iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** XI **Month of publication:** November 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review of Detection & Prevention Techniques of Black & Gray Hole Attacks in MANET

Manan Arora
Student M.Tech (IT), Department of Computer Science, Lovely Professional University, Phagwara, India

Abstract- Mobile ad hoc network (MANET) is a self-organizing, self-configuring wireless network consisting of mobile nodes. It does not require any centralized access point. There is no need for any fixed infrastructure for nodes to communicate between themselves. Manet is vulnerable to various attacks due to lack of centralized monitoring and regular changing topologies. Security has become one of the challenging issues to protect MANET from various malicious attacks and provide protected communication between nodes. In this paper a study made on different methods that have designed to detect and prevent Black and Gray hole attack in MANET. A comparison table is designed to compare different methods.
Keywords- MANET, Gray hole attack, Black hole attack, AODV

I. INTRODUCTION

The rapid growing technology in wireless network has directed in the development of new communication system. As a result we are getting a new network called Mobile Ad hoc Network (MANET). Mobile Ad hoc Network is a collection of self-configuring & self-maintaining mobile nodes that do not require any fixed infrastructure to communicate. In MANET if source and destination node are within the communication range of each other than source node can send the packet to destination node directly otherwise intermediate nodes are responsible to route the packet from source to destination node.

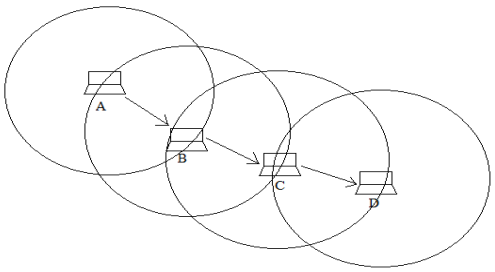


Figure 1: Ad hoc Network

Routing in Mobile Adhoc Network has become a challenging task due to regular changing topology. The mobility feature of MANET make it difficult to securely route the packet from source to destination. In MANET, there is no restriction on nodes to join or leave the network, therefore any node can leave or join the network at anytime. This property of MANET makes it very difficult to secure the MANET from various type of attacks including Black & Gray hole attacks. The paper investigate the different methods for preventing and detecting black & gray hole attacks.

Rest of this paper is organized as follows. In section 2, we discuss about AODV protocol. Black and Gray hole attack is discussed in section 3 & 4 respectively. In section 5, Review of different methods has been discussed. Section 6 comprises the different methods. Finally in section 7, the conclusion has been presented.

II. AODV ROUTING PROTOCOL

AODV is an ad-hoc on demand distance vector routing protocol that establishes route to the destination when it is desired by the source node. It maintains these routes as when needed by the source node. It offers quick adoption to dynamic link conditions, low processing, memory overhead, low network utilization, and determines unicast routes to the destinations within the ad-hoc network [1]. Route Request (RREQ), Route Reply (RREP), Route Error (RERR) messages are three control packets that are used in AODV. RREQ and RREP are used in route discovery process and RERR is used in maintenance phase [2]. AODV also maintains destination sequence number for each routing table entry.

AODV protocol firstly discover the route by using route discovery process, In route discovery process firstly, source node broadcast a Route Request Packet (RREQ) to all its neighbors, and they transmits packet to their neighbors until and unless

they find a valid route to the destination. After receiving Route Reply (RREP) messages, source node check its table and selects the route with the highest sequence number. If a link breaks, neighbors of that link broadcast Route Error Message (RERR) through the network to alert other nodes about this failure [2].

III. BLACK HOLE ATTACK

Black hole attack is one of most frequent attack that happened in the network. In black hole attack the malicious node falsely advertise that it has the shortest path to the destination. The reason behind such malicious activity is to stop the destination from receiving the packets. In Black hole attacker introduced itself as the destination or it has the shortest path to the destination by replying with a high sequence number RREP message. The source node selects the high sequence RREP message and ignores all other RREP message including the correct ones and starts transmitting the data packets to the malicious node. The malicious node will not forward any data packet to other nodes instead it will drop all the data packets. This type of attack is very severe to detect and we proposed a technique to detect black hole attack.

IV. GRAY HOLE ATTACK

Gray hole attack is bit similar to black hole attack with a small variation where the malicious node does node drop the whole packets instead it will drop some selective packets. In Gray hole [2] attack, a node which is member of the network, gets RREQ packets and create a route to destination. After creating the route, it drops some of data packets. Gray hole attack is very difficult to detect because malicious node do not drop data packets regularly but instead it will drop the data packets occasionally. Therefore sometimes node will act normal node and sometime node switch to malicious node.

V. REVIEW OF THE METHODOLOGIES

In the below section, review of different methods for detection and prevention of black and gray attacks has done.

A. First Methodology

Processes for Detection and Removal of Gray & Black hole attacks are [3,5] :

1) Source Node detection process of Gray & Black hole

a) Divides all data packets into **k** equal parts.
b) Send a message to destination node informing number of packets to be sent.
c) Broadcast the messages to all the neighbours and instruct them to monitor next node.
d) Source node starts data transmission.
e) Set timer until get number of packet destination received.
f) Initiate removing process, if announced packets is not equal to received packets.
g) Starts removing process of black/gray hole if no message received till timer terminated.

2) Destination Node detection process of Gray & Black hole: After receiving the packets from source containing the information of number of packets to be send by source. Destination node sets the timer to zero and starts counting the packets. After counting the packets, send received packet number to source. If any difference between packets number, starts gray & black hole detection.

3) Neighbourhood Nodes detection process of Gray & Black hole: After receiving a neighbourhood monitoring message from source node, all the nodes starts a packets counter to count packets of its neighbour.

4) Source Node removal process of Gray & Black hole

a) Source node gets vote of one node's neighbours about the maliciousness.
b) According to the votes of neighbours, starts counter for malicious node in finding malicious table.
c) If votes of neighbours about maliciousness exceeds from a limit, source enters that node in Gray & Black hole table and finds a route to the destination.

5) Neighbours Node removal process of Gray & Black hole: After getting monitoring message, neighbour nodes start counting numbers of packets that malicious node sends. If number of passed messages is less than a limit, inform about it to source node.

B. Second Methodology

SCAN [6], implements two protect Mobile Ad hoc Network:

1) Local Collaboration: In this, all neighbouring nodes monitor each other and also sustain the routing table of each other. A token authentication system is used by each node for authentication in the network. If a suspicious node is found in the network, other nodes revoke its token and alert token revocation to all other nodes. After that, suspicious node inserted in token revocation list. Malicious node will isolate from network.
2) Information Cross-Validation: Each node monitors its neighbour nodes information by cross-checking neighbours routing tables and overheard transmission.

C. Third Methodology

The method [7] is based on Intrusion Detection System nodes. IDS nodes protect the network from Black hole attack. Every IDS nodes in the network covers an area.

Assumption in the algorithms:

1) IDS nodes are in each other range that can exchange BLOCK messages for detecting black hole messages.
2) Authentication mechanism is considered between IDS nodes, so that one IDS node cannot change or drop BLOCK messages.
3) Every IDS should overhear its area's routing messages.

D. Forth Methodology

The Watchdog Method [8] uses a watchdog timer for the detection of malicious node in the network. Every node monitors its next neighbour node. If any node finds packet forwarding misbehaviour or any packet dropping in a predefined period of time for its next node, the next node announce as malicious node to the source.

E. Fifth Methodology

This Method [9] is based on Optimal Path and Hash Scheme. The Method selects the second shortest route for the transmission of data packets and avoids the Black & Gray hole attack by discarding first shortest route. The method also provides more security for data integrity.

VI. COMPARISION OF DIFFERENT METHODS ON GRAY & BLACK HOLE ATTACK

In this section, a comparison of different methods is done. This comparison is based on different parameters.

Table 1: Comparison of methods

Methods for Detecting attacks	Black hole attack detection	Gray Hole Attack Detection	Mistakes in Detection of attacks	Overhead
1) Detection & Removal of cooperative Black & Gray hole attack in MANET	Yes	Yes	Few	Overhead of voting from neighbours
2) Detection Using SCAN approach	Yes	Yes	Many(as it do not use threshold value)	Use token authentication technique for each node
3) Prevention of Black hole attack using Intrusion Detection System	Yes	No	Few	IDS

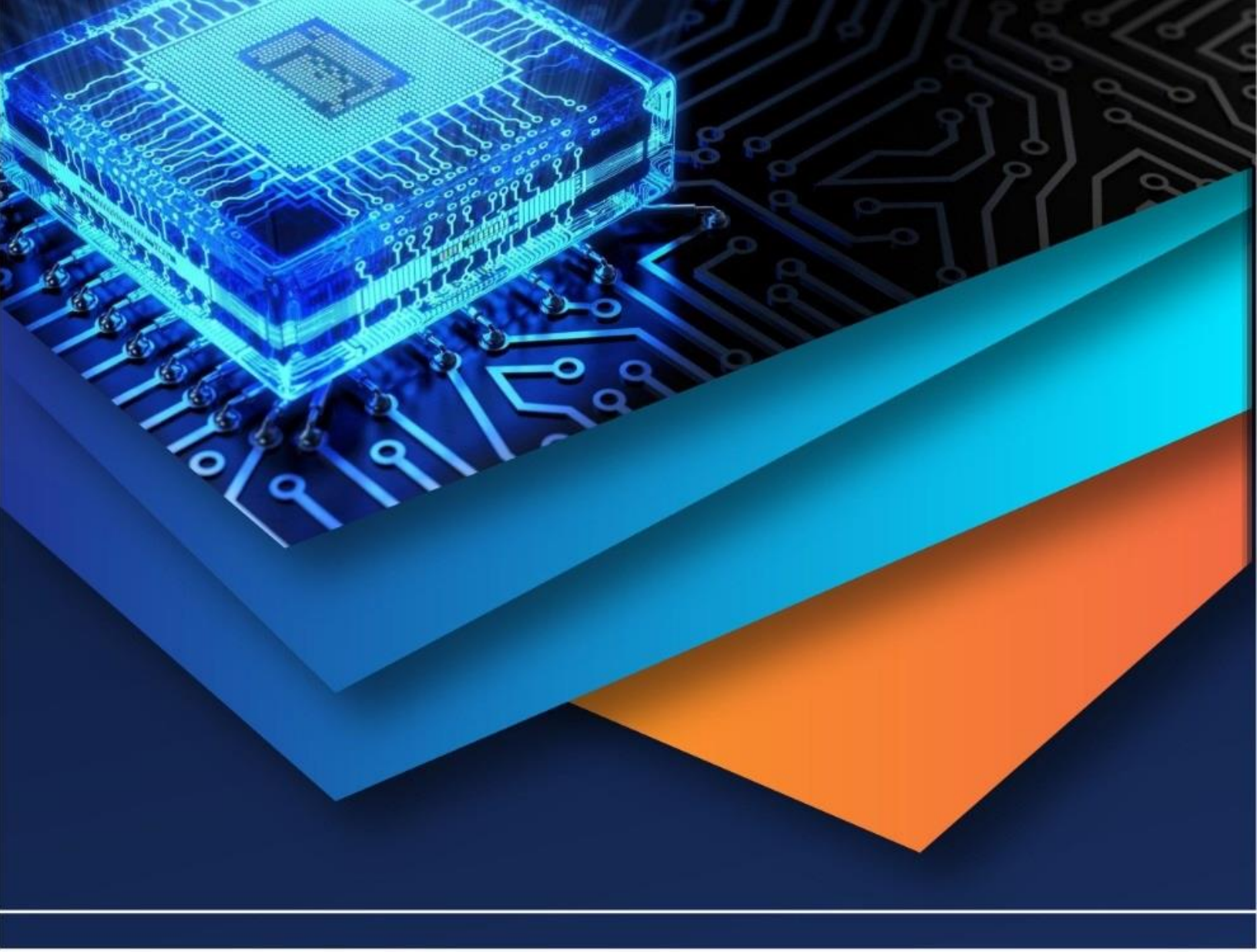
4) Detection Using Watchdog Technique	Yes	Yes	Many	Monitoring of next node
5) A Mechanism for detection of Gray hole attack in MANET	Yes	Yes	Few(as it is using three times chances)	DRI tables, probe packets
6) A method for detection of cooperative Black hole attack in MANET	Yes	No	Many	DRI tables, cross checking method
7) Prevention of black/gray hole attack using Optimal Path	Yes	Yes	Few(because it always select the second-shortest route)	None
8) A Mechanism to prevent black /gray hole attack using Destination Sequence Number	Yes	Yes	Few	DSN threshold value comparison

VII. CONCLUSION

This paper shows the various works related to prevention and detection of Black and Gray Hole attacks in Mobile Ad-hoc Network. Black and Gray hole attack reduces the performances of the network and also affects the end to end packet delivery ratio. Gray hole attacks are more hard to detect than Black hole as in gray hole nodes suddenly act as malicious and suddenly as normal. This paper also comprises the different methods introduce for detecting and preventing Black and Gray hole attack. Each method has its advantages and limitations.

REFERENCES

[1]. Nitesh A. Funde, P. R. Pardhi, "Detection and Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2013
[2]. Marjan Kuchaki Rafsanjani, Zahra Zahed Anvari, Shahla Ghasemi, "Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET", IJCA Special Issue on " Network Security and Cryptography" NSC,2011
[3]. 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
[4]. Harmandeep Kaur, Ramanjit Singh, "A Novel Approach to Prevent Black Hole Attack in Wireless Sensor Network", International Journal For Advance Research in Engineering and Technology, Vol. 2, Issue VI, June 2014
[5]. Shalini Jain, Mohit Jain, Himanshu Kandwal, "Advanced Algorithm for Detection and Prevention the Cooperarte Black and Gray Hole Attacks in Mobile Adhoc Network", 2010 International Journal of Computer Applications(0975-8887), Volume 1 – No.7
[6]. H. Yang, J. Shu, X. Meng, S. Lu, "SCAN: Self-Organised Network-Layer Security in Mobile Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, Vol. 24, Issue 2, pp. 261-273, February 2006
[7]. M. Su, Y. Su, " Prevention of Selective Black Hole Attacks on Mobile Ad hoc Network through Intrusion Detection System", Computer Communication, Vol. 34 , Issue 1, pp. 107-117, 2011
[8]. Sergio Marti, T. J. Giuli, Kevin Lai, Mary Baker, " Mitigating Routing Misbehaviour in Mobile Ad hoc Networks", In Proceedings of the 6th Annual International Conference on MOBICOM, Bostan, Massachusetts, United States, 255-265, 2011
[9]. Hizbullah Khattak, Ni-zamuddin, Fahad Khurshid, Noor ul Amin, "Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash", IEEE (645-648) 978-1-4673-5200-0/13/2013
[10]. Meenakshi Patel, Sanjay Sharma, "Detection and Prevention of Routing Attacks in MANET using AODV", ISSN : 2277-9043 International Journal of Advanced Research in Computer Science and Electronics Engineering, Volume 1, Issue 1, March 2012



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY