Enhanced Security Design for Threshold Cryptography in Ad Hoc Network

Sheng-Ti Li, Xiong Wang

Abstract— **A mobile ad hoc network (MANET) is an autonomous system of mobile nodes. The nodes are free to move arbitrarily. Due to lack of a centralized secure infrastructure, the communication is prone to security attacks and the nodes can be easily compromised. Threshold cryptography proved to be an effective scheme for key management and distribution. However it adds overhead to routing and increases traffic in the network. Furthermore, attacks such as wormhole and Denial of Service (DoS) can compromise routes through spoofing ARP or IP packets, passively or actively. Due to bandwidth constraints and energy conservation, an efficient implementation of the scheme is critical. We present a new approach to facilitate certificate packet delivery and reduce the overhead caused by threshold cryptography. Our experimental simulation indicated good performance of the new approach.**

Keywords— **MANET, threshold cryptography, group signature, security**

I. Introduction

SECURITY problems in MANET in term of authentication have been studied extensively in over two decades. Key management and asymmetric key distribution were evaluated as feasible methods. However, relatively less attention has been dedicated to the security of the routing protocol itself. Zhou and Hass introduced the public key infrastructure (PKI) for MANET [25]. Čapkun, Buttyán and Hubaux proposed a self-constructed certificate without a single trusted third-party [5], [2]. Kong et al. [8] validated threshold cryptography signatures with asymmetric mechanisms. The central component of threshold cryptography is the group signature or the secret sharing protocol, where a signature is divided into 2k+1 pieces and a client seeking authentication needs to receive at least k pieces to construct a valid signature. There are also works evaluating the feasibility of group signature with AODV, an IP-based, on demand routing protocol [23], [6]. One of the characteristics of on demand routing algorithms is the separation of routing discovery and route maintenance. The main task for the routing discovery protocol is to broadcast requests and collect replies. Unfortunately, the broadcast mechanism itself opens a security hole to malicious attacks. The routes and packets in 802.11b can be easy targets. Papadimitratos and Haas presented Secure Routing Protocol (SRP) to combat attacks via a security association between source and destination nodes [19]. Barrière et al. [1] and Fabian Kuhn [9] used geographical based logic to define the whole routing path. Hu, Perrig, and Johnson proposed solutions via time and geography analysis against wormhole attacks [12], [13]. Michiardi, and Molva [17], [18] analyzed spoofing attacks rooted on selfishness of nodes. In this paper, we present a new approach to deal with security problems in routing protocols. We focus on Dynamic Source Routing (DSR) as our test bed for its efficiency [10], rich information in the routing discovery packets, and independency from addressing issues [16], [3]. Our main contributions are in two-fold. First, we propose a geography based routing discovery protocol combined with threshold cryptography. Second, we design a scheme for both secure routing discovery and ARP management that is robust against forged ARP and IP. The rest of the paper is organized as follows. Section II discusses security issues in the implementation of a reliable authentication protocol for MANET. Section III presents our solution against spoofing in secret sharing cryptography with enhanced DSR. Section IV gives an empirical validation of our security design using OPNET Modeler. Section V summarizes our research and concludes the paper.

S. T. Li is with Department of Computer Science California State University at Fullerton (USA) E-mail: shengti@ecs.fullerton.edu.

X. Wang is with Department of Computer Science California State University at Fullerton (USA) E-mail: wang@ecs.fullerton.edu. Contact author.

II. Routing Security and Potential Attacks

Traditional key-based security schemes need to maintain a strong, unbreakable entity, for either symmetry or asymmetry cryptography. However, nodes in MANET have limit energy conservation and they are vulnerable to malicious attacks. An authentication scheme that is based on single trusted third party is not feasible for MANET. PKI with threshold cryptography has been recognized as one of the most effective tools in providing security in MANET [23]. Threshold cryptography is centered on a secret sharing protocol that was developed by Shamir [21]. Similar schemes have been developed extensively in the literature. For example, Zhou and Hass [25] proposed using distributed delegations in MANET. Related concepts were discussed in [26], [4], [11]. Similar to route discover protocol, the group signature protocol locates authorized nodes via broadcasting. A nature of broadcasting is its lack of destination information. In other words, we accept any kind of feedback corresponding to this broadcast request. Some spoofing attacks take advantage of this weakness by forging information or entering the promiscuous mode to receive information. These attacks can be easily achieved via ARP cache poisoning. Some intrusions could be detected by RARP. However, the cost would be too high

for MANET. Moreover, current ad hoc secure routing does not detect whether an access request reaches authorized nodes safely nor does it detect DoS attacks launched at authorized nodes.

III. A Secure Geography Based Routing Protocol

In Shamir's threshold cryptography, the authentication protocol requires a node to receive enough partial signatures from other authenticated nodes to construct a full signature. A node sends out a request for certification (CREQ) and any nodes that receive the request will process this request and send a partial signature back (CREP) if qualified. The original sender collects those CREP to construct a valid full signature if there are enough replies within certain period of time. Similarly, the routing discovery protocol also sends out Route Request Query (RREQ) and collects Route Request Reply (RREP) in various on-demand ad hoc routing discovery protocols. The difference is in the reply mechanism. For RREQ packets, the destination node sends a RREP and the nodes on the reversed route propagate the reply before time expires. In contrast, the CREQ needs to reach multiple nodes to get partial signatures. Thus a qualified node not only replies with a CREP, but also relays the CREQ to other nodes. Various addressing schemes can be used to reach multi nodes, such as multicast address. Nevertheless, the purpose of re-constructing a full signature is to use it as a certificate to request for services from certain destination authorized node. Even if the client seeking services has successfully re-constructed a full signature, it still needs to send out a RREQ to get a route to the destination resource. In essence, a routing discovery begins after the authentication is complete. The routing discovery goes through similar process as the authentication.

A. A Combined Reply Packet for CREP and RREP

Like in [14], [22], [23] we distinguish two types of nodes, one is qualified to sign certificate (*AN*, Authority Node), the other can only send out request for certification (*RN*, Request Node). The challenge for this protocol is to help an *RN* get enough partial signatures from *AN*s. An *RN* sends out CREQ whenever it needs authentication. Before the CREQ timeout, the *RN* keeps listening in order to collect enough partial signatures and in the meantime helps forward other CREQ from other *RN*s. On the other hand, an *AN* listens for CREQs. Once an *AN* receives a CREQ, it checks whether the CREQ is valid. If it is, the *AN* signs its partial signature, sends a CREP to the source and forward the CREQ if the CREQ is not timeout. If the CREQ is not valid or it is timeout, the *AN* simply drops the packet. Assume that the *RN* re-assembles the full signature successfully and attempts to connect to the destination *AN* for services. The *RN* will need to start another broadcast to inject the RREP into the route. The route request is considered redundant since the CREP for certification should have similar information in its packet. The DSR packet doesn't rely on IP-routing overhead in each node but the travel history of each packet to discover the route. Also the routing table in DSR doesn't depend on topology understanding. The *RN* should not need a second flood for routes while its CREP already brings back rich information.

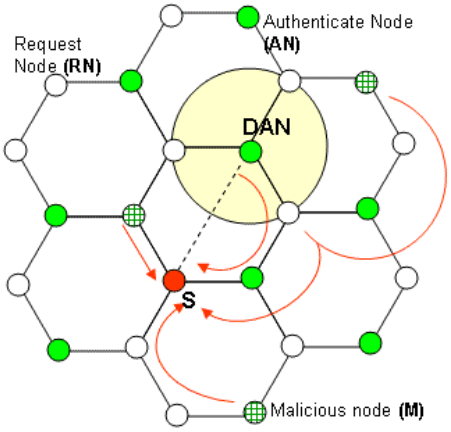

Fig. 1. DoS Attack via ARP Poisoning

B. ARP Poisoning and Broadcast Storm

Key distribution and management can be handled well via the secret sharing scheme, but malicious nodes can still target *RN* or *AN* with DoS. The most serious attack can block *RN* from accessing the destination *AN* even after the *RN* successfully re-constructs a full signature. In a real word example, a missile might fail to fire because the operator had difficulty in finding a communication route to the missile. Unfortunately, those generals who signed their signatures won't be aware of the problem. In ARP poisoning, a particular attack can be launched by sending bogus ARP information about the destination *AN*. As shown in Figure 1, malicious nodes can send out RREP with its MAC address to mislead the source node. The attack might be a wormhole if the attacker only wants to overhear the information, however, it could be a DoS attack by blocking destination node receiving queued packets from the source. Address resolution protocol (ARP) is an essential part as long as IP addressing scheme is still used in 802.11b. The most common way to prevent ARP poisoning is static ARP table for each node. A drawback for this solution is the difficulty of address changing. However, the trade off for this option seems not bad if we can improve performance and security tremendously. The significant improvement of the performance is the elimination of broadcast storm caused by reply messages, as shown in Figure 2. A well-designed static ARP table can still work with changeable IP address and eliminate unnecessary broadcast. For example, we can assign each node with three different IP addresses and use interfaces to rotate the matching channels and addresses. Nevertheless, this would be an optional choice since

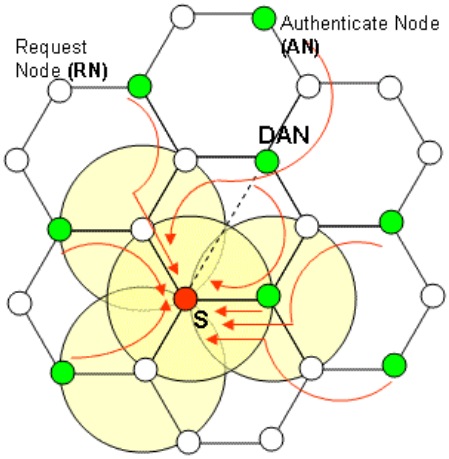

Fig. 2. Reply Broadcast Storm

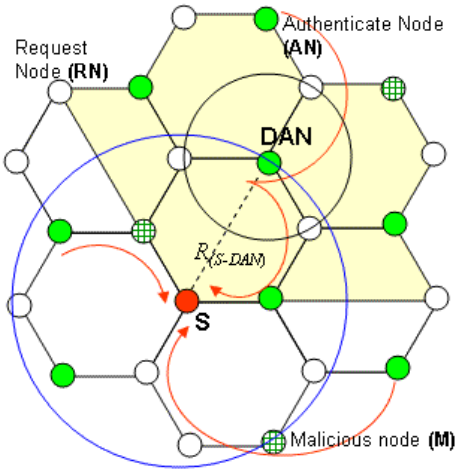

Fig. 3. A Geography Based Filter

not all the existing scenarios can have static ARP table. Another way to reduce broadcast storm is discussed next.

C. A Geography Based Filter

The group signature scheme can only protect the shared secret, not the routing information itself. We purpose a new approach against DoS based on the spatial relation in the request node (R), the destination authorized node (DAN), and other authorized nodes (ANs). In our hybrid discover protocol design, our goal is to protect the route from S to DAN while collecting partial signatures. DAN needs to give up the reply opportunity since DAN itself is the most possible target of attacks. In Figure 1, the malicious node can also corrupt the route by providing forged routing packets from the very beginning. Let $D(n_i, n_j)$ be distance between nodes n_i and n_j. If $D(S, AN)$ is shorter than $D(S, DAN)$ in the same radio propagation range of the source S, an AN will not reply the RREQ message. It can only send back its partial signature or only passes it to the next node. These ANs are also considered high risks because any misbehavior node can fake route replies. To detect malicious nodes in this area, node S wastes unnecessary energy to perform RARP. The protocol only asks DAN to give its signature when RREQ reaches DAN. After DAN signs the RREQ, the packet needs to be passed to other ANs to verify this signature and send RREP back to S. To prevent TCP failure caused by cached routes, we select those routes with DAN information. The qualified reply packets we accept are from nodes replying a route with DAN in the route. This route carries DAN's signature and another AN's authorization. A multilevel trust can be made by setting the number of ANs need to be passed before any AN sends an RREP to the RREQ.

There are other advantages we get from this through spatial relationship. First, the reply ARP broadcast would be limited to certain direction and the cached MAC-IP can be reused. Second, since reply must be returned via DAN, reply time can be more distributed. The route should be formed as bellow:

$$S(n) \rightarrow [RN_i or AN_i] \rightarrow DAN$$

$$\rightarrow [RN_j] \rightarrow AN \rightarrow [(Options)]$$

There are possibilities that other RNs might be in this chain. The propagation radius denoted Pr is the same for every node, including malicious nodes. Each node has three neighbors with equal distance. For mobile adversaries between S and DAN, attacks need to broadcast CREP and RREP to gain responses from other ANs. In Figure 3, the broadcast from the malicious node (M) connecting to S makes no difference from DAN's broadcast. In Figure 4, the intruder needs to compromise an AN to get the partial signature before forging the message. For any node such that $D(S, M)$ is greater than $D(S, DAN)$ and is located in the shaded area, DoS attacks toward DAN will fail because when packets travel to DAN, the packages are considered in a loop and get dropped by DSR algorithm itself. The qualified reply will need

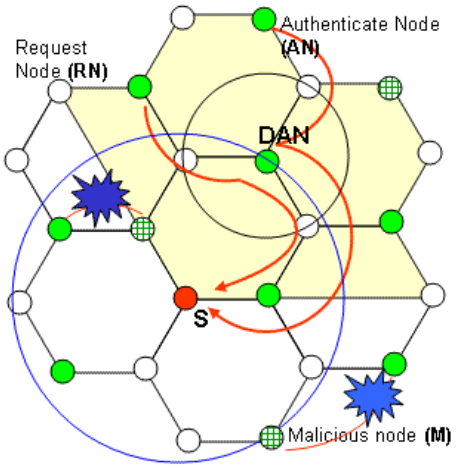

Fig. 4. Geographic Distributed Reply

to perform two tasks: to get DAN's signature and to find at least one more AN after DAN is found. The two-step source routing performs the administrator's job in BSD with LSRR (Loose Source and Record Route) in RFC 791. Compared with reputation based scheme, there is no extra overhead we need to pay. Methods using various multicasting scenarios only reduce the reply broadcast storm but leave more security problems in DoS for weakening the broadcast randomness. Malicious nodes can still attack in this scheme. However, the attacks would become passive. In other words, it depends on the next replied AN. Another method to compromise group signature is to attack other ANs to cause single reply failure. Due to fault tolerance in threshold cryptography, the attack only affects the success of the request when enough ANs fail to reply. Our design also prevents wormhole attack between R and DAN, since no reply messages will be directly accept between them if the mobile adversary performs the same routing algorithm.

IV. Evaluation

We propose a hybrid threshold signature scheme along with a geography based filter. The model we design considers different speeds and ARP cache sizes. Our simulation uses OPNET Modeler 10.0. MANET module. We modified the DSR module to implement our geography based filter, the hybrid route discovery, and group signature protocol. All simulations have 60 MANET nodes, 20 of which are ANs, the rest are RNs, in a 400m square area. Each RN attempts to connect to a specific DAN with partial signatures gathering from ANs in the area for average 60 seconds, observing Poisson distribution. The total simulation time for each scenario is 900 seconds. We define a successful request as a TCP remote access with enough partial signatures, in this case, more than 7 signatures. The Successful Request Rate (SRR) is defined as bellow:

$$SuccessfulRequestRate = \frac{\#ofSuccessfulRequests}{Total\#ofRequests}$$

A. ARP Cache

We conducted experiments to evaluate performance of fixed and mobile nodes with different ARP cache sizes. We found that ARP cache is still helpful in MANET. Another performance comparison was done using pre-define static ARP table to improve successful request rate. The static ARP table records IP-MAC address mapping before the simulation starts to send request packets. Nodes can load partial tables into memory depending on the cache size. We found that without the static ARP table the successful request rate drops down dramatically. The most significant improvement was observed when nodes act dynamically. We believe that ARP doesn't impact performance much for most fixed node scenario because of the fixed geographical relationship. Table I lists the parameter settings in the experiments. Table II lists the successful request rate in different settings. In all experiments, the data rate was fixed at 1 Mbps. In the mobile cases, the speed was set to 20 m/s.

Scenario	RN	AN	ARP	Rate	Speed
ARP1	40	20	1	1	0
ARP10	40	20	10	1	0
ARP25	40	20	25	1	0
ARP40	40	20	40	1	0
Mobile Arp1	40	20	1	1	0
Mobile Arp10	40	20	10	1	20
Mobile Arp25	40	20	25	1	20
Mobile Arp40	40	20	40	1	20
No Static Arp	40	20	25	1	20

TABLE I
Parameters for ARP Experiments.

	ARP1	ARP10	ARP25	ARP40
Fixed	88.97	93.79	85.76	86.03
Mobile	90.86	91.03	94.66	95.54
No Static	N/A	N/A	38.77	N/A

TABLE II
Successful Request Rate.

B. Speed

To evaluate the performance of dynamic movement, we added mobility for nodes in the scenarios. Five different speeds are compared in our simulation, namely 0, 1, 5, 10, and 20 m/s. It was observed that, compared with other ground speeds including 0, the successful request rate didn't drop much when the moving speed went up nor did the received CREP rate. The topology changes as nodes move around but it has no impact on the protocol. The results in table 4.4 show that although we exclude certain replies through geography based filter, the group signature protocol still performs robustly. Due to the nature of DSR and radio propagation, the packet records DAN and AN by time only. A route may still have very good chance to reach the DAN and successfully set up the TCP connection. Table III lists the parameter settings in the speed experiments and the successful request rates (SRR) in different settings.

Scenario	RN	AN	ARP	Speed	SRR
Speed0	40	20	1	0	91.72
Speed1	40	20	1	1	91.21
Speed5	40	20	1	5	91.92
Speed10	40	20	1	10	91.55
Speed20	40	20	1	20	90.86

TABLE III
Parameters and SRR for Speed Experiments.

V. Conclusion

The group signature authentication protocol is designed to make communication in MANET securer and can be implemented with various on demand routing protocols. One drawback for the secret sharing scheme is that too many entities communicate the secret at the same time. Previous works proposed various flooding mechanisms, such as multicasting, to reduce the reply storm. However, simply reduce reply entities might results in security issues such as DoS attacks targeting a specific group of nodes. Also, neither threshold scheme nor the routing protocol can prevent DoS attacks from compromising the route to DAN. If we fail to access DAN, the service request would still fail even after the certificate request succeeds. The advantage of using the geography based filter is that both the reply storm from neighbors and potential DoS attacks are stopped. So far, since IP is still the major address scheme in 802.11b, there is no way we can avoid ARP cache poisoning. We suggest that MANET nodes should use static ARP table design to reduce the risk and to take advantage of the efficiency, especially with mobile nodes. The limitation of IP address changing is considered reasonable since MANET is used for special purpose most of the time. In this paper, we use Modeler to evaluate our security design. The authenticate handshaking is integrated with the threshold signature scheme by creating a delegation. Our simulation provides a feasible framework to develop a prototype for securing MANET with geography based routing. Figure 5 summarizes the impact of different settings on the successful request rate. The number of RNs was fixed at 40 and the number of ANs was fixed at 20. The data rate was fixed at 1 Mbps. More works need to be done for implementing the proposed approach with various routing protocols.

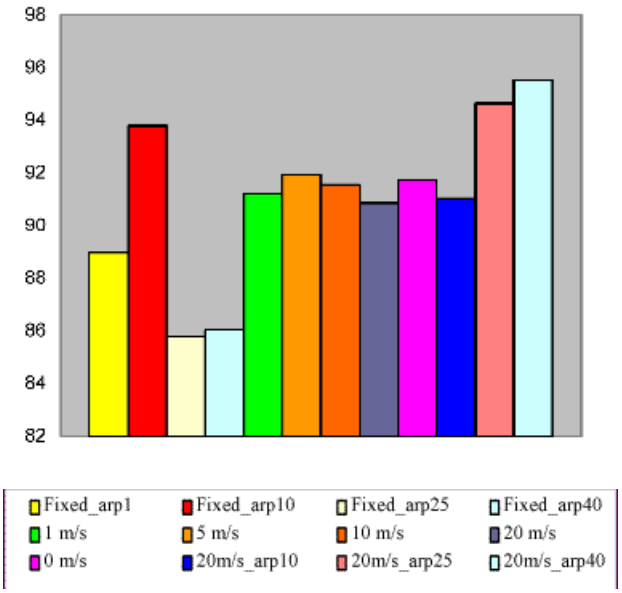

Fig. 5. Successful Request Rate for the Scenarios with 20 ANs

References

[1] L. Barrière, P. Fraigniaud, L. N. J. Opatrny, "Robust position-based routing in wireless ad-hoc networks with unstable transmission ranges," *Proceedings of the 5th international workshop on Discrete algorithms and methods for mobile computing and communications*, Rome, Italy, 2001

[2] L. Buttyán and J. P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," to appear in *ACM/Kluwer Mobile Networks and Applications (MONET)*, Vol. 8 No. 5, October 2003.

[3] J. Broch, D. A. Maltz, D. B. Johnson, Y-C. Hu, J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," *MOBICOM 1998*, 85-97.

[4] Y.-S. Chen, "Wireless Public Key Infrastructure (WPKI) Technical Standards," *NETSEC 2000 Conference*, Taiwan.

[5] S. Čapkun, L. Buttyán and J. P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *ACM International Workshop on Wireless Security*, 2002.

[6] C. Carter, S. Yi, and R. Kravets, "ARP Considered Harmful: Manycast Transactions in Ad Hoc Networks," IEEE WCNC 2003.

[7] E. Cole, *Hackers Beware: The Ultimate Guide to Network Security*, 1st edition, August 13, 2001, Que.

[8] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Wireless Mobile Networks," *ICNP*, pages 251–260, 2001.

[9] F. Kuhn, R. Wattenhofer, Y. Zhang, A. Zollinger, "Geometric Ad-Hoc Routing: Of Theory and Practice," *Twenty-Second ACM Symposium on Principles of Distributed Computing (PODC 2003)*, July 13-16, 2003, Boston.

[10] L. M. Feeney, "An Energy-consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks," *Proceedings of the 45th IETF Meeting: MANET Working Group*, Oslo, Norway, July, 1999.

[11] M. Gasser and E. McDermott, "An architecture for practical delegation in a distributed system," *Proceedings of the 1990 IEEE Symposium on Security and Privacy*, pp. 20-30, Oakland, CA, May 1990.

[12] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *The 8th ACM International Conference on Mobile Computing and Networking*, September 2002

[13] Y-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," *IEEE INFOCOM 2003.*

[14] C. Ho, K. Obraczka, G. Tsudik, and K. Viswanath, "Flooding for Reliable Multicast in Multi-Hop Ad Hoc Networks," *Wireless Networks (WINET 2001).*

[15] G. Holland, N. H. Vaidya, "Analysis of TCP Performance over Mobile Ad Hoc Networks," *MOBICOM 1999*, 219-230.

[16] D. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing (T. Imielinski and H. Korth, eds.)*, Kluwere Academic Publishers, 1996.

[17] P. Michiardi and R. Molva, "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks," *European Wireless Conference*, 2002.

[18] P. Michiardi and R. Molva, "Ad hoc network security," *ST Journal of System Research*, Volume 4, N1, March 2003.

[19] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad Hoc Networks," *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, San Antonio, TX, January 27-31, 2002.

[20] R. Stevens, *The Protocols (TCP/IP Illustrated, Volume 1)*, 1st edition , January 1994, Addison-Wesley Pub Co.

[21] A. Shamir, "How to Share a Secret," *CACM*, 22(11): 612-613, 1979.

[22] K. Viswanath and K. Obraczka, "An Adaptive Approach to Group Communications in Multi-Hop Ad hoc Networks," *International Conference on Networking (ICN 2002).*

[23] S. Yi and R. Kravets, "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks," *The 2nd Annual PKI Research Workshop (PKI 03).*

[24] S. William, *Cryptography and Network Security: Principles and Practice*, 3rd edition, 2003, Prentice-Hall.

[25] L. Zhou and J. Z. Haas, "Securing Ad Hoc Networks," *IEEE Network Magazine*, vol. 13, no.6, 1999.

[26] L. Zhou S. B. Fred, and R. van Renesse, "COCA: A Secure Distributed Online Certification Authority," *ACM Transactions on Computer Systems*, (20)4:329-368, November 2002.