ISSN 2319-2720

Volume 3, No.3, July – September 2014

International Journal of Computing, Communications and Networking

Available Online at http://warse.org/pdfs/2014/ijccn03332014.pdf

A SURVEY ON SECURITY ISSUES AND DEFENSE MECHANISMS IN MANETs

Deepa M[1], Parvathi M[2]

[1]PG Scholar, Nandha Engineering College, Erode, mm.deepa@gmail.com
[2]Associate Professor, Nandha Engineering College, Erode, mparvathicse@gmail.com

ABSTRACT

Mobile ad hoc networking has become the recent trends and challenging areas of wireless technology which promises their presence in our lives. There are diversity of variables in ad hoc network which have different impact on security issues and design. Certainly the risk of security in ad hoc network increases when the distance between the nodes increases. If the nodes are very far the risk also increases. Standard information security measures such as encryption and authentication do not provide complete protection, and, therefore, intrusion detection and prevention (IDP) mechanisms are widely used to secure MANETs. This paper focuses on the various types of attacks in the network layer and the protective measures proposed in the literature. Also a comparative analysis of various protection schemes is included in this paper.

Keywords: attacks, authentication, encryption, intrusion

1. INTRODUCTION

A MANET is a collection of mobile nodes that communicate over wireless links which do not have a centralized infrastructure and management system. Since the nodes are mobile, the network topology changes rapidly over time. Since the network does not have a centralized infrastructure, the nodes must themselves discover the network topology and delivery of messages.[1]

The dynamic nature of the network has posed serious communication issues such as noise and interference. In addition, the links typically have a very limited bandwidth than a wired network. Each node in an ad hoc network can function as both a host and a router, and the network control is distributed among the nodes. The freedom of mobility of nodes makes MANETs easy to construct at low cost. Due to their mobility nature MANET is used in applications such as military, emergency situations, disaster and so on. The most challenging task of MANET is the constraints on bandwidth and power.

1.1 Network Security in MANETs

Security is a very difficult task to achieve in mobile ad hoc networks. There are different variables which makes security difficult to achieve. . Especially environment, topology, dynamic network, infrastructure affect the security in the network. There are other complications such as frequent topology changes, unreliability and limited bandwidth which add threats to network security. Various protocols and intrusion detection mechanisms have been proposed as a solution for securing the network with the consideration of the above described variables.

2. VULNERABILITIES OF THE MOBILE AD HOC NETWORKS

2.1 Lack of security

The mobility of nodes in mobile ad hoc network makes the network insecure. The nodes are not restricted to leave or move both inside and outside the network. This makes the ad hoc network vulnerable to attacks. The mobile ad hoc network is not protected with firewalls or gateways which attracts the malicious nodes to attack the targets.[6].

2.2 Dynamic Topology

Mobile Ad hoc network nodes are independent and free to move. The freedom of mobility makes the network topology dynamic. Due to dynamic topology It is hard to track the malicious node in a network. Rather than outside attacks the threats from inside the network is more challenging.[6]

2.3 Lack of Centralized Management

Due to lack of centralized infrastructure in mobile ad hoc networks, it is very hard to monitor the traffic in a highly dynamic and large scale network. This problem results in failure of transmission of data.[6]

2.4 Power Supply

The mobile ad hoc network is battery operated which is a bounded power supply. Due to bounded power supply method the MANET is posed to several vulnerabilities. The first problem is denial – of – service attacks which disrupts the routing operations. So, any type of failure in mobile ad hoc network causes many problems. The problem also occurs when any node suffers from running off battery power. [6]

3 SECURITY THREATS IN MANETS

The mobile ad-hoc networks are prone to many different types of attacks. Since ad hoc networks are infrastructureless networks, problem fixing is very difficult. Current MANETs are basically vulnerable to two different types of attacks: active attacks and passive attacks.[7]

3.1 Passive Attacks

Passive attacks are the one where the intruder enter into the network, analyse the traffic and obtain some valuable information without disturbing the operation of the network and the traffic flow. This leads to the problem of breaching the confidentiality of the network such as topology and the locality of nodes. Some examples of passive attacks are as follows:

3.1.1 Eavesdropping

The wireless network is equipped with a transceiver, where a message sent by a node can be heard by every node in the network within the radio range. If no standard security measures had been done the intruder can get some useful information without the knowledge of the sender and receiver.

3.1.2 Traffic Analysis

Traffic analysis is an attack where the attackers listen to the traffic and identify the location of the target nodes based on the communication pattern and the characteristics of the information transmission .Extraction of information can be one even if the information are well encrypted. Though this type of attack does not pose serious threat to the network but it constitutes the violation of confidentiality

3.2 Active Attacks

Active attacks are the attacks which disturb the network operations and can degrade the performance of the network drastically. The severity may go up to bringing down the network and may cause network outage. In this type of attack, the intruders get into the network. They can modify, intercept, fabricate or drop the packets which are being transmitted. Attack can be caused by a single intruder or multiple intruders.

3.2.1 Attacks using Modification

Modification is a type of attack where an unauthorized person can enter into the network and gain access and also tampers with the asset. A malicious node can redirect the traffic and conduct DOS attacks by modifying message fields or by forwarding routing message with false values.

3.2.2 Attacks through Fabrication

Fabrication is an attack in which an authorized party not only gains the access but also inserts counterfeit objects into the system. In MANET, fabrication results in the generation of false routing messages. These attacks are very difficult to verify as they behave as original messages.

3.2.3 Lack of Cooperation

Mobile ad-hoc networks rely on the cooperation of all the participating nodes. The MANET is more powerful when more nodes more nodes transfer traffic. In this case any node may fail to cooperate to preserve its own resources and using the resources of other nodes. These nodes are called as selfish nodes. The following are the types of active attacks.

3.2.4 Black hole attack

In a black hole attack a malicious node advertises itself as a valid path to the destination. The attacker can consume the packet without forwarding to the destination. As a result the packets are simply dropped or forwarded to another location which was not actually the target.[5]

3.2.5 Neighbour attack

A node on receiving the packet records its ID in the packet before forwarding the packet to the next node. However in neighbour attack, the attacker forwards the packet without specifying its ID to the next node. This results in an interruption in packet forwarding because the nodes of different communication range believe as neighbours. The attacker leaves the path as soon as the false messages are sent.

3.2.6 Wormhole attack

Wormhole attack is the most powerful attacks in MANETs. In this type of attack two or more malicious nodes cooperate between them and exchange message along the existing path. This attack is also known as tunnelling attack. These attacks are very severe and even penetrate channels which are confidential. The severity is high because of the participation of two or more malicious nodes.

3.2.7 DoS (Denial of Service) attack

In this type of attack, an attacker prevents the legitimate users from accessing a particular resource. Routing table overflow is a form of denial of service attack, in which the malicious node floods the network with routing packets and consumes the bandwidth of the network. This prevents the route establishment. Sleep deprivation consumes the battery power of a specified node by making constant routing decisions

3.2.8 Information Disclosure attack

In this attack, the unauthorized nodes in the network gains confidential information from the compromised nodes. The information such as network topology, location of nodes and optimal routes to the destination may be leaked by the compromised nodes. Attacks such as location disclosure and traffic analysis belong to this category.

3.2.9 Rushing attack

On demand routing protocols are more vulnerable to this type of attack. During the route discovery process, the attacker node receives the route request packet and floods the entire network. As the nodes already receive the duplicate packets, it discards the legitimate route request send by the nodes.

3.2.10 Jellyfish attack

This attack is very similar to black hole attack. The attacker intrudes into the network and when it receives the data packet, it delays forwarding the data packet for some time of no reason. This degrades the network performance and results in high end to end delay. Real time applications are adversely affected when there is high end to end delay.

3.2.11 Byzantine attack

It is also called as impersonation attack. In this attack, one or more compromised intermediate nodes carries out the attack. The result of the attack may be creation of routing loops, packet dropping which degrades the routing performance of the network. Also the routing table may contain false routing updates.

3.2.12 Sybil attack

In the Sybil attack, an attacker creates large number of identities in a highly reputed system. A malicious node can behave as if it is having a large influence and substantially controls the entire network.

3.2.13 Misrouting attack

In the misrouting attack, a malicious node redirects the routing message and sends data packet to the wrong destination. In this type of attack, either the destination address is modified or the next hop node.

3.2.14 Resource consumption attack

In this attack, a malicious node consumes the resources such as battery power, bandwidth, etc. of other nodes in the network. The attacks may be in the form of unnecessary route request packets or frequent generation of beacon packets.

3.2.15 Routing table poisoning

In this attack, a malicious node sends false routing updates to other uncompromised nodes. As a result, the routing table contains false updates. Network congestion and inaccessibility are the effects of this attack

3.2.16 Gray hole attack

In this attack, an attacker drops all data packets except the control messages and route through the network. This type of dropping is very difficult to detect.[8] [9]

4. CHALLENGES IN MANETS

Security is the major concern in mobile ad hoc networks because of its unique characteristics such as lack of infrastructure and dynamic topology. There are interesting challenges in a WMANET, in addition to security. The challenges include

- Multicast routing protocol design
- MAC layer protocols development
- Efficient load balancing
- End-to-End Quality of Service (QoS) provision
- Power efficient protocol design
- Cross-layers design for wireless networks
- Multipath routing

5. DEFENSE MECHANISMS

Following are the various defense mechanisms. Table1 shows defense mechanism for various attacks.

5.1 Defence against Packet Dropping

Packet dropping is one of the serious threats in MANETs and significant research has been conducted to protect against such attacks. The authors[4] proposes cooperative participation of nodes where each node monitors the behaviour of neighbours. If any node is found dropping the packets the trust value is collected from the neighbours of the suspicious node. If the suspicious node has a low trust value compared with the majority of the nodes a global alarm is raised.

Marti et al. [3] proposed a mechanism consisting of two parts: watchdog and pathrater. Watchdog uses promiscuous listing to identify the nodes that drop packets and pathrater maintains the path of every node and decreases its rating when it learns its packet dropping behaviour from watchdog. To mitigate the effect of packet dropping, path rater selects the path based on the nodes' rating.

Table1: Defense mechanism for various attacks

ATTACK TYPES	**DEFENSE TECHNIQUES**
Data packet dropping	Trust-based approach[4]
	Watchdog and Path rater[3]
Black hole	Topology graph[2]
	RREP sequence number of intermediate nodes[12]
Grey hole for DSR	Aggregated signature algorithm[8]
Grey hole for AODV	Monitoring behaviour in terms of RREP
Rushing attack	Secure Routing protocol [10] SMT protocol [16]

5.2 Defence Against Black Hole Attacks

There are several mechanisms of Defense proposed against black hole attacks. Black hole attack can be classified as single black hole attack and collaborative black hole attacks. The detection scheme uses on a neighbourhood-based method to recognize the black hole attack. To build a correct path to the destination routing recovery protocol is used. In [12] a black hole detection scheme based on sequence number checking of the RREP packets. They considered a scenario where an intermediate node is an attacker and suggested that, whenever a node sends a RREP back to a source node, the intermediate node should also generate a request for a sequence number to the destination node.

5.3 Defence Against Grey Hole Attacks

Xiaopeng and Wei [8] proposed an aggregated signature algorithm for grey hole detection. This uses DSR routing protocol. Every node in this scheme uses signature for a grey hole detection for forwarding packets. Another technique was proposed in the literature in which a Distributed Certificate Authority (DCA) to update key management information. This helps the detection process that uses the aggregate signature algorithm.

Table 2: Analysis of Various Security Techniques

SCHEMES	**TECHNIQUES**
EAACK[1]	Acknowledgement based IDS which uses digital signature to prevent forged acknowledgement packets.
SPREAD[13]	Uses multipath routing where secret message is transformed into multiple shares and deliver via different paths to the destination
USOR[14]	Combination of group signature and ID-based encryption for route discovery. Protects against inside and outside attacks
SPAWN[15]	The concept of observer obscurity is used for secure privacy preserving
PRISM[11]	Location centric on demand routing scheme which uses secure group signature scheme and location information to prevent against inside and outside attacks

5.4 Defence against Rushing Attacks

In [16] the authors proposed a Secure Message Transmission (SMT) protocol that ensures a secure end-to end data forwarding protocol. They suggested that SMT can be used mainly for protecting the data forwarding operation, while route discovery procedures that are vulnerable to routing attacks such as rushing attacks can be secured using the Secure Routing Protocol (SRP) [10], an Internet Draft earlier proposed by the same authors in an attempt to mitigate the effects of misbehaving nodes in routing operations. However, they did not evaluate the effectiveness of SRP against routing attacks.

5.5 Analysis of various security techniques

Table 2 shows various security techniques which is described below. EAACK scheme is Acknowledgement based IDS which uses digital signature to prevent forged acknowledgement packets. SPREAD uses multipath routing where secret message is transformed into multiple shares and deliver via different paths to the destination. USOR uses a combination of group signature and ID-based encryption for route discovery. It protects against inside and outside attacks. The concept of observer obscurity is used for secure privacy preserving in SPAWN. PRISM is a location centric on demand routing scheme which uses secure group signature scheme and location information to prevent against inside and outside attacks.

6 CONCLUSION

MANETs has become the recent technology trend because of its infrastructureless nature and application in situations such as emergencies and disaster. This paper focuses on the state –of- art routing attacks and the protection techniques. Though various protection techniques have been implemented, providing security in all scenarios seems critical. Various security problems have been analysed and all the solutions might not be cost effective. Research should focus on the feasibility of security techniques and prevention from unexpected attacks to achieve MANET a reliable network.

REFERENCES

1. Elhadi m. shakshuki , nan kang, and tarek r. sheltami, " **EAACK—A Secure intrusion-detection system for manets**", *IEEE transactions on industrial electronics*, vol. 60, no. 3, march 2013.

2. E.Padilla, N.Aschenbruck, P.Martini, M.Jahnke and JTolle, "**Detecting Black Hole Attack in Tactical MANETs using Topology Graph**",Proc.IEEE Conference on Local Computer Networks, 2007

3. S. Marti, T.J. Giuli, K.Lai and M. Baker,"**Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks**", Proc. International Conference on Mobile Computing and Networking, pp 255- 265, 2000.

4. J. Sen, M. Chandra, P. Balamurlidhar, S.G. Harihara and H.Reddy, "**A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad hoc Networks**", *Proc. IEEE Conference on Telecommunication and Malaysian International Conference on Communication (ICT-MICC)*, 2007

5. Jaydip Sen, Sripad Koilakonda , "**A mechanism for detection of cooperative black hole attack in mobile ad hoc networks**", *Intelligent systems, modelling and simulation (ISMS),2011 Second International conference*

6. Ernesto Jiménez Caballero, "**Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem**", 2006.

7. A. Nadeem and M.P Howrath, "**A Survey of MANET Intrusion Detection &Prevention Approaches for Network Layer Attacks**",*IEEE Communications & Tutorials*,Vo1 15,No.2 , 2013

8. G.Xiaopeng and C.Wei, "**A Novel Grey Hole Attack Detection Scheme for Mobile Ad-Hoc Networks**", *Proc. IFIP International Conference on Network and Parallel Computing*, 2007.

9. C. Wei, L. Xiang, B. Yuebin and G.Xiopeng, "**A New Solution for Resisting Grey Hole Attack in Mobile Ad Hoc Networks**", *Proc. IEEE Conference on Communication and Networking*, China 2007.

10. P. Papadimitratos, Z.J. Haas and P. Samar, "**The Secure Routing Protocol (SRP) for Ad Hoc Networks**", *IETF Internet Draft*, December 2002

11. Karim El Defrawy,, and Gene Tsudik, " **Privacy-Preserving Location-Based On-Demand Routing in MANETs**", *IEEE Journal On Selected Areas In Communications*, VOL. 29, NO. 10, December 2011.

12. Jaydip Sen, Sripad Koilakonda, "**A mechanism for detection of cooperative black hole attack in mobile ad hoc networks**", *Intelligent systems, modelling and simulation (ISMS)*, 2011 Second International conference.

13. Wenjing Lou, Wei Liu,and Yanchao Zhang, "**SPREAD :Improving network security by multipath routing in mobile ad hoc networks**" Springer- Ad hoc Networks 2012.

14. Zhiguo Wan , Kui Ren and Ming Gu , "**USOR : An Unobservable secure on demand routing protocol for mobile ad hoc networks**",*IEEE Transactions On Wireless Communication* 2012.

15. Muthumanickam Gunasekaran and Kandhasamy Premalatha, " **SPAWN: A**

Secure Privacy-preserving architecture in wireless mobile ad hoc networks", *EURASIP Journal on Wireless Communications and Networking* 2013, 2013:220.

16. P. Papadimitratos and Z.J. Haas, "***Secure Message Transmission in Mobile Ad Hoc Networks",*** *Elsevier Journal of Ad Hoc Networks*, Vol.1, No.1, pp 193-209, 2003.