INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

DETECTION AND PREVENTION MECHANISM FOR GREY AND BLACK HOLE ATTACK IN A MOBILE AD-HOC NETWORK

MISS SNEHAL V. RAUT[1], ANKIT R. MUNE[2], DR. H. R. DESHMUKH[3],

1. M E. Scholar, Department of Computer Science, IBSS COE Amravati , India.
2. Assistant Professor, Department of Computer Science, IBSS COE Amravati, India.
3. Professor& HOD, Department of Computer Science, IBSS COE Amravati, India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Now-a-days Mobile Ad-hoc Network (MANET) are becoming famous in different areas like military applications, environment application etc. MANET is a virtual network which makes connection virtually or wirelessly in network and that connection is made with network nodes or hops. In MANET nodes are movable. As a result, many attacks occur by attacker on virtual MANET. Grey & Black hole attack is an ancient attack of MANET, which held on routing layer & brings major effect on network. Therefore, we are going to study about Black hole & Grey hole attack or selective forwarding attack. A different technique to prevent and detect these attacks describe in the paper. We conclude plan for future work.

Keywords: A Mobile Ad-hoc Network, Grey hole, Black hole, Network layer.

Corresponding Author: MISS SNEHAL V. RAUT

Access Online On:

www.ijpret.com

How to Cite This Article:

Snehal V. Raut, IJPRET, 2015; Volume 3 (9): 456-462

PAPER-QR CODE

INTRODUCTION

Due to increasing complexity of the Internet itself, the operation of a computer network is a challenging task, especially if the network is connected to or part of the Internet, which is characterized by the interconnection of lots of different devices, domains and controlled by separate network management authorities. Existing internet protocols are weaker with security issues against the network infrastructure that cause serious problems. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. As a consequence, there must be proper systems that need to monitor and supervise their network permanently to guarantee proper functioning and detect and mitigate network problems. The ultimate goal for a Mobile Ad-hoc Network is to provide security solutions.

A Mobile Ad-hoc Network is highly susceptible to various attacks. Two of the major routing attacks are black hole and gray hole attacks. These attacks can be classified into two categories, attacks on Internet connectivity and attacks on mobile ad hoc networks. They can also drop the packets partially or fully to perform various attacks; black hole, grey hole, wormhole etc. Also, many other routing layer attacks are possible despite of many cryptographic security mechanisms. To achieve such type of attacks attacker may physically acquire the router to make it drop packets. Attacker may simply hijack the mesh node in the Mobile Ad-hoc Network to launch a selective forwarding attack.

In this paper, we focus on the detection and prevention of black hole attack or selective forwarding attack. A different technique to prevent and detect these attacks describe in the paper. We conclude plan for future work.

REVIEW OF LITERATURE

Jain, Jain & Kandwal (2010) propose an algorithm to detect a chain of cooperative malicious node in ad-hoc network that disrupts transmission of data by feeding wrong routing information along with the detection algorithm. **Chandure, Bakshi, Tidke & Lokhande** (2012) address the problem of detection & prevention of gray hole attack in mobile ad-hoc network. **Shanhanmuganathan & Anand** (2012) surveyed about the different types of attacks occurred in the network layer in MANET. **Karlof** (2014) first proposed selective forwarding attack and suggested a multipath forwarding approach to detect it. **Singh, Singh & Rashmi Singh** (2014) presents a review of different security mechanism to eliminate the black hole / gray hole attack from the network. **Wahane & Kanthe** (2014) suggests the modification of Ad Hoc on Demand Distance Vector Routing Protocol. **Kaur & Singh** (2014) deals with the study of analysis of delay

occurs by these attack in Wireless Mesh networks and its types and also study various techniques to detect and prevent network from black hole and grey hole attack.

A Mobile Ad-hoc Network (MANET)

MANET can be defined as collection of mobile nodes. It is an infrastructure less network. The mobile nodes in the network dynamically setup paths among themselves to transmit packets from the source to destination and it is a self-configuring network.

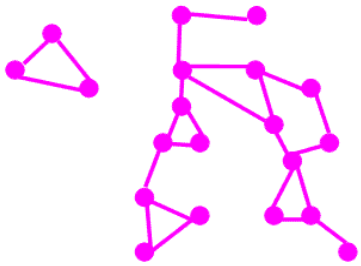

Figure 1: Basic Idea about the MANET Structure [9]

The MANET security can be classified in to 5 layers, as Application layer, Transport layer, Network layer, Link layer, and Physical layer. However, the focus is on the network layer, which considers mainly the security issues to protect the ad hoc routing and forwarding protocols. [9]

Gray hole attack

Gray hole attack is one of the attack in network layer which comes under security attacks. The nature of MANET is a dynamically changing process, due to its dynamically changing process its vulnerable for wide range of attack.

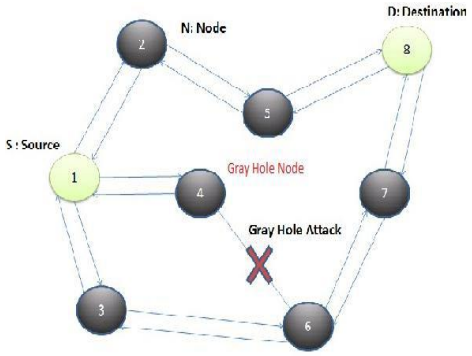

Figure 2: Example of Gray Hole Attack [11]

Black hole attack

In a black hole attack, the malicious node (referred to as black hole) replies to every routing request saying that it has a route to the given destination. . So, unsuspecting nodes start sending data to the destination through the black hole. This way a black hole diverts most of the traffic in the network to itself, and later dumps it. A gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later. This anomalous behavior of malicious nodes prevents a trust based security solution from detecting them.

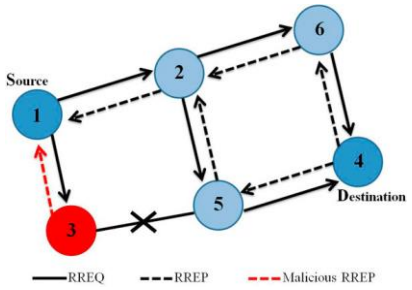

Figure-3 The single black hole problem.

Figure- 3 is an example of single black hole attack in the mobile ad hoc networks.[1] Node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes afalse response that it has the quickest route to the destination node. Therefore node 1 erroneously judges

the route discovery process with completion, and starts to send data packets to node 3. In the mobile ad-hoc networks, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily and the network operation is suffered from this problem.[1]

Network layer attack

In Ad-hoc networks routing mechanism has three layers namely Network, Physical and MAC layers play a vital role. MANETs are more vulnerable to various attacks; all these three layers suffer from different attacks and it cause routing disorders. The different kind of attacks in the network layer varied such as selective forwarding attack and modifying some parameters of routing messages. [9]

Routing outing attack

There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. Various attacks on the routing protocol are described briefly below:

• Routing Table Overflow: In this attack, the attacker tempts to create routes to nonexistent nodes.

•Routing Table Poisoning: The Compromised nodes in the network send fictitious routing updates packets sent to other uncompromised nodes.

• Packet Replication: In this attack, an adversary node replicates stale packets.

• Route Cache Poisoning: Each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past.

• Rushing Attack: On demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. [9]

Prevention and detection techniques for black hole/grey hole attack

A various method has been proposed to detect and prevent black hole/ gray hole attacks. They are as follows. [15]

1. Detecting packet forwarding misbehavior, this works on the principle of flow conservation in a network. Every node of the network uninterruptedly checks their neighboring nodes and bring up-to-date the list of that nodes which they have overheard freshly. In this algorithm it does not need various nodes to overhear each other's received and transmitted packets. This method may lead to false allegations alongside correctly behaving nodes.

2. The DRI (Data Routing Information) method which has the track of past routing experience among moving nodes (router) in the network and verifying of RREP messages from intermediate nodes by start nodes to ascertain the cooperative black hole nodes, and exploit the improved AODV routing protocol to accomplish this approach.

3. The dynamic learning method is to discover the black hole node. In this approach, the normal nodes state views are updated periodically to adapt to the frequent network changes and clustering-based technique is adopted to identify nodes that deviate from the normal state. It is required to observe if the characteristic change of a node exceeds the threshold within a period of time. If yes, this node is judged as a black hole node, otherwise, the data of the latest observation is added into dataset for dynamic updating purposes. However, it does not involve

a detection mode, such as revising the AODV protocol or deploying IDS nodes, thus, it does not isolate black hole nodes.

Learning process is enlisting the entire malicious node locally at each node whenever they behave as a source node. After receiving this message the backbone node arbitrarily carries out the normal functioning by transferring the data pick out form one of the free IP addresses. By receiving the allotted IP address the new node directs an acknowledgement to the backbone node. Now from the time when the allocation is only under the control of the backbone nodes then the dynamic pool of unused/restricted IP address of the network at any point of time is known only to the backbone node.

Conclusion

Misbehavior of nodes causes the damage to the nodes & packet and the whole network has been attacked in the network layer. Security is the most important feature for deployment in MANET. We have seen the number of attacks happened in network layer and especially for gray hole attack. MANET proves to different limitations and weakness due to its dynamic nature. Therefore we have to use a new technique to overcome this problem. Our aim is to detect and mitigate the false node which is acting as a normal node, which is very hard to find out. But if we design a new approach of detecting the attacker node we can ensure that there is a safety in the network [9]. Once security is lost in the network then the entire network will get failed. Gray hole attack ultimately decrease the concert of the network. The main goal of the gay hole attack should be the improvement of security and as well as the performance of the network.

Future work

Many Problems in ad-hoc network remain to be investigated. New Method should be introduced for detecting & preventing from the gray hole attack or behavior of malicious node because of the different attacks on the ad-hoc network. The performance of the network gets decreases. Future work will involved some new additional features or parameters using which there is a much more increment in the performance metrics of the network as well as try to avoid the different attacks which occur on the network with the use of different routing protocols available in MANET. As future work, we intend to develop simulations to analyze the performance of the proposed solution and mainly concentrate on one thing that there is a minimum amount of packets loss during the transmission.

REFERENCES:

1. Tseng, 'Human-centric Computing and Information Sciences; http://www.hcis-journal.com/content/1/1/4 , 2011

2. Suhasini 'International Journal of Advance Research in Computer Science and Management Studies' Volume 2, Issue 5, May 2014 pg. 299-306

3. Jaspreet, 'International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 9, September 2014 pg. 142.

4. International Journal of Computer Applications (0975 – 8887) Volume 95– No.23, June 2014

5. International Journal of Advances in Engineering & Technology, Nov. 2012. 68 Vol. 5, Issue 1, pp. 67-76

6. American Journal of Engineering Research (AJER) 2014 w w w . a j e r . o r g Page 42

7. Vandna Dahiya, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.7, July- 2014, pg. 466-473

8. The International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.6, December 2014

9. V. SHANMUGANATHAN & T.ANAND International Journal of Computer Networks and Wireless Communications Vol.2, No6, December 2012 pg 647

10. International Journal of Computer Networks and Wireless Communications Vol.2, No6, December 2012

11. Chandure, Bakshi, Tidke, Lokhande, International Journal of Advances in Engineering & Technology, Nov. 2012. 67 Vol. 5, Issue 1, pp. 67-76

12. IOSR Journal of Computer Science, PP 59-67 www.iosrjournals.org

13. International Conference on Advances in Engineering & Technology – 2014

14. Gayatri Wahane & Prof. Ashok Kanthe, 'The International Journal of Multimedia & Its Applications' Vol.6, No.6, December 2014

15. Rupinder Kaur and Parminder Singh, International Journal of Computer Applications, Volume 1 – No. 737.