Proposed Theory for Detecting and Recover Gray-hole Attack in AODV based MANET

[1]Mr. Nikhilesh B. Kapdi, [2]Dr. Tejas P. Patalia
[1]M.Tech Scholar, [2]Associate Professor
V.V.P. Engineering College, Rajkot, INDIA
[1]kapdinikhilesh@gmail.com, [2]pataliatejas@rediffmail.com

Abstract— **Security on different layer is most important and essential requirement in MANETs (mobile ad hoc networks). Here we present a proposed theory for detecting and recover gray hole attack in AODV based MANET. Here we consider study of AODV protocol, and gray hole attack of network layer attacks. In MANET at a same time multiple receivers and senders can communicate with each other and the resources are limited, lack of centralized authority and also the network topology is dynamic due to these characteristics MANET is more vulnerable to the different security attacks. Basically the attacks in MANET are active or passive. The Gray-hole attacks are belonging to network layer and belong to active attacks. Active attack can be INTERNAL or EXTERNAL. These type of attacks are attempt to destroy or alter the data being transferred in a network. The attack carried out by the internal node of the network is known as the internal active attack. And the attack carried out by the node which is not belonging to the network is known as external active attacks. So here we give one algorithm for detecting and recover Gray-Hole attack.**

Index Terms— **MANET (Mobile ad hoc network), Routing Protocols, AODV Protocol, Gray-hole attack, Proposed Theory.**

I. Introduction

In MANET (mobile ad hoc network), mobile hosts act as nodes that are communicate with each other in temporary wireless network which has no any centralized administration and any fixed infrastructure. And also MANET is referred as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets of data. Hence, MANETs are suitable for applications in which no infrastructure exists such as military, emergency services, communications with mobility and mining operations. Also the design of network protocols for these networks is a complex issue. There are some major security aspects that need to be addressed for maintain a secure and reliable mobile ad-hoc network environment.

Those are as following

Confidentiality of information

Protection from all unintended entities that expose any type of information. This aspect is very difficult to achieve because in MANET it is very easy for the intermediate node to expose the information as it is use packet routing algorithm.

Verification of user

Authentication of each node is essential otherwise unwanted entity can access the unauthorized node or sensitive information or also can interfering with the operation of other nodes.

Integrity of message

Message is never altered when it is transmitting.

Non-repudiation

Ensures that sending and receiving node can never deny ever while sending or receiving the message.

Availability of service

Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services.

II. Routing Protocols

In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination.

Classification of Routing Protocols in MANET's

Classification of routing protocols in MANET is explained in following figure.

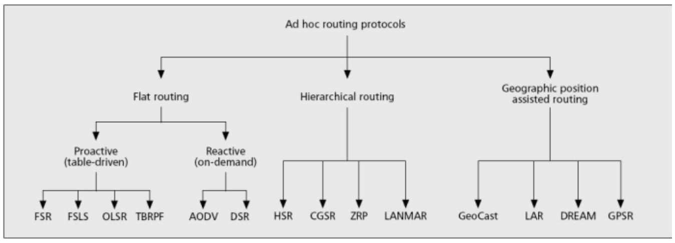

Figure 1 Classification of Routing Protocols

Table-Driven routing protocols (Proactive)

These protocols are also called as proactive protocols since they maintain the routing information even before it is needed. Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. Many of these routing protocols come from the link-state routing. There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth.

On Demand routing protocols (Reactive)

These protocols are also called reactive protocols since they don’t maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network.

III. AODV PROTOCOL

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

Working of AODV

Each mobile host in the network acts as a specialized router and routes are obtained as needed, thus making the network self-starting. Each node in the network maintains a routing table with the routing information entries to it’s neighbouring nodes, and two separate counters: a node sequence number and a broadcast-id.

- source-addr
- source-sequence# -to maintain freshness info about the route to the source.
- dest-addr
- dest-sequence# - specifies how fresh a route to the destination must be before it is accepted by the source.
- hop-cnt

1. Source ’S’ has to send data to destination.
2. S sends RREQ to its neighbours A, B, C.
3. B finds the path in its routing table (with destn seq-number s1 and hop count c1) and sends RREP to S.
4. C sets up reverse path.
5. C forwards RREQ to its neighbours D and E.
6. E sets up reverse path.
7. E forwards RREQ to its neighbours F and G.
8. E deletes the reverse path after a time out period as it does not receive any RREPs from F and G.
9. D finds the path (with dest seq-number s2 which is greater than s1 and hop count c1) in its routing table and sends RREP to C.
10. C receives RREP from D and sets up forward path and forwards RREP to S.

IV. GRAY-HOLE ATTACK

In gray hole attack, a node that is a member of the network, gets RREQ packets and creates a route to destination. After creating route, it drops some of data packets. This kind of dropping against black hole, does not drop all data packets. Attacker drops occasionally packets. It means attacker sometimes acts like a normal node and other times as a malicious node [12].

- A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively.
- There are various denial-of-service attacks. One of them is gray hole attack[7].
- Gray hole attack is an attack in which some selective data packets are dropped by the malicious node.
- Gray hole attack is harder to find because of some data packets reached the destination and destination thinks that it is getting the full data [12].
- In gray hole attack, a node that is a member of the network, gets RREQ packets and creates a route to destination. After creating route, it drops some of data packets.
- This kind of dropping against black hole, does not drop all data packets.
- Attacker drops packets occasionally. It means attacker sometimes acts like a normal node and other times as a malicious node.

The Gray-Hole attack is a kind of Denial of Service (DOS) attacks. In this attack, an adversary first exhibits the same behavior as an honest node during the route discovery process, and then silently drops some of the data packets sent to it for further forwarding even when no congestion occurs. The malicious nodes could degrade the network performance disturb touted discovery process. Following figure describe the gray hole attack.

Gray-Hole attack is the extension of Black-Hole attack but in the case of Black-Hole attack it is easy to detect it but in the case of Gray-Hole attack it is very difficult to detect it because this node only sometimes act as a malicious other it act as an Promiscuous node.

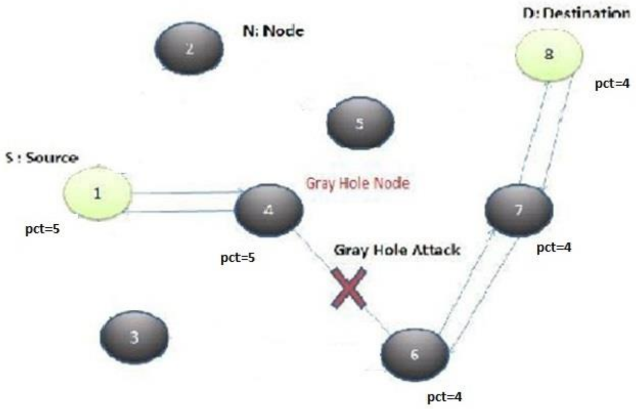

Figure 2 Gray-Hole Attack

V. Proposed Theory

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

Easy Identify algorithm to Prevent Gray and Black hole attack

1. According to the AODV protocol Source node find the destination route path
2. After finding the destination path first source node send the massage which contain the total no. of data packets and add of previous node (pnadd) to the next node.
3. So now every nodes in a route have both
   1. total no. of data packet
   2. add. Of previous of previous node
4. Now source node gives the serial no. to all the data packet and sending the data packets. Every node compare the serial no. of Data packet with sending packet by its previous node.
5. Now if the node detects the misbehavior of its previous node it will send the message to the source node with the identification no. of malicious node.
6. Now source node broad cast the alarm message with the id of affected node to black listed it and then it will again find the destination path.

Advantages - Using this algorithm we can directly catch the node affected by the Gray-Hole attack. To find a malicious node is easy by using this algorithm.
Disadvantages - We can use this algorithm if and only if when the path is established.

VI. CONCUSION

In this survey paper, we try to find the impact of Gray-Hole attack that belong to the network layer on the security system in the mobile adhoc networks, which may be a main disturbance to the operation of it. Due to nature of mobility dynamic structure and open media MANET are much more unsecure to all kind of security risks as covered. As a result, the security needs in the MANET are much higher than those in the traditional wired networks.

Through this algorithm here we try to find Gray-Hole attack in AODV based MANET and also we try to recover it.

REFERENCES

[1] Abhay Kumar Rai, Rajiv RanjanTewari&Saurabh Kant Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication,” International Journal of Computer Science and Security (IJCSS) Volume: 4 Issue: 3.

[2] D. DjeNouri and L. Khelladi, “ A Survey of Security Issues In Mobile Ad Hoc And Sensor Networks”, IEEE Communications surveys and Tutorials, Fourth Quarter 2005, vol. 7, no. 4., pp. 2-28.

[3] D.B. Johnson, D.A. Maltz, Y.C. Hu, and J.G. Jetcheva,Dynamic Source Routing in Ad Hoc Wireless Networks,Mobile Computing, Kluwer Academic Publishers, Vol. 5,pp. 153-181, 1996.

[4] Krishna Gorantala “Routing Protocols in Mobile Ad-hoc Networks” June 15, 2006 Ume°a University Department of Computing Science SE-901 87 UME°A SWEDEN

[5] K. Elissa, “Title of paper if known,” unpublished. Krishna Gorantala “Routing Protocols in Mobile Ad-hoc Networks” June 15, 2006 Ume°a University Department of Computing Science SE-901 87 UME°A SWEDEN

[6] Biswas, K., and Liakat Ali, M. D. 2007 Security Threats in Mobile Ad Hoc Network. Master Thesis. Thesis no: MCS-2007:07., Blekinge Institute of Technology.

[7] Ullah, I., and Rehman, S. U. 2010 Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols. Master Thesis. Thesis no: MEE-2010-2698., Blekinge Institute of Technology.

[8] Jain, S., Jain, M., and Kandwal H. 2010. Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. J. Computer Applications, Vol. 1, No. 7, 37-42.

[9] Yanbin Yang and Hongbin Chen “An Improved AODV Routing Protocol for MANETs”

[10] Ashok Desai , Prof. Purvi ramanuj “Agent-based Mechanism for Gray-Hole Detection in MANET” in International Journal of Innovative Research & Studies.

[11] Marjan Kuchaki Rafsanjani, Zahra Zahed Anvari, Shahla Ghasemi “ Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET” IJCA Special Issue on “Network Security and Cryptography” NSC, 2011

[12] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala” A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks” 2012 Second International Conference on Advanced Computing & Communication Technologies