Modern Techniques for Securing AdHoc Networks

[1]Anusha Shetty [2] Weerdhaval Chowgule
[1][2]-Student,VTU,Belagavi
[1] anushashetty814@gmail.com[2] weerdhaval.chowgule2@gmail.com

***Abstract*- Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we study the threats an ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, we take advantage of the inherent redundancy in ad hoc networks multiple routes between nodes to defend routing against denial of service attacks. We also use replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which forms the core of our security framework.**

I.INTRODUCTION

Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Figure 1 shows such an example: initially, nodes A and D have a direct link between them. When D moves out of A's radio range, the link is broken. However, the network is still connected, because A can reach D through C, E, and F. Military tactical operations are still the main application of ad hoc networks today. For example, military units (e.g., soldiers, tanks, or planes), equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms. Security is an important issue for ad hoc networks, especially for those security-sensitive applications. To secure an ad hoc network, we consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation .

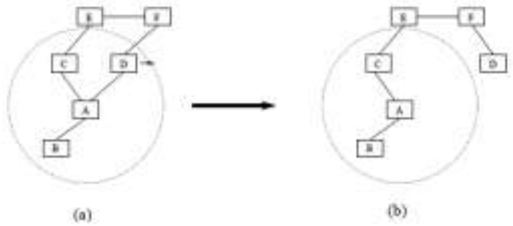

Figure 1: (a). When node D moves out of the radio range of A, the network topology changes to the one in (b).

Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework. Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield. Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.

Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Finally, non-repudiation ensures that the origin of a message cannot deny having sent the message. Nonrepudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised. There are other security goals (e.g., authorization) that are of concern to certain applications, but we will not pursue these issues in this paper.

The salient features of ad hoc networks pose both challenges and opportunities in achieving these security goals.First, use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. Secondly, nodes, roaming in a hostile environment (e.g., a battlefield) with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, we should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within the network by compromised nodes. Therefore, to achieve high survivability, ad hoc networks should have a distributed architecture with no central entities. Introducing any central entity into our security solution could lead to significant vulnerability; that is, if this centralized entity is compromised, then the entire network is subverted. Thirdly, an ad hoc network is dynamic because of frequent changes in both its topology and its membership (i.e., nodes frequently join and leave the network). Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromised. Unlike other wireless mobile networks, such as mobile IP [21, 24, 31], nodes in an ad hoc network may dynamically become affiliated with administrative domains. Any security solution with a static configuration would not suffice. It is desirable for our security mechanisms to adapt on-the-fly to these changes. Finally, an ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

II.SECURE ROUTING

To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. Routing protocols [30, 25, 32, 16, 23] proposed for ad hoc networks cope well with the dynamically changing topology. However, none of them, to our knowledge, have accommodated mechanisms to defend against malicious attacks. Routing protocols for ad hoc networks are still under active research. There is no single standard routing protocol. Therefore, we aim to capture the common security threats and to provide guidelines to secure routing protocols. In most routing protocols, routers exchange information on the topology of the network in order to establish routes between nodes. Such information could become a target for malicious adversaries who intend to bring the network down. There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce excessive traffic load into the network by causing retransmission and inefficient routing. The second and also the more severe kind of threats comes from compromised nodes, which might advertise incorrect routing information to other nodes. Detection of such incorrect information is difficult: merely requiring routing information to be signed by each node would not work, because compromised nodes are able to generate valid signatures using their private keys. Diversity coding [1] takes advantage of multiple paths in an efficient way without message retransmission. The basic idea is to transmit redundant information through additional routes for error detection and correction. For example, if there are n disjoint routes between two nodes, then we can use n−r channels to transmit data and use the other r channels to transmit redundant information. Even if certain routes are compromised, the receiver may still be able to validate messages and to recover messages from errors using the redundant information from the additional r channels.

III.KEY MANAGEMENT SERVICE

We employ cryptographic schemes, such as digital signatures, to protect both routing information and data traffic. Use of such schemes usually requires a key management service.We adopt a public key infrastructure because of its superiority in distributing keys and in achieving integrity and non-repudiation. Efficient secret key schemes are used to secure further communication after nodes authenticate each other and establish a shared secret session key. In a public key infrastructure, each node has a public/private key pair. Public keys can be distributed to other nodes, while private keys should be kept confidential to individual nodes. There is a trusted entity called

Certification Authority (CA) [11, 17, 26] for key management. The CA has a public/private key pair, with its public key known to every node, and signs certificates binding public keys to nodes.The trusted CA has to stay on-line to reflect the current bindings, because the bindings could change over time: a public key should be revoked if the owner node is no longer trusted or is out of the network; a node may refresh its key pair periodically to reduce the chance of a successful brute-force attack on its private key.

A.System model

Our key management service is applicable to an asynchronous ad hoc network; that is, a network with no bound on message-delivery and message-processing times. We also assume that the underlying network layer provides reliable linksi. The service, as a whole, has a public/private key pair. All nodes in the system know the public key of the service and trust any certificates signed using the corresponding private key. Nodes, as clients, can submit query requests to get other clients' public keys or submit update requests to change their own public keys.

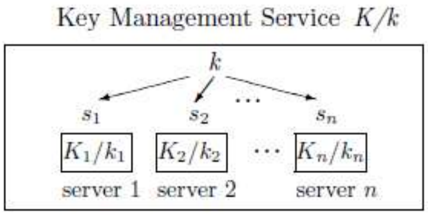

Figure 2:The service, as a whole, has a public/private key pair K/k. The public key K is known to all nodes in the network, whereas the private key k is divided into n shares s1, s2, . . . , sn, one share for each server. Each server i also has a public/private key pair Ki/ki and knows the public keys of all nodes.

Internally, our key management service, with an (n, t+1) configuration (n, 3t+1), consists of n special nodes, which we call servers, present within an ad hoc network. Each server also has its own key pair and stores the public keys of all the nodes in the network. In particular, each server knows the public keys of other servers. Thus, servers can establish secure links among them. We assume that the adversary can compromise up to t servers in any period of time with a certain duration. If a server is compromised, then the adversary has access to all the secret information stored on the server. A compromised server might be unavailable or exhibit Byzantine behavior (i.e., it can deviate arbitrarily from its protocols). We also assume that the adversary lacks the computational power to break the cryptographic schemes we employ

A.Threshold cryptography

Distribution of trust in our key management service is accomplished using threshold cryptography [4, 3]. An (n, t + 1) threshold cryptography scheme allows n parties to share the ability to perform a cryptographic operation (e.g., creating a digital signature), so that any t + 1 parties can perform this operation jointly, whereas it is infeasible for at most t parties to do so, even by collusion. When applying threshold cryptography, we must defend against compromised servers. For example, a compromised server could generate an incorrect partial signature. Use of this partial signature would yield an invalid signature. Fortunately, a combiner can verify the validity of a computed signature using the service public key. In case verification fails, the combiner tries another set of t + 1 partial signatures. This process

continues until the combiner constructs the correct signature from t + 1 correct partial signatures. More efficient robust combining schemes are proposed [13, 12]. These schemes exploit the inherent redundancies in the partial signatures (note that any t+1 correct partial signatures contain all the information of the final signature) and use error correction codes to mask incorrect partial signatures. In [13], a robust threshold DSS (Digital Signature Standard) scheme is proposed. The process of computing a signature from partial signatures is essentially an interpolation. The authors uses the Berlekamp and Welch decoder, so that the interpolation still yields a correct signature despite a small portion (fewer than one fourth) of partial signatures being missing or incorrect

IV.RELATED WORK

Secure routing in networks such as the Internet has been extensively studied [36, 27, 30, 45, 46, 18]. Many proposed approaches are also applicable to secure routing in ad hoc networks. To deal with external attacks, standard schemes such as digital signatures to protect information authenticity and integrity have been considered. For example, Sirios and Kent [45] propose the use of a keyed one-way hash function with windowed sequence number for data integrity in point-to-point communication and the use of digital signatures to protect messages sent to multiple destinations. Perlman [26] studies how to protect routing information from compromised routers in the context of Byzantine robustness. The study analyzes the theoretical feasibility of maintaining network connectivity under such assumptions. Kumar [27] recognizes the problem of compromised routers as a hard problem, but provides no solution. Other works [30, 25, 26] give only partial solutions. The basic idea underlying these solutions is to detect inconsistency using redundant information and to isolate compromised routers. For example, in [26], where methods to secure distance-vector routing protocols are proposed, extra information of a predecessor in a path to a destination is added into each entry in the routing table. Using this piece of information, a path-traversal technique (by following the predecessor link) can be used to verify the correctness of a path. Such mechanisms usually come with a high cost and are avoided because routers on networks such as the Internet are usually well protected and rarely compromised. In authentication architecture for mobile ad hoc networks is proposed. The proposed scheme details the formats of messages, together with protocols that achieve authentication. The architecture can accommodate different authentication schemes. Our key management service is a prerequisite for such a security Architecture

V.CONCLUSION

In this paper, we have analyzed the security threats an ad hoc network faces and presented the security objectives that need to be achieved. On one hand, the security-sensitive applications of ad hoc networks require high degree of security; on the other hand, ad hoc networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad hoc networks. The idiosyncrasy of adhoc networks poses both challenges and opportunities for these mechanisms.This paper focuses on how to secure routing and how to establish a secure key management service in an ad hoc networking environment. These two issues are essential to achieving our security goals. Besides the standard security mechanisms, we take advantage of the redundancies in ad hoc network topology and use diversity coding on multiple routes to tolerate both benign and Byzantine failures. To build a highly available and highly secure key management service, we propose to use threshold cryptography to distribute trust among a set of servers. Furthermore, our key management service employs share refreshing to achieve proactive security and to adapt to changes in the network in a scalable way. Finally, by relaxing the consistency requirement on theservers, our service does not rely on synchrony assumptions. Such assumptions could lead to vulnerability. A prototype of the key management service has been implemented, which shows its feasibility.The paper represents the first step of our research to analyze the security threats, to understand the security requirements for ad hoc networks, and to identify existing techniques, as well as to propose new mechanisms to secure ad hoc networks. More work needs to be done to deploy these security mechanisms in an ad hoc network and to investigate the impact of these security mechanisms on the network performance

ACKNOWLEDGMENT

I Would Like To Take This Opportunity To Express My Deep Sense Of Gratitude To My Parents For Their Valuable Inspiration And Guidance Without Which The Proposed Work Would Not Have Progressed To Its Present State.

REFERENCES

E. Ayanoglu, C.-L. I, R. D. Gitlin, and J. E. Mazo. Diversity coding for transparent self-healing and fault-tolerant communication networks. IEEE Transactions on Communications, 41(11):1677–1686,November 1993.

[2] M. Castro and B. Liskov. Practical Byzantine fault tolerance. In Proceedings of the 3rd USENIX Symposium on Operating System Design and Implementation (OSDI'99), pages 173–186, New Orleans, LA USA, February 22–25, 1999. USENIX Association, IEEE TCOS, and ACM SIGOPS.

[3] Y. Desmedt. Threshold cryptography. European Transactions on Telecommunications, 5(4):449–457, July–August 1994.

[4] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In G. Brassard, editor, Advances in Cryptology Crypto'89, the 9th Annual International Cryptology Conference, Santa Barbara, CA USA, August 20–24,1989, Proceedings, volume 435 of Lecture Notes in Computer Science, pages 307–315. Springer, 1990.

[5] Y. Desmedt and S. Jajodia. Redistributing secret shares to new access structures and its applications. Technical Report ISSE TR-97-01, George Mason University, July 1997.

[6] A. Ephremides, J. E. Wieselthier, and D. J. Baker. A design concept for reliable mobile radio networks with frequency hopping signaling. Proceedings of the IEEE, 75(1):56–73, January 1987.

[7] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In Proceedings of the 28th Annual

Symposium on the Foundations of Computer Science, pages 427–437. IEEE, October 12–14,1987.

[8] M. J. Fischer, N. A. Lynch, and M. S. Peterson. Impossibility of distributed consensus with one faulty processor. Journal of the ACM, 32(2):374–382, April 1985.

[9] Y. Frankel, P. Gemmel, P. MacKenzie, and M. Yung. Optimal resilience proactive public-key cryptosystems. In Proceedings of the 38th Symposium on Foundations of Computer Science, pages 384–393,Miami Beach, FL USA, October 20–22, 1997. IEEE.

[10] Y. Frankel, P. Gemmell, P. MacKenzie, and M. Yung. Proactive RSA. In B. S. Kaliski Jr., editor,Advances in Cryptology Crypto'97, the 17th Annual International Cryptology Conference, Santa Barbara,CA USA, August 17–21, 1997, Proceedings, volume 1294 of Lecture Notes in Computer Science, pages 440–454. Springer, 1997.

[11] M. Gasser, A. Goldstein, C. Kaufman, and B. Lampson. The digital distributed systems security architecture.In Proceedings of the 12th National Computer Security Conference, pages 305–319, Baltimore,MD USA, October 10–13, 1989. National Institute of Standards and Technology (NIST), National Computer Security Center (NCSC).

[12] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust and efficient sharing of RSA functions. In N. Koblitz, editor, Advances in Cryptology—Crypto'96, the 16th Annual International Cryptology Conference, Santa Barbara, CA USA, August 18–22, 1996, Proceedings, volume 1109 of Lecture Notes in Computer Science, pages 157–172. Springer, 1996.

[13] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust threshold DSS signatures. In U. M. Maurer, editor, Advances in Cryptology—Eurocrypt'96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12–16, 1996, Proceedings, volume 1233 of Lecture

Notes in Computer Science, pages 354–371. Springer, 1996.

[14] L. Gong. Increasing availability and security of an authentication service. IEEE Journal on Selected Areas in Communications, 11(5):657–662, June 1993.

[15] Z. J. Haas and B. Liang. Ad hoc mobility management using quorum systems. IEEE/ACM Transactions on Networking, 1999.

[16] Z. J. Haas and M. Perlman. The performance of query control schemes for zone routing protocol. In SIGCOMM'98, June 1998.

[17] A. A. Hassan, W. E. Stark, and J. E. Hershey. Frequency-hopped spread spectrum in the presence of a flower partial-band jammer. Transactions on Communications, 41(7):1125–1131, July 1993.

[18] R. Hauser, T. Przygienda, and G. Tsudik. Lowering security overhead in link state routing. Computer Networks, 31(8):885–894, April 1999.

[19] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. Proactive public-key and signature schemes. In Proceedings of the 4th Annual Conference on Computer Communications Security, pages 100–110, Zurich, Switzerland, April 1–4, 1997. ACM.

[20] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: How to cope with perpetual leakage. In D. Coppersmith, editor, Advances in Cryptology—Crypto'95, the 15th Annual International Cryptology Conference, Santa Barbara, CA USA, August 27–31, 1995, Proceedings, volume 963 of Lecture Notes in Computer Science, pages 457–469. Springer, 1995.

[21] J. Ioannidis, D. Duchamp, and J. M. Gerald Q. IP based protocols for mobile internetworking. ACM SIGCOMM Computer Communication Review (SIGCOMM'91), 21(4):235–245, September 1991.

[22] S. Jacobs and M. S. Corson. MANET authentication architecture. Internet Draft (draft-jacobs-imepauth- arch-01.txt), February 1999.

[23] P. Jacquet, P. Muhlethaler, and A. Qayyum. Optimized link state routing protocol. IETF MANET,Internet Draft, November 1998.

[24] S. Jarecki. Proactive secret sharing and public key cryptosystems. Master's thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA USA, September 1995.

[25] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad-hoc wireless networks. Mobile Computing, 1996.

[26] C. Kaufman. DASS: Distributed authentication security service. Request for Comments 1507, September 1993.

[27] B. Kumar. Integration of security in network routing protocols. SIGSAC Reviews, 11(2):18–25, 1993.

[28] D. Malkhi and M. Reiter. Byzantine quorum systems. Distributed Computing, 11(4):203–213, 1998.

[29] D. Malkhi and M. Reiter. Secure and scalable replication in Phalanx. In Proceedings of the 17th Symposium on Reliable Distributed Systems, pages 51–58, West Lafayette, IN USA, October 20–22, 1998. IEEE Computer Society.