Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

An Approach for Detecting Black Hole Attack in AODV Routing Protocol for MANETs

[1]Vijayashree V, [2]Nisha C P, [3]Suma R, [4]Dr. Siddaraju B

Abstract

Wireless networks are said to be susceptible on DOS attacks. It does not contain infrastructure network as it has the capability of working without the support of centralized administration. In MANET malicious attackers can access the network as it cannot provide any guarantee that is vulnerable to attacks . Networks face problem of accessing information from unauthorized nodes. Black hole is a risk of security where the malicious node admits the shortest path so as to receive the packet. The proposed approach uses three methods like: finding the minimum time of the reply message, exceeding threshold sequence number and using Promiscuous node for detecting Black hole attack. From this approach we can increase throughput by decreasing packet sending delay and packet process ratio.

Keywords: Mobile Ad hoc network, Black hole attack, Promiscuous node, packet sending delay.

1. INTRODUCTION

A network is a cluster of many nodes connected together this is also called as wired network. There is another network called wireless network where mobile nodes are not connected to each other, here nodes are able to communicate with each other in order to send and receive packets. Wireless nodes need not have central node to manage the network flow this network are known as Mobile wireless networks also called as MANET[16]. In MANET, each node in the topology of the network is free to join and can be left at any time which makes Ad hoc network infrastructure network which results in making network unpredictable and changes rapidly. Because of these reasons any foreign node can access the network easily.The controlling and servicing actions are done by themselves if the central control is absent.

For forwarding and receiving the packets the network consists of a router which helps in doing this without any centralized administration. In the presence of MANET we could not guess the topology and results in malicious node, hence security plays a major role. Security prevents the unauthorised nodes from using the network [19]. There are other security[15] issues in MANET were parameters of the routing messages are changed hence wrong packets flow in wrong direction to wrong destination. There is chance of changing sequence numbers which results in wrong mechanism of transmitting packets in network. The attacks[19] are of two different attacks namely passive and active attack. Passive attack are difficult to detect because it will retrieve data without making any changes to actual data it does not affect the normal functioning hence it is very dangerous than active attacks [17]. In case of active attacks the malicious nodes in the network collect information required and perform required changes hence active attacks are easy to detect as the user notice the changes or modifications done. In Active attacks there are two more attacks external and internal attacks. When attacks are made by foreign or outside node it is known as external attack. Whereas attacks made by nodes within the network are said to be internal attacks. In this paper we approach an efficient method to overcome issues made by malicious node or black hole attack by using ADOV routing protocol.

Routing protocols

Since ad hoc plays in a area where there is no fixed or unpredictable network, hence each node communicate with each other by forwarding packets themselves and create connectivity. The connectivity has been supported by routing protocols namely, AODV (Ad-hoc on Demand Distance Vector) DSR (Dynamic Source Routing) DSDV (Destination Sequenced Distance Vector).As shown in Fig 1 : Also acting as host, each node will be acting as a router in order to discover path and sends packets. The major goal of an routing protocol is to provide optimal path with minimum distance or nearest path from source to destination.

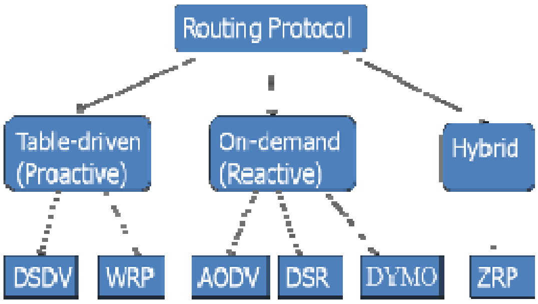

Fig 1: Hierarchy of routing protocols

A. Proactive protocols

Proactive protocols are basically table-based. The entire topology of the network is represented in terms of tables. These tables are regularly updated within the nodes . In order to update the tables, topology information should be swapped between the nodes on regular basis results in pressure on the network.

Example: of proactive protocol is DSDV (destination-sequenced-distance-vector). It is a table-based routing system which is based on Bellman-Ford algorithm. By the result of development done to Bellman-ford algorithm, the problems of loops in routing tables are replaced by sequence numbers. The DSDV are used by ad-hoc networking mobile were every node behaves as a router. DSDV requires regular update its routing table, which make use of battery power even though network is stable.

B. Reactive protocols

Reactive protocols are demand based protocols. These protocols do not attempt to modify the information in routing table regularly. Routing information are called only when it is necessary, and identification of path to forward packets are dependent on the sender, which questions the whole network. The disadvantage of reactive protocol is delay in route discovery, since these protocols do not maintain a continuous routing table.

Example: Dynamic Source Routing (DSR) is an on-demand protocol. Every individual that helps in forwarding packets will add its possessing address to its list carried in the packet. The purposed node will produce a reply messages that contain the list of addresses received in the route application and forward it back along the pathway to the source. When node is not capable of confirming its successful submission of packet t tries to resend packet. If there is N number of resending packet fails then protocol generates a error message and send it to the source node.

C. Hybrid Routing Protocols

Hybrid routing protocols differ from previous two protocol. Because here the nodes in a group are organized and are assigned each with a functionalities. Here router table and altered packet size are reduced only a part of the network is included instead of whole, thus overhead on control is reduced. Here in this protocol a group of nodes are formed close to each other forming a cluster. Each group will have a leading which will communicate with other nodes instead of individual node communication.

Example: is AODV routing Protocol.

An Overview of AODV Protocol and Black hole attack

Ad Hoc on-demand vector routing protocol is a reactive protocol for both networks so that these nodes will maintain routes only between the nodes which are need for communication in order to forward packets. AODV routing protocol [11] is based on both DSDV and DSR algorithm . It demands the route at the start of the communication session and uses until it breaks then creates or setup a new route further. In this mechanism nodes do not contain information about whole route path except information about source and destination. Hence AODV messages will not have increasing size but uses sequence numbers to identify how fresh a route is.

AODV protocol is composed of 2 mechanisms

1. Route discovery: This contains route request (RQ) and route reply (RP) control messages in this phase.

2. Route maintenance: This contains route error control message in this phase.

Whenever a node wants to forward packet to a destination it will search for ‘fresh route’ in route table as to check whether a new route is available for transmitting packet to destination. If not, node will take an initiative to discover path by broadcasting a (RQ) route request message for every nodes nearby nodes, this RQ message will further be forwarded to its intermediate nodes this process will continue until a now fresh route is discovered to the destination. At this stage a RP message is created. The RP travels back to the RQ node. .Now a RQ will be replied by an intermediate node, where this intermediate node will send a RP to the destination. This way a fresh route is generated .By this way a shortest route will be selected to forward packet to destination and will be updated for further communication between nodes.

During this process there may be a chance of attacker node trying to access packets from sender node which is the source node. Since malicious node sends the RQ message saying that it has a nearest path to the destination, packet will be sent to malicious node this attack of packet is known as Black hole attack [20] . As shown in Fig 2.

Including this there are two more attacks called Gray Hole [12]attack which selective forwards packet to destination and Warm Hole attack in this attacker in a network records bits at one position and sends them selectively to another location.

Black hole attack is the Denial Of Service [18] in which a malicious node fakes that it has a shortest path to the destination by taking advantage of the routing protocol.

When a source node sends RQ request message to its neighboring nodes to search fresh or new paths to the destination. Malicious node replies immediately to the sender node as it has nearest path to the destination. The source or sender node thinks that route discovery process is complete. Without having routing table malicious nodes reply request s accepted by the sender accepts the reply request of the malicious node discarding reply request of other nodes. Instead of replying back the attacker drops the received message.

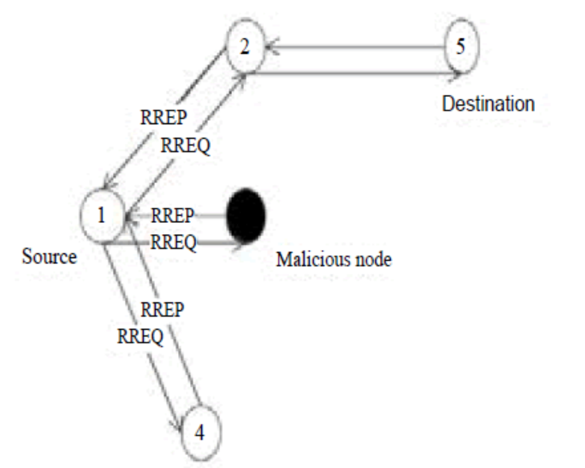

Figure 5: Black Hole Attack.

Fig 2 : Black Hole Attack

Further we are discussing case study on real time problem
,describing about literature survey and briefly explaining the optimal solution for black hole attack using defense mechanism also mentioning performance metrics and ending with conclusion.

2. CASE STUDY

A huge extortion cyber-attack hit dozens of nation, blocking computer data for ransom at hospitals, telecommunication firms and so on. The attack affects Britain's local service forcing affected hospitals to shutdown wards and emergency rooms. Similar attacks were reported in Spain, Portugal and Russia.

Two firms of security Kaspersky cab and Avast said they had found out the malware behind the attack.

The Russian Ministry has confirmed cause for this disaster is'Ransomware' attack which blocked data on infected computers and orders money to release it. Hospitals in Britain say there is no access to their computer and source.

3.LITERATURE SURVEY

In mobile Ad hoc network nodes are mobile that is nodes move from one network to another without any communication. The network does not provide security hence nodes can be subjected to various attacks. In this study Semih Dokurer et.al., [1] found out the methods that cause the presence of a Black hole. In further study we also implement the solution for this. This attack includes the presence of malicious node which contains the shortest path for receiving the packets. Using AODV routing protocol the black hole attack on Ad hoc network can be examined.

H.A. Esmaili et. al., [2] identified that how these attacks can be prevented so that security can be provided. He declared that if the network consists of malicious nodes then packet delivery ratio will be down or less. The paper describes the Black hole attack which occurs in the Ad hoc networks. Malicious nodes send an reply to the source node after receiving the packet. And as result the required destination will not receive the packet.

Security has been widely the major issue that seen in Ad hoc networks. Lu et. al., [3] proposed SAODV which is the further development to the AODV. Source node on receiving the reply from the nodes that the nodes are ready to transfer the packets to destination, it sends the packets to the nearest node with shortest path to the destination. If there is an attack from the black hole, after receiving the packets immediately the reply is sent to the source that the packet is received.

Deng et. al., [4] also noticed that the path has to been considered even after receiving the packets. Every information in the nodes should have the flow like next hop to send the proper reply. When the route reply has been received by the source node it sends the further request to the neighbour node. The source node identifies the safe path for transferring the packets. Also detects the node as a Black hole in the presence of malicious ode.

Kamini Maheshwar et. al., [5] described methods which includes the detection of the Black hole using AODV protocol. And advanced approaches have been utilized based on the drawbacks that appear in the network.
Packet drop will be occurred that is source node instead of transfering the node to correct destination drops this path and forward it to malicious node.

Joglekar C.M et. al., [6] Have told that we try to implement the measures to provide security against the black hole attack in the network. And the solutions are obtained at the starting stages of the attack without consumption of time. The blackhole will be removed in Mobile Ad hoc network.

Chinky Jain et. al,. [7] mainly focused on the black hole attack in MANET (Mobile Ad hoc Network). We are aware that security plays a major role in the network , we look forward to solve this attack by giving an algorithm approach which analyze the attacks and provide better security to the network . The effects that are produced by the attacks are detected using simulation and proper result is obtained for it.

As the nodes are mobile that is it moves from one place to another a black hole may enter the network, receive the packet and continue the activity. Therefore there are weaknesses in the security, which is the major issue in MANETs. MANETs are more vulnerable so V.Kaviyarasu et al., [8] explained that vulnerability can be analyzed in case of Distributed Denial of Service in MANETs. And security can be granted and network performance will be increased.

Mobile Ad hoc networks are distributed over various sectors and find many applications. It does not contain any centralized infrastructure and is vulnerable to many kinds of attacks and we focus particularly on Black hole attack. in this paper John Haggerty et. al., [9] proposed about obtaining the required methods to reduce these attacks to provide security.

In case of attacks there is contribution of malicious nodes in the network. AODV(Ad hoc on Demand Distance Vector) is the main routing protocol used in the Ad hoc networks. In this paper Dr. S. Tamilarasan et al. [10] have given the ways to identify the malicious nodes in the network and try to avoid the presence of black hole and increase the network performance.

4. PROPOSED METHODS FOR THE BLACK HOLE DETECTION

To prevent Black hole attack a mechanism is proposed. This defense mechanism will detect attackers and provide efficient transmission of packets from source to destination on the right shortest route.

Defense mechanism against Black hole attacks contains three steps

Step 1:In the first step of the defense mechanism or black hole detection process is based on timing information presenting NRMT. To prevent Black hole attack, every node in the network contains Neighborhood Route Monitoring Table (NRMT) .The information that which route to be serviced is given by NRMT. It includes source ID, source Sequence number, Destination sequence number, Destination ID and a threshold value of sequence number [13], the NRMT maintains the process that is when the request (RQ) is sent to the source node and the reply (RP) after being sent to the destination. In the network if suppose the node is the normal one after receiving the (RQ) packet it looks into the routing table that whether we are transferring to the correct destination or not, if proper then (RP) packet is sent to the source node in the right path. Routing information is checked using MIN-TIME. If the node is Black hole it immediately sends the (RP) to the source without checking the route table. NRMT will have the information of timings, after receiving the route reply(RP) every node finds out the difference between the (RQOT) route request out time and (RPIT) Route reply in time with the DIFF-TIME. If the node is Black hole then Diff-TIME is going to be less than the MIN-TIME.. Thus this node will be identified as attacker or black hole.

Step 2: In the second step the defense mechanism is based on threshold value of sequence number. RPs sequence number will contain maximum sequence number in DOS which is known as threshold value [14]. In this process if the value of current RP sequence number is more than threshold value then this node is identified as black hole and is discarded or deleted from the routing table .If the node is confirmed as a malicious node then all the other nodes in the network are notified with a message not to utilize any network resources. Refer Fig 3

Step 3: This defense mechanism based on Promiscuous node. We have given an example where a node A wants to exchange message with node D and this network contains a malicious node node F. As usual node A forward a RQ packet in the network and waits for the response from the node to send RP that obtained fresh route to the destination node D. In this case there are two cases:

Case 1: The route reply (RP) is received from the destination node.

Case 2: The reply which is obtained from the intermediate node , and the node preceding this node will actually switch to the promiscuous mode and send an HELLO message to the destination. If it receives the message then it is proved that the route is safe or else the node is foreign node and that particular path could not be chosen.

PERFORMANCE METRICS

1. Network Throughput

Network throughput is defined as number of data moved from one node to other successfully.

End-To-End delay

End-To-End delay is amount time taken by a node to transmit data from one node to other.

3. Network Load

Network load plays a major role which effects on networks protocol, which refers overall load that is impact by the entire higher layer in WLAN nodes in the topology.

4. Latency

Latency is amount of time taken by a packet of data to get from one designated point to another.

5. Packet Delivery ratio

It is referred to a ratio of amount of packets delivered successfully to packets that are sent by the source node

Fig 3 : Flow chart for detection of Black Hole

5. CONCLUSION

In this appealed paper we have discussed about routing protocols. Security Problems caused by Black hole attacks. We have proposed an efficient and feasible solution in AODV protocol using defense mechanism for to detecting and preventing Black hole attack in MANETs to produce safe and secure routes. By defense mechanism as mentioned we can decrease the number of attacker nodes and redirect a secure route in the network. Preventing of Black hole is challenging task in Ad hoc network. In future progress we have an intension to develop simulation to analyse the results of the proposed feasible solutions based on performance parameters.

6. REFERENCES

[1]Dokurer,s.,Erten,M. Y., Akar,E. C.,Performance analysis of ad-hoc networks under black hole attacks.in IEEE Southeast Co, pp. 148-153,Richmond,USA(2007).

[2]Songbai Lu,Longxuan Li , Kwon-Yan Lam and Lingvan Jai "SAODV: A MANET rouing Protocol that can Withstand Black Hole Attack,"Proceedings of international conference on computational intelligence and security, 2009,pp.421-425

[3]Esmaili,A. H., Khalili Soja, R. M., Ghraee, H. performance analysis of AODV under Black hole attack through use of OPNET simulator, world of science and information technology journal, 1(2),49—52,2011.

[4]Hongmei Deng, Wei Li and Dharma P, Agarwal,"Routing security in wireless Ad hoc networks", IEEE Communication Magazine vol.40,2002,pp. 70-75.

[5]Kamini Maheshwar, Divakar singh, "Black Hole Effect Analysis and Prevention Through IDS in MANET Environment" European Journal of Applied Engineering and Scientific Research, 1(4),pp.84-90,2012.

[6]Joglekar C.M., "Acknowledgement based security for MANETs Against DDOS Attacks" SVIT Chincholi,SPP University., Pune Journal of Electronics and Communication Engineering., pp 18-23.

[7]Chinky Jain and Pradeep Tyagi "Simulation of Black Hole Attack In MANET" International Journal Of Engineering and Computer Science ISSN: 2319-7242 Vol 5 issue 08 august 2016.

[8] V.Kaviyarasu and S Baskaran : "security In MANET Against DDOS Attack"; International Journal Of Computer Trends and Technology IJCTT-Vol 7 number 1-jan 2014

[9] John Haggerty and Albandari Alsumayt : "A Survey of Mitigation Methods Against DOS Attack On MANETS"; Science in Information Conference 2014 Aug 27-29,2014 London UK

[10]Dr. S. Tamilarasan: "Securing AODV Routing Protocol from Black Hole Attack"; International Journal of Computer Science and telecommunication Vol 3,Issue 7 July 2012.

[11]K Lakshmi and S Manjupriya et. al, "Modified AODV Protocol Against Black Hole Attacks in MANET"; International Journal of Engineering and Technology Vol 2(6),2010,444-449.

[12]Nisha and Sandeep Arora et.al, "Analysis of Black Hole and Gray Hole Attack on RP-AODV in MANET"; International Journal of Engineering Research and Technology Vol 2 Issue 8,aug 2013.

[13]Govind Sharma and pramod Kumar singh :" An Effective Prevention of Black Hole Problem in AODV Routing Protocol in MANET"; 2012 IEEE 11th International Conference on Trust , Security and Privacy in Computing and Communication.

[14]Ranjeet kaur et.al :"Security against DDOS Attacks in MANETS "; International Journal of Computer Science and Mobile Computing , Vol 3 Issue 3 Mar 2014 pg.1024-1030.

[15]Rajib Das:"security Measures for Black Hole Atack in MANET:An approach.

[16]Ms.Nidhi Sharma :"Black Hole node Attack in MANET"; 2012 Second International Conference on

Advance Computing and Communication Technology.

[17]Pooja Gudadhe ;"Detection o Denial of Service Attacks on Wireless Network"; International Journal of advanced research in Computer Engineering and technology. Vol 4 Issue 11 Nov 2015.

[18]Ms.Sanam E Anto :"A Survey on DOS Attacks and Detection Schemes in Wireless Mesh Networks. International Conference on Modelling Optimisation and Computing April 10 & 11 2012.

[19]Er. Meenakshi Sharma :"DOS Attack Mitigation in MANET"; IJEDR Vol 4 Issue 3 2016.

[20]Gayathri Bendali :"An Improved Black Hole Attack Detection and prevention method for Wireless Ad hoc Networks"; International Conference IEEE 2016

Author's details

1 Vijayashree V, Student, Department of Computer Science and Engineering,T.John Institute of Technology, Karnataka, India, vijayashree96gowda@gmail.com

2 Nisha C P, Student, Department of Computer Science and Engineering, T.John Institute of Technology, Karnataka, India, nivcp15@gmail.com

3 Suma R, Associate Professor, Department of Computer Science and Engineering, T.John Institute of Technology, Karnataka, India, sumar@tjohngroup.com.

4 Dr.Siddaraju B, Professor & Head, Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Karnataka, India, siddaraju.ait@gmail.com