ISSN:0975-9646

A Survey on Security Vulnerabilities And Its Countermeasures At Network Layer In MANET

Rishikesh Teke[#1], Prof. Manohar Chaudhari[*2]

[#]*Department of Comp. Sci and Engg, Sinhgad Institute Of Technology*
Lonavala, Maharashtra India
**Asso. Professor, Department of Comp. Sci and Engg, Sinhgad Institute Of Technology*
Lonavala, Maharashtra India

***Abstract*—Mobile ad-hoc network is widely used in today's world as MANET is having characteristics such as wireless connectivity, dynamically changing topology. In MANET mobile nodes also acts as router and interchange the data packets. MANET is used where fixed infrastructure is unavailable or infeasible. Such applications are battlefield communications, crisis management, emergency response operations etc. For these kind of application security is major issue. In MANET as mobile nodes also routes packet and lack of centralized point they are vulnerable to various routing attacks. In this paper we attempt to survey on routing attacks such as Blackhole, Wormhole, Grayhole, Packet Drop attack on various routing protocols like AODV and DSR with their countermeasures.**

Keywords—Blackhole Attack; Countermeasures; Grayhole Attack; Mobile Ad-hoc Networks (MANET); Packetdrop Attack; Wormhole Attacks;.

I. INTRODUCTION

In mobile ad-hoc network (MANET) communication is carried out via multi-hop paths. MANET having collection of autonomous mobile nodes without fixed infrastructure and centralized control point. In MANET due to movement of mobile nodes network topology may change continuously and unpredictably over the time. A typical MANET is as shown in Figure-1.The routes in MANET are not stable and this fluctuation in routes varies with respect to time. At the time of connection establishment in MANET mobile node advertise for the route request in the form of routing messages. Existing routing protocols mobile nodes unable to find malicious node in the network thus malicious node take it as advantage and generate fake routing message to advertise non-existing connection links also floods incorrect information. This dynamic nature of MANET make it vulnerable for routing attacks. Most of the routing protocols in MANET are unsecure and are vulnerable for various attacks which makes devastating effects in the network.

A lot of research has been done on security issues in MANET. Most of the attacks done in the routing mechanism of routing protocols.

In MANET there are three types of protocols :

1.Proactive Routing protocols: These protocols are table driven and select path on the freshness of routes by periodically distributing routing tables throughout the network. Examples of such protocols are Optimized Link State Routing (OSLR) and Destination Sequenced Distance Vector(DSDV).

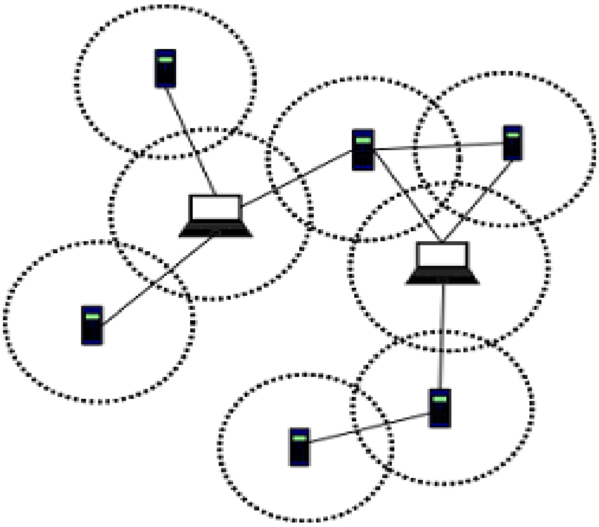

Figure 1. A Typical MANET.

2.Reactive Routing Protocols: These kind of protocols finds path on demand by flooding with Route Request packets. Examples of Reactive Routing Protocols are Ad-hoc On Demand Distance Vector Routing(AODV) and Dynamic Source Routing(DSR).

3.Hybrid Routing Protocols: These kind of protocol is combines advantages of proactive and reactive routing protocol. Initially routing is done using proactively mechanism and then serves demand from additionally activated nodes through reactive flooding. Zone Routing Protocol(ZRP) is an Example of Hybrid protocol.

II. TYPES OF ATTACK IN MANET

A. Active Attacks

Attacks in which malicious nodes actively participate and disrupt the network operation are called Active attacks. In active attacks malicious nodes alter the information or provide fake information in the network. Active attacks can be Internal or External. External attacks done by node that do not belong to the network where internal attacks done by malicious node which belongs to the network. Spoofing, Denial of Service(DoS), spoofing, modification, impersonation are types of active attacks.

B. *Passive Attacks*

Attacks which does not disrupt the normal operation of the network is called Passive attacks. Passive attacks are hard to detect as they never harms the operations of network. Confidentiality of information is violated in this kind of attacks. Passive attacks are traffic analysis, eavesdropping and monitoring.

III. Security Vulnerabilities At Network layer

In MANET all routing protocols depends upon active co-operating nodes which provide routing between mobile nodes to establish and setup the network. Ad-hoc On Demand Distance Vector(AODV)[5] and Dynamic Source Routing(DSR)[6] are two widely used protocols in MANET. These protocol won't have inbuilt routing security and thus several attacks can be mounted on these protocols. Protocol uses Route Request messages and Route Reply messages to setup connection between source and destination. Also mobile nodes maintains their routing table in cache for further communication. Routing messages and routing tables in cache are main weaknesses of routing protocol on which malicious node can attack and disrupt the network.

Following are the major routing attacks in MANET

1. Black Hole Attack :

In two phases blackhole is done. First phase, malicious node attacks on routing protocol such as AODV and exploits its routing mechanism such that if source broadcasts its route request blackhole responds that request sending route reply packet and advertise itself having valid route to destination. The routing mechanism selects path to destination via malicious node. In second phase malicious node gets incoming packets and discards without forwarding them.[8]

2. Wormhole Attack

Wormhole attack is replay attack on routing control plane. Without increasing hope count value, attacker node tunnels request packets to destination.[9] Attacker node records packets at one location and replay them at another location this tunneling can be wired or wireless communication. Attacker node manipulate nodes and that nodes sends their traffic through attacker node. Thus attacker node can have aggregate traffic of nodes and can modify , record or even drops the packet.[7]

3. Grayhole Attack

Grayhole is variants of Blackhole attack where malicious nodes interchanges their states from black hole to honest intermittently and vice versa.[2][11] Grayhole nodes partially drops packets due to malicious nature and congestion in network. Due to such interchanging behaviour grayhole is difficult to detect and prevent[12].

4 Packet Drop Attack

Packet Drop is kind of Denial of Service(DoS), in which malicious node drops packets passing or routing through it. Instead of attracting neighboring nodes traffic Packet dropping node only drops packets and also Blackhole attack completely degrade performance but Packet Drop attack degrade it partially so it is different from Blackhole attack.[4] There are various for dropping packets like energy consumption or packet sniffing purpose.

IV. Related work

Security countermeasures are broadly classified into two areas one is prevention techniques and another is detection techniques. We did extensive survey of major attacks and their countermeasures from following research papers.

Jian-Ming Chang at el [3] propose a scheme called Cooperative Bait Detection Scheme(CBDS) for detecting and preventing grayhole and blackhole attack in MANET. CBDS is uses DSR[6] as underlying routing protocol. In this approach source node takes help from trusted neighbouring node and sends its address as destination address to other nodes. After sending RREQ message in the network, if there is malicious node then it sends RREP message to source node having valid route to given destination address and other trusted neighbouring node will not send RREP message. Malicious node detected and prevented using reverse tracing technique.

Jaydip Sen et al [8] focuses on cooperative blackhole attack. They provided mechanism to detect cooperative blackhole in MANET. In cooperative blackhole attack two malicious nodes cooperatively advertise themselves as a valid route and intercept the packets and drops them without forwarding it. To tackle such attack authors modified AODV protocol in which Data Routing Information (DRI) table is maintained at each node. Two parameters in DRI table, one is 'through' means data packet routes through node and another is 'from' means data packet routes from node. For these parameter they assigned two Boolean values, 1 for true and 0 for false. If there is malicious node in network it neither passes data packet through it nor sends from it, so both values in DRI table for a malicious node is zero. Thus malicious node in the network can be detected. Extra space is needed for storing DRI table for each node and also these entries can updates when the network changes. This approach having advantage is that as MANET changes topology dynamically so if there is blackhole if it is internal or external it can detect efficiently.

G. S. Bindra et al [13] extends the DRI table entries and give another modified DRI table which will detect and remove co-operative blackhole as well as grayhole attack in MANET. EDRI also implemented in AODV protocol. In this table *CTR*, *BH* and *Time* fields are added in which *CTR* stands for keeping number of times node behaved maliciously, *BH* keeps record of blackhole if value is 1 it is considered to be malicious in its latest interaction else it is 0 and at last *Time*r field used to define duration for which the node would be considered malicious. These extra fields also tracks the grayhole attack. As *CTR* field indicates how many times node behaved maliciously and with *BH* field detects grayhole. EDRI table requires extra space for storing extra tree fields of information but it gives a complete solution for detection and removal of blackhole as well as grayhole attack.

J. Eriksson et al [7] proposed a practical countermeasure on the wormhole attack. They used a combination of strict timing constraints and authentication for prevention of wormhole attack in MANET. Algorithm having two phases first is Rendezvous phase in which nodes exchanges their nonces which having strict timing constraints. After successful exchange of nonces Second phase contains authentication between nodes which ensures that link is trustworthy. Paper described how truelink counters forwarding attack, masquerade attack and double masquerade attack. Truelink is also immune to physical layer wormholes. One of the important task in truelink is link verification maintenance. Authors proposed two link verification techniques one is proactive link verification in which when a new neighbor is found link verification is initiated this step is carried out before routing layer is notified of the neighbor discovery. Second link verification method is reactive link verification in which a node waits until it receives a broadcast packet across a previously unverified link. At this time, it initiates a link verification exchange with sender of the packet. Advantages of this mechanism is that we can apply this mechanism on any routing protocol used for communication and can also be implemented in IEEE 802.11 hardware with backward compatibility.

A M Kanthe et al [4] proposed solution on packet drop attack. Packet dropping node only drops packets entering through it and will never intentionally attracts networks traffic, it is minor as compared to blackhole and grayhole attack. Authors proposed mechanism in which AODV protocol is modified. Modification contains a Trust list maintained at each node locally and reputation based approach which fetches information like total sent packets by replying nodes and total packets dropped by replying nodes. Thus trust is maintained in nodes and if there is packet dropping node its entry is discarded from trusted list. It is helpful for the detection and prevention of packet drop attacks in MANET.

S. Banerjee[1] proposed an algorithm in which total data traffic is divided into small sized blocks to detect malicious node in MANET. In this method exchange of preclude-postclude messages is carried out where source node sends preclude message and postclude is reply from destination. On reception of postclude message node checks the data loss during transmission is within threshold range if not it initiates process for detecting and removing of malicious node. This scheme is used for greyhole and blackhole attacks in MANET. To detect and remove malicious node, source node sends query message to all its neighbours which includes time out period. When timeout occurs result message or node is malicious message is replied to source node. Then source node will append that node in findmalicious table and initialise value voting as 1 if it is not already there otherwise increments by one. If that voting count exceeds threshold value node is considered as malicious node.Thus this method is triggered when there is actual data communication takes place.

Intrusion Detection Systems are helpful to detect and prevent intrusion of malicious activity in the network. Tiranuch Ananvalee and Jie Wu[10] did survey on Intrusion Detection Systems which can be applied on MANET. Authors classified architectures for IDS in MANET. One of the architecture is Stand alone Intrusion Detection systems in which IDS runs on each node independently to determine intrusion. Another architecture Distributed and cooperative Intrusion Detection systems in this architecture an IDS agent is running on each node. Every node participates in intrusion detection and response by having an IDS agent running on them. IDS agent detects and collects local events and data to identify whether malicious activity is taking place or not. Third architecture is Hierarchical Intrusion Detection Systems in which network is divided into clusters. An IDS agent is running on each node. At the top there is clusterhead present which monitors the network and responsible for initiating a global response when intrusion is detected. Authors also described five sample Intrusion Detection Systems for MANETs. They also focuses on Intrusion Detection Techniques for Node cooperation in MANET.

V. MERITS AND DEMERITS OF COUNTERMEASURES ON ATTACKS IN MANET

attacks	**Survey on attacks and countermeasures in MANET**		
	Countermeasures	***Merits***	***Demerits***
Blackhole and Greyhole	Cooperative Bait Detection Scheme(CBDS)[3]	It detects greyhole as well as blackhole attack	If at worst case all the neighboring node are malicious the algorithm may not detect malicious behavior
Cooperative Blackhole	Detection of cooperative blackhole using DRI table[8]	Simple method and data structure, efficient method to detect Cooperative blackhole attack	This method is only limited to cooperative blackhole attack
Wormhole	Truelink concept a practical countermeasure of wormhole attack[7]	It can be implemented in software as well as in hardware to tackle wormhole attack in various protocols	Frequently link verifiaction is needed
Packet-drop	Trusted list[4]	Efficient technique for detection of packet dropping node	Maintaing true list is tricky and can be vulnerable to attack
Cooperative blackhole and greyhole	Perclude-postclude messaging for detection and findmalicious table to remove malicious node[1]	Removes all kinds of blackhole and greyhole attacks efficiently	Perclude-postclude messages increase network traffic and may cause congestion in network.

VI. Conclusion

In this paper, we discussed on various attacks on the mobile ad hoc networks. These attacks degrades performance of MANET. To tackle these attacks, we studied countermeasures on these specific attacks such as blackhole , grehole, wormhole and packet drop attack. These countermeasures are applicable only for specific protocols because every protocols works differently. There is need to develop a protocol which is secure from such kind s of attacks.

References

[1] Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks," Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[2] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad, "A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks**,**" International Journal of Computer Applications (0975 – 8887) Volume 53– No.16, September 2012.

[3] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai," Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," IEEE SYSTEMS JOURNAL,Unpublished.

[4] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad, " The Impact of Packet Drop Attack and Solution on Overall Performance of AODV in Mobile Ad–hoc Networks," International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2249-8958, Volume-2, Issue-2, December 2012.

[5] C. Perkins, E. B. Royer and S. Das, "Ad hoc On Demand Distance Vector (AODV) Routing, Internet Draft", RFC 3561, IETF Network Working Group, July 2003.

[6] D. Johnson, Y. Hu, D. Maltz," The Dynamic Source Routing Protocol (DSR)," RFC 4728, Network Working Group, February 2007.

[7] J. Eriksson, S. V. Krishnamurthy, M. Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 2011. The Communications and Networks Consortium sponsored by the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program.

[8] Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks," Second International Conference on Intelligent Systems, Modelling and Simulation, 2011.

[9] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah, " MANET Routing Protocols and Wormhole Attack against AODV," IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[10] Tiranuch Anantvalee, Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," Wireless/Mobile Network Security , pp.170–196, 2006,Springer.

[11] V. Shanmuganathan, T.Anand, "A Survey on Gray Hole Attack in MANET*"*, International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No6, December 2012.

[12] Onkar V. Chandure, V. T. Gaikwad, "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV routing protocol in MANET", International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2607-2613.

[13] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal, "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANET", International Conference on System Engineering and Technology, September 11-12, 2012.