International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October2009
1793-8201

Secure Routing Techniques for MANETs

Dr. Harsh Sadawarti and Anuj K. Gupta, Member, IAENG

***Abstract*— In this paper we present a survey of various existing secure routing protocols for mobile ad hoc networks (MANETs). A** mobile ad-hoc network **is a self-configuring network of mobile nodes, connected by wireless links, which act as routers and are free to move randomly and organize themselves arbitrarily. These types of networks operate in the absence of any fixed infrastructure which makes them easy to deploy but it becomes difficult to make use of the existing routing techniques for network services. In order to facilitate communication within the network, a Routing Protocol (RP) is used to discover routes between nodes. The primary goal of such an ad-hoc network RP is correct and efficient route establishment between a pair of nodes so that messages may be delivered in time. The wireless and distributed nature of MANETs poses security a great challenge to system designers. This paper contains two main sections: first section presents a short literature study on various types of security attacks and routing security schemes that have been proposed to prevent and/or detect these attacks and second gives a state-or-the-art review of the existing secure Routing Protocols designed for MANETs with a comparison for typical representatives.**

***Index Terms*—Security Attacks, SRP, SEAD, Ariadne, ARAN, AODV.**

I. INTRODUCTION

Mobile ad hoc (or spontaneous) networks are IP networks made up of a collection of wireless and mobile nodes communicating via radio links that can temporarily form a network whenever they coexist in the same neighbourhood without any fixed infrastructure such as base stations for mobile switching and no centralized administration. The overall network topology is highly dynamic and can change from time to time. All the nodes and routers are made to move freely throughout the network irrespective of their neighbours. The nodes generally have a limited transmission range, so each node seeks some assistance of its neighbouring nodes to forward packets. Specially configured Routing Protocols are implemented to establish routes between nodes which are discussed later in the paper. The major problem in MANETs is the security which is primarily due to the open nature and no fixed topology of the MANET environment. Similarly, routing in MANETs is a critical issue of concern because each node in turn acts as a router for the next node.

These routers are free to move randomly and organize themselves arbitrarily. The information is exchanged and updated dynamically from time to time. In this paper various approaches have been studied to overcome the security problems and different existing Routing Protocols have been reviewed which are designed for secure routing in MANETs.

Dr. Harsh Sadawarti is Professor in Dept. of Computer Science & Engineering at RIMT – Institute of Engineering & Technology, Mandi Gobindgarh, Punjab, India. He has done B.Tech., M.Tech. and Ph.D. in Computer Science. He is member of IEEE.

Anuj K. Gupta is Assistant Professor in Dept. of Computer Science & Engineering at RIMT – Institute of Engineering & Technology, Mandi Gobindgarh, Punjab, India. He has done B.Tech., M.Tech. and currently pursuing Ph.D. in Computer Science. He is member of IAENG.

II. SECURITY ISSUES

A number of attacks compromise the safe exchange of information in MANETs, which can be categorized using different criteria. There are two kinds of attacks that can be launched against MANETs: Passive and Active. A Passive Attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Passive attacks basically involve obtaining vital routing information by sniffing about the network. Such attacks are usually difficult to detect and hence, defending against such attacks is complicated. Even if it is not possible to identify the exact location of a node, one may be able to discover information about the network topology, using these attacks. An Active Attack, however, injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The goal is basically to attract all packets to the attacker for analysis or to disable the network. Such attacks can be detected and the nodes can be identified.

In passive attacks, the attacker doesn't disturb the routing protocol. It only eavesdrop the traffic and extract the valuable information from it. Whereas in active attacks, the malicious nodes can disturb the correct functioning of a Routing Protocol by modifying its routing information, by impersonating other nodes or by fabricating false routing information [1]. Passive attacks can be prevented using various encryption mechanisms. Only active attacks can be carried out at routing level. These can either be external or internal. External attacks can be passive and active. Passive attacks are unauthorized interruption of the routing packets and active attack is from outside sources to degrade or damage message flow between nodes. A compromised node is categorized as internal attack. This is most severe threat for MANETs. This may broadcast wrong routing information to other nodes. Active external attacks on the wireless routing protocol can be described as denial-of-service attacks.

A detailed coverage of the two types of attacks is present in [2]. A secure MANET environment should provide confidentially, integrity, authenticity, availability and non-repudiation. The Vulnerabilities that make MANETs highly insecure are discussed as follows:

- Dynamic nature of wireless communication.
- Node Security & tampering.
- Limited power in nodes.
- Absence of infrastructure.

- Lack of fixed network topology.

Apart from the attacks prevailing in MANETs, there are a variety of threats which are divided into two categories: threats to network mechanism and threats to security mechanism [5]. The following are few attacks based on routing mechanism [3]:

Black Hole

The black hole attack is briefly introduced in [20]. In the attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.

Worm Hole

In a wormhole attack, two malicious collaborating nodes which are connected through a private network, can record packets at one location in the network and tunnel them to another location through the private network and retransmits them into the network [2].

Routing Table Overflow

In a routing table overflow attack the attacker attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation [22].

Sleep Deprivation

The sleep deprivation is briefly introduced in [6]. Usually, this attack is practical only in ad hoc networks, where battery life is a critical parameter. Battery powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes, or by forwarding unnecessary packets to the node using, for example, a black hole attack.

Location Disclosure & Impersonation attacks

A location disclosure attack can reveal something about the locations of nodes or the structure of the network. The information gained might reveal which other nodes are adjacent to the target, or the physical location of a node [21].

Denial of Service and Exhaustive attack

These attacks are among the most prominent types of attacks. In denial of service (DoS) attacks the adversary prevents or prohibits the normal use or management of network facilities or functionality. DoS attacks can be launched at any layer of an ad hoc network to exhaust node resources [23].

The prevention of attacks on the routing mechanism will be discussed in next section. The threats to security mechanism include replacing public keys / compromised private or shared keys. The key management is one of the major issues in MANETs. This may be simplified by a Central Trust Authority (CTA) which implements initial authentication to all the nodes. One such variant of CTA is Distributed Public Key Model which is discussed in [7]. Current security study for the ad hoc networks is scattered on special topics such as intrusion detection, secure routing, and key management. Brief introduction to each of these topics is being presented further.

A. Intrusion Detection

The ad hoc networks have inherent vulnerabilities that are not easily preventable. Intrusion prevention measures, such as encryption and authentication, are required to protect network operation. But these measures cannot defend compromised nodes, which carry their private keys. Intrusion detection presents a second wall of defence. It is a necessity in the ad hoc networks to find compromised nodes promptly and take corresponding actions to against. A distributed and cooperative architecture for better intrusion detection was proposed in [24]. Based on the proposed architecture, a statistical anomaly detection approach is used. The detection is done locally in each node and possibly through cooperation with all nodes in the network. But how to define the anomaly models based on which trace data is still a main challenge.

B. Key Management

Cryptographic schemes, such as digital signatures, are employed to protect both routing information and data traffic. These schemes usually require a key management service. A public key infrastructure is adopted because of its superiority in distributing keys, achieving integrity, non-repudiation, authenticate each node and establish a shared secret session key. In this, 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 a certification authority (CA) 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 detail is present in [7].

III. SECURE ROUTING

Routing in MANETs is a critical issue since collaboration between nodes is required to relay packets on behalf of one another, thus each node acts like a router. To preserve the security of MANETs from attacks, a routing protocol must fulfil certain set of requirements [1], to ensure proper functioning of the path from source to destination in presence of malicious nodes.

These are:

- Authorized nodes should perform route computation and discovery.
- Minimal exposure of network topology
- Detection of spoofed routing messages
- Detection of fabricated routing messages
- Detection of altered routing messages
- Avoiding formation of routing loops
- Prevent redirection of routes from shortest paths.

A number of secure routing protocols [8] have been recently developed that conform to most of the requirements. These protocols employ a variety of cryptographic tools for protecting the vulnerabilities in different routing protocols. As shown in Figure 1, routing protocols for MANETs can be classified into two main categories [4]:

• Proactive or table-driven routing protocols
• Reactive or on-demand routing protocols

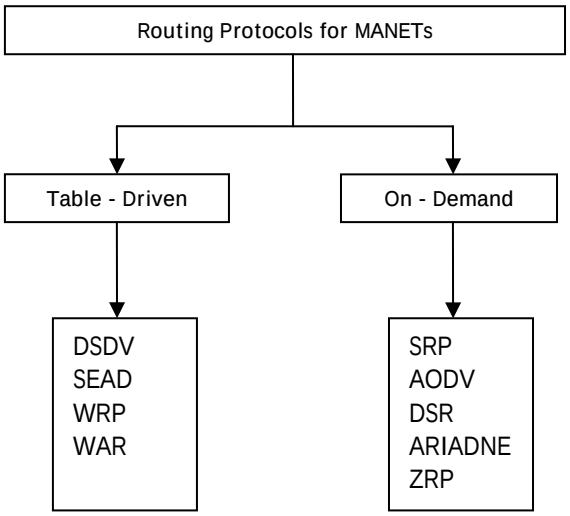

Fig.1: Type of Routing Protocols for MANETs

In table-driven nodes exchange routing information periodically to maintain a consistent route in each node for every other node in the network, as in Distance Vector Routing Protocol (SEAD), discussed in [9]. Whereas in on-demand, a node initiates a Route Request mechanism called Route Discovery whenever it needs to reach a destination and the routes are created accordingly for single time use. The most common protocols that implement this mechanism are AODV (Ad hoc On Demand Vector routing) [3] and DSR (Dynamic Source Routing) [2]. The table-driven ad hoc routing approach is similar to the connectionless approach of forwarding packets, with no regard to when and how frequently such routes are desired. It relies on an underlying routing table update mechanism that involves the constant propagation of routing information. This is not the case, however, for on-demand routing protocols. When a node using an on-demand protocol desires a route to a new destination, it will have to wait until such a route can be discovered. On the other hand, because routing information is constantly propagated and maintained in table-driven routing protocols, a route to every other node in the ad hoc network is always available, regardless of whether or not it is needed. This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are -

1. Respective amount of data for maintenance.
2. Slow reaction on restructuring and failures.

On the other hand, the Reactive protocols find a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are -

1. High latency time in route finding.
2. Excessive flooding can lead to network clogging.

In this paper we have presented a critical analysis of the above mentioned secure routing protocols discussed below. Table 1 list some of the basic differences between the two categories of MANETs Routing Protocols.

TABLE I: COMPARISON BETWEEN TIME-DRIVEN & ON DEMAND ROUTING PROTOCOLS

Parameters	Table-Driven	On-Demand
Storage Requirements	**Higher**	**Dependant on no. of routes maintained or needed**
Route Availability	**Always available**	**Computed as per need**
Periodic Route Updates	**Required always**	**Not required**
Delay	**Low**	**High**
Scalability	**100 nodes**	**> 100**
Control Traffic	**High**	**Low**
Routing Information	**Keep**	**Doesn't keep**
Routing Philosophy	**Mostly flat**	**Flat**

A. Secure Routing Protocol (SRP)

It is proposed by Papadimitratos and Haas. SRP is applied as an extension of a multitude of existing RPs such as DSR [11] and ZRP [12]. This protocol counters the malicious behaviour that guarantees the acquisition of correct topological information in a timely manner [10]. The protocol is proven robust against a se of attacks that attempt to compromise the route discovery. It provides the correct routing information regarding a pair of nodes provided they have prior security association. The source node initiates the route discovery by sending a Route Request (RREQ) packet (identified by a pair of identifiers, a query sequence number & a random query identifier) to the destination and replies are sent back strictly through the same route. SRP can only handle Black Hole attacks and not Worm Hole attacks. However, it can nevertheless prevent them.

B. SEAD

It is a Distance Vector Routing Protocol based on Destination Sequences Distance Vector (DSDV) Ad Hoc Routing [13]. It is a lightweight secure routing protocol presented by Hu, Johnson & Perrig [9]. The designers of SEAD used efficient one-way Hash functions to provide authentication for both the sequence number and metric field in each routing entry. They avoid asymmetric cryptography to protect against DoS attack and to overcome limited CPU processing capability. The receiver of the achieved either through Message Authentication Certificate (MAC) [14] or some broadcast authentication mechanism. It is too susceptible to Worm Hole attacks like SRP.

C. ARIADNE

It is another On-Demand Routing Protocol presented by Hun, Johnson & Perrig [2] based on DSR. It maintains authenticity on end-to-end basis, using symmetric key cryptography. It can authenticate routing messages using either shared secret keys, digital signatures or shared secrets in combination with broadcast authentication like TESLA [15]. The Protocol enables the destinations to authenticate the Route Request sent by source node. The RREQ contains MAC which can be easily verified by the destination node. A per-hop hashing technique is used to verify that no node is missing from the node list [16]. Route maintenance is done using Distance Secure Routing (DSR) mechanism. However, Ariadne is very much immune to Worm Hole attacks through clock synchronization between nodes, but not in all

situations.

D. ARAN

It is presented by Dahill. It relies on a trusted certificate server. Every node forwarding a Route Request or Reply is required to sign the packet. It detects and protects against malicious actions carried out by 3rd party and peers [1]. It uses public key cryptography to obtain a public key certificate from TCA. ARAN introduces authentication, message integrity and non-repudiation to an ad hoc environment as a part of a minimal security policy. The route maintenance is done through special error messages. The source code initiates and the route discovery packet that is verified by the destination before the RREQ is sent back. It prevents impersonation attacks by providing end-to-end and hop-to-hop authentication of route discovery & reply messages. It is also not capable to handle wormhole attacks and the uses of asymmetric cryptography makes it more valuable to DoS attacks. All the routing messages are authenticated at every hop from source to destination as well as on reverse path from destination to source.

E. AODV

Ad Hoc On-Demand Distance Vector is based on on-demand mechanism that relieves nodes from frequently generating and storing route entries, but introduces a delay caused by the Route Discovery procedure [18, 19]. It finds routes only when required and hence is reactive in nature. The major vulnerabilities present in AODV protocols are: Deceptive increase of sequence number and Deceptive decrease of hop count. Zapata [17] applies security extensions to AODV using one-way hash functions to serve metric fields in Route Request (Route Discovery). He introduced Secure-AODV (SAODV) [18] where he suggests using digital signatures to authenticate non-mutable data in an end-to-end manner. Hash chains are used to secure mutable fields such as hop count. It is an extension to AODV Routing Protocol. It is used to protect Route Discovery mechanism of AODV by providing security features like integrity, authentication and non-repudiation. Table 2 shows the comparisons between some of the above discussed protocols [25].

Table II: COMPARISON OF MAIN AD-HOC ROUTING PROTOCOLS

Parameters	DSDV	AODV	DSR
Reactive	No	Yes	Yes
Multiple Routes	No	No	Yes
Loop Free	Yes	Yes	Yes
Distributed	Yes	Yes	Yes
QoS support	No	No	No
Power Efficiency	No	No	No
Periodic Updates	Yes	Yes	No
Multicast	No	Yes	No
Unidirectional link support	No	No	Yes

IV. CONCLUSION

Mobile ad-hoc networks have properties that increase their vulnerability to attacks. We have discussed and presented various issues such as security attacks and threats that can cause vulnerability in MANETs. Also we presented some Secure RPs designed for different conditions that help in safe & secure routing in MANETs. SEAD is a Distance Vector Routing Protocol while others discussed above are On-Demand RPs. The SOADV provides requisite measures for protection of route discovery and transfer of data. we have presented a robust routing security mechanism for MANETs which implements defence against various types of external attacks, detects malicious behaviours and provides a plan for their detections and provide a safer environment. With authenticated assured, secure routing can be successful in MANETs & the malicious nodes can be identified and excluded from routing. we plan to continue our work in field of securing MANETs & present more security routing techniques for MANETs. However, if seen together due to the dynamic & unpredictable nature of MANETs, the limited power of mobile nodes & limited CPU processing capability, the setting of a completely secure mechanism for MANETs seems to be unfeasible. In this paper, we have studied the security issues in the ad hoc networks and surveyed the security attacks. We found that the existing solutions cannot fully solve the security issues for the MANETs well.

PERSONAL THOUGHTS

In this paper, we have tried to focus on various attacks posed on MANETs & the study of different routing protocols to provide a secure transmission of data on MANETs. Moreover, the security for the ad hoc networks is still in its infancy. Since the ad hoc networks are dynamic by nature, they require a dynamic security solution that fits this fundamental characteristic. More survey is still a requirement to justify the theoretical conclusions with experimental data.

REFERENCES

[1] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," in Proceedings of the International Conference on Network Protocols (ICNP), pp. 78-87, 2002.

[2] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2002.

[3] Janne Lundberg, Routing Security in Ad Hoc Networks. Tik-110.501 Seminar on Network Security,

[4] http://citeseer.nj.nec.com/400961.html.2000.H. Dang, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine, 0163-6804, pp. 70-75, October 2002.

[5] Jean-Pierre Hubaux, Levente Buttyan, Srdjan Capkun. The Quest for security in Mobile Ad Hoc Networks. Proceedings of the 2001 ACM International Symposium on Mobile ad Hoc networking & computing, Long Beach, CA. 2001.

[6] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," Security Protocols, 7th International Workshop, LNCS, Springer-Verlag, 1999.

[7] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no.6, November/December 1999.

[8] "Secure routing protocols for mobile ad-hoc wireless networks," in Advanced Wired and Wireless Networks, T.A.Wysocki, A.Dadej, and B. J. Wysocki, Eds. Springer, 2004.

[9] Y.C. Hu, D.B. Johnson and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," IEEE, Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), 0-7695-1647-5, 2002.

[10] P. Papadimitratos and Z.J. Haas. "Secure routing for mobile ad hoc networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[11] D.B. Johnson, D.A Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks," Ad Hoc Networking, C.E. Perkins, Ed., Addison-Wesley, 2001, 139-172.

[12] Z. J. Haas, M. Perlman, "The Performance of Query Control Schemes of the Zone Routing Protocol" IEEE/ACM Transactions on Networking, vol. 9, no. 4, pp. 427-438, Aug 2001.
[13] C.E. Perkins, and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector (DSDV) for Mobile Computers," Proc. ACM Conf. Communications Architectures and Protocols (SIGCOMM'94), London, UK, August 1994, pp. 234-244.
[14] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104, February 1997.
[15] Vesa Karpijoki. Security in Ad Hoc Networks. Tik-110.501 Seminar on Network Security.
[16] http://citeseer.nj.nec.com/karpijoki01security.html.2000. 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.
[17] Manel Guerrero Zapata. "Secure ad hoc on-demand distance vector (SAODV) routing". IETF MANET Mailing List, Message-ID 3BC17B40.BBF52E09@nokia.com,
[18] ftp://MANET.itd.nrl.navy.mil/pub/MANET/2001-10.mail, October 8, 2001.M. Zapata, N. Asokan, "Securing ad hoc routing protocols", WiSe'02, ACM 1-5813-585-8, September 28, 2002, pp.1-10.
[19] C.E Perkins, E.M. Royer, and S. Das, "Ad hoc On-demand Distance Vector (AODV)," RFC 3561, July 2003.
[20] F. Wang, B. Vetter, and S. Wu, "Secure Routing Protocols: Theory and Practice," Technical Report, North Carolina State University, May 1997.
[21] N. Ahuja and A. Menon, "Security in Mobile Networks : Ad-hoc and Infrastructure," Computer and Information Sciences, University of Florida, Dec 2001.
[22] H. Li, Z. Chen, X. Qin, C. Li, H. Tan, "Secure Routing in Wired Networks and Wireless Ad Hoc Networks," Technical Report, Department of Computer Science, University of Kentucky, April 2002.
[23] M. Jakobsson, W. S, and Y. B, "Stealth Attacks on Ad-Hoc Wireless Networks," in proc. Vehicular Technology Conf., October, 6-9 2003.
[24] Yongguang Zhang, Wenke Lee. Intrusion Detection in Wireless Ad-Hoc Networks. Proceedings of MobiCom 2000, Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6-11 Aug. 2000.
[25] http://www.cmpe.boun.edu.tr/~emre/ research/msthesis/node1.html.