IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. V (Mar-Apr. 2014), PP 113-116
www.iosrjournals.org

Network Layer Attacks and Their Countermeasures in Manet: A Review

1Manisha, 2Dr. Mukesh Kumar
1Banasthali Vidyapith, Rajasthan
2Associate Professor ,TIT&S, Bhiwani,Haryana

Abstract: *Mobile ad hoc network(MANET) is a collection of mobile nodes that are free to move in any direction. It is an infrastructureless network means it has no fixed or predefined network. MANET is a self configuring network with no central authority. Security is one of important and desired feature and the major aspect to be concerned in MANET. The performance and security of MANET is affected by various security attacks. MANET is not only affected by the attacks that are faced in wired or wireless medium but it also has its own security threats. This paper outlines various network layer security attacks and their preventive measures in Mobile Ad-hoc Network.*

Keywords:-*MANET , security, attacks, malicious node, countermeasures.*

I. Introduction

In the past few years there is a rapid development in the area of mobile computing. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of **Mobile Ad Hoc Networks**. A MANET is an autonomous collection of mobile nodes that can change locations dynamically . Since the nodes are mobile, the network topology changes rapidly and randomly . The MANET network is decentralized. The examples can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. As MANETs are dynamic in nature, they are typically not very secure, so it is important to be cautious what data is sent over a MANET .Security is the aspect not to be treated lightly. This is the most desired feature of communication. According to layered architecture there are different different attacks on each layer of MANET but This paper insight the network layer attacks in manet and their countermeasures to prevent those attacks for security purpose.

Network layer attacks

Network layer is affected by various security threats.These attacks may be passive or active.Various network layer attacks are listed in the figure 1.

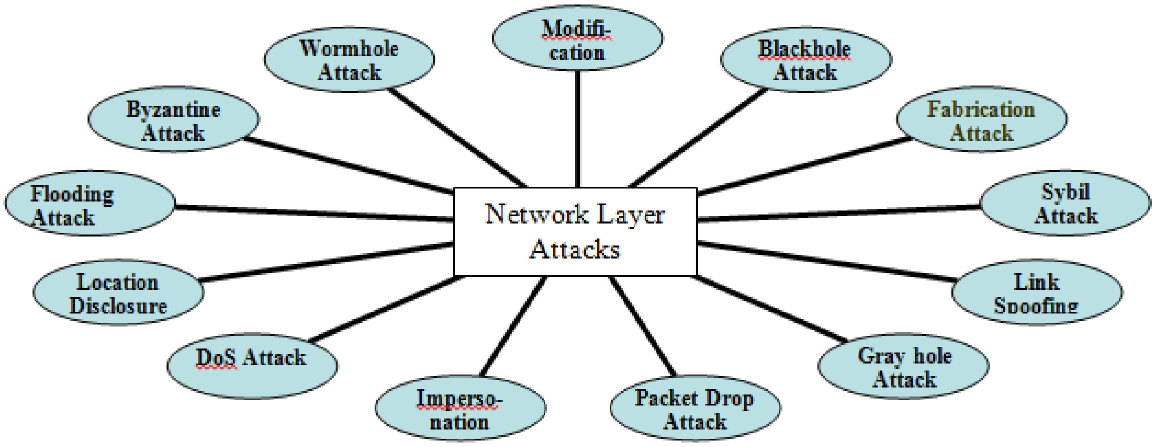
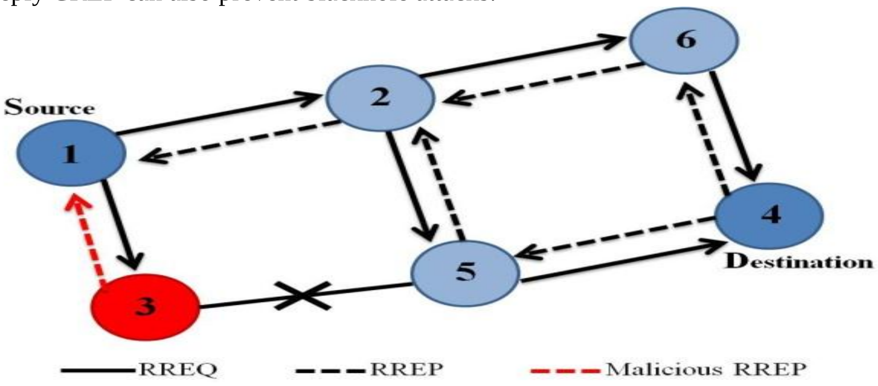


Fig 1: Network layer attacks in MANET

1.1 BLACKHOLE Attack

In blackhole attack the malicious node consumes all the packet meant for destination node.The malicious node waits for RREQ from other nodes,when the it get the RREQ packet,it immediately sends a false RREP packet to claim that it has optimum path to the destination node even if it doesnot have.The source node then ignores all RREP from rest of nodes and selects the malicious one for forwarding packets.in above figure node 3 is malicious node.

Countermeasures:- A DPRAODV (Detection, Prevention and Reactive AODV) protocol is designed to prevent the blackhole attack[3]. Authentication mechanisms, based on the hash function are proposed to identify multiple black holes cooperating with each other[12]. Wait and check the replies mechanism[13] is also proposed to find a safe route for packets. Security-aware ad hoc routing protocol (SAR), is also proposed that can be used for protection against blackhole attacks.Introduce route confirmation requests CREQ and route confirmations reply CREP can also prevent blackhole attacks.



1.2 WORMHOLE attack

In wormhole attack two colluding attackers have a high speed link between them. One attacker tunnels the received packets to another attacker node and retransmits them to the network. This tunnel between the attacking nodes is called wormhole. Wormholes are very hard to detect and they can damage the network without even knowing the network.

Countermeasures: TrueLink is a timing based preventative countermeasure to this attack. Also Packet leashes, are proposed to detect wormhole attack. Leash is any information added to a packet designed to restrict the packet's maximum allowed transmission distance. Geographical leash ensures that the recipient of the packet is within a certain distance from the sender node. Temporal leash ensures that the packet has an upper bound of its lifetime (restricts the maximum travel distance).The SECTOR mechanism[3] is also proposed to detect wormholes without the need of clock synchronization. Directional antennas are also proposed to prevent wormhole attacks.

1.3 BYZANTINE attack

A compromised intermediate node or a set of compromised intermediate nodes[1] works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths,or selectively dropping packets, which results in disruption or degradation of the routing services.

Countermeasures:-A secure on-demand MANET routing protocol, named Robust Source Routing (RSR) is proposed as countermeasure of Byzantine attacks[14]. A Chord mechanism is proposed which is a distributed hash table (DHT).

1.4 FLOODING attack

In this attack, the attacker exhausts the network resources[11], such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance.

Countermeasures:-Calculate rate of neighbour's RREQs and block them if they exceed their threshold limit.Also use statistical analysis to detect varying rates of flooding.

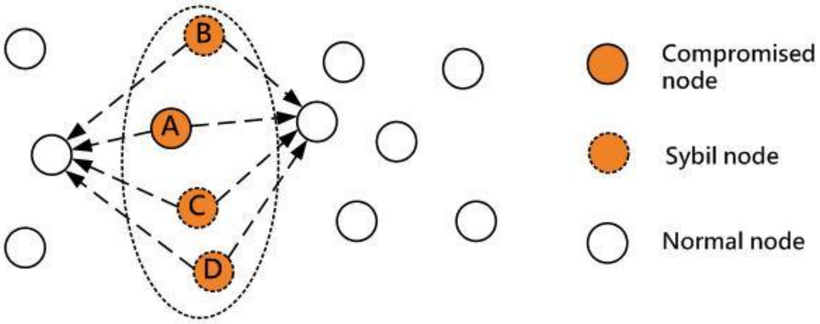
1.5 LINK SPOOFING attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations.

Countermeasures:-One of the preventive measure is equip nodes with GPS[5] and calculate whether two nodes could really have a link. Another solution is to include the 2-hop neighbors in the Hello message, this gives every node a 3-hop topology of the network, less expensive then special hardware, but is defeated by spoofing outside of 3-hops

1.6 SYBIL attack

A faulty node or an adversary may present multiple identities to a network in order to appear and function as multiple distinct nodes. After becoming part of the network, the adversary may then overhear communications or act maliciously. By presenting multiple identities, the adversary can control the network substantially.



Coutermeasures:-A robust Sybil attack detection framework[3] is proposed for MANETs based on cooperative monitoring of network activities.

1.7 MODIFICATION attack

In a modification attack, intruders make some changes to the routing messages, and thus endanger the integrity of the packets in the networks[10]. Since nodes in the ad hoc networks are free to move anywhere and self-organize, relationships among nodes at some times might include the malicious nodes. These malicious nodes might exploit the sporadic relationships in the network to participate in the packet forwarding process, and later launch the message modification attacks.

Countermeasures:-The security protocol SEAD [16] is used here as an example of a defense against modification attacks. Similar to a packet leash , the SEAD protocol utilizes a one-way hash chain to prevent malicious nodes from increasing the sequence number or decreasing the hop count in routing advertisement packets. A new key management scheme[15] is implemented in NTP protocol can also be a solution to this attack, since Node Transition Probability (NTP) based algorithm provides maximum utilization of bandwidth during heavy traffic with less overhead.

1.8 FABRICATION attack

Fabrication is an active attack or forge in which instead of modifying or interrupting the existing routing packets in the networks[10], malicious nodes gains access and also generate their own false routing packets to cause chaos in the network operations. They could launch the message fabrication attacks by injecting very huge packets into the networks such as in the sleep deprivation attacks. Such kind of attacks can be difficult to identify as they come as valid routing Constructs.

Countermeasures:-Secured consistent network can cop up with fabrication attacks in MANET.

1.9 LOCATION DISCLOSURE attack

An attacker discover the Location of a node or structure of entire networks and disclose the privacy requirement of network .The Adversaries try to figure out the communication parties and analyze traffic to learn the network traffic pattern . The leakage of such information is distructive for security.

Countermeasures:-An approach uses geometric constraints and heuristics[3] to find node positions efficiently can be used to prevent such attack.Based on the localization precision that such an ”omniscient” attacker can reach, we will be able to evaluate the quality of future, more realistic attack models.

1.10 GRAY HOLE attack

This attack is also known as routing misbehavior attack which leads to dropping of messages.in this attack the nodes will drop the packets selectively. Gray hole attack has two phases.In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

Countermeasures:-As a countermeasure of grayhole attack ,signature algorithm is proposed to trace packet dropping nodes.

1.11 IMPERSONATION attack

Impersonation attacks are launched by using other node's identity,such as IP or MAC address.Impersonation attacks are sometimes are the first step for most attacks,and are used to launch further ,more sophisticated attacks.

Countermeasures:-To prevent impersonation attacks,a multifactor authentication framework is used by using two distinct authentication factors; certified keys and certified node characteristics. ARAN provides authentication and non-repudiation services using predetermined cryptographic certificates for end-to-end authentication. In ARAN, each node requests a certificate from a trusted certificate server.

1.12 PACKET DROP attack

Malicious or attacker nodes drop all packets that are not destined for them.Malicious nodes aim to disrupt the network connection and performance,while selfish nodes aim to preserve their resources. Packet Dropping attacks can prevent end-to-end communications between nodes,if the dropping node is at a critical point. It might also reduce the network performance by causing data packets to be retransmitted.
Countermeasures:- A two folded approach, to detect and then to isolate such nodes is proposed which becomes the part of the network to cause packet dropping attacks.

1.13 DENIAL OF SERVICE attack

In denial of service attack the attackers makes an attempt to make the network resources or a node or machine temporarily unavailable to its actual users. They sends fake requests to the target so that it becomes unavailable to service its intended users .In such type of attacks the target may be temporarily down or may be destroyed. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table overflow,or poisoning.
Countermeasures:-Firewall can be used to prevent DoS attacks. A DoS mitigation technique that uses digital signature is proposed to prevent such type of attacks. Also proposed an efficient on-the-fly search technique to trace back DoS attackers.

II. Conclusion

In this paper, one can see the various network layer attacks on mobile ad-hoc networks. This paper outlines characteristics of various attacks that can be considered while designing the security measures for ad hoc networks .By investigating these attacks and their characteristics one can design new security measures or protocols to protect MANETs. Outlined countermeasures can be used to protect ad-hoc networks from various attacks. In this paper, we tried to inspect existing countermeasures of network layer security attacks in Mobile Ad hoc network.

References

[1] Rajni Sharma, Alisha saini," *A Study of Various Security Attacks and their Countermeasures in MANET,"*International Journel of Advanced Research in Computer Science and Software Engineering,Volume 1,Issue 1,December 2011.

[2] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "*A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks* ," Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.

[3] Mangesh M Ghonge, Pradeep M Jawandhiya, Dr. M S Ali,"*Countermeasures of Network Layer Attacks in MANETs*," IJCA special issue on "Network Security and Cryptography ",NSC,2011.

[4] K. SIVAKUMAR, Dr. G. SELVARAJ,"*Overview of Various Attacks in MANET and Countermeasures for attacks*," International Journal of Computer Science and Management Research, Vol 2 Issue 1 January 2013.

[5] Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala,"*A Review of Current Routing Attacks in Mobile Ad Hoc Networks*," International Journal of Computer Science and Security, volume (2) issue (3).

[6] PRADIP M. JAWANDHIYA, MANGESH M. GHONGE, DR. M.S.ALI, PROF. J.S. DESHPANDE," *A Survey of Mobile Ad Hoc Network Attacks*," International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071.

[7] Himani Yadav and Rakesh Kumar," *Identification and Removal of Black Hole Attack for Secure Communication in MANETs*," *I*nternational *J*ournal of *C*omputer *S*cience and *T*elecommunications [Volume 3, Issue 9, September 2012].

[8] G.S. Mamatha, Dr. S.C. Sharma," *Network Layer Attacks and Defense Mechanisms in MANETS- A Survey*," International Journal of Computer Applications (0975 – 8887) Volume 9– No.9, November 2010.

[9] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao,"*A survey of black hole attacks in wireless mobile ad hoc networks*", Tseng et al. Human-centric Computing and Information Sciences 2011, @ 2011 springer.

[10] 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*," International Journal of Advanced Engineering Technology E-ISSN 0976-3945.

[11] Manjeet Singh, Gaganpreet Kaur," *A Surveys of Attacks in MANET*," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.

[12] Zhao Min and Zhou Jiliu1, "*Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks*", 2009 International Symposium on Information Engineering and Electronic Commerce.

[13] Latha Tamilselvan and Dr. V Sankaranarayanan, "*Prevention of Blackhole Attack in MANET*", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007).

[14] Claude Cr´epeau, Carlton R. Davis and Muthucumaru Maheswaran, "*A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes* ", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) 0-7695-2847-3/07 $20.00 © 2007 IEEE.

[15] Vaithiyanathan, Gracelin Sheeba.R, Edna Elizabeth. N, Dr.S.Radha, "*A Novel method for Detection and Elimination of Modification Attack and TTL attack in NTP based routing algorithm* ", 2010 International Conference on Recent Trends in Information, Telecommunication and Computing 978-0-7695-3975-1/10 $25.00 © 2010 IEEE.

[16] Y. Hu, D. Johnson, and A. Perrig,"*SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks*." Proc. of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), pp. 3-13, 2002.