Volume 2, No. 6, June 2011
Journal of Global Research in Computer Science
REVIEW ARTICLE
Available Online at www.jgrcs.info
ISSN-2229-371X

ASSESSMENT OF SECURITY IN MOBILE AD-HOC NETWORKS (MANET)

Deepak Chayal*, Dr. Vijay Singh Rathore**

Research Scholar*, Director**
NIMS University, Jaipur*
S.K.College, Jaipur**
deepak_chahal@yahoo.co.in

Abstract: With the proliferation of cheaper, smaller, and more powerful mobile devices, mobile ad hoc networks (MANETs) have become one of the fastest growing areas of research. This new type of self-organizing network combines wireless communication with a high degree node mobility. Unlike conventional wired networks they have no fixed infrastructure (base stations, centralized management points and the like). Mobile ad hoc networks (MANETs) are one of the fastest growing areas of research. Conventional networks use dedicated nodes to carry out basic functions like packet forwarding, routing, and network management. In ad hoc networks these are carried out collaboratively by all available nodes. In this paper, we'll discuss about the MANET specific attacks, security challenges, goals and protocols alongwith the techniques used to secure MANETs.

INTRODUCTION

Attacks on an ad hoc network routing protocols generally fall into one of two categories: routing disruption attacks and resource consumption attacks. In a routing disruption attack, the attacker attempts to cause legitimate data packets to be routed in dysfunctional ways. In a resource consumption attack, the attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth, or to consume node resources such as memory (storage) or computation power. From an application layer perspective, both attacks are instances of a Denial-of-Service (DoS) attack. An attacker may attempt to make a route through itself appear longer by adding virtual nodes to the route; we call this attack *gratuitous detour*, as a shorter route exists and would otherwise have been used. In ad hoc network routing protocols that attempt to keep track of perceived malicious nodes in a "blacklist" at each node, such as is done in watchdog and pathrater [1], an attacker may *blackmail* a good node, causing other good nodes to add that node to their blacklists, thus avoiding that node in routes.

MANET SPECIFIC ATTACKS

The unique characteristics of MANET routing algorithms result in new sets of wireless computing attacks. The majority of these attacks are directed at the algorithmic capabilities; the means of communicating routing information and the transporting of data. A partial listing of MANET specific attacks follows:

Altering Radio Route Tables –
Hack the radio and modifying routing tables and the propagation of these alterations [2].

Black Listing –
Trick a network/system into believing a good node is behaving maliciously .

Jamming –
Selectively jamming routing messages that define the network. Jamming a central node can break down a network. Timed jamming at intervals can cause the appearance of messages being lost, route loss.

Jellyfish –
Active insertion of jitter/delay into packet routing harms QoS and can deny timely packet delivery[3].

Replay –
A node in a network may rebroadcast the energy from a neighboring node, extending its range. Thus node B, hearing the replayed message of A by C, will believe that the shortest route is through A. Nodes A and B have no knowledge that packets are being replayed. This is a type of Man in the Middle attack, classified as an unauthenticated node having inserted itself into the network function [4].

Selfish Node –
Nodes that refuse to fully participate in routing.

Sink Hole –
Taking on more routing than needed, forcing data thought it self; becoming an overly critical network node [5].

SECURITY CHALLENGES

Some of the security challenges in MANET are:

Channel vulnerability:
Broadcast Wireless channels allow message Eavesdropping and Injection easily.

Bnode vulnerability:
Nodes do not reside in physically protected places, thus easily fall under attack.

Absence of infrastructure:
Certification/ Authentication Authorities are absent.

Dynamically Changing Network Topology
Puts security of routing protocols under threat.

Power and Computational Limitations

Prevent the use of complex Encryption Algorithms.

SECURITY GOALS OF MANETs

At the highest level, the security goals of MANETs are not that different from other networks. Most typically authentication, confidentiality, integrity, availability, and non-repudiation.

Authentication

is the verification of claims about the identity of a source of information. Authenticity is essentially assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. Authentication can be providing using encryption along with cryptographic hash function, digital signature and certificates. Without authentication, an adversary could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operations of the other nodes [6].

Confidentiality

means that only authorized people or systems can read or execute protected data or programs. It should be noted that the sensitivity of information in MANETs may decay much more rapidly than in other information.

Integrity

Means that the information is not modified or corrupted by unauthorized users or by the environment. Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [7]: *Malicious altering and Accidental altering.*

Availability

Refers to the ability of the network to provide services as required. The term *Availability* means that a node should maintain its ability to provide all the designed services regardless of the security state of it.

Non-Repudiation

ensures that committed actions cannot be denied. In MANETs security goals of a system can change in different modes (e.g. peace time, transition to war, and war time of a military network). The characteristics of MANETs make them susceptible to many new attacks. At the top level attacks can be classified according to network protocol stacks.

Access control/ authorization:

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users.

Anonymity:

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

Scalability:

Scalability is not directly related to security but it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

SECURE AD HOC ROUTING PROTOCOLS

Several researchers have proposed secure routing protocols. Several routing protocols have been proposed for routing in ad hoc networks; however, until recently, security in such networks has not yet enjoyed much attention from the research community. As a result, ad hoc network routing protocols that assume a trusted environment are highly vulnerable to attack; for example using the wormhole or rushing attacks, an adversary can paralyze ad hoc networks.

SEAD [8]

The Secure Efficient Ad hoc Distance Vector (SEAD) is a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector (DSDV) algorithms. To developing SEAD, follow the table driven approach. In table driven routing protocol maintain at all times routing information regarding to the network connectivity of every node to all other nodes. It is also known as proactive routing protocol.

SRP [9]

Secure Routing Protocol (SRP) was developed based on Destination Source Routing protocol (DSR). The operation of SRP requires the existence of a Security association (SA) between source node initiating a route query and the destination node. The security association can be utilized in order to establish a shared secret key between the two nodes, which is used by SRP.

ARIADNE

Ariadne is a secure routing protocol developed by Yih-Chun Hu, David B. Johnson and Adrian Perrig based on the Dynamic Source Routing protocol (DSR). Ariadne is an on-demand routing protocol, which find routes as when it required, dynamically. Ariadne uses MAC s and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime. It contains two phases in its routing mechanism; Route discovery and Route maintenance. In the route discovery phase the source node establishes a route by flooding route request packets (RREQ).

ARAN

The Authenticate routing for ad hoc network (ARAN) is a secure routing protocol for MANETs, developed by Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz and Elizabeth M. Belding-Royer based on AODV. ARAN utilizes cryptography mechanism in order to achieve security goals such as; authentication, message integrity, and non-repudiation in ad-hoc networks. It uses asymmetric cryptography to securing routing in an ad hoc network and require universal trusted third party.

SOADV [10]

Secure Ad hoc On-demand Distance Vector (SAODV) is a proposal for security extensions to the AODV protocol. The proposed extensions utilize digital signatures and hash chains in order to secure AODV packets. In order to facilitate the transmission of the information required for the security mechanisms, SAODV defines extensions to the standard AODV message format. SAODV is a widely implemented protocol in industry due to its strong security features. SADOV uses a central key management in its routing topology. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts. Tunneling attacks are possible through two compromised nodes. Wormhole attacks are always possible with compromised nodes in any ad hoc network topology. The use of sequence numbers could prevent most of the possible reply attacks.

TECHNIQUES USED TO SECURE MOBILE AD-HOC NETWORKS

In order to provide solutions to the security issues involved in mobile ad-hoc networks, we must elaborate on the two of the most commonly used approaches in use today:

Prevention

Prevention dictates solutions that are designed such that malicious nodes are thwarted from actively initiating attacks. Prevention mechanisms require encryption techniques to provide authentication, confidentiality, integrity and non-repudiation of routing information. Among the existing preventive approaches, some proposals use symmetric algorithms, some use asymmetric algorithms, while the others use one-way hashing, each having different trade-offs and goals. Prevention mechanisms, by themselves cannot ensure complete cooperation among nodes in the network.

Detection and Reaction

Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes. All protocols in this category are designed such that they are able to detect malicious activates and react to the threat as needed.

CONCLUSION

The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers. A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range uses intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication to automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network.

REFERENCES

[1] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks. In Proceedings of the Sixth Annual IEEE/ACM International Conference on Mobile Computing and Networking (MobiCom 2000), pages 255–265, August 2000.

[2] K. Sanzgiri, B. Dahill, B.N. Levine, E. Royer, and C. Shields. "A Secure Routing Protocol for Ad Hoc Networks" Technical Report 01-37, Department of Computer Science, University of Massachusetts, August 2001.

[3] I. Aad, J. Hubaux, and E. Knightly. "Denial of Service Resilience in Ad Hoc Networks," ACM MobiCom, September 2004.

[4] M. Brumster, and T. Le. "Optimistic Tracing in MANET," Florida State University, Department of Computer Science, March 2006.

[5] A. Burg. "Ad hoc Network Specific Attacks," Ad hoc networking: Concepts, Applications and Security Seminar, Technische Universität München, 2003.

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

[7] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.

[8] Y-C Hu, D. B. Jhonson, and A. Perrig, " SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Network," in Poceeding of 4th IEEE workshop on Mobile Computing System and Applications.

[9] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad hoc Network," in Proc. of CNDS 2002.

[10] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad hoc Wireless Network," Mobile Computing, T. Imielinski and H. Korth, Ed. Kluwer, 1996.