SEGURANÇA EM REDES SEM FIO AD HOC: GERENCIAMENTO DE CHAVE DE GRUPO

ERIC RICARDO ANTON*, OTTO CARLOS MUNIZ BANDEIRA DUARTE*

**Grupo de Teleinformática e Automação*
COPPE/EE – Programa de Engenharia Elétrica
Universidade Federal do Rio de Janeiro

Emails: eric@gta.ufrj.br, otto@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 alguns protocolos para o estabelecimento de chaves de grupo e analisada a viabilidade da suas utilizações em ambiente ad hoc. 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.

Abstract— This paper analises security issues of 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. Key establishment protocols are presented and analized. 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.

Key Words— Computer Networks, Network Security, Key Management, Wireless Ad Hoc Networks.

1 Introdução

As aplicações em redes sem fio têm alcançado um sucesso extraordinário nestes últimos anos. Este sucesso é devido à sua característica intrínseca de não possuir fios, que facilita a instalação, extensão e manutenção de uma rede e, principalmente, por permitir a mobilidade. Toda uma nova geração de dispositivos portáteis vêm sendo disponibilizados comercialmente tais como, telefones celulares, assistentes pessoais digitais (*Personal Digital Assistant* - PDA), fones auriculares etc. Por outro lado, a comunicação sem fio é normalmente realizada por radiofreqüências que é um meio altamente vulnerável, uma vez que permite a escuta da comunicação por qualquer dispositivo que esteja no raio de ação do transmissor. Assim, a comunicação sem fio é normalmente acompanhada de mecanismos de segurança de modo a garantir a integridade e a privacidade da comunicação, assim como a autenticação das entidades envolvidas.

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 comunicam-se usando sempre um ponto de acesso. Um exemplo 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 que estejam no seu alcance, não havendo, portanto, a figura centralizadora do ponto de acesso. As redes ad hoc aplicam-se a cenários de comunicação onde são disponibilizados um certo número de dispositivos confinados em um ambiente desprovido de qualquer infraestrutura de rede. Como exemplo de ambientes sem infraestrutura, podem ser citados ilhas, locais de difícil acesso (montanhas, florestas, desertos, geleiras etc.), eventos (shows artísticos, comícios etc.) ou locais em situações de emergência (inundações, terremotos, falta de energia, resgate de reféns em assaltos e seqüestros etc.). Uma rede ad hoc pode ser constituída e uma reunião eletrônica pode ser facilmente viabilizada. Neste caso, pode-se supor que todos os dispositivos são estáticos ou com pouca mobilidade, e são mutuamente alcançáveis. Assim, não há problema de acessibilidade e a comunicação entre os dispositivos é direta.

Outra possibilidade de redes ad hoc consiste na comunicação com múltiplos saltos, ou seja, dois dispositivos que são mutuamente inalcançáveis podem se comunicar se houver pelo menos uma cadeia de dispositivos que seja alcançável por ambos. Neste tipo de rede, ao contrário das redes convencionais, todos os dispositivos são capazes de realizar operações de roteamento. Um possível cenário onde pode ser útil este tipo de rede seria composta de diversos dispositivos, estáticos ou com pouca mobilidade, onde o alcance da comunicação entre dois dispositivos é ampliada usando outros dispositivos como simples repetidores. Entre as aplicações possíveis pode ser citada a configuração em rede dos diversos quiosques em uma estação balneária com distância máxima entre dois dispositivos maior que o raio de ação de um dispositivo sem fio.

Um cenário bem complexo seria a configuração em rede de dispositivos sem fio móveis confinados em uma área maior que o raio de alcance de um dispositivo. Isto implica em redes ad hoc de múltiplos sal-

tos onde não é garantida a acessibilidade de todos os dispositivos. Devido à mobilidade dos dispositivos, o conjunto de estações alcançáveis é dinâmico, pois varia no tempo. Isto implica os dispositivos serem capazes de rotear as mensagens e, também, que as tabelas de roteamento sejam constantemente atualizadas, uma vez que a alcançabilidade depende da localização momentânea de um dispositivo em relação aos demais. Uma aplicação deste cenário pode ser uma operação de guerra onde os soldados se locomovem e uma rede se instala e se reconfigura dinamicamente. Outra aplicação pode ser uma operação policial em um morro para prender traficantes.

Este artigo aborda o problema de se conseguir uma comunicação de grupo segura entre dispositivos sem fio de uma rede ad hoc. Em particular, será analisado o problema de se conseguir compartilhar uma chave secreta entre os membros de um grupo. De posse da chave secreta, os membros encriptariam e decriptariam as mensagens enviadas. Apenas o estabelecimento e o gerenciamento da chave secreta do grupo serão analisados; a comunicação multidestinatária, o roteamento e o controle de congestionamento e erros estão fora do escopo deste trabalho.

Para o estabelecimento de comunicações de grupo seguras é necessário o compartilhamento de uma chave criptográfica secreta entre os membros deste grupo. Esta chave comanda os procedimentos de segurança envolvidos, como encriptação e decriptação de mensagens.

Este artigo analisa a aplicação destas técnicas em redes sem fio não infra-estruturadas, ou ad hoc, e propõe um protocolo para descoberta dos membros de um grupo.

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 é abordada a questão do estabelecimento de chaves em redes ad hoc e proposto um protocolo para a descoberta dos membros de um grupo. A Seção 4 apresenta comentários finais sobre este trabalho.

2 Gerenciamento de chave de grupo

O gerenciamento de chave de grupo inclui as atividades de estabelecimento e manutenção da chave de grupo. As atividades de manutenção consistem nas trocas da chave utilizada, seja devido à adição ou exclusão de membros do grupo ou devido à utilização da chave por períodos longos de tempo. Uma boa política de gerenciamento de chave é fundamental para a prestação de serviços de segurança.

O estabelecimento da chave de grupo pode ocorrer de forma centralizada, também denominada distributiva, onde uma entidade é responsável pela geração da chave e sua distribuição aos demais membros. Esta abordagem apresenta a vantagem de ser simples. No estabelecimento de chave de grupo distribuído, ou contributivo, os membros do grupo contribuem para a geração da chave. Sua vantagem é ser tolerante a falhas e diminui os riscos de vícios na geração de chaves por uma única entidade. A técnica contributiva permite variações quanto à definição do grupo responsável pelo estabelecimento da chave que pode exigir a totalidade dos membros ou um sub-conjunto dos membros. O grupo parcial pode ser constituído de um número mínimo de membros (Haas e Zhou, 1999), ou obrigatoriamente um sub-conjunto prioritário de seus membros.

O grupo pode ser estático ou dinâmico. O grupo dinâmico permite a exclusão ou abandono de membros assim como a inclusão de novos membros. O gerenciamento de chave de um grupo dinâmico pode oferecer o serviço sigilo do futuro, quando os membros que abandonam o grupo não conseguem acesso às futuras chaves de grupo, e de sigilo do passado, onde um novo membro do grupo não consegue acesso às chaves antigas do grupo.

Neste artigo, são enfocados alguns protocolos para o estabelecimento distribuído de chaves de grupo que atendem aos requisitos de sigilo do passado e do futuro. São apresentados o algoritmo Diffie-Hellman, que é o principal algoritmo para o estabelecimento de chave secreta entre duas entidades, e alguns dos principais protocolos para estabelecimento de chave de grupo em redes convencionais. Estes protocolos são extensões naturais do algoritmo Diffie-Hellman para o caso de múltiplos participantes, conforme definido por Steiner et al. (1996), herdando portanto todas as suas características de segurança, e proporcionam um acordo contributivo da chave de grupo.

2.1 O Algoritmo Diffie-Hellman

Desenvolvido por Diffie e Hellman (1976), este algoritmo permite o estabelecimento de uma chave criptográfica secreta entre duas entidades por meio da troca de dados utilizando um canal inseguro de comunicação. A execução do algoritmo entre duas entidades A e B segue os seguintes passos:

- A e B concordam[1] na utilização de dois números p e g escolhidos aleatoriamente, tais que p é primo e grande e $g < p$;
- A escolhe um número aleatório secreto S_A e B escolhe um número aleatório secreto S_B;
- A calcula um valor público $T_A = g^{S_A} \bmod p$ e B calcula um valor público $T_B = g^{S_B} \bmod p$;
- A envia T_A para B e B envia T_B para A;

[1]Todas as informações trocadas entre as entidades fazem uso de um meio inseguro, sendo portanto de conhecimento público.

- A calcula ${T_B}^{S_A} \bmod p = (g^{S_B})^{S_A} \bmod p$ e B calcula ${T_A}^{S_B} \bmod p = (g^{S_A})^{S_B} \bmod p$.

Como $(g^{S_A})^{S_B} \bmod p = (g^{S_B})^{S_A} \bmod p = K$, estas duas entidades compartilham a chave criptográfica secreta K.

Em outras palavras, duas entidades trocam informações por um meio onde qualquer um pode escutar e no final do processo as duas entidades, e só estas duas entidades, conseguem compartilhar uma mesma chave secreta.

A segurança deste algoritmo se baseia na dificuldade de se calcular a chave secreta $K = g^{S_A S_B} \bmod p$, mesmo conhecidos os valores públicos $g^{S_A} \bmod p$ e $g^{S_B} \bmod p$, quando o número primo p é suficientemente grande.

2.2 *Protocolo de Ingemarsson et al.*

Este protocolo, apresentado por Ingemarsson et al. (1982), foi uma das primeiras tentativas de se estender o algoritmo Diffie-Hellman para o caso de múltiplos participantes. Os n membros do grupo devem estar dispostos na forma de um anel lógico. Ao início da execução do protocolo cada participante M_i, $i \in [1, n]$, gera um valor aleatório secreto S_i que é sua contribuição para a chave de grupo. A cada rodada do algoritmo cada participante eleva o valor recebido na rodada anterior ao seu valor secreto S_i e envia-o ao próximo nó da seqüência, ocorrendo portanto a transmissão de n mensagens entre os n membros do grupo. Após $n - 1$ rodadas, todos os nós terminam por calcular a mesma chave de grupo $K_n = g^{S_1 \cdot S_2 \cdot \ldots \cdot S_n}$. A principal desvantagem desta proposta consiste no elevado número de mensagens necessárias à sua execução, bem como no elevado número de operações de exponenciação (ver Tabela 1 e Figura 2).

2.3 *Protocolo de Burmester e Desmedt*

Este protocolo, apresentado por Burmester e Desmedt (1994), é executado em três rodadas, que consistem das seguintes operações, executadas por cada participante M_i, $i \in [1, n]$:

- geração de um valor aleatório secreto S_i e envio aos demais participantes do valor $z_i = g^{S_i}$ por difusão;
- cálculo e transmissão por difusão aos demais participantes do valor $X_i = (\frac{z_{i+1}}{z_{i-1}})^{S_i}$;
- computação da chave de grupo $K_n = z_{i-1}^{nS_i} \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \cdot \ldots \cdot X_{i-2} \bmod p$.

A chave de grupo obtida é da forma $K_n = g^{S_1 \cdot S_2 + S_2 \cdot S_3 + \ldots + S_n \cdot S_1}$. Esta chave compartilha as características de segurança apresentadas pelo protocolo Diffie-Hellman Este protocolo é eficiente quanto ao número total de rodadas, o que poderia proporcionar uma execução mais rápida. No entanto, estas rodadas requerem a execução de n transmissões simultâneas por difusão, o que geralmente não é possível, mesmo em redes sem fio, pois somente pode haver um nó difundindo mensagens a cada instante. Devido a esta característica, a implementação deste protocolo deve ocorrer por meio do envio seqüencial de mensagens de difusão, o que anula a vantagem de serem necessárias poucas rodadas, pois o envio de cada mensagem por difusão comporta-se como uma rodada. É necessário ainda um elevado número de operações de exponenciação.

2.4 *Protocolos Hipercubo e Octopus*

O protocolo Hipercubo, apresentado por Becker e Wille (1998) procura contornar o elevado número de mensagens do protocolo de Ingemarsson et al. 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. Um subconjunto dos nós é disposto na forma de um hipercubo, formando um núcleo. Os demais nós ficam à margem deste 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.

2.5 *A família de protocolos CLIQUES*

Desenvolvida por Steiner et al. (Steiner et al., 1996; Steiner et al., 1998; Ateniese et al., 1998; Ateniese et al., 2000; Steiner et al., 2000), a família de protocolos CLIQUES é composta por protocolos de gerenciamento de chave para grupos dinâmicos. Dois destes protocolos, IKA.1 e IKA.2 (*Initial Key Agreement* 1 e

2), são definidos para o estabelecimento da chave de grupo. Os demais protocolos executam a adição e a exclusão de membros e subgrupos e a troca da chave de grupo utilizada.

2.5.1 IKA.1

O protocolo IKA.1[2] é composto por duas etapas:

1. $M_i \Rightarrow M_{i+1}$:
   - $\{g^{\frac{S_1 \cdot S_2 \cdot \ldots \cdot S_i}{S_k}} \mid k \in [1,i]\}$, $g^{S_1 \cdot S_2 \cdot \ldots \cdot S_i}$
2. $M_n \Rightarrow M_i$:
   - $\{g^{\frac{S_1 \cdot S_2 \cdot \ldots \cdot S_n}{S_i}} \mid i \in [1,n-1]\}$,

para $i \in [1, n-1]$, onde n é o número de participantes (membros do grupo), g é a base da exponenciação, M_i é o i-ésimo membro do grupo, S_i é o expoente aleatório secreto gerado por M_i e K_n é a chave de grupo compartilhada pelos n membros.

Na primeira etapa são coletadas as contribuições de todos os membros do grupo, o que ocorre ao longo de $n-1$ rodadas. 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 de dados ao próximo membro do grupo.

O nó M_4, por exemplo, recebe o conjunto $\{g^{S_1 \cdot S_2 \cdot S_3}, g^{S_1 \cdot S_2}, g^{S_1 \cdot S_3}, g^{S_2 \cdot S_3}\}$, e envia a M_5 o conjunto $\{g^{S_1 \cdot S_2 \cdot S_3 \cdot S_4}, g^{S_1 \cdot S_2 \cdot S_3}, g^{S_1 \cdot S_2 \cdot S_4}, g^{S_1 \cdot S_3 \cdot S_4}, g^{S_2 \cdot S_3 \cdot S_4}\}$. O conjunto enviado pelo i-ésimo nó é composto por i valores intermediários, cada um contendo $i-1$ 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 (M_n) recebe um conjunto cujo valor cardinal é $g^{S_1 \cdot S_2 \cdot \ldots \cdot S_{n-1}}$ e com base neste valor calcula a chave de grupo $K_n = g^{S_1 \cdot S_2 \cdot \ldots \cdot S_n}$.

Na segunda etapa, sua contribuição é acrescentada a cada um dos valores intermediários, que são difundidos para todos os demais. Cada um dos valores intermediários possui a contribuição de todos exceto um dos membros. Cada membro M_i, para calcular a chave de grupo, localiza o valor intermediário que lhe corresponde (aquele que não possui sua contribuição) e eleva-o à sua contribuição S_i, obtendo K_n.

2.5.2 IKA.2

A execução do protocolo IKA.1 exige a realização pelo i-ésimo nó de $i+1$ operações de exponenciação. Em alguns ambientes é desejável a minimização do esforço computacional exigido de cada membro para o estabelecimento da chave, como por exemplo em grupos com elevado número de participantes ou formados por equipamentos com limitado poder de processamento. Visando minimizar este esforço, foi proposto o protocolo IKA.2[3], que é conceitualmente similar, mas composto por quatro etapas:

1. $M_i \Rightarrow M_{i+1}$, $i \in [1, n-2]$:
   - $g^{S_1 \cdot S_2 \cdot \ldots \cdot S_i}$
2. $M_{n-1} \Rightarrow M_i$, $i \in [1, n-2]$:
   - $g^{S_1 \cdot S_2 \cdot \ldots \cdot S_{n-1}}$
3. $M_i \Rightarrow M_n$, $i \in [1, n-1]$:
   - $g^{\frac{S_1 \cdot S_2 \cdot \ldots \cdot S_{n-1}}{S_i}}$
4. $M_n \Rightarrow M_i$, $i \in [1, n-1]$:
   - $\{g^{\frac{S_1 \cdot S_2 \cdot \ldots \cdot S_n}{S_i}} \mid i \in [1,n-1]\}$.

Na primeira etapa são coletadas as contribuições dos $n-2$ primeiros membros do grupo por meio do envio de uma única mensagem, que acumula todas as colaborações anteriores, de um membro para o próximo. Na segunda etapa M_{n-1} difunde a mensagem recebida, acrescida de sua colaboração, para todos os $n-2$ primeiros membros. Cada membro retira, na terceira etapa, da mensagem recebida sua contribuição e envia este resultado para o último membro do grupo. Na última etapa, M_n reúne os valores recebidos, eleva cada um deles ao seu expoente S_n e difunde estes resultados a todos os demais membros do grupo, permitindo que eles calculem a chave de grupo.

Estes dois protocolos apresentam a vantagem de requerer um baixo número de mensagens (ver Tabela 1 e Figura 2). O protocolo IKA.2 alcançou o objetivo de reduzir o número de operações de exponenciações necessárias, sendo o que necessita de um menor número destas operações. Esta família de protocolos, ao contrário dos protocolos anteriormente apresentados, provê ainda mecanismos específicos para adição e exclusão de membros do grupo, não sendo necessária a execução completa do procedimento de estabelecimento de chave. Esta característica reduz os custos envolvidos e facilita a oferta dos serviços de sigilo do passado e do futuro.

2.6 Comparação entre os protocolos

A Tabela 1 apresenta uma comparação entre os protocolos para estabelecimento de chave de grupo apresentados[4]. São expostos, para cada protocolo, o número total de mensagens trocadas, o número total de operações de exponenciação efetuadas e se há necessidade de sincronismo entre os participantes no momento de

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

[3]Este protocolo foi anteriormente denominado GDH.3.

[4]O protocolo Octopus foi excluído desta análise pois os números de mensagens e exponenciações dependem do número nós que compõem o núcleo.

envio de uma mensagem a outro participante. A Figura 2 expõe os dados da Tabela 1 de uma forma gráfica.

	Mens.	Exp.	Sinc.
Ing.	$n(n-1)$	n^2	Sim
B-D	$2n$	$n(n-1)$	Sim
Hipercubo	$n \cdot \log_2 n$	$2n \cdot \log_2 n$	Sim
IKA.1	n	$\frac{n(n+3)}{2} - 1$	Não
IKA.2	$2n-1$	$5n-6$	Não

Tabela 1: Comparação entre os protocolos apresentados para estabelecimento de chave de grupo.

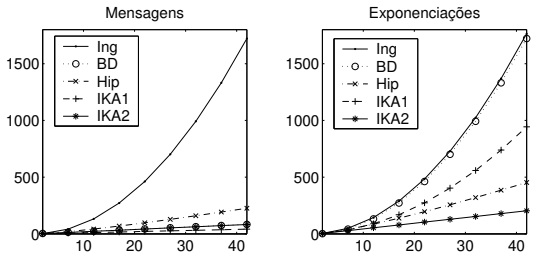

Figura 2: Número de mensagens e de operações de exponenciação um função do número de nós para cada protocolo.

O protocolo IKA.1 apresenta melhor desempenho com relação ao número de mensagens, seguido pelos protocolos IKA.2 e de Burmester e Desmedt. Com relação ao número de operações de exponenciação, o melhor desempenho é apresentado pelo protocolo IKA.2, seguido pelos protocolos Hipercubo e IKA.1. A análise destas duas métricas em conjunto aponta como mais interessantes os protocolos IKA.1, IKA.2 e Hipercubo. O protocolo de Ingemarsson et al. pelas duas métricas é muito custoso. O protocolo de Burmester e Desmedt é muito custoso com relação ao número de exponenciações. Com relação ao número de mensagens, seu desempenho é bom, mas equivalente ao do protocolo IKA.2.

3 Estabelecimento de chave de grupo em redes ad hoc

O estudo das características das redes ad hoc permite perceber que uma abordagem centralizada para o gerenciamento da 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 e não há como repô-la. Um servidor centralizado pode ainda consistir em um ponto de gargalo na rede, prejudicando o desempenho do estabelecimento da chave.

Dos protocolos apresentados na Seção 2, os protocolos da família CLIQUES, além de estarem entre os que apresentam melhor desempenho, não necessitam de sincronismo entre os membros do grupo, como o protocolo Hipercubo, e são os únicos a apresentarem facilidades de adição e exclusão de membros do grupo. Estas razões levam à escolha dos protocolos da família CLIQUES como os mais apropriados para o gerenciamento de chave secreta em ambientes ad hoc. Esta família de protocolos necessita de uma ordenação entre os membros que define, em particular, a seqüência percorrida pelas contribuições dos membros do grupo e o nó que será o último da seqüência. A forma como esta ordenação deve ser estabelecida não é definida, ficando a critério da implementação utilizada. Esta ordenação pode ser fixa, utilizando uma seqüência predefinida, ou ser determinada durante a execução do protocolo para estabelecimento da chave.

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 levar à comunicação de dois dispositivos através de uma extensa cadeia de dispositivos, gerando encaminhamentos ineficientes de mensagens, como ilustrado pela Figura 3. O estabelecimento da chave de grupo seria mais eficiente se fosse utilizada, por exemplo, a seqüência de nós 1-5-3-2-4-6. Esta abordagem exige ainda o conhecimento *a priori* de todos os nós que participarão do grupo, o que em muitas situações é inviável. Há ainda a possibilidade de bloqueio 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 acessibilidade com o nó vizinho seja restabelecida.

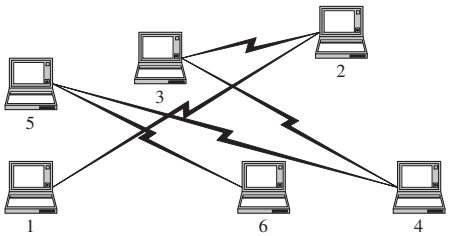

Figura 3: Troca desnecessária de mensagens no CLIQUES.

3.1 *Um protocolo para a descoberta de membros do grupo*

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[5]. 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, assumindo o papel de M_n. 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 do 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.

4 Comentários finais

Este artigo enfocou a segurança em comunicações de grupo. Alguns protocolos baseados no algoritmo Diffie-Hellman foram apresentados e analisada a aplicação destes protocolos em ambientes ad hoc.

A família de protocolos CLIQUES se mostrou a mais adequada para o ambiente ad hoc por possuir melhor desempenho quanto ao número de mensagens enviadas e ao número de operações de exponenciação necessárias, por não necessitar de sincronismo entre os membros do grupo, e por permitir a determinação da ordem dos membros do grupo durante a execução do protocolo para estabelecimento da chave.

Foi proposto um protocolo para o descobrimento dos nós presentes na rede de modo a determinar a seqüência de nós a ser seguida para o estabelecimento da chave. Mostrou-se como 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.

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

Referências

Ateniese, G., Steiner, M. e Tsudik, G. (1998). Authenticated group key agreement and friends, *Proceedings of the 5th ACM Conference on Computer and Communications Security*.

Ateniese, G., Steiner, M. e Tsudik, G. (2000). New multiparty authentication services and key agreement protocols, *IEEE Journal on Selected Areas in Communications* **18**(4).

Becker, K. e Wille, U. (1998). Communication complexity of group key distribution, *5th ACM conference on Computer and Communication Security*.

Burmester, M. e Desmedt, Y. (1994). A secure and efficient conference key distribution system, *Advances in Cryptology – EUROCRYPT '94*, pp. 275–286.

Diffie, W. e Hellman, M. (1976). New directions in cryptography, *IEEE Transactions on information Theory* **IT-22**(6): 644–654.

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

Ingemarsson, I., Tang, D. T. e Wong, C. K. (1982). A conference key distribution system, *IEEE Transactions on Information Theory* **IT-28**(5): 714–720.

Steiner, M., Tsudik, G. e Waidner, M. (1996). Diffie-Hellman key distribution extended to group communication, *3rd ACM Conference on Computer and Communications Security* .

Steiner, M., Tsudik, G. e Waidner, M. (1998). CLIQUES: A new approach to group key agreement, *18th International Conference on Distributed Computing Systems* .

Steiner, M., Tsudik, G. e Waidner, M. (2000). Key agreement in dynamic peer groups, *IEEE Transactions on Parallel and Distributed Systems* **11**(8): 769–780.