Universidade Federal de Pernambuco
Graduação em Engenharia da Computação
Centro de Informática
2013.2

Mecanismo de Segurança para Redes Móveis Ad Hoc

Proposta de trabalho de Graduação

Aluno: Gregório Patriota Correia (gpc@cin.ufpe.br)

Orientador: Djamel Fawzi Hadj Sadok (jamel@cin.ufpe.br)

Recife, 29 de Novembro de 2013

Sumário

Contexto

Com o avanço das tecnologias, a miniaturização dos *mainframes* disponibilizou dispositivos de grande poder computacional com um alto grau de mobilidade, em conjunto com os recentes avanços na comunicação sem fio permitiram que esses diferentes dispositivos (computadores portáteis, PDAs e telefones celulares, por exemplo) se comuniquem e interajam sem a existência de um elemento central de controle. Este tipo de redes é conhecido como ad hoc. Redes ad hoc são redes sem fio, cujos nós são dinâmicos e móveis e também podem se comunicar com outros nós sem uma coordenação central ou uma infraestrutura de comunicação pré-estabelecida para fornecer suporte ao compartilhamento de informações e a cooperação.

A falta desse elemento central que coordena o tráfego da rede é considerada como uma vantagem e ao mesmo tempo uma desvantagem dessa arquitetura. A vantagem refere-se ao custo de implantação e manutenção dessas redes, não há uma estrutura física para manter e implantar, sua alta volatilidade faz com que a topologia se adapte a qualquer ambiente. Porém, a falta de um elemento central impõem problemas de balanceamento de tráfego na rede e como crítica é um ponto critico na segurança dos dados, portanto é uma desvantagem.

O crescimento das redes ad hoc ampliou o número de aplicações que usam este tipo de infraestrutura e as, consequentemente, uma maior aplicabilidade. Esse crescimento por sua tornou maior a exposição dos dados que trafegam nessas redes.

Atualmente, para proteção dos dados há diversas técnicas de criptografias, porém devido à natureza das redes ad hoc nem todos os esquemas de criptografias existentes para redes estruturadas são diretamente aplicados as redes ad hoc. Os esquemas podem ser adaptados para o ambiente não estruturado, como utilizar abordagens de chaves públicas e privadas ou uso de esquemas de hash nas redes ad hoc.

Devido às restrições energéticas e de processamento cada alternativa deve ser bem avaliada para não comprometer o tempo de existência da rede. É preciso garantir que a informação protegida esteja segura sem afetar o desempenho da rede. Garantir que uma informação está segura é assegurar que o tempo de criptoanálise seja maior que o tempo de vida da informação ou que o custo para sua criptoanálise seja maior que o valor da informação.

Objetivos

Este trabalho de graduação (TG) tem como objetivo pesquisar e desenvolver aplicações e serviços em redes de infraestrutura considerada crítica como em empresas geradoras de energia, petróleo e gás, indústrias, transporte público, entre outras.

Para proteger as informações dessas redes será projetado um mecanismo de criptografia sobre o framework HTR (Heterogenous Technologies Routing) para garantir integridade e autenticidade às mensagens de controle.

Um esquema baseado em HMAC (Hash-based Message Authentication Code) será implementado mantendo-se a chave secreta para os nós e variando os algoritmos de hash, tais como: MD5, SHA-1, SHA-256, SHA-384, SHA-512.

Uma análise para avaliar o impacto na rede será realizada, utilizando como métricas: tempo de convergência, consumo energético e overhead na rede. Os dados serão coletados e comparados com a rede HTR sem a utilização do esquema de criptografia a ser definido neste TG.

Resumindo, o objetivo principal é obter um esquema seguro, baseado em um dos algoritmos de hash mencionados acima, que garanta integridade e autenticidade aos dados da rede com o menor impacto sobre a mesma.

Cronograma

Segue o cronograma das atividades relacionadas para o desenvolvimento deste TG, relacionando o tempo para realizar cada atividade.

Atividade	Dezembro/2013				Janeiro/2014				Fevereiro/2014				Março/2014			
Levantamento do estado da arte																
Definição da arquitetura e Prototipação																
Implementação																
Validação e Testes																
Coleta e Análise de Resultados																
Escrita da Monografia																
Apresentação do TG																

Referências

E. Souto, R. Aschoff, J. Lima Junior, R. Melo, D. Sadok, and J. Kelner, “HTR: A framework for interconnecting wireless heterogeneous devices”, in Consumer Communications and Networking Conference (CCNC), 2012 IEEE, 2012, pp. 645-649.

A. Hasflund, A. Tønnesen, R. Bjørgum Rotvik, J. Andersson, and Ø. Kure, “Secure Extension to the OLSR protocol”, in OLSR Interop and Workskop, 2004.

S. Agrawal, S. Jain, and S. Sharma, “A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks”, in Journal of Computing, vol. 3, January 2011

K. Sanzgiri, B. Dahill, B.N. Levine, C. Shiels, and E. M. Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks”, in 10th IEEE International Conference on Network Protocols, 2002

H. Yang, H. Luo, S. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions”, in IEEE Wireless Communications, February 2004

Willian Stallings, “Criptografia e segurança de redes, Princípios e práticas”, 4º Edição, Pearson Prentice Hall

Assinaturas

Recife, 29 de Novembro de 2013

X

Djamel Fawzi Hadj Sadok
Orientador

X

Gregório Patriota Correia
Aluno