Secure Adhoc Network

[1,]Pawan Bhadana , [2,]Ritu Khurana, [3,]Chanchal , [4,]Manisha

[1,] *Associate Professor, Department of Computer Engineering, B.S.A. Institute of Technology & Management, Faridabad, India*

[2,] *Assistant Professor, Department of Computer Engineering, B.S.A. Institute of Technology & Management, Faridabad, India*

[3,4] *Computer Science & Engineering, B.S.A. Institute of Technology & Management, Faridabad, India*

ABSTRACT

Now a day, it is no longer optional to have security solutions even inevitable for every kind of organizations and individuals. There are number of generic tools which are common for organizations as well as for individual users to provide security which includes; Anti-Spam, Anti-Virus etc., and network security have become essential issue in MANET. Security is one of the main issues in the MANET especially with respect to size and complexity of the network. The aim of the thesis is to discuss different aspects of security in MANET (e.g. multi-layer intrusion detection technique in multi hop network of MANET, security problems relates between multihop network and mobile nodes in MANET etc) and also implement some of the solutions (e.g. comparative study of different routing protocol (AODV, DSR and TORA) security threats within MANET network like intruder behavior, tapping and integrity, MANET link layer and network layer operations with respect to information security etc) with respect to MANET network.This paper also discusses different number of scenarios of MANET network which we implement in our simulation. In our simulation we use to implement different routing protocols and also did comparative study that which one is better with respect to different aspects. We also use to implements mechanisms of intruder behavior, tapping and integrity, and MANET link layer and
network layer operations with respect to information security.

KEYWORDS: *MANET, Security, tapping, intruder.*

I. INTRODUCTION

Mobile ad hoc network got outstanding success as well as tremendous attention due to its self maintenance and self configuration properties or behavior.

There are different types of challenges in mobile ad hoc network which are given below:

- Open network architecture
- Shared wireless medium
- Stringent resource constraints
- Highly dynamic network topology

Mobile ad hoc network has different challenges with respect to wireless security due to some of the following reasons:

[1] The wireless network especially liable to attacks because of active eavesdropping to passive interfering.
[2] Due to lack of Trusted Third Party adds, it is very difficult to deploy or implement security mechanisms.
[3] Mostly Mobile devices have limited computation capability and power consumption functionalities which are more vulnerable to Denial of Service attacks. It is also incapable to run heavy security algorithms which need high computations like public key algorithms.
[4] Due to MANET's properties like infrastructure less and self-organizing, there are more chances for trusted node to be compromised and launch attacks on networks. In other words we need to cover up from both insider and outsider attacks in MANET, in which insider attacks are more difficult to deal with.
[5] It is difficult to distinguish between stale routing and faked routing information because of node mobility mechanism. In node mobility mechanism it enforces frequent networking reconfiguration which creates more chances for attacks.

There are mainly three main security services for MANETs: Authentication, confidentiality, integrity.

- Authentication means correct identity is known to communicating authority.
- Confidentiality means message information is kept secure from unauthorized access.

Integrity means message is unaltered during the communication between two parties. Once authentication is achieved in MANET then confidentiality is just a matter of encrypting algorithm on the session by using keys. These security services can be provided singly or in combination, it only depends on our requirements. In this paper we will focus on the fundamental security problems of the Mobile ad hoc network connectivity between mobile nodes from one network to another network, and how it works in client (mobile nodes) server (mobile server) architecture with respect to security.

II. BACKGROUND

There are some ultimate goals regarding security solutions with respect to Mobile ad hoc networks or we can say there are some security services which should be fulfill in order to enforce security like authentication, confidentiality, integrity to mobile users, we also use another term for them CIA which should be fulfill. In order to achieve goal in security, whatever the security solution it is? But it should provide complete protection to entire protocol stack.

Table 2.1 shows the security issues with respect to each layer.

S. No	Layer	Security Issues
1	Application Layer	In this layer we should prevent viruses, application abuses, worms, as well as malicious nodes.
2	Transport Layer	It provide authentication and provide secure end-to-end communications through data encryption between two nodes.
3	Network Layer	This layer deals with the protection of routing as well as forwarding protocols.
4	Link Layer	In this layer we mainly concern with the protection of wireless MAC protocol and also provide link-layer security.
5	Physical Layer	In this layer we should prevent signal jamming as well as denial-of-service attacks.

2.1.Challenges

One of the fundamental vulnerability of MANETs comes from open peer-to-peer architecture. In case of wired networks there are dedicated routers but in case of mobile ad hoc network each mobile node acts as a router in order to forward packets for one node to other node. According to security information with respect to MANET network are vulnerable compromises or physical capture, especially at the end of low-end devices due to weak protection.

There are some characteristics of security solutions of MANETs which will clearly provide multi fence security solutions with respect to network protection and also provide desirable network performance.

1. The security solution should also implement across many individual components in order to provide collective protection to secure entire network.
2. 2. The security solution should also provide security with respect to different layers of the protocol stack and each layer provide line of defense.
3. The security solutions should avoid threats from both outsiders as well as inside.
4. The security solutions should enforce all three components of security like prevention, detection, and reaction.
5. The security solutions should be affordable as well as practical in resource constrained and highly dynamic networking scenario.

2.2.Routing protocol description

There are basically there kind of routing protocols which are:

- **Table driven routing protocols**

In these routing protocols each node in the network maintains the complete routing information of the network by occasionally updating the routing table.

- **On-Demand routing protocols**

While in this kind of routing protocols, a node simply maintains routes information to get destination that it needs to send required data packets.

- **Hybrid routing protocols (ZRP)**

In this type of routing protocol is the combination of the above two categories. In which nodes belonging to a particular geographical area or within a certain detachment from an anxious node are said to be in routing area and uses table driven routing protocol. Communication between nodes in different areas will rely on the source initiated or on-demand routing protocols. This routing protocol Include ZRP.

2.2.1 AODV

AODV using a classical distance vector routing algorithm. It is also shares DSR's on-demand discovers routes. During repairing link breakages AODV use to provide loop free routes. It does not add any overhead to the packets, whenever a route is available from source to destination. Due to this way it reduces the effects of stale routes and also need for route maintenance for unused routes.

2.2.2 DSR

The DSR is an on-demand routing protocol that is based on source routing. It uses no periodic routing messages like AODV, and due to this way it reduces network bandwidth overhead, and also avoids large routing updates as well as it also reduces conserves battery power.

2.2.3 TORA

The TORA is an adaptive, scalable and efficient distributed routing algorithm. It is mainly designed for multi-hop wireless networks as well as highly dynamic mobile environment. It is also called source-initiated on-demand routing protocol.

III. MANET ATTACKS &SECURITY

3.1 Security

Security aspects play an important role in almost all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place (e.g. in tactical applications) to routing, man-in-the-middle and elaborate data injection attacks.

3.2 Protecting Mobile ad-hoc network

The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them.

3.4. Reactive Approach

Seeks to detect security threats and react accordingly.

3.5. Proactive Approach

Attempts to prevent an attacker from launching attacks through various cryptographic techniques: This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network.

3.6.Attacks

There are two mainly protocols are used in MANET networks, Link layer protocol are used to provide connectivity between different mobile nodes in order to ensure one-hop connectivity by using multihop wireless

channels. On the other hand if we like to extend connectivity to different multiple hops then MANET network uses network layer protocols.

3.7.Network Layer operation

There are two main network-layer operations in MANET.

1. Ad hoc Routing
2. Data packet forwarding

They interact with each other and delivering packets from source to destination. The main function of the ad hoc routing protocols is to provide routing among nodes; they exchange routing messages between different mobile nodes in order to maintain routing information at each node. According to the routing states, the second network layer operation data packets are used to forward data by intermediate next node which is an established route to the destination node. These both operations are vulnerable to malicious attacks, and which will lead to various types of malfunction in network layer.

3.8. Network Layer Attack

Due to this reason network-layer generally fall into two categories attack:

Routing attacks

Packet forwarding attacks(based on the target operation of the attacks)

3.9.Active Attacks

There are also some different active attacks which are really difficult to locate or identify because these attacks are more sophisticated and they are considered as subtle routing attacks some of them are given below :

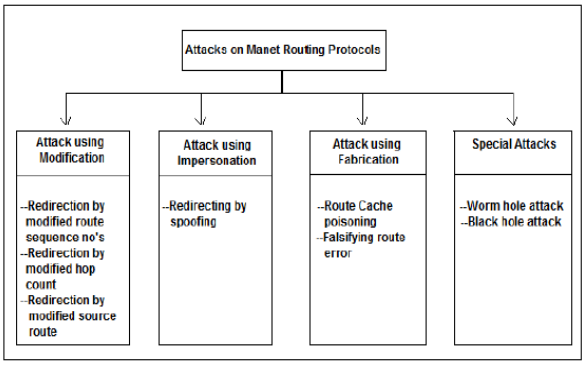
- Attacker may further subvert existing nodes in the network.
- They can also fabricate their identity
- They can also impersonate other legitimate node
- Attackers in pair nodes may create a wormhole
- They also creates shortcut in normal flows between each other
- The attackers target the route maintenance process and advertise operational link is broken

3.10.Routing Attacks

Generally there are four different types of MANET routing protocol attacks which is divided in to two main types which are given below:

1. Routing disruption attacks
2. Resource consumption attacks

In case of routing disruption attacks, the main task of attacker is to disrupt routing process by routing packets in order to introduce wrong paths. In case of resource consumption attacks are concerned the main task of the attacker is to introduce some non-cooperative or selfish nodes that can be used to inject false packets due to this way load on the network increases and it will become a cause of consuming network bandwidth.



3.11.Security steps to avoid Attacks in MANET

Secure Multicasting

There is an architecture usually used to secure multicast traffic that is DIPLOMA. DIPLOMA stands for DIstributed Policy enfOrceMent Architecture which is use to protect or secure end user services as well as network bandwidth.

3.12.Secure routing

One of the primary challenges of secure routing is to provide authentication (trustworthiness) of users in the network.

3.13.Privacy-aware and Position based Routing

In case of position based routing mechanism, a mobile node within the MANET network broadcast its position co-ordinates as well as its one-hop neighbors. This information can easily be attacked, so therefore privacy-aware mechanism is together with position based routing in order to provide secure communication. PPBR stands for privacy aware and position based routing in which a mobile node mainly takes pseudo identifiers that are usually dynamic and it is also use to provide end-to-end inconspicuousness to other nodes.

3.14.Key management

Certified Authority (CA) is one of the mechanism which provide key management; if it is compromised then entire network can easily be damaged.

3.15.Intrusion detection System

Intrusion detection system is a complete security solution which provides information about malicious activities in the network, it also uses to detect and report about malicious activities.

3.16.Multi-layer Intrusion detection technique

Multi-layer intrusion detection technique is a technique in which an attacker attacks at multiple layers in order to stay below the detection threshold so that they will escape easily whenever a single layer impropriety detects.

IV. PERFORMANCE EVALUATION &DESIGN

4.1 OPNET Usability

One of the most common methods is to conduct research in the fields of networking as well as security is to simulate and evaluate the routing protocol(s) in different kinds of network based scenarios. Our paper is mainly based on two tasks, one is concern with theoretical study and the other one is based on the implementation and experiments of the MANET in security which we perform in OPNET simulation environment. We are using the Optimized Network Engineering Tool (OPNET) software for our simulations.

4.2 Security Metrics Review

There are some quantitative metrics which can be used to evaluate the performance of routing protocol.

1. End-to-end load, throughput and delay
2. Packet sent and received
3. Download response time
4. Efficiency

V. OPNET SIMULATION

There are seven different network scenarios which we implement in our OPNET simulation and they are given below:

1. MANET with DSR routing protocol.
2. MANET with TORA routing protocol.
3. MANET with AODV routing protocol.
4. MANET with routing protocol with respect to security parameters with an intruder.
5. MANET with routing protocol without firewall.
6. MANET with routing protocol with firewall.
7. MANET with routing protocol with firewall as well as with VPN.

5.1Network Scenarios Descriptions

We implement first three scenarios with different routing protocols with profile config, application config and Rx Group config and server for communication and also use 25 mobile nodes for wireless communication. All these devices are explained well in the below network component section. All nodes in the network are configured to run AODV, DSR, and TORA routing protocol one by one in the first three scenarios respectively; and we also use to configure FTP traffic for our result observations. The Rx group config node is added to speed up the simulation. It is configured to eliminate all receivers that are over 1500 meters away. In case of AODV scenario, AODV parameters are used as suggested by RFC and WLAN data rate is 1Mbps.

Second, most important scenario with respect to security policy implementation, in this scenario we use an intruder which is an un-authentic user, how a network would be safe and secure in different network attacks by an intruder.we also implement two mobile ad hoc networks which are sharing information through internet and how we make information secure that's the main task of last three scenarios. In the first scenario we implement network scenario without firewall and VPN and how will we make network free of information security we will discuss this in the next two scenarios. In the next scenario in which we implement our network scenario with firewall setting and we also compare our result with the previous scenario where we implement our scenario without firewall network settings. In the firewall scenario, firewall (Router C) use to configure IP Forwarding Rate, IP Gateway Function, RIP Start Time, RIP Process Mode and Proxy Server Information mechanisms.

In the last scenario, we implement the secure information mechanism by comparing our results. In this scenario we implement firewall as well as VPN network configuration in order to secure our information and safe our communication. In VPN scenario, it configures Virtual Private Network (VPN) attribute configuration details for tunneling supported at the IP layer.

5.2 Network Components

In the above simulation model there are different types of network components are used and these are given below:

[1] There are 25 Wlan workstations with mobile node type are used in first four network scenarios.
[2] There is one Wlan server with mobile node type is used.
[3] There is one application configuration model is used in the network topology.
ACE Tiers information
[4] Application spécification
[5] Voice encoder schèmes
[6] There is also one profile configuration model is used in the network topology.
[7] There is also one dynamic receiver group config node is used in the network model.

VI. RESULT &ANALYSIS

6.1.Throughput among AODV, DSR and TORA

If there is high load traffic then packet drop, in case of high mobility TORA performs better but in other cases it has low throughput. AODV shows best performance in case of throughput.

Delay among AODV, DSR and TORA

DSR and TORA show poor delay due to the reason of its routes because typically their routes are not the shortest. At start of route discovery phase; their routes are not shortest over a period of time due to its node mobility. AODV shows low delay and even it can be better with some fine-tuning.

Load among AODV, DSR and TORA

In case of load TORA's performance is very impressive due to its substantial work to erase routes even when those routes are not in use; we know that TORA shows good performance for small networks with high mobility. AODV also perform well as compare to DSR because byte overhead and packet overhead of AODV are less than DSR's overhead. DSR has high load because of high number of its route discoveries and wide flooding network discovery.

Traffic sent among AODV, DSR and TORA

DSR has high traffic sent as compare to other two routing protocols, after that AODV and TORA respectively.

Traffic received among AODV, DSR and TORA

DSR has high traffic as compare to other two routing protocols, after that AODV and TORA respectively.

Download response time among AODV, DSR and TORA

AODV has high download response time and then TORA and DSR respectively.

6.2 INTRUDER BEHAVIOR (INTEGRITY ASPECT)

An intruder allocate in the network then its block by the server for security by using Net Doctor and security demands in order to avoid intruder behavior from the network. Once server finds an intruder then it will develop complete network route discover map among nodes. We come to know that its an intruder and try to damage our network then through security demand mechanism we block complete application traffic at intruder mobile node because our security system tells us that its an intruder and it should be blocked in the network. By using security demand procedure we blocked its application traffic so that there will be no miss use of the network recourses as well as network information among the users and here we are not talking about the overall traffic.

6.3 INFORMATION SECURITY OVER LINK LAYER AND NETWORK LAYER

We also implement network methodology with respect to firewall. In the first scenario we implemented network without firewall and here we implement with firewall in order to compare page response time; with firewall load on the network increase because it will check traffic packet one by one for the safety of network so that there will no attack by any intruder or any malicious data in the network. As we know that in the last three scenarios we analyze http traffic that's why we discussed page response time. In the second case we have 0.00610 sample sum mean with respect to traffic. If we compare this sample mean with respect to to previous case then we come to know that its high value of page response time as compare to without firewall case because when security increase so it takes more time to give response and thus the page response time increase.

Now as we can see that the response time is high value so we try to overcome that problem thus we implement the idea of VPN which give us more security and also the page response time value decrease. So we implement network methodology with respect to firewall as well as VPN. In the first two scenarios we implemented network without firewall and with firewall and in the last scenario here we implement network with firewall as well as with VPN in order to overcome the difference which we got in the first two scenarios. with firewall increases load on the network because it will check traffic packet one by one for the safety of network so that there will no attack by any intruder and there is no malicious data in the network. In the third case we have 0.00368 sample sum mean with respect to traffic. If we compare this sample mean with respect to to previous two cases then we come to know that now our network is also more secure due to encapsulation of data in VPN tunneling and also the page response time value decreases as compare to with firewall case.

VII. DISCUSSIONS OF SIMULATION ANALYSIS

Here is the overall comparison of AODV, DSR and TORA with respect to delay, throughput, load, traffic sent, traffic received, Upload response time and download response time.

S.No	Parameters	DSR	AODV	TORA
1	Throughput (bits/sec)	2850	3460	2605
2	Delay (sec)	0.0050	0.0019	0.0026
3	Load (bits/sec)	2800	2663	2260
4	FTP Traffic sent (bytes/sec)	53	50	39
5	FTP Traffic received (bytes/sec)	53	50	39
6	Download response time (sec)	0.12	0.70	1.30

7.1.FUTURE WORK

During our thesis, we also find some of the points that can be further researched and explored in the future, such as there should be some standardized intrusion detection techniques can be used and the techniques which already have get further improved. However, in our thesis we recognized that the current evaluation for state-of-the-art wireless security solutions is quite ad hoc. There are some drawbacks which should be improved and some of them are given below:

Lacks of effective analytical tools especially in case of large scale wireless network setting.

- Find out and block an authenticated user, which start miss behaving inside the network.
- The multidimensional trade-offs among security strength.
- Communication overhead.
- Computation complexity.

- Energy consumption.
- Scalability still remains largely unexplored.

There should be developed an effective evaluation methodology and toolkits that will probably be used and need interdisciplinary efforts from different research communities which are working in mobile systems, cryptography, and wireless networking. In case of Transient Multicast security is still an open problem.

REFERENCE

[1] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing*, T. Imielinski and H. Korth, Ed., Kluwer, 1996.

[2] C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," *2nd IEEE Wksp. Mobile Comp. Sys. and Apps.*, 1999.

[3] IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1997.

[4] B. Schneier, *Secret and Lies, Digital Security in a Networked World*, Wiley, 2000.

[5] Shuyao Yu, Youkun Zhang, Chuck Song, and Kai Chen. A security architecture for Mobile Ad Hoc Networks.

[6] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks," *ACM MOBICOM*, 2002.

[7] M. Zapata, and N. Asokan, "Securing Ad Hoc Routing Protocols," *ACM WiSe*, 2002.

[8] B. Dahill *et al.*, "A Secure Protocol for Ad Hoc Networks," *IEEE ICNP*, 2002.

[9] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," *IEEE INFOCOM*, 2002.

[10] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," *ACM MOBICOM*, 2001.

[11] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," *IEEE MILCOM*, 2002. [11] P. Kyasanur, and N. Vaidya, "Detection and Handling of MAC Layer Misbehavior in Wireless Networks," *DCC*, 2003.

[12] Kimaya Sanzgiri, Bridget Dahill, Brian N. Levine, and Elizabeth M. Belding-Royer.

[13] *"A Secure Routing Protocol for Ad Hoc Networks"*. Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, November 2002, pp. 78-90.

[14] Yi-an Huang and Wenke Lee. *"Attack analysis and Detection for Ad-hoc Routing protocols"*. Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Riviera, France. September 2004.

[15] Y. Hu, A. Perrig, D. Johnson. "*Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks"*. Proceedings of The 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), March 2003.

[16] M. Alicherry and A.D. Keromytis, "Securing MANET Multicast Using DIPLOMA", in Proc. IWSEC, 2010, pp.232-250.

[17] Panagiotis, Papadimitratos; Zygmunt, J. Haas;,"Secure Routing for Mobile Ad hoc Networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002