Design of a Scheme for Secure Rouitng in Mobile Adhoc Networks

Sesha Bhargavi Velagaleti[#1], Dr.M.Seetha[#2], Dr.S.Viswanadha Raju[#3]

[1#]*Assistant Professor, IT Departmnet, GNITS, Shaikpet, Hyderabad, India.*

[2#] *Professor, CSE Departmnet, GNITS, Shaikpet, Hyderabad,India .*

[3#] *Professor, CSE Departmnet, JNTUK, Hyderabad, India.*

***Abstract*— A Mobile Ad hoc Network (MANET) consists of a set of communicating wireless mobile nodes or devices that do not have any form of fixed infrastructure or centralized authority. The security in MANET has become a significant and active topic within the research community. This is because of high demand in sharing streaming video and audio in various applications, one MANET could be setup quickly to facilitate communications in a hostile environment such as battlefield or emergency situation likes disaster rescue operation. In spite of the several attacks aimed at specific nodes in MANET that have been uncovered, some attacks involving multiple nodes still receive little attention. A reason behind this is because people make use of security mechanisms applicable to wired networks in MANET and overlook the security measures that apply to MANET. Furthermore, it may also have to do with the fact that no survey or taxonomy has been done to clarify the characteristics of different multiple node attacks. In this paper, we briefly discuss about the security problems with the existing protocols and further discuss possible solutions for them.**

***Keywords*— Mobile Ad Hoc Network, Security, Protocols, Attacks**

I. INTRODUCTION

A Mobile Ad Hoc Network(MANET) is a network consisting of a collection of nodes capable of communicating with each other without help from a network infrastructure. Applications of MANETs include the battlefield applications, rescue work, as well as civilian applications like an outdoor meeting, or an ad-hoc classroom. With the increasing number of applications to harness the advantages of Ad Hoc Networks, more concerns arise for security issues in MANETs. The nature of ad hoc networks poses a great challenge to system security designers due to the following reasons: *firstly*, the wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering; *secondly*, the lack of an online CA or Trusted Third Party adds the difficulty to deploy security mechanisms; *thirdly*, mobile devices tend to have limited power consumption and computation capabilities which makes it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms; *fourthly*, in MANETs, there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks, in another word, we need to consider both insider attacks and outsider attacks in mobile ad hoc networks, in which insider attacks are more difficult to deal with; *finally*, node mobility enforces frequent networking reconfiguration which creates more chances for attacks, for example, it is difficult to distinguish between stale routing information and faked routing information. There are five main security services for MANETs: *authentication, confidentiality, integrity, non-repudiation, availability*. *Authentication* means that correct identity is known to communicating partner; *Confidentiality* means certain message information is kept secure from unauthorized party; *integrity* means message is unaltered during the communicaiton; *nonrepudiation* means the origin of a message cannot deny having sent the message; *availability* means the normal service provision in face of all kinds of attacks. Among all the security services, authentication is probably the most complex and important issue in MANETs since it is the bootstrap of the whole security system. Without knowing exactly who you are talking with, it is worthless to protect your data from being read or altered. Once authentication is achieved in MANET, confidentiality is a matter of encrypting the session using whatever key material the communicating party agree on. Note that these security services may be provided singly or in combination. In this paper, we propose a security architecture from a layered view, then the functionalities of each layer is described. We further analyze the application of the proposed security architecture in military applications.

MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A

MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

II. Security Problems with Existing Ad hoc Routing Protocols

The main assumption of the previously presented ad hoc routing protocols is that all participating nodes do so in good faith and without maliciously disrupting the operation of the protocol [1,2]. However, the existence of malicious entities cannot be disregarded in any system, especially in open ones like ad hoc networks. The RPSEC IETF working group has performed a threat analysis that is applicable to routing protocols employed in a wide range of application scenarios [3]. According to this work, the routing function can be disrupted by *internal* or *external* attackers. An internal attacker can be any legitimate participant of the routing protocol. An external attacker is defined as any other entity. As we have previously noted, we consider denial-of-service attacks that target the utilized wireless medium, such as frequency jamming, outside the scope of our threat model. Two commonly used countermeasures against jamming are *frequency hopping spread spectrum* (FHSS) and *direct sequence spread spectrum* (DSSS) [4]. Furthermore, outside the scope of our threat model are transport layer attacks, such as session hijacking, and application layer attacks, such as repudiation-based attacks and user information disclosure.

The strongest assumption for an external attacker is that it is able to eavesdrop the communication between two legitimate network participants, inject fabricated messages and delete, alter or replay captured packets. Weaker assumptions of external attackers include the ability to inject messages but not read them, or read and replay messages but not inject new ones, or just the ability to read messages. Cryptographic solutions can be employed to prevent the impact of external attackers by mutual authentication of the participating nodes through digital signature schemes [5]. However, the underlying protocols should also be considered since an attacker could manipulate a lower level protocol to interrupt a security mechanism in a higher level. Although these attacks are a significant part of a complete threat assessment, our analysis focuses only on network-layer threats and countermeasures.

Internal attackers have the capabilities of the strongest outside attacker, as they are legitimate participants of the routing process. Having complete access to the communication link they are able to advertise false routing information at will and force arbitrary routing decisions on their peers [6]. One of the most difficult to detect problems in routing is that of *byzantine failures*. These failures are the result of nodes that behave in a way that does not comply with the protocol. The reasons for the erroneous behavior could be software or hardware faults, mistakes in the configuration, or malicious compromises. Attempts to solve the problem of byzantine failures have been proposed for both infrastructure [7] and infrastructureless networks [8].

Based on this threat analysis and the identified capabilities of the potential attackers, we will now discuss several specific attacks that can target the operation of a routing protocol in an ad hoc network.

- *Location disclosure* [10]: Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [9], or with simpler probing and monitoring approaches an attacker is able to discover the location of a node, or even the structure of the entire network.
- *Black hole* [6]: In a black hole attack a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.
- *Replay* [4]: An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.
- *Wormhole* [11]: The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network. One attacker, say node A, captures routing traffic at one point of the network and tunnels them to another point in the network, say to node B, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers.
- *Blackmail* [12]: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated [13].
- *Denial of service*: Denial of service attacks aim at the complete disruption of the routing function and therefore the whole operation of the ad hoc network. Specific instances of denial of service attacks include the *routing table overflow* [10] and the *sleep deprivation torture* [14]. In a routing table overflow

attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

- *Routing table poisoning*: Routing protocols maintain tables which hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in selection of non-optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network.

III. IMPLENTATIONS AND VALIDATIONS

a. Implementation of Spatial Location Based Service

We had implemented a Location Based Service (LBS) which is an information service, accessible with mobile devices through mobile networks. [12] It includes services to identify an object in a particular location such as discovering a list of colleges or hospitals in a particular location. This application consists the logic for SMS receiving and sending through SMS push and pull mechanism. Any mobile user who wants to use these services can simply send a message stating whereabouts of his requirements to a cell which in turn is connected to the LBS server. Reply will be sent according to the requirements of the user by considering the respected database through the mobile connected to the server. Figure 1 provides the architecture of our location based service. Figure 2 provides output of the spatial application.

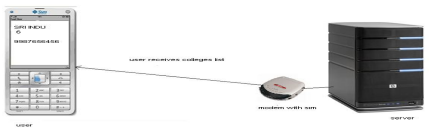

FIGURE 1. THE ARCHITECTURE OF OUR LOCATION BASED SERVICE

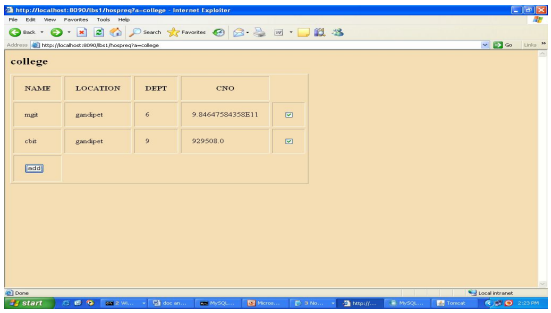

FIGURE 2. OUTPUT OF THE SPATIAL APPLICATION

b. Implementation of Advanced Scheme of Digital Signature Standards

We had implemented and integrated advanced scheme of Digital Signature Standards into the Semantic Web Security architecture. We used ECC (Elliptic Curve Cryptography) digital signature scheme and a new forward-secure digital signature scheme is proposed in order to reform the limitations of DSA. In this new scheme, although the digital signature's private key is under the control of a one-way function and continually changed in different durations with time goes by; its public key remains the same. The attacker could not fake the older signature even if the private key is leaked out in some period of time. In this way this scheme makes sure of the security of former phases. The validity of the new scheme is proved and the security is analyzed in this implementation. Figure 3 represents the overall class diagram of the advanced DSA. Figure 5 shows the output screen shot of the application.

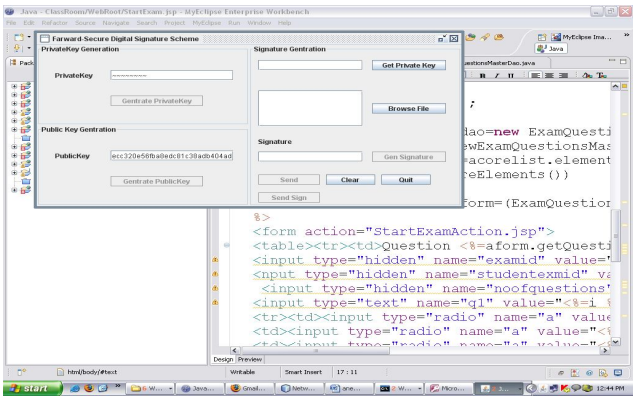

FIGURE 3. OUTPUT SCREEN SHOT OF THE ADVANCED DSA APPLICATION.

.

IV. CONCLUSIONS

In this work we have dealt with security issues in mobile ad hoc networks. We have focused on designing a security architecture in tackling security challenges mobile ad hoc networks are facing.

We present a security architecture in a layered view and analyse the reasoning for such a security architecture, and apply the proposed security architecture in some possible scenarios. we expect

this security architecture can be used as a framework when designing system security for ad hoc networks.

REFERENCES

[1] D.B. Johnson, D.A. Maltz, Y.-C. Hu, and J.G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR)," Internet Draft, draft-ietf-manet-dsr-07.txt, February 2
002.

[2] C.E Perkins, E.M. Royer, and S. Das, d hoc On-demand Distance Vector (AODV)," RFC 3561, July 2003.

[3] S. Murphy, "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt, October 2002.

[4] A.D. Wood, and J.A. Stankovic, "Denial of Service in Sensor Networks", *IEEE Computer*, vol. 35, no. 10, October 2002, pp. 54-62.

[5] K. Zhang, "Efficient Protocols for Signing Routing Messages," *Proc. Symp. Network and Distributed Systems Security (NDSS'98)*, San Diego, CA, March 1998, pp. 29-35.

[6] P. Papadimitratos, and Z.J. Haas, "Securing the Internet Routing astructure," *IEEE Communications*, vol. 10, no. 40, October 2002, pp. 60-68.

[7] R. Perlman, "Network Layer Protocols with Byzantine Robustness," Ph.D. Dissertation, MIT/LCS/TR-429, MIT, October 1988.

[8] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," *WISE'02*, Atlanta, Georgia, September 2002, pp. 21-30.

[9] J.-F. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems," *Proc. Workshop on Design Issues in Anonymity and Unobservability*, Berkeley, CA, July 2000, pp. 7-26.

[10] J. Lundberg, "Routing Security in Ad hoc Networks," http://citeseer.nj.nec.com/400961.html.

[11] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Networks," *Proc. 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom'03)*, San Francisco, CA, April 2003.

[12] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," *Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications*, Callicoon, NY, June 2002, pp. 3-13.

[13] L. Zhou, and Z.J. Haas, "Securing Ad hoc Networks," *IEEE Network Magazine*, vol. 6, no. 13, November/December 1999, pp. 24-30.

[14] F. Stajano, and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad hoc Wireless Networks," *Proc. 7th Int'l. Workshop on Security Protocols*, Cambridge, UK, April 1999, pp. 172-194.

[15] An Analysis of Collaborative Attacks on Mobile Ad hoc Networks Cong Hoan Vu, Adeyinka Soneye, School of Computing Blekinge Institute of Technology Soft Center SE – 37225 RONNEBY,Sweeden.