iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

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

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Survey on Black Hole Attack Detection and Prevention Techniques

Neha[1], Manmohan Sharma[2]
School of Computer Science and Engineering, Lovely Professional University, India

Abstract- Mobile Ad Hoc Network can be defined as a system of self governing, independent mobile nodes that communicate over wireless links with no fixed infrastructure. Due to its fundamental characteristics like lack of fixed infrastructure, dynamic topology and wireless nature, MANET faces various security issues. One such security issue is Black Hole Attack. In this attack, malicious node pretends itself as a node having shortest path from source to destination. As a result, source node decides to transmit data through malicious node and then malicious node decides whether to forward or drop the packet sent by sender. So, to provide secure transmission against Black Hole Attack, researchers from time to time proposed different security measures and routing protocols. This paper summarizes and compares the work done by some of these researchers.
Keywords- MANET, Black Hole Attack, AODV, Flooding, Security

I. INTRODUCTION

Mobile ad-hoc network [1][3][4], is a wireless network having no fixed infrastructure for communication and each node, itself, act as a router and is responsible for receiving or sending of messages. There is no centralized node which means that network is to be managed by each node involved in network. It can also be defined as a system of independent, self governing mobile nodes that transmit information to other nodes in network without any fixed infrastructure. This is in contrast to cellular network where two mobile nodes communicate through wires and cables.

Communication in MANET is carried out in two different ways: one, direct communication which takes place when nodes are inside the range of one another. However, problem arises when the communicating nodes are not within range, then they use peer-to-peer multi hop communication via intermediate nodes. MANET's usually use on demand routing protocols based on flooding technique.

Routing is to find route through which message from sender will be delivered to receiver or reply from receiver will be received by sender. For transmission of messages in multi hop, MANET uses reactive protocols, shown in figure1, which are based on flooding technique.

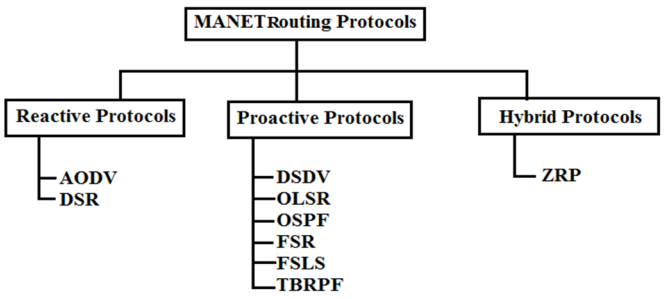


Figure 1 Hierarchy of routing protocols

Flooding[1][2][5][6] is a technique in which a node sends the message to all its neighbors and those neighbors further broadcasts the message till it gets distributed in entire network. Transmission of message in such way is referred as blind flooding but sometimes broadcasting of message is limited to some geographical area or some specific nodes, this refers to efficient flooding. However, flooding itself has some issues of overhead and collision and to solve them, researchers are working from long time.

MANET, because of its basic characteristics, is more susceptible to security attacks as compared to wired network. Attacks in MANET are classified on the basis of source of attacker or on the basis of behavior of attacker. On the basis of source, it is further

©IJRASET 2015: All Rights are Reserved

categorized into External attacks, in which attacker is not part of network but tries to access the network and on getting access, it start doing activities which interrupt the performance of network and Internal attacks, in which intruder is part of network. The attacker remains inside the network and try to have access to the messages for which it is not authorized. And on the basis of behavior, it is categorized into Active attacks, in which intruder try to modify messages sent by sender and Passive attacks, in which intruder only listen the communication between sender and receiver, rather than doing any modification to the messages being sent. MANET also faces the problem of:

A. Wormhole attack*:* In this, packet received from one location is send to some other location on a single route only. It detects the single route and will use it repeatedly. So, it prevent discovery of any other route in the network for the same source and destination node.
B. DoS attack*:* In this, excessive messages are sent to server or in network to reject valid user's access to resource or server and the return address are invalid in it.
C. Grayhole attack*:* In this attack, malicious node fakes that it has valid route to D but when message is sent to it, it simply drops it instead of sending to D. Grayhole attack is different from Blackhole attack.
D. Selfish node attack: In this, malicious nodes are not part of network but use network resources and save own resources.
E. Flooding attack: In this, network is flooded with packets. Depending on type of packet used, it is classified into three types namely: HELLO flooding, RREQ flooding and DATA flooding.

II. BLACK HOLE ATTACK

Black Hole Attack [11][12][8][9], is one of the security attacks in which malicious node promotes itself as a node which has shortest path from source to destination. Black Hole Attacks are categorized into [9]: Single Black Hole Attack and Cooperative Black Hole Attack.

A. Single Black Hole Attack: These are the attacks in which only one node act as malicious node in whole network.
B. Cooperative or Collaborative Black Hole Attack: These are the attacks in which multiple nodes as a group act as malicious nodes.

In [12], it is explained that when a node wishes to send data to any other node in network, it sends a RREQ message to all its neighbors that may include the malicious node as well. If any node has fresh route from itself to destination, it responds to RREQ message. If reply from normal node reaches the source node first, whole transmission works well, but if reply from malicious node reaches source first, it makes source node think that the route discovery process is complete and it starts sending messages through malicious node. As a result, all the packets sent by sender to destination through the malicious node get lost.
The complete scenario [9] of black hole attack is shown in Figure 1 and explained below.

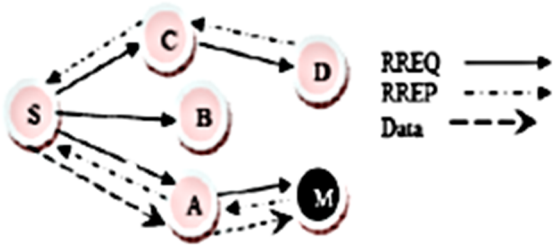


Figure 1 Black hole attack [9]

Here node S is the source node which wants to have communication with node, D considered as destination. So, node S will first send a RREQ message to all its neighbors namely A, B and C. If node A has a route to D, it will send a RREP message to S. But node M being the malicious node will send a false RREP via A with very high destination sequence. As a result, S will assume that path from S to D via A is the shortest and it will indirectly send data to Black Hole node (M) thinking that there exists a path to D

©IJRASET 2015: All Rights are Reserved

via A. Because of which the whole data gets trapped instead of reaching to destination.

III. DETECTION AND PREVENTION TECHNIQUES

Patel and Dadhaniya [11] proposed a 3-step host based Intrusion detection technique in which each node acted as IDS node. It detects a malicious node based on sequence number generated by it. If sequence number generated by replying node is greater than the sequence number generated by source node, then the replying node is considered as malicious node and the messages sent by it are also blocked, by transmitting node id to all other nodes. The simulation results of the paper showed that there was an increase in PDR and average throughput.

Deng et al. [12] presented a solution for solving problem of Black Hole Attack. In this technique, along with the RREP message, information regarding the neighbor of replying node is also asked and when RREP message reaches source, source instead of sending message immediately sends another message to neighbor of replying node asking whether the intermediate node which is replying for RREQ message really has path to destination or not. But it had limitation that it increased the message overhead so it can be used to verify identity of node which is under doubt of being malicious and it also assumed that Black hole nodes cannot work in group.

Raj and Swadas [13] proposed a method DPRAODV to detect black hole node based on RREP sequence number and threshold value. If the value of RREP sequence number comes out to be greater than the threshold value then the node sending this RREP will be considered as malicious. Further this malicious node is isolated from network by sending a control message ALARM to all other nodes and a list of blacklisted nodes is created. The simulation results showed that there was an increase in packet delivery ratio but also an increase in routing overhead and delay in message delivery.

Mistry et al. [14] did a modification in working of source node by the addition of new function for storing RREP messages for some specified time, a table which stores these RREP messages, a timer and Mali_node id for detecting black hole node and to keep record of all malicious nodes present in network. This technique discards the RREP message stored in table which has highest value of destination sequence number and node sending this RREP will be considered as malicious and its identity will be stored as malicious id. This method leads to an increase in memory and time overhead but increase in packet delivery ratio compensated for that overhead.

Bhosle et al. [15] proposed a watch dog mechanism in which an additional information is stored in tables at all nodes to detect the presence of attacking node. In this the nodes keep track of the packets they send and packets they drop, and if the value of packet drop ratio increases from threshold the node will be considered as an attacking node.

Table 1 Comparison between Black Hole Attack Detection and Prevention Techniques

Attributes / Techniques	Packet Delivery Ratio	Overhead	Throughput	Delay in Message	Memory Usage
Patel and Dadhaniya[11]	Increase	---	Average	---	---
Deng et al. [12]	Increase	Increase	---	---	---
Raj and Swadas [13]	Increase	Increase	---	Increase	---
Mistry et al. [14]	Increase	Increase	---	---	Increase

©IJRASET 2015: All Rights are Reserved

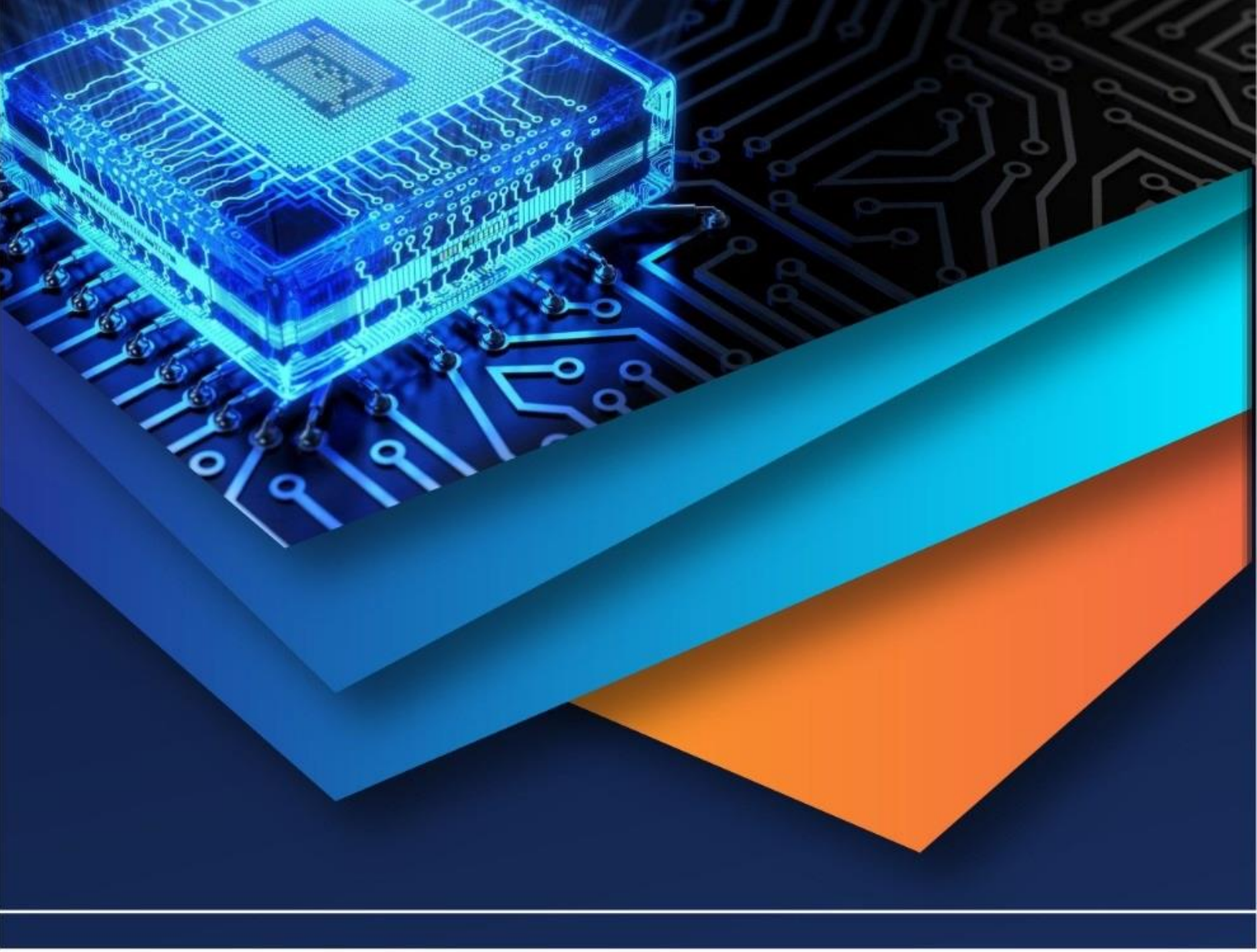
IV. CONCLUSION

This paper discussed the problem of black hole attack in MANET and various detection and prevention techniques which can be used to discover the secure path between source and destination avoiding the interruption by malicious nodes in route. Each one of the techniques discussed have own advantage and disadvantage as shown in table 1 and challenges in which further work can be done.

REFERENCES

[1] Y. Ko, N.H. Vaidya, "Flooding-Based Geocasting Protocol for Mobile Ad Hoc Networks", Mobile Networks and Applications; Dec 2002; 7, 6; ABI/INFORM Global pg. 471.
[2] A. Qayyum, L. Viennot, A. Laouiti, "Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks", in Proceedings of the 35th Hawaii International Conference on System Sciences – 2002.
[3] C.M. Cordeiro and D.P. Agrawal, "Mobile ad hoc networking", GBR Research Center for Distributed and Mobile Computing, ECECS, University of Cincinnati.
[4] L.M. Feeney, "Lecture Notes on Introduction to MANET Routing". Available: http://www.nada.kth.se/kurser/kth/2d1490 /05/lectures/feeney_mobile_adhoc_routing.pdf.
[5] S. Pleisch, M. Balakrishnan, K. Birman, R.V. Renesse, "MISTRAL: Efficient Flooding in Mobile Ad-hoc Networks", MobiHoc'06, May 22–25, 2006, Florence, Italy.
[6] Y. Yi, M. Gerla and T.J. Kwon, "Efficient flooding in ad hoc networks using on-demand (passive) cluster formation".
[7] I. Ullah, S.U. Rehman, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", Available: http://www.bth.se/fou/cuppsats.nsf/all/448194ba63f382fdc1257751006226b8/$file/Final_Thesis_Report_irua08_resa08%20Analysis%20of%20Blackhole%20Attack.pdf.
[8] M.A. Shurman and S.M. Yoo and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE'04, April 2-3, 2004.
[9] J. Kumar, M. Kulkarni, D. Gupta, "Effect of Black Hole Attack on MANET Routing Protocols", I. J. Computer Network and Information Security, 2013, 5, 64-72, Published Online April 2013 in MECS.
[10] N. Bhalaji, A. Shanmugam, "Defence Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET", Journal Of Advances In Information Technology, Vol. 2, No. 2, May 2011.
[11] N. Patel, A. Dadhaniya, "Detection of Black Hole Attack in MANET using Intrusion Detection System", International Journal of Advance Engineering and Research Development (IJAERD, Vol 1, Issue 5,May 2014.
[12] H. Deng, W. Li, and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazines, vol. 40, no. 10, October 2002.
[13] P.N. Raj, P.B. Swadas, "DPRAODV: A Dyanamic Learning System against Black Hole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009.
[14] N. Mistry, D.C. Jinwala, M. Zaveri, "Improving AODV Protocol against Black hole Attacks", in Proc. of the International Multi Conference of Engineer and Computer Science, Vol. 2, 2010.
[15] A.A. Bhosle, T.P. Thosar and S. Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol.2, No.1, February 2012.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)