ISSN:0975-9646

Onkar V Chandure et al / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2607-2613.

A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV routing protocol in MANET

Onkar V. Chandure[1#], Prof. V. T. Gaikwad[2#]

[1]*ME- I.T (Student), SIPNA's College of Engineering & Technology, Amravati (MS) INDIA*

[2]*Associate Professor, Dept of CSE, SIPNA's College of Engineering & Technology, Amravati (MS) INDIA*

Abstract: **MANET has no clear line of defense, so, it is accessible to both legitimate users and malicious attackers. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. In this we develop a security based technique using some routing protocols so as to recognize & eradicate the problem of gray hole attack in mobile adhoc network. In first phase we develop the method to handle the spiteful node in the network.In the next phase of protocol is to implement the gray hole attack so as to recognize gray hole attack & find out its consequences on the adhoc network. By simulation results, we show that proposed security technique to achieve the desired result .Simulation wiil be carried out using network simulator tool (ns-2) so as to address the problem of gray hole attack.**

Keywords: **Adhoc network, Gray Hole, Security threat, ns-2.**

I. INTRODUCTION

An adhoc network has a certain characteristic, which imposes new demands on the routing protocol .The most important characteristics are the dynamic topology, which is a consequence of node mobility. A mobile ad-hoc network (MANET) is a network [1, 2, 7] formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. The MANET is more vulnerable to be attacked than wired network. These vulnerabilities are nature of the MANET structure that cannot be removed. As a result, attacks with malicious intent have been and will be devised *to exploit* these vulnerabilities and *to cripple* the MANET operation. The most important characteristics are the dynamic topology, which is a consequence of node mobility. A Mobile Ad -Hoc Network (MANET) is a group of mobile nodes that cooperate and forward packets for each other. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network. In this work, we discuss one such attack known as Gray Hole Attack on the widely used AODV (Ad -hoc On-demand Distance Vector) routing protocol in MANETs. A mechanism presented shows the method to detect & prevent from gray hole attack in Mobile ad hoc network [9]. It is an autonomous system, where nodes/stations are connected with each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. This property of the nodes makes the mobile ad hoc networks unpredictable from the point of view of scalability and topology. In ad hoc networks, the routing protocols are divided into three categories: Proactive, Reactive and Hybrid.

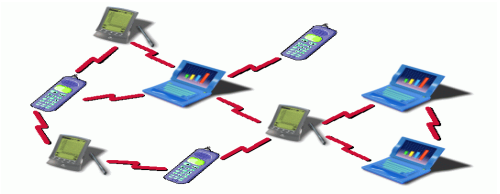

Fig 1: Basic concept about the MANET

II. LITERATURE REVIEW & RELATED WORK

S.Banerjee et. al. [3] has also proposed an algorithm for detection & removal of Black/Gray Holes. S.Ramaswamy et. al. [4] presented an algorithm to prevent the co-operative black hole attacks in ad hoc network. This algorithm is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attacks. According to their algorithm instead of sending the total data traffic at once, they divide it into small sized blocks, in the hope that the malicious nodes can be detected& removed in between transmission. Marti et al [5] proposed to trace malicious nodes byusing watchdog/pathrater. In watchdog when a node forwards apacket, the node's watchdog verifies that the next node in the path also forwards

the packet by promiscuously listening to the next node's transmissions. Gonzalez et al [6] presents a methodology, for detecting packet forwarding misbehavior, which is based on the principle of flow conservation in a network. The problem of security and cooperation enforcement has received considerable attention by researchers in the ad hoc network community. Mechanisms or technique to prevent the routing layer from malicious attacks for securing the system of a MANET by cryptographic techniques are proposed by Y. Hu, Perrig and Johnson [7], Papadimitratos and Hass [8], Snazgiri [9]. Technique to deal with the authentication of malicious user or malicious situation related with the security have been proposed by Zhou and Haas [10] with the help of Trusted certificate authority procedure.Buttyan and Hubaux [11] have presents aself organized PGP-based mechanism to authenticate nodes using chains of certificates and transitivity of trust. Zeshan [12] proposed a two-fold approach for detection and isolation of nodes that drops data packets. Usha and Radha [13] proposed extension to the TWOACK scheme, in which each node must send back a normal Ack to its immediate source node after receipt of any kind of packet. This scheme requires an end to end Ack packet (i.e. Nack) to be sent between the source and the destination.

III. ANALYSIS OF AODV PROTOCOL

The AODV protocol builds on the DSDV algorithm .it is an on demand routing algorithm. But in contrast to DSR it is a not source based routing scheme rather every hop of a route maintains the next hop information by its own. Operation of the protocol is divided into two functions, route discovery & route maintenance. At first all the nodes send hello message on its interface and receive hello message from its neighbors. This process repeats periodically to determine neighbor connectivity when a route is needed is to some destination, the protocols start route discovery .It uses two term route request & route reply. This RREP packet is unicast to the next node on RREP path. The intermediate node on receiving the RREP packet make reversal of path set by the RREQ packet. As soon as RREP packet is received by the source, it starts data transmission on the forward path set by RREP packet. Sometimes while data transmission is going on, if path break occurs due to mobility of node out of coverage area of nodes on the active path, data packets will be lost. When the network traffic requires real time delivery (voice, for instance), dropping data packets at the intermediate nodes can be costly. Likewise, if the session is a best effort, TCP connection, packet drops may lead to slow start, timeout, and throughput degradation. It is crucial for AODV to properly handle the sequence numbers A node has to update its own sequence number in two cases:

A] Control Messages in AODV:

• *Sequence Number and Routing Table Management:*

• Before starting a route discovery process, the node has to increment its own sequence number.

• A destination node has to update its own sequence number to the maximum of its current sequence number and the destination sequence number in RREQ packet immediately before transmitting the RREP packet.

The sequence numbers in the routing table entries may be changed by the node only in the following circumstances:

• Offer of a new route to itself, if it is the destination node.

• Reception of an AODV message with new information about the sequence number for a destination.

• Expiration of path or path breaks.

When a node receives an AODV control message, either to create or to update a route for a particular destination, it searches its routing table for an entry to the destination. If there is no route entry, it creates a new one with the sequence number contained in the control packet, or else the sequence number is set invalid. Otherwise, the node compares the existing entry with the new information and updates it if either

• The new sequence number is higher than in the routing table entry.

• The sequence numbers are equal and the new hop count plus one is smaller than in the existing route.

• The sequence number is unknown.

Besides the destination sequence numbers, the routing entry for each valid route contains a precursor list. This list contains all precursor of the node which is able to forward packets on this route. All neighboring nodes to which a RREP was generated or forwarded are included in this list. In the event of a next hop link breakage, notifications are sent to those nodes.

• *Route Request Message RREQ:*

Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

• *Route Reply Message RREP:*

A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

• *Route Error Message RERR:*

Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, Route error (RERR) message is generated by the node in order to notify other nodes that the link is down.

B] Route Discovery in AODV: When a node "N1" wants to initiate transmission with another node "N7", it will generate a route request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forward to the neighbors, and those node forward the control message to their neighbors' nodes. This process of

goes on until it finds a node that has a fresh enough route to the destination or destination node is located. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "N1" and destination node "N7". Once the route is establish node "N1" and "N7" can communicate with each other. The following diagram show exchange of control messages between source node and destination node.

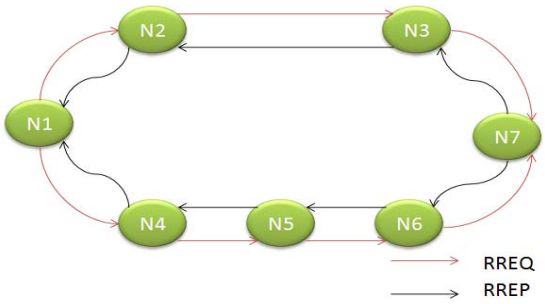

Fig 2: Route Discovery in AODV

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating destination node to the neighbor's nodes, the link is broken between "N5" and "N6", so a route error RERR message is generated at node "N6" and transmitted to the source node informing the source node a route error.

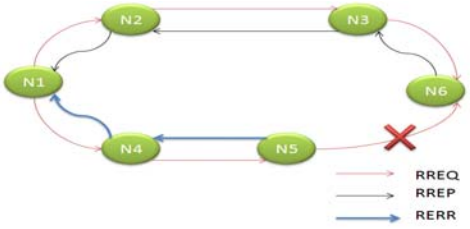

Fig 3: Route Error Message in AODV

IV. ATTACKS ON ADHOC NETWORK

A] Gray Hole Attack:

Every node maintain a routing table that stores the next hop node information for a route a packet to destination node ,When a source node want to route a packet to the destination node , it uses a specific route if such a route is available in it's routing table.otherwise , nodes initiates a route discovery process by broadcasting *Route Request* (RREQ) message to it's neighbours. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node.A *Route Reply* (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination.We now describe the gray hole attack[10] on MANET'S .The gray hole attack has two phases , In first phase, a mallicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intension of interupting or corrupting packets, event though route is spurious.In second phase ,nodes drops the interupted packets with a certation probability.detection of gray hole is difficult process. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack [14].

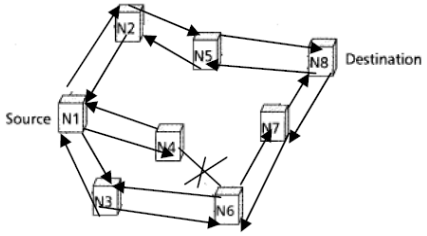

Fig 4: Basic Idea about the Gray hole attack in MANET

B] Black Hole Attack:

In this type of attack, a malicious node falsely advertises good path (e.g., shortest path or most stable path) to the destination node during the path finding process. The intension of the malicious nodes could be to hinder the path finding process or to interrupt all the data packets being sent to the concerned destination node. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [15]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [16]

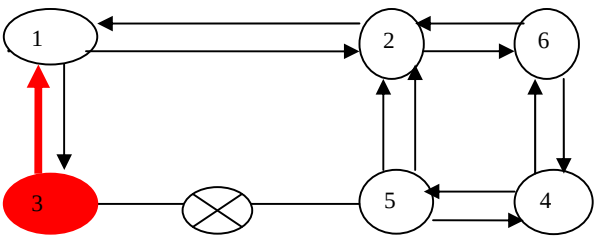

Fig 5: Basic Idea about the Black Hole Attack Problem

The method how malicious node fits in the data routes varies. Fig. 5 shows how black hole problem arises, here node "1" want to send data packets to node "3" and initiate the route discovery process. So if node "3" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "1" before any other node. In this way node "1" will think that this is the active route and thus active route discovery is complete. Node "1" will ignore all other replies and will start seeding data packets to node "3". In this way all the data packet will be lost consumed or lost.

V.SECURITY THREATS IN THE NETWORK

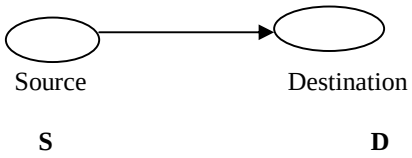

Fig 6: *Normal flow*

• *Interuption: An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability.*

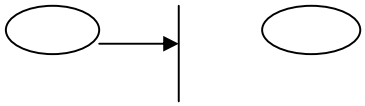

Fig 7: Interruption

• *Interception: An unauthorized party gains access to an asset.This is an attack on confidentiality.unauthorised party may be a person, a program or a computer.*

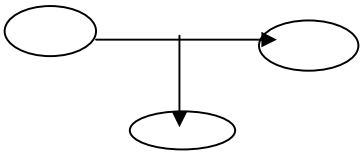

Fig 8: Interception

• *Modification: An unauthorized party not only gains access but tampers with an asset.This is an attack on integrity.Eg.changing values in data file.*

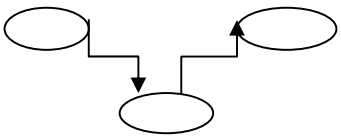

Fig 9: Modification

• *Fabrication: An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity.*

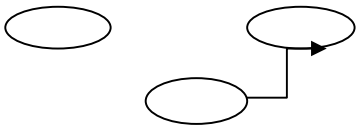

Fig 10: *Fabrication*

VI.PROPOSED MECHANISM

We consider a MANET consisting of similar types of nodes. Each node may freely roam, or remain stationary in a location for an arbitrary period of time. In addition, each node may join or leave the network, or fail at any time. The nodes perform peer-to-peer communication over shared, bandwidth constrained, error-prone, and multi-hop wireless channel. For the purpose of differentiation, we assume that each node has a unique nonzero ID. All the links in the network are assumed to be bi-directional. However, unlike most of the current security frameworks for MANETs, the proposed mechanism does not assume promiscuous mode of operation of the wireless interfaces of the nodes. The promiscuous mode may not only incur extra computation overhead and energy consumption in order to process the transit packets, but also it will not be feasible in cases where the nodes are equipped with directional antennas. There may be varying number of gray hole nodes in the network at different points of time and these malicious nodes may cooperate with each other to disrupt the communication in the network. The proposed mechanism involves recognition & eradication technique to identify any malicious gray hole node in the network. Once a node is detected to be really malicious, the scheme has a notification mechanism for sending messages to all the nodes that are not yet suspected to be malicious, so that the malicious node can be isolated and not allowed to use any network resources. The mechanism consists of local anomaly security procedures which are invoked sequentially.

VII. CONCLUSION & FUTURE WORK

Misbehavior of nodes may cause severe damage, even fails whole of the network. In this paper, we have presented the impact of gray hole attack in mobile adhoc network & its consequences. Mobile Ad-hoc networks has been active research based area over the past few years. But the it is vulnerable to various types of attacks. Misbehavior of nodes causes the damage to the nodes & packet also. Gray hole attack cause damage to the network & also it is difficult to detect. Proposed approach can be integrated on the basic of routing protocols such as AODV.To show the effectiveness and result of proposed approach, implementation work on Network Simulator 2 still in progress. Future works will include some mechanism so as to recognize & eradicate the gray hole attack in mobile ad-hoc network.

REFERENCES

[1] K. Snazgiri, B. Dahill, B. Levine, C. Shields, and E.A. Belding-Royer, "*Secure routing protocol for ad hoc networks*," In Proceedings of International Conference on Network Protocols (ICNP), Paris, France, November 2002.

[2] L. Zhou, and Z. Haas, "*Securing ad hoc network*," IEEE Network Magazine, Special issue on network security, Vol. 13, No. 6, November/December 1999, pp. 24-30.

[3] Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA

[4]Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya,John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. *Proceedings of the 6th annual international conference on Mobile Computing and Networking (MOBICOM)*, Boston, Massachusetts, United States, 2000, 255-265.

[6] Oscar F. Gonzalez, Michael Howarth, and George Pavlou, Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks. Center for Communications Systems Research, University of Surrey,Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.

[7] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad-hoc networks," *In Proceedings of the 8th Annual International Conference on Mobile Computing and Networking* (MobiCom 2002), pp. 12-23, ACM Atlanta, GA, September 2002.

[8] P. Papadimitratos, and Z. Haas, "*Secure routing for mobile ad hoc network*s," In Proceedings of SCS Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 2002.

[9] K. Snazgiri, B. Dahill, B. Levine, C. Shields, and E.A. Belding-Royer, "*Secure routing protocol for ad hoc networks*," In Proceedings of International Conference on Network Protocols (ICNP), Paris, France, November 2002.

[10] L. Zhou, and Z. Haas, "*Securing ad hoc network*," IEEE Network Magazine, Special issue on network security, Vol. 13, No. 6, November/December 1999, pp. 24-30.

[11] L. Buttyan, and J. Hubaux, "*Enforcing cooperation in self organizing mobile as hoc networks*," In Proceedings of IEEE/ACM Workshop on Mobile Ads Hoc Networks, Technical report DSC/2001/046, EPFL-DIICA, August 2002.

[12]Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema,and Attique Ahmed, "*Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks,"* in 2008. International Seminar on Future Information Technology and Management Engineering, November 2008, pp. 568-572.

[13] S. Usha, S. Radha, *"Co-operative Approach to Detect Misbehaving Nodes in MANET Using Multi-hop Acknowledgement Scheme," i*n 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, December 2009, pp.576-578.

[14] Zhu, C. Lee, M.J.Saadawi, T., "*RTT-Based Optimal Waiting time for Best Route Selection in Ad hoc Routing Protocols,"* IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.

[15] K. Biswas and Md. Liaqat Ali, "*Security threats in Mobile Ad Hoc Network"*, Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.

[16] G. A. Pegueno and J. R. Rivera, "*Extension to MAC 802.11 for performance Improvement in MANET"*, Karlstads University, Sweden, December 2006.