Vol. 1, Spl. Issue 2 (May, 2014) e-ISSN: 1694-2329 | p-ISSN: 1694-2345
GV/ICRTEDC/52

A REVIEW OF DIFFERENT BLACK HOLE DETECTION TECHNIQUES IN MANET

[1]Rahul kumar, [2]Monika Sachdeva
Department of CSE, SBS State Technical Campus, Ferozepur, Punjab, India
[1]rkr708@gmail.com, [2]monika.sal@rediffmail.com

Abstract—Mobile ad-hoc network is the collection of different mobile hosts that does not communicate via particular predefined topology. The mobile nodes create their own topology whenever needed. Due to this nature of MANET there is an increasing chance of attacks on the MANET. Black hole attack is a denial of service attack in which the malicious node behaves like it has as a shortest path to reach destination node with minimum hope count and maximum sequence number. But once the path is selected through these nodes to reach the destination they will drop the data packets without transferring it to the destination. In this paper a review of different detection and prevention techniques for the black hole attack in MANET is presented.

***Keywords*—**Mobile Ad Hoc Network, Dos, Black Hole Attack.

I. INTRODUCTION

Mobile ad-hocnetwork is formed with mobile nodes such as laptops, cell phones etc. Each device in a MANET is free to move independently in any direction and there are no routers or access point. Every device acts both as host and as a router to establish a route[1]. There is no pre defined infrastructure required. When any source node wants to send data to the destination, packets are transferred directly to the destination if it is in range of source node and if not, data is transferred through the intermediate nodes. The structure of MANET is shown in the figure-1 where A, B anc C are mobile nodes.

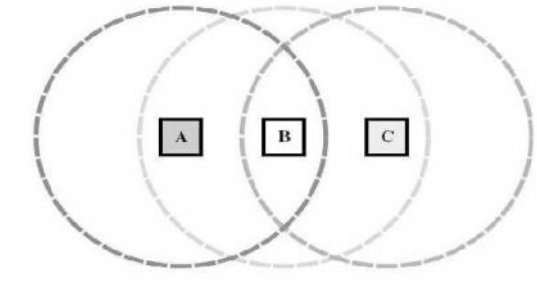

Figure 1: A Mobile Ad-hoc Network

II. Routing in MANET

The process of creating the route and then transfering data to the desired destination is called routing.The routing protocol in MANET is mainly categorized into Proactive, reactive and hybrid routing protocol.

A. Proactive routing protocol:

In proactive routing protocol every node proactively searches for the route to the other node and periodically exchanges routing message in order to maintain routing table up-to-date. [1]Node also contains the information about any change or updating in the network. Here some predefined paths are available in the network and when any node intent to transfer data to other node it may use these routes. The benefits of these are that they perform quick action because of the availability of the routes, no need to discover the route and ultimately the delay will be less. The drawbacks of these protocols are that every node contains the information about all those nodes where it is not required to communicate and use too many resources when the network is highly dynamic.

The examples of such protocols are DSDV (Destination Sequence Distance Vector), OLSR (Optimized Link State Routing Protocols), Wireless Routing Protocols (WRP)

B. Reactive routing protocol:

In Reactive routing protocols the route is searched between sources to destination node only when two nodes intend to transfer data, so this is also referred to as on demand routing protocol [1]. In such protocols, establishing a new route consists of three phase i.e. discover the route, establish the route and maintain the route. The discovery phase consists of RREQ (Route Request), RREP (Route Reply) and RRER (Route Error) message. The source node broadcasts a RREQ message into the network. A node that receives a fresh RREQ message will checks whether it has got a route to the destination node and if so it sends back an RREP message. If not, the RREQ message is broadcasted to its neighbor. The nodes maintain only the active routes. A drawback of such protocols is the delay due to the route discovery [2]. Examples of these protocols are AODV (Ad-hoc On Demand Distance Vector) and DSR (Dynamic Source Routing) protocols

*C. Hybrid protocols:*Hybrid protocols make use of both proactive and reactive routing protocols [2]. Examples of this type of protocols are ZRP(Zone Routing protocol)

III. SECURITY IN MANET

A. Security challenges in MANET

Security is the essential component for any networkbut security problem in MANET are more vulnerable to attack as compared to wired network because of its following unique characteristics like

1) Dynamic Network Topology: In MANET there is a dynamically changing network topology because of node mobility. As the mobile nodes changes their position in the network that leads to continues change in the topology and route. There is frequent partitioning of network takes place which may result in data loss.

2) Limited Bandwidth: The bandwidth of MANET is limited due to wireless communication. Wireless links have lower capacity as compared to wired links.

3) Limited energy resources: All the mobile nodes in Ad-hoc network such as laptops, cell phones are battery powered device. And these devices have some limited storage capacity.

*4) Open medium:*The nodes have freedom to join and leave the network.A node can communicate with other anytime if it is range, due to this it is more susceptible to attack.

5) Cooperative Algorithms: The routing algorithm of MANET is cooperative that requires the mutual trust between the nodes.

6) Lack of Centralized Monitoring: MANETs does not have any established infrastructure and centralized administration. This lack of centralized management leads MANET more vulnerable to attacks. [3], [4].

B. Security mechanism in MANET:

These are some security criteria are made to secure the network.

1) Authentication: Authentication ensures that the particular participants have a right to access the network by checking their identities. This prevents the unauthorized user to communicate.

2) Non-repudiation: Non-repudiation ensures that the sender and receiver of message cannot disavow that they have ever sent or receive such a message.

3) Availability: This recognizes the presence of node to provide services to the user. Due to more availability of node these is increase in the chance of attacks especially the Dos attack.

3) 4) Integrity: Integrity ensures the identity of the message that is going to send.

5) Confidentiality and privacy: Sometimes there are certain peoples have a privilege to access some private data and no other user will access them that ensure confidentiality. [3], [4].

IV. ATTACKS IN MANET

Because of some properties of MANET many attacks attract towards it. We categories these attacks as External attacks and internal attacks.

A. External attacks

External attacks are launched by nodes that are not the part of network. The Malicious nodes observe the network continuously from outside the network, and always try for a chance to get access in the network. Once they get access to the network they perform the attack. This attack badly affectsthe network like decrease the speed of data transfer, decrease the performance of the node and the data packets become insecure. These type of attacks can be prevented by security mechanism like Authentication and non-repudiation, Confidentiality and privacy. All types of viruses are the examples of External attacks. In the figure-2 “M” is the malicious node that attacks externally.

B. Internal attacks

The attack caused due to malicious nodes that are physically present in the network is internal attack. The attacker becomes the part of network and behaves like the original node. It is very hard to remove these attacks. Black hole attacks, Grey hole attacks are the examples of internal attacks. In the figure-3 “M” is the malicious node that is the part of network.

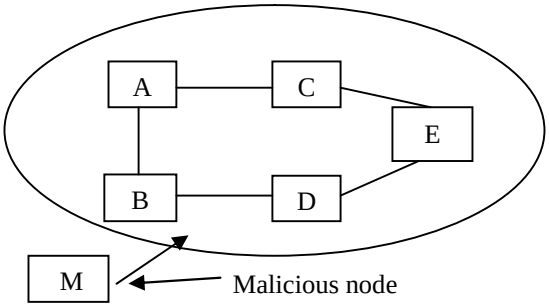

Figure-2: External Attacks

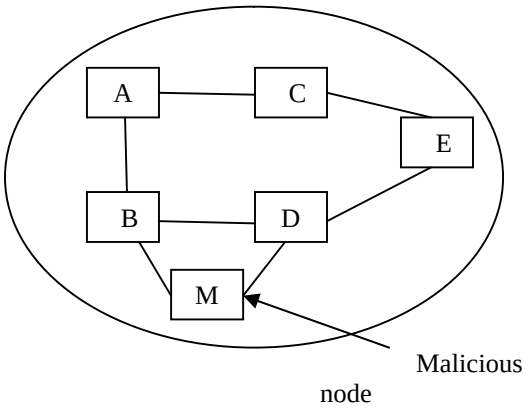

Figure-3: Internal Attack

V. BLACK HOLE ATTACK

Black hole attack refers to attack by malicious node that forcefully acquire the route from source to destination by falsely advertise itself as a fresh route with minimum hop count and maximum sequence number to reach the destination. But when the route is selected through these nodes it will drops the data packets somewhere else instead of destination.[1], [13]. These are internal attacks. The figure shows how black hole problem arises.

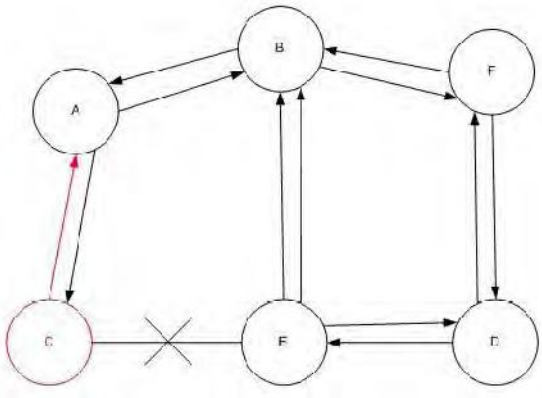

Figure-4:Black hole attack

Here “A” is the source node that wants to send data packet to the destination node D. To establish the route the source node initiates the route discovery process. On receiving the RREQ packets from the source node the malicious node “C” immediately sends an RREP packet that indicates it has a fresh route with minimum distance to reach the specified destination. The Node “A” will start sending data packets to “C” and this node cause the black hole attack.

A. Types of Black hole attack

1). Single black hole attack: The attack caused by individual black hole node in a network is referred to as single black hole attack. In the figure “M” is the malicious node that performs the black hole attack. The sender node sends data to the receiver node via malicious node and this single node drops all the data packets somewhere else. This type of attack is single black hole attack.

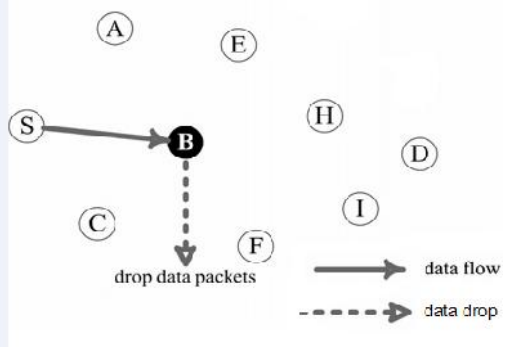

Figure-5: Single black hole attack

2) Collaborative black hole attack: The attack caused by two or more than two malicious nodes is referred to as collaborative black hole attack. In the figure-6 B1 receives the packets from S and then sends it to other black hole node B2 ant then B2 node drops the data packets [13]. These types of black hole attacks are very hard to detect and prevent.

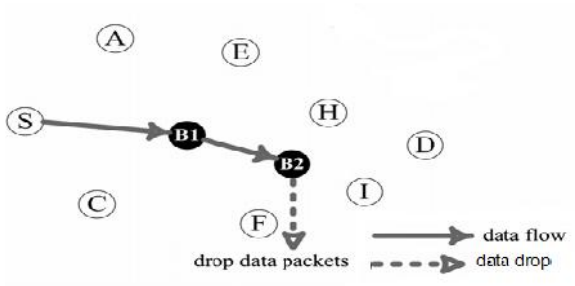

Figure-6:Collaborative black hole attack

VII. LITERATURE SURVEY

In this paper we will study about different black hole detection and prevention techniques.

HizbullahKhattak et al [6] proposed optimal path routing and hash method in which they use second optimal path instead of first one for the prevention of black hole attack and hash method for further detection of malicious node in the network. In case of AODV when the source node receives RREP messages from different intermediate nodes that has the route to reach the destination it just discards the first RREP message. In this way, it would be difficult for the black hole node to monitor the entire network to know where to place itself in a network. For further detection the source node sends the hash value of message with first message to the destination when destination node receives all the data packets in the dedicated time, destination node apply hash function on the data packets and compute hash value. If this value matches with the previous one it means all the packets have been received successfully. Otherwise, the destination broadcasts the data packets error (DPE) message to the source node.

Fidel Thachil et al [7] proposed a trust based approach for AODV protocol. In this approach every node monitors neighboring nodes and calculates its trust value. If this value goes below threshold value then the monitoring node considered as malicious node. The trust value of a node is calculated as a ratio of number of packets dropped to the number of packets to be forwarded by that node. The cache mechanism is implemented by every node in order to confirm that data sent by it are being forwarded or notElmarGerhards-Padilla et al [8] introduced TOGBAD technique using Topology graphs to identify black hole nodes. They first take knowledge about network topology and the number of neighbor of a node is calculated and forms a topology graph. Finally for each hello message, the originators number of neighbors checked according to the message for plausibility against the number according to the graphs. An alarm is triggers if there is a difference between the two numbers.

Sanjay K Dhurandher et al [9] gives GAODV a modified AODV against single and collaborative black hole attack. This is based on sending a conformation packet that is verified by destination to check the presence of black hole node. For this there are some other packets used along with RREQ and RREP packets that are CONFIRM, CHCKCNFRM, RERLYCONFIRM. When intermediate node send RREP to source node it also send CONFRM message to the destination. After receiving RREP source node send CHCKCNFRM to the destination. If RERLYCONFIRM comes from destination node then this is a secure path.

Romina Sharma et al [10] provide a modified AODV protocol to prevent black hole attack. They modify the working of AODV by adding next hope information in RREP message. They use two more control message that is FRREQ (Further route request), and FRREP (Further route reply).Once the source node receive RREP from intermediate node, it send FRREQ message to the node next to the intermediate node. If the next node send FRREP message to the source node then it is considered as honest node and it will send the data packets.

Nabarunchatterjee et al [11] proposed a triangular encryption technique for the detection of black hole attack. According to this approach source node send a plain text with RREQ, when intermediate node receives RREQ, it sends this packet to destination node instead of RREP to the source node. Destination node encrypts the plain text with pre agreed partition with key and sends it with RREP. On receiving these packets intermediate node update their index and hope count. If the RREP packet contains cipher text it is sure to have reached the destination.

S. L. Dhende et al [12] gives a 2 Acknowledgement technique to detect black hole attack. According to this source node after broadcasting RREQ message wait for more than one reply. After receiving first reply it starts timer. It will store sequence number and time at which packet arrives in Collect Route Reply Table. It will select first two routes after time out and send the packets to both of them and check the data arrive at next node. If next node receives data it will automatically generate 2 ACK packets otherwise it is malicious node and the data will send to another link

.Ming-Yang Su et al [13] proposed a intrusion detection system (IDS) topreventselective black hole attack. In this method several IDS nodes are deployed in MANET. These IDS nodes perform ABM (Anti Black Hole Mechanism). ABM is the mechanism in which suspicious value of node is calculated according difference in routing message transmitted by it. Ids node generate an alarm if it detects the presence of malicious node.

VIII. CONCLUSION

In this paper we have studied about MANET, some security issues in MANET and security mechanism in MANET. We studied about possible attacks in MANET especially Black hole attack which is a malignant thread in the network. In this attack some malign nodes perform a malicious action which results in escaping the data from the selected route instead to reach the destination. These nodes first consent the source to route the data to receiver but it drops data somewhere else. This attack is performed by single node called single Black hole attack as well as multiple nodes called as collaborative black hole attack. There are different techniques given by different authors to detect and prevent black hole attack. So this is very dangerous attack which if never detected timely can leads to decrease the performance of our network and the loss of our sensitive data especially in case of tactical MANETs(used for military purposes)[6]. The different black hole detection techniques, their merits and demerits are discussed in the table-1.

REFERENCES

1. M. Mohanapriya, IlangoKrishanamurthi, “Modified DRS protocol for detection and removal of selective black hole attack in MANET” ComputElectrEng(2013).
2. ShashankKhare, Manish Sharma, Namrata Dixit and SumitAgrawal “Security in routing protocol to avoid threat of black hole attack in MANET”. VSRD-IJEECE, Vol. 2 (6), 2012, 385-390.
3. HimainiYadav, Rakesh Kumar “A Review on Black hole attack in MANETs ”.International journal of engineering research and application, Vol. 2, Issue 3, May-Jun2012, pp.1126-1131
4. Raja KarpagaBrinda., Chandrasekar. “Defence strategy for the detection of Black hole attack in drs”Sri Shakthi Institute of Engineering and Technology, Coimbatore, India,2011
5. ShashiGurung and Krishan Kumar Saluja “Miting Impact of black hole attack in MANET”, DOI:02.ITC.2014.5.560, Association of computer Electronics and Electrical Engineers, 2014.
6. HizbullahKhattak, Nizamuddin, FahadKhurshid”Preventing black and grey hole attacks in AODV using optimal path routing and hash” IEEE 987-1-4673-5200-0/13. 2013.
7. Fidel Thachil, K C Shet “A trust based approach for AODV protocol to mitigate black hole attack in MANET” International conference of computer science, 978-0-7695-4817-3/12.2012 IEEE.
8. ElmarGerhards-Padilla Nils Aschenbruck ,Peter Marlini “Detecting black hole attack in tactial MANET using topology graphs” IEEE Conference on local Computer Networks 0742-1303/07. 2007.
9. Sanjay, Issac, Raveena and Prashant “A modified AODV against single and collaborative black hole attack in MANET” International conference on advanced information networking and application workshops 978-0-7695-1/13. 2013.
10. Romina Sharma, Rajesh Shrivastava “Modified AODV protocol to prevent black hole attack in Mobile ad-hoc network” International Journal of innovative research and development. ISSN (online).
11. NabarunChatterjee, Jyotsna Kumar Mandal “Detection of Black Hole Behaviour using Triangular Encryption in NS2” Ist International conference on computational Intelligence : Modeling Techniques and Applications(CIMTA-2013).
12. L.Dhende,D.MBhalero “A Mechanism for Detection of black hole attack in mobile ad-hoc networks”international journal of engineering and technology(IJERT).ISSN:2278-0181.Vol.1 Issue 6 august-2012
13. Ming-Yang Su “ Prevention of selective black hole attack on mobile ad-hoc network through intrusion detection system” Elsevier Accepted 20 August 2010.

Table.1

S.No	Author's Name	Proposed Methodology	Merits	Demerits
1	HizbullahKhattak Nizamuddin, Fahad Khur And Noor Ul Amin	Optimal path routing and hash method-here second RREP will considered instead of first and then hash method is applied for further malicious action	Prevent black, grey and cooperative attack, this method has further detection that maintain integrity	The verification of hash message by destination node takes place which is time consuming.
2	Romina Sharma And Rajesh shrivastava	Modify AODV is used and two more control message is used that is FRREQ FRREP for the confirmation of route	This scheme is very simple and there are no any complicated expressions and reduce packet delivary ratio.	Routing overhead increase and never prevent cooperative attack
3	Sanjay K Dhurandher Issac Woungang Raveena Mathur And Prashant Khurana.	GAODV is used and here any node on receiving RREQ send RREP to source and CONFIRM to destination, then source node send CHCKCNFRM to destination then destination node send REPLYCONFIRM to source node.	Prevent black and cooperative attacks.This increase data delivery and send data only when the route is completely verified. The end to end delay is 0.9 times greater than convential AODV.	Data traffic increase due to the presence of three new control messages. This technique is time consuming and packets have to wait.
4	Fidel Thachil And K.C Shet	Trust based approach here every node monitors its neighboring node and make its trust value if this value goes below the threshold then this node is removed	There is no over head because there is no any extra node; trust is based upon number of packets forward.	This method makes the trust value on the basis of resent packet but node may starts attack after long time.
5	S.L.Dhende And D.M.Bhalerao	Two ACK Scheme here source node select first two replies with next hope detail and send a packet to both node and check whether packet receive at next node if so then it send 2 ACK to source	This method select two routes if one route is malicious then it selects other route.	After sending data packets the source node has to wait for the acknowledgement, never prevent cooperative attacks.
6	Nabarun Chatterjee And Jyotsna K Madal	Triangular Encryption here the sender and receiver use pre agreement on partition and key of encryption and then the RREP with no cipher is dropped	Here encryption is used so fake RREP is not forwarded to the source and save the time	With increase in number of node the speed of the process become slow.

.