ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

A Survey Report on the Security Threats and Challenges in MANET

S.Divya gnanarathinam [1], T.Varalakshmi [2], P. Theerka [3]

P.G. Student, Dept of IT, Bannari Amman Institute of Technology, Sathyamangalam, Erode, India[1]

P.G Student, Dept of IT, Bannari Amman Institute of Technology, Sathyamangalam, Erode, India[2]

P.G Student, Dept of IT, Bannari Amman Institute of Technology, Sathyamangalam, Erode, India[3]

ABSTRACT: Due to the rapid improvement in radio technologies such as Bluetooth and IEEE 802.11, a new concept of networking has become apparent; this is known as ad hoc networking where potential mobile users are brought within a particular range for communication. Due to the speedy development of network for both military and commercial distributed and group based applications, security is a crucial necessity in mobile adhoc network (MANETs). MANETs are more in danger to security attacks due to the lack of a trusted centralized authority and limited resources when compared to wired networks.In this paper, we study the threats faced by an adhoc network and the security goals to be achieved. We suggest a brief introduction to the types of attacks and possible counter measures to prevent the attacks of the Mobile Adhoc Networks.

KEYWORDS: MANET, Security, IEEE802.11, vulnerability, authentication, threats, ad hoc network.

I. INTRODUCTION

AD-HOC networks are a new paradigm of wireless communication for mobile hosts or nodes. Ad hoc networks do not depend on any fixed infrastructure. Instead, hosts depend on each other to keep the network in connection. The nodes of an adhoc network are all mobile so that they can communicate with each other within a particular radio range through direct wireless links or multihop routing techniques.

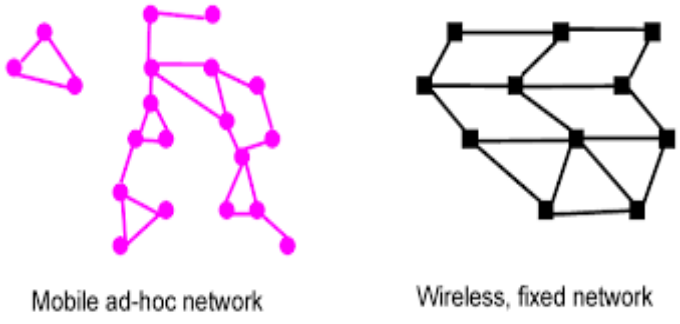

Figure 1: MANET and Wireless Fixed Network

1.1 Mobile Ad-hoc Network Characteristics

Ad-hoc network is becoming popular for its unique characteristics. For the sake of obtaining some interesting features, ad-hoc network should have different properties such as peer-to peer among hosts; protocol for multihop routing, the network is autonomous and also auto configured and moreover the network is dynamic. Some of the characteristics which differentiate ad hoc wireless networks from other networks are:-

- Dynamic Network Topology
- Multi-hop radio relaying

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

- Repeated breakage of links due to mobile nodes
- Constraint resources such as bandwidth, computing power and battery lifetime etc.,
- Instant deployment
- Communication channel is highly insecure in wireless communication. Overhearing and concealing can be done very easily.
- Fluctuating Link Capacity
- Due to limited power in the mobile nodes, denial of service is created. In this case, additional transmissions or expensive computations are caused by the attacker.

II. RELATED WORK

S. Madhavi et al have examined the vulnerabilities of wireless networks and included intrusion detection in the Security architecture for mobile computing environment. A system called MIDS (Mobile Intrusion Detection System) had been proposed which is suitable for multi-hop ad-hoc wireless networks. This proposed system detects nodes misbehaviour, and also the anomalies in packet forwarding, such as dropping of intermediate nodes or delay of packets.

Vladimir Berman et al has recommended directional antennas and intelligent multipath routing to enhance end-to-end data confidentiality and data availability in terms of outsider attacks. The goal is to distort rogue attempts to gain unauthorized access to classified information or disrupt the information flow. The cooperation between the physical, link, and network layers is examined.

Haiyun Luo et al have proposed a self-securing approach, in which multiple nodes are coordinated and joined together to provide authentication services for other nodes in the network. They have first formalized a localized trust model which lays the foundation for the design. They have further proposed refined localized certification services and developed a new scalable share update to withstand more powerful adversaries.

III. SECURITY GOALS FOR AN AD HOC NETWORK

Availability: This ensures survivability irrespective of the Denial of Service (DOS) attacks. In the physical and media access control layer, the attacker can use jamming techniques to block the communication on the physical channel. The attacker can damage the routing protocol on the network protocol.
Confidentiality: This ensures that particular information is never revealed to unauthorized entities.
Integrity: Message which is being transmitted over the network is never corrupted.
Authentication: Enables a node to ensure the identity of the peer node it is communicating with. Without knowing the identity, an attacker would impersonate a node, thus acquiring unauthorized access to resource and sensitive information.
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 steal any useful information.
Attacks using fabrication: Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect by the user.

IV. SECURITY ATTACKS AND ITS COUNTER MEASURES

Attacks on a network are divided into two categories – (i) Internal attack and (ii) External attack.
In Internal attack , the attacker wants to acquire the access to the network and to get involved in the network activities, either by some malicious attack to get the access to the network as a new node, or by directly finding the ground of a current node and uses the node as the way to do its malicious behaviours.
In External attacks, the attacker aims to cause congestion and to disturb the nodes from providing its services or to propagate fake routing information
Current MANETs are extremely vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is an attack in which the misbehaving node has to fetch some energy costs in order to perform

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

the threat. On the other hand, passive attacks mainly occur due to lack of cooperation between the nodes with the idea of saving the energy selfishly.

I. **Black hole:**

In a black hole attack, a malicious node introduces incorrect route replies to the route requests it receives in order to advertise itself as the node which has the shortest path to the destination. These fake replies can be forged to divert network traffic through this malicious node for eavesdropping, or else to simply attract all traffic to it in order to carry out a denial of service attack by dropping the packets which are been received.

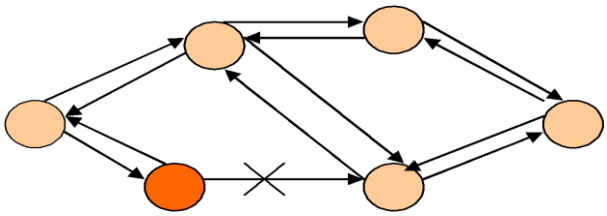

Figure 2: Problem of black hole

II. Wormhole:

In a wormhole attack, the attacker receives the packets at one location in the network, and "tunnels" them to another node or edge in the network, and then repeats them into the network from that point. With respect to the tunnelled distances which are longer than the normal wireless transmission range of a single hop, it is easy and simple for the attacker to make the tunnelled packet arrive with better metric when compared to a normal multihop route. For example, by the usage of a single long directional wireless link or through a direct wired link to a conspiring attacker. For the attacker, it is also possible to forward each bit of data over the wormhole directly. The attacker need not wait for an entire packet to be received before beginning to tunnel the bits of the packet. This can minimize the delay introduced by the wormhole. If the attacker tunnels the data truthfully and accurately, no damage or harm is done; because the attacker actually provides a useful service in connecting the nodes in the network more efficiently. However, in the wormhole the attacker has the very powerful position when compared to other nodes in the network, and the attacker could make use of this position in a variety of ways. Wormhole attacks are a major threat to mobile adhoc routing protocols. For example, when this type of wormhole attack is used against an on-demand routing protocols such as Dynamic Source Routing(DSR) or Adhoc On Demand Vector routing(AODV), the attacker could prevent the discovery of any routes through the wormhole.

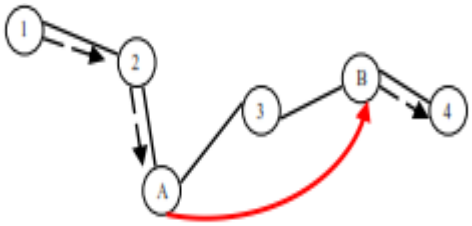

Figure 3: A wormhole attack performed by colluding malicious nodes A and B

III. Spoofing attack:

Spoofing is a special case of integrity attacks in which a compromised node impersonates an authorized one due to the lack of authentication in the ad hoc routing protocols. The major outcome of this spoofing attack is the exaggeration of the network topology which may cause network loops or partitioning. Integrity and authentication is lacking in this routing protocols which leads us to the fabrication attacks that may result in erroneous and false routing messages.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

IV. Rushing attack:

Rushing attack is a type of attack which results in denial-of- service when used against all previous on-demand ad hoc network routing protocols. For example, DSR, AODV, and other secure protocols which are based on them such as ARAN and SAODV cannot discover their routes longer than two hops with respect to this attack. Therefore, we should develop Rushing Attack Prevention (RAP) which is a generic defense against the rushing attack for all on-demand routing protocols that can be applied to any of the existing on-demand routing protocols to allow that protocol to withstand and resist the rushing attack.

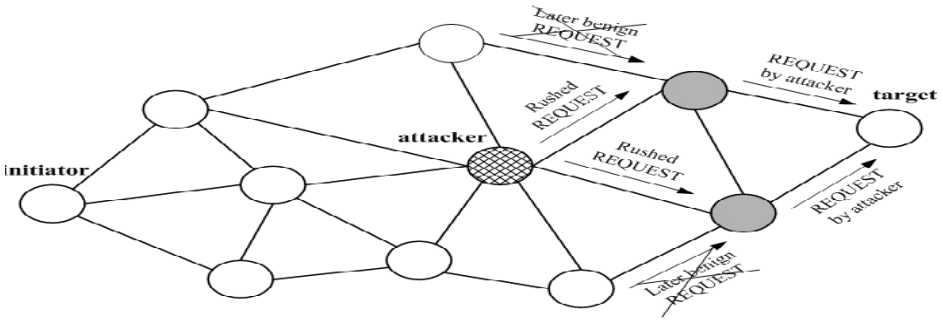

Figure 4: Rushing Attack example

V. Masquerading:

When the neighbour does the acquisition process, an intruder from outside could masquerade a nonexistent or existing IS by tethering itself to communication link and illegally affixing in the routing protocol domain by compromising the authentication system.

VI. Denial of Service:

The powerful attack in Adhoc Networks is the Denial of service attacks which focus at the complete disruption of the routing function and hence result in the disruption of the entire operation of the ad hoc network. Specific occurrences of denial of service attacks include the overflow of the routing table and the sleep deprivation torture. In this routing table overflow attack, the malicious node overloads the network with false route creation packets in order to have the resources of the participating nodes and damage the establishment of authorized routes. Then the other attack which is the sleep deprivation torture attack aims at the consumption of batteries of a specific node by keeping it involved in routing decisions constantly.

Table 1. Security Attacks on each layer in MANET

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding, Traffic analysis, monitoring, disruption, MAC (802.11), WEP, Weakness Jamming, interceptions, eavesdropping
Network layer	Wormhole, black hole, Byzantine, flooding, resource consumption, location disclosure attacks.
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Table 2. Security Solutions for MANET

Layer	Security Issues	Solutions
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses	Adequate security solution Firewalls, IDS etc.
Transport layer	Authentication and securing end-to- end or point-to- point communication through data encryption	Adequate security solution use of public cryptography (SSL, TLS, SET,PCT) etc.
Network layer	Protecting the ad hoc routing and forwarding protocols	No effective mechanism for Source authentication and message integrity mechanisms to prevent routing message modification, but now using some Securing routing protocols (e.g. IPSec, ESP, SAR, ARAN) to overcome black hole, impersonation attacks, packet leashes, SECTOR mechanism for wormhole attack etc. final solution is inadequate secure routing for ad hoc network.
Data link layer	Protecting the wireless MAC protocol and providing link layer security support	No effective mechanism to prevent traffic analysis and monitoring, secure link layer protocol like LLSP, using WPA etc. finally anonymity is inadequate for adhoc network.
Physical layer	Preventing signal jamming denial-of- service attacks	Using Spread spectrum mechanisms e.g. FHSS, DSSS etc.

V. CONCLUSION

In this paper, we have surveyed several attacks which occur in the several different layers in the ad-hoc networks. We have also reviewed about the several security concepts in an adhoc network. We have also scrutinized the security challenges and the ways to overcome those challenges in the ad-hoc network. A brief abstract of the characteristics of the mobile ad-hoc network is also been discussed. Lot of research is still under discussion about the security threats in a mobile adhoc network and the solutions to overcome them. Finally, this survey report can be very well used for the research works based on the security and its challenges in MANET's.

REFERENCES

[1] I.Ilyas, Mahammad,"The hand books of Ad hoc Wireless Networks-II series" CRC Press LLC, USA.
[2] C.Sivarammurthy, B.S.Manoj,"Adhoc wireless networks- II edition", Pearson education of India.
[3] Elizabeth M. Royer, Charles E. Perkins," An Implementation Study of the AODV Routing Protocol" IEEE 2000, vol no.7803-6596-8/00.
[4] NedaMoghim, FaramarzHendessi, NaserMovehhedinia, "An improvement on wireless ad hoc network routing based on AODV" IEEE 2002, vol.no.7803-7510-06/02.
[5] Jin Taek Kim, Jeong-Ho Kho, Chang-Young Lee, Do- Won Lee, Cheol-Soo Bang, Geuk Lee," A Safe AODV Security Routing Protocol"-International Conference on Convergence and Hybrid Information Technology 2008, IEEE 2008,vol no. 978-0-7695-3328-5/08.
[6] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc. of

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

IEEE Inforcom, 2002.

[7] Y o n g g u a n g Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *Ad Hoc Networks Technologies and Protocols (Chapter 9)*, Springer, 2005.

[8] P a n a g i o t i s Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 31)*, CRC Press LLC, 2003.

[9] Y i -an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in *Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks*, Fairfax, Virginia, 2003, pp. 135 – 147.

[10] Sergio Marti, T. J. Giuli, Kevin Lai and Mary Baker, Mitigating routing misbehavior in mobile ad hoc networks, in *Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom'00)*, pages 255–265, Boston, MA, 2000.

[11] Jiejun Kong, Xiaoyan Hong, Yunjung Yi, JoonSang Park, Jun Liu and Mario Gerlay, A Secure Ad-hoc Routing Approach Using Localized Self-healing Communities, in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 254–265, Urbana–Champaign, Illinois, 2005.

[12] Y. Hu, A. Perrig and D. Johnson, Wormhole Attacks in Wireless Networks, *IEEE Journal on Selected Areas inCommunications, Vol. 24, No. 2*, February 2006.