Volume 1, No. 1, May-June 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SECURITY DEPLOYMENT IN MOBILE ADHOC NETWORKS

Verma Neeraj Kumar*
Sr. Lecturer, Dept. of Computer Science and Eng.,
Krishna Institute of Management and Technology,
Moradabad, U.P, India
er.neerajkumar@gmail.com

Mohd Wazih Ahmad
Sr. Lecturer, Dept. of Computer Science and Eng.,
Galgotia's College of Engg. & Tech. ,
Greater Noida, U.P, India
mail.java@yahoo.com

Mohammad Islam
Sr. Lecturer, Dept. of Computer Science and Eng.,
Galgotia's College of Engg. & Tech. ,
Greater Noida, U.P, India
islam_cs1@yahoo.co.in

Narendra Kr. Teotia
Sr. Lecturer, Dept. of Computer Science and Eng.,
Galgotia's College of Engg. & Tech. ,
Greater Noida, U.P, India
nkteotia2004@gmail.com

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.

Keywords: Manet, Elliptic Curve Cryptography, Intrusion-detection system, GloMoSim, Adhoc, MAC.

I. INTRODUCTION

Wireless networking is a fast growing technology that enables users to access information and services electronically, regardless of their geographic location. The use of wireless communication between mobile users has become increasingly popular due to recent technological advancements in computer and wireless technologies. This led to the lower prices and higher data rates, which are the two main reasons why mobile computing is expected to see increasingly widespread use and applications. There are two distinct approaches for enabling wireless communications between mobile hosts. The first approach is to use a fixed network infrastructure that provides wireless access points. In this network, a mobile host communicates to the network through an access point within its communication radius. When it goes out of range of one access point, it connects with a new access point within its range and starts communicating through it. An example of this type of network is the cellular network infrastructure. A major problem of this approach is handoff, which tries to handle the situation when a connection should be smoothly handed over from one access point to another access point without noticeable delay or packet loss another issue is that networks based on a fixed infrastructure are limited to places where there exists such network infrastructure. The second approach is to form an ad-hoc network among users wanting to communicate with each other. This means that all nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network.

A **mobile ad hoc network** (**MANET**) is a collection of two or more mobile devices equipped with wireless communications and networking capability. Alternately, MANET is a self-configuring and adaptive network of mobile devices connected by wireless links [1]. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The nodes are interconnected by single-hop or multiple hop wireless connection, and each node may serve as a packet level router for other nodes in the same mobile ad hoc network [2].All nodes are equal and may join or leave at any time, and have equal right to the medium. In fact, it's very much like an Ethernet, where we may add or remove node at discretion. Routes between two hosts in MANET may consist of hops through other hosts in the network [9]. The task of finding and maintaining routes in MANET is nontrivial since host mobility causes frequent unpredictable topological changes [3]. A number of MANET protocols for achieving efficient routing have been recently proposed. They differ in the approach used for searching a new route and/or modifying a known route, when hosts move. It is assumed that each node is aware of the geographic location of all other nodes in MANET. Of course, for this to work all nodes must be able to see all the other nodes of the network, to be able to establish communication with them [4]. When a node goes out of range, it just looses connection with the rest of the ad-hoc

network. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes [5].

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid- to late 1990s [6]. Many academic papers evaluate protocols and abilities assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other and usually with nodes sending data at a constant rate. Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol, and other measures.

This form of networking is limited in range by the individual nodes transmission ranges and is typically smaller compared to the range of cellular systems. However, ad-hoc networks have several advantages compared to traditional cellular systems. The advantages include 'on-demand' setup, fault tolerance, and unconstrained connectivity. A key feature that sets ad-hoc wireless networks apart from the more traditional cellular radio systems is the ability to operate without a fixed wired communications infrastructure and can therefore be deployed in places with no infrastructure [11]. This is useful in disaster recovery, military situations, and places with non-existing or damaged communication infrastructure where rapid deployment of a communication network is needed. A wireless ad-hoc environment introduces many problems such as mobility, security of data and limited bandwidth.

II. OBJECTIVES

Wireless ad-hoc networks are very vulnerable to attacks for many reasons. On the one hand, eavesdropping on the wireless transmissions using passive attacks is relatively easy. On the other hand, communication protocols can be breached using well-directed active attacks. Moreover, these attacks can be carried out on multiple layers of the ISO-OSI networking model. For example, denial of service attacks can be carried out on the physical layer (jamming the transmission frequency); on the data link layer by permanently occupying the medium; on the network layer by well targeted propagation of incorrect routing information; and on the application layer (distributed denial of service attacks)[7]. Other popular attack like manin- the-middle, replay or data corruption are still feasible on wireless ad-hoc networks. Combination attacks that plunge the network into a state of constant re-organization, thereby increasing maintenance traffic and reducing network throughput are also possible.

The application of well-proven traditional security mechanisms in wireless ad-hoc networks is impractical because of the nature of these networks (lightweight devices, limited bandwidth and dynamic unstable links). In most cases, the implementation of a central trusted authority enforcing authentication and authorization is not feasible. With the explosive growth of wireless networks, research on ad-hoc networks has also increased. Security in wireless ad-hoc networks is still at its infancy [8]. Security of such a network has always been an important issue. In this dissertation, we analyze the fundamental security requirement of MANET and challenges faced by it. An attempt will be made to propose a network security framework for secure data communication. We shall also discuss the vulnerable features and threats of MANET along with few defense mechanisms.

III. HARDWARE & SOFTWARE PLATEFORM REQUIREMENT

Analysis, simulation, hybrid simulation and testbed measurements are well known techniques for evaluating and ad hoc network protocols [14]. At a time when ad hoc network "standards" are being proposed in the MANET (Mobile Ad Hoc Networks) working group of the IETF, it is clearly important to have a set of reliable performance evaluation and measurement tools to compare various proposals in a consistent environment that can be calibrated and replicated. In our study, we shall use the simulator GloMoSim for the performance study of the MANET.

In GloMoSim we are building a scalable simulation environment for wireless and wired network systems. It is being designed using the parallel discrete-event simulation capability provided by Parsec [9]. GloMoSim currently supports protocols for a purely wireless network. In the future, we anticipate adding functionality to simulate a wired as well as a hybrid network with both wired and wireless capabilities. Most network systems are currently built using a layered approach that is similar to the OSI seven layer network architecture. The plan is to build GloMoSim using a similar layered approach. Standard APIs will be used between the different simulation layers [13]. This will allow the rapid integration of models developed at different layers by different people. The general hardware requirements for the study of GloMoSim environment are:

A. Pentium 2.33-GHz processor or faster (3.00 GHz is recommended)
B. 512 MB of RAM (1.0 GB is recommended)
C. 120 GB of HDD.
D. CD-ROM or DVD-ROM drive
E. Keyboard and a Microsoft Mouse or some other compatible pointing device
F. Video adapter and monitor with Super VGA (800 x 600) or higher resolution
G. MS Window 2000/ XP

IV. PROBLEM DEFINITION

Mobile Ad-hoc Networks (MANETs) are composed of a set of communicating devices which are able to spontaneously interconnect without any pre-existing infrastructure. Our purpose of the research is to identify various problem areas in ad-hoc networks relating to data communication and security.

For any wireless networking technology, security is considered one of the most crucial factors to gain greater acceptance. In ad hoc network, as one component of the wireless technologies, security is one of the crucial components that needs due attention. Ad hoc networks are

much more vulnerable to security attacks than conventional wired networks. The reasons: open wireless medium; capture of unattended roaming nodes and impersonation; decentralized coordination protocols vulnerable to attack (e.g. contention based MAC); lack of centralized certificate authority for key exchange; use of cache proxies that can be easily hit by DDoS attacks etc.

In our study, we shall explore the various mechanisms for the designing and implementing the security schemes for intrusion detection and prevention. The study of various key and trust management schemes to prevent external attacks and various secure MANET routine protocols to prevent internal attacks, is also proposed.

V. IMPLEMENTATION AND FUTURE SCOPE

Security is a paramount concern in mobile ad hoc network (MANET) because of its intrinsic vulnerabilities. The emergence of new applications of ad hoc network necessitates the need for strong privacy protection and security mechanisms of MANET.

While the proposed techniques can prevent and deter certain attacks in MANET, there is a limitation to the effect of prevention techniques in general. Firstly, this technique is designed for a set of known attacks. They are unlikely to prevent your threats that are designed to circumvent the existing security measures. We must have another mechanism to detect this newer attack. Secondly, each of the prevention techniques come with added overhead and complexity. With the resource constraints in MANET, it is not realistic to have all known prevention techniques activated at all time.

To facilitate this, we need to have a good understanding of the resource consumption characteristics of the prevention techniques or to develop good strategy for activating the appropriate mechanisms according to run time conditions.

Security research has taught us that we need to deploy defense-in-depth or layered security mechanisms because security is a process (or a chain) i.e. as secure as it's weakest link. In addition to prevention, we also need detection and response, as well as security policies and vulnerabilities analysis. Our proposed work can be extended through the extension of the current routing protocol by making the communication more secured has been proposed [Gue01] to protect the routing protocol messages.

VI. METHODOLOGY

A. Literature survey.
B. Development of models (Mathematical and Computers).
C. Real time simulation of models developed.
D. Interpretation of the result.
E. Publication of the technical papers.
F. Improvement by the feedback from the technical publication.
G. Model studies in the field.
H. Compilation of the final results, the theories developed/ evolved and preparation of the thesis.

VII. REFERENCES

[1] Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". *'Reilly Wireless Dev Center* . http://www.oreillynet.com/pub/a/wireless /2004/ 01/22/ wirelessmesh. html. Retrieved 2009-01-20.

[2] David B. Johnson. "Routing in ad hoc networks of mobile hosts". 'In Proc. of the IEEE Workshop on Mobile Computing Systems and Applications, pages 158–163, December 1994'.

[3] BOSE, P., MORIN, P., STOJMENOVI ´C, I., AND URRUTIA, J. Routing with guaranteed delivery in ad hoc wireless networks. Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DialM '99), Aug. 1999.

[4] M. S. Corson and A. Ephremides, "A distributed routing algorithm for mobile wireless networks," ACM J. Wireless Networks, vol. 1, no. 1, pp. 61–81, 1995.

[5] V.D. Park and M.S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proc. IEEE INFOCOM '97, Apr. 1997.

[6] S. Basagni, I. Chlamtac, V. Syrotiuk, and B. Woodward, "A Distance Routing Effect Algorithm for Mobility (DREAM)," Proc. Fourth Ann. ACM/IEEE Int'l Conf. Mobile Computing and Networking (MobiCom '98), Aug. 1998.

[7] S. Murthy and J.J. Garcia-Luna-Aveces, "An Efficient Routing Protocol for Wireless Networks," ACM Mobile Networks and Applications J., special issue on routing in mobile communication networks, Oct. 1996.

[8] Basagni, S.I Chlamatac,V.R Syrotiuk, and B.A Woodward, "A distance Routing Algorithm for Mobility" Proc. MOBICOM ,1998, 76-84.

[9] S. Yi, P. Naldurg, R. Kravets, "Security-Aware Ad-Hoc Routing for Wireless Networks,"UIUCDCS-R-2001-2241 Technical Report, Aug. 2001.

[10] G. Pei, M. Gerla and X. Hong, "LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility,"*First Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC),* August 2000.

[11] Ad Hoc Networking, C.E. Perkins, editor, Addison-Wesley Longman, 2001.[Pap02b] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks,"

[12] N. Nikaein, H. Labiod, and C. Bonnet, "DDR-Distributed Dynamic Routing Algorithm for Mobile Ad hoc Networks," *First Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC),* August 2000.

[13] Y.Hu, A.Perrig, and D.Johnson Packet leashed: A defense against wormhole attacks in wireless and ad

hoc networks. In proceeding of IEEE INFOCOM'03, 2003. Y.Hu, A.Perrig, and D.Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proceedings of ACM MobiCom Workshop-Wise 03,2003.*