Volume 4, Issue 4, April 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review on Detection of Blackhole Attack Techniques in MANET

Pooja
MTech Scholar
Department of Computer Science and Applications
Kurukshetra University, Kurukshetra, India

Vinod Kumar
Asst. Professor
Department of Computer Science and Applications
Kurukshetra University, Kurukshetra, India

Abstract- Mobile Ad-Hoc Networks (MANET) is top area of research. MANET is self-configured, self- administered and self-organized network. In MANET, nodes are not bodily connected to each other, but the communication can takes place if nodes are in each other's transmission range. Because of mobile nature of nodes, the topology of MANET changes from time to time and they lack fixed infrastructure, due to which MANET is open to many security attacks. In this paper, the author discusses Blackhole Attack, which is one of the serious attacks in MANET and comparison of various Blackhole Attack detection techniques.

Keywords- MANET, Blackhole Attack, Security issues, Techniques, Metrics

I. INTRODUCTION

MANET is a combination of three words: Mobile means which is in moving state, Ad-hoc means for temporary purpose and NETwork means collection of computers. MANET consists of wireless mobile nodes and forms a network for temporary purpose. Nodes in MANET can both act as host or router. MANET has no centralized authority and fixed infrastructure in MANET. The characteristics of MANET pose a number of challenges and these are:

Dynamic topologies: Due to dynamic nature of MANET the nodes are moving randomly which changes their topologies with time. This includes Unidirectional and Bidirectional Links as shown in figure 1[16].

Bandwidth restrictions: In MANET, links between the nodes have lesser capacity than their wired networks.

Energy-constrained operation: All nodes in MANET depend on batteries for their energy. So energy conservation is the important system design criterion for optimization.

Limited physical security: Wireless networks are susceptible to security attacks like eavesdropping, IP spoofing and denial-of-service (DOS) attacks.

Limited Resources: MANETS have low computational capacity and storage capacity.

Multihop Communication: Multihop communication implies that if source node and destination nodes are not in the transmission range, then communication will take place with the support of other nodes.

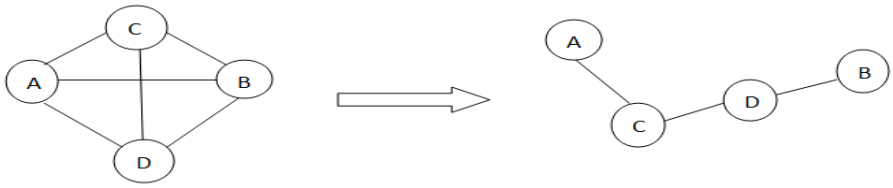

Fig. 1 Dynamic Topology of MANET

To provide a secure networking environment following services [10] are required:

Authentication: A node must identify with whom it is communicating with.

Confidentiality: Information is never revealed to intruder.

Integrity: The sent message should not be altered in between the transmission.

Non-repudiation: After sending the information, the sender cannot refuse and after receiving the information, the receiver cannot refuse.

Availability: All Nodes should be available all the time for communication. A node need continue to provide services despite attacks eg: key management service.

Detection and isolation: Protocol should discover malicious nodes and isolate them, so that they cannot interfere with routing.

1.1 Classification of Attacks:

On the basis of the source of the attacks [6]:

1. **External attack**: External attack occurs because of the nodes that are not the part of the network.
2. **Internal attack**: Internal attack occurs by the nodes that belong to the network (compromised nodes).

On the basis of the behavior of the attacks [6]:

1. **Passive Attacks**: They obtain the information of data exchange in the network but do not cause any modification in the data or do not disrupt the ongoing communication [11].
2. **Active Attacks**: They obtain the information of data exchange in the network and modify the data or disrupts the ongoing communication[11]

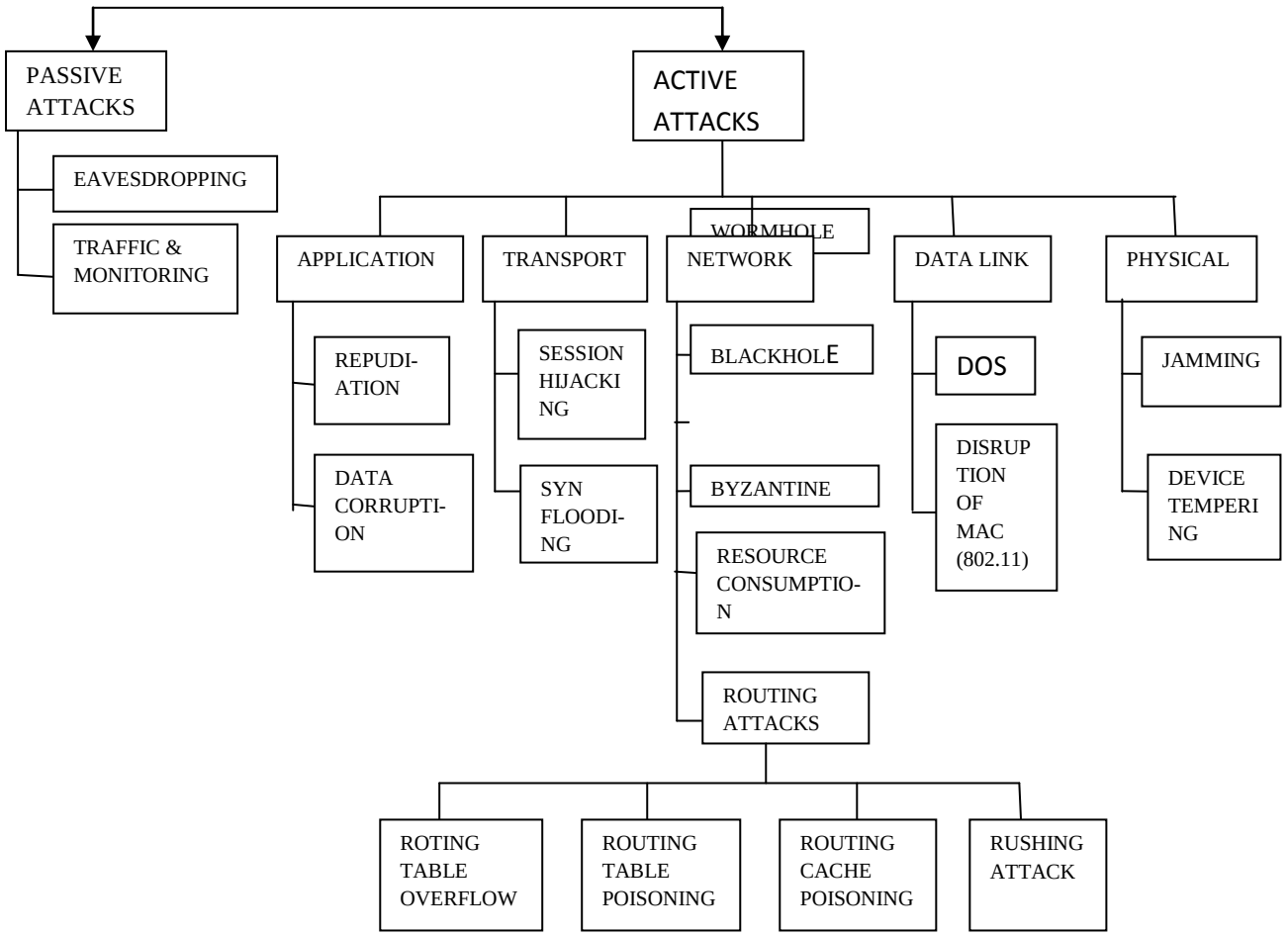

Fig. 2 Attacks on Protocol Stack

II. BLACK HOLE ATTACK

It is very severe attack in MANET. In Black hole Attack, an nasty node broadcasts to all the neighbor node that it has the smallest route to the goal node without looking into its routing table. Source will forward its data to this malicious node. And after getting all the data it does not forwards to the destination, but drops all the data [1].

Figure 3 explains the how Black hole problem occurs. Node A sends data to node D and the route finding process is started. It sends RREQ message to all its neighbor nodes. Node C is nasty node and declares that it has smallest route to the target node. It will then send the RREP message to the node A. Node A will assume that this is the shortest route and will overlook all other replies. When node C received all data packets, it will crash all data. Like this, a nasty node attracts all the net traffic towards itself by advertises that it has the smallest path to the goal node, hence reason data loss in the network.

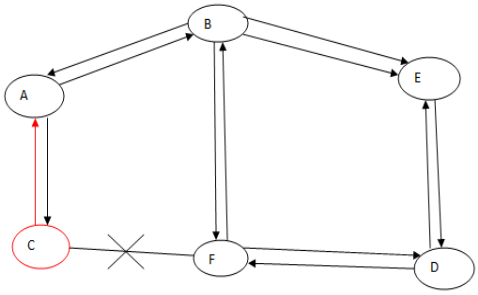

Fig. 3 Black Hole Problem

In AODV, we can categorize a black hole attack [6] in two types:

- **Internal Black Hole Attack:**
  In this type of attack, an internal nasty node fits itself in between route of the sender and receiver. Once it gets chance the nasty node makes itself as a authorized node. Then after it can disturb the ongoing communication of the network
- **External Black Hole Attack:**
  An external attack actually remains outside of the net and refuses access to network traffic or creates jamming in network or by aborts the operation of entire network. It can become an internal attack when it take in charge of internal nasty node and manage it to hit other nodes in network zone.

A. Single Black hole Attack:

In single black hole attack, there is only one malicious node in a zone. Other nodes will be authorized node [2].
As shown in figure 3. Node A is starting node and Node D is ending node. Node C is a malicious node and replies the RREQ packet sent from starting node A, and makes a fake reply that it has the smallest route to the ending node. So node A thinks the route discovery process is completed, and starts to send data packets to node C. In MANET, a malicious node drops all the data packets. This problem is known as a black hole problem in MANET.

B. Collaborative Black hole Attack:

In this blackhole attack, more than one malicious nodes are present in the network. It is also known as Black Hole Attack with malicious nodes [2]. Figure 4 shows the collaborative BlackHole Attack, in which the two malicious nodes are C and D. Node A is the source node and node G is the destination node.

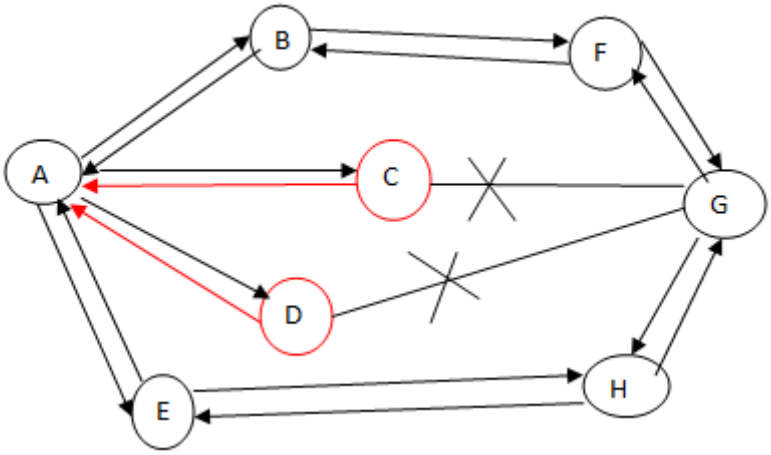

Fig. 4 Collaborative Blackhole Attack

III. LITERATURE SURVEY

Rajib Das et al. [12] proposed an algorithm which focused on analyses and improves the security of AODV protocol. Their algorithm can detect and remove Blackhole nodes from MANET at the starting. Their paper also provided a practical study which shows effects of blackhole attack.
Semih Dokurer et al. [13] presented a very easy solution to conquer black hole. Their solution enhanced the network performance by 19% in the presence of black hole. Their study investigated the consequences of black hole attacks on the network. For this purpose they introduced a new protocol called "BLACKHOLEAODV". After that they implemented a new protocol called "IDSAODV". They compare the results with and without black hole in the network.
Mangesh et al. [5] explained all the existing countermeasures for the Network layer attacks. They gave countermeasures for Blackhole attack, Wormhole Attack, Impersonation Attack, Modification Attack, Denial of Service Attacks, Grayhole Attack, Sybil attack, Packet drop attack, Byzantine Attack and Location Disclosure Attacks.
Elmar Gerhards-Padilla et al. [14] presented a TOGBAD (Topology Graph based Anomaly Detection) approach to detect Blackhole Attack in Tactical MANET. It was new centralized approach used topology graphs to identified nodes which creates black hole. To obtain the information about the network topology, they used well-established techniques.
Arnab Mitra et al. [3] proposed a Black Hole Detection tactic and alive nodes detection methodology which was based on Artificial Neural Network (ANN). That approach was helpful in minimizing the damage in reliable routing procedure. They used computation which was based on Perceptron model to the spot black hole and alive node. Their proposed tactic was implemented at both ends of a MANET structural design.
Swati Saini and Vinod Saroha [4] proposed an algorithm which was based on Fuzzy Logic to detect a black hole with AODV protocol. They also analyzed Packet Loss, Packet Loss Rate, Last Packet Time, Packet Delay and Bit Rate.

From the above study I have summarized the following comparisons among various techniques. I have listed their tool used, Routing protocol, Metrics, advantages and disadvantages.

Table 1 Comparison of various Blackhole Detection Techniques

PARAMETERS → / TECHNIQUES ↓	TOOL	ROUTING PROTOCOL	METRICS	ADV.	DISADV.
IDSAODV	NS-2	AODV	1. Packet Loss	1. Reduced the packet loss by about 19%. 2. No modifications in packet format. 3. No additional overhead.	1. Third RREP message did not have positive results to the packet loss.
DPRAODV	NS-2	AODV	1. Packet Delivery Ratio. Avg.end-to-end delay 2. Normalised routing overhead	1. Very simple and efficient way. 2. Increases the PDR.	1. Increases avg.end-to-end delay. 2. Increases Normalized routing overhead.
TWO AUTHENTICATION MECHANISM (MAC & PRF)	NS-2	AODV	1. Packet Delivery Ratio 2. Control overhead 3. Delay 4. Detection time	1. Two Authentication Mechanism eliminate the need of PKI.	1. Did not discuss about handling of unlimited message
WAIT & CHECK	GloMo Sim	AODV SAODV(proposed)	1. Packet Delivery 2. Ratio average end-to-end delay 3. Routing Overhead	1. In SAODV PDR increases up to 90-100%. 2. Increases avg. end-to-end delivery.	1. Increases waiting time 2. Routing overhead is slightly more
TOGBAD	NS-2	OLSR	1. Packet Delivery Fraction(PDF) 2. diff	1. Detect a black hole node immediately.	1. Does not examined attacks against itself

The following terms must be known to the readers:

1. **Metrics** [16**]** is a property of a route in computer networking. It consist any value used by a routing protocol to decide this route should be chosen or another. The routing table includes only the best feasible routes, while topological databases or link-state may include all other information. For example, Routing Information Protocol uses the metric called hop count to decide the best feasible path. The data will be routed in that direction of the gateway which has smallest hop count.

In above table following metrics are used:

- **Packet Loss:** In Packet loss, some data packets are discarded due to the network error or buffer overflow.

- **Packet Delivery Ratio:** $\frac{\text{Data received by the receiver}}{\text{Data sent out by the sender}}$

- **Average End-to-end delay:** Total time taken by the packet to reach the destination from the source across the network. It can be calculated as:

$$d_{end\text{-}to\text{-}end} = d_{transmission} + d_{propogation} + d_{processing}$$

- **Normalized Routing overhead:** $\frac{\text{Routing-related transmissions (RREQ, RREP, RERR etc)}}{\text{Data transmissions in a simulation}}$

- **Control overhead**: In Control Overhead, Transmissions are counted instead of packets.

- **Detection Time**: It is measured by:

  The attack detection time - the traffic start time

IV. PROPOSED WORK

From the analysis of existing solutions for malicious node detection and prevention, MAC based solutions are quite suitable for mobile ad-hoc networks and have good performances if they are well designed. A solution for Black hole attack detection and prevention is proposed that uses the one-way-hash function H to generate MAC for RREP packet.

A **Message Authentication Code** (**MAC**) is a small part of information, which is used to authenticate and to provide integrity on the message. Cryptographic Hash Function is the only possible way to generate MACs. A MAC algorithm, accepts a variable length message as input, and outputs a fixed length MAC, also known as tag.

In cryptography, a **keyed-hash message authentication code** (**HMAC**) is a unique method for generating a MAC. It uses a cryptographic hash function with a mixture of secret cryptographic key. There are so many cryptographic hash function, such as Message-Digest algorithm (MD5) or Secure Hash Algorithm (SHA-1), they can be used in the generation of an HMAC; the resulting MAC algorithm is known as HMAC-MD5 or HMAC-SHA1 respectively.

V. CONCLUSION

MANET is fastest growing area of research today. Because of its dynamic nature, it is open to many attacks. This paper firstly discusses the brief introduction of MANET, its issues, services provided by a secure network framework and classification of attacks. Then an introduction about MANET is given. The paper surveys the research work of different authors. Some authors modified the existing protocols and some proposed their new protocols. Then a comparison of Blackhole detection techniques in a tabular form is given.

REFERENCES

[1] Tarunpreet Bhatia, A.K.Verma, "Security Issues in MANET: A Survey on Attacks and Defense Mechanism", International Journal of Advanced Research in Computer Science and Software Engineering, vol.3, issue 6, pp.1382-1394, 2013.

[2] Kriti Gupta, Maansi Gujral and Nidhi, "Secure Detection Technique Against Blackhole Attack For Zone Routing Protocol in MANETS", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 6, June 2013.

[3] Arnab Mitra, Rajib Ghosh, Apurba Chakraborty and Debleen Srivastva, "An Alternative Approach to Detect Presence Of Black Hole Nodes in Mobile Ad-Hoc Network Using Artificial Neural Network ", International Journal of Advanced Research in Computer Science and Software Engineering, vol.3, issue 3, pp.113-122,2013.

[4] Swati Saini and Vinod Saroha, "Analysis and Detection of Black Hole Attack in MANET", International Journal of Science and Research, vol.2, issue 5, 2013.

[5] Mangesh M Ghonge, Pradeep M Jawandhiya and Dr.M S Ali, "Countermeasures of Network Layer Attacks in MANET", IJCA Special issue on "Network Security and Cryptography", NSC, 2011.

[6] Irshad Ullah and Shoaib Ur Rehman, "Analysis of Black Hole Attack on Mobile Ad Hoc Networks using Different Manet Routing Protocols" June 2010.

[7] Payal N. Raj and Prashant B. Swadas**, "**DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET**",** IJCSI International Journal of Computer Science Issues, Vol. 2, ISSN (Online): 1694-0784, ISSN (Print): 1694-0814,2009.

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

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

[10] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and solutions", IEEE Wireless Communications. 11 (1), pp. 38-47,2004.

[11] Sevil Sen, John A. Clark, Juan E.Tapiador, "Security Threats in Mobile Ad Hoc Networks".

[12] Rajib Das, Dr.Bipul Syam Purkayastha and Dr.Prodipto Das, "Security Measures for Black Hole Attack in MANET: An Approach".

[13] Semih Dokurer, Y.M.Erten and Can Erkin Acar, "Performance analysis of ad-hoc networks under black hole attacks".

[14] Elmar Gerhards-padilla, Nils Aschenbruck and Peter Martini, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs Network ", 32nd IEEE Conference on Local Computer Networks.

[15] Sridhar Iyer, IIT Bombay http://www.it.iitb.ac.in/~sri/talks/manet.ppt.

[16] http://en.wikipedia.org/wiki/Metrics_(networking).

