Key Management for Heterogeneous Ad Hoc Wireless Networks *

Seung Yi, Robin Kravets
Department of Computer Science
University of Illinois at Urbana-Champaign
Urbana, IL 61801
{seungyi,rhk}@cs.uiuc.edu

1 Introduction

Since its birth more than two decades ago, public key cryptography has been recognized as one of the most effective mechanisms for providing fundamental security services including authentication, digital signatures and encryption for dynamic networks. Effective management of keys, or digital certificates holding the keys, is one of the key factors for the successful wide-spread deployment of public key cryptography. PKI (Public Key Infrastructure), an infrastructure for managing digital certificates, was introduced for this purpose. The most important component of PKI is the CA (Certificate Authority), the trusted entity in the system that vouches for the validity of digital certificates. The success of PKI depends on the availability of the CA to the principals in the system (or the nodes in the network) since a principal must correspond with the CA to get a certificate, check the status of another principal's certificate, acquire another principal's digital certificate, and so on. PKI has been widely deployed for wired networks and some infrastructure-based wireless networks. Since good connectivity can be assumed in such networks, the main thrust of research in such environments has focused on the availability of the CA and the scalability of the CA to handle a large number of requests.

However, it is still unclear if such approaches can be extended to ad hoc networks. Connectivity, which was assumed to be good in previous PKI solutions, is no longer stable in ad hoc networks. Unfortunately, maintaining connectivity is one of the main challenges in ad hoc networks, since the inherent infrastructurelessness of ad hoc networks makes it hard to guarantee any kind of connectivity. Another serious problem present in ad hoc networks is the physical vulnerability of the nodes themselves. Considering that most ad hoc networks will be deployed with mobile nodes, the possibility of the nodes being captured or compromised is higher than in wired networks with stationary hosts. Mobile nodes in a infrastructure-based wireless networks have the same vulnerability, but they can rely on the infrastructure for detection of compromised nodes and potentially some help with recovery. With an infrastructure-based solution, mobile nodes may store all sensitive information in the infrastructure and maintain minimal information in the device. Since there is no stable entity in an ad hoc network, the vulnerability of ad hoc nodes is even higher.

Currently proposed solutions for providing PKI for ad hoc networks address the physical vulnerability of the nodes by employing the distribution of CA functionality across multiple nodes and using threshold cryptography[4, 2]. These approaches also increase the availability of the CA. The first challenge in such approaches is picking which nodes should be a part of the distributed CA. A random set of nodes from a network can be chosen to play the role of CA. Such a random choice may not be best for security of the whole network. The second challenge is how to provide efficient, yet effective, communication between the mobile nodes and the CA nodes to create the illusion of an available CA, even in dynamic networks with possible compromises or partitions.

This work describes a framework to provide efficient yet effective distributed CA service for ad hoc wireless networks. We select physically or computationally more secure nodes as MOCAs (MObile Certificate Authority) and use threshold cryptography[1] to distribute the CA's private key among these MOCA nodes. We also provide a protocol for clients to contact MOCAs and get certification services without incurring excessive overhead.

2 MOCA Approach

The main technique in our approach is to use threshold cryptography to distribute the CA's private key among many nodes that collectively act as the CA for the network. Given this distributed approach, there are two main challenges: (1) How to pick the MOCA nodes and (2) How to make them available for services.

*This work was supported in part by the National Science Foundation under grant ANI-0081308.

Proceedings of the 10 th IEEE International Conference on Network Protocols (ICNP'02)
1092-1648/02 $17.00 © 2002 IEEE

In our work, MOCAs are chosen based on an observation of heterogeneity within an ad hoc network. Most existing work blindly considers all nodes in an ad hoc network to be identical, which is not necessarily true. For example, in a military battle field scenario (one of MANET's most popular examples), there can be many different types of mobile nodes in the field (e.g. infantry soldiers, tanks, platoon leader's jeeps, command and control vehicles, etc). This heterogeneity can be exploited when choosing the MOCA nodes. Physically more secure and computationally more powerful nodes are the typical choices for MOCAs. These selected MOCAs share the secret and collectively provide CA functionality.

Client nodes are equipped with MP(MOCA certification Protocol), which enables communication with a sufficient number of MOCAs in an efficient and effective way. In initial version of MP, clients flood the network with certification requests and MOCAs that receive the request reply with a certification reply. This approach works very well in terms of success ratio but has high overhead due to its flooding nature. To alleviate this overhead, we investigated the cache tables of client nodes and discovered that with a certain amount of certification traffic in the network, a mobile node tends to have many cached routes entries to enough MOCA nodes. To exploit this, we developed a unicast-based optimization of MP that uses multiple sets of unicasts without route discovery when there are enough cached routes in the client's local cache. Since there can be more than enough cached routes, we tested three different selection criteria: closest MOCAs, freshest MOCAs, and random MOCAs.

3 Preliminary Results

We use NS-2 network simulator for our simulations. Our initial flooding based approach shows a good success ratio but suffers from overhead due to flooding.

Fig. 1 shows the number of successfully received certification replies for 1000 certification requests. 30 MOCAs are deployed in the network, so the maximum number of replies for a certification request is 30. Under varying mobility patterns, more than 90% percent of requests are answered with 15 or more replies.

While all three of our unicast-based protocols work more efficiently than flooding, closest-unicast that picks the closest MOCAs from the client turns out to be the best in success ratio and latency. Fig. 2 shows the comparison of success ratios between different flavors of unicast-based protocols. Flooding is shown as the baseline. More detailed simulation results are available in [3].

Our simulation results show the effectiveness of our approach and we provide some insights into the configuration of such security services in ad hoc networks.

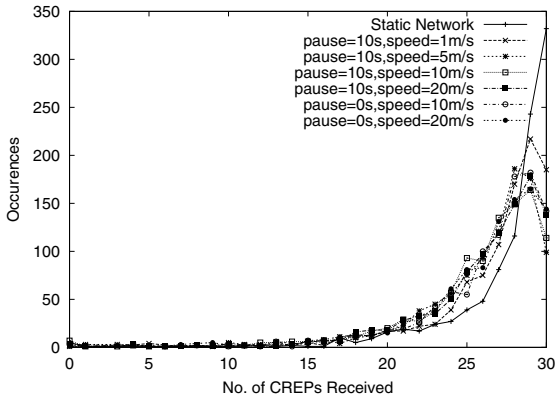

Figure 1. No. of received certification replies with flooding

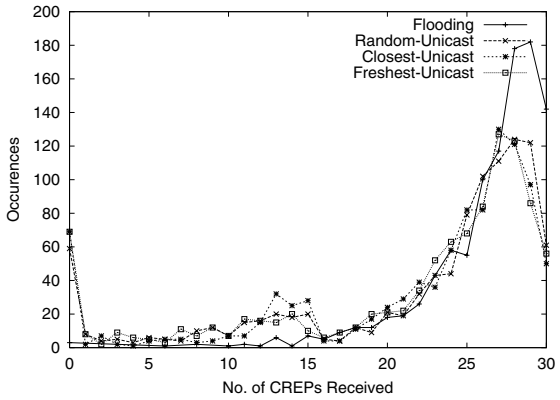

Figure 2. No. of received certification replies with unicast-base protocols

References

[1] Y. Frankel and Y. G. Desmedt. Parallel Reliable Threshold Multisignature. Technical Report TR-92-04-02, Univ. of Wisconsin–Milwaukee, 1992.

[2] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks. In *Proceedings of ICNP '01*.

[3] S. Yi and R. Kravets. Key Management for Heterogeneous Ad Hoc Wireless Networks. Technical Report UIUCDCS-R-2002-2290/UILU-ENG-2002-1734, University of Illinois at Urbana-Champaign, 2002.

[4] L. Zhou and Z. J. Haas. Securing Ad Hoc Networks. *IEEE Network Magazine*, Nov. 1999.

Proceedings of the 10 th IEEE International Conference on Network Protocols (ICNP'02)
1092-1648/02 $17.00 © 2002 IEEE