Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 6, June 2016, pg.182 – 189

Analysis of Security Attacks and Solution on Routing Protocols in MANETs

Anil Saini[1], Anu[2]

Assistant Professor[1,2]

[1,2]Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119

saini.anil143@gmail.com, anu.duhan@yahoo.com

Abstract-- MANETs are fast emerging as alternate network architecture to infrastructure networks. It is finding many applications and the constraints of processing power, memory, and bandwidth will be soon being overcome with the rapid improvement in the technologies. However the major concern which will remain is the security of the network. MANETs differ largely in the routing mechanism in the network layer from other wireless networks and therefore require different security schemes to secure the routing protocols. The security of the routing protocols is the major active area of research. In this paper author analyze the routing process, their vulnerabilities and the various types of attacks which can be launched by exploiting the same, to disrupt the routing process or launch DoS attacks. The author also reviews the possible countermeasure against these attacks and listed out the advantages as well as the limitations of the countermeasures.

Keywords-- Black Hole Attack, Flooding Attack, MANETs, Rushing Attack, Sybil Attack, Wormhole Attack

I. INTRODUCTION

Ad hoc wireless technology is an emerging approach to wireless communication with potential applications in random and dynamic environments. In contrast to cellular and infrastructure based networks, it does not possess any fixed infrastructure or central administrator such as router. MANET is a set of independent system of mobile nodes that move freely and randomly. Its network topology is dynamic in nature and may change speedily and randomly. Due to this the intercommunications among nodes keep on changing. MANET [2, 5] depends on many other aspects including location of request initiator, topology of network and optimum selection of routers and specific underlying features that could work on finding the path rapidly and efficiently. The threats to MANETs at different layers are same as that of any infrastructure wireless network, except at network layer, where routing protocols are more vulnerable to attack because of the cooperative nature of the nodes and lack of infrastructure for routing. The threats at different layers in MANET are dealt in the same manner as these are dealt for infrastructure network, but at the network layer the routing protocols need to be protected. Number of routing protocols have been proposed for MANETs, which can be classified into three categories; proactive

© 2016, IJCSMC All Rights Reserved

based and reactive based and hybrid. The Internet Engineering Task Force (IETF), MANET Working Group has produced Request for Comments (RFC) for "Ad-hoc on Demand Distance Vector (AODV)" [2], "Demand Source Routing (DSR)", "Optimized Link State Routing (OLSR)", "Zonal Routing Protocol (ZRP)" and "Topology Dissemination Based on Path Forwarding (TBRPF)". However, none of these protocols specify any security measures, thus exposing them to variety of attacks. In this paper we have studied the vulnerabilities of the routing protocols and the attack mechanism by the malicious nodes which can possibly lead to various external and internal attacks. The current literature on the protection measures for detection and isolation of the malicious nodes have also been reviewed in this paper.

The rest of the paper is organized as follows: in Section II, the Routing Process and vulnerabilities of routing protocols are discussed. In Section III, various attacks which can be launched exploiting the vulnerabilities and the summary of attacks and their countermeasures are discussed. Section IV presents the concluding remarks.

II. ROUTING PROTOCOLS AND VULNERABILITIES

In Pro-Active routing protocol [3], every node maintains a routing table which has the routing information to every other node in the network, whether it has data to send or not. The routing information is built in each node through the exchange of Hello Messages which have connectivity information with its neighbors. The neighborhood connectivity information is shared among all nodes in the network through Topology Control (TC) Message updates. Every node in the network maintains number of routing tables to store the updates which are time driven and event driven. The optimum routes to all other nodes are deduced from this information. Several protocols in this category have been proposed. These protocols have the advantage of minimum time delay in searching the route but consume lot of resources in terms of bandwidth, memory and power of the nodes. These protocols therefore do not perform well for large networks with more number of mobile nodes since these results in large routing tables and excessive control traffic on the network.

In Reactive routing protocols [3], on the other hand, the route to the destination is obtained when the node has the data to send to another node. The routing process involves the Route Discovery process and Route Maintenance Process. In AODV [2][4] for instance, when a source node has data to send it broadcasts a "Route Request" (RREQ) message to its neighbors, who in turn rebroadcasts the RREQ message, if they are not the destination node or do not have fresh enough route to the destination. Source sequence number and destination sequence number in the RREQ message are used for preventing loops and determining the freshness of the route respectively. Hop count in the RREQ message is incremented every time the message is rebroadcasted by the intermediate node and is used to determine the shortest path to the destination. Each node receiving the route request caches a route back to the originator of the request, so that a unicast "Route Reply" (RREP) message can be sent from the destination along the shortest path to the originator, or likewise from any intermediate node that is able to satisfy the request. An intermediate node can send a RREP message if it has a route with equal to or higher destination sequence number than what is in the RREQ message. In the Route Maintenance process the nodes monitor the link status of next hops in active routes with the help of Hello Messages. When a link breaks in an active route, a "Route Error" (RERR) message notifies other nodes about the loss of link. The link could be part of number of routes to the different destinations and the RERR message will indicate all those destinations. In order to enable such reporting each node maintains a "precursor list", containing address for each of its neighbors that are likely to use it as a next hop towards each destination.

The routing protocols are vulnerable because of the use of cooperative routing algorithms which have no security features, limited resources with nodes, dynamic topology of the network and absence of any security infrastructure in the network. The vulnerabilities of the routing protocols emerge from the routing process. The control messages which are exchanged for establishing the routes, route maintenance and updating of routing tables are vulnerable to attack from the malicious nodes. A malicious node in a proactive routing protocol can attack the Hello and TC messages in order to poison the routing process. In the Reactive Routing protocol the malicious node can attack the RREQ, RREP and RERR control messages. A malicious node can act as a source node or an intermediate node. When it is acting as a source node it can either use its own address, the address of an existing node or an arbitrary node to launch an attack. When the malicious node is acting as intermediate node it can either modify or replay the received packets which can lead to route disruption or Denial of Service.

III. SECURITY ATTACKS ON ROUTING PROTOCOLS

Various types of attacks on routing protocols for MANETs are known. These can be mainly classified as "Route Disruption Attacks" and "Denial of Service (DoS) Attacks". In the Route Disruption Attacks the malicious or compromised/selfish node will disrupt the route by interposing itself in the selected route causing legitimate data packets to be routed in dysfunctional manner. In the DoS attack the objective is to unnecessarily use network resources. In this section we will discuss the mechanism for launching some of the attacks on the routing protocols.

© 2016, IJCSMC All Rights Reserved

A. **Black Hole Attack:** In "Black Hole Attack" [5] a malicious node exploits the vulnerabilities of route discovery procedure of a reactive routing protocol. The malicious node as an intermediate node on receipt of a RREQ message sends a RREP with the destination sequence number larger than is in the RREQ message indicating that it has a fresh route to the destination. This RREP from malicious node will reach source node before the reply send by destination/ legitimate intermediate node. The source node will thus select the route which passes through malicious node. By repeating this for RREQs received from other sources the malicious node captures several routes attracting the data traffic from all sources towards it thus creating a black hole in the network. The malicious node can then misuse or discard the traffic. The Fig. 1 shows the malicious node (MN) sending fake RREPs to two sources in the network and capturing the routes of both the sources thus creating a Black hole.

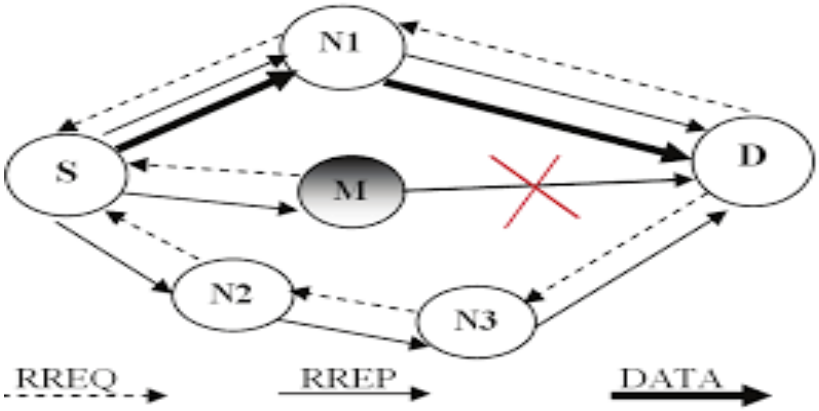

Fig1: Black Hole Attack

B. **Gray Hole Attack:** In "Grey Hole Attack", [6] the malicious node first captures the route as in Black hole attack by exploiting the vulnerabilities of route discovery process of the routing protocols and then it drops the intercepted packets with a certain probability. The malicious node in this type of attack may drop packets coming from certain specific nodes while forwarding all the packets for other nodes or it may drop packets for some time and behave normally for rest of the time or a combination of the above two, thereby making detection of malicious node very difficult. Fig. 2 shows the Gray Hole Node (GHN) drop the packets coming from the target node.

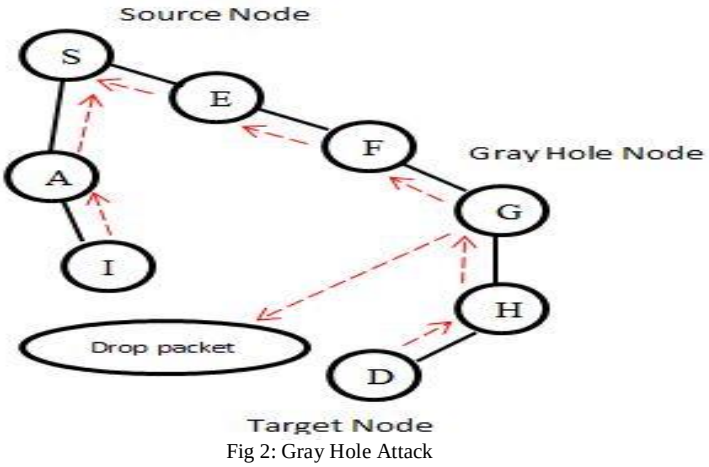

Fig 2: Gray Hole Attack

C. **Rushing Attack:** In "Rushing Attack" [7] the malicious node rushes i.e. transport earlier the RREQ message to its neighbors thus suppressing the rebroadcast from legitimate nodes. In the reactive routing protocols an intermediate node responds only to the first RREQ message which is received and suppresses other duplicate RREQ packets by the use of the source sequence numbers. The malicious node transmits the RREQ message earlier than well behaved nodes by either removing the delays which the message has to suffer at the MAC layer or by using long range wireless

© 2016, IJCSMC All Rights Reserved

transmission. As the RREQ only passes through malicious node, it interposes itself in the selected route and thereafter causes legitimate data packets to be routed in dysfunctional manner.

D. **Wormhole Attack:** "Wormhole attack" [5][8] is launched by a two or more colluding malicious nodes which captures the packet at one location, transports it over the tunnel to the other location and replays at the distance location bypassing the intermediate node. The tunnel so created gives an impression that the two nodes are one hop away and thus provides the shortest path to the destination. The pair of colluding malicious node creates traffic choke points which are under the control of attackers and can be utilized to launch the active or passive attacks. The tunnel can be established by either In-Band Channel or Out- Band Channel. In Out-Band Channel the colluding nodes establish a direct link between the two colluding nodes by long range wireless transmission or by a private high speed network. On the contrary, the In-band channel does not use the external communication medium to create the tunnel; instead it uses encapsulation to develop a covert overlay tunnel over the existing wireless medium. A wormhole attack is equally dangerous for both proactive and reactive routing protocols. It is possible even if all communications provide authenticity and confidentiality. Fig 3 shows MN1 and MN2 creating illusion of being neighbors by encapsulation to develop a covert overlay tunnel over the existing wireless medium. It sends false advertisement of 1-hop link between MN1 and MN2 without the actual exchange of Hello messages.

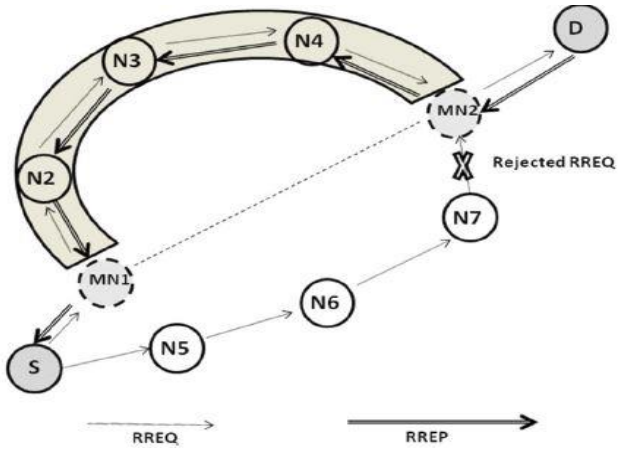

Fig 3: Wormhole Attack

E. **Sybil Attack:** In "Sybil Attack" [9] [10] a malicious node creates and controls multiple identities. A node in the network is identified by a unique identifier (address) and there is one-to-one mapping between the node and the identity. Two different identities represent two different nodes. MANETs do not have any centralized identity management mechanism thus a malicious node can assume multiple identities and can create several virtual nodes by assuming new identities. The Sybil attack can be launched in two ways, in the first case a malicious node creates a new identity after discarding the previously created identity and therefore one identity of attacker is active at one time. The aim of such attack is to delink the malicious node from its earlier malicious activities. In the second case the malicious node assumes several identities simultaneously with the aim to cause disruption in the network. The malicious node can get identities in two ways, the first is by assuming arbitrary identities and the second is by spoofing the identities of legitimate nodes. The Sybil attack can affect both "proactive and reactive routing protocols". In proactive protocols it can add itself to the neighborhood of the other nodes with fake/spoofed identities thus misdirecting data to the malicious node. In reactive routing protocols it can disrupt the routing process by forming counterfeit identities or can cause DoS attacks by using multiple identities.

F. **Flooding Attack:** In "Flooding Attack" [11] the attack is launched by flooding of RREQ message in the reactive routing protocol. A malicious node can flood the network with route request to the nonexistent or arbitrary destinations. The purpose is to unnecessarily use bandwidth, computational resources, memory resources, power resources, and prevents the normal operation of the routing-protocol. In proactive protocols flooding of the TC message will cause such an attack. As these protocols create and maintain routes to all other nodes in the network through exchange of TC messages, whose rate is not controlled, these are more vulnerable to such attacks.

© 2016, IJCSMC All Rights Reserved

TABLE 1: SUMMARY OF ATTACKS AND THEIR COUNTERMEASURES

Sr. No.	Types of attacks and Routing Protocol Vulnerabilities	Suggested Countermeasures	Advantages/Disadvantages of the Scheme
1.	**Black Hole Attack** • The Malicious node interposes between source nodes and destination nodes. • Intermediate malicious node sends fake RREP. Manipulates Destination Sequence number and hop count. Attracts data traffic towards itself. • It discards data traffic and prevents from reaching destination. Most effective against reactive routing protocols, viz. AODV & DSR	• "Chavda, K." in [13] proposes Comparison of Destination Sequence numbers of at least two RREPs. • Detection of malicious node if destination sequence number is arbitrarily high.	• Simple and minimum overheads. • Unable to isolate the malicious node if it does not use arbitrary high destination number.
		• "Abdelhaq, M." in [14] proposes Local Intrusion Detection (LID) security mechanism. • RREP from the intermediate node is checked by immediately previous node by sending a FRREQ message to the next node.	• An improvement over the earlier scheme Source Intrusion Detection (SID) Mechanism. • More complex.
2.	**Grey Hole Attack** • Malicious node exploits same vulnerabilities as in Black Hole Attack. • It exhibits malicious behavior in different ways. May discard data traffic of specific nodes while behaving normally for other nodes or may discard data traffic for some time and behave normally for rest of the time or a combination of the above two.	• "Sen, J." in [6] proposes, monitoring and analysis of the behavior of neighboring nodes with respect to data traffic. The malicious nodes are detected if traffic pattern does not conform to lay down rules.	• Significant high detection rate with moderate traffic overheads.
3.	**Rushing Attack** • Malicious node rushes the RREQ message to its neighbors thus suppressing the rebroadcast of RREQ from legitimate nodes. • Malicious node rushes the RREQ message by either removing the delays which the message has to suffer at the MAC layer or by transmitting using long range wireless transmission. • Malicious node interposes itself in the selected route and thereafter causes legitimate data packets to be routed in dysfunctional manner.	• "Hu, Y." in [17] proposes Secure Neighbor Detection, Secure Route Delegation, and Randomized RREQ forwarding. • Secure Neighbor Detection allows each neighbor to verify that the other is within a given maximum transmission range. • The Randomized Selection of RREQ message to be forwarded, replaces traditional duplicate suppression in on demand route discovery.	• It will require extra hardware to determine the location of nodes using GPS or synchronized clock.

© 2016, IJCSMC All Rights Reserved

4.	**Wormhole Attack** • Two or more colluding malicious nodes captures the traffic at one end replays at the distance location bypassing the intermediate nodes. • The malicious nodes create a tunnel to give an impression that the two nodes are one hop away and thus provide the shortest path to the destination. • The tunnel can be established by either In-Band Channel or Out-Band Channel. • The pair of colluding malicious node creates traffic choke points which can be utilized to launch the active or passive attacks. • It is equally dangerous for both proactive and reactive routing protocols. It is possible even if communications provide authenticity and confidentiality.	• "Hu, Y." in [18] has proposed Temporal and geographical Packet Leaches to protect against the attack.	• Require extra hardware in terms of GPS / tightly synchronizes clock.
		• "Mary, E." in [8] has proposed Wormhole Secure Routing using certificate chaining has been proposed. • The protocol uses round trip time (RTT) between nodes to issue certificates to the legitimate nodes.	• The technique may give false alarm due to variations in the RTT.
		• "Mahajan, V." in [19] proposes a technique that exploits the anomaly in the network behavior for in-band wormhole attack in proactive protocol. • The anomalies in the path length and in incompatible hop delays and end-to-end delay have been used to detect Wormhole.	• Detection with moderate traffic overheads.
5.	**Sybil Attack** • Malicious node creates and controls multiple identities. • Exploits vulnerability of absence of any centralized identity management mechanism. • Malicious node can either create a new identity after discarding the previously created identity or can create several identities simultaneously with the aim to cause disruption in the network. • The Sybil attack can affect both proactive and reactive routing protocols.	• "Abbas, S." in [10] has proposed, Distributed technique for Sybil attack detection when attacker concurrently uses all the identities. • Movement of all the identities when the node moves in the network is captured. • Identities travelling the same path are considered Sybil identities.	• GPS for location determination and directional antenna are required
		• "Kesidis, S." in [7] has proposed, a technique which utilizes received signal strength in order to differentiate legitimate and Sybil nodes. • The entry and exit behavior of the nodes is analyzed and is compared against a threshold.	• Light weight technique with low traffic overheads. No extra specialized hardware like directional antennas, GPS and centralized TTP required.
6.	**Flooding attack** • A malicious node can flood the network with route request to the nonexistent or arbitrary destinations. • The purpose is to unnecessarily use bandwidth, computational resources, memory resources, power resources, and prevents the normal operation of the routing-protocol.	• "Zhang, S" in [20] has proposed a technique in which each node monitors its neighbors' RREQ and if rate exceeds the predefined threshold, the node is declared as malicious.	• Attack goes unnoticed below the fixed threshold. • Legitimate node may get blacklisted if identity is impersonated by malicious node.
		• "Desilva, S." in [21] has proposed an improvement to fixed threshold for deciding the malicious behavior of flooding node.	• Reduces the impact of the attack for varying flooding rates.

© 2016, IJCSMC All Rights Reserved

	• Broadcast of RREQ in Reactive routing protocols and TC control messages in Proactive routing protocols.	• The proposed technique is an adaptive technique based on statistical analysis to decide the threshold for declaring a malicious node.	

IV. CONCLUSIONS

In this paper we have analyzed the routing process, their vulnerabilities and the various types of attacks which can be launched by exploiting the same, to disrupt the routing process or launch DoS attacks. We have also reviewed the possible countermeasure against these attacks and listed out the advantages as well as the limitations of the countermeasures, the same have been summarized in Table 1. It has been observed that although active research is being carried out in this area, the proposed solutions are not complete. There are limitations in all solutions which may be of high computational or communication overhead or the ability to cope with single malicious node and ineffectiveness against multiple colluding malicious nodes. Some solutions require specialized hardware like GPS or directional antennas and some other may require major modification of the existing protocol. In most cases the proposed solutions are able to combat only one or two types of attacks and are still vulnerable to unexpected attacks. The research therefore has to be not only to improve the effectiveness of the security schemes but also on minimizing the cost to make them suitable for a MANETs.

REFERENCES

[1] Bakht, H., "Survey of Routing Protocols for Mobile Ad Hoc Networks", International Journal of communication technology and research, vol. 1(6), Oct. 2011.
[2] Perkins, C., et al. "Ad hoc On-Demand Distance Vector (AODV) Routing" RFC 3561.
[3] Mohseni, S. et al., "Comparative Review Study of Reactive and Proactive Routing Protocols in MANETs", 4th IEEE DEST 2010
[4] Mulert, J. V. et al., "Security Threats and Solutions in MANETs: A case study using AODV and SAODV", Journal of Network and Computer Application, vol. 35, no. 4, pp. 1249-1259, Feb. 2012.
[5] Nakayama, H. et al., "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communications, October 2007
[6] Sen, J. et al., "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", ICICS, 2007
[7] Kesidis, G. at al., "Robust Sybil Detection for MANETs", 18th ICCCN (IEEE), 2009.
[8] Mary, E. at al., "A Certificate-Based Scheme to Defend Against Worm Hole Attacks in Multicast Routing Protocols for MANETs", IEEE Conference on Network Security, 2010.
[9] Brooke, J. et al., "Towards Sybil Resistant Authentication in Mobile Ad Hoc Networks", Fourth International Conference on Emerging Security Information, Systems and Technologies (IEEE), 2010.
[10] Abbas, S. et al., "Lightweight Sybil Attack Detection in MANETs", IEEE Systems Journal, Vol. 7, No. 2, June 2013.
[11] Hafeez, R. et al., "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, vol. 2(3), Jan. 2008.
[12] Mitchell, C. J. at al., "Malicious attacks on ad hoc network routing protocols." International Journal of Computer Research, 2009.
[13] Chavda, K. et al., "Removal of Black Hole Attack in AODV Routing Protocol of MANET", 4th ICCCNT, Tiruchengode, July 2013.
[14] Abdelhaq, M. et al. "A local Intrusion Detection Routing Security over MANET Network", International Conference on Electrical Engineering and Informatics, Indonesia, July 2011.
[15] H. Deng at al., "Routing security in ad hoc networks", IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, 2002.
[16] Howarth, M. P. et al., "A survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, 2013.
[17] Hu, Y. at al., "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the ACM Workshop on Wireless Security, SanDiego, California, pp. 30-40, September 2003.

© 2016, IJCSMC All Rights Reserved

[18] Hu, Y. et al., "Wormhole Attacks in Wireless Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370-380, February 2006.
[19] Mahajan, V. et al., "Analysis of Wormhole Intrusion Attacks In MANETs", MILCOM (IEEE), 2008.
[20] Zhang, S. at al., "A New Routing Attack in Mobile Ad Hoc Networks," International Journal of Information Technology, vol. 11, no. 2, pp. 83-94, 2005.
[21] Desilva, S. at al., "Mitigating Malicious Control Packet Floods In Ad Hoc Networks," Proceedings of IEEE Wireless Communications and Networking Conference 2005, vol. 4, pp. 2112- 2117, March 2005.

© 2016, IJCSMC All Rights Reserved