ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

A survey of cooperative blackhole attack in mobile ad hoc networks

Prof. Ajit Singh, Anju Sharma

CSE (Network Security), SES BPSMV University,

Khanpur Kalan, Sonepat, Haryana

***Abstract*— A MANET is an infrastructure less network that consists of mobile nodes that communicate with each other over wireless links. In the absence of a fixed infrastructure, nodes have to cooperate with each other in order to provide the necessary network functionality for discovery and maintaining path. One of the principal routing protocols used in Ad hoc networks is AODV protocol. The security of the AODV protocol is threaded by a particular type of attack called 'Black Hole' attack. In this attack a malicious node advertises itself such a way that it has the shortest path to the destination node. This paper gives solution for co-operative Black Hole Attack at the time of route discovery phase and gives solution without monitoring other nodes.**

***Keywords*— Mobile Ad hoc Network (MANET), network, cooperative node, blackhole attack, ADHOC, MAC**

I. INTRODUCTION

Wireless ad hoc networks give the concept of distributed architecture so that the sharing of information as well as resources can be done effectively. A mobile ad hoc network is defined as a wide public area network in which number of mobile nodes are connected. Mobility is the key property of such kind of network. These kind of networks performs the communication with multiple nodes under multiple controller devices. A mobile network is defined as a distributed network that have different kind of communicating devices such as mobiles, laptops etc. This kind of networks performs the multi-hop communication over the network. The data is transmitted over these networks using radio waves.

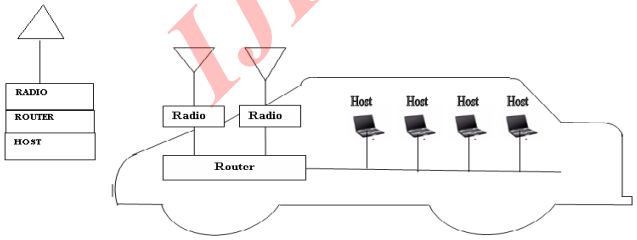

Figure 1: An Example of MANETs

Here Figure 1 is showing the example of a standard mobile ad hoc network. The network is equipped with different kind of communicating devices. There are different definitions of an ad hoc network respective to the type of devices as well as the communication devices involved in the system itself. These networks are defined here under.

A mobile ad hoc network is responsible to perform the communication between the mobile devices without setting up any dedicated or static infrastructure. The work includes the specification of dedicated routers and other communication devices without the inclusion of cables. It is actually described as the autonomous communication system in which wireless links are connected in the form of arbitrary graph. Such kind of networks can be established in the form stand alone acquired fashion and provide the effective communication over the network.

A mobile network perform the multi-hop cellular network model that requires the base stations as the main controller points. These kind of networks can perform the reliable communication between two or more mobile nodes. In these networks, the base stations can be defined at fix locations. In this mobile network, an infrastructure less network topology is defined. This network architecture is defined in a P2P

network. The decision of next node selection depends on different vectors such as number of packets transmitted in store and forward approach. In such network, a source and destination nodes are specified and the intermediate communicating nodes are selected by the network itself dynamically according to the routing information over the network. The multi-hop communication example is shown in Figure 2

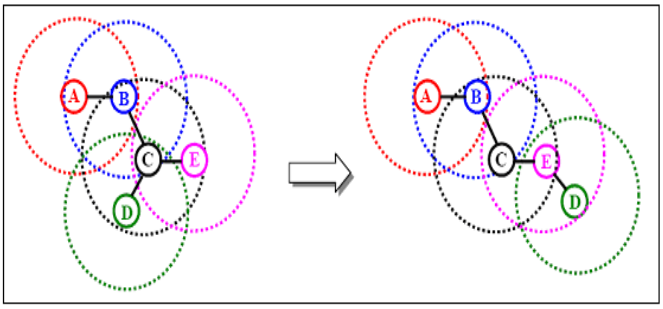

Figure 2: Multi-hop Communication in MANET

The main communicating criterion of MANET is the selection of next node. This can be done in static or dynamic way. The static routing can be performed by maintaining a routing table and the dynamic routing is identified as the on demand routing. This kind of routing start with the source node and with the definition of coverage range the next neighbour node will be selected for the communication. This process is repeated till the destination node not arrived.

II. BLACKHOLE ATTACK

In this attack, When a source node wants to send data packets to a destination node, if there has no route available in its RT(route table), it will initiate the routing discovery process. Assume that node B to be a malicious node (as shown in Figure 3 and 4). Using the routing AODV protocol, node B claims that it has the routing to the destination node whenever it receives RREQ packets, and sends the response to source node at once. The destination node may also give a reply. If the reply from a normal destination node reaches the source node of RREQ first, everything works well; but the reply from node B could reach the source node first, if node B is nearer to the source node. Moreover, node B does not need to check its RT when sending a false message; its response is more likely to reach the source node firstly. This makes the source node thinks that the routing discovery process is completed, ignores all other reply messages, and begins to send data packets. The forged routing has been created. As a result, all the packets through node B are simply consumed or lost. Node B could be said to form a black hole in the network, and we call it as the black hole attack.

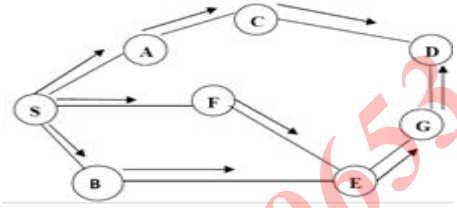

Figure 3: Propagation of RREQ message

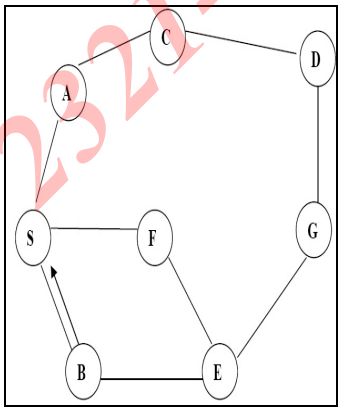

Figure 4: Propagation of RREP message

Attack Scenarios

In each attack scenario all the good nodes behave well consistently throughout, however the behaviour of malicious nodes varies with the attack type as described below.

- Case 1: Single Black Hole Attack.

In case of a single node attack, the node drops all the packets instead of forwarding to destination. In that case black hole node may send the RREP with its own identity black hole node replies with higher sequence number because they do not know the exact sequence number of the destination node. Consider the network topology described in Figure 5. Here Node S is the source node and node D is the destination node. Source Node broadcast RREQ packet to the neighbour nodes. Node BH is the black hole node and it responds to source node with RREP and the encrypted packet P. Node BH RREP is

choosed among various replies due to its Largest Sequence Number & Minimum Hop Count. As RREP is processed at Source Node, Source Node checks by applying the global Symmetric cryptosystem, it firstly decrypts the message. As BH is the black hole node, at source node the packet P may not be decrypted successfully or it has invalid MAC or T_S is not in reasonable time delay range or decrypted Ts is not same as the one in the packet without encryption. In all these cases SN discards the packet because MAC or key might be potentially forged. In addition, a packet with an invalid MAC is discarded. SN sends out an alarm message to isolate the malicious node in the network. All nodes of the network after getting the alarm message flushes all the entries related to Node BH from the respective tables.

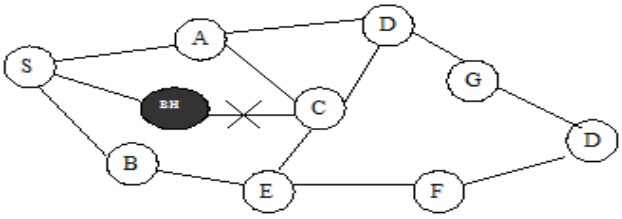

Figure 5: Network Topology for Single Black hole attack

- Case 2: Cooperative Black Hole Attack.

In case of a cooperative black hole attack, the BH forwards all the data to BH' and BH' drops them instead of forwarding to the destination node as shown in network topology. Here Node S is the source node and node D is the destination node. Source Node broadcast RREQ packet to the neighbour nodes. Node BH and BH' is the black hole nodes and BH responds to source node with RREP and the encrypted packet P. Node BH RREP is choosed among various replies due to its Largest Sequence Number & Minimum Hop Count. As RREP is processed at Source Node, Source Node checks by applying the global Symmetric cryptosystem, it firstly decrypts the message. As BH is the black hole node, at source node the packet P may not be decrypted successfully or it has invalid MAC or T_S is not in reasonable time delay range or decrypted Ts is not same as the one in the packet without encryption. In all these cases SN discards the packet because MAC or key might be potentially forged. SN sends out an alarm message to isolate the malicious node in the network.

III. CHARACTERISTICS OF NETWORKS

- Network Size: The size of a network is defined in terms of network area as well as in the form of network nodes. A Mobile network can perform a long distance communication upto LOS by using the multi-hop communication.
- Connectivity: The connectivity is defined in the form of link selection for the next node. To identify the neighbour of a node, the coverage range analysis is done over the nodes.
- Distributed Operation: These kind of networks does not having any centralized control to perform the network operations. The network is distributed among the terminals.
- Multi-Hop Routing: To enable the infrastructure free communication as well as long distance communication, the multi-hop communication is provided by mobile network.

IV. LITERATURE REVIEW

In Year 2012, Rajesh Yerneni performed a work, " Enhancing performance of AODV against Black hole Attack". In this paper, a method is proposed called Secure-Ad hoc On demand Distance Vector (SAODV) algorithm that mitigates black hole attack by analyzing destination sequence number and validating the destination by random value. Simulation results show that the proposed protocol provides better security by increasing the packet delivery ratio when compared to AODV in presence of black hole attacks.

In Year 2008, Hesiri Weerasinghe performed a work," Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks:Simulation Implementation and Evaluation". In this paper, Author proposed a solution to identifying and preventing the cooperative black hole attack. Presented solution discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. In this paper, via simulation, Author evaluate the proposed solution and compare it with other existing solutions in terms of throughput, packet loss percentage, average end-toend delay and route request overhead.

In Year 2011, Mehdi Medadian performed a work," Detection and Removal of Cooperative and Multiple Black Hole Attack in Mobile ADHOC Networks". In this paper, an approach is proposed to combat the Cooperative/ Multiple Black hole attack by using negotiation with neighbors who claim to have a route to destination. the Simulation's results show that the proposed protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.

In Year 2011, Harsh Pratap Singh performed a work," Guard against cooperative black hole attack in Mobile Ad-Hoc Network". To preventing black hole attack, this paper presents RBS (Reference Broadcast Synchronization) & Relative velocity distance method for clock synchronization process in Mobile ad-hoc Network for removal of cooperative black hole node. This paper evaluates the performance in NS2 network simulator and Presented analysis indicates that this method is very suitable to remove black hole attack.

In Year 2010, Poonam Gera performed a work," Trust Based Multi-Path Routing for End to End Secure Data Delivery in MANETs". In this paper, Author propose a novel method to enhance security in both phases. Author present the design of a routing protocol based on trust, which ensures secure and undisrupted delivery of transmitted data. An end to end encryption technique is used to self encrypt the data without the necessity of a cryptographic key.

V. EXISTING METHODOLOGY

A mobile network is a dynamic reconfigurable network with heavy traffic over the network. As the network is available widely, there are more chances of inclusion of external nodes that behave as the attack node. One of the such problem in mobile network is the cooperative blackhole or grayhole attack. In which more than one nodes cooperatively perform the attack. In such attack, the malicious blackhole nodes communicate effectively between them but as they get the packet from some other node, they does not forward the packets. The presented work is about the table driven analysis will be performed over each node to identify the trustfulness of a node.

In this work, the existing AODV protocol will be modified and a new bit will be defined to define the trustful status. If the status is 1, the node is valid node and if it is 0 the node is blackhole node and no communication will be performed over that node. As the communication will be performed, each node will be analysed by its neighbouring nodes and build a trust table. Each neighbour node to that node will perform the REQ and wait to get the ACK. Identify the number of request performed and the replied received. This whole information will be maintained in a shared table. With three fields, source node, destination node and REPLY status. The reply status is by default 0 as the successful replied is received by a node, the value in the table changed to 1. Now the protocol will check this shared table and identify the REQ-RPLY ratio. If the Ratio is greater than the threshold value, the node is taken as the valid node and communication over that node is performed.

VI. SOURCES OF DATA

To work with mobile network we need to define a mobile network with n number of nodes. For this we need to collect the information about the network scenario. The scenario includes the information like

- No of Nodes
- Mobility
- Channel Type
- Propagation
- Transmission Speed
- Packet Size

To represent all these parameters we need to collect relevant scenarios. We can collect these scenarios either from some existing literature.

VII. PROPOSED WORK

Our aim is to remove the cooperative blackhole node from the network. It will improve the network throughput. This can be fulfilled if following objectives are met: i) To identify the Blackhole node over the active path by performing a nearest neighbor analysis. As the blackhole node will be identified a status set will be performed by using bit change .ii) To perform the communication over the safe path in the network. iii) To define a eventual process to identify all the passive blackhole attack over the network that are not the part of active communication path. The analysis of the work will be performed under different communication parameters such as network throughput, error rate etc.

ISSN: 2321-9653

VIII. RESEARCH METHODOLOGY

The proposed work is about to detect the cooperative blackhole nodes in a mobile network and to generate a secure and reliable path. In this work, a nearest neighbour analysis will be performed to identify an active blackhole node in the active path. As the node will send a ROUTE REQ message to the neighbouring nodes and if some node does not return then REPY in the specified time interval then it is taken that the node is a blackhole node. To ensure the status of node, all neighbours to that node will perform the request to that suspected node. If maximum nodes does not get the reply. The node is declared as the blackhole node and its status will be set to disable by including a status bit. Once the black hole node is detected, next neighbour is detected as the compromising node and the transmission will be performed through that compromising node.

As the attack will be detected, an eventual process will be generated separately to identify all the blackhole nodes that are present in cooperation with blackhole node. These blackhole nodes can be active or passive. A nearest neighbour analysis will be performed by all neighbours to identify the blackhole nodes in the chain. The step by step work of the given research proposal is shown as

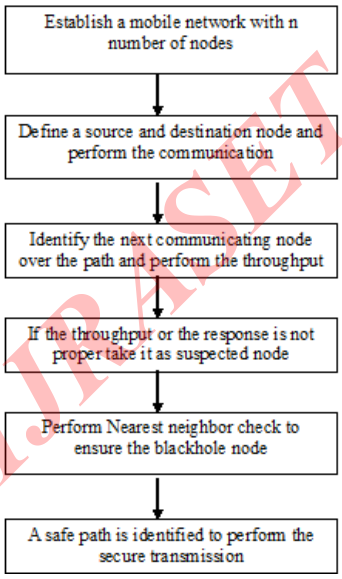

Figure 6: Path Generation

In order to find the black hole nodes among the network, a source node can take advantages of MAC and Timestamp (T_s) to detect all Black hole nodes. In the black hole node detection phase, all detected misbehaving nodes can be excluded from the route.

Here Source Node checks by applying the global Symmetric cryptosystem, it firstly decrypts the message. If message is decrypted successfully and after decryption same MAC is found and Ts is in reasonable time delay range and decrypted Ts is the same as the one in the packet without encryption. Then this packet is regarded as a valid packet and this routing is also regarded as a secure routing from the source node to the destination node. Then the source node begins to send data packets. Else message is not decrypted successfully or MAC is not found or T_s is not in reasonable time delay range or decrypted T_s is not the same as the one in the packet without encryption. Then Source Node (SN) discard the packet because the key is disclosed before it receives the packet and MAC might be potentially forged. SN send out an alarm message to isolate the Black hole node in the network.

IX. CONCLUSION

Blackhole attack is non cooperation in certain network operations, i.e. dropping of packets which may affect the performance, but can save the battery power. In this paper work is about to remove the cooperative blackhole node from the network. It will improve the network throughput. Along with this the work will give an efficient and reliable transmission over the network.

REFERENCES

[1] Rajesh Yerneni," Enhancing performance of AODV against Black hole Attack",

CUBE 2012, September 3–5, 2012, Pune, Maharashtra, India. ACM 978-1-4503-1185-4/12/09

[2] Hesiri Weerasinghe," Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks:Simulation Implementation and Evaluation", International Journal of Software Engineering and Its Applications Vol. 2, No. 3, July, 2008

[3] Mehdi Medadian," Detection and Removal of Cooperative and Multiple BlacHole

Attack in Mobile ADHOC Networks", 2011 International Conference on Computer and Software Modeling IPCSIT vol.14 (2011) © (2011) IACSIT Press, Singapore

[4] Sweta Jain," A Review Paper on Cooperative Blackhole And Grayhole Attacks in Mobile Ad hoc Networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.3, September 2011

[5] Sanjay Ramaswamy," Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".

[6] Varsha Patidar," Black Hole Attack and its Counter Measures in AODV Routing Protocol", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5

[7] Harsh Pratap Singh," Guard against cooperative black hole attack in Mobile Ad-Hoc Network", International Journal of Engineering Science and Technology (IJEST) ISSN : 0975-5462 Vol. 3 No. 7 July 2011

[8] Poonam," Eliminating Misbehaving nodes by Opinion Based Trust Evaluation Model in MANETs", ICCCS'11, February 12–14, 2011, Rourkela, Odisha, India. ACM 978-1-4503-0464-1/11/02

[9] Poonam Gera," Trust Based Multi-Path Routing for End to End Secure Data Delivery in MANETs", SIN'10, Sept. 7–11, 2010, Taganrog, Rostov-on-Don, Russian Federation. ACM 978-1-4503-0234-0/10/09

[10] M.Shobana," GEOGRAPHIC ROUTING USED IN MANET FOR BLACK HOLE DETECTION", CCSEIT-12, October 26-28, 2012, Coimbatore [Tamil nadu, India]

ACM 978-1-4503-1310-0/12/10

[11] Poonam," Misbehaving nodes Detection through Opinion Based Trust Evaluation Model in MANETs", International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET, Mumbai, India ICWET'11, February 25–26, 2011, Mumbai, Maharashtra, India. ACM 978-1-4503-0449-8/11/02

[12] Kamaljit Kaur," Comparative Analysis of Black Hole Attack over Cloud Network using AODV and DSDV", CCSEIT-12, October 26-28, 2012, Coimbatore [Tamil nadu, India] ACM 978-1-4503-1310-0/12/10

[13] B.Revathi," A Survey of Cooperative Black and Gray hole Attack in MANET", International Journal of Computer Science and Management Research Vol 1 Issue 2 September 2012 ISSN 2278-733X

AUTHORS

First Author – Prof. Ajit Singh, M.Tech (Professor in CSE and IT Department) ,SES BPSMV University, Khanpur Kalan, Sonepat, Haryana)

Second Author – Anju Sharma, M.Tech (Pursuing), CSE (Network Security), SES BPSMV University, Khanpur Kalan, Sonepat, Haryana