques de falsa acusação

entretanto torna o sistema vulnerável aos ataques.

Com isso, pode-se concluir que a configuração do IKM é vital para o seu correto funcionamento, pois deve-se encontrar um meio termo entre resistência a ataques e o funcionamento correto das revogações. Tudo isso prevendo o número máximo de atacantes que o sistema deve suportar. Esta análise é vital para qualquer sistema que venha a usar o IKM e ela faz parte de trabalhos futuros.

Sobrecarga de comunicação para a revogação O IKM também foi analisado considerando a sobrecarga de comunicação na revogação e na atualização das chaves. A sobrecarga do sistem nas outras operações é apresentada no artigo original do IKM [20].

A Figura 4a apresenta a sobrecarga de comunicação em quantidade de mensagens para $n = 10$, $t = 5$ e $\beta = 1$. É importante ressaltar que esse é o cenário que apresenta a menor sobrecarga, visto que cada acusador deve contatar apenas um nó do D-PKG. Para seis acusadores, são necessárias cerca de 80 mensagens para revogar uma única chave. Dessas mensagens, 60% delas têm como origem o D-PKG e como destino nós regulares e 30% são trocadas entre os nós do D-PKG.

A Figura 4b apresenta a sobrecarga de comunicação em quantidade de mensagens para $n = 20$, $t = 10$ e $\beta = 1$. Nesse caso, com 10 acusadores, o algoritmo requer aproximadamente 150 mensagens para revogar uma chave, sendo que cerca de 70% são mensagens trocadas entre D-PKGs. A quantidade de mensagens chega a quase 200, com 14 acusadores. Os resultados mostram que a sobrecarga da revogação das chaves no IKM depende diretamente do valor de t.

Por fim, a Figura 5 apresenta a sobrecarga de comunicação na atualização das chaves. Pode-se verificar que a sobrecarga também é diretamente proporcional ao valor de t.

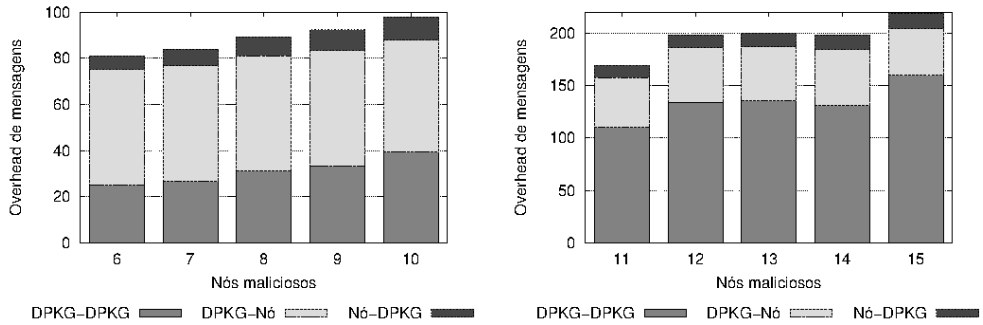

Figura 4. Sobrecarga na revogação de chaves

5 Conclusões

A próxima geração de comunicação móvel irá unir tecnologias das redes com fio e das redes sem fio móveis (MANETs). Porém, isso ainda é um grande desafio, visto que as MANETs ainda possuem muitas vulnerabilidades.

A criptografia é a principal técnica utilizada para prover segurança em MANETs. Diversos esquemas de gerenciamento de chaves podem ser encontrados na literatura. Entre eles há os esquemas de gerência de chaves baseados em identidades, que têm chamado a atenção devido à adaptação às características das MANETs. O *Identity-based key management* (IKM) é o principal esquema para tais redes.

Este trabalho apresentou uma avaliação do IKM sob ataques de falsa acusação (*Bad Mouthing*). Os resultados mostraram que o IKM é vulnerável ao ataque de falsa acusação. Além disso, pode-se notar que, para aumentar a segurança do IKM contra falsas acusações, é necessário usar um parâmetro β com valores altos. Porém, valores altos de β podem desabilitar todo o mecanismo de revogação do IKM. Outros aspectos de segurança do IKM foram estudados, tal como o particionamento de rede. Trabalhos futuros incluem o estudo do IKM sobre outros ataques e aspectos de segurança e a proposta de um esquema mais seguro de gerenciamento de chaves baseado em identidade.

Referências Bibliográficas

[1] Marc Bechler, Hans-Joachim Hof, Daniel Kraft, Frank Pählke, and Lars Wolf, *A cluster-based security architecture for ad hoc networks*, Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '04), vol. 4, IEEE Communications Society, marÃ§o 2004, pp. 2393–2403.

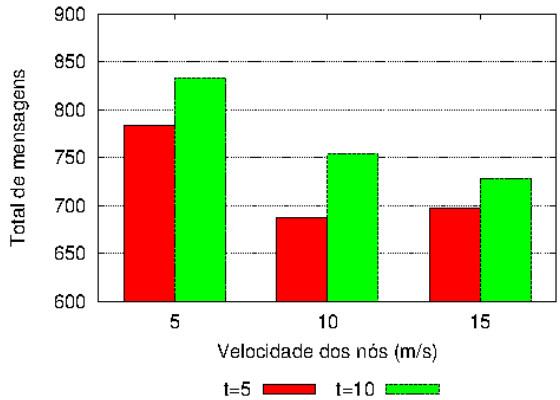

Figura 5. Sobrecarga de comunicação na atualização de chaves

[2] Muhammad J. Bohio and Ali Miri, *Efficient identity-based security schemes for ad hoc network routing protocols*, Ad Hoc Networks **2** (2004), no. 3, 309–317.

[3] Dan Boneh and Matthew K. Franklin, *Identity-based encryption from the weil pairing*, Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '01) (London, UK), Springer-Verlag, 2001, pp. 213–229.

[4] Hung-Yu Chien and Ru-Yu Lin, *Improved id-based security framework for ad hoc network*, Ad Hoc Networks **6** (2008), no. 1, 47–60.

[5] Imrich Chlamtac, Marco Conti, and Jennifer J.-N. Liu, *Mobile ad hoc networking: imperatives and challenges*, Ad Hoc Networks **1** (2003), no. 1, 13–64.

[6] Eduardo da Silva, Michele N. Lima, Aldri L. dos Santos, and Luiz Carlos P. Albini, *Identity-based key management in mobile ad hoc networks: Techniques and applications*, IEEE Wireless Communications Magazine **15** (2008), 46–52.

[7] Eduardo da Silva, Murilo Soares Lima, and Luiz Carlos Pessoa Albini, *Demonstrating the security vulnerabilities of the identity-based key management scheme for manets*, Proceedings of the 7th IEEE/SBrT International Telecommunications Symposium (ITS' 10), IEEE Communications, sep 2010.

[8] Hongmei Deng, Anindo Mukherjee, and Dharma P. Agrawal, *Threshold and identity-based key management and authentication for wireless ad hoc networks*, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) (Washington, DC, USA), vol. 2, IEEE Computer Society, 2004, p. 107.

[9] Djamel Djenouri, Lyes Khelladi, and Ndjib Badache, *A survey of security issues in mobile ad hoc and sensor networks*, IEEE Surveys and Tutorials **7** (2005), no. 4, 2–28.

[10] Anne Marie Hegland, Eli Winjum, Stig F. Mjolsnes, Chunmig Rong, Oivind Kure, and Pal Spilling, *A survey of key management in ad hoc networks*, IEEE Communications Surveys **08** (2006), no. 03, 48–66.

[11] Katrin Hoeper and Guang Gong, *Bootstrapping security in mobile ad hoc networks using identity-based schemes with key revocation*, Tech. Report CACR 2006-04, Centre for Applied Cryptographic Research, University of Waterloo, Waterloo, ON, Canada, 2006.

[12] J. Gnana Jayanthi, S. Albert Rabara, and A. Rex Macedo Arokiaraj, *Ipv6 manet: An essential technology for future pervasive computing*, Communication Software and Networks, International Conference on **0** (2010), 466–470.

[13] Jonathan Katz and Yehuda Lindell, *Introduction to modern cryptography (chapman & hall/crc cryptography and network security series)*, Chapman & Hall/CRC, 2007.

[14] Aram Khalili, Jonathan Katz, and William A. Arbaugh, *Toward secure key distribution in truly ad-hoc networks*, Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT '03) (Washington, DC, USA), IEEE Computer Society, 2003, p. 342.

[15] Donggang Liu, Peng Ning, and Kun Sun, *Efficient self-healing group key distribution with revocation capability*, Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03) (New York, NY, USA), ACM, 2003, pp. 231–240.

[16] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, Danvers, MA, USA, 1996.

[17] Adi Shamir, *Identity-based cryptosystems and signature schemes*, Proceedings of Advances in Cryptology (CRYPTO 84) (New York, NY, USA), Springer-Verlag New York, Inc., 1985, pp. 47–53.

[18] Bing Wu, Jianmin Chen, Jie Wu, and Mihaela Cardei, *A survey on attacks and countermeasures in mobile ad hoc networks*, ch. 12, pp. 103–136, Springer-Verlag, New York, NY, USA, 2006.

[19] Seung Yi and Robin Kravets, *MOCA: Mobile certificate authority for wireless ad hoc networks*, Proceedings of the 2nd Annual PKI Research Workshop (PKI '03) (Gaithersburg, MD, USA), NIST – National Institute of Standards and Technology, 2003.

[20] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang, *Securing mobile ad hoc networks with certificateless public keys*, IEEE Transactions on Dependable and Secure Computing **3** (2006), no. 4, 386–399.

[21] Lidong Zhou and Zygmunt J. Haas, *Securing ad hoc networks*, IEEE Network **13** (1999), no. 6, 24–30.