International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
www.ijset.com, Volume No.1, Issue No.2 pg:01-06 01 April 2012

Security Challenges In Ad Hoc Networks

Ashutosh Yadav
Information Technology Department
SSSIST,
Sehore, India
ashutosh_0507@yahoo.co.in

Mr. Gajendra Singh Chandel
Information Technology Department
SSSIST,
Sehore, India
Gajendrasingh86@rediffmail.com

ABSTRACT-Ad hoc networks are special networks that do not require an infrastructure. Nodes of such networks are usually mobile and wireless. Wireless nodes use a shared medium for communication, so they are able to communicate with many nodes directly provided they are within communication range of those nodes.

In this article we present a study of secure ad hoc routing protocols for wireless Networks. Ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. Attacks on ad hoc network routing protocols disrupt network performance and reliability with there solution. We briefly present the most popular protocols that follow the table-driven and the source-initiated on-demand approaches. The comparison between the secure routing protocols and parameters of ad hoc network shows the performance according to secure protocols. We discuss in this paper routing protocol and challenges and also discuss authentication in ad hoc network.

KEYWORDS: Wireless Network, Ad hoc Network, Security Service, Routing Protocols, Routing Authentication, Hash function and Secure Routing Protocols.

I. INTRODUCTION

Ad hoc networks are special networks that do not require an infrastructure. Nodes of such networks are usually mobile and wireless. Wireless nodes use a shared medium for communication, so they are able to communicate with many nodes directly provided they are within communication range of those nodes.

Wireless networks [34] consist of a number of nodes which communicate with each other over a wireless channel which have various types of networks: sensor network, ad hoc mobile networks, cellular networks and satellite networks. Wireless sensor networks consist of small nodes with sensing, computation and wireless communications capabilities.

Ad-hoc networks are a new paradigm of wireless communication for mobile hosts where node mobility causes frequent changes in topology. Ad hoc networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support movablity and organize themselves arbitrarily. This means that the topology of the ad hoc network changes dynamically and unpredictably. Moreover, the ad hoc network can be either constructed or destructed quickly and autonomously without any administrative server or infrastructure. Without support from the fixed infrastructure, it is undoubtedly arduous for people to distinguish the insider and outsider of the wireless network. That is to say, it is not easy for us to tell apart the legal and the illegal participants in wireless systems. Because of the above mentioned properties, the implementation of security infrastructure has become a critical challenge when we design a wireless network system. If the nodes of ad hoc networks are mobile and with wireless communication to maintain the connectivity, it is known as mobile ad hoc network (MANET) and require an extremely flexible technology for establishing communications in situations which demand a fully decentralized network without any fixed base stations, such as battlefields, military applications, and other emergency and disaster situations.

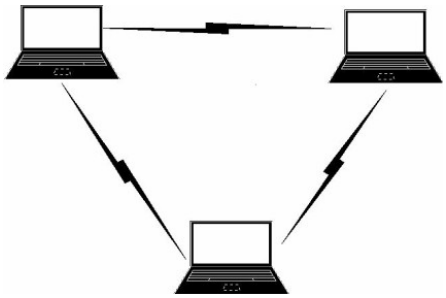

FIGURE 1: AD HOC NETWORK

Figure 1 shows three node where ad hoc network where every node is connected to wireless, and work as access point to forward and receive data. This article discuss attacks on ad hoc networks and discusses current approaches for establishing cryptographic keys in ad hoc networks. We describe the state of research in secure ad hoc routing protocols, routing challenges and its research issues.

II. ROUTING PROTOCOL AND ITS CHALLENGE IN AD HOC NETWORK

In this section we are going to discuss different approaches adopted for routing and security challenges in Ad hoc networks.

A. ROUTING PROTOCOLS

Routing in mobile ad hoc networks faces additional problems and challenges [22], [30] when compared to routing in traditional wired networks with fixed infrastructure. There are several well known protocols in the literature that have been specifically developed to cope with the limitations imposed by ad hoc networking environments. Most of the existing routing protocols follow two different design approaches to confront the inherent Characteristics of ad hoc networks: the *tabledriven* and the *source-initiated on-demand* approaches.

Table-driven ad hoc routing protocols maintain at all times routing information regarding the connectivity of every node to all other nodes that participate in the network. Also known as *proactive*, [49] these protocols allow every node to have a clear and consistent view of the network topology by propagating periodic updates [27]. An alternative approach to that followed by table-driven protocols is the source-initiated on-demand routing. According to this approach, a route is created only when the source node requires a route to a specific destination. A route is acquired by the initiation of a *route discovery* function by the source node.

Table 1 shows the various type of routing protocols according to parameter which are response time, bandwidth and energy.

Parameter	Network	Protocols	Examples
Response Time And Bandwidth	Ad hoc	Proactive protocols	Destination-sequenced Distance-Vector (DSDV)
			Optimized Link- State Routing (OLSR)
		Reactive protocols	Ad Hoc On-Demand Distance-Vector (AODV)
			Dynamic Source Routing (DSR)
			Geography-based routing
			Cluster-based (or *hierarchical*) routing
Energy	Sensor	Network structure	Flat network routing
			Hierarchical network routing
			Location based routing
		Protocol operation	Negotiation based routing
			Multi-path based routing
			Query based routing
			QoS based routing
			Coherent based routing

TABLE 1: CLASSIFICATION OF ROUTING PROTOCAL

B. SECURITY CHALLENGES IN AD HOC NETWORKS

Use of wireless links renders an Ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion [9],[10],[52].Eavesdropping might give an attacker access to secret information thus violating confidentiality. Active attacks could range from deleting messages, injecting erroneous messages; impersonate a node etc thus violating availability, integrity, authentication and nonrepudiation. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, we need to consider malicious attacks not only from outside but also from within the network from compromised nodes. Thus following are the ways by which security can be breached. [56]

_ **Vulnerability of Channels:** As in any wireless network, messages can be eavesdropped and fake messages can be injected into the network without the difficulty of having physical access to network components.

_ **Vulnerability of nodes:** Since the network nodes usually do not reside in physically protected places, such

as locked rooms, they can more easily be captured and fall under the control of an attacker.

_ **Absence of Infrastructure:** Ad hoc networks are supposed to operate independently of any fixed infrastructure. This makes the classical security solutions based on certification authorities and on-line servers inapplicable.

_ **Dynamically Changing Topology**:
Ad-hoc network is dynamic due to frequent changes in topology. Even the trust relationships among individual nodes also changes, especially when some nodes are found to be compromised. Security mechanism need to be on the dynamic and not static and should be scalable.

III. SECURITY MODEL

In this section we first discuss security goals attacks and thus secure routing protocol which are
Following:

A. SECURITY GOALS FOR AD HOC

_ **Availability:** Ensures survivability despite Denial Of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key
management service.

_ **Confidentiality:** Ensures certain information is never disclosed to unauthorized entities.

_ **Integrity:** Message being transmitted is never corrupted.

_ **Authentication:** Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

_ **Non-repudiation:** Ensures that the origin of a message cannot deny having sent the message.

_ **Non-impersonation**: No one else can pretend to be another authorized member to learn any useful information.

_ **Attacks using fabrication:** Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.

B. ATTACK ON AD HOC NETWORK

There are various types of attacks on ad hoc network which are describing following:

_ **Location Disclosure:** Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [20], 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:** 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[26]. 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:** 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:** 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 [53]. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, 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. The solution to the wormhole attack is *packet leashes*.

_ **Blackmail:** 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 [58]. 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.

Denial of Service: Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network [15]. Specific instances of denial of service attacks include the *routing table overflow and* the *sleep deprivation torture*.. 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 attack 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 that 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 [15]. 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 the selection of non-optimal routes, the creation of routing loops, bottlenecks, and even portioning certain parts of the network.

_ **Rushing Attack:** Rushing attack is that results in denial-of-service when used against *all* previous on-demand ad hoc network routing protocols [55].

_ **Breaking the neighbor relationship:** An intelligent filter is placed by an intruder on a communication link between two ISs(Information system) could modify or change information in the routing updates or even intercept traffic belonging to any data session.

_ **Masquerading:** During the neighbor acquisition process, a outside intruder could masquerade an nonexistent or existing IS by attaching itself to communication link and illegally joining in the routing protocol do main by compromising authentication system. The threat of masquerading is almost the same as that of a compromised IS.

_ **Passive Listening and traffic analysis:** The intruder could passively gather exposed routing information. Such a attack can not effect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected. However, the confidentiality of user data is not the responsibility of routing Protocol

C. ROUTING SECURITY IN AD HOC NETWORK

The contemporary routing protocols for Ad hoc networks cope well with dynamically changing topology but are not designed to accommodate defense against malicious attackers. No single standard protocols capture common security threats and provide guidelines to secure routing. Routers exchange network topology informally in order to establish routes between nodes another potential target for malicious attackers who intend to bring down the network..

Detection of compromised nodes through routing information is also difficult due to dynamic topology of Ad hoc networks [22]. Routing protocols for Ad hoc networks must handle outdated routing information to accommodate dynamic changing topology. False routing information generated by compromised nodes can also be regarded as outdated routing information. As long as there are sufficient numbers of valid nodes, the routing protocol should be able to bypass the compromised nodes, this however needs the existence of multiple, possibly disjoint routes
between nodes. Routing protocol should be able to make use of an alternate route if the existing one appears to have faulted

D. ROUTING AUTHENTICATION

Routing authentication is one of the important factors in ad hoc networks during route discovery because ad hoc is infrastructure less network. So it is required that a reply coming from a node against a route request must be authentic. That's why authentication protocol is required between the nodes of ad hoc network

IV. SECURE ROUTING PROTOCOLS

A. ARAN
Authenticated Routing for Ad-hoc Networks (ARAN) detects and protects against malicious actions by third parties and peers in Ad-hoc environment. ARAN introduces authentication, message integrity and non-repudiation to an Ad-hoc environment [12][30]. ARAN is composed of two distinct stages.

B. SEAD
Our Secure Efficient Ad hoc Distance vector routing protocol (SEAD) is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, in spite of active attackers or compromised nodes in the network[50].

C. SRP
Secure Routing Protocol [4][13] (Lightweight Security for DSR), which we can use with DSR to design SRP as an extension header that is attached to ROUTE REQUEST and ROUTE REPLY packets.

D. SECURE AODV
The SecAODV [54] implements two concepts secure binding between IPv6 addresses and the independent of any trusted security service, Signed evidence produced by the originator of the message and signature verification by the destination, without any form of delegation of trust.

E. BISS
Building Secure Routing out of an Incomplete Set of Security Associations (BISS) [38], the sender and the receiver can establish a secure route, even if, prior to the route discovery, only the receiver has security associations established with all the nodes on the chosen route. Thus, the receiver will authenticate route nodes directly through security associations.

F. SLSP
The Secure Link State Protocol (SLSP) [30] for mobile ad hoc networks is responsible for securing the discovery and distribution of link state information. The scope of SLSP may range from a secure neighborhood discovery to a network-wide secure link state protocol.

G. TIARA
Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms (TIARA) mechanisms protect ad hoc networks against denial-of-service (DoS) attacks launched by malicious intruders. TIARA addresses two types of attacks on data traffic which are flow disruption and resource depletion..

H. ARIADNE
A Secure On Demand Routing Protocol for Ad Hoc Networks (ARIADNE) using the TESLA [43][44] broadcast authentication protocol for authenticating routing messages, since TESLA is efficient and adds only a single message authentication code (MAC) to a message for broadcast authentication.

I. SAR
Security-Aware ad hoc Routing (SAR) that incorporates security attributes as parameters into ad hoc route discovery. SAR enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad hoc routing protocols.

V. COMPARISONS OF SECURE PROTOCOLS

At the last we provide the comparison of different secure routing protocols of ad hoc network using table 1 and table 2. In table 1 shows defense against different type of attack. Comparison shows which protocol is better in different type of attacks. For example replay attack cover by ARAN but it is not coverable by RAP [58].

Attack	Protocol							
	ARAN	SRP	SEAD	ARIADEAN	SAODV	SLSP	OSRP	RAP
Location Disclosure	No	No	No	No	No	No	No	No
Black- Hole	No	No	No	No	No	No	Yes	No
Replay	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Worm hole	No	No	No	No	No	No	No	No
Black mail	NA	NA	NA	NA	NA	NA	NA	NA
Denial of services	No	Yes	Yes	Yes	No	Yes	No	No
Routing table poisoning	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Rushing attacks	Yes	No	Yes	Yes	No	No	No	Yes

Table 2: DEFENSE AGAINST ATTACK

VI. CONCLUSION

We have presented an overview of the existing security scenario in the Ad-Hoc network environment. Key management, Ad-hoc routing of wireless Ad-hoc networks were discussed. Adhoc networking is still a

raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. The key management protocols are still very expensive and not fail safe. Several protocols for routing in Ad-hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application.

VII. REFERENCES

[1] Adrian Perrig Ran Canetti J. D. Tygar Dawn Song "*The TESLA Broadcast Authentication Protocol*", UC Berkeley and IBM Research.
[2] Ajay Mahimkar, R. K. Shyamasundar "*S-MECRA A Secure Energy-Efficient Routing Protocol for Wireless Ad Hoc Networks*" IEEE 2004
[3] Alia Fourati, Khaldoun Al Agha, Hella Kaffel Ben Ayed "Secure and Fair Auctions over Ad Hoc Networks" *Int. J. Electronic Business, 2007*
[4] Anand Patwardhan, Jim Parker, Michaela Iorga. Anupam Joshi, "*Tom Karygiannis, Secure Routing and Intrusion Detection in Ad Hoc Networks*" 3rd International Conference on Pervasive Computing and Communications (PerCom 2005), Kauai Island, Hawaii**.**