Volume 6, Issue 2, February 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Evaluation of Security Threats and Solutions in MANET'S

Arun Kumar Yadav[*]
Assistant Professor,
Department of Comp. Sc., UCK, K.U.
Kurukshetra, Haryana, India

Karan Singh
Research Scholar,
Department of Comp. Sc. & App. K.U.
Kurukshetra, Haryana, India

Abstract: Bluetooth and IEEE 802.11 standard are some radio technologies which added a new concept for connecting mobile devices via wireless connections; this is known as Mobile Ad hoc Networks (MANETs) where mobile users arrive within the range for communication. This network is made of self-configuring network of wireless links connecting mobile devices/nodes. Without help of any fixed access point nodes make an arbitrary type topology where routers/nodes can move as required for wireless communications. Till date security issues in MANETs are not fully achieved because MANET has dynamic changing topology while communicating between nodes. The security services such as authenticity, data integrity, secure communication between layers and confidentiality are highly required for MANETs. In this paper, different types of attacks, threats in MANET's network layer and some secure routing protocols are discussed.

Keywords: Active and Passive attack, Ad hoc networks, IEEE 802.11, MANET.

I. INTRODUCTION

In area of wireless network communication a new concept Mobile Ad hoc NETwork (MANET) has emerged. MANET do not need any fix access point/fixed infrastructure as in wired network. Instead, the hosts/nodes make a network which is a dynamically (movable) self -configuring network (see in fig. 1).

The communicating node themselves works for dynamically discovering other nodes to communicate in MANET. In MANET, a host enlists other hosts for forwarding packets within range. Each wireless mobile node behaves like a host and as a router forwarding packets for other wireless mobile nodes in the network that may not be within the direct transmission range of each other. Each device in MANET takes part in an ad hoc routing protocol that allows it to find out various multi-hop paths through the network to any other participating node.

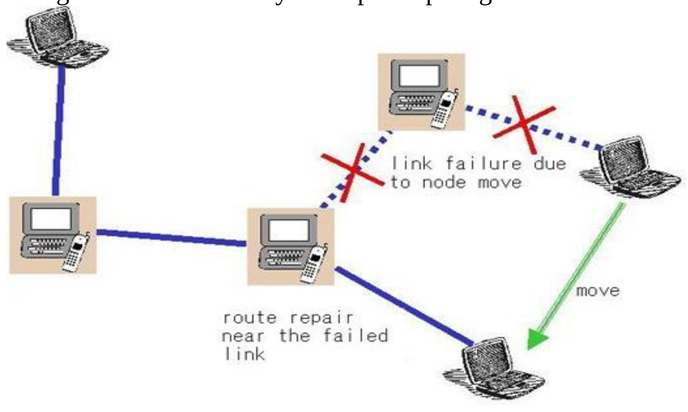

link failure due to node move
move
route repair near the failed link

Fig. 1: Architecture of Mobile Ad-hoc Network (MANET)

The military security purpose and at the time of natural disaster when wired network are destroyed MANETs are most useful. Like other networks MANET also having many security challenges. MANET having some common security threats which also faced in both wired and wireless networks with additional security attacks unique to itself [1]. Due to infrastructure less (boundary is not defined of this network) network it is difficult to discover that which node having malicious activity, junk packets and intentionally drop useful packets at the time of attacks.

1.1 Communication in Mobile Ad hoc Network

Traditional fixed architecture based network need dedicated node for packet forwarding, routing, and network management. In MANETs these tasks are performed by helping each other's by all active nodes. Nodes that are within each other's reachable wireless radio range can communicate directly via wireless links, while those that are not in direct range must dependent on intermediate nodes to act as routers to access/forward messages and this whole process is supported by its multi-hop characteristics. For example, node A can communicate with node D by using the shortest path A-B-C-D as shown in Fig 2. If node P moves out then alternative route to node D will be A-E-F-C-D.

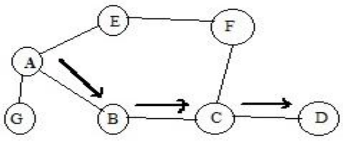


Fig. 2: Communication between MANET's node

1.2 Characteristics of MANETs

The characteristics which MANETs have to achieve are self-configuration, peer-to-peer connection among hosts and dynamic, multi-hop routing protocol to distinguish the MANET from other networks some basic characteristics[1] are as follows:-

- **Autonomous Behavior:** In MANET, each node acts as both host and router. That is it is autonomous in behavior.
- **Multi-hop radio relaying:** When a source node and destination node for a message is out of the radio range, the MANETs are capable of find out various path via any intermediate node which is in direct range of network this is multi-hop routing process.
- **Distributed Operation:** for security, routing and host configuration, centralized firewall is absent here and proposed topology is infrastructure less.
- **Dynamic Network Topology:** The nodes can join or leave the network anytime, making the network topology dynamic in nature.
- **Fluctuating Link Bandwidth:** The effects of high bit error rate are more common in wireless communication. More than one end-to-end path can use a given link in ad hoc wireless networks, and if the links were to break, could disrupt several sessions during period of high bit transmission rate.
- **Limited Energy Resources:** Mobile nodes are characterized with less memory, power and light weight features [2]. Wireless devices are battery powered therefor designing energy efficient mechanisms are an important feature in designing algorithms and protocols. Mechanisms used to reduce energy consumption include (a) communicating devices goes into sleep state when having no any sending and receiving of data (b) routing paths that minimize energy consumption, (c) construct communication and data delivery structures that minimize energy consumption, and (d) reduce networking overhead.

1.3 Goals in Mobile Ad-hoc Networks

Some goals that expected from MANETs are as follows:-

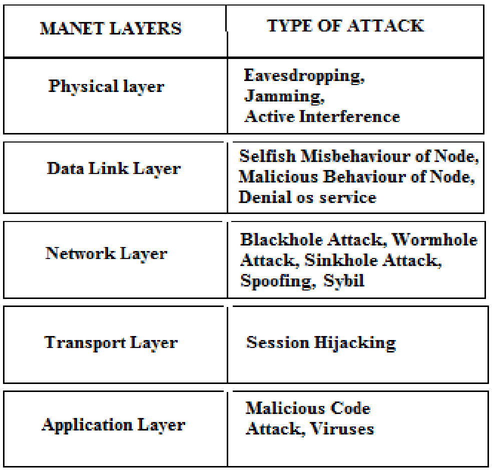
- Secure routing and transfer protocols.
- Quality of services (QoS): QoS defines assurance of data packets delivery at communicating destination.
- Easy discovery of node when any devise want to connect.
- Bi-directional communication between nodes.

1.4 Advantages of MANETs

Some advantages of MANETs [3]:

- Provide access to information and services supporting their movable geographical position in network.
- These networks can be set up at any place and time.
- This is not centralized network. Self-configuring, dynamic, movable network, nodes are also act as routers. Less expensive as compared to wired network.
- Scalable—accommodates the addition of more nodes.
- Improved flexibility.

II. TYPES OF ATTACKS IN MANETs



MANET LAYERS	TYPE OF ATTACK
Physical layer	Eavesdropping, Jamming, Active Interference
Data Link Layer	Selfish Misbehaviour of Node, Malicious Behaviour of Node, Denial os service
Network Layer	Blackhole Attack, Wormhole Attack, Sinkhole Attack, Spoofing, Sybil
Transport Layer	Session Hijacking
Application Layer	Malicious Code Attack, Viruses

Fig. 3: Attacks corresponding to MANET layers

MANET having many security issue. Connections are open and dynamically movable in MANET therefore malicious attacker can attack this network. Attacks corresponding to each layer are shown in Fig 3. These attacks are broadly divided into two types [4]: internal and external attacks.

2.1) Internal attacks:

In internal attack the malicious user wants to gain the access to the network and participate in the network activities for disturbing the communication internally. Attacker can join network by a fake node for accessing network resources. Internal attacks further divided into four types:-

- **Dropping Attacks:** Dropping attacks can destroy end-to-end communications between nodes, if the dropping node is in the network and if behaving like active node. Most of routing protocol has no mechanism to detect whether data packets have been forwarded or not this leads dropping attack.
- **Modification Attacks:** These attacks change the contents of packets and disrupt the communication between MANET's nodes. Sinkhole attacks are the example of modification attacks. In sinkhole attack, the malicious node represents itself as it has shortest path to the destination. In this way malicious node can access rights to important routing information.
- **Fabrication Attacks:** Attacker in fabrication attack provides new fake messages in network between nodes to disrupt the routing process.
- **Timing Attacks:** In this type of attacks, malicious user attracts other nodes by showing itself as a node closer to the source node. Timing attacks technique used in "rushing attacks" and "hello flood" attacks.

2.2) External attacks:

The attacker in external attacks aims to cause congestion, initiates fake routing information for destination nodes or disturb nodes from providing services. External attack has two types:-

a) Active attack is an attack where attacker can modify data packets, injects the packets, drop the packets thus information can be change in messages. Actives attacks examples are in Fig. 3.

b) Passive attacks attacker snoops data over the network without changing it [5]. Passive attack target the confidentiality attribute of network and done for recognize the communication pattern between nodes. Passive attacks are as follows:-

- **Traffic Monitoring:** This passive attack developed for identify the communication parties and functionality and this information taken up by monitoring can lead to launch further attacks .Traffic monitoring attacks not only damaged MANET but also other wireless network such as cellular, satellite and WLAN also suffer from this.
- **Eavesdropping**: The term eavesdrop means overhearing without expending any extra effort. Message transmitted can be overlapped by overhearing and fake message can be injected into network by unintended node.
- **Traffic analysis:** This passive attack used to target the information about the nodes which are communicated with each other and how much data is processed by these nodes.
- **Syn flooding:** This attack is denial of service (DoS) attack. An attacker may repeatedly make much new connection request this result in keep busy the whole network and connection are exhausted or reach a maximum limit.

III. SECURITY ATTACKS IN MANET'S NETWORK LAYER

In MANET network there are security issues in almost each layers (see fig. 3). In this paper main focus is on network layer security threats and attack.

Following are the attacks in network layer:-

3.1 Spoofing:

Malicious node in this attack represents itself as a valid node of that network and pretend another node's identity.

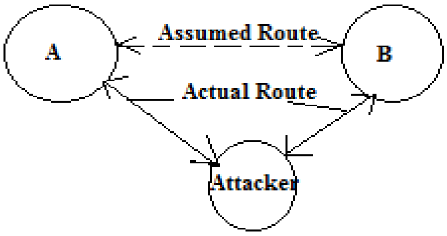


Fig. 4: Spoofing (Man in Middle) attack

Now this malicious node affects communication, sniffs and disturbs access rights [6].

3.2 Blackhole Attack:

In this type of attacks, malicious node captures the request form source and sends response to source behaving like destination node [7]. All the packets from source then consume by malicious node are destroyed see in (in figure 5).

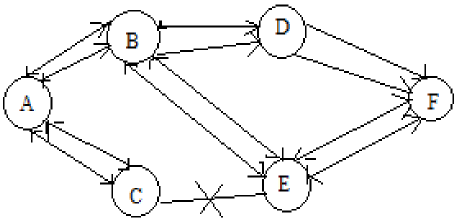


Fig. 5: Blackhole attack

When source node wants to communicate to destination node, it starts the path discovery process. Then malicious node catches request of source node, and immediately sends response to source. If reply from node malicious node reaches first to the source than the source node then ignores all other reply messages from network and begin to send packet via malicious route node. As a result, all data packets are consumed or lost at malicious node.

3.3 Wormhole Attack*:*
An attacker records a new fake optimal path which is external shortest path between nodes.

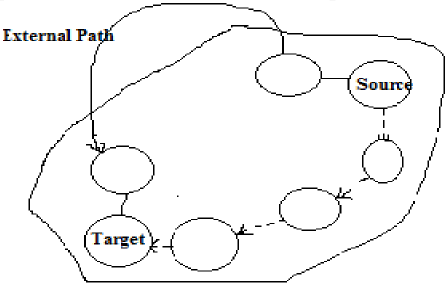


Fig. 6: Wormhole attack

This shortest path acts as a tunnel between nodes and being a shortest path this tunnel is selected as new route by routing algorithms for data transmission[6] [8] and in this way real transmission path destroyed (see Fig. 6). This tunnel is referred as wormhole.

3.4 Sybil Attacks*:*
In Sybil attack single node can take up the identity of a group in network, can assume role of many nodes and can monitor them at a time [2] [9] (see in Fig. 7). This process degrades the performance of this Sybil group.

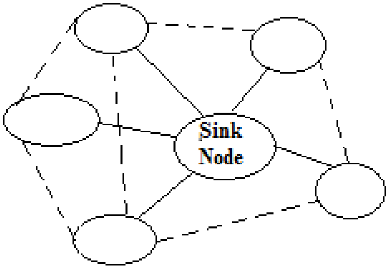


Fig. 7: Sybil attack

3.5 Fabrication:
Attacker in fabrication attack [10] provides new fake messages in network between nodes to disrupt the routing process. Such kind of attacks can be difficult to identify because these acts as valid routing mechanism, especially in the case of fabricated routing error messages, which shows that a neighbor moved out of network and not connected.

3.6 Sinkholes*:*
In a Sinkhole attack [6] [11], the attacker sends fake routing information via a node showing that it has a shortest path to the target which causes other nodes in the MANET to route data packets through this malicious node. Thus, the malicious node gets rights to access all the traffic for any damage.

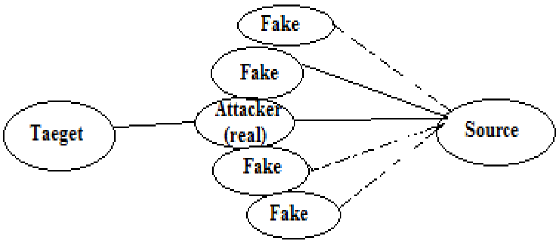


Fig. 8: Sinkhole attack

IV. SECURE AD HOC ROUTING PROTOCOLS

In last section the attacks are mentioned in network layer, to protect from these attacks some secure protocols are available. Several solutions proposed by researcher like DSDV [12] [13] and AODV [14]. Since routing is an important function for ad hoc networks, therefore this should be as secure as possible. Another important thing is analysis the examination of assumption, governing protocols and requirements that each solution depend on. A protocol might be able to satisfy certain security issues but its functional requirements [15] and way of its implementation might ruin its successful employment. These solutions can be categorized in three parts:-

4.1 Symmetric Cryptography Solutions

- Secure Efficient Ad hoc Distance Vector (SEAD)
- Secure Routing Protocol (SRP)
- Ariadne

4.2 Asymmetric Cryptography Solution

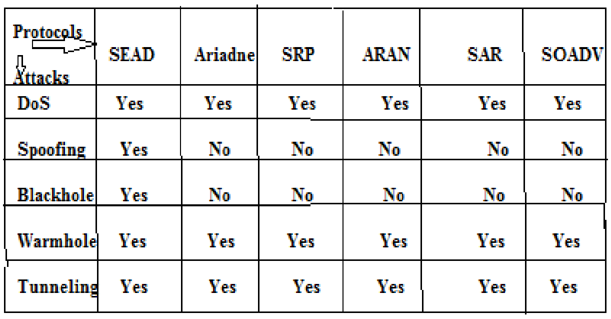
- Authenticate routing for ad hoc network (ARAN)
- SAR

4.3 Hybrid Solutions

- Secure Ad hoc On-demand Distance Vector (SAODV)

Comparative study [9] of these protocols and corresponding to their type of attack is given in table 1. SEAD, Ariadne, SRP, ARAN, SAR and SOADV protocols and by which attack these protocol protects the MANET are in table 1.

Table 1: Comparison study table for Secure Routing Protocols



Protocols → ↓ Attacks	SEAD	Ariadne	SRP	ARAN	SAR	SOADV
DoS	Yes	Yes	Yes	Yes	Yes	Yes
Spoofing	Yes	No	No	No	No	No
Blackhole	Yes	No	No	No	No	No
Warmhole	Yes	Yes	Yes	Yes	Yes	Yes
Tunneling	Yes	Yes	Yes	Yes	Yes	Yes

V. CONCLUSION

In this paper, one can see that attacks against the MANETs may depend on 1) on which communication layer the attacks are targeting, 2) Which environment the attacks are launched, and 3) What level of ad hoc network mechanisms is targeted?

There are several attack characteristics that must be considered in designing any security measure for the ad hoc network. Due to nature of mobility and open media MANET are much more prone to all kind of security risks as covered. As a result, the security needs in the MANET are much higher than those in the traditional wired networks. After that some secure protocols also discussed for solve security problems. A new model can be designed using these secure protocols which can handle these attacks. For achieve security all the nodes can be authorized by using the "digital certificate" or "digital signature". By using authentication process malicious node (attacker) can prevent from entering into the network.

REFERENCES

[1] Mr. Vikas Kumar, Mr. Amit Tyagi, Mr. Amit Kumar, **"**Mobile Ad-hoc Network: Characteristics, Applications, Security Issues, Challenges and Attacks", IJARCSSE, Volume 5, Issue 1, January 2015

[2] Sarvesh Tanwar, Prema K.V., "Threats & Security Issues in Ad hoc network: A Survey Report", IJSCE, Volume-2, Issue-6, January 2013

[3] Aditya Bakshi, A.K.Sharma, Atul Mishra, **"**Significance of Mobile AD-HOC Networks (MANETS)", IJITEE, Volume-2, Issue-4, March 2013.

[4] Himadri Nath Saha , Dr. Debika Bhattacharyya , Dr. P. K.Banerjee, Aniruddha Bhattacharyya ,Arnab Banerjee , Dipayan Bose, "study of different attacks in MANET with its detection & mitigation schemes", IJAET/Vol.III/ Issue I/page-no383-388January-March, 2012.

[5] Satyam Shrivastava, Sonali Jain, "A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network", IJCSET, Vol. 4 ,page-222, 03 Mar 2013.

[6] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", IJEAT, Volume-1, Issue-5, June 2012

[7] Aarti and S.S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", IJARCSSE, Vol 3, Issue 5, May 2013.

[8] Yih-Chun Hu, Adrian Perrig, David B. Johnson, “Wormhole Attacks in Wireless Networks”, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.

[9] Kuldeep Sharma, Neha Khandelwal, Prabhakar M, “An Overview Of security Problems in MANET”.

[10] Sachin Lalar, “Security in MANET: Vulnerabilities, Attacks & Solutions”, IJMCR, Vol.2 , Jan-Feb 2014**.**

[11] Sonal R. Jathe1, Dhananjay M. Dakhane, “Indicators for Detecting Sinkhole Attack in M”NET", IJETAE, Volume 2, Issue 1, January 2012

[12] Monis Akhlaq, M. Noman Jafri, Muzammil A. Khan and Barber Aslam, “Addressing Security Concerns of Data Exchange in AODV Protocol”, World Academy of Science, Engineering and Technology 16, pp. 29-33, 2006

[13] Pradip M. Jawandhiya et. al. / International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071

[14] C. Perkins, E. Belding-Royer and S. Das, “Ad-Hoc On-Demand Distance Vector (AODV) Routing”, RFC3561, July 2003.

[15] Sunil taneja and Ashwani Kush, “ A Survey of Routing Protocols in Mobile Ad-Hoc Networks”, International Journal of Innovation, Management and Technology, Vol. 1, No. 3, 279-285, August 2010.