IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

A Survey on MANET Security Challenges, Attacks and its Countermeasures

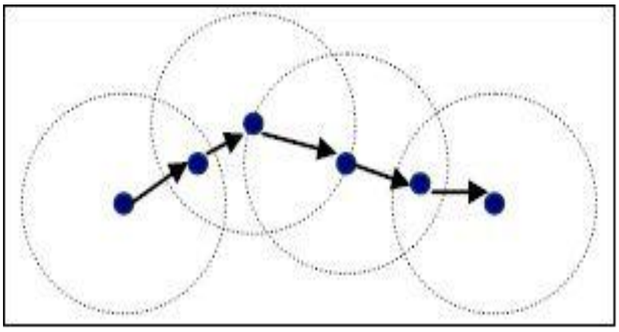
Harpreet Singh Bedi[1], Shekhar Verma[2], Mohit Goel[3]
School of Electronics and Electrical Engg, LPU, Punjab[1, 2, 3]

Abstract: The increase in availability and acceptance of mobile wireless devices has lead researchers to develop an inclusive variety of Mobile Ad-hoc Networking (MANET) protocols to activity the single communication opportunities existing by these devices. Devices are able to communicate directly using the wireless range in a peer-to-peer fashion, and route messages through in-between nodes, however the nature of wireless public communication and mobile devices result in many routing and security challenges which must be addressed before deploying a MANET. Ad-hoc networks have lots of challenges than traditional networks. It has challenges like infrastructures and self organizing networks. They don't have any fixed infrastructure. In Manets there will be no centralized authority to manage the network. Nodes have to rely on other nodes to keep the network connected. As the ad-hoc network is dynamic and every transmission in these networks become vulnerable to many number of attacks and security becomes a major issue.

Keywords: Mobile Ad-hoc Networking (MANET), peer-to-peer fashion, Bluetooth.

1. INTRODUCTION

Wireless technologies such as Bluetooth or the 802.11 standards allow mobile devices to found a Mobile Ad-hoc Network (MANET) by connecting lethargically through the wireless medium without any centralised structure. MANETs offer several advantages over traditional networks including reduced infrastructure costs, ease of establishment and fault tolerance, as routing is performed individually by nodes using other intermediate network nodes to forward packets, this multi-hopping reduces the chance of bottlenecks, however the key MANET attraction is greater mobility compared with wired solutions.



Security of MANETs is another major deployment concern; due to the mobility and wireless nature of the network malicious nodes can enter the network at any time, the security of the nodes and the data transmitted needs to be considered.

2. SECURITY GOALS

a) Authentication: Authentication ensures that the communication or transmission of data is done only by the authorized nodes. Without authentication any malicious node can pretend to be a trusted node in the network and can adversely affect the data transfer between the nodes.

b) Availability: Availability ensures the services should be available even in the presence of the attacks. Systems should be able to take care of various attacks such as denial of services, energy starvation attacks, and node misbehaviour.

c) Confidentiality: Confidentiality ensures that data should be accessible only to the intended party. No other node except sender and receiver node can read the information. This is implemented through data encryption techniques.

d) Integrity: Integrity ensures transmitted data is not being altered by any other malicious node.

e) Non-Repudiation: Non-repudiation ensures that neither a sender nor a receiver should not deny a transmitted message.

3. MANET SECURITY CHALLENGES

1) Dynamic topology: In Manets node may join or leave dynamically. As node moves frequently establishing trust among nodes are very difficult.

2) Battery Constraints: Mobile nodes will be running with battery. If node power utilized unnecessarily then node may comes to idle state.

3) Lack of Central Authority: In MANET there will be no centralized authority like infrastructure network. So implementing security without centralized authority is a challenging task.

DOI 10.17148/IJARCCE.2016.58129

4) Insecure Environment: Nodes may move randomly in MANET. So malicious node may attack and steal the data.

4. ATTACKS ON MANET

Active Attacks

Performed by attackers for replicating, modifying and deletion of exchanged data. They try to change the behavior of the protocol. These attacks are meant to degrade or prevent message flow among the nodes. Such attacks collectively can be called as DOS attacks that either degrade or completely block the communication between the nodes. Another type of attack involves insertion of extraneous packets in the network to cause congestion. Outdated routing information may be replayed back to the nodes in the network. Active attacks can be detected sometimes and this reason makes active attack less used by an attacker.

Passive Attacks

As discussed in this type of attack involves unauthorized listening of the routing packets. Attacker may eavesdrop on all the routing updates. In this case an attacker does not disrupt the operation of a routing protocol rather it only listens to it to discover the valuable information about the routing. Such attacks are difficult to be detected. From the routing packets an attacker may understand about a node which is important in the network and route to that node is being requested very often by every other node. So an attacker tries to disable.

Physical Layer Attacks

1) Eavesdropping: In eavesdropping attack, attacker tries to get the secret information during communication.
2) Jamming: Jamming attack will be implemented by knowing the frequency malicious nodes sends jam signal to disturb the communication.
3) Active Interference: An active interference is a type of denial of service attack which distorts the communications.

Link Layer Attacks

The data link layer can classified as to what effect it has on the state of the network as a whole.
1) Selfish Misbehaviour of Nodes: In the selfish misbehaviour nodes will act as selfish and will not be willing to participate in forwarding process
2) DOS Attack: This attack prevents authorized access of resources to the legitimate node.
3) Resoure Exhaustion: Malicious nodes makes repeated collision to drain the battery power
4) Malicious Behaviour of nodes The main task of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when the communication takes place between neighbouring nodes..

Network Layer Attacks

Black Hole Attack:
In black hole attack the attacker node advertises other node that it has shortest route to reach destination. If this reply reaches before the actual reply a forged route will be established including the malicious node. Now the malicious node can drop packet or perform DOS attack or Man in the middle attack.

Wormhole Attack:
In wormhole attack involves the cooperation between two attacking nodes [18]. One attacker captures the packet and tunnels it to the other attacker. The link between the attackers is high speed communication link. These two attackers makes the topology under their control.

Routing Table Poisoning Attack: In routing table poisoning attack attacker poisons the routing table by changing the routes in the routing table. Other way is to inject RREQ packet with high sequence number. The packet with low sequence number will be deleted. This leads to selection of wrong routes.

Transport Layer Attacks

Session Hijacking: In session hijacking attacker hijacks the session after its set up. Here the attacker spoofs the IP address and launches the various attacks using the right sequence number.

Application Layer Attacks

Malicious code attacks: Malicious code attacks include, Viruses, Worms can attack both operating system and user application.

Multilayer Attacks: The DoS attacks, impersonation attacks, man-in-the middle attacks, and many other attacks can target multiple layers.

Table 1 Layer Attacks in MANET

Layers	Attacks	Solutions
Physical	Jamming	Using Spread spectrum mechanisms FHSS, DHSS
	Eavesdropping	
	Active Interference	
Data Link	Selfish Misbehaviour of Nodes	Secure link layer protocol like LLSP using WPA
	Malicious Behaviour of nodes	
	DOS	
	Misdirecting Traffic	

	Attacking neighbour sensing protocols	
Network	Worm Hole Attack	Securing routing protocols like SAODV, SAR, ARAN to overcome black hole, impersonation attacks, packet leashes, SECTOR mechanism for wormhole attack
	Black Hole Attack	
	Byzantine Attack	
	Information Disclosure	
	Resource Consumption	
	Routing Attack Routing Table Overflow Routing Table Poisoning Packet Replication Route Cache Poisoning Rushing Attack	
Transport	Session Hijacking SYN Flooding	Securing End to End communication (SSL, TLS, SET)
Application	Virus, Worms Dos, Man in the Middle Attack Impersonation	Firewalls

5. SECURITY SOLUTIONS IN MANET

Bridget, Brain Neil, Elizabeth Royer, Clay Shields	Active Attacks	ARAN	Cannot defend against authenticated Selfish nodes
Chu-Hsing Lin,Tunghai Univ, Taipei,Wei-Shen Lai,Yen-Lin Huang; Mei- Chun Chou [21]	Wormhole attack	SEAD	It doesn't provide a way to prevent an attacker from tampering with "next hop" or "destination" columns. Instead, it relies on doing neighbor authentication, which is bad in establishing routes

Physical Layer

At this layer spread spectrum technology such as frequency hopping (FHSS) & direct sequence (DSSS) [5] can be used to prevent eavesdropping attack. It changes frequency in random fashion to make signal capture difficult It also minimizes the potential for interference from other radio & electromagnetic devices.

Link Layer

Traffic analysis is prevented by encryption at data link layer. WEP has been widely criticized. A dynamic mix method is used to hide the source & destination information during message delivery via cryptography method & to "mix" nodes in the network [12]. WEP and WPA provides authentication mechanism for any node to join in network. LLSP is used to provide security at data link layer. But LLSP uses encryption algorithm to prevent from attacks. SLSP is used to prevent DOS attack, Man in the middle attack and its suitable for authenticating new nodes and not suitable for real time traffic.

Network Layer

SAODV routing protocol is used to prevent against blackhole attack but it requires heavy weight encryption algorithm [8]. (SAR) can be used to defend against black hole attacks. In SAR it needs excessive encryption and decryption at each hop. ARAN can be used to defend against impersonation & repudiation attacks. It may not defend against authenticated selfish nodes. Security protocol SEAD is used against modification attacks [13]. Table 2. Describes the network layer protocols and its limitations.

Transport Layer

In transport layer end-to-end encryption provides message confidentiality between two nodes. SSL protocol implements end to end security for a session.

Attacks are DoS attacks, impersonation attacks, man-in-the-middle attacks. The countermeasures for these attacks need to be implemented at different layers

6. CONCLUSION

In this paper we have surveyed several attacks related to different layers in ad-hoc networks. As ad hoc networks are vulnerable to many types of attacks the security of this network is a major issue. Many researchers are trying to prevent the attacks done on ad-hoc networks at various levels. A variety of such attacks have been discussed. We have overviewed the challenges and solutions of the security threats in mobile ad hoc networks. In our study, we present a variety of attacks related to different layers. Here we focus on the currently used security countermeasures to defend against these attacks. A lot of research is still being carried out to identify new threats to ad-hoc networks & securing them.

REFERENCES

[1] Hao yang, Haiyun luo, Fan ye, Songwu lu, and Lixia zhang,"Security in Mobile Adhoc Networks:Challenges and Solutions", IEEE WirelessCommunications, Feb 2004

[2] C.-K Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall, New Jersey, pp: 34-37, 2007.

[3] C. Siva Ram Murthy, and B.S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall communications

engineering and emerging technologies series Upper Saddle River, New Jersey, 2004

[4] I.Chlamtac, M.Conti, and J.Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," Ad Hoc Networks, vol. 1, no. 1, pp. 13-64, 2003.

[5] J.P.Hubaux, L.Buttyan, S.Capkun, "The Quest For Security In Mobile Ad Hoc Networks," Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), October,

[6] A.Menaka Pushpa M.E., "Trust Based Secure Routing in AODV Routing Protocol", IEEE 2009, ISSN: 978-1-4244-4793-0/09, pp. 1-6.

[7] H. Deng, W. Li, Agrawal, D.P., "Routing security inwireless ad hoc networks," Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804

[8] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing for Ad Hoc Networks,"Proc. of MobiCom 2002, Atlanta, 2002.

[9] S.marti. T.Giuli, K. Lai, and M.Baker, Mitigating routing misbehavior in mobile ad-hoc networks.in proc. Of MOBICOM, 2000

[10] V. Cahill et al., "Using trust for secure collaboration in uncertain environments," Pervasive Computing, IEEE, vol. 2, no. 3, pp. 52–61, 2003.

[11] A. A. Pirzada and C. Mcdonald, "Trust Establishment In Pure Adhoc Networks," Wireless Personal Communications, vol. 37, no. 1- 2, pp. 139- 168, Apr. 2006.

[12] S. Marti, T. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MOBICOM), Boston, 2000.

[13] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-hoc Networks, Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MOBICOM), Boston, 2000.

[14] T.Karygiannis And L.Owens, Wireless Network Security-802.11, Bluetooth And Handheld Devices. National Institute Of Standards And Technology. Technology Administration, U.S Department Of Commerce, special Publication 800-848, 2002.

[15] L.Hu And D. Evans, Using Directional Antennas To Prevent Wormhole Attacks.Pro Of Networks And Distributed System Security Symposium (NDSS).

[16] M. Ilyas, The Handbook Of Ad-Hoc Wireles Networks, CRC Press, 2003.

[17] X.Lin, R.Lu, H.Zhu, P.H.Ho, X.Shen and Z.Cao, "ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks," IEEE International Conference on Communications, ICC '07, pp. 1247 –1253, June 2007

[18] B.Kannhavong, H.Nakayama, Y.Nemoto, N.Kato, A.Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks," IEEE Wireless Communications, vol. 14, issue 5, pp. 85-91, October 2007

[19] T.R.Andel and A.Yasinsac, "The Invisible Node Attack Revisited," Proceedings of IEEE Southeast Con 2007, pp. 686 – 691, March 2007

[20] Seung Yi, Prasad Naldurg, Robin Kravets," A Security-Aware Routing Protocol for Wireless AdHoc

DOI 10.17148/IJARCCE.2016.58129