Estabelecimento de Chave de Grupo em Redes Ad Hoc *

Eric Ricardo Anton
eric@gta.ufrj.br

Otto Carlos Muniz Bandeira Duarte
otto@gta.ufrj.br

Grupo de Teleinformática e Automação
COPPE/EE – Programa de Engenharia Elétrica
Universidade Federal do Rio de Janeiro
http://www.gta.ufrj.br/

Resumo

Este trabalho analisa a segurança de comunicações de grupo em redes sem fio ad hoc. Neste novo ambiente, ao contrário do que ocorre em redes convencionais, não há qualquer infra-estrutura e os nós dependem uns dos outros para manter a rede conectada. São apresentados e analisados, considerando o ambiente ad hoc, protocolos para o estabelecimento de chaves de grupo. É apresentada uma proposta para o estabelecimento de uma chave de grupo que serve de base para a implantação de serviços de segurança entre os membros de uma rede ad hoc.
Palavras-chave: Redes de Computadores, Segurança, Gerenciamento de Chave, Redes Sem Fio Ad Hoc.

Abstract

This paper analyzes security issues on group communications in wireless ad hoc networks. This new environment, unlike traditional networks, has no infrastructure and the nodes depend on each other to keep the network connected. Protocols for group key establishment are presented and analyzed considering the ad hoc environment. A proposal for group key establishment among the members of an ad hoc network is presented and is the base for the deployment of security services.
Keywords: *Computer Networks, Security, Key Management, Wireless Ad Hoc Networks.*

1 Introdução

O crescimento de aplicações orientadas a comunicações de grupo, como áudio e vídeo conferência, televisão via *Internet*, transmissão de vídeo em camadas e aplicações cooperativas, exige mecanismos que garantam a integridade e a privacidade das informações transmitidas e a autenticação das entidades envolvidas. Comunicações de grupo seguras necessitam do compartilhamento de uma chave criptográfica secreta entre os membros deste grupo. Diversas propostas para se estender o protocolo Diffie-Hellman [1] de modo a permitir o estabelecimento de uma chave secreta entre várias entidades foram apresentadas. Uma das primeiras foi apresentada por Ingemarsson *et al.* [2], baseia-se na disposição dos membros na forma de um anel

*Este trabalho foi realizado com recursos da FUJB, CNPq, CAPES, COFECUB e FAPERJ.

lógico e necessita de um grande número de mensagens para ser executada. Becker e Willie [3] propõem o estabelecimento da chave de grupo por meio de uma disposição lógica em forma de hipercubo. Steiner *et al.* [4, 5, 6, 7, 8] propõem a coleta de informações fornecidas pelos membros do grupo seguida da distribuição destas informações a todos os membros ao final da execução do protocolo. Todas estas propostas se baseiam em redes convencionais.

Este artigo analisa a aplicação destas técnicas em redes sem fio não infra-estruturadas, também denominadas redes ad hoc. Os principais protocolos de estabelecimento de chave são descritos, as características do ambiente sem fio são apresentadas e alguns cenários são estudados.

O artigo está dividido da seguinte forma. Na Seção 2 são apresentados os principais conceitos relacionados ao estabelecimento de chaves de grupo e os protocolos já mencionados para estabelecimento de chaves de grupo. Na Seção 3 são expostas algumas características do ambiente ad hoc e abordada a questão do estabelecimento de chaves neste ambiente. Na Seção 4 é analisada por simulação a questão da alcançabilidade em redes ad hoc. A Seção 5 apresenta comentários finais sobre este trabalho.

2 Gerenciamento de chave

O estabelecimento da chave a ser utilizada pode ocorrer de forma centralizada (também denominada distributiva) ou distribuída (ou contributiva). Na forma centralizada, uma entidade é responsável pela geração da chave e sua distribuição aos demais membros. Esta abordagem apresenta a grande vantagem de ser simples. Na forma distribuída, todos os membros do grupo contribuem para a geração da chave. Pode haver uma abordagem híbrida, na qual apenas um subconjunto dos membros é responsável pela geração da chave, que é depois distribuída aos demais membros. Em [9] é proposta uma arquitetura na qual um serviço de gerenciamento de chave é distribuído entre vários nós, sendo necessário o consenso de um número mínimo desses nós.

Ao contrário do que ocorre em comunicações entre apenas duas entidades, para cenários de comunicações em grupo a manutenção da chave deve considerar o dinamismo do grupo devido à possibilidade de membros serem adicionados ou removidos após o estabelecimento da chave. Neste caso, o gerenciamento de chave pode atender a dois tipos de requisitos: sigilo passado (*backward secrecy*) e sigilo futuro (*forward secrecy*). Um protocolo possui sigilo passado se um novo membro do grupo não consegue acesso às chaves antigas do grupo, e possui sigilo futuro se membros que abandonam o grupo não conseguem acesso às futuras chaves de grupo. Estas características são essenciais para aplicações onde deseja-se que um membro excluído do grupo não receba mais as informações transmitidas pelo grupo, e que um novo membro do grupo passe a receber estas informações.

Neste artigo, são enfocados alguns protocolos para o estabelecimento distribuído de chaves de grupo que atendem aos requisitos de privacidade passada e futura. São apresentados a seguir alguns dos principais protocolos para estabelecimento de chave de grupo em redes convencionais. Todos são extensões do protocolo Diffie-Hellman para o caso de múltiplos participantes e proporcionam um acordo contributivo da chave de grupo. Tendo sido especificados respeitando os requisitos apresentados pelo protocolo Diffie-Hellman, estes protocolos herdam todas as suas características de segurança.

2.1 Protocolo de Ingemarsson *et al.*

Este protocolo, apresentado por Ingemarsson *et al.* [2], foi uma das primeiras tentativas de se estender o protocolo Diffie-Hellman para o caso de múltiplos participantes. Os participantes devem estar dispostos na forma de um anel lógico. Cada participante escolhe um expoente aleatório e ao receber um valor enviado pelo nó anterior, eleva este valor ao expoente escolhido, repassando esta informação ao próximo nó da seqüência. Após $n-1$ rodadas, todos os nós terminam por calcular a mesma chave de grupo. A principal desvantagem desta proposta consiste no grande número de mensagens necessárias ao estabelecimento da chave.

2.2 Protocolos Hipercubo e Octopus

O protocolo Hipercubo, apresentado por Becker e Wille [3] procura contornar o grande número de mensagens do protocolo anterior por meio da disposição lógica dos nós na forma de hipercubo. Para o caso de 4 nós dispostos em forma de quadrado é estabelecida uma chave ($g^{S_a S_b}$) entre A e B e outra ($g^{S_c S_d}$) entre C e D, que são utilizadas para estabelecer uma chave ($g^{(g^{S_a S_b})(g^{S_c S_d})}$) única entre as 4 entidades, conforme apresentado na Figura 1. Este comportamento pode ser generalizado para cenários com um maior número de nós, devendo o número de participantes ser igual a 2^d e sendo necessárias d rodadas para a execução do protocolo.

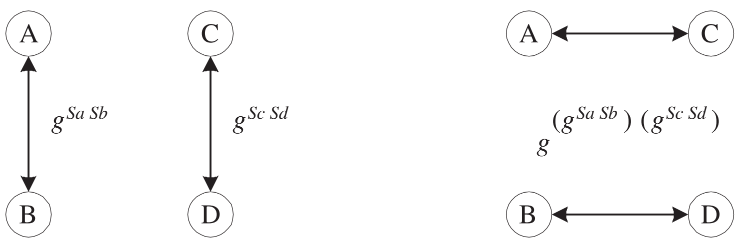

Figura 1: Protocolo Hipercubo para n = 4.

O protocolo Octopus é uma extensão do protocolo Hipercubo para um número qualquer de nós. Alguns nós formam um núcleo, dispostos na forma de um hipercubo, e os demais nós localizam-se próximos aos nós de núcleo. Cada nó do núcleo estabelece uma chave com cada nó de sua periferia por meio do protocolo Diffie-Hellman e utiliza o produtório destas chaves no estabelecimento de uma chave com os demais nós do núcleo, conforme especificado pelo protocolo Hipercubo. Esta chave é posteriormente distribuída aos nós periféricos.

2.3 A família de protocolos CLIQUES

Desenvolvida por Steiner *et al.* [4, 5, 6, 7, 8], a família de protocolos CLIQUES é composta por protocolos para o gerenciamento de uma chave de grupo entre integrantes de grupos dinâmicos.

O protocolo IKA.1[1] é composto por duas etapas. Na primeira etapa são coletadas as contribuições de todos os membros do grupo, o que ocorre ao longo de $n-1$ rodadas.

[1]Este protocolo foi anteriormente denominado GDH.2.

$$M_i \Rightarrow M_{i+1}: \quad \{g^{\frac{N_1 \cdot N_2 \cdot \ldots \cdot N_i}{N_k}} \mid k \in [1,i]\}, g^{N_1 \cdot N_2 \cdot \ldots \cdot N_i}$$

$$M_i \Leftarrow M_n: \quad \{g^{\frac{N_1 \cdot N_2 \cdot \ldots \cdot N_n}{N_i}} \mid i \in [1, n-1]\}$$

n	número de participantes (membros do grupo)
g	base da exponenciação
M_i	i-ésimo membro do grupo
N_i	expoente aleatório gerado por M_i
K_n	chave de grupo compartilhada pelos n membros

Cada membro do grupo (exceto o primeiro) recebe um conjunto de dados que representa as contribuições parciais de todos os membros que o antecedem na execução do protocolo. O membro adiciona sua contribuição e repassa um novo conjunto para o próximo membro do grupo.

O nó M_4, por exemplo, recebe o conjunto $\{g^{N_1 \cdot N_2 \cdot N_3}, g^{N_1 \cdot N_2}, g^{N_1 \cdot N_3}, g^{N_2 \cdot N_3}\}$, e envia ao próximo membro o conjunto $\{g^{N_1 \cdot N_2 \cdot N_3 \cdot N_4}, g^{N_1 \cdot N_2 \cdot N_3}, g^{N_1 \cdot N_2 \cdot N_4}, g^{N_1 \cdot N_3 \cdot N_4}, g^{N_2 \cdot N_3 \cdot N_4}\}$, que é composto por i valores intermediários, cada um contendo $n-1$ expoentes, e um valor cardinal contendo i expoentes que corresponde à potência da exponenciação elevada a todas as contribuições geradas até o momento.

O último membro do grupo (M_n) recebe um conjunto cujo valor cardinal é $g^{N_1 \cdot N_2 \cdot \ldots \cdot N_{n-1}}$. Com base neste valor é calculada a chave de grupo $K_n = g^{N_1 \cdot N_2 \cdot \ldots \cdot N_n}$. Sua contribuição é acrescentada a cada um dos valores intermediários.

Na segunda etapa, os valores intermediários são difundidos pelo último membro para todos os demais membros, por meio dos valores intermediários calculados. Com base nesses valores, cada membro calcula a chave K_n.

Esta família de protocolos, ao contrário dos protocolos anteriormente apresentados, provêem mecanismos específicos para adição e exclusão de membros do grupo, não sendo necessária a execução completa do procedimento de estabelecimento de chave. Esta característica facilita muito a oferta dos serviços de sigilo passado e futuro.

3 Estabelecimento de chave de grupo em redes ad hoc

As redes sem fio podem ser classificadas em redes com ou sem infra-estrutura. As redes infra-estruturadas são caracterizadas pela comunicação dos dispositivos móveis com um ou mais equipamentos centralizadores denominados pontos de acesso. Os dispositivos devem comunicar-se utilizando sempre um ponto de acesso. Um exemplo muito comum deste tipo de rede é a rede de telefonia celular, onde cada aparelho comunica-se com uma estação rádio-base, mas nunca diretamente com outro telefone.

Em redes sem infra-estrutura, também denominadas redes ad hoc, todos os dispositivos são capazes de estabelecer uma comunicação direta com outros dispositivos, não havendo o conceito de ponto de acesso. O uso deste tipo de rede é indicado em ambientes onde não há uma infra-estrutura de comunicação disponível, como em situações de resgate, tragédias naturais, expedições a regiões remotas ou aplicações militares.

As redes ad hoc são classificadas em redes de comunicação direta e em redes de múltiplos saltos. Nas redes de comunicação direta, cada dispositivo somente é capaz de comunicar-se com dispositivos que estejam ao seu alcance[2]. Em redes ad hoc de múltiplos saltos, dois dispositivos que são mutuamente inalcançáveis podem se comunicar se houver pelo menos uma cadeia de dispositivos que seja alcançável por ambos.

Devido às características deste novo ambiente, os aspectos de segurança válidos em redes convencionais não são totalmente aplicáveis a redes ad hoc, pois as características do ambiente restringem a viabilidade dos mecanismos de segurança normalmente utilizados, assim como os níveis de segurança e desempenho alcançados. O desempenho das operações realizadas é um fator muito importante neste ambiente devido às características geralmente encontradas nos dispositivos, como baixo poder de processamento e memória, restrito alcance de transmissão e limitada duração das baterias. Outras limitações incluem menos banda-passante e taxas de erro de transmissão mais elevadas.

Em redes sem fio infra-estruturadas a questão de alcançabilidade de um dispositivo se resume a estar posicionado dentro de uma célula da rede, em última análise, dentro do raio de atuação da estação rádio-base. Em redes ad hoc os próprios dispositivos atuam também como roteadores. Os dispositivos podem se comunicar desde que haja uma cadeia de dispositivos que permita o encaminhamento da informação da origem até o destino. Assim, a alcançabilidade não se limita a um raio de ação, mas à conjunção dos raios de ação de cada dispositivo. Desta forma, a localização momentânea de um dispositivo com relação aos demais influi na sua alcançabilidade.

O estudo das características das redes ad hoc permite perceber que a utilização de uma abordagem centralizada para o gerenciamento de uma chave de grupo não é conveniente devido a fatores como a dificuldade de se garantir que o nó que atua como servidor esteja permanentemente disponível. A indisponibilidade pode ser temporária, como por exemplo quando o nó se afasta dos demais, ou permanente, quando sua reserva de baterias se esgota ou o dispositivo é danificado. Um servidor centralizado pode ainda consistir em um ponto de gargalo na rede, prejudicando o desempenho do estabelecimento da chave.

3.1 Protocolos CLIQUES em ambiente ad hoc

Dos protocolos apresentados na Seção 2, os protocolos da família CLIQUES são os únicos a apresentar facilidades de adição e exclusão de membros do grupo. Por esta razão, estes protocolos foram escolhidos como os mais apropriados para implementação das aplicações visadas em ambientes ad hoc.

Esta família de protocolos necessita de uma ordenação entre os membros que define a seqüência percorrida pelas contribuições dos membros do grupo e o nó que será o último da seqüência. A forma como é estabelecida esta ordenação não é definida, ficando a critério da implementação utilizada. Esta ordenação pode ser fixa, seguindo uma seqüência predefinida, ou ser determinada durante a execução do protocolo para estabelecimento da chave. Para utilização em redes ad hoc, nas quais geralmente há uma constante mobilidade dos nós participantes, a utilização de uma seqüência predefinida pode ser ineficiente, uma vez que a ordem pode não corresponder ao melhor posicionamento geográfico dos dispositivos. Por exemplo, uma ordem fixa pode obrigar à comunicação de dois dispositivos através de uma grande cadeia de dispositivos, gerando trocas desnecessárias de mensagens, como ilustrado pela Figura 2, além de exigir o conhecimento *a priori* de todos os nós que participarão do grupo, o que em muitas situações é inviável. Esta abordagem pode apresentar problemas adicionais, como a possibilidade de blo-

[2]Alcance de comunicação de ambos os dispositivos, limitação imposta pelos transceptores de rádio ou infravermelho.

queio do protocolo caso um membro, quando for sua vez de receber ou enviar sua contribuição para a chave, esteja indisponível durante um longo período de tempo. Esta situação impede o protocolo de ser completado até que a conexão com o nó vizinho seja restabelecida.

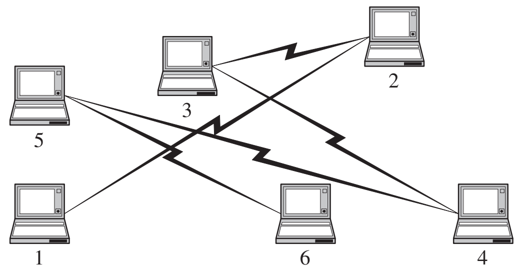

Figura 2: Troca desnecessária de mensagens no CLIQUES.

Este trabalho propõe um protocolo para o estabelecimento de uma ordenação entre os membros do grupo, no qual a descoberta de novos membros se dá durante a execução do protocolo de estabelecimento da chave. Cada nó quando necessita enviar sua colaboração para o próximo nó da seqüência executa uma busca por outros membros, dentro dos quais deve escolher um como o próximo. Baseando-se em conceitos utilizados por protocolos reativos de roteamento, esta descoberta se dá por meio do envio de uma mensagem por inundação[3]. Todos os nós que recebem esta mensagem e que ainda não colaboraram para a geração da nova chave enviam uma mensagem de resposta. Caso não sejam recebidas respostas, o nó pode tentar novamente ou assumir que não há mais nós na rede e finalizar o estabelecimento da chave. Caso sejam recebidas mais de uma resposta, um dos nós que respondeu é escolhido como o próximo da seqüência de contribuições para a chave.

A questão da alcançabilidade dos nós deve ser considerada, pois a inalcançabilidade de alguns nós durante a execução do protocolo de estabelecimento de chave pode levar ao estabelecimento da chave de grupo entre apenas alguns membros. Após alguns ou todos os nós que estavam inalcançáveis entrarem em contato com os nós que possuem a chave de grupo, pode ser executado um protocolo que altere a chave de grupo para incluir os novos membros, obedecendo ao critério de sigilo passado.

Um problema surge quando durante o estabelecimento da nova chave de grupo um ou mais nós que possuíam a chave até então utilizada tornam-se inalcançáveis, não tomando conhecimento da nova chave estabelecida. A readmissão destes nós no grupo pode exigir uma nova troca de chave, gerando um ciclo vicioso no qual a chave de grupo é constantemente alterada devido à indisponibilidade temporária de alguns membros, tornando inviável a comunicação segura e eficiente entre os participantes do grupo. A seção seguinte apresenta alguns resultados obtidos com a análise da influência de alguns parâmetros dos cenários utilizados sobre a alcançabilidade dos nós.

[3]Uma mensagem enviada por inundação é retransmitida apenas uma vez por todos os nós que a recebem.

4 Cenários

Um protótipo do protocolo IKA.1 atuando em conjunto com o protocolo proposto para descoberta de membros foi implementado no simulador de redes de computadores ns-2 (*Network Simulator* 2). Os cenários de topologia e movimentação dos nós foram criados utilizando o gerador de cenários `setdest`. Esta ferramenta, distribuída com o simulador, gera cenários aleatórios com base nos seguintes parâmetros: as dimensões da área (retangular) sobre a qual os nós se movimentam, o número de nós, a velocidade máxima e o tempo de pausa desses nós e o tempo total de simulação.

Foram analisadas as influências do número de nós presentes nos cenários e da variação do raio de alcance dos nós. Percebeu-se que, conforme esperado, o aumento do número de nós presentes no cenário aumentou a alcançabilidade geral dos nós. Isto ocorreu pelo fato de um maior número de nós aumentar a probabilidade de existência de uma cadeia de nós entre dois nós que não são vizinhos[4].

O aumento do raio de transmissão também colaborou para o aumento da alcançabilidade dos nós. Embora em situações práticas o aumento dos alcances dos transceptores seja uma tarefa inviável, devido a fatores como o restrito suprimento de energia, este resultado ressalta que o desempenho de uma rede ad hoc, no que se refere à alcançabilidade, tende a aumentar na medida em que aumenta a relação entre o raio de transmissão e a área de movimentação.

Para cenários com muitos nós ou com raios de alcance grandes todos os nós estiveram disponíveis a todos os demais a todo instante.

5 Comentários finais

Este artigo enfocou a segurança em comunicações de grupo. Alguns protocolos baseados no protocolo de Diffie-Hellman foram apresentados a analisados. A aplicação destes protocolos em ambientes ad hoc foi estudada. Devido às características das redes ad hoc, concluiu-se que abordagens centralizadas são vulneráveis ao problema da inalcançabilidade.

A família de protocolos CLIQUES se mostrou a mais adequada para o ambiente ad hoc por não exigir uma ordenação fixa como o protocolo de Ingemarsson *et al.*, nem a necessidades de dispositivos geograficamente privilegiados como os protocolos Hipercubo e Octopus.

Foi proposto um protocolo para a descoberta dos nós presentes na rede de modo a determinar a seqüência de nós a ser seguida para o estabelecimento da chave. Esta proposta foi simulada para vários cenários e concluiu-se que o problema da inalcançabilidade pode levar à constante troca da chave de grupo, o que consiste em um tema ainda aberto para a realização de trabalhos futuros.

Referências

[1] W. Diffie e M. Hellman, "New directions in cryptography", *IEEE Transactions on information Theory*, vol. IT-22, no. 6, pp. 644–654, novembro de 1976.

[2] I. Ingemarsson, D. T. Tang e C. K. Wong, "A conference key distribution system", *IEEE Transactions on Information Theory*, vol. IT-28, no. 5, pp. 714–720, setembro de 1982.

[4]Dois nós são considerados vizinhos quando estão sob alcance mútuo de transmissão.

[3] K. Becker e U. Wille, “Communication complexity of group key distribution”, in *5th ACM conference on Computer and Communication Security*, novembro de 1998.

[4] M. Steiner, G. Tsudik e M. Waidner, “Diffie-Hellman Key Distribution Extended to Group Communication”, *3rd ACM Conference on Computer and Communications Security*, março de 1996.

[5] M. Steiner, G. Tsudik e M. Waidner, “CLIQUES: A New Approach to Group Key Agreement”, *18th International Conference on Distributed Computing Systems*, maio de 1998.

[6] G. Ateniese, M. Steiner e G. Tsudik, “Authenticated Group Key Agreement and Friends”, in *Proceedings of the 5th ACM Conference on Computer and Communications Security*, novembro de 1998.

[7] G. Ateniese, M. Steiner e G. Tsudik, “New Multiparty Authentication Services and Key Agreement Protocols”, *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 4, abril de 2000.

[8] M. Steiner, G. Tsudik e M. Waidner, “Key Agreement in Dynamic Peer Groups”, *IEEE Transactions on Parallel and Distributed Systems*, vol. 11, no. 8, pp. 769–780, agosto de 2000.

[9] Z. J. Haas e L. Zhou, “Securing Ad Hoc Networks”, *IEEE Network Magazine*, vol. 13, no. 6, pp. 24–30, novembro/dezembro de 1999.