# Mobile Ad Hoc Networks Security

G.V.S. Raju
*Peter T. Flawn Professor*
University of Texas at San Antonio
*Life Fellow*
Institute for Electrical and Electronics Engineers

Rehan Akbani
*Ph.D. Student*
University of Texas at San Antonio

### *Abstract*

This paper is concerned with security in mobile ad hoc networks (MANETs). MANETs have unique characteristics and constraints that make traditional approaches to security inadequate. In particular, it is not appropriate to assume preexisting shared secret keys or authentication among members. The lack of an infrastructure exacerbates the situation. Therefore the issues of authentication, key distribution, and intrusion detection require different methods, which are discussed in this paper.

Traditional authentication, key distribution, and intrusion-detection methods are often too inefficient to be used in resource-constrained devices in MANETs. We propose to combine efficient techniques from elliptic curve cryptography (ECC) and a distributed intrusion-detection system (IDS) based on threshold cryptography. We also propose to use a distributed certifying authority (CA) along with per-packet and per-hop authentication for addressing the issues mentioned above. The model assumes that no single node can be trusted and relies instead on a distributed trust model.

### *I. Introduction*

MANETs consist of mobile nodes interconnected by multihop communications paths or radio links. A MANET consists of mobile platforms, known as nodes, which are free to move at any speed in any direction and organize themselves randomly. The nodes in the network function as routers, clients, and servers. These nodes are constrained in power consumption, bandwidth, and computational power. MANETs lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks. Wireless links make MANETs more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. It is also easier for them to enter or leave a wireless network because no physical connection is required. They can also directly attack the network to delete messages, inject false packets, or impersonate a node. This violates the network's goals of availability, integrity, authentication, and nonrepudiation. Compromised nodes can also launch attacks from within a network. Most proposed routing algorithms today do not specify schemes to protect against such attacks. This paper gives methods that are pertinent for authentication, key distribution, intrusion detection, and rerouting in case of Byzantine failures in MANETs. We include in this paper past, current, and future directions of research in these areas.

### *II. State of the Art*

MANET security involves authentication, key establishment and distribution, and encryption. Routing protocols in [10,13,14] assume preexistence and presharing of public and secret keys for all initial members. These protocols neglect key exchange and authentication, which are very important in MANETs. Recently Zhou and Haas [12] introduced the idea of distributing a CA throughout the network, in a threshold fashion, at the time of network formation. This CA would allow trust relations to be created in the network while also being resilient to some intrusions, malicious insiders, and breaks in connectivity. In [12], however, the resource limitations of devices in ad hoc networks are not addressed. Because public key and threshold cryptography are computationally expensive and require large memory, this method does not meet these resource limitations. Khalili, Katz, and Arbaugh [8] extended this technique to reduce the resources needed by using an ID–based system. Luo et al. [7] developed scalable, distributed authentication services in ad hoc networks. In their approach, multiple nodes collaboratively provide authentication services for any node in the network. In [6], Desmedt gives recent research aspects of threshold cryptography. In this paper, we extend these techniques to provide an integrated scheme to address the security issues mentioned earlier.

### *III. Proposed Scheme Outline*

We outline in this section approaches to key exchange, authentication, and intrusion detection. For key exchange,

we propose to use ECC. We have done considerable work in MANETs [9,10,11] in the area of routing with minimum delay and maximum available bandwidth. We have worked with network security in the past [11,15] and investigated use and effectiveness of utilizing ECC. We have already developed our own software that implements ECC [15], and it runs on different devices and platforms. Our study shows that ECC can be used effectively in MANETs because of their lower resource requirements. We also reviewed earlier methods of IDS originally proposed by [12] and propose new software methods. Key exchange, authentication, and intrusion detection methods are described in detail in sections V, VI, VII, respectively.

## *IV. Threshold Cryptography*

Often, the sender/receiver is an organization. The goal of threshold cryptography (TC) is to split a cryptographic operation among multiple users so that some predetermined number of users can perform the desired (cryptographic) operation. In organizations, many security-related actions are taken by a group of people instead of an individual so there is a need for guaranteeing the authenticity of messages sent by a group of individuals to another group without expansion of keys and/or messages. To avoid a key management problem and to allow distribution of power, an organization should have one public key. The power to sign should then be shared, to avoid abuse and to guarantee reliability. The goal of TC is to make this possible. The basic idea is as follows: a cryptofunction $g$ is homomorphic, i.e.,

$$g_b(k_1 + k_2) = g_b(k_1) * g_b(k_2)$$

where b is the input message, and $k_1$, $k_2$ belong to keyspace, $k = k_1 + k_2$.

Both RSA and ECC are homomorphic. Therefore, threshold cryptography is applicable and cryptographic operations can be split among multiple users such that any subset comprising of $t$ users can perform the desired operation, where $t$ is a predefined number. In a $t$ out of $n$ scheme, any set of $t$ users can perform the desired operation, while any set of ($t$-1) users or less cannot. A cryptographic scheme based on threshold cryptography is secure against an attacker as long as the attacker compromises no more than ($t$-1) nodes.

## *V. Decentralized Authentication of New Nodes*

In the scheme designated by Luo, Zerfos, Kong, Lu, and Zhang [7], two nodes authenticate each other using signed unforgeable certificates issued by a virtual trusted CA. Multiple nodes will function collectively as a CA. Authority and functionality of an authentication server is distributed across $k$ nodes that collaboratively serve and provide authentication services. A central CA is not reasonable in MANET architectures because they are vulnerable as a single point of compromise and/or failure.

A local trust model is necessary in order to perform any type of authentication services. A user is considered trusted if any $k$ trusted entities claim so within a fixed time period. These $k$ entities are usually among the user's one-hop neighbors. $K$ may be either a globally set parameter or may be a function of location (i.e., majority of each node's neighboring nodes).

All authenticated nodes carry a certificate signed with the network secret key (SK). Authenticated nodes help each other forward and route packets, while unauthenticated nodes are denied access to network resources. Authenticated nodes also perform network monitoring for suspicious activity from their neighbors. The mechanisms to monitor and detect misbehavior are defined at the individual node. When a node attempts to renew its certificate, it sends a request to its neighboring nodes. If the neighbor node's records show that the requesting node is well behaved and that the node is not presently on the certificate revocation list (CRL), the node returns a partial certificate by applying its share of SK. The CRL contains a list including ID of misbehaving nodes and a list of their accusers. If a user determines that a node is misbehaving, the accuser directly flags the misbehaving node as convicted in the CRL, and the accuser floods its neighbors with a signed accusation of that node. When a node receives a signed accusation of a node, they first check to see if the accuser is a revoked user. If so, the accusation is dropped. If the accusation is valid, the user updates their CRL by adding the accuser to the accused node. If a node contains less than $k$ accusers, that node is flagged as suspect. If the node passes the threshold of accusers, then it is flagged convicted.

Lou et al. use RSA for authentication. We propose below authentication based on ECC cryptography because it suits MANETs due to small key sizes. The secrecy of the master secret key lies within the $k$ threshold polynomial sharing mechanism. By threshold secret sharing, the master secret key is shared among network nodes. Each node, $node_i$, holds a secret share, and any number of such secret share holders function collectively as a CA. Besides the system key pair, we propose that each node holds a personal ECC key pair $\{_{ni}, P_{xi,yi}\}$. To certify its personal keys each node holds a certificate in the form $< node_i , P_{xi,yi} >$. The certificate is valid only if it is signed by the system's secret key.

## *VI. Per-Packet and Per-Hop Authentication*

In our scheme, a new node has to be initially authenticated by each of its neighbors to join the network as mentioned in section V. Once that has been accomplished, each packet sent out by the node to its one-hop neighbor is authenticated by the neighbor using a packet authentication tag. The one-hop neighbor then replaces the tag with its own authentication tag and forwards the packet to its neighbor. This next neighbor verifies the new authentication tag as coming from its immediate neighbor and the process is repeated iteratively until the packet reaches its destination. Therefore, each packet is authenticated at every hop [17].

This scheme has the advantage that it is resistant to denial of service (DoS) attacks and session hijacking attacks such as man-in-the-middle attack. The alternative to per-hop authentication is multihop or end-to-end authentication where authentication is accomplished only by the final receiving node of the packets. The receiver may discover that the packet is bogus and drop it; however, the packet has drained valuable resources such as bandwidth and battery power of all the intermediate nodes that forwarded it. An attacker could use this to his advantage and flood the network with bogus packets in order to initiate a DoS attack. On the other hand, in one-hop authentication the packet is dropped immediately by the attacker's first neigh-

bor, and it does not traverse the network, making DoS attacks very difficult.

Per-packet authentication makes session hijacking formidable for the attacker. In session hijacking attacks, such as man-in-the-middle attacks, the attacker allows the sender to be authenticated normally and then takes over the sender's connection and injects his own packets. The receiver thinks the packets are still coming from the authenticated sender. This is the drawback of authenticating on a connection or session basis rather than on a per-packet basis. In the per-packet authentication case, the receiver will know instantly when a certain packet does not originate from the authenticated sender because every packet is checked for authenticity. The attacker cannot inject false packets claiming to be from the sender.

## *VII. Intrusion Detection in MANETs*

An effective IDS is a key component in securing MANETs. Two different methodologies of intrusion detection are commonly used [2, 4]: anomaly intrusion detection and misuse intrusion detection.

Anomaly-detection systems are usually slow and inefficient and are prone to miss insider attacks. Misuse-detection systems cannot detect new types of attack. Hybrid systems using both techniques are often deployed in order to minimize these shortcomings [2, 3].

### *A. Tracing Intruders Using Mobile Agents*

Many network-based IDSs utilize a central intrusion-detection server that does most of the processing under a client/server model. Every other node on the network, referred to as the target node, transfers its entire system log to the server and the server analyzes the entire log file for intrusions. The drawback of such an approach is that huge amounts of data contained in the system logs need to be transferred periodically to the server. If the intrusion is detected during the remote login session of the attacker, then a mobile agent can trace the session back to the source by migrating back up the chain of intermediate nodes until it reaches the originating node.

In [3], intrusion detection is performed by a centralized server, called the manager. Entire system logs are not sent to the server at regular intervals. Sensor programs at each target node monitor the node in search of marks left by suspected intruder (MLSI). Such marks can be suspicious events such as modification of system files, or launching of root shells, or opening sockets for listening as root. If the sensor program detects an MLSI, it sends out an alert to the manager in real time through the network. The manager in turn launches a tracing agent on the target machine. The tracing agent then launches an information-gathering agent on the same machine.

While this architecture provides a means to trace the attack back to the source machine and identifies the intermediate nodes used in the attack, it suffers from some serious drawbacks. Each network segment has a single manager that is responsible for performing the actual intrusion detection. The presence of such a centralized entity means that there exists a single point of failure. A single manager needs to process data from several target nodes, which results in a system that is not very scalable. Furthermore, in the case of MANETs we cannot assume that a centralized server such as the manager can exist. In a truly mobile ad hoc network, we cannot delegate any crucial responsibility to a single node. In addition, the scheme relies on running agents on a node that is suspected of having been compromised. These agents send back information, which must be reliable. If a node has been compromised, we cannot assume that any information obtained from that node by the agents is totally reliable. The attacker can potentially block the agents from running on a compromised node, or alter its output to send back inaccurate or false information. We need an IDS that is decentralized and where agents do not need to run on potentially already compromised nodes. We addressed these issues in the following section.

### *B. Intrusion Detection Using Autonomous Agents*

Balasubramaniyan et al [2] have proposed an architecture called autonomous agents for intrusion detection (AAFID). This architecture is also intended for intrusion detection in wired networks with a fixed infrastructure. Its basic design, however, is decentralized, and we propose to modify to work in MANETs environment.

The AAFID architecture consists of three main components: agents, transceivers, and monitors. Each node in a network runs one or more agents, which continuously monitor the activity in the node for suspicious behavior, similar to the MLSI events in [3]. Each node also has a single transceiver running, which controls and communicates with the agents. The agents alert the transceiver each time they detect a suspicious event. The transceiver may start or stop other agents or issue control commands to running agents in order to reconfigure them to focus on certain aspects of system behavior. If enough suspicious events are discovered, the transceiver may raise an alarm. Hence, the transceiver functions as the data collection and analysis agency within a single host. Whereas agents cannot generate an alarm, transceivers can generate an alarm if they conclude that an intrusion has occurred.

The third component monitors run on selected nodes in the network according to the original AAFID architecture proposed in [2]. Monitors receive information from several transceivers and also from other monitors. They function as higher-level data collection and processing entities and collect network-wide data. All transceivers report their findings to at least one or more monitors. On the basis of these reports, a monitor may deduce the overall status of the network and take appropriate action.

In this paper we propose modifications to the AAFID architecture to make them more suitable for MANETs. In the absence of any infrastructure, the duty of monitoring cannot be assigned to a few arbitrary nodes in the MANET. Instead, every node needs to run a monitor program, as well as a transceiver and agent programs. The transceiver is mainly concerned with events internal to the node itself and detects intrusion within the node. The monitor, however, keeps track of intrusions in other nodes and stores the current status of the network in the node's vicinity. When a transceiver detects a possible intrusion, it immediately alerts the monitor running on the same node. That monitor in turn alerts all neighboring monitors running on neighboring nodes about the possibility of an intrusion on this node. The neighboring

nodes can then try not to route packets via the compromised node and to deauthenticate it.

This scheme has the advantage that it is decentralized so there is no single point of failure. Furthermore, each node has its own IDS, which can function more or less independently of the other nodes, although some status about the other nodes is communicated to it. In the event an IDS fails on one node, the impact would not be too great as the IDSs on the other nodes will continue to function. To make the system secure, however, it is necessary to employ authentication so that it is no longer easy for an attacker to impersonate another node and claim that an intrusion has been detected in it. There is also the possibility that an intruder can disable the IDS system on a node before it has had the chance to detect the intrusion and alert its neighboring nodes. The chances of this happening can be minimized by using an efficient IDS, which provides only a very small window of time between the attack taking place and the alert being sent out.

## *VIII. Conclusion and Future Work*

We combined efficient techniques from ECC, along with a distributed CA, per-packet and per-hop authentication, and distributed IDS based on threshold cryptography for addressing the issues of key exchange, authentication, and intrusion detection. The model assumed that no single node can be trusted and relied instead on a distributed trust model.

In the future research the overall scheme will be evaluated in terms of security, reliability, efficiency, and scalability. Its feasibility and application in a practical setting will also be studied.

## *References*

[1] B. Mukherjee, T. L. Heberlein, and K. N. Levitt, "Network Intrusion Detection," *IEEE Network*, 8(3): 26–41, 1994.

[2] J. S. Balasubramaniyan et al., "An Architecture for Intrusion Detection using Autonomous Agents," Proceedings of the Fourteenth Annual Computer Security Applications Conference, 1998.

[3] M. Asaka et al., "A Method of Tracing Intruders by Use of Mobile Agents," in proceedings of the Internet Society, 1999.

[4] S. Kumar and E. Spafford, "An Application of Pattern Matchin in Intrusion Detection," Technical Report 94-013, Dept. of Computer Science, Purdue University, 1994.

[5] M. Crosbie and G. Spafford, "Active Defense of a Computer System Using Autonomous Agents," Technical Report 95-008, COAST Group, Dept. of Computer Science, Purdue University, 1995.

[6] Y. Desmedt, "Some Recent Research Aspects of Threshold Cryptography," in proceedings of the First International Workshop on Information Security: 158–173, 1997.

[7] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-Securing Ad Hoc Wireless Networks," to appear in proceedings of the 2002 IEEE Symposium on Computers and Communications, Italy, July 2002.

[8] A. Khalili, J. Katz, and W. Arbaugh, "Toward Secure Key Distribution in Truly Ad-Hoc Networks," in proceedings of the 2003 Symposium on Applications and the Internet Workshops.

[9] G.V.S. Raju, G. Hernandez, and Q. Zou, "Quality of service routing in ad hoc networks," IEEE WCNC 2000, Vol. 1, 2000.

[10] G.V.S. Raju and G. Hernandez, "Routing in Ad hoc networks," in proceedings of the IEEE–SMC International Conference, October 2002.

[11] G.V.S. Raju and J. Charoensakwiroj, "Wireless Communications," *Annual Review of Communications, Vol. 57* (Chicago: IEC, 2004).

[12] L. Zhou and Z. Haas, "Securing Ad Hoc Networks," *IEEE Network Magazine*, 13(6), November/December 1999.

[13] P Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad hoc Networks," in proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference, January 2002.

[14] A. Perrig, R. Szewcyzk, V. Wen, D. Culler, and J.D. Tygar, "Spins: Security Protocols for Sensor Networks," in proceedings of Mobile Computing and Networking 2001.

[15] G.V.S. Raju and R. Akbani, "Elliptic Curve Cryptosystems and its Applications," in the proceedings of the IEEE-SMC Conference, October 2003.

[16] V.S. Miller, "Use of Elliptic Curves in Cryptography," in Advances in Cryptology (Proceedings of CRYPTO 1985), Springer Verlag Lecture Notes in Computer Science 218, 1986, pp. 417–426.

[17] G.V.S. Raju and Rehan Akbani, "Some Security Issues in Mobile Ad-hoc Networks," in proceedings of the Cutting Edge Wireless and IT Technologies Conference, November 2004.