BIOINFO Security Informatics
ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 2, 2012, pp.-37-40.
Available online at http://www.bioinfo.in/contents.php?id=344

A NEW WAY TO FIND OUT SUSPECTED NODE AS WELL AS REDUCE THE IMPACT OF GRAY HOLE ATTACK IN ADHOC NETWORK

LOKHANDE P.M.[1] AND THAKARE A.P.[2]

[1]M.E-C.S.E., Sipna's COET, Amravati, MS, India.
[2]Dept. of Electronics & Telecom, Sipna's COET, Amravati, MS, India.
*Corresponding Author: Email- priyanka.20it@gmail.com, apthakare40@rediffmail.com

Received: March 15, 2012; Accepted: April 12, 2012

Abstract- In this paper, we develop a methodology so as to find out the suspected node in the adhoc network & also focus on the packet loss attack in adhoc network. The main goal of this presented work is to implement the method using which we will try to improve the performance of the adhoc network. Mobile ad hoc networks are highly susceptible to routing attacks because of their dynamic topology and lack of any infrastructure. A gray hole is a node that selectively drops and forwards data packets after it advertises itself as having the shortest path to the destination node in response to a route request message from a source node. We devise an efficient method to detect and avoid gray hole attacks as well as suspected node in the adhoc network using AODV protocol. Simulation will be carried out in ns-2.

Keywords- Adhoc network, ns-2, AODV, gray hole, Routing.

Citation: Lokhande P.M. and Thakare A.P. (2012) A new way to find out suspected node as well as reduce the impact of gray hole attack in Adhoc network. BIOINFO Security Informatics, ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 2, pp.-37-40.

Introduction

A mobile ad-hoc network (MANET) is a network [1, 2, 3] formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. These attacks can be classified into two categories, attacks on Internet connectivity and attacks on mobile ad hoc networks. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. Each node in MANET acts a router that forwards data packets to other nodes. Therefore, selection of effective, suitable, adaptive and robust routing protocol is of utmost importance. There are three types of routing protocols: Proactive Protocols, Reactive Protocols and Hybrid Protocols. Proactive protocols are table-driven that constantly update lists of destinations and routes. Reactive protocols respond on demand. Hybrid protocols combine the features of reactive and proactive protocols. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In a MANET, the users_ mobile devices are the network, and they must cooperatively provide them functionality usually provided by the network infrastructure (e.g., routers, switches, servers). In a MANET, no infrastructure is required to enable information exchange among users_ mobile devices. We can envisage these devices an evolution of current mobile phones, and emerging PDA_s equipped with wireless interfaces. The only external resource needed for their successful operation is the bandwidth, often the (unlicensed) ISM band. Nearby terminals can communicate directly by exploiting, for example, wireless LAN technologies. Devices that are not directly connected, Communicate by forwarding their traffic via a sequence of intermediate devices. Suspected nodes aim to deliberately disrupt the correct operation of the routing protocol, denying network services if possible. Such nodes can use or modify sensitive routing information. The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations.

The mobile ad hoc network has the following typical features [4]:

- Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

 Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.

 Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Related Work

Secure routing in the Internet has, of course, received increased attention [4]. Nodes operating in promiscuous mode overhear the transmissions of their successors and may verify whether the packet was forwarded to the downstream node and check the integrity of the forwarded packet. Upon detection of a misbehaving node, a report is generated and nodes update the rating of the reported misbehaving node. In this section we mainly focus on the analyzing & defend the system from malicious impact of different attacks on MANET. AODV [5] is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. Gray Hole attack [6], which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replies true Route Reply (RREP) messages to nodes that initiate RREQ message. Gray Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In this section we explore related work on security challenges in MANETS.Banerjee et. al. [7] has also proposed an algorithm for detection & removal of Black/Gray Holes. 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 [8], Papadimitratos and Hass Snazgiri . In this section we mainly focus on the analyzing & defend the system from malicious impact of different attacks on MANET. A detailed section on securing the AODV protocol is given in this publication. The first approach of securing the AODV protocol has been made by Zapata with his SAODV [9]. In a second publication [10] the protocol is presented in greater detail.

Routing protocols in adhoc network

MANET routing protocols can be categorized into 2 classes as: table-driven/proactive and source-initiated (demand-driven)/ reactive. Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they response to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. On demand protocols create routes only when desired by source nodes [11,12]. When a node requires a route to destination, it initiates route discovery process within the network. This process is completed once a route is found or all possible route permutations are examined. Once a route is discovered and established, it is maintained by route maintenance procedure until either destination becomes inaccessible along every path from source or route is no longer desired. The routing protocols are mainly categorized into three categories: Proactive, Reactive & Hybrid. Hybrid protocol uses the features of reactive and proactive protocol. Most of hybrid routing protocols are designed as a hierarchical or layered network framework.

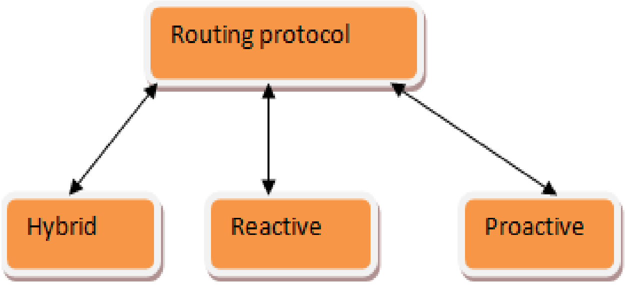

Fig. 1- MANET Protocol

A. AODV Protocol

AODV [13] is an improvement of DSDV algorithm previously described. It is typically minimizes the number of required broadcasts by creating routes on a demand basis, while DSDV algorithm maintain a complete list of routes. The authors of AODV classify it as a pure on demand route acquisition system, since nodes that are not on a selected path do not maintain routing acquisition or participate in routing table exchanges. In AODV, when a source node S wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives later will be ignored by the destination node. AODV is constructed based on DSDV routing. In AODV, each node only records the next hop information in its routing table but maintains it for sustaining a routing path from source to destination node. If the destination node can't be reached from the source node, the route discovery process will be executed immediately. In the route discovery phase, the source node broadcasts the route request (RREQ) packet first. Then all intermediate nodes receive the RREQ packets, but parts of them send the route reply (RREP) packet to the source node if the destination node information is occurred in their routing table. On the other hand, the route maintenance process is started when the network topology has changed or the connection has failed. The source node is informed by a route error (RRER) packet first. Then it utilizes the present routing information to decide a new routing path or restart the route discovery process for updating the information in routing table. It is crucial for AODV to properly handle the sequence numbers.

AODV Characteristics:

- Will find routes only as needed
- Use of Sequence numbers to track accuracy of information
- Only keeps track of next hop for a route instead of the entire route

- Use of periodic HELLO messages to track Neighbors.

The Ad-Hoc On-demand Distance Vector (AODV) routing protocol is one of several published routing protocols for mobile ad- hoc networking. AODV (Ad-hoc On-demand Distance Vector) is a loop -free routing protocol for ad-hoc networks. It is designed to be self-starting in an environment of mobile nodes, withstanding a variety of network behaviors such as node mobility, link failures and packet losses. The optimization of AODV is based on the recent draft of the AODV specification [14].

The essential functionality of AODV includes:

- RREQ and RREP messages (for route discovery)
- RERR messages, HELLO messages, & precursor lists for route maintenance.
- Sequence numbers
- Hop counts
- Expanding ring search

B. DSR

The design idea of DSR is based on source routing. The source routing means that each data packet contains the routing path from source to destination in their headers. Unlike the AODV which only records the next hop information in the routing table, the mobile nodes in DSR maintain their route cache from source to destination node. In terms of the above discussion, the routing path can be determined by source node because the routing information is recorded in the route cache at each node. However,

the performance of DSR decreases with the mobility of network increases, a lower packet delivery ratio within the higher network mobility. .operation of DSR is divided into two functions route discovery, route maintenance. Route discovery operation is used when routes known to known hosts are required. Route maintenance is used to monitor correctness of established route s & to initialize route discovery if a route fails. The Dynamic Source Routing is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration. The DSR protocol allows nodes to dynamically discover a source route across multiple network hops to any destination in the ad hoc network. Each data packet sent then carries in its header the complete, ordered list of nodes through which the packet must pass, allowing packet routing to be trivially loop-free 1and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded. By including this source route in the header of each data packet, other nodes forwarding or overhearing any of these packets may also easily cache this routing information for future use. The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network: Route Discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.

C. DSDV

DSDV is a table driven routing scheme for an ad hoc mobile networks based on the Bellman Ford algorithm [15,16]. The main contribution of this algorithm was to solve the routing loop problem. In DSDV each node maintains a route to every other node in the network and thus routing table is formed. Each entry in the routing table contains sequence numbers which are even if a link is present; else, an odd number is used. The number is generated by the destination, and the emitter needs to send out the next update with this number. DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle.

Gray Hole Attack in adhoc network:

Detection of gray hole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to overload. In AODV protocol 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 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 Gray Hole Attack [6] a malicious node refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray Hole nodes in MANETs are very effective. The simulation results will show that the mechanism is effective and efficient. The gray hole attack ultimately reduced the performance of the adhoc network as well as loss the data packets. Fig.2 having the following features:

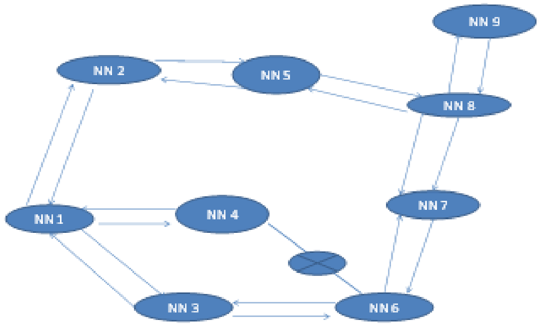

Fig. 2- Gray Hole Attack

NN- stands for node ID,N1-source node,N9-Destination node. In fig 2 we are considering one network having total nine nodes naming as Node NN1 as source node and NN 9 as a destination nodes. Intermediate nodes are the neighbor nodes. It basically follows the Route Request and Route reply message during the propagation request. from the we can clearly identifies then there is break down of link between node NN4 and NN6 ,the cross mark clearly indicate that there is a occurrence of the gray hole attack ,because of which link gets fail and there is a loss of information also. means there is no propagation of information between the NN4 and NN6 nodes it's only because of gray hole attack. Gray hole attack is just act as a role of slow poison in the network because it is not having fixed probability of losing the data. it may loss some percent of data or it may loss your whole data.

Proposed Mechanism

Proposed mechanism is divided into two parts 1] Proposed objectives 2] proposed work

A. **Objectives** of this proposed work are summarized as follow

- Finding the impact of Gray Hole/ packet loss attack in the light of Network load, packet delivery ratio (PDR) and End to End delay (e2e) in MANET.
- Simulating Gray Hole attack using Ad- hoc On Demand Vector (AODV) Routing protocol.
- Comparing the results of AODV protocol before gray hole attack and after Gray Hole attack.
- Proposed new security methodology in AODV protocol as a counter measure of gray hole attack.

B. Proposed work

a. Stage 1: AODV Protocol Implementation

- This module focuses on the implementation aspect of AODV protocol in MANET.

b. Stage 2: Gray Hole Implementation

- In this module, implementation of gray hole attack in MANET & it's consequences is taken into consideration & it is going to be resolved into three phases 1] Route Request 2] Route Reply 3] Route Error message.

c. Stage 3: Security Implementation

- In this module proposed security technique is going to be implemented which is mainly concern about reducing the impact of gray hole attack on adhoc network & improve the performance of the network.

d. Easy way to treat with the Suspected or Doubtful Node

The main intension of the suspected or doubtful node is to create a disturbance in the adhoc network, because of which there is a loss of packets during the transmission in the network due to which there performance metrics parameters of the adhoc network gets degrade. To solve the above problem follow the some steps:

DSN – Destination Sequence Number, NNID – Node ID, DN-ID – Doubtful Node ID. RR- Request Reply Table

Point 1: Start with the initialize process Retrieve the current time then join the current time with waiting time (WT)

Point 2: Store all the Route Replies DSN and NNID in RR-Table Repeat the above process until the time exceeds.

point 3: Finding & & avoidance of doubtful node Access the first entry from RR-Table, If DSN is much greater than SSN then discard entry from RR-Table and store its NID in DN-ID.

Point 4: Node collection, sort the contents of RR-Table entries according to the DSN Select the NID having highest DSN among RR-table entries.

Point 5: Continue Default Process

Access doubtful node finding procedure Default AODV Protocol The above procedure starts from the starting process, first set the waiting time for the source node to receive the RREQ coming from other nodes and then add the current time with the waiting time. Then in storing process, store all the RREQ Destination Sequence Number (DSN) and its Node NNID n RR-Table until the computed time exceeds. Generally the first route reply will be from the suspected or doubtful node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the suspected node, immediately delete that entry from the RR-Table. This is how suspected node is find out. Final process is selecting the NNID that has the higher destination sequence number, is obtained by sorting the RR-Table according to the DSEQ-NO column, whose packet is sent to Suspected node finding in order to continue the default operations of AODV protocol.

Conclusion & Future work

In this paper ,we mainly focus on the effect of gray hole attack on the adhoc network, due to which there is a loss of packets in the during the transmission phase. In this attack there is no fixed probability of losing the data in the network also suspected node tries to disturb the network and also degrade the network performance. Proposed solution will involve a security based technique so as to minimize the effect or remove the gray hole attack from the network as well as secure the network.

References

[1] Snazgiri K., Dahill B., Levine B., Shields C. and Belding-Royer E.A. (2002) *International Conference on Network Protocols*.

[2] Zhou L. and Haas Z. (1999) *IEEE Network Magazine,* 13(6), 24-30.

[3] Hu Y., Perrig A. and Johnson D. (2002) 8*th Annual International Conference on Mobile Computing and Networking* 12-23.

[4] Papadimitratos P. *Secure Routing: Methods for Protecting Routing Infrastructures - A Survey*.

[5] Deng H., Li W. and Agrawal D.P. (2002) *University of Cincinnati IEEE Communication Magazine*.

[6] Vishnu K. and Paul A.J. (2010) *International Journal of Computer Applications*, 1(22), 38-42.

[7] Sukla Banerjee (2008) *World Congress on Engineering and Computer Science*.

[8] Zapata M.G. (2001) *ftp://manet.itd.nrl.navy.mil/pub/manet*.

[9] Zapata M.G. and Asokan N. (2002) *ACM Workshop on Wireless security*, 1-10.

[10] Johnson D. and Maltz D. (1996) *Mobile Computing,* 153-81.

[11] Perkins C. and Royer E. (1999) 2*nd IEEE Mobile Comp. Sys. and Apps*.

[12] Perkins C., Belding-Royer E. and Das S. (2003) *IETF RFC* 3561.

[13] Yang H., Shu J., Meng X. and Lu S. (2006) *IEEE Journal on Selected Areas in Communications*, 24(2), 261-273.

[14] Perkins C.E. and Bhagwat P. (1994) *ACM,* 234-244.