Network Performance Centric Security Design in MANET

Hao Yang
hyang@cs.ucla.edu

Gary Zhong
gzhong@cs.ucla.edu

Songwu Lu
slu@cs.ucla.edu

CS Department, UCLA, Los Angeles, CA 90095

"In theory there is no difference between theory and practice. In practice there is..."

–Bruce Schneier in *Secrets and Lies* [3],2000

Security is a basic requirement for mobile ad hoc networks. Several recent papers [4, 1, 2] have started to address security issues in such networks. While these early proposals each have their own merit, they mainly focus on the security vigor of the design and leave the *network performance* aspect largely unaddressed. As a result, these solutions may be extremely secure from the cryptographic standpoint, but their real performance when deployed in the network is unclear. This concern is further aggravated by the unique characteristics of ad hoc networks, such as highly dynamic network topology, frequent node arrival/departure, and bandwidth-constrained wireless links.

In this work, we shift our main attention from the cryptography-centric design approach to a more network-centric design scheme, and focus on the practical network performance aspect of the security design. Our goal is to develop *network performance-centric* security solutions that effectively balance security strength and network performance in practice.

We focus on node authentication, the basic component in a security solution. At the first stage, we investigate several design choices – centralized, peer-to-peer, and localized authentication schemes, and examine their network performance by extensive simulations. The centralized scheme [4] is similar to the TTP (Trusted Third Party) authentication widely used in the wired networks, in which authentication is done via the third-party certificate authority (CA). The peer-to-peer authentication scheme [1] bears the same philosophy as PGP, where authentication is done through a chain of trust relationship that forms the "web of trust". The localized scheme [2] is specially designed for ad hoc networks, in which each node is authenticated and monitored by its multiple local neighboring nodes.

The simulation results are summarized in Table 1.
Scalability: We examine whether the design scales to the number of nodes. The average node speed is 10m/s, and there is no channel error and other ongoing traffic (benchmark setting). When the number of nodes increases from 40 to 100, the success ratio of the authentication request in centralized scheme drops from 92% to 22%; the success ratio in peer-to-peer scheme remains stable around 88%; while the success ratio in localized scheme remains stable around 96%.
Availability: We increase the network traffic load and examine whether the design provides "anytime, anywhere" security service to the mobile hosts. For a 60-node setting with average speed of 10m/s, when the network traffic load increases from 0 to 100 pkt/s (packet size 512B), the success ratio in centralized schemes drops from 80% to 45%; the success ratio in peer-to-peer scheme almost remains stable around 85%; while the success ratio in localized scheme remains stable around 95%.
Robustness: We examine the robustness feature for different channel conditions. For the same 60-node setting, when the channel error rate increases from 0 to 10%, the success ratio in centralized scheme drops from 80% to 50%; the success ratio in peer-to-peer scheme drops from 85% to 82%; while the success ratio in localized scheme drops from 95% to 93%.

The fundamental reason for the performance difference is the traffic pattern in these schemes. The localized scheme has the best network performance in that the traffic is not only distributed in the network, but also confined in the local neighborhood. As a result, the impact of network scale, traffic load, channel error, mobility, etc., on the localized authentication service is very small in most scenarios.

The current study provides two guidelines for future security design in ad hoc networks: 1) the network performance aspect should be explicitly considered in the design; 2) in order to have good network performance, it is desirable for the security solution to have localized traffic pattern. Our next-stage effort focuses on devising new network mechanisms to improve the performance of the security design.

References

[1] J. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *Proc. ACM MobiHOC*, 2001.
[2] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for manet. In *Proc. IEEE ICNP*, 2001.
[3] B. Schneier. *Secret and Lies, Digital Security in a Networked World*. Wiley Computer Publishing, 2000.
[4] L. Zhou and Z. Haas. Securing ad hoc networks. *IEEE Networks*, 13(6):24–30, 1999.

Scheme	Centralized	Peer-to-Peer	Localized
Scalability	Bad	Good	Good
Availability	Bad	Uncertain	Good
Robustness	Bad	Uncertain	Good
Communication	Centralized	Distributed	Localized
Computation	Undertaken solely by the servers	Shared by the nodes	Shared by the nodes

Table 1: Network Performance Comparison of Three Authentication Schemes