UTILIZAÇÃO DE CHAVE DE GRUPO PARA PROTEÇÃO DE REDES *AD-HOC*[*]

Fernando C. A. Verissimo, Luciano R. de Albuquerque e Luís Felipe M. de Moraes
Laboratório de Redes de Alta Velocidade – RAVEL
COPPE/Programa de Engenharia de Sistemas e Computação
Universidade Federal do Rio de Janeiro – UFRJ
Caixa Postal: 68.511 – 21941-972 – Rio de Janeiro, RJ – Brasil
{verissimo,aluciano,moraes}@ravel.ufrj.br

Resumo

Este artigo apresenta uma abordagem sobre os problemas encontrados pela vulnerabilidade da comunicação entre terminal de dados sem fio móveis, utilizando uma rede ad hoc. Além disso, antecipa os problemas de substituição de chaves entre os terminais de dados numa rede ad hoc baseada do padrão IEEE 802.11. Um algoritmo de distribuição de chaves em grupo é discutido. Finalmente, é concluído que a rede ad hoc pode não ser mais vulnerável que uma rede também sem fio infra-estruturada.

1-Introdução

A grande proliferação das tecnologias de comunicação em meios não confinados (sem fios) deverá resultar num uso cada vez maior de dispositivos sem fio (*wireless*), para as mais diversas aplicações e serviços. Uma previsão feita neste cenário em abril de 2002, [DE-VR02], indica que na metade daquele ano seria ultrapassada a barreira de 1 bilhão de celulares no mundo.

Neste cenário, as redes sem fio para comunicações móveis entre terminais de dados deverão ser responsáveis pelo suporte a uma grande parcela das aplicações utilizadas. Por exemplo, redes locais sem fio já se constituem numa excelente alternativa para integração de dispositivos diversos numa área restrita (*WLAN*s). Além disso, alguns dos padrões utilizados para interligar entre si equipamentos sem fio, com utilização de pontos de acesso para redes cabeadas (redes estruturadas), estão também sendo propostos para utilização em redes *ad hoc*.

No cenário de redes, de uma forma geral, um dos principais requisitos é a segurança dos diversos sistemas e dispositivos envolvidos. Assim, faz-se necessária a garantia de que as informações que circulam estejam protegidas, contra leituras/alterações indevidas, duplicações ou eliminações feitas por pessoas não autorizadas.

No cenário das redes sem fio, apesar dos aspectos mencionados serem análogos àqueles das redes cabeadas, as ameaças e os riscos trazidos pelo uso do meio físico não confinado, inerente à tecnologia utilizada, são motivos de maiores preocupações. Quando falamos de rede sem fio *ad hoc* as preocupações aumentam, pois a disponibilidade de servidores de autenticação e repositórios de chaves públicas não é uma alternativa eficiente. Este trabalho está inserido exatamente nesse contexto.

2-Redes *Ad Hoc*

A principal característica de uma rede *ad hoc* [YI01, ZHAN00] é o fato de não possuir infra-estrutura. Os nós que compõem uma rede sem fio desse tipo são capazes de se comunicar uns com os outros funcionando eles mesmos como roteadores.

Sua topologia é dinâmica, sofrendo diversas mudanças devidas a mobilidade de seus nós durante a existência da rede. O fato de ser formada por nós móveis é uma indicação de que

[*]Este trabalho teve o suporte da FAPERJ (Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro).

normalmente esses equipamentos têm serias restrições quanto ao consumo de energia para se manterem funcionando. Sendo assim, o consumo devido ao processamento necessário para que rotas entre nós sejam descobertas e mantidas deve ser cuidadosamente controlado. Nesse aspecto os protocolos de roteamento tornam-se pontos críticos para um bom funcionamento da rede.

Os nós que podem ser contatados por um determinado nó, sem a necessidade de outros intermediários para realizar o roteamento dos pacotes transmitidos, são conhecidos como nós vizinhos ao nó transmissor. Por exemplo: se um determinado nó, digamos o nó *A*, for capaz de se comunicar com os nós *C*, *D* e *F* sem a necessidade de intermediários, dizemos que esses três nós são vizinhos de *A*.

2.1-Protocolos de Roteamento

Os protocolos de roteamento são responsáveis por encontrar, estabelecer e manter rotas entre dois nós que desejam se comunicar. É importante que esses protocolos gerem o mínimo de overhead possível e que a quantidade de banda consumida por eles também seja pequena.

Basicamente, os protocolos de roteamento podem ser classificados como pró-ativos e reativos [ROYE99]. Esse trabalho os descreve sucintamente, dando um exemplo de cada tipo.

2.1.1-Protocolos Pró-ativos

Basicamente, são protocolos que procuram manter tabelas de roteamento sempre com as rotas para todos os destinos possíveis. As rotas são mantidas mesmo que não sejam usadas em nenhum momento.

2.1.1.1-Destination-Sequenced Distance-Vector (*DSDV*)

Mantém rotas para todos os possíveis destinos da rede em sua tabela de roteamento. Mensagens periódicas são enviadas por *Broadcast*, onde cada nó informa as mudanças que ocorreram em sua tabela de rotas [PERK94].

Existem dois diferentes tipos de mensagens para atualização das rotas:

- Mensagens curtas contendo apenas as últimas rotas que sofreram alguma modificação. Esse tipo de mensagem deve caber em um único NPDU (Network Protocol Data Unit), diminuindo assim a quantidade de tráfego gerado por um broadcast.
- Mensagens completas, contendo toda informação da tabela de roteamento. Mensagens desse tipo geram uma grande quantidade de tráfego. Para evitar uma sobrecarga da rede essas mensagens devem ser enviadas com uma freqüência relativamente baixa.

Quando um nó recebe informações sobre rotas que ele já possui, ele é capaz de diferenciar as novas informações das antigas através do campo *sequence number*. A rota que possui o maior valor para o *sequence number* terá preferência. Aquela que possui o menor número será descartada ou mantida como uma rota alternativa de menor importância. Se os valores do campo *sequence number* forem iguais, é dada preferência para a rota com a menor quantidade de saltos para alcançar o destino.

2.1.2-Protocolos Reativos

As tabelas de roteamento desses protocolos possuem apenas rotas que foram solicitadas. Após um determinado tempo sem serem utilizadas, são excluídas.

2.1.2.1-*Ad Hoc* On demand Distance Vector (AODV)

Nesse protocolo quando um nó precisa entrar em contato com um outro nó para o qual ele não possui uma rota em sua tabela, é iniciado o processo de descoberta de rota. Esse processo consiste no broadcast de um *Route Request*, *RREQ*, para todos os nós vizinhos desse que deseja descobrir a nova rota. Seus vizinhos por sua vez propagam essa requisição. O processo se repete até que o nó destino seja alcançado ou que um nó intermediário conhecendo a rota até o destino seja encontrado. Durante esse processo de descoberta da rota, os nós que recebem a RREQ incluem entradas temporárias em suas tabelas, registrando a origem da mensagem RREQ.

Quando o destino ou um nó intermediário que possua uma rota para o mesmo é encontrado, um *Route Reply*, RREP, é enviado de volta para a origem da requisição. Enquanto a mensagem RREP é propagada cada nó que a recebe incrementa o campo correspondente à quantidade de saltos necessários para se alcançar o destino.

O *AODV* mantém suas rotas através de mensagens periódicas enviadas por um nó para aqueles vizinhos os quais possuam rotas que passam através dele. Assim, seus vizinhos são capazes de saber se a rota ainda existe ou não. Caso a mensagem HELLO não seja recebida durante um determinado período de tempo, assume-se que ocorreu uma quebra em algum link pertencente à rota, tornando-a inválida. Se a rota ainda estava sendo usada o nó pode realizar uma nova requisição, RREQ, em busca de uma nova rota.

3-Falhas de segurança

A natureza de uma rede *ad hoc* faz dela insegura. O grau de comprometimento entre seus membros é alto, já que todos dependem uns dos outros para o pleno funcionamento da rede. Sendo assim, a conclusão disso é que a forma como uma rede desse tipo deve ser protegida não pode ser a mesma adotada em redes cabeadas. Cada um de seus membros deve estar preparado para enfrentar um adversário, garantindo indiretamente maior grau de segurança para toda a rede. O nível de segurança depende de todos os nós.

No nível da camada de rede, por exemplo, um nó inimigo ou comprometido pode participar do processo de descoberta de rotas e aproveitar-se disso. Os pacotes de *route request* (*RREQ*) e *route reply* (*RREP*) podem ser alterados enquanto trafegam, ou podem ser forjados causando diversas anomalias no funcionamento da rede [DAHI01,ZHAN00].

Atacantes que consigam alterar o campo *destination sequence numbers*, a quantidade de saltos registrada no cabeçalho do pacote de roteamento ou criar mensagens falsas de erro e atualizações de rotas, serão capazes de realizar ataques de negação de serviços e criar rotas falsas.

Obviamente, levando ao mau funcionamento da rede ou até mesmo fazendo com que ela pare de funcionar.

4-WiFi Protected Access, version 1

O interesse do grupo de pesquisa no qual trabalhamos é estudar segurança de redes para o padrão IEEE 802.11. Por esta razão estamos interessados em estudar os protocolos desenvolvidos no âmbito do IEEE 802.11i. O IEEE 802.11i é um grupo de trabalho destinado a projetar os mecanismos de segurança para o padrão conhecido como *WLAN*. Esse grupo de trabalho vem dando passos importantes na direção de melhorar a sensação de segurança nesse padrão.

No ano passado, foi publicado por Housley, Whiting e Ferguson, [HOUS02], um algoritmo de sumarização (*hash*) que vai ser adicionado aos algoritmos de criptografia do novo protocolo de segurança do padrão *WLAN*, o *WPA v1* (*WiFi Protected Access, version 1*). O

ATKH (*Alternate Temporal Key Hash*) partiu de uma sugestão de Ron Rivest, que ao responder as acusações atribuídas ao RC4, aconselhou, entre outras sugestões, a adoção de um algoritmo de sumarização da chave antes de atribuí-la ao algoritmo de embaralhamento.

No WPA v1, o dispositivo móvel começa com uma chave-base secreta de 128 bits, chamada de *TK* (*Temporal Key*), então ela é combinada com o *TA* (*Transmitter Address*), o endereço *MAC* do transmissor, criando a chave chamada de *TTAK* (*Temporal and Transmitter Address Key*), ou a "Chave da Fase 1". A *TTAK* é então combinada com o IV (Vetor de Inicialização) para criar as chaves que variam a cada pacote, chamadas de *RC4KEY*. Cada chave é utilizada pelo RC4 para criptografar somente um pacote.

O *WPA v1* faz com que cada estação da mesma rede utilize uma chave diferente para se comunicar com o ponto de acesso. O problema da colisão de chaves do *RC4* é resolvido com a substituição da *TK* antes que o *IV* assuma novamente um valor que já assumiu, ou seja, a cada vez que o *IV* assuma o seu valor inicial, o *TK* deve assumir um valor distinto. A forma como é gerenciada essa troca de *TK*s não foi padronizada e será sugerida nesse trabalho.

5-Estabelecimento de chave de grupo em rede *ad hoc*

Esse trabalho não aborda o problema da autenticação de um novo nó móvel à rede, remetendo o leitor à pesquisa na literatura existente [ATEN00]. O que será sugerido é um possível mecanismo de troca de chaves, neste caso específico do padrão *WLAN*, as *TK*s.

O *WPA v1* atua na camada de enlace, ou seja, sob a camada de rede, onde o roteamento é tratado e as falhas descritas na seção 3 são apresentadas. Uma vez que o intruso não é capaz de decodificar o fluxo de pacotes, ele é incapaz de atacar a rede.

Nós estamos apresentando o IKA.1 como um possível algoritmo para a troca das *TK*s entre os membros já autenticados de uma rede *ad hoc*, uma vez que dissemos na seção anterior, esta chave temporária necessita ser substituída de tempos em tempos.

5.1-Initial Key Agreement 1

O protocolo IKA.1 foi desenvolvido por Steiner *et al* [STEI98]. Esse protocolo é composto de duas fases. Primeiramente, todos os nós móveis, exceto o último, envia um conjunto de números para o próximo nós. Cada elemento do conjunto é o resultado da exponenciação de uma base pré-combinada por todos os nós a números sorteados pelos nós móveis. O conjunto é formado pela base elevada a todos os números sorteados por todos os nós móveis, incluindo aquele que está enviando, e todas as combinações possíveis da base elevada a *i-1* números, dentre os *i* números sorteados até esse *i*-ézimo nó que está enviando. Veja abaixo:

$$N_i \Rightarrow N_{i+1} : \left\{ b^{S_1.S_2....S_i}, \left[b^{\frac{S_1.S_2....S_i}{S_j}} \middle| j \in (1,i) \right] \right\};$$

$N_i \rightarrow i$-ézimo nó; $b \rightarrow$ base; $S_i \rightarrow$ número sorteado pelo i-ézimo nó

Ex: O nó 4, recebe o seguinte conjunto $\left\{ b^{S_1.S_2.S_3}, b^{S_2.S_3}, b^{S_1.S_3}, b^{S_1.S_2} \right\}$, e envia ao próximo nós o seguinte conjunto $\left\{ b^{S_1.S_2.S_3.S_4}, b^{S_2.S_3.S_4}, b^{S_1.S_3.S_4}, b^{S_1.S_2.S_4}, b^{S_1.S_2.S_3} \right\}$.

Na segunda fase, após o último nó receber o conjunto de números do seu antecessor, conjunto esse que possui *n* elementos, ele eleva cada elemento do conjunto ao seu número sorteado, mantém consigo o primeiro elemento do conjunto, que é a chave, e envia cada elemento restante no conjunto para cada um dos *n-1* outros nós. Cada nó vai receber do *n*-ézimo nó um elemento do conjunto e o vai elevar ao seu próprio número sorteado, obtendo assim, também, a chave, já conseguida pelo *n*-ézimo nó. Veja abaixo:

$$N_n \Rightarrow N_i : \left\{ b^{\frac{S_1 . S_2 \ldots . S_i}{S_i}} \middle| i \in (1, n-1) \right\}$$

6-Conclusão e Trabalhos Futuros

Os problemas de segurança são agravados quando ambientados em redes *ad hoc.* A vulnerabilidade do meio não confinado, a descentralização dos serviços de roteamento e autenticação e, geralmente, a baixa capacidade computacional dos terminais móveis componentes das redes, torna o desafio de manter segura uma rede *ad hoc.*

Entretanto, este trabalho conclui que se o problema da segurança no padrão *WLAN* puder ser resolvido na camada de enlace, o fato da rede ser infra-estruturada ou *ad hoc* será indiferente. Os problemas de segurança no padrão *WLAN* ainda é alvo de muita pesquisa, mas os avanços já vem sendo feitos. Ainda nesse ano o *WPA v.1* já deverá ser embutido nos novos dispositivos móveis.

Logicamente, esse trabalho não abordou os estudos na área de autenticação de um novo nó, que é importantíssimo para assegurarmos a viabilidade de todo o processo, mas isso já vem sendo largamente estudado, e também será alvo dos nossos próximos estudos.

7-Referências

[ANTO02] E. R. Anton e O. C. M. B. Duarte, "Estabelecimento de chave de grupo em redes *ad hoc*", *II Workshop Brasileiro em Segurança de Sistemas Computacionais*, XX Simpósio Brasileiro de Redes de Computadores, Búzios, Brazil, maio, 2002.

[ATEN00] G. Ateniese, M. Steiner e G. Tsudik, "New multiparty authentication services and key agreement protocols", *IEEE Journal on Selected Areas in Communications,* 18(4), 2000.

[DAHI01] B. Dahill, B. N. Levine, E. Royer e C. Shields. "A Secure Routing Protocols for *Ad Hoc* Mobile Wireless Networks", *Tech. Rep. 01-37, Department of Computer Science, University of Massachusetts*, agosto, 2001.

[DEVR02] J. de Vriendt, P. Lainé, C. Lerouge, e X. Xiaofeng, "Mobile network evolution: A revolution on the move. Broadband access series", *IEEE Communications Magazine*, abril 2002.

[HOUS02] R. Housley, D. Whiting e N. Ferguson, "Alternate Temporal Key Hash", *IEEE 802.11, TGi*, IEEE 802.11-02/282r2, 2002.

[JOHA99] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek e D. Degermark, "Scenario-based Performance Analysis of Routing Protocols for Mobile *Ad Hoc* Networks", *MobiCom'99*. 1999.

[PERK94] C. E. Perkins e P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", *ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, pp. 234-244, 1994.

[RIVE01] R. Rivest, "RSA security response to weakness in Key Scheduling Algorithm of RC4", *http://www.rsasecurity.com/*. Acesso em: 13 dezembro 2001, 2001.

[ROYE99] E. M. Royer e C. K. Toh, "A Review of Current Routing Protocols for *Ad Hoc* Mobile Wireless Networks", *IEEE Personal Communications*, abril, 1999.

[STEI98] M. Steiner, G. Tsudik e M. Waidner, "CLIQUES: A New Approach to Group Key Agreement", *18th International Conference on Distributed Computing System*, maio, 1998.

[YI01] S. Yi, P. Naldurg, e R. Kravets, "Security-Aware Ad-Hoc Routing for Wireless Networks", *The Second ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'01)*, agosto, 2001.

[ZHAN00] Y. Zhang e W. Lee, "Intrusion Detection in Wireless *Ad Hoc* Networks", *MobiCom'2000*, agosto, 2000.