Methodology for Detecting and Thwarting DoS in MANET

Kanchan
M.Tech,Student
MMU, Mullana

Sanjeev Rana
Associate Professor
MMU, Mullana

ABSTRACT
An ad hoc network is the assortment of cooperative wireless nodes without existence of any access point or infrastructure. The presence of malicious nodes in an ad hoc network deteriorates the network performance. A novel approach for malicious nodes detection is proposed here to protect against DoS attack in ad hoc on-demand distance vector routing protocol. The proposed approach employs a method for determining conditions under which malicious node should be monitored. Apart from identification of malicious node, it has been observed that this approach leads to less conservation and less communication breakage in ad hoc routing. The experimental results demonstrate that the proposed approach can effectively detect malicious nodes.

Keywords
MANET, AODV routing protocol, Denial of Service.

1. INTRODUCTION
An ad-hoc network is a collection of mobile nodes that are capable of forming a network without any fixed infrastructure. Multi hop routing is used when the nodes are not in each other's radio range. Moreover, each host acts as router. Nodes have unrestricted mobility and connectivity that causes frequently changes in network topology. Ad-hoc network is useful in situations where geographical or terrestrial constraints demand totally distributed network system without any fixed base station, such situations could be in battle fields or in any other disaster situations. Due to such characteristics, the wireless ad hoc networks are highly susceptible to various malicious attacks.
In ad hoc network, there exists a variety of attacks [3, 4] which are classified into two types: (i) passive attacks and (ii) active attacks. In passive attacks, data are exchanged in the network without any modification, whereas in active attack data are modified or altered. Internal attacks can change normal functionality of a node by updating its information. Eavesdropping, traffic analysis, monitoring are some of the examples of passive attacks, whereas blackhole attacks, neighbour attacks, sequence number attacks [5], DoS [6, 7] and so on are examples of active attacks. Literature review suggests that ad hoc routing is seriously affected because of malicious node and has a detrimental effect on network performance and reliability [8].

We discuss about a method that offers detection and prevention of Denial of Service (DoS) attack which is caused due to misbehavior of the malicious node in the routing activity of the ad-hoc network and the network fails to provide the services. So a security mechanism is required to detect the misbehaving nodes and isolate the network from the attack caused by the malicious node. [3]

2. DENIAL OF SERVICE ATTACK
An attacker attempts to prevent legitimate and authorized users from the services offered by the network. A denial of service (DoS) attack can be carried out in many ways. The classic way is to flood packets to any centralized resource present in the network so that the resource is no longer available to nodes in the network, as a result of which the network no longer operating in the manner it was designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. DoS attacks can be launched against any layer in the network protocol stack. On the physical and MAC layers, an adversary could employ jamming signals which disrupt the on-going transmissions on the wireless channel. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. For example, an adversary node could participate in a session but simply drop a certain number of packets, which may lead to degradation in the quality of service being offered by the network. On the higher layers, an adversary could bring down critical services such as the key management service.

3. MOTIVATION
Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

3.1 Aims and Objectives
- The study focus on analysis of Denial of Service attack in MANET and its consequences.
- Simulating the Denial of Service attack using Ad-hoc on-demand distance vector (Reactive) routing protocols.
- Isolate the network from Denial of Service attack.

4. RELATED WORK

Security is an important issue in the integrated MANET-Internet environment we have to consider the attacks on internet connectivity and also on the ad hoc routing protocols like Destination sequenced distance vector, Dynamic source routing, Temporary ordered routing algorithm and ad hoc demand distance vector.[1][2]

Sonali Bhargava and Dharma P. Agrawal, identify certain misbehaviors caused by malicious node and also proposed Intrusion Detection and prevention model to prevent several identified attacks.[3]

Ping, Zhoulin, Yiping, Shiyong present a new DoS attack called ad hoc flooding attacks and prevent this attack by FAP (Flooding attack Prevention) with little overhead.[4]

Gao Xiaopeng, chen Wei, discusses the Gray hole attack, type of DoS attack and use aggregate signature algorithm to trace packet dropping node that cause Gray Hole attack.[5]

Sidra Izza, M Hasan, presented a distributed dynamically configurable Firewall architecture that uses the3 ingress and aggress filtering to resist the DoS.[6]

Ahsan and Debashish, present a series of architectural changes aimed at preventing most flooding DoS attacks and making the other attacks easier to defend.[7]

5. ASSUMPTION AND BACKGROUND

In this section we outline the assumptions we make regarding the properties of ad-hoc networks. Furthermore, we give the brief description of AODV, the routing protocol.

5.1 Assumption

- When a node is within radio range of another node they are termed as neighbors.
- Every node of the network is not a malicious node.
- There should be more number of genuine node as compared to malicious node

5.2 Overview of Routing Protocol [10]

AODV [1, 9] is a well-known on-demand routing for MANETs. It is an enhancement of proactive routing protocol destination-sequenced distance vector [10]. It reduces the number of broadcasts by creating on-demand routes as opposed to proactive routing protocols. It maintains two procedures (i) route discovery and (ii) route maintenance, which are briefly discussed in the following sections.

(i) Route Discovery

In this process, AODV entails flooding of route request (RREQ) packets generated by source node. These packets contain address of destination and are broadcasted by intermediate nodes. To find a path to the destination, source node broadcasts an RREQ packet. The neighbours in turn broadcast packets to their neighbours till it reaches an intermediate node or destination. Information of RREQ packet is forwarded by intermediate nodes which can be changed or modified on the basis of hop-by-hop procedure. This forwarded information is circulated by an intermediate node. Such node keeps this record in the routing table. In AODV, modified information is maintained by hop count, which is incremented by 1(HC+ ¼ 1) at every hop that forwards RREQ. These RREQ packets hold sequence number to ensure that selected route is loop free, and it also ensures that intermediate node should reply only latest information (not duplicated/old information). A node discards packet, if it has been received already. This information is used to construct route reverse path for the route reply packet. As the route reply packet traverses back to the source, then intermediate nodes store this forwarded information into their tables.

(ii) Route Maintenance

In this process, if source node or intermediate node realizes link failure, then it sends link failure notification to its upstream neighbours. So, source can reinitiate route discovery if needed.

6. PROPOSED APPROACH

Proposed work introduces a solution to identify malicious node in MANETs using AODV. This scheme keeps record of all nodes present in the network. After detection of malicious node, it is isolated from network. The following algorithm describes the methodology for detection and prevention from denial of service attack in AODV routing protocol.

1. Set a thresh hold value for Packet Drops
2. Monitor the Sequence Numbers
3. Count the Packet Drops
4. If Packet Drops > thresh hold value then
    - Raise Alarm
    - Delete the routes of the nodes on the basis of packet dropped by them
5. Maintain a log file to prove that identified nodes are responsible for maximum packet drops, hence removed.

6.1 Detection

We are using aodv routing protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network. Before transmission neighbor discovery procedure will run. After discovery TCP connection is established between the mobile nodes. As the connection is established, TCP session is automatically created. By using flow monitor procedure we are monitoring the flow of each node. If the packet reached to the malicious node, it will drop the packet and the sequence number of the packet is disturbed. By monitoring the sequence number it will be detected that somebody is misbehaving with the network. Now, we will check the data sent and received by each and every node in the network. If the data drop value is greater than the threshold value than that node is detected as misbehaving node or malicious node of the network. The various steps followed to prevent the network from DoS attack are:

- TCP connection is established between two mobile nodes to send the data.

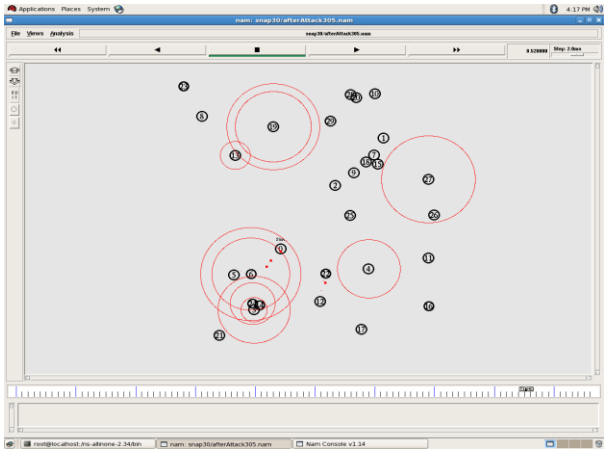
- As the connection is established, a TCP session is automatically created.
- In this TCP session flow of each node is monitored using flowmoniter procedure.
- If the packet drop value of the node is greater than the threshold value implies that the particular node is responsible for DoS in the network.

6.2 Prevention

- First of all, detect the malicious node by using detection scheme described in the above section.
- Then the detected malicious node is deleted from the routing table.

7. SIMULATION SCENARIO AND RESULTS

We did the simulation using NS-2.34 network simulator with 30 nodes including 5 malicious nodes.



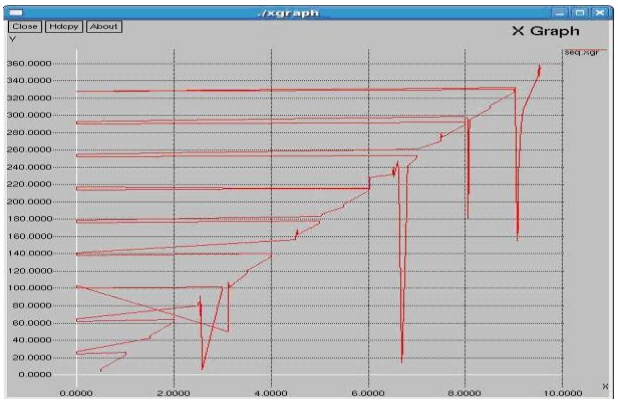
Simulation Time	10 minutes
Traffic Type	CBR@0.5
Protocol Used	TCP
Adhoc Routing Protocol	AODV
Total Number of Nodes	30
Malicious Node	5
Total Mobile Nodes	30
Pause time	0.5ms

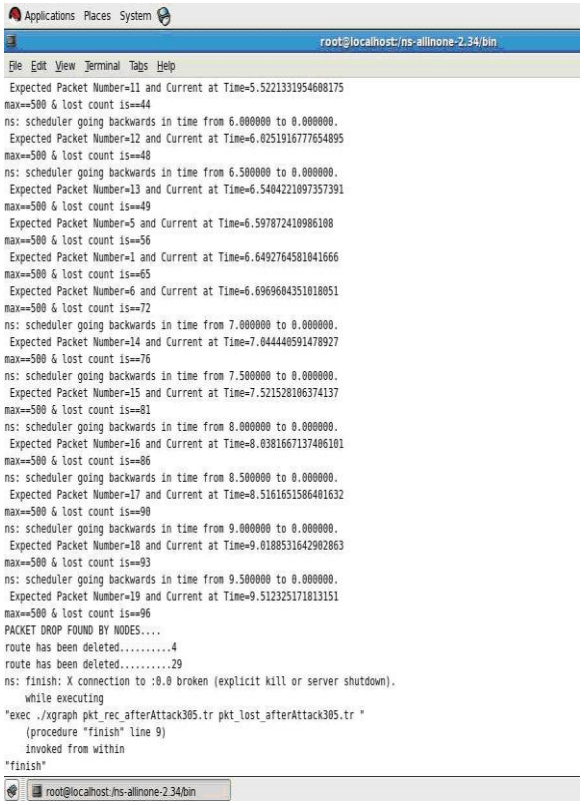
7.1 Detection on the basis of Sequence Number

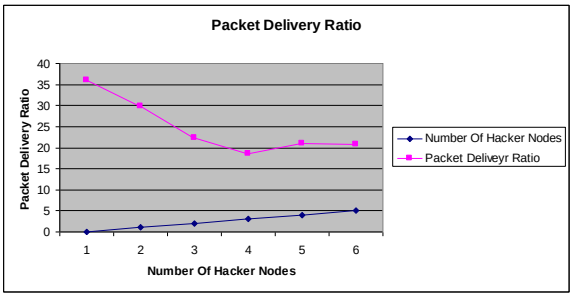
For the detection process, the sequence number of the packets is monitored. If the expected sequence number is not in continuation, that implies may be some malicious activity is running that should be stopped for smooth functioning of network. The graph below shows the change in expected sequence number. If there is any packet drop, it will cause change in the sequence number.

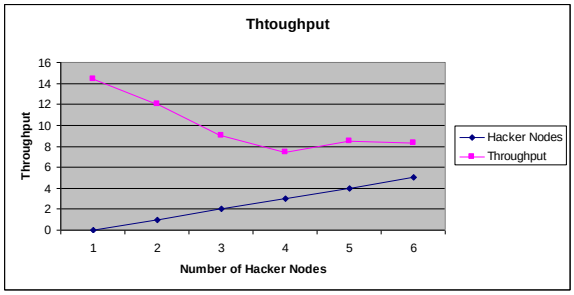
7.2 Malicious Nodes Deleted on the basis of Threshold Value

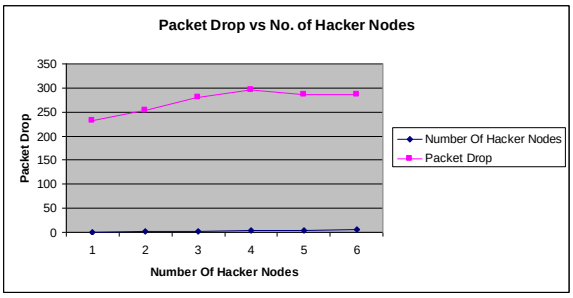
After detection, the flow of packets is monitored, if the packet drop is more than the threshold value. An alarm is raised and the node is deleted from the route on the basis of packet dropped by them.

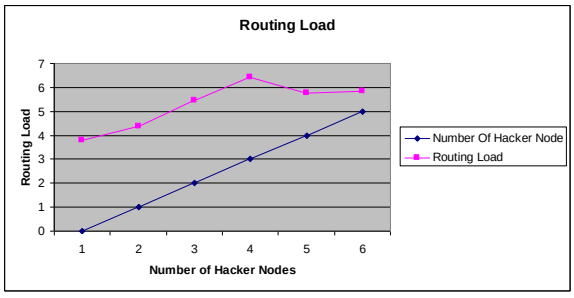












8. CONCLUSION

Simulation results show that presence of malicious nodes affect the performance of network but when our purposed method detects and removes them from network, network reaches to a stable state. Number of packet drops increases proportionally with the number of malicious nodes. As the packet drop increases, it also affects the packet delivery ratio, routing load and throughput etc. Packet flow is monitored and when packet drops increases, it causes a frequent change in sequence number and when it crosses a threshold limit, then alarm is raised and finally malicious nodes are removed from network on the basis of losses caused by them. After the detection and removal of malicious nodes, we can observe that network comes to a stable state. We also maintained a log file to prove that the identified nodes are the malicious nodes, that's why they are removed from network. So we can say that our purposed method is simple and effective which can secure the network with minimal cost.

9. FUTURE SCOPE

The focus is on finding a sustainable relationship between the total number of nodes in the network, the number of malicious nodes that can be tolerated and the number of friends per node needed to achieve that and also analyze the scalability, cost/benefit ratio, throughput and overhead for achieving security

10. REFERENCES

[1] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah, MANET routing pretocols and Warm hole attack against AODV, IJCSNS,VOL.10 No.4,April 2010.

[2] Abhay kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhya, Different types of attack on integrated MANET –Internet Communication.

[3] Sonali Bhargava and Dharma P. Agrawal, 2001.IEEE Std 0-7083-7005-8,Security enhancement in AODV protocols for wireless Ad-hoc networks.

[4] Gao Xiaopeng, Chen Wei, A Novel Gray Hole Attack detection Scheme for Mobile Ad-hoc Networks, IFIP International Conference on Network and Parallel Computing, 2007.

[5] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhong, Resisting Flooding attacks in Adhoc Networks, IEEE, International Conference on Information Technology: Coding and Computting(ITCC'05).

[6] Sidra Akram, Izza Zubair, M Hasan Islam IEEE Std 978-1-4244-4615-5, Fully distributed dynamically configurable firewall to resist DoS attacks in Manet, 2009.

[7] Ahsan Habib, Debashish Roy, Steps to Defend against DoS attacks, ICCIT 2009, Dec 2009.

[8] M. G. Zapata and N. Asokan, " Secure Ad hoc Routing Protocols," in Proceeding of the ACM Workshop on Wireless Security, Atlanta, GA September, 2002.

[9] Y. C. Hu, A. Perrig, and D. B. Johnson, " Ariadne: A Secure On Demand Routing Protocol for Ad hoc Network," in Proceeding of 8th ACM Int'l, Conf. on Mobile Comp, Georgia, September 2003.

[10] Georgy Sklyarenko,"AODV Routing Protocol," in [MatrNr : 3935701]*.

[11] Sonja Buchegger, Jean-Yves Le Boudec, Nodes bearing Grudges: Towards routing security, Fairness and Robustness in mobile Ad hoc networks.

[12] Geng Peng and ZouChuanyun,Routing attacks and solutions in Mobile Ad-hoc Network.