A Survey of Different Attacks on MANET Emphasizing at Network Layer

Mahima Trivedi, Er. Pawan Patidar, Dr. M. K. Rawat

Abstract— Mobile Adhoc Network is one of the hottest topics of the research these days. To accomplish a secure MANET is a major concern. An ad hoc infrastructure of MANET presents new challenges in this field. A Mobile ad hoc network is said to be less defendable against Denial of Service (DoS) attacks, which can be vigorously commenced by a malicious attacker node. In this manuscript, we are going to review the impact of DoS flooding attack in Manet when the Ad hoc on demand distance vector routing (AODV) works on it as a source routing protocol. We will start from recollecting different security issues of MANET and later the discussion will be flown to the AODV DoS flooding attack.

Keywords: DoS Attack, AODV, Flooding.

1 INTRODUCTION

A Mobile Ad-hoc network is composed of a no. of mobile devices that are able to communicate with each other. Being the Ad-hoc nature, any predefined infrastructure or core administration is absent in these kind of networks. In MANET, nodes and devices are allowed to move in and out of the network. These nodes can be any mobile device such as a laptop, personal digital assistance (PDA), or mobile phone etc. These nodes or devices can act as host as well as a router and can form dynamic and changing topologies. This way, MANET can be called as self organized and self configurable network. In addition to the mobility these networks offer some more charismatic features which make them to be deployed in a wide range of applications. These are: an open medium, dynamic change of topology, absence of a central administration, algorithm deploying cooperation etc. These glittering features of MANET made it more delicate towards security.

Routing in MANETs is one of the most imperative areas of research. Major routing protocols that work in MANETs are: OLSR, AODV [1], DSR etc. AODV is a reactive routing protocol premeditated for these kind of network. DoS attack to which, this protocol is majorly vulnerable is, Flooding. In the upcoming sections, we will discuss them in detail.

2 SECURITY ISSUES IN ADHOC ROUITNG

Security of Mobile ad hoc networks [2] is an important barrier. In Manet routing, exchange of information about network topology is done between nodes, as they are also routers. This can be a bottleneck too because any malicious node can give wrong information about redirection of traffic or to stop it. We can easily conclude that routing protocols on MANET are frail towards security. Let's discuss some problems with adhoc routing protocols [3]:

- *Mahima Trivedi is currently pursuing masters degree program in eComputer science engineering in LNCT, Indore, India. E-mail: trivedimahima.cs@gmail.com*
- *Er. Pawan Patidar is Asst. Prof. in Computer Science Engineering Dept in in LNCT, Indore, India. E-mail: pawan.patidar1@live.com*
- *Dr. M. K. Rawat is Head of the Dept. of Computer Science Engineering Dept in in LNCT, Indore, India. E-mail:drmkrawat@gmail.com*

2.1 Infrastructure of adhoc network

Absence of a fixed infrastructure enables nodes to route packets on their own. Each node in the network depends upon neighbouring nodes to rote their packets.

2.2 Dynamic Topology

Arrangement of nodes in the network is not fixed and can change because of mobility. Adhoc networks contain node that changes their locations frequently. This characteristic of adhoc is a primary cause of problems, especially in the case when multiple networks mix together. It is possible that duplicate IP addresses are present in the network which is not easy to resolve. This issue can make easy occurrence of attacks.

2.3 Wireless Communication

Wireless channels are prone to noise because of poor protection; therefore control message can easily temper. A malicious node can easily affect the traffic by jamming, distorting interrupting or spying the information.

2.4 Implicit Trust Relationship:

All adhoc routing protocol works on the trust basis and assumes each node to be honest. This feature allows malicious node to get entered in the network and affect it, just by providing wrong information.

3. DoS Attacks on different Layers [4]:

3.1 Multilayer Attack:

Those attacks that are likely to subsist in any of the layer of the protocol stack, falls into this category. Denial of service, impersonation is some of major multilayer attacks.

3.1.1 Denial of Service:

In DoS attack, the attacker node tries to thwart victim from the services it offers and make the network or its resources unavailable. The DoS attack can be occurred at any layer in form of Jamming, flood-

ing which will be discussed in further sections.

3.1.2 Impersonation:
Impersonation attack can be a first step to any of the attack. For instance, an attacker, before launching any other attack can first change its IP address or MAC address.

3.1.3 Man-in-the –middle Attack:
In this attack, the attacker parks itself in between sender and receiver and then snuffles the data transmission. In some cases, impersonation is also possible.

3.2 Attacks on the Physical Layer:

3.2.1 Jamming Attack:
It is a DoS attack in which a jammed or interfered signal is launched to cause lost or corrupted messages. If an attacker is having a powerful transmitter, it can generate a strong signal that can overpower the radio signals, which will result in disrupted communication.

3.2.2 Eavesdropping:
Listening and reading of message by any unintended receiver. Maximum wireless networks use the RF spectrum and by nature they broadcast. So it becomes very easy for an intruder to listen and intercept the message by just tuning into an appropriate frequency.

3.3 Attacks on Datalink Layer:

3.3.1 Disruption:
Link layer protocols manage the one hop connectivity among neighbours. Attacker can affect the cooperation of the layer protocols. For instance, MAC protocols have to coordinate the transmission of the nodes on the common transmission medium.

3.3.2 Traffic Analysis:
Traffic analysis can be implemented to launch and plan other attacks. One can monitor and identify communication parties and their functionalities to avail information.

3.4 Attacks on Network Layer:

3.4.1 Flooding Attack:
Flooding attack is a kind of DoS attack, in which the attacker node broadcast the superfluous bogus packet in the network to weaken the availability of resources and thus the throughput gets reduced and a valid user becomes unable to consume the resources\. The flooding attack can take place in almost all secure on demand routing algorithm like AODV, SAODV, ARAN, SRP etc.

3.4.2 RREQ Flooding:
In this attack, the attacker chooses an IP address which is actually absent from the network or may select a random IP address. The attacker here actually does not wait for the round trip time and continues to send the same packet again and again.

3.4.3 Data Flooding:
In the data flooding, the attacker node floods the network by conveying futile data packets. In this, the attacker first creates a path to all nodes and then proceeds further by sending the large amount of useless data packets.

3.4.4 Wormhole Attack:
In wormhole attack, a malicious node captures the packet at one location, and excavates them to another location. This disrupts the routing mechanism of the network.

3.4.5 Blackhole Attack:
It works with two properties. First, it uses certain routing protocol such as AODV, and advertises itself as a node having valid identity and becomes a part of a convincing route. Second, it consumes the packet instead of forwarding it.

3.4.6 Rushing Attack:
Two mischievous nodes can form a tunnel to perform wormhole attack. This tunnel can be used to propagate the packets faster than multihop route. It can act as an effective DoS attack against routing protocols of the MANET

3.5 Attacks on Transport Layer:

3.5.1 SYN Flooding:
SYN flooding attack is a DoS attack. In this, a malicious node creates a number of half open TCP connections with a victim node and never completes the handshake to fully open connection.

3.5.2 Session Hijacking:
Attacker makes parody of victim's IP address, knows the exact sequence number and then performs DoS attack. In elaborative manner, the attacker sends false session data, the receiving node will acknowledge by sending ACK to the sender node. Finding unexpected sequence numbers this the victim will try to resynchronize by sending ACK with the expected sequence number. This process goes on and on, and creates an ACK storm.

3.6 Attacks on Application Layer:

3.6.1 Mobile Virus and Worms:
Many malicious programs are spread out in the network. Any malicious program or a mobile virus can attack a system in two ways: First is IP address scanning in which probe packets are generated at many different IP addresses.

3.6.2 Repudiation:
It refers to a denial of participation in which a node must not deny to be a part or being a major party in communication.
When citing a section in a book, please give the relevant page numbers [2]. In sentences, refer simply to the reference number, as in [3]. Do not use "Ref. [3]" or "reference [3]" At the beginning of a sentence use the author names instead of "Reference [3]," e.g., "Smith and Smith [3] show ... ." Please note that references will be formatted by IJSER production staff in the same order provided by the author.

4. AODV and Flooding Attack:

Flooding attack [5] can adversely affect network resources such as

battery power, computation power and bandwidth. Also, it badly affects the performance of routing mechanism of a major routing protocol AODV. Following listed some bad effects of Flooding attack:

- Degraded the performance in terms of buffer
- Degraded performance in wireless interface
- Degraded performance in RREQ packets
- Degraded performance in terms of life time of MANET

AODV is designed to be exerted in the autonomous environment of mobile ad hoc network. In these kind of network, communication takes place on the grounds of mutual trust and nodes can easily assume that there no malicious node in the network. AODV, is more vulnerable to be affected in its route discovery process. DoS can easily take place at this stage. While discovering route, AODV broadcasts a Route Request (RREQ) packet in the network which contains a broadcast id, source and destination addresses and hop counts. After sending, it waits for route reply (RREP) or any other control packet. After waiting for a specific time, it tries the same process once again to get a valid route. Any security mechanism is absent in AODV, that is why DoS flooding attack can easily take place.

5. Related Works:

There exist diff DoS attacks like Flooding, wormhole, black hole etc. Amongst them, flooding attack is considered as one of the most harmful attack. [6] Discussed that it can degrade the performance of a MANET by 84-90%. The primary focus of these DoS attacks is to drain the network resources i.e. Bandwidth and to misuse the computation power of a mobile node thereby throwing the routing mechanism into disarray. This results in degradation of network performance in terms of DoS, wastage of bandwidth, wastage of a node's computation power and low battery life. As mentioned earlier, the flooding attack tries to generate routes that not even exist in the entire network. Many prevention mechanisms have been introduced so far to fortify this attack. Some of them are FAP [7], IDSs [8], Encryption techniques [9] etc.

Flooding attack can adversely affect network performance by draining battery and computation power as well as the bandwidth of the network. It can be of different types depending upon the layer, for example RREQ flooding [10] attack is triggered on the network layer, and SYN flooding [11] attacks on transport layer. With this change, the underlying protocols change from layer to layer. Let us now discuss different prevention mechanisms introduced so far. A self organized public key management was introduced in [12], for supporting routing protocols of MAnet. [13] Discussed another approach which was based on cryptography. They presented a mechanism for distributing certificate authority (CA) public key. By doing this they tried to form a collective CA service. Apart from these cryptographic approaches, some traffic based approaches has also been deployed. Neighbour suppression method [14], in which each node monitors and calculates the rate of its neighbour node's RREQ. If it exceeds the predefined threshold, the node is blacklisted. Another adaptive technique was presented in [15], which is based on statistical analysis for detecting RREQ floods. Flooding attack prevention (FAP) was method tested on AODV routing protocol. Adaptive intrusion detection technique [16] uses anomaly based intrusion detection as its grounds. It works in two phases, training phase and testing phase. Normal behaviour of the network is recorded in training phase and any fluctuation or change is detected in the testing phase by comparison. A trust based prevention mechanism was presented in [17] and [18]. In this technique, they introduced three filtering criteria to mark three node relationships i.e. friend, acquaintances and stranger. They included the concept of delay queue to handle nodes with higher mobility. Along with these filtering based techniques, we have capability based approach, to handle flooding attacks on transport layer. These methods are based on the principle "Deny by Default". In this technique, each node is assigned a capability which is a special token. This capability is issued by the responder of any transport layer flow to initiator, to urge a limit on the amount of traffic that can be sent through the flow within a certain period of time. When it comes to a monitoring based approach, it becomes easy and proves proper justification to participating nodes.

6. Conclusion and Future Work

MANET is said to be more vulnerable towards security threats. DoS attack in Mobile adhoc Network is one of the most likely to occur attack. RREQ flooding attack in AODV, being a DoS attack can severely damage the network performance. In this paper, we have discussed the effect of the attack in the network. We have also reviewed different techniques to encounter the attack. On the basis of these works done so far, we can conclude that in future, a fuzzy rule based approach can be implemented to accomplish a promising counter method.

References

[1] Perkins eg. al. "Adhoc on demand distance vector (AODV) Routing" , July2003.
[2] K. Sharma, Neha Khandelwal and Prabhakar M, "An overview of security problems in MANET" psrcenter.org.
[3] Praveen Joshi, "Security issues in routing protocols in manet at networ klayer" Elsvier 2011
[4] Khushboo sawant,Dr. M. K. Rawa,"Survey of flooding attacks on manet", Int. Journal of engineering research and applications 2014
[5] Bhuvaneshwari K. , Dr. A Francis saviour devraj,"Examination on impact of flooding attack on manet and to accentuate on performance degradation" Int. J Advanced networking and Apps. 2013
[6] Phillipe OWEZARSKI, "On the impact of DoS attack on internet traffuc characterstics and QoS", IEEE Xplore, 2005
[7] Ping yi,Zhoulin Dai, Shiyong zhang,Yiping Zhong, A new routing attackin mobile ad hoc networks" Internatiinal journal of info. Tech. vol III no.2.
[8] Yi-an Huang, Wenkee led, "A cooperative intrusion detection system for Ad hoc networks" Psrcentre.org.
[9] A. amuthan, B. Aravind bardwaj,"Secure routing scheme in manet using secret key sharing" Int. Journal of Computer Applications May 2011
[10] Ipsa De, Debutta barman roy," Comparative study on attacks on AODV based mobile Ad hoc networks" Ipsa de et. al. int. Journal on cs and engg, 2011
[11] Haining wang, Danlu Zhang,Kang G. Shan,"Detecting SYN flooding attacks"
[12] K. Sahadeviah, OBV Ramanaiah,"Self organized public key cryptography in mobile ad hoc networs"
[13] Mohd. A. Alhabeeb,Abdullah Almuhaideb and phu dung le,"

Holistic approach for critical system security:flooding prev. And mal. Packet stopping" Journal of telecomm. Vol I Issue 1 ,2010.
[14] Jian-Hua Song, Lang hong, yu zhang,"Effective filtering scheme against RREQ flooding attack" in preceedings of seventh International conference on parallel and distributed computing Applications and Technologies(PDCAT '06) 2006.
[15] Samam Desilva, Rajendra V. Boppan,"Mitigating malicious control packet floods in Ad hoc Networks", IEEE wireless communications and networking conference, March 2005.
[16] Adnan Nadeem, Michael howarth," Adaptive intrusion detection and prevention os denial of service attacks in MANETS" ACM 2009
[17] Shishir K. Shandilya, Sunita Sahu ,"A trust based security scheme fir RREQ flooding attack in MANET" International journal of computer applications aug 2010.
[18] Ujwala D. Khartad and R. K. Krishna,"Route request flooding attack using trust based security scheme in manet", International journal of smart sensors and Ad hoc Networks (IJSSAN), 2014.