Aspectos e Mecanismos de Segurança em Redes Ad Hoc *

Luiz Gustavo S. Rocha
lgrocha@gta.ufrj.br

Otto C. M. B. Duarte
otto@gta.ufrj.br

Grupo de Teleinformática e Automação
COPPE/POLI - PEE/DEL
Universidade Federal do Rio de Janeiro
http://www.gta.ufrj.br/

Resumo

Ao contrário das redes de comunicação tradicionais, as redes sem fio e sem infra-estrutura (Redes Ad Hoc) demandam mecanismos provedores de segurança que se compatibilizem com as características deste novo paradigma de redes de comunicação de dispositivos móveis.

A maior parte da pesquisa em redes ad hoc destina-se ao desenvolvimento dos mecanismos básicos de operação. Muito ainda deve ser feito no que tange aspectos de segurança, principalmente considerando cenários de operação hostis como em aplicações militares e comerciais. Os requisitos e a complexidade dos mecanismos de segurança devem variar com o tipo de aplicação.

As redes ad hoc apresentam vulnerabilidades em diversos níveis nas suas atuais implementações, sendo o objetivo das pesquisas em segurança o de dotar estas implementações de mecanismos capazes de conferir à rede a segurança em seus diversos aspectos, respeitando as limitações do sistema, como a escassez de recursos de rádio, bateria, processamento e memória.

Neste artigo serão apresentados os principais aspectos e alguns mecanismos propostos para segurança em redes ad hoc.

Palavras-chave: Redes de Computadores, Segurança, Redes Sem Fio Ad Hoc, Ataques.

Abstract

Unlike traditional communications networks, wireless ad hoc networks require mechanisms that offer security and that matched with the features of this new mobile device communication paradigm.

Research on ad hoc networks has been focused, up until now, on development of basic operation mechanisms. There is a lot of work to be done about security aspects, especially envision hostile operation scenarios like in a military or commercial application. The complexity and requirements of those security mechanisms must be adaptable with the kind of application.

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

Ad hoc communication networks have show vulnerabilities in several levels of its implementation. The aim of the research on security is to give to this implementation the mechanisms that will make security operations possible, always in concern of the system limitations, like radio resources, battery, processing and memory.

This paper is going to present a brief overview about main aspects and some mechanisms proposed for the security system in the ad hoc networks.

Keywords: *Computer Networks, Security, Wireless Ad Hoc Networks, Attacks.*

1 Introdução

Os requisitos de segurança de redes ad hoc estão intrínsicamente ligados ao tipo de cenário de aplicação da tecnologia [1, 2]. Atualmente, operações táticas militares é a principal aplicação. Unidades de combate ou resgate, equipadas com dispositivos de comunicação sem fio, em incursão num terreno hostil, constituem uma rede ad hoc a fim de trocar informações sobre a missão de forma segura.

Se todos, ou a maior parte, dos atributos de segurança que uma aplicação como esta requer forem atingidos, a próxima *killer application* promete ser o *m-commerce*. O comércio eletrônico móvel, juntamente com a propaganda direcionada, promete impulsionar o mercado da comunicação sem fio devido às novas possibilidades de transações que esta tecnologia traz. Mas para tanto os mecanismos de segurança devem estar aptos para conferir ao sistema como um todo uma operação segura. Cabe ressaltar que estes mecanismos devem estar consoantes com as restrições encontradas nos sistemas de comunicação móvel, tais como escassez de recursos de rádio, pouca memória, baixa capacidade de processamento e duração restrita da bateria.

Posto isto, deve-se imaginar que as abordagens tradicionais dos problemas de segurança em redes de comunicação não são totalmente e facilmente portáveis para estes cenários de aplicação, permanecendo como desafio o desenvolvimento e implementação de mecanismos de segurança robustos, do ponto de vista das ameaças para a rede, flexíveis, do ponto de vista da dinâmica da rede, e compatível, do ponto de vista das restrições do sistema.

O objetivo deste artigo é oferecer uma visão geral da área de segurança em redes ad hoc focalizando os principais aspectos e as principais tendências dos mecanismos de segurança para redes ad hoc.

Este trabalho está organizado da seguinte forma. Na Seção 2 são definidos os critérios e os objetivos do sistema de segurança para redes ad hoc. A Seção 3 descreve os pontos vulneráreis e os tipos de ataque que ameaçam uma rede ad hoc. São apresentados na Seção 4 os esquemas e mecanismos propostos para a solução de alguns dos problemas de segurança em redes ad hoc. Por fim, na Seção 5 são apresentadas as conclusões deste trabalho e possibilidades de trabalhos futuros.

2 Critérios e Objetivos da Segurança

Geralmente são considerados os seguintes atributos de segurança para redes de comunicação: disponibilidade, confidencialidade, integridade, autenticidade, e não-repúdio [3, 1]. Estes constituem o conjunto de características que o sistema de segurança deve conferir à rede. A disponibilidade refere-se a sobrevivência da rede mesmo sob ataque de impedimento de serviço ou operação lançado sobre alguma das camadas do sistema. A confidencialidade assegura que certo tipo de informação não seja descoberta por entidades não autorizadas. A integridade deve

garantir que uma mensagem não é corrompida quando transferida na rede a não ser por falha na interface de rádio, mas nunca por comportamento malicioso de um nó. A autenticação deve capacitar os nós de confirmar a identidade de seus pares de comunicação, evitando tentativas de mascaramento e personificação por nós mal intencionados. O não-repúdio confere ao sistema a capacidade de sempre identificar a origem de uma mensagem, o que é muito útil quando da necessidade de detectar nós comprometidos.

O objetivo do sistema de segurança é conferir à rede as características supracitadas em função das restrições encontradas, da dinâmica do comportamento da rede e ainda, apresentar-se escalável e sem comprometer o desempenho da rede. Assim sendo, pode-se dizer que o desenvolvimento e a implementação de uma arquitetura de segurança para redes ad hoc que atenda a estas especificações constituem tarefas custosas em todos os sentidos [4, 5].

O tipo de aplicação à que se destina a rede dá a palavra final sobre as qualidades do sistema de segurança a ser empregado [6, 4, 7]. Diferentes cenários podem relaxar ou restringir as primitivas de segurança da rede. A segurança deve estar presente nos diversos níveis, desde a aplicação até a segurança física do dispositivo, sempre mantendo esta dependência.

As idéias básicas dos mecanismos de segurança para redes ad hoc descendem das abordagens tradicionais dos problemas de segurança das redes de comunicação convencionais [8, 3]. Portanto ainda se fazem presentes as idéias de protocolos de autenticação, assinaturas digitais, chaves criptográficas e outras.

3 Vulnerabilidades e Ataques

Pode-se distinguir essencialmente dois grandes conjuntos de vulnerabilidades, vulnerabilidades dos mecanismos básicos e vulnerabilidades dos mecanismos de segurança [9]. A primeira pode ser tratada basicamente por esquemas de criptografia, ou seja, os mecanismo básicos de operação da rede, onde o roteamento é o mais crítico deles, passariam a trocar informações criptografadas. A segunda é mais complexa e agrega um certo número de diferentes soluções, mas tronou-se consenso que o ponto crítico é o gerenciamento das chaves do sistema de segurança [8, 10]. As redes ad hoc, devido a possibilidade de emprego em ambientes hostis, devem agregar mecanismos de forma a contornar o estado vulnerável em que se pode encontrar a rede quando da captura de um dos seus dispositivos.

O sistema torna-se vulnerável em relação aos mecanismos básicos quando, de alguma forma, é possível injetar, modificar ou replicar informações errôneas sobre a operação da rede, ou ainda, comportar-se de forma maliciosa e não cooperativa objetivando a interrupção da operação da rede. Com relação aos mecanismos de segurança, apresenta-se vulnerável o sistema que permite a criação, distribuição e uso de chaves de criptografia indevidamente e maliciosamente por entidades não autorizadas com o objetivo de acessar como membro autenticado os recursos e serviços da rede.

As ameaças que intentam contra as redes ad hoc vão desde a captura do dispositivo móvel até aos níveis da aplicação [9]. Os ataques podem ser classificados como ativos ou passivos e internos ou externos [2]. Tais ataques visam basicamente a descoberta de informações antes inacessíveis e o impedimento da realização dos serviços da rede. O mais severo dos ataques é o ativo interno onde o nó torna-se comprometido e realiza um ataque dito protegido, já que ele é um nó autenticado da rede, podendo inclusive vários destes nós comprometidos operar em grupo. O menos comprometedor dos ataques, mas não menos importante, é o tipo passivo externo que consiste na “escuta” das informações que trafegam na interface de rádio.

A ameaça de impedimento de serviço constitui um grade risco num sistema distribuído, como em uma rede ad hoc, e pode ter sua origem numa falha de operação não intencional ou em ações maliciosas por parte de elementos da rede. Suas conseqüências para operação da rede dependem do tipo de aplicação e do poder de ataque dos malfeitores. O ataque de personificação também pode trazer grandes prejuízos aos usuários da rede, já que consiste na capacidade de um nó disfarçar-se de outro e manter um comportamento malicioso a fim de inserir e obter informações não disponíveis para sua real identidade. A possibilidade de descoberta de uma informação por entidade não autorizada na rede deve ser amplamente combatida principalmente em se tratando de aplicações militares e comerciais. Estas informações críticas devem ser protegidas contra ataques de exposição a fim de manter em sigilo detalhes como localização dos nós, chaves, senhas e identidade de operadores e proprietários dos dispositivos [1, 2, 8].

4 Medidas de Segurança

4.1 Proteção Física

A primeira medida de segurança cabível e comum a todos os sistemas é a segurança física do dispositivo móvel de comunicação. Isto não consiste em tarefa simples já que pode-se imaginar cenários onde é constante a ameaça de captura do dispositivo. A tecnologia de *smart cards* pode ser uma solução tentando centralizar as informações vitais em si e utilizando o dispositivo móvel apenas como interface (ex.: SIM *cards* do GSM) [9]. A implementação de um hardware *tamper resistent* não é uma solução definitiva ainda devido a limitação dos *smart cards* e a possibilidade do obtenção de suas informações, por meios óbvios e outros bem menos convencionais (ex.: hardware específico).

4.2 Proteção do Enlace

Como toda a comunicação é feita pelo ar, uma estratégia de transação de informações adequada deve ser empregada para evitar que um *jamming* ou *eavesdropping* sejam feitos com facilidade, por outros aparelhos semelhantes ou por um hardware específico. Uma solução possível é o espalhamento do espectro por salto em freqüências (FHSS) [8, 10]. Nesta técnica a banda total disponível é dividida em sub-canais que são selecionados para utilização de forma aleatória (ex.: na implementação do Bluetooth).

4.3 Proteção dos Mecanismos Básicos e de Segurança

Para proteção dos mecanismos básicos de operação da rede a solução mais intuitiva é proteger suas trocas de mensagens assim como é feito com as informações dos usuários da rede. Para tanto devem ser adotados esquemas de criptografia adaptados para estes ambientes. Sendo assim, chega-se ao ponto mais vulnerável do sistema de segurança que é gerenciamento das chaves do esquema de criptografia. Por razões de eficiência um bom esquema faria uso de chaves assimétricas para a autenticação e para o estabelecimento seguro de chaves simétricas que seriam posteriormente utilizadas para a comunicação entre os nós. Este esquema de chaves deve levar em conta características como: as propriedades da autoridade da rede, acessibilidade de um nó em relação à rede, o comportamento da fase de inicialização do esquema, o tipo de relação entre os nós e entre os nós e a autoridade da rede e, por fim, a distribuição da confiança na rede [9].

A parte do problema que abrange a inicialização do sistema de segurança (*bootstrap*) é uma estrada por onde poucos se aventuraram a caminhar, com relação às outras características as propostas mais recentes baseiam-se em dois princípios que tendem a cobri-las bem, sendo estes: a redundância na topologia da rede e a distribuição de confiança na rede [3].

Nestes cenários são empregados esquemas de criptografia, como assinaturas digitais, com infra-estrutura de chave pública, onde cada nó possui um par de chaves (uma pública e a outra privada), e uma entidade confiável, denominada autoridade de certificação. Esta entidade fica responsável pela associação confiável entre os nós da rede e suas chaves públicas. Enquanto um nó detém confidencialmente sua chave privada, a sua chave pública deve ser anunciada na rede. Cabe ressaltar que o próprio serviço de certificação também possui um par de chaves pública/privada. A diferença nesta abordagem para redes ad hoc é que a responsabilidade de gerenciamento de chaves será distribuída numa comunidade de nós. A chave pública do serviço de certificação é conhecida por todos os nós integrantes da rede, mas a chave privada do serviço é dividida e compartilhada entre *n* nós que passam a ser denominados de servidores. Todos os nós da rede podem submeter pedidos de chaves públicas da rede e renovações da própria chave para este serviço de certificação distribuído.

4.3.1 Criptografia por Limiar

O controle das chaves por certificação com assinaturas digitais vem acompanhado de um mecanismo de criptografia por limiar (*threshold criptography*), que permite a $(t+1)$ partes das *n* partes distribuídas nos *n* servidores realizarem o serviço de certificação de forma distribuída, sendo impossível para até *t* partes, inclusive por conspiração, proceder com o serviço. Pode-se dizer então que o esquema é tolerante a *t*, dos *n* servidores, estarem comprometidos ou fora de operação naquele instante. A Figura 1 mostra a arquitetura do serviço de certificação de chaves públicas por assinaturas compartilhadas.

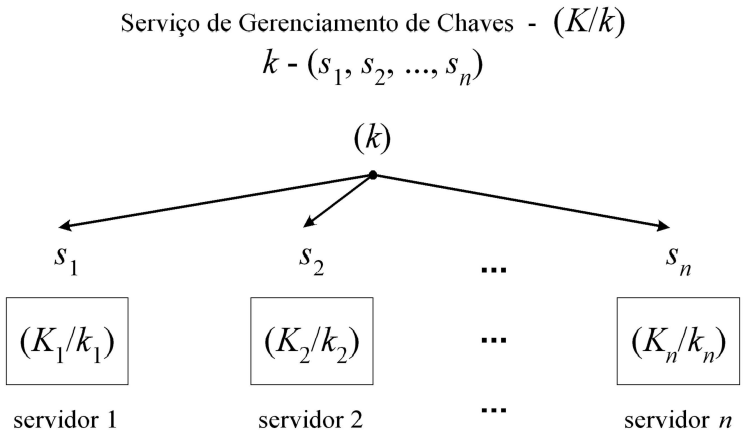

Figura 1: Esquema de gerenciamento de chaves criptográficas para assinaturas compartilhadas de certificados

A criptografia por limiar opera numa configuração $(n, t+1)$, onde *n* partes compartilham a operação de criptografia, a assinatura digital por exemplo, baseada no seu pedaço recebido da chave privada *k* do serviço, sendo suficientes apenas $t+1$ partes quaisquer para a operação completa e correta do serviço. Há ainda a participação de um dos *n* servidores como uma figura

especial, que passa a ser designado combinador, que computa a assinatura final para o certificado com base nas assinaturas parciais a ele enviadas. Nenhuma informação adicional é visível para o nó combinador. Esta operação de combinação também pode ser feita em redundância de $(t+1)$ servidores a fim de garantir a legitimidade da assinatura e onde qualquer um deles pode verificar a validade da assinatura computada, por meio da chave pública do serviço de certificação [6, 3]. A Figura 2 mostra um exemplo de criptografia por limiar numa configuração (3,2) ocorrendo a falha natural ou descarte proposital da informação de um dos *n* servidores.

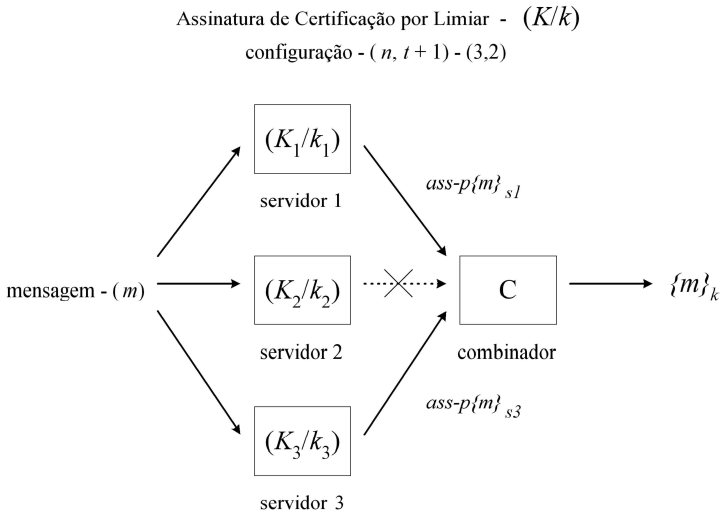

Figura 2: Esquema de criptografia por limiar para certificação compartilhada

4.3.2 Atualização Compartilhada

O esquema de criptografia limiar traz a reboque o mecanismo de atualização compartilhada (*share refreshing*) que tem como objetivo introduzir medidas de segurança pró-ativas e a característica de adaptabilidade ao sistema de segurança. Estas visam tolerar ataques de adversários que se movem pelos nós da rede e cobrir a dinâmica de uma rede ad hoc com relação a topologia e conjunto de membros.

O mecanismo de atualização compartilhada permite que os servidores computem novas partes de *k* partindo das antigas partes e em colaboração com outros servidores. Dados os *n* servidores e as *n* partes da chave privada *k*, cada parte s_i em um servidor *i*, são geradas em cada servidor *n* subdivisões da sua parte de *k*, que são $(s_{i1}, s_{i2}, ..., s_{in})$. Então cada subdivisão s_{ij} é direcionada ao servidor *j*, por enlace seguro, de forma que o servidor *j* de posse do conjunto $(s_{1j}, s_{2j}, ..., s_{nj})$ das subdivisões pode computar, juntamente com sua divisão de *k* antiga, sua nova divisão [3, 6]. Esta operação é factível baseada na propriedade homomórfica das divisões e subdivisões de uma chave *k* [3].

Novamente este esquema opera numa configuração $(n, t+1)$. Este mecanismo também pode evoluir de forma que $(n, t+1)$ passe para $(n', t'+1)$ o que permite a flexibilização em relação a detecção de servidores comprometidos, a indisponibilidade temporária de um enlace e a dinâmica da topologia e do conjunto de membros da rede [3, 6]. A Figura 3 apresenta de forma esquemática o mecanismo de atualização.

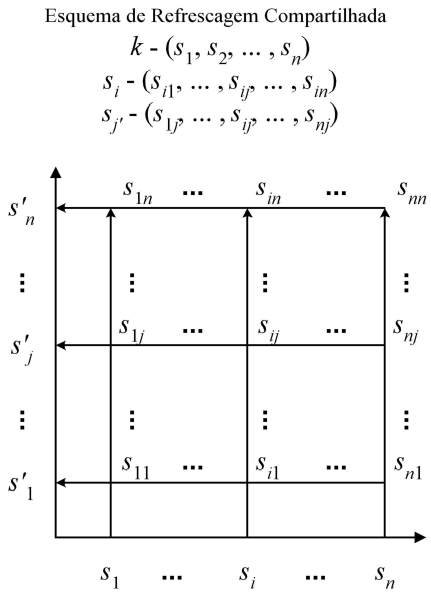

Figura 3: Esquema de atualização compartilhada das chaves distribuídas

5 Conclusão

Neste trabalho procuramos ressaltar as características das redes ad hoc de forma poder levantar os problemas relativos a segurança apontando as vulnerabilidades desta tecnologia de comunicação mediante ameaças. Muito ainda deve ser pesquisado e implementado com o objetivo de tornar realidade os cenários de aplicação que podemos imaginar para esta tecnologia. Grandes avanços foram obtidos nos mecanismos de descentralização de confiança e aproveitamento de redundância na rede, mas pouco se têm visto a respeito da fase inicial da configuração do sistema de segurança. Os esquemas apresentados como solução parcial das vulnerabilidades dos mecanismos básicos de operação e de segurança possuem, em análises preliminares, bom desempenho, conferindo robustez e flexibilidade ao sistema. Aplicações em fase de implementação que se valeram das idéias aqui expostas obtiveram resultados satisfatórios em relação aos objetivos do sistema de segurança.

A abordagem baseada em certificação alcança vários dos requisitos de segurança e juntamente com o esquema de criptografia por limiar e o mecanismos de atualização compartilhada apresentam-se plenamente consoantes com as especificações do sistema de segurança caracterizado para a tecnologia de comunicação de redes ad hoc. Um sistema implementado com esta arquitetura torna-se tolerante à falhas, seja por comportamento malicioso (nós comprometidos) ou por falha natural da operação, sendo então adequado para redes com a dinâmica caractrística das redes ad hoc.

Medidas pró-ativas, como a atualização compartilhada e a renovação de certificados, podem introduzir um *overhead* no processo de comunicação, não chegando a comprometer o desempenho da rede, mas trazendo grande benefícios em relação a proteção contra adversários móveis na rede.

Muito ainda deve ser estudado a fim de viabilizar o emprego das redes ad hoc em aplicações mais sensíveis em requisitos de segurança, como por exemplo o *m-commerce*. As restrições em relação aos dispositivos de comunicação móvel ainda são um desafio para a implementação de

esquemas mais complexos, porém mais robustos em presença de ameaças, para a arquitetura do sistema de segurança. Embora os mecanismos básicos de operação da rede já comportem o comportamento dinâmico e imprevisível das redes ad hoc, novas abordagens são esperadas a respeito da arquitetura do sistema de segurança. A disseminação desta tecnologia de comunicação está atrelada ao desenvolvimento de mecanismos que venham garantir os requisitos de segurança necessários a cada aplicação.

Referências

[1] A. Vanhala, "Security in ad hoc networks", in *Research Seminar on Security in Distributed Systems*, 2000.

[2] V. Kärpijoki, "Security in ad hoc networks", in *Seminar on Network Security*, 2001.

[3] L. Zhou e Z. J. Haas, "Securing ad hoc networks", *IEEE Networks*, 1999.

[4] M. Schmidt, "Subscriptionless mobile networking: Anonymity and privacy aspects within personal area networks", tech. rep., Institute for Data Communications Systems, University of Siegen, Germany, 2001.

[5] A. J. Lalana Kagal, Jeffrey Undercoffer e T. Finin, "Vigil: Enforcing security in ubiquitous environments", tech. rep., University of Maryland, Baltimore County, 2001.

[6] J. Kong, P. Zerfos, H. Luo, S. Lu e L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks", tech. rep., Computer Science Department, University of California at Los Angeles, 2001.

[7] E. Skow, J. Kong, T. Phan, F. Cheng, R. Guy, R. Bagrodia, M. Gerla e S. Lu, "A security architecture for application session handoff", tech. rep., Computer Science Department, University of California at Los Angeles, 2001.

[8] M. Jakobsson e S. Wetzel, "Security weaknesses in bluetooth", tech. rep., Lucent Technologies - Bell Labs, Information Sciences Research Center, 2001.

[9] J. Hubaux, L. Buttyan e S. Capkun, "The quest for security in mobile ad hoc networks", in *ACM Symposium on Mobile Ad Hoc Networking and Computing - MobiHOC*, 2001.

[10] M. Träskbäck, "Security of bluetooth: An overview of bluetooth security", tech. rep., Department of Electrical and Communications Engineering, Helsinki University of Technology, 2000.