Projeto do trabalho da disciplina de Sistemas Distribuídos

Eduardo da Silva

1. Proposta inicial

Uma rede *ad hoc* móvel é um grupo de computadores móveis sem fio, chamados nós, que cooperam entre si realizando o encaminhamento de pacotes, de forma a possibilitar a comunicação entre os nós, mesmo que a distância entre os nós comunicante ultrapasse ao limite de transmissão do sinal direto sem fio [Hu et al. 2005].

Diversas são as dificuldades encontradas para prover segurança nas redes *ad hoc* móveis, devido a diversos fatores. Alguns desses fatores foram discutidos em [Buttyan and Hubaux 2003] e são apresentados a seguir:

- o canal de comunicação sem fio é vulnerável, assim, as mensagens transmitidas na rede podem ser capturadas e também mensagens falsas podem ser injetadas na rede;
- os nós também são vulneráveis, principalmente por não estarem localizados em uma sala fisicamente protegida;
- a ausência de infraestrutura faz com que soluções clássicas de segurança, baseadas em autoridades certificadoras, não seja aplicáveis a essas redes;
- a topologia dinâmica dessas redes dificulta o processo de roteamento dos pacotes na rede, e ainda, informações incorretas de rotas podem ser criadas por intrusos ou por nós comprometidos. O desafio dos algoritmos de roteamento está em distinguir entre as mudanças de rotas causadas por mudança na topologia, das mudanças que foram causadas de forma maliciosa.

O objetivo desse trabalho é apresentar uma proposta de um esquema de gerenciamento de chaves. Esse esquema, discutido em [Capkun et al. 2003] tem como finalidade suprir uma dessas necessidades de segurança em rede *ad hoc* móveis discutida anteriormente: o gerência de chaves. O desafio dessa área está no fato de que, para prover segurança em redes *ad hoc* móveis é necessário que o esquema de segurança seja auto-organizável, ou seja, que a segurança da rede não dependa de qualquer autoridade confiável central[Capkun et al. 2003].

[Capkun et al. 2003] propõe um esquema de gerenciamento de chaves usando os princípios do PGP (*Pretty Good Privacy*). O funcionamento e as características do PGP são discutidas em [Zimmermann 1995] e, dentre as principais características do PGP, uma importante é o gerenciamento de chaves. No PGP o acordo das chaves é realizado mediante a confiança entre os pares comunicantes. Como conseqüência dessa características, as redes que utilizam uma comunicação baseada em PGP, possuem um fenômeno chamado do *Small World* [Capkun et al. 2002].

Esse esquema erá implementado utilizando o simulador NS-2 (*Network Simulador -2*)e serão apresentados os resultados e conseqüências de sua utilização, como: utilização de recursos e vulnerabilidades.

Referências

Buttyan, L. and Hubaux, J.-P. (2003). Report on a working session on security in wireless ad hoc networks. *SIGMOBILE Mobile Computing and Communications Review*, 7(1):74–94.

Capkun, S., Buttyan, L., and Hubaux, J.-P. (2002). Small worlds in security systems: an analysis of the pgp certificate graph. In *NSPW '02: Proceedings of the 2002 workshop on New security paradigms*, pages 28–35, New York, NY, USA. ACM Press.

Capkun, S., Buttyan, L., and Hubaux, J.-P. (2003). Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 2(1):52–64.

Hu, Y.-C., Perrig, A., and Johnson, D. B. (2005). Ariadne: a secure on-demand routing protocol for ad hoc networks. *Wirel. Netw.*, 11(1-2):21–38.

Zimmermann, P. R. (1995). *The official PGP user's guide*. MIT Press, Cambridge, MA, USA.