ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

Detection and Prevention of Grayhole, Blackhole and Wormhole Attacks in MANET Using IIRD

Amandeep Kaur Grewal [1], Er. Gurpreet Singh [2]

M. Tech, Department of Information Technology, AIET Faridkot, Punjab, India [1]

Assistant Professor, Department of Computer Science, AIET Faridkot, Punjab, India [2]

ABSTRACT : Wireless networks have gained a lot of popularity today, as the users want wireless connectivity irrespective of their geographic positions. MANET is one of such wireless adhoc networks. The openness of the mobile ad-hoc networks makes it vulnerable to the security threats. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANETs). Black hole attack, Wormhole and Gray hole attack are one of the security threats in which the traffic is redirected to such a node that actually does not exist in the network by sending the false data streams to the target nodes. This may lead to drop in throughput and packet delivery ratio. MANETs must have a secure way for transmission and communication, which is quite challenging and a vital issue. In order to provide secure communication and transmission of data packets, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. In this paper, the technique Integrated Intelligent Route Discovery (IIRD) is proposed, which aims to detect and isolate the above attacks in MANET. Therefore, it leads to increase in Packet Delivery ratio and Throughput.

KEYWORDS: MANET, Wormhole, Grayhole, Blackhole, IIRD, Throughput, Packet Delivery ratio, AODV

I. INTRODUCTION

Mobile Ad-hoc Network is a self-organizing and self-configuring multi-hop wireless ad-hoc network where the structure of the network changes dynamically due to the mobility of the nodes. The nodes in the network not only act as hosts but also as routers that send the data from one node to the other node in the network. Each node in the MANET uses wireless interface to communicate with the other nodes. The nodes in the network performs all the routing activities by themselves only. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure such as access points or base stations [1]. Without any help of fixed infrastructure such as access points or base stations, these networks are fully distributed and can work at any place. However, there are still many problems about MANETs, such as security problem, finite transmission bandwidth, and restricted hardware. [2]

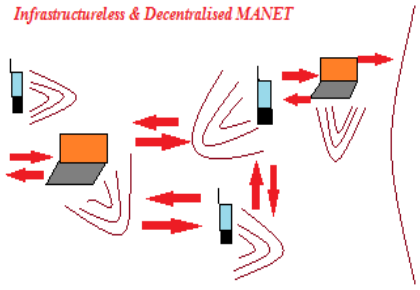

Fig. 1. Mobile Ad-Hoc Network[3]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

II. CHARACTERISTICS OF MANET

Mobile ad hoc network is a collection of self-governing and moving elements such as laptop, smart phone, tablet PC etc. The mobile nodes can dynamically self-organize in arbitrary temporary network topology. There is no preset infrastructure thus it does not have the clear boundary. Some characteristics are:

1. **Infrastructure less**: MANET is an infrastructure less system which has no central server, or specialized hardware and fixed routers. All communications between nodes are provided only by wireless connectivity.
2. **Scalable**: The scalability of Mobile ad hoc networks depends upon the number of nodes and the area of the topology. These are non-scalable when the area of the network topology is increased. [4]
3. **Dynamic Topology**: Nodes are free to move without restrictions with different speeds; thus, the network topology may change randomly at unpredictable time. The nodes in the MANET establishing their own network and also dynamically establish routing among themselves as they travel around.
4. **Cooperativeness**: It is assumed by the routing algorithm of MANET that all the nodes of the network are cooperative and non-malicious. Due to which the malicious attacker can easily become part of the network and can halt the activities of the network.
5. **Limited Power Supply**: The nodes of the ad hoc network works in a very selfish manner when there is very limited power supply. Mechanisms should be employed to security from security threats and improving the power consumption.

III. SECURITY ATTACKS

Mobile Ad hoc networks are difficult to defend to various attacks not only from outside but also from inside i.e. network it. Two different levels of attacks are mainly subjected in Ad-hoc network. On the basis of the behaviour of attacks, the attacks can be classified into two parts i.e. passive attacks and active attacks.

Passive Attacks

This attack transferred the data to other nodes in network without interrupting the communication of the operation. MANETs are more capable to passive attacks. Detection of passive attacks is difficult since the operation of network itself doesn't get affected. In order to overcome these attacks, powerful encryption algorithms are used to encrypt the data being transmitted. The various passive attacks are eavesdropping, traffic analysis etc.

Active Attacks

This attack is very serious attack in network which stops the flow of messages between the nodes. Active attack can be internal or external. An external active attack can be brought out by outside sources that do not belong to the network. Internal active attack is malicious nodes that are part of the network. This attack is more difficult and hard to detect than external attacks [5].

Blackhole Attack

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the mobile ad hoc networks [6].

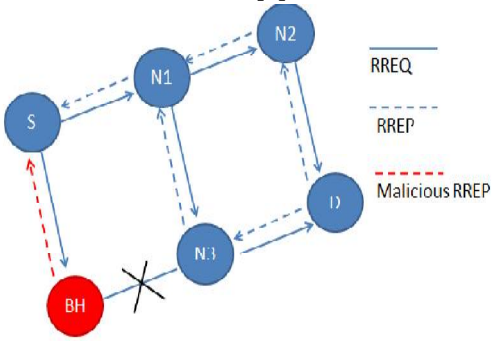

Fig 2: Black hole Attack [7]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

Gray Hole Attack: This attack is also known as route misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability [8].

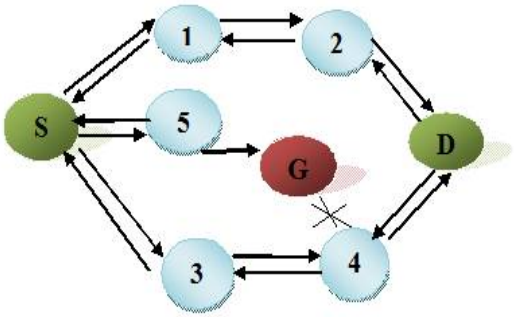

Fig. 3 Gray Hole Attack [9]

In Wormhole Attack, the nodes in the network try to create illusion for the targeted nodes of the network that they have shortest route in the network than the original routing path to deliver the packets to the destination. This creates a misconception among the legitimate nodes of the network regarding the routing paths that are to be selected based on the distance of the routes in the network. The attacking nodes do not require any prior knowledge of the network and the concerned security mechanisms implemented on it for secure transmission. In this type attack, the two or more threatening nodes are connected directly to each other through a link which is known as tunnel. The malicious node present on either side captures the packet from the legitimate node and by encapsulating the packet, transmits it to another malicious node in the network.[10]

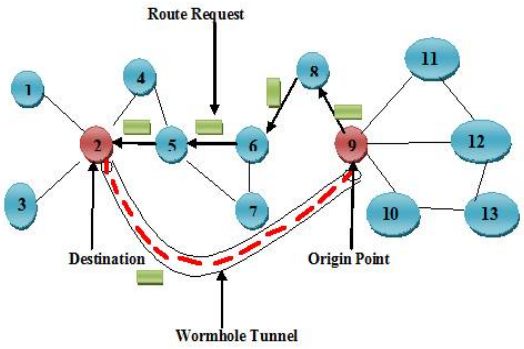

Fig.4 Wormhole Attack [11]

IV. RELATED WORK

Ashish Kumar Jain[12] investigated a new solution by using trust based approach in MANET. In order to defend against the wormhole attack, he uses the combination of parameters like energy, number of connections and buffer length of a node. Trust value of node is computed based on these parameters. The proposed approach compares trust of each node with threshold value of the network trust. The result of this comparison clarifies that selected node is either fake or legitimate.

Rashika Indoria et al. (2015) [13] evaluated that a wireless ad hoc network is a network where nodes can communicate with each other due to infrastructure less network. This infrastructure can be set up easily with very low cost. Due to dynamically based network connectivity, the decision of which nodes transfer the packets to other nodes is called ad-hoc network. With the help of radio waves, mobile nodes can communicate to each other freely in a MANET.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

P. V. Venkateswara Rao et.al (2015) [14] proposed that MANETs are vulnerable to different kinds of attacks due to permanent properties. The popular attack in MANET is the Black Hole attack which is most common in routing protocol AODV.
In this paper, the authors simulate the Black-hole attack in AODV using NS2 Simulator for both SANETS and MANETS by changing node density in the context of responsive and non-responsive traffic. The simulation results shows when there is black-hole attack the performance of throughput, PDR is less and end-to-end delay, routing load is high.
S.Banerjee et. al.[15] designed an algorithm for countering and removing of both the black and gray hole attacks in MANET. According to this algorithm, the complete data traffic is divided into small chunks so that the malicious nodes can be easily detected and removed. Flow of traffic is continuously checked by the neighbors of each node. Destination node sends the acknowledgement number back to the source node, which enables the source node to check for the possibility of any malicious nodes. But this technique leads to some false attributes, that is , even when the node is not the malicious one, it may present it as the false one.
Rutvij, Sankita and Devesh [16] proposed detection mechanism of black holes in the network with the increase in packet delivery ratio (PDR) and lowered routing overhead. It is done by confirming the validity of routing information by the nodes receiving RREP packets.

V. PROPOSED METHOD

The IIRD (Integrated Intelligent Route Discovery) is proposed Algorithm. It will be implemented using AODV protocol using NS-2 Simulator.

- Nodes in a path computes RTT values based on the time between the RREQ sent and RREP received.
- The RTT computation is based on its own clock.
- Compute per hop distance value using RTT value.
- The computed per hop distance value and timestamp are stored in each packet header.
- This information's are stored to identify the malicious link.
- Every node in a path computes per hop distance with its neighbor and compares it with the prior per Hop distance.
- If the per hop distance exceeds the maximum threshold range, RTh, go to next step. Check for the maximum count a link takes part in the path.
- If FC> FCthreshold, then the link is malicious.
- Mark the link as threat and the corresponding node informs other nodes to alert the network. These malicious nodes are then isolated from the network.

Algorithm to Detect Malicious Node Attack in MANET's
Notation:
MN: malicious node N_{RREP}: RREP from an intermediate node

1. Begin
2. For (source node)
3. {
4. Broadcast RREQ packet to every neighbor node
5. Receive RREP
6. RREP will be IIRD among various reply having largest sequence number &minimum hop count and all other RREP buffered at originating node
7. Process RREP
8. }
9. If (Information is trust Worthy && replied info is right)
10. Declare node as trustworthy node
11. Else
12. {
13. Declare N_{RREP} as MN

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

14. Call removal of malicious node();
15. }

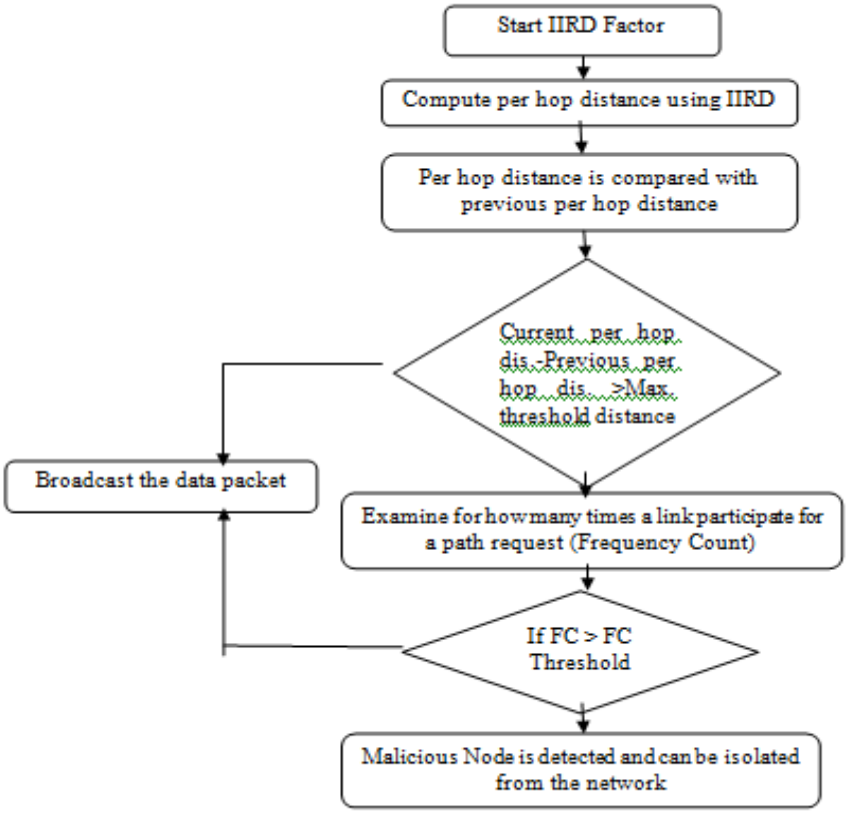

Fig. 5 Flowchart of Proposed Work

VI. RESULT ANALYSIS

The algorithm's performance has been observed and analyzed on the basis of result of simulation is performed on the NS2. The NS2 framework is initially studied and then framework has been modified along with IIRD in order to analyze various algorithms. Results are observed under low and high Traffic Environment.

The simulation parameters are defined in Table 1. These include network size, max speed, min speed, transmission range and number of nodes. We implemented proposed algorithm, previous algorithm in NS-2 and the performance comparison is done among them.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

Table 1 Input Values from Simulator

S. No.	Parameter	Value(s)
1	Simulator used	NS 2.35
2	Simulation Time	10 sec
3	Simulation Area	1000 X 1000
4	MAC	802.11
5	Number of nodes	55
6	Speed of Nodes	2 to 16 (m/sec)
7	Mobility Model	Random Waypoint

In what follows, the visual interpretations of the results during and after simulation of the proposed IIRD are displayed.

Table 2: The Results

Parameters	Under Black hole ,Gray hole and Wormhole Attack	After Proposed Technique IIRD
Number of nodes	55	55
Average throughput	156.79kbps	167.2kbps
Packet delivery ratio	10534	10540

Throughput Performance Comparison Throughput is defined as the total number of data packets delivered over the total simulation time. It is used to define the performance of the network and measured in bits per second within run time.

Throughput = Total Data bits / Simulation Runtime

Fig.6 Comparison of Throughput

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

The analysis of Throughput with Black hole, Grayhole and Wormhole attack with IIRD under Black hole attack is shown in Fig.6. This figure shows that Throughput using IIRD is high as compared to under attacks our proposed technique the results are better.

Packet Delivery Ratio Comparison

Packet delivery ratio can be calculated as the ratio between the number of data packets send by the source and the number of data packets received by the destination. Higher the value of PDR better will be the protocol

Packet Delivery Ratio = Total No. of Packets received by Destination/ Total No. of Packets Sent by Source

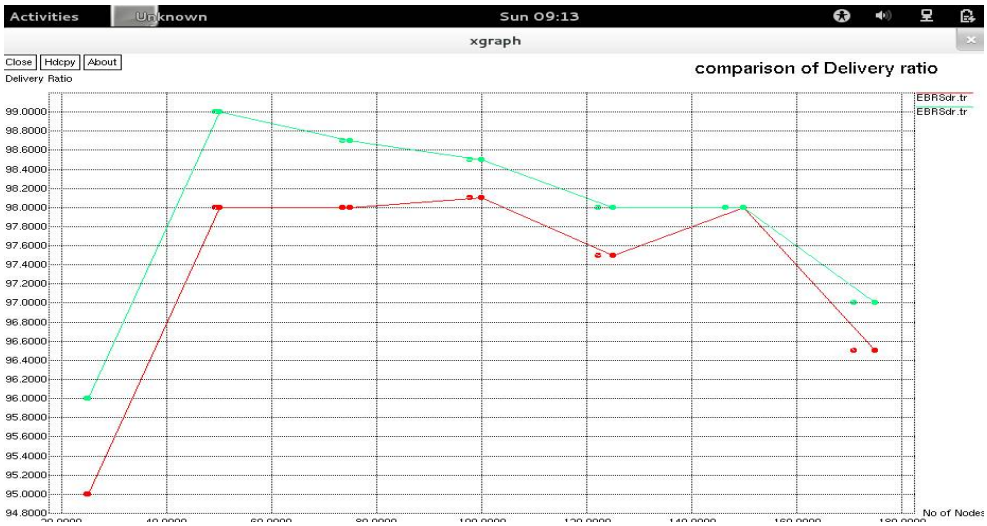

Fig.7 Comparison of Packet Delivery Ratio

The analysis of Packet Delivery ratio between Black hole, Grayhole and Wormhole Attack and IIRD are shown in figure7 the shows that Delivery ratio using IIRD is high as compared to cooperative black hole, wormhole and grayhole attack but in our proposed technique the results are better as compared to previous Technique

VI. CONCLUSION AND FUTURE WORK

A Black Hole, Wormhole and Gray hole attacks are is one of the serious security problems in MANETs. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes The proposed technique is hybrid in nature and based on the concept of IIRD. It provides a solution for identification of Black Hole, Worm Hole and Gray hole Attack and removal of attacks from the network. We can extend our simulation model other different types attacks. The technique can also be extended to increased nodes density and the area of the nodes. So, the proposed network can be enhanced in future using the above parameters.

REFERENCES

[1] Ravinder Kaur and Jyoti Kalra, "Detection and Prevention of Black Hole with Digital Signature", IJARCSSE, Vol.4, Issue 4, August 2014.
[2,] Priyanka Goyal, Vinti Parmar and Rahul Rishi, "MANET : Vulnerabilities, Challenges, Attacks, Applications", IJCEM, Vol.11, January 2011
[3,9] Amandeep Kaur Grewal, Asst. Prof. Gurpreet Singh," A Review on Attacks in Mobile Ad hoc Network (MANET)", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 5 Issue: 1
[4] Mahima Chitkara, Mohd. Waseem Ahmad," Review on MANET: Characteristics, Challenges, Imperatives and Routing Protocols ", IJCSMC, Vol. 3, Issue. 2, February 2014, pg.432 – 437
[5] Rozy Rana, Kanwal Preet Singh, "Performance Evaluation of Routing Protocols (AODV, DSDV and DSR) with Black Hole Attack", International Journal of Science and ResearIIRD, Volume 3, Issue 7, July 2014
[6] Jasvinder, Monika Sachdeva "A survey of behavior of MANET routing protocol under black hole attack" International Journal of Advanced Research in Computer Science and Software Engineering, volume 3,issue 8, august 2013.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

[7] International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015 Prevention of black hole attack by different methods in MANET. Nakka Nandini, Reena Aggarwal
[8] Shani Makwana1, Krunal Vaghela,"Cooperative Gray Hole Attack Detection and Prevention Techniques in MANET: Review", IJSR, Volume 4, Issue 1, January 2015
[10,15] F. Anne Jenefer , D. Vydeki ,"Performance Analysis of Mobile Ad Hoc Network in the Presence of Wormhole Attack", International Journal of Advanced Computer Engineering and Communication Technology (IJACECT), Volume-2, Issue – 1, 2013
[11] Amandeep Kaur Grewal," A Survey paper on Wormhole Attacks in MANET", International Journal of Computer Engineering and Applications, Volume X, Issue I, Jan. 16
[12] Ashish Kumar Jain, Ravindra Verma,"Trust - Based solution for Wormhole Attacks in Mobile Ad Hoc Network ",(GJMS), Volume-4, Issue-12, November- 2015
[13] Rashika Indoria, Deepak Motwani," An Approach of Detecting Black Hole Attack in MANET using Modified TAODV Protocol", International Journal of Computer Applications, Volume 129 – No.12, November 2015
[14] P. V. Venkateswara Rao, S. Pallam Setty, "Investigating the Impact of Black Hole Attack on AODV Routing Protocol in MANETS under Responsive and Non-Responsive Traffic", International Journal of Computer Applications, Volume 120 – No.22, June 2015
[16] Rutvij H. Jhaveri , Sankita J. Patel," DoS Attacks in Mobile Ad-hoc Networks: A Survey.", Second International Conference on Advanced Computing & Communication Technologies, p535-540, 2012