Implementação de um esquema de gerenciamento de chaves auto-organizado para redes ad hoc móveis

Eduardo da Silva[1]

[1] Universidade Federal do Paraná – Departamento de Informática
Caixa Postal 19081 – CEP 81531-900 – Curitiba – PR

eduardo.silva@gmail.com

Abstract. *It is proposed in this paper the implementation and tests of self-organized key management model fo mobile ad hoc networks presented in [Capkun et al. 2003a]. This model allows users to generate themselves theirs private-public keys, to issue certicates each others and to perform authentication without any central service. This model is very interesting to mobile ad hoc networks, since it does not require any trusted authority, even in the system initialization phase. The implementation and tests will be performed using NS-2.*

Resumo. *É proposto nesse artigo a implementação e testes do modelo de gerenciamento de chaves auto-organizado para redes ad hoc móveis apresentado em [Capkun et al. 2003a]. Esse modelo permite que os usuários gerem seus pares de chaves públicas e privadas, emitam certificados uns aos outros e realizem autenticação sem qualquer serviço centralizado. Esse modelo é bastante interessante para redes ad hoc móveis, uma vez que não necessita de qualquer autoridade confiável, nem mesmo na fase de inicialização do sistema. A implementação e testes serão realizados com a ferramenta NS-2.*

1. Introdução

Uma rede *ad hoc* móvel (MANET) é um grupo de computadores móveis sem fio, chamados nós, que cooperam entre si realizando o encaminhamento de pacotes, de forma a possibilitar a comunicação entre os nós, mesmo que a distância entre os nós comunicantes ultrapasse ao limite de transmissão do sinal direto sem fio [Hu et al. 2005]. Caso a distância entre os dois nós pares comunicantes ultrapasse ao limite de transmissão de sinal direto entre eles, os outro nós pertencentes à rede *ad hoc* realizam o roteamento e encaminhamento dos pacotes pela rede. Uma característica das redes *ad hoc*, é a ausência de infra-estrutura, ou seja, os nós pertencem a uma rede onde não existe o papel de uma unidade central, como por exemplo, uma estação base.

Diversas são as dificuldades encontradas para prover segurança nas MANETs, devido a diversos fatores. Alguns desses fatores foram discutidos em [Buttyan and Hubaux 2003] e são apresentados a seguir:

- o canal de comunicação sem fio é vulnerável, assim, as mensagens transmitidas na rede podem ser capturadas e também mensagens falsas podem ser injetadas na rede;
- os nós também são vulneráveis, principalmente por não estarem localizados em uma sala fisicamente protegida;

- a ausência de infraestrutura faz com que soluções clássicas de segurança, baseadas em autoridades certificadoras, não seja aplicáveis a essas redes;
- a topologia dinâmica dessas redes dificulta o processo de roteamento dos pacotes na rede, e ainda, informações incorretas de rotas podem ser criadas por intrusos ou por nós comprometidos. O desafio dos algoritmos de roteamento está em distinguir entre as mudanças de rotas causadas por mudança na topologia, das mudanças que foram causadas de forma maliciosa.

Segundo [Capkun et al. 2003a] existem duas maneiras de se adicionar segurança em uma rede *ad hoc*:

1. por meio de um domínio de autoridade, onde os certificados e/ou chaves são emitidos por uma autoridade única, geralmente na fazer de configuração ou inicialização do sistema, ou;
2. por meio de uma completa auto-organização do sistema, onde a segurança não confia ou depende de qualquer autoridade confiável ou um servidor fixo, nem mesmo na fase de inicialização.

Nesse artigo, é assumida a segunda abordagem e é apresentado um sistema de gerenciamento de chaves-públicas auto-organizável que permite aos usuários criarem, armazenarem, distribuirem e revogarem seus chaves públicas sem a ajuda de nenhuma autoridade confiável ou servidor fixo. Esse sistema foi proposto por [Capkun et al. 2003a], e é parte de um projeto de pesquisa intitulado *Terminodes*[1].

[Capkun et al. 2003a] propõe um esquema de gerenciamento de chaves usando os princípios do PGP (*Pretty Good Privacy*). O funcionamento e as características do PGP são discutidas em [Zimmermann 1995] e, dentre as principais características do PGP, uma importante é o gerenciamento de chaves: no PGP o acordo das chaves é realizado mediante a confiança entre os pares comunicantes. Como conseqüência dessa características, as redes que utilizam uma comunicação baseada em PGP, possuem um fenômeno chamado do *Small World* [Capkun et al. 2002].

Na seção 2 são apresentadas as características do gerenciamento de chaves em redes *ad hoc*. Também é discutido os problemas da utilização de uma autoridade certificadora central em uma rede *ad hoc*. Em seguida são apresentadas as operações básicas para o funcionamento do modelo de gerência de chaves proposto em [Capkun et al. 2003a]. Depois, é apresentado o esquema de criação e troca dos certificados de chaves públicas.

A seção 3 apresenta, de forma resumida, o funcionamento do algoritmo de construção dos repositórios de certificados. A implementação desse algoritmo é realizada utilizando o simulador NS-2 (*Network Simulador -2*) e são apresentados os resultados e as conseqüências de sua utilização, como utilização de recursos e vulnerabilidades do modelo.

2. O gerenciamento de chaves em redes *ad hoc*

Muitos objetivos da segurança podem ser obtidos utilizando mecanismos criptográficos. Por outro lado, os mecanismos criptográficos desenvolvidos para redes *ad hoc*, bem como para as redes tradicionais, confiam que o gerenciamento das chaves criptográficas está sendo realizado de forma apropriada.

[1]Projeto Terminodes - http://www.terminodes.org

Em redes *ad hoc* o gerenciamento de chaves é um grande desafio. Os mecanismos tradicionais de gerenciamento de chaves não são adequados para as redes *ad hoc*, uma vez que necessitam de uma entidade confiável central, conhecida da como Autoridade Certificadora (AC). O principal problema de qualquer sistema de segurança baseado em chaves-públicas é fazer com que a chave pública de cada usuário da rede seja disponibilizada para os demais usuários de forma que sua autenticidade seja verificada. Esse problema é ainda maior nas MANETs, uma vez que que não existe o papel de uma autoridade central na rede. Outra características das MANETs é que ele podem ser particionadas devido o dinamismo de sua topologia.

Uma abordagem amplamente utilizada para a solução dos problemas de gerenciamento de chaves-públicas é a utilização de certificados de chaves-públicas. Um certificado de chave-pública é uma estrutura de dados na qual a chave-pública é associada a uma identidade por meio da assinatura digital do emissor do certificado. Na maioria dos esquemas propostos para a utilização de certificados de chaves-pública, existe o papel de uma terceira entidade, conhecida como Autoridade Certificadora (AC).

De certa forma, como citado em [Zhou and Haas 1999], é uma questão problemática utilizar uma única AC em uma MANET, uma vez que a AC é responsável pela segurança da rede inteira, e assim é um ponto vulnerável da rede. Caso a AC fique indisponível, os nós da rede não podem obter as chaves públicas atuais dos outros nós, e como conseqüência, não podem estabelecer uma comunicação segura com os demais nós. Também se uma AC fica comprometida, um atacante pode assinar certificados falsos usando uma chave privada obtida da AC comprometida e, personificar qualquer outro nó, ou ainda, revogar um certificado válido.

A proposta de [Capkun et al. 2003a] é que os próprio nós emitam os certificados uns aos outros, não precisando assim de qualquer autoridade certificadora central.

2.1. Operações básica da solução

Nessa seção são apresentadas as operações básicas do modelo de gerenciamento de chaves proposto por [Capkun et al. 2003a]. Nesse modelo, as chaves públicas e os certificados do sistema são representados por um grafo direcionado $G(V, A)$, onde V representa o conjunto dos vértices e A o conjunto das arestas. Os vértices representam as chaves públicas e as arestas representam os certificados. Resumidamente, caso exista uma aresta direta conectando dois vértices (K_u à K_v), então existe um certificado assinado com a chave pública de u que associa K_v ao uma identidade.

Conforme explicado em [Capkun et al. 2003b], esse modelo de gerenciamento de chaves-públicas auto-organizável é similar ao PGP, no sentido que os usuário emitem certificados uns aos outros, baseados em seus relacionamentos pessoais.

Em [Buttyan and Hubaux 2003], os autores definem, que diferente do PGP, os certificados não são armazenados em um repositório central. Pelo contrário, os repositórios de chaves são distribuídos pelos nós da rede. Cada usuário mantém um repositório local de certificados. Quando um usuário u deseja verificar a autenticidade da chave-pública K_v de um usuário v, o usuário u tenta encontrar uma caminho direto do vértice K_u até K_v. Ele realiza essa operação realizando uma fusão dos repositório locais de certificados de K_u e K_v, conforme apresenta a figura 1.

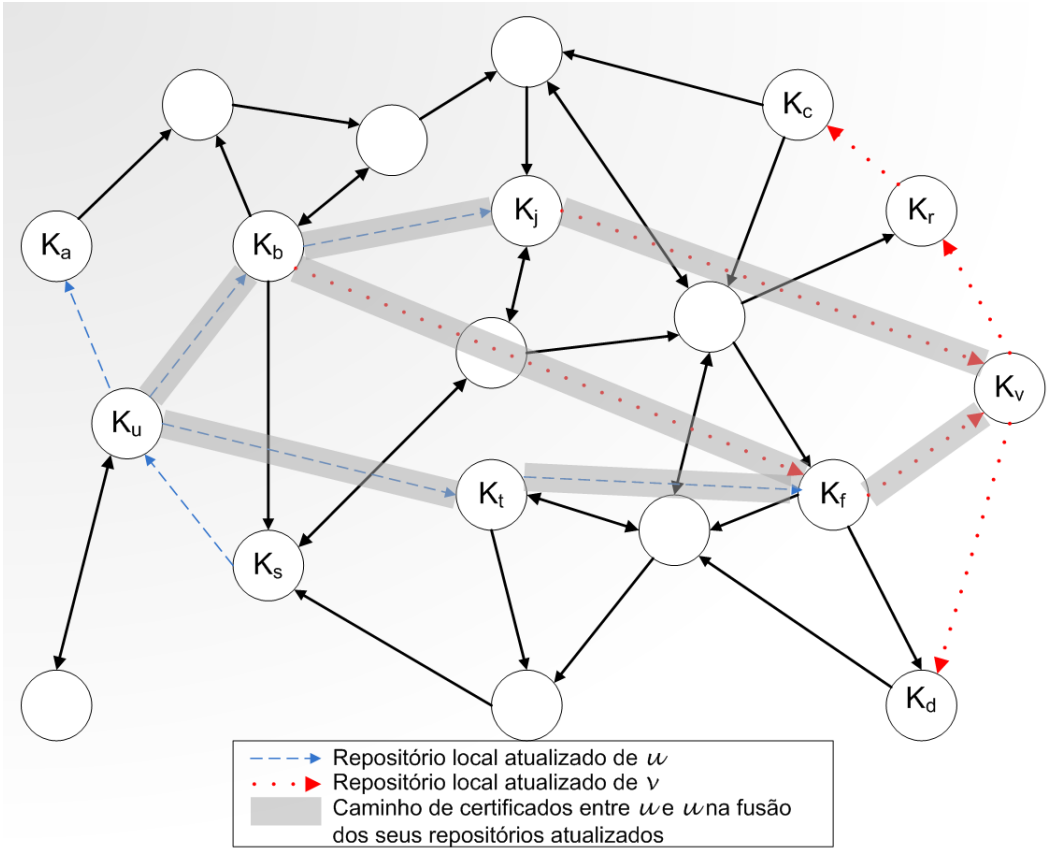

Figura 1. Grafo de certificados e os caminhos de certificados

A figura apresenta uma visão geral dos certificados válidos de toda a rede. As arestas azuis representam o subgrafo G_u e as arestas vermelhas o subgrafo G_v. Quando u tenta autenticar a chave pública K_v de v, ele faz a fusão dos repositórios de certificados atualizados de u e v e encontra um ou mais caminhos válidos para a autenticação. Isso é representado pelas arestas sombreadas do grafo.

Esses repositórios locais descritos anteriormente, são chamados repositórios atualizados, e para o nó u são denotados por G_u, ou grafo de certificados atualizado de u. Cada nó também mantém um repositório local de certificados não atualizados, que são denotados por G_u^N, ou grafo de certificados não atualizados de u.

Quando o nó u tenta verificar a autenticidade de uma chave pública K_v de um usuário v, e não encontra um caminho de certificados na fusão dos repositórios locais de certificados de u e de v, ele procura um caminho de certificados na fusão do seu repositório local de certificados atualizados com o seu repositório local de certificados não atualizados ($G_u \cup G_u^N$).

2.2. A criação e troca dos certificados de chaves públicas

No modelo proposto em [Capkun et al. 2003a] a chave pública de um usuário e sua chave privada correspondente é criada pelo próprio usuário. Similarmente ao PGP, os certificados de chaves públicas são emitidos pelos usuários. Assim, se o usuário u acredita que uma chave pública K_v pertence a um usuário v, ele então emite um certificado de chave-pública, associando K_v ao usuário v por meio da assinatura de u.

Os certificados são emitidos por um tempo limitado, chamado T_v. Quando os

certificados expiram e o seu emissor acredita que que a associação do usuário com a chave pública seja ainda válida, ele pode atualizar o mesmo certificado, agora com um novo tempo de expiração.

Em [Capkun et al. 2002] os autores mostram uma análise da utilização de grafos de certificados tipo o PGP. O artigo mostra, que devido ao relacionamento social existente entre os usuários da rede, a utilização de grafos de certificados baseados nas características do PGP, no sentido de que o próprios usuários emitem os certificados de chave-pública uns aos outros, possuem um fenômeno definido como "mundo pequeno"[2].

Cada nó realiza periodicamente uma troca de seus certificados com todos os seus nós vizinhos. Ele envia para os seus vizinhos o seu repositório local de certificados atualizados e não-atualizados. Assim, após uma fase inicial de convergência, chamada de T_{CE}, todos os certificados da rede serão armazenados por todos os nós da rede.

Nessa mensagem de troca, o nó u por exemplo, não envia todos os seus certificados atuais, mas somente uma lista de identificadores únicos. Os nós vizinhos de u que recebem a mensagem, respondem com os valores $hash$ dos certificados que estão em seus repositórios atualizados e não atualizados. O nó u então realiza uma checagem dos valores recebidos e envia para o vizinho somente os certificados que ele ainda não possui ou revalida os certificados que não estão atualizados, ou seja, estão expirados.

2.3. Revogação dos certificados

Os certificados podem ser revogados de forma explícita ou de forma implícita. Na revogação explícita, o nó emissor emite um testamento de revogação explícita para todos os nós que solicitaram dele o certificado de chave pública agora revogado. O nó emissor possui uma lista de todos os nós para os quais ele enviou um certificado por ele emitido, o que facilita a revogação dos certificados.

Na revogação implícita, a revogação é baseada no tempo de expiração dos certificados. Caso um certificado expire, e o nó emissor não envie uma revalidação do certificado, então o certificado é revogado implicitamente, e transferido do repositório local de certificados atualizados dos nós para o repositório local de certificados não atualizados dos mesmos nós.

3. O algoritmo proposto

Nessa seção é descrito o algoritmo de de construção Grau Máximo[3] para a construção dos repositórios atualizados. Uma descrição mais detalhada do algoritmo pode se encontrada em [Capkun et al. 2003a]

O algoritmo Grau Máximo seleciona um subgrafo de duas partes logicamente distintas: um subgrafo de entradas e um subgrafo de saída, ou seja, um subgrafo que possui os vértices que estão chegando a um nó e outro com os vértices que estão saindo de um nó. Quando inicia a partir do vértice K_u, o algoritmo gera o caminho dos vértices de saída $e_{out} = min(deg_{out}, c)$ e o caminho dos vértices de entrada $e_{in} = min(deg_{in}, c)$, onde:

- deg_{out} corresponde o número de arestas saída de K_u;

[2]Tradução do fenômeno Small World

[3]Traduzido de *Maximum Degree*

- deg_{in} corresponde o número de arestas entrando em K_u, e;
- c é uma constante que representa o número desejável de caminhos a ser construído.

Os tamanhos dos caminhos de entrada e saída, representados por l_{in} e l_{out} respectivamente, são calculados pela função $s/2e_{in}$ e $s/2e_{out}$ respectivamente, sendo que s é uma entrada do algoritmo que representa o número necessário de vértices do subgrafo resultante.

O algoritmo executa em duas rodadas. Na primeira, inicia do vértice K_u, ou seja, a chave-pública do usuário que está construindo o subgrafo, e inclui nesse subgrafo de saída e_{out} as arestas de saída que originaram de K_u, juntamente com seus respectivos vértices associados. Esse conjunto de vértices destino é chamado D_{out}. Na prática, os vértices de saída de um vértice K_u corresponde a todos os certificados emitidos por u. Nos passos seguintes, as aresta e_{out} e seus respectivos vértices de terminação são selecionadas e o processo se repete. Na prática, significa que o nó u pergunta aos nós pertencentes ao vértices em D_{out} pela lista de suas arestas de saída. A construção do subgrafo de entrada de u é similar.

4. Cronograma das atividades

O cronograma sugerido para a realização das pesquisas está descrito na tabela 1. Conforme o cronograma, as atividades iniciaram na semana do dia 06 de abril e se extendem até o dia 16 de junho de 2007, com a apresentação do artigo e dos resultados.

Atividades	**06.04**	**20.04**	**04.05**	**19.05**	**02.06**	**16.06**
Levantamento do tema	•					
Pesquisa do tema	•	•	•			
Desenvolvimento no NS		•	•	•	•	
Escrita da pesquisa		•			•	•
Conclusões						•
Apresentação						•

Tabela 1. Cronograma de atividades proposto

5. Considerações finais e trabalhos futuros

O modelo proposto é bastante interessante para as redes *ad hoc* móveis, uma vez que os próprios usuário podem emitir o seus certificados. É necessário ainda, realizar a implementação do modelo proposto em [Capkun et al. 2003a] e buscar obter os mesmos resultados nos testes para mostrar a viabilidade da implementação do modelo.

Como próximos passos para o artigo, é necessário realizar um estudo profundo do algoritmo *Maximun Degree* e da construção dos certificados de grafos PGP proposto em [Capkun et al. 2002] e por fim a implementação desses no NS-2.

Referências

[Buttyan and Hubaux 2003] Buttyan, L. and Hubaux, J.-P. (2003). Report on a working session on security in wireless ad hoc networks. *SIGMOBILE Mobile Computing and Communications Review*, 7(1):74–94.

[Capkun et al. 2002] Capkun, S., Buttyan, L., and Hubaux, J.-P. (2002). Small worlds in security systems: an analysis of the pgp certificate graph. In *NSPW '02: Proceedings of the 2002 workshop on New security paradigms*, pages 28–35, New York, NY, USA. ACM Press.

[Capkun et al. 2003a] Capkun, S., Buttyan, L., and Hubaux, J.-P. (2003a). Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 2(1):52–64.

[Capkun et al. 2003b] Capkun, S., Hubaux, J.-P., and Buttyan, L. (2003b). Mobility helps security in ad hoc networks. In *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*.

[Hu et al. 2005] Hu, Y.-C., Perrig, A., and Johnson, D. B. (2005). Ariadne: a secure on-demand routing protocol for ad hoc networks. *Wirel. Netw.*, 11(1-2):21–38.

[Zhou and Haas 1999] Zhou, L. and Haas, Z. J. (1999). Securing ad hoc networks. *IEEE Network*, 13(6):24–30.

[Zimmermann 1995] Zimmermann, P. R. (1995). *The official PGP user's guide*. MIT Press, Cambridge, MA, USA.