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.343 – 349

Effect on Various Parameters under Black Hole Attack in MANETs using INRD Technique

Navpreet Kaur Dhanju[1], Pardeep Kaur Khehra[2], Er. Puneet Kumar[3], Dr. Rachit Garg[4]

[1]Student, M-tech (CSE), SSCET, Amritsar, Punjab, India

[2]Student, M-tech (CSE), SSCET, Amritsar, Punjab, India

[3]Assistant Professor (CSE), SSCET, Amritsar, Punjab, India

[4]Principal, SSCET, Amritsar, Punjab, India

[1] nvdhanju92@gmail.com, [2] kaurdeep1493@gmail.com, [3] puneetsrisai@gmail.com

---

Abstract: Black hole is a malicious node that always gives the false replay for any route request without having specified route to the destination and drops all the received packets. This can be easily engaged by misusing vulnerability of on demand routing protocol AODV The existing method identified the attacked node, retransmit the packets and again find a new route from source to destination. Here the proposed method broadcast the INRD to the whole nodes in the network. This method prevents the black hole attack imposed by malicious nodes.

Keywords: MANETS, BLACKHOLE, RREQ, RREP, INRD

I. INTRODUCTION

Manet is defined as a wireless network which is collection of mobile hosts without required any centralized access point like base station [4]. Due to dynamic nature of their topology because nodes should be able to join or leave the network as they wish [3]. Each and every act as a host or as a router or both in the same time [5]. All devices communicate with each other through wireless medium using intermediate devices because there is no direct path from source to the destination so that source sends Packets to the intermediate node which forwards the data packet to the destination [6].

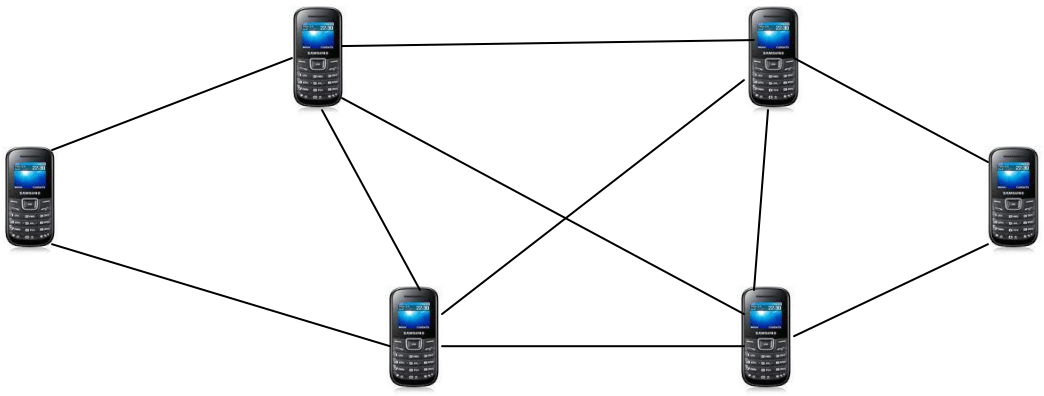

Fig.1 (MANETS)

For communication purpose from source to destination, a suitable route in the presence of any one routing protocols. These routing protocols like AODV, GRP, DSR, DSDV etc. But there are many security attacks which degrade the performance of Manets like black hole attack, warm hole attack, sinkhole attack, gray hole attack etc [8] .

Characteristics & Applications of Manets [7]:

a) Autonomous & Infrastructure less
b) Multihop routing
c) Dynamic n/w topology
d) Variation on link and node capabilities
e) Energy-constrained operation
f) Scalability
g) Military network
h) Sensor network
i) Automotive applications
j) Emergency services

II. BLACKHOLE ATTACKS

Black hole is defined as serious attack for Manets. In this attack, a malicious node is used to create fake path between source to destination, but when sender node sends data packets to destination node using that path. Malicious node takes the data packets from sender node & not sends to destination position. In this way malicious node drops data packets or sends to fake address. When one malicious node is used for attack purpose known as single black hole attack. Two or more malicious nodes are work together to carry the attacks are called cooperative black hole attack [2][7].

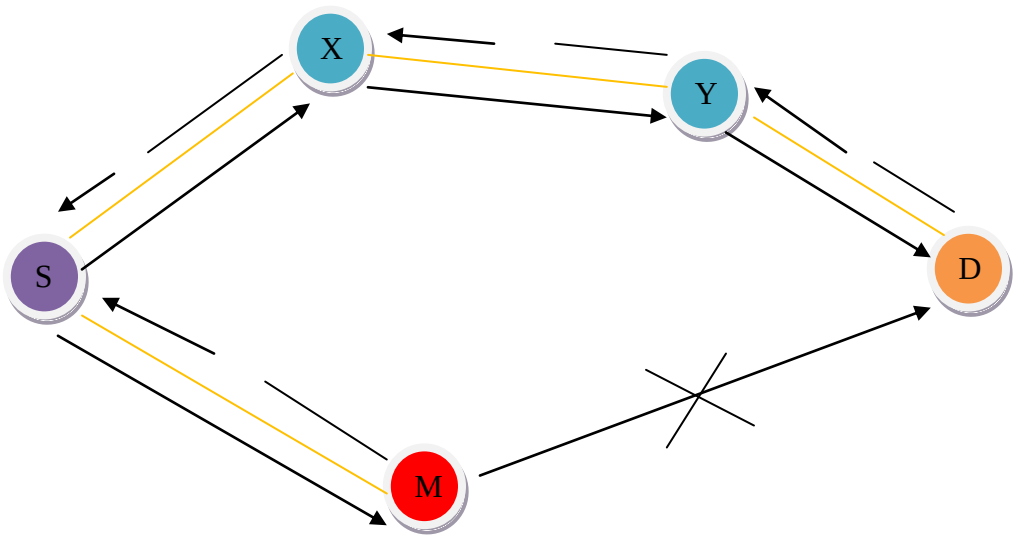

Fig.2 (Black hole attack)

In given fig.2, S act as source node, D act as a destination node, X, Y are neighbor nodes or intermediates nodes between sources to destination path. M act as a Malicious or attacker node.

III. RELATED WORK

Priya Jeejo Payyappilly et al [1], proposed a new approach which is used to detection and prevention of collaborative black hole attack. A trust value is used for distinguish the malicious node from genuine node. At starting, each node act as equally and trusted. Trust is based on RREQ sent , RREP received and received data packets. Trust is decreased when RREP is received before a predefined time. To identify of black hole node DSN (destination sequence number) is used. For prevention, malicious node removes from its routing table.

Ravinder Kaur, et al [2] proposed digital signature which is verification technique to detect the malicious node in the network. Source node is send route request to neighbor nodes in AODV. If destination node received that request then OK otherwise route request broadcast to next nodes until the destination is found. RREQ packet header contains information regarding visiting node (node-id) in node info column which also contains the number of visiting nodes used in path. TTL scheme is used at the destination site. According to this scheme, destination node selects the shortest path with less number of nodes. The destination node unicast the reply whose header contains all information of visiting nodes or digital info column which contains genuine digital signature of all nodes. Receiving node received data packets & verifies or compare with digital signature from its data base. If the signature is match then that node is genuine otherwise considered as a malicious node . After detection of malicious node, this information is broadcast to all the neighbors' nodes. Process is repeated until the secure path is not found.

Romina Sharma et al [3] , proposed modify the AODV protocol to prevent black hole attack . According to this, adding next hop information in the RREP message and two other control message including further route request

and further route reply. Source node broadcasts RREQ. RREPs will receive by source with next hop information. After that, source node sends further route request (FRREQ) to all next hop nodes. After receiving FRREP source node sends data packets to the destination with the shortest path. If next hop node is black hole, FRREQ will not reach to next hop node & no FRREP will send to source node. So source node not sends data packets to path which is suggested by black hole node.

IV. PROPOSED WORK

In the proposed system INRD broadcasting method is used. In this method once the malicious node is identified, the particular node id is transmitted to the entire network therefore whether the malicious node take part in two or more path packets does not move towards the malicious node because whole nodes in the network should know about the malicious node.

a) Route Discovery & Data Transmission

The Route Discovery Process is done initially by sending the route request by INRD node which will find the malicious activity in the network .The INRD node find whether the route from the intermediate node to the destination node exists or not. When the source node receives the Further Reply from the next hop, it extracts the check result from the reply packets. If the result is yes, we establish a route to the destination and begin to send out data packets. If the next hop has no route to the inquired intermediate node, but has a route to the destination node, we discard the reply packets from the inquired intermediate node, and use the new route through the next hop to the destination. At the same time, send out the broadcast message to whole network to isolate the malicious node. . Thus we avoid the black hole problem and also prevent the network from further malicious behavior.

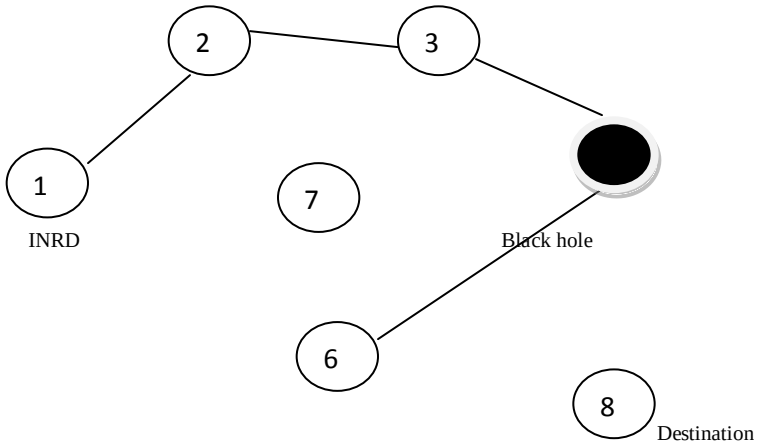

Fig 3.Black hole Detection

The Fig 3 shows the INRD node is finding path in the network if requested path is not provided by the intermediate node it.

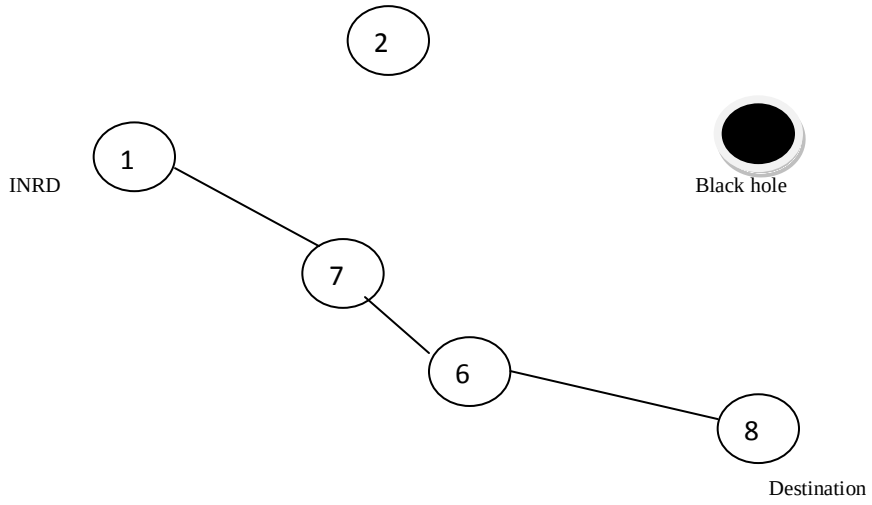

Fig 4. New route Discovered by INRD node

Consider it as malicious node and exclude it from the network. And broadcast the identity of malicious node so that the other transmission should not be done by malicious node

b) Proposed Algorithm

In the Proposed technique to detect the malicious node in network and Intelligent nodes are used for prevention and detection of black hole attack in the network In AODV the route request is send to neighbor nodes by the source node. If destination node is one of them then ok otherwise route request broadcast to next node until the destination is found. The route request (RREQ) packet header contains the information of visiting node (node id) in node information column and hop count column which contains the number of visiting nodes used in path. Using INRD path updated by these node will be used for prevention and detection proposed algorithm

Step 1: Generate Manet scenario using NS2

Step 2**:** Start with some initial elements like 'no of nodes', 'neighbor node', 'malicious node intelligent node

Step 3: Initialize with n no. of nodes.

Step 4: Implement INRD technique.

Step 5: initially Start INRD algorithm for finding malicious node in this process malicious node is detected

Step 6: In INRD the malicious node detected will be isolated from network and information regarding malicious node is broadcasted in the network

Step 7: Then finally With INRD Algorithm the secure network free from black hole will be formed

Step 8: This process continuation until the black hole is removed from network

V. RESULT ANALYSIS

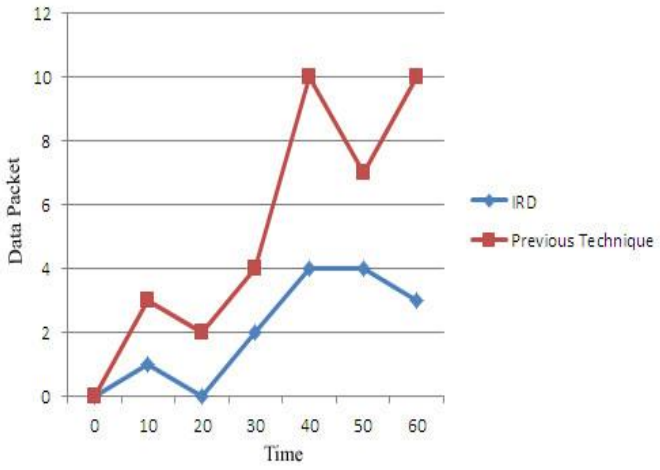

Fig 5. Packet delivery ratio

The comparison of packet delivery ratio vs. Time and Throughput vs. time in the INRD method and Previous method is given in the fig 5and fig 6. The graph shows that better results in INRD method

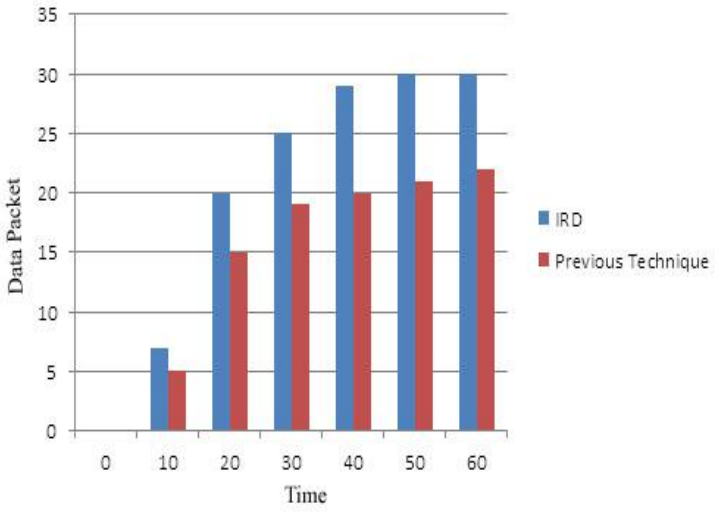

Fig 6 .Throughput

VI. CONCLUSION

In this paper, we solved the problem of black hole attacks in MANET routing. The INRD broadcasting method provides improved performance of throughput packet delivery ratio and reduced packet loss comparing with Previous method Therefore INRD broadcasting method provide improved network performance and minimum packet loss in the packet transmission.

REFERENCES

[1]. Priya Jeejo Payyappilly, Pinaki A. Ghosh, "Secure Method for AODV Routing By Detection and Prevention of Collaborative Blackhole Attack in MANET" International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June-2015.

[2]. Ravinder Kaur, Jyoti Kalra, "Detection and Prevention of Black Hole Attack with Digital Signature" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 8,August 2014.

[3]. Romina Sharma, Rajesh Shrivastava, "Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network" International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.

[4]. Ketan Sureshbhai Chavda, "A Performance analysis of AODV under Blackhole Attack in MANET" International Journal of Technology in Computer Science & Engineering, Volume 1(2), June 2014.

[5]. Azza Mohammed, Boukli Hacene Sofiane and Faraoun kamel Mohamed, "A Cross Layer for Detection and Ignoring Black Hole Attack in MANET" I.J. Computer Network and Information Security, September 2015.

[6]. Aman Saurabh, Rakesh Yadav, Harjeet Kaur, "Identifying & Isolating Multiple Black Hole Attack on AODV protocol in MANET" International Journal of Innovative Research in Science, Engineering and Technology" Vol. 4, Issue 5, May 2015.

[7]. Mohamed Elboukhari, Mostafa Azizi, Abdelmalek Azizi, "Impact analysis of Black hole attacks on Mobile Adhoc networks performance" International Journal of Grid Computing & Applications (IJGCA) Vol.6, No.1/2, June 2015.

[8]. Sumer Singh, Chakshu Goel, Gurjeevan Singh, "MAODV: To Identify a Secure Route Selection in MANET under Blackhole" International Journal of Computer Application, Volume 58–No.22, November 2012.

