A Framework for Key Management in Mobile Ad Hoc Networks

George C. Hadjichristofi, William J. Adams, and Nathaniel J. Davis IV
Virginia Polytechnic Institute and State University, Blacksburg, Virginia 24061, USA
{ghadjich, wjadams, ndavis}@vt.edu

Abstract

Recently proposed key management systems (KMSs) provide limited functionality in highly partitioned mobile ad hoc networks. In this paper we present a framework for key management that provides redundancy and robustness for Security Association (SA) establishment between pairs of nodes in mobile ad hoc networks. Our KMS uses a modified hierarchical trust Public Key Infrastructure (PKI) model in which nodes can dynamically assume management roles. The system ensures high service availability for the network members through a number of schemes. A novel behavior grading mechanism provides security criteria for the network nodes and aids the management functions of the KMS to revoke or reissue certificates for nodes. This mechanism is based on the notion of trust, and more specifically on SAs among nodes in the entire network. In this paper we give an overview of the framework of the system and present a performance analysis of the system based on certificate issuance and acquisition. Finally, we compare our KMS with threshold cryptography schemes.

1. Introduction

A mobile ad hoc network (MANET) is a collection of independent mobile nodes. MANET links are wireless, which results in communications that are less dependable than wired links and have capacity constraints. A MANETs is vulnerable to eavesdropping and the nodes in this network often have little physical protection. In order to counteract some of these threats, a MANET uses mechanisms such as IP Security (IPsec), to secure transmitted data. However, prior to IPsec deployment, nodes need to establish Security Associations (SAs). During the establishment of an SA, two nodes authenticate each other using certificates, which are a primary form of identity verification. A Key Management System (KMS) creates, distributes, and manages these certificates. Thus, the KMS is at the heart of the network's defenses.

We developed a KMS that: (1) provides high service availability in highly partitioned networks, (2) requires minimal pre-configuration during the network deployment phase, and (3) can accommodate new nodes joining the network.

The contribution of this paper is the KMS framework and, more specifically, the unique way the various components that comprise a KMS interoperate. Of significant importance is the introduction of a behavior grading scheme that interoperates with the KMS and aids the certificate revocation and reissuance process. We provide an analysis of the availability of the KMS and compare it with threshold cryptography schemes.

The rest of the paper is organized as follows: Section 2 presents an overview of the previous work conducted related to KMSs. Section 3 presents the various roles that nodes undertake in the KMS and describe their functions based on those roles. Next, in Section 4, we explain the security aspects of our scheme, such as behavior grading. In Section 5, we present the performance analysis of our scheme and compare it to threshold cryptography schemes. Finally, Section 6 summarizes our contribution.

2. State of the art

Other researchers have studied ways to develop key management schemes to enhance the efficiency of establishing SAs in MANETs. Zhou and Haas [1] proposed a partially distributed key management service for MANET that utilized threshold cryptography. A public/private key pair, K/k, was created for the entire KMS. The system's private key, k, was divided into *n* shares, assigning one share for each server. In addition, each server was pre-configured with the public key of the other servers. When signing a certificate, a server generated a partial signature and sent it to an arbitrarily selected combiner. The combiner collected a number of signatures, computed the certificate of a node and sent

the certificate to that node. Authors in [2] proposed a similar threshold cryptography system that allowed new nodes joining the network to obtain a share of the KMS' private key. The advantage of this scheme as compared to [1], was that it increased availability and spread the load of key management service over a higher number of servers. Based on other experts in the field [5], this system seemed to be vulnerable to the Sybil attack [7] because of the network-wide distribution of the private key. Yi and Kravets [3] extended the work done in [1] for application in a MANET. They defined tunable parameters that could be used in the operation of their KMS.

The authors in [4] continued this line of investigation and applied the KMS proposed by Zhou and Haas [1] on a cluster-oriented network. Cluster heads were assigned the role of signing certificates for other nodes. The authors introduced the idea that nodes had to present a certain number of warrants from existing full members verifying their credentials before they could obtain partial certificates from cluster heads (and become full members of the network). Unlike our KMS, these threshold cryptography KMSs [1][3][4], seemed to be unsuitable for highly partitioned MANETs, as shown in our analysis in Section 5.

The authors in [5] proposed a Public Key Infrastructure (PKI) anarchy model similar to Pretty Good Privay (PGP). The KMS system allowed all of the nodes in a MANET to issue certificates to each other. In their later work [8], the authors noted that this system required a costly initialization phase in terms of both overhead and time since each node had to build its local certificate repository to be able to use the services of the system. Moreover, this scheme utilized transitivity of trust, which had the fatal problem of the untrustworthiness of certificate chains that is inherent in PKI anarchy models.

3. Description of the system

One of the objectives of our KMS system was to be flexible enough to provide sufficient functionality for existing nodes as well as new ones. At the same time, we wanted to provide reasonable security criteria to the nodes in order to establish trust between them.

This KMS was implemented in the test bed described in [9] and integrated with FreeS/WAN IPsec, an off-the-shelf implementation of IPsec. Our KMS in that test bed provided authentication information to the nodes to establish SAs and setup IPsec tunnels between them. A more detailed description of our KMS is provided in [10].

In our network environment, we assumed that nodes could leave and join the network at any point in time and users could generate their own keys. Our KMS used a modified hierarchical model, shown in Fig. 1. The roles that were undertaken by the nodes in the hierarchical model were: Root Certificate Authority (RCA), Delegated Certificate Authority (DCA), and Temporary Certificate Authority (TCA).

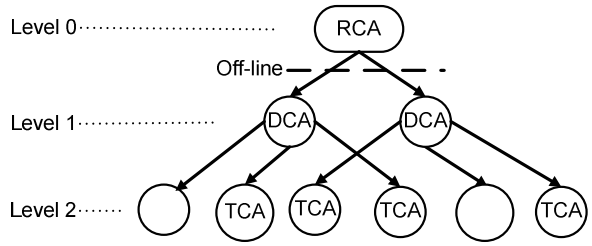

Figure 1. Modified Hierarchical PKI Model.

An RCA node was off-line so that it would be protected from malicious attacks. The dynamic nature of a MANET did not allow it to actively participate in the network, and restricted it from contributing to the management functions of the KMS, such as reissuance. Therefore, the RCA's main function was limited to providing certificates for nodes planning to register into the network. This function was significant because any node that had an RCA certificate could register into the network and serve as a DCA. In this way, RCA certificates promoted minimal pre-configuration of the DCAs at the initial steps of KMS's deployment and facilitated dynamic deployment of additional DCAs during the network lifetime. Moreover, possession of an RCA certificate increased availability for new nodes joining the network by allowing them to temporarily establish SAs with other nodes using that certificate. An RCA certificate was obtained via out-of-band methods.

The KMS was comprised of a number of DCAs in order to increase service availability. We assumed that not all the nodes in a network had the same position or function. The nodes that volunteered to be DCAs had more important positions within the network (e.g., administrators) and were not constrained by battery power or processing capabilities.

The DCAs managed, stored and distributed certificates for the nodes within the network. DCAs issued certificates to nodes after presenting their credentials either via out-of-band or via online connectivity through peer nodes. A new node did not have to physically encounter a DCA because the authentication method was recorded on its certificate. The information served as an initial indicator of trust that could be placed on the certificates during an SA negotiation. This functionality promoted more flexibility because new nodes could establish SAs with peer nodes (at a lower trust level,) until they

physically encountered a DCA and registered using out-of-band methods.

The purpose of TCAs in the KMS was to provide service to new nodes joining the network that had no access to any DCA. In contrast to DCAs, any node in the network could serve as a TCA regardless of their position or reputation (see Section 4) in the network. TCAs signed temporary certificates for physically collocated new nodes to enable them to establish temporary SAs with other network nodes. TCAs authenticated the new nodes using out-of-band methods. The TCAs included their DCA certificate as part of the certificate they issued to a new node. Since each DCA certificate included the behavior grading (see Section 4) of a node, it provided the network nodes with an indication of the trustworthiness of the certificate issuer. By default, a TCA-signed certificate was given a lower trust level than a DCA-signed certificate. The level of trust of a TCA-signed certificate would be translated by other nodes as being equal to or less than that of the TCA that signed the certificate. The short validity period of a TCA certificate motivated nodes to register in the network via a DCA and establish permanent credentials.

3.1. SA establishment

The KMS provided two mechanisms to expedite SA establishment for existing nodes in a partitioned environment: DCAs and Trusted Peers (TPs). An existing network node first queried any of the available DCAs. If all of the DCAs were unavailable due to network partitioning, a node obtained a peer's certificate by contacting the TPs of its peer. This functionality was achieved by having each node store the certificates of the nodes that established an SA with it, thus acting as a repository for the certificates of its TPs. A high number of TPs per node increased the probability that a node could obtain the certificate of its peers. The difference between TPs in our KMS and "friends" in [8] is presented in [10]. Unlike existing network nodes, new nodes could only establish temporary SAs through possession of an RCA or TCA certificate, as described above.

4. Balancing Flexibility and Availability

In order to balance the flexibility and increased availability of the KMS and provide security in the system, we introduced two concepts in addition to revocation: non-repudiation, and behavior grading. Due to space limitations revocation is not presented in this paper (see [10] for more details).

With non-repudiation, the originating nodes signed the transactions of the KMS, providing proof of the origin of each transaction. In addition, transactions were verified by at least two other nodes or DCAs. This verification was important because it prevented any node or DCA from modifying the data transferred and allowed the detection of malicious activity by nodes.

The KMS provided additional security to the system by combining node authentication with an additional element, node behavior. A behavior grading scheme required each node to grade the behavior of other nodes. The KMS recorded and evaluated the behavior of nodes. This information was included in the nodes' certificates and provided credentials to negotiating peers to decide whether they should trust one other. Through this scheme, nodes were not as dependent on strict identity verification since they also had the ability to judge the trustworthiness of a peer node based on its behavior in the network. As a result, the need to reissue or revoke certificates was less frequent. The behavior grading mechanism recorded the nodes' level of trustworthiness using three parameters: positive reputation, negative reputation and complaint counter.

Positive reputation recorded the number of TPs of a node. After an SA was established between two nodes, the two nodes reported the names of their new TP to a DCA, which incremented their positive reputation.

A node's *negative reputation* described the number of peers that no longer trusted a particular node. If a node deemed that its TP was no longer trusted it dissolved the SA with its peer and send a complaint informing the DCA. Once the DCA obtained the complaint from a node, it sent a copy of the complaint and/or updated certificates to both nodes that had an SA. The malicious node no longer had an SA with its peer and was in effect isolating itself by decreasing the number of nodes that trusted it in the network. In addition, the notification sent to the malicious node indicated immediate repercussions by negatively affecting that node's reputation.

The criteria for the decision of trusting or distrusting a peer were addressed in our work in [11]. It was envisioned that this KMS might operate with an Intrusion Detection System (IDS) [6] providing behavior feedback to a node. In [11] we provided a method that a node could use to aggregate feedback from the behavior grading scheme of the KMS and from an IDS in order to produce a reputation index. The node would use that reputation index and decide whether to trust its peer based on its individual security policy. The feedback from the IDS would depend on the type of intrusion detection, such as routing activity.

The *complaint counter* indicated the number of times that a node complained about its TPs, thus

discouraging malicious behavior. The complaint counter was incremented on the certificate of the node that reported the complaint.

In addition to nodes grading their TPs, each DCA graded its peer DCAs. This mechanism provided a *balance of power* among DCAs and increased the security of the system. Malicious activity could occur in the form of incorrectly displayed information and was identified by the lack of proof for the particular action, which changed that information.

5. Simulation

We investigated the performance of this KMS with regards to certificate issuance and acquisition to assess its effectiveness in providing service in a highly partitioned network environment. In addition, we compared certificate issuance in our scheme and in threshold cryptography schemes. Certificate issuance/re-issuance required nodes to communicate directly with any of the available DCAs whereas certificate acquisition was dependent on the existence of DCAs and/or TPs.

This investigation was carried out with a Monte Carlo simulation analysis. This type of analysis is without a time axis. Seven hundred different static network topologies were generated and the connectivity was analyzed based on network parameters, such as radio range and node density. This number of network topologies ensured a 95% confidence interval.

All nodes had the same radio range and all links were bi-directional. The simulation assumed that two nodes could communicate with each other when their radio range was equal or greater to the distance between them. The radio ranges in our analysis were selected between 100-300 meters, and facilitated data collection for both partitioned and connected networks (see Fig. 2). We assumed a fixed area of $1000x1000m^2$ with 40, 80 and 120 nodes. The nodes were uniformly distributed in the network. The percentage of nodes selected to be DCAs or TPs was set to be 10-20%.

The results of interest for our system were:

Availability: the percentage of nodes out of the total nodes in a network that could contact any DCA or TP.

ASPLN: the Average Shortest Path Length between any node in a network and its nearest DCA/TP. ASPLN represented the path length to obtain a service. The shorter the path length, the higher the probability that the node could obtain service in a MANET environment.

The result of interest for threshold cryptography schemes was *PRN/D* (Percentage of Reachable Nodes/DCAs), which indicated the percentage of DCAs that were reachable by a single node during certificate issuance when that node was *not* isolated in the network.

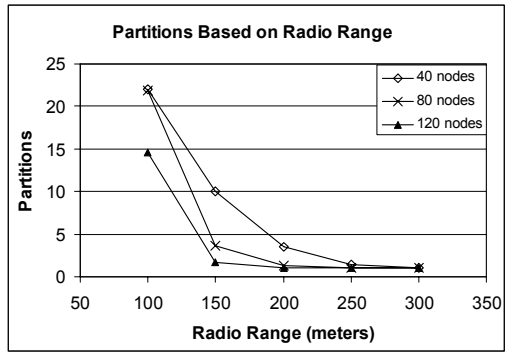

Figure 2. Number of network partitions.

5.1. Certificate Issuance and Acquisition

Fig. 3 depicts the availability of the KMS based on the radio range and, more specifically, its effectiveness in distributing certificates in a partitioned environment. As the number of DCAs increased from 1 DCA to 10% DCAs (of the total number of nodes), they distributed or issued certificates to nodes more effectively. In addition, the existence of 10% of TPs for a node (20% DCAs +TPs) could significantly increase SA establishment as a node could more easily obtain other nodes' certificates, especially in the case where DCAs were unavailable.

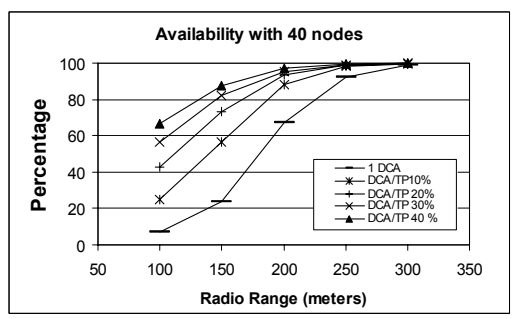

Figure 3. Availability with 40 nodes.

Fig. 4 presents availability from a different perspective by fixing the radio range at 100 meters, which represented a highly partitioned network. The effectiveness of *certificate issuance* can be observed by considering 10-20% out of the combined number of DCAs and TPs shown on the x-axis of the graph. For the case of *certificate acquisition*, the whole range of DCAs and TPs (10-40%) could be considered, since nodes could either obtain certificates from DCAs or

TPs. The relative increase in availability, for the 10%-40% range of DCAs and TPs, was higher for the 40-node network (25-67%) as compared to the relative increase of the 80 (51-85%) and 120-node (79-95%) networks, because the 40-node network was more partitioned.

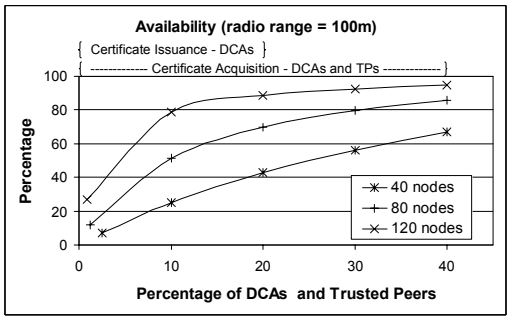

Figure 4. Availability with r=100m.

When using a higher radio range, such as 250m (see Fig. 3), the network became connected and the entire network was encompassed in a single partition. At this radio range, the *Availability* increased to 100% and ASPLN was used to determine the effectiveness in the service availability of the KMS by illustrating the shortest path to a server. Fig. 5-6 demonstrated the variation in the path length depending on the number of DCAs/TPs, and radio range. As the number of DCAs/TPs increased, the path length decreased to a value of one. Overall, the path length varied between 1 and 3 hops, which was relatively low compared to the centralized case (see Fig. 5 - 1 DCA). In addition, within a 3 hop path length it was more likely that a node obtained service from a DCA or TP in a MANET environment.

It is important to notice the hump in the path length in Fig. 6 for the 40-node network, which was caused by the change in connectivity. This variation in path length was non-intuitive because ASPLN did not decrease as the radio range increased but fluctuated due to the existence of network partitions. The reason for this variation was that initially the short radio range partitioned the network into a number of small size partitions (see Fig. 2). Therefore, if a DCA was available in a small partition, the path length to that DCA was short, since it was constrained by the size of the partition. As the connectivity increased, the partition size of the existing partitions increased since nodes joined to form bigger clusters. If a DCA was available in that cluster, then the path length to that DCA was on average longer. As the radio range and the degree of connectivity increased even more, then the ASPLN reached a maximum value (e.g., 190m for 40 nodes), which to some level represented the connectivity at which maximum cluster sizes existed. If nodes used an even higher radio range, clusters started to merge, enabling the nodes to find shorter paths to the DCAs/TPs. As a result, the ASPLN decreased exponentially.

Another significant observation was that this variation for the 40 node network was not similar to the 80 and 120 node networks (see Fig. 6). These networks had higher degrees of connectivity and were at different phases of the path length variation. For example, the path length for the 120 node network was similar to the final stage of the 40 node network (>200m), where ASPLN decreased exponentially.

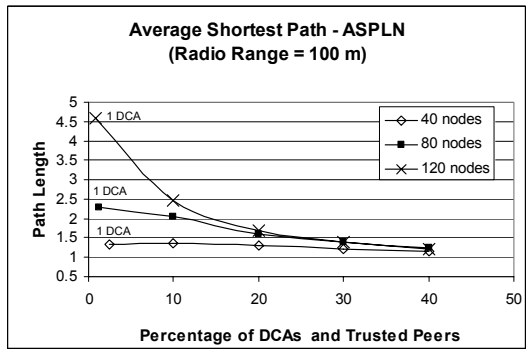

Figure 5. Shortest path to a server.

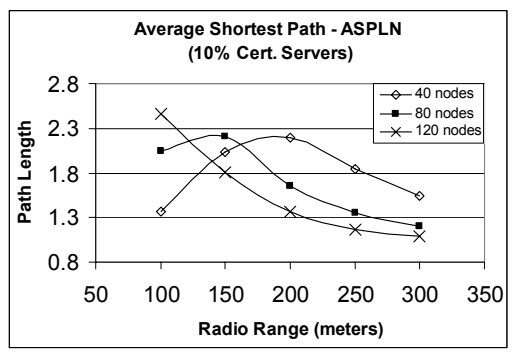

Figure 6. ASPLN for 10% Servers.

5.2. Threshold cryptography schemes

Threshold cryptography schemes lead to less accessibility to DCAs during certificate issuance especially in rapidly deployed partitioned environments. In these schemes, a single node had to contact a percentage of nodes acting as CAs and obtain partial certificates, before it could build its certificate. Fig. 7 demonstrated the ability of a single node to reach a percentage of CAs, when that node was not isolated in the network. For example, for a 40 node network and a radio range of 150 meters a node could only reach 22% of the number of DCAs. If the node had to access 80% of the DCAs in the network to obtain partial certificates then it had to retransmit a

number of times to be able to access a sufficient number of DCAs. In our KMS, access to 22% DCAs almost guaranteed certificate issuance from the first connection attempt to a DCA (assuming 4 DCAs).

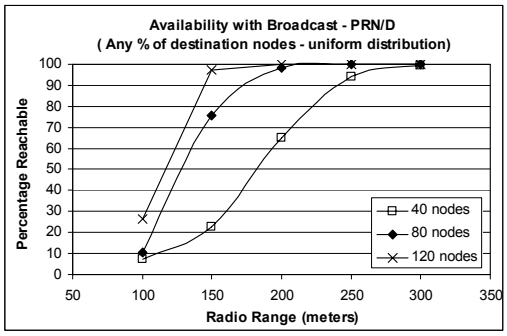

Figure 7. DCAs reached by one node.

6. Conclusion

We have presented a framework for a distributed KMS that increased service availability for highly partitioned networks. Our system integrated a number of components in a unique way to counteract the limitations of previous KMSs. The system utilized a modified hierarchical PKI model consisting of a control plane of RCAs, DCAs, and TCAs (Fig. 1). The RCAs authenticated new nodes and issued them RCA certificates. New nodes could use the RCA certificates to register in the network and serve as DCAs, minimizing pre-configuration. In addition, new nodes could establish temporary SAs in the absence of DCAs, thus introducing more flexibility into the KMS. The DCAs issued, revoked, distributed and managed certificates based on the behavior grading of the nodes and the security policies at the network and node level. The TCAs aided new nodes to join the network by issuing temporary certificates whenever DCAs were unavailable. In addition, the TPs of each node acted as repositories increasing the availability of certificates in a partitioned network.

In addition to revocation [10], security in the KMS was provided via behavior grading and non-repudiation. The behavior grading scheme of the KMS relaxed the need of relying on strict identity verification and allowed nodes to judge other nodes based on their trustworthiness. Trustworthiness was expressed in the form of network-wide SAs between nodes in the entire network. The KMS avoided transitivity of trust because it did not utilize chains of trust. The transactions of the system were recorded in a non-reputable manner and were verified by more than two other nodes, providing balance of power among nodes and DCAs.

Our simulation demonstrated that deploying a number of DCAs and utilizing TPs could significantly increase availability and aid SA establishment in a highly partitioned network environment. In addition, our scheme could provide higher guarantees for issuing certificates to nodes compared to threshold cryptography schemes.

Future work on this research, include investigating the impact of mobility on the KMS functions and ways of extending the KMS to handle complex security policies.

7. References

[1] L. Zhou and Z. Haas, “Securing Ad Hoc Networks,” *IEEE Network*, vol. 13, no. 6, November/December 1999, pp. 24–30.

[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 the 9th International Conference on Network Protocols (ICNP)*, November 2001.

[3] S. Yi, R. Kravets, “MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks,” 2nd Annual PKI Research Workshop Program (PKI 03), Gaithersburg, Maryland, April 2003.

[4] M Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf, “A Cluster-Based Security Architecture for Ad Hoc Networks,” *IEEE INFOCOM*, 2004.

[5] S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, 2003, pp. 52-64.

[6] Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad Hoc Networks,” *Proceedings of the Sixth International Conference on Mobile Computing and Networking (MobiCom 2000),* Boston, MA, August 2000.

[7] J. Douceur, “The Sybil Attack,” *in Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 2002.

[8] S. Capkun, J.-P. Hubaux, and L. Buttyan, "Mobility Helps Security in Ad Hoc Networks," *presented at Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, Maryland, USA, June 2003.

[9] L. DaSilva, S. Midkiff, J. Park, G. Hadjichristofi, K. Phanse, T. Lin, and N. Davis, “Network Mobility and Protocol Interoperability in Ad Hoc Networks,” *IEEE Communications Magazine*, Vol.42, November 2004, pp. 88-96.

[10] G. Hadjichristofi and N. Davis, "Improving the Robustness of Establishing Security Associations for Mobile Ad Hoc Networks" Technical report, http://www.irean.vt.edu/navciiti/, November 30, 2004.

[11] W. Adams, G. Hadjichristofi, and N. Davis, Calculating a Node's Reputation in a Mobile Ad Hoc Network, *Proc. Int'l Performance Computing and Communications Conference,* AZ, April 2005.