RESEARCH ARTICLE OPEN ACCESS

Survey of DOS Flooding Attacks over MANET Environment

Khushboo Sawant, Dr. M.K Rawat
Department of Computer Science & Engineering Lakshmi Narayan College of Technology Indore, India

ABSTRACT
Mobile ad hoc network (MANET) is one of the most up-and- coming fields for research and review of wireless network. Essential requirement in MANET is security .In ad hoc network the communicating nodes sets new challenges for the security architecture because it doesn't necessarily feed on fixed infrastructure. The ad-hoc network is more vulnerable to denial of service attacks (DOS) forcefully initiate through malicious nodes or attacker. In this paper, we are illustrate the occurrence of flooding attack and their exposed to the possibility of being attacked or harmed effects which give chance to a legitimate node for doing other attacks too. So we proceed towards is to identify the presence or existence of DOS flooding attack using secure routing protocols.

Keywords: DOS attack, flooding attack, Routing Protocols, Security.

I. INTRODUCTION

MANET is a wireless network consists of mobile nodes that form a short-lived network in the absence of any centralized supervision in such an environment. MANETs consist of mobile nodes that are free in moving in and out in the network [1]. Nodes can be anything like systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and free to moving in and out in the network. At the same time nodes can act as host as well as router and form inconsistent topologies pivot on their comparability with each other in the network. Because of their self alignment ability these nodes have the capability to reconfigure itself. Internet Engineering Task Force (IETF) has MANET working group (WG) that Develop and promotes the internet standards as well as IP routing protocols.

Routing protocols is one of the worthwhile areas of research. Many routing protocols have been promote and developed for MANETS, i.e. AODV, OLSR, DSR etc.

MANETs have been many characteristics like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms which often suffer from security attacks because of its features and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the Security threats. The MANETs work with a decentralized administration so that on the basis of mutual trust communication occurs within the network. This features form ad hoc network more undefended to be utilize by an intruder with in n Inside the network. Wireless links also makes the MANETs more likely or liable to be influenced or harmed by a particular thing, which make it trouble free for the intruder to go inside the network and gain access to the existing communication.

1.1 SECURITY ISSUES

A crucial barrier with wireless network is its security. When data is transmitted there is always the probability that attacker nodes hacking the data and gain access to the network and misuse the data. For observing the certainty of ad hoc networks we required certain parameters. The basic parameters are:-

Availability: Availability means the information should be available when ever required.

Confidentiality: Confidentiality ensures that information must be confidential from unauthorized user.

Integrity: Integrity assures that a message is not modified by intruder.

Authentication: both the parties must be authenticating each other at the time of communication.

Non repudiation: Non repudiation ensures that sender and receiver of a message cannot deny that they have ever sent or received such a message.

Anonymity: Anonymity means all information about identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

Authorization: This property allocates different access goodness to many types of users.

II. SECURITY ATTACKS IN MANTES

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network. The attacks in MANETs are divided into two major types.

2.1 INTERNAL ATTACKS

Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes [2]. Internal attacks are sometimes more difficult to handle as compare to external Attacks, because an internal attack occurs due more trusted nodes.

2.2 EXTERNAL ATTACKS

These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc [2]. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories:

2.2.1 PASSIVE ATTACKS

MANETs are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. But it includes the unauthorized “listening” to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic [2]. Detection of such type of attacks is difficult since the operation of network itself doesn’t get affected. In order to overcome this type of attacks powerful encryption algorithms are used to encrypt the data being transmitted.

2.2.2 ACTIVE ATTACKS

Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks [2].These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of Packets, DoS, congestion etc. In [1][3] the authors survey attacks like flooding attack ,black hole attack ,link withholding attack ,link spoofing attack ,replay attack ,wormhole attack, colluding misrelay attack and gave their countermeasures using some cryptography and key management techniques in mobile ad hoc network and introduced a new attacks that is Ad Hoc Flooding Attack, which acts as an effective denial of service attack against all currently proposed ad hoc network routing protocols[1].

III. CLASSIFICATIONS OF ATTACKS

The characteristics of MANETs make them susceptible to many new attacks [2]. These attacks can occur in different layers of the network protocol stack.

LAYER	Types of Attacks
Multilayer	Denial of service attack, Impersonation attack
Application	Repudiation ,Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, SYN Flooding attack
Network	Black hole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay attacks, Link Withholding, Resource Consumption Attack, Sybil attack ,Byzantine Attack
Data Link	Selfish misbehavior, traffic Analysis, malicious behavior
Physical	Eavesdropping, jamming, active interference

3.1 MULTI-LAYER ATTACK

Multilayer attacks are those attacks that could exist in any layer of the network protocol stack so it is important to provide a route with secure robustness in wireless ad hoc networks. Denial of service (DOS) and impersonation are some of the common multilayer attacks .Wireless ad hoc networks can be exploited to various kinds of attacks [2] .Among them, the ad hoc flooding attack can easily cause denial of service attacks by overfill many route request or data packets within the network.

3.1.1 DENIAL OF SERVICE

In denial of service attack, a malicious node attempts to prevent victim and authorized node from services offered by the network and make resources or services unavailable to their intended users. DoS attack can be launched against any layer in the network protocol stack [5]. On physical layer and MAC layers, attacker can use jamming approach to interfere with communication on physical channel. Whereas On network layer the attacker can exploit the routing protocol and disturb the normal functioning of the network. On higher layers; the attacker could bring down high level services by injects a large amount of junk packets into the Network. These packets over carry a significant portion of network resources, and bring wireless channel & network contention in the ad hoc network. Some of the DoS attacks are described below:

JAMMING ATTACK: In this form of attack, the attacker initially keeps observing the wireless medium in order to get the frequency at which the destination node is acquiring signals from the sender. It then transmits signals on that frequency so that error-free reception at the receiver is hindered. The intention of a jammer is to influence with authentic wireless communications. A jammer can accomplish this target by either intercepting a real traffic source from sending out a packet, or by preventing the reception of legitimate packets.

DISTRIBUTED DOS ATTACK: In this attack several malicious nodes that are distributed throughout the network are colludes and prevent victim nodes from gain accessing the services offered by the network. Distributed DoS is a severe threat for MANETs because they can be smash only because of their limited battery power so that network can easily become congested due to its relatively limited bandwidth compared to fixed networks
Different types of DDoS attacks:

Active DDos attack: - misbehaving node damage other nodes in order to consume battery life of victim node for their own communication

Passive DDos attack: - occurred only because of lack of cooperation in between legitimate nodes

RUSHING ATTACK: Rushing attacks in mobile ad hoc networks (MANETs) is results in denial-of-service cause system resources to become inadequate and cut off a legitimate node from the network. A rushing attack used against on demand routing protocols. In most of applications on demand routing are used because it have lower overhead and fast reaction time. Therefore, this form of attack significantly influences network comparability as well as capability of networking functions such as control and message delivery.

SLEEP DEPRIVATION: the attacker collaborate with the node in such a way that it appears to be legitimate; however the purpose of interaction is to keep the victim node out of its power conserving sleep mode. An attacker can cause sleep deprivation by make use of the vulnerability of the route discovery process of protocols such as AODV and DSR, for example, by sending a RREQ packet periodically so that the victim node has to process these packets causing consumption of its battery power.

FLOODING ATTACK: Flooding attack is a denial of service type of attack in which the adversaries' node broadcast the redundant false packet in the network to exhaust the available resources and reduces the throughput of the network so that valid or legitimated user can not able to use the network resources for well defined communication. The flooding attack is possible in all most all the secure on demand routing like SRP, SAODV, ARAN, Ariadne etc. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the host's memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service. The number of RREQ that can be originated per second is limited. After broadcasting a RREQ, the initiator will wait for a ROUTE REPLY.- If a route is not received within round-trip milliseconds, the node may try again to discover a route by broadcasting another RREQ, until it reaches a maximum of retry times at the maximum TTL value. But for the second RREQ, the time to wait for the ROUTE REPLY should be calculated according to a binary exponential back off, by which the waiting time now becomes 2 * round-trip time. Depending upon the type of packet used to flood the network, flooding attack can be categorized in two categories.

RREQ FLOODING: In RREQ flooding attack the attacker selects many IP addresses which are not in the network or select random IP addresses depending on knowledge about scope of the IP address in the network. In Malicious RREQ Flooding attack an intruder broadcasts a RREQ with a destination IP address and does not wait for the ring traversal time and continuous resending the same packets with higher TTL value.

DATA FLOODING: In the data flooding, malicious node flood the network by sending useless data packets. In the data flooding, first malicious node built a path to all the nodes then sends the large amount of fake data packets.

3.1.2 Vulnerabilities in AODV

Flooding attacks can incredibly reduce the performance of reactive routing protocol and affect a node in following ways [8]:-

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

Vulnerabilities in AODV is designed for use in networks where the communication is occur on the basis of mutual trust between nodes and can assume there is no malicious intruder node. Taking the operation of AODV, basically its route discovery process, it is more vulnerable to DoS attacks such as sleep deprivation and the rushing attack. In the route discovery procedure of AODV broadcasts a RREQ packet containing a broadcast id, source & destination addresses, and hops count and destination sequence number & wait for a specific time for getting a RREP or other control packet. If this time was expire; node may try same process once again for getting a valid route. AODV Provides no security mechanism so that DOS flooding attack can easily be done.

IV. RELATED WORKS

Significant works have been done in securing the ad network. Some researches defined the method for secure routing but secure routing also can not able to handle the flooding attack. The data flooding attack causes Denial of Service (DoS) attacks by flooding many data packets. However, there are a few existing defence systems against data flooding attacks. Moreover, the existing schemes may not guarantee the Quality of Service (QoS) of burst traffic since multimedia data are usually burst.

In [5], author proposed the period-based defence mechanisms which mainly focus on RREQ flooding attacks rather than the data flooding attack. So it is possible to reduced the throughput of burst traffic by compete with simple threshold.

In [6], author develops Rushing Attack Prevention (RAP), a generic defense against the rushing attack for on-demand protocols because it can be performed by a relatively weak attacker. This approach is generic, so any protocol that relies on duplicate suppression in Route Discovery can use our results to fend off rushing attacks. When integrated with a secure routing protocol, RAP incurs no cost unless the underlying secure protocol cannot find valid routes. When RAP is enabled, it incurs higher overhead than do standard Route Discovery techniques, but it can find usable routes when other protocols cannot, thus allowing successful routing and packet delivery when other protocols may fail entirely.

In [7], author proposed a secure link state protocol (SLSP) for mobile ad hoc networks, which can be multiply beneficial to the network operation. SLSP is robust against individual Byzantine adversaries. Its secure neighbor discovery and the use of NLP strengthen SLSP against attacks that attempt to exhaust network and node resources.

In [8], author mainly focused on preventing denial-of-service (DoS) attacks & illustrates how intruders can exploit the route discovery procedure of reactive routing protocol to cause certain DoS attacks in MANET. to detect DoS and propose an anomaly-based intrusion detection system that uses a combination of chi-square test & control chart to first detect intrusion and then identify an intruder and show that it generate low detection & high false alarm rates.. Adaptive Intrusion Detection & Prevention (AIDP) finally isolates the nodes from the network to prevent intrusion.

In [9], the author described the Route request flooding attack with its effects in MANET and message format and damages caused by it. Then also conclude that the flooding attack is detected and prevented using core node. The influence of flooding attack on the entire network performance is analyzed under the circumstances of different parameters including the number of attack nodes, flooding frequency, network bandwidth, and the number of normal nodes.

In [10], the author proposed trust estimation technique which uses the DSR on demand routing protocol to detect & mitigate the effect of RREQ flooding attack in the networks with high node mobility. In this work, based on the trust value they categorized the nodes in three categories: Friends, acquaintance and stranger. Stranger are the non trusted node, friends are the trusted node and acquaintance has the trust values more than stranger and less than friends. Based on relationship they define the threshold values.

V. TECHNIQUES REVIEW

Many Authors research the causes of Dos attacks and conclude the advisory effect of Dos attack, i.e flooding of packet and make a loop. Because of Dos flooding attack the network throughput is degrade with dropping of packet and many unwanted malicious node/attacker node can be easily join the network. it is also type of multilayer attack in which there is also possibility of attacker to do other attacks too at the same time. In this paper we survey the main cause of dos flooding attack and different methodology that has been used by many author to prevent dos attack, i.e.:-

Methods	**Advantages**	**Disadvantages**
New fangled method	easily reduced the throughput of burst traffic by using blacklist of data packets	resource exhaustion
The flooding attacks prevention Scheme	It may cut off the path when many data packets are transmitted to the victim node .	FAP .in this method flooding packet still exists in the network
The rushing attack prevention Scheme	It provides provable security properties even against the strongest rushing attackers	It incurs higher overhead
A Trust Based Security scheme	It efficiently reduces the flooded RREQ packets from the network.	it does not work well with higher node mobility
Secure link State Routing Scheme	It robust against individual attackers and doesn't synchronize the topology maps across all nodes.	It remains vulnerable to colluding attackers
Key management scheme	It provides security goals like authentication ,integrity etc by using encryption Techniques & some secure protocol	it introduced heavy traffic load to exchange and verify keys
Adaptive intrusion Detection & Prevention Scheme	It reduces the control packet overhead & increases the network throughput with very high success rate and very low false alarm rate	Processing overhead on the network

VI. CONCLUSIONS

In these paper we briefly discussed one of the crucial security attack in MANET i.e. DOS Flooding .In our future work, we will further develop Flooding attack prevention schme (FAP) to improve its attack prevention rate against larger number of collaborates flooded packets and we will also enhance the security features of FAP by path cut off methods to identify core nodes of flooded packets in well founded communication to detect Dos flooded attack.

REFERENCES

[1] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong, A New Routing Attack in Mobile Ad Hoc Networks, published in International Journal of Information Technology Vol. 11 No. 2, , pp. 83−94,

[2] Abhay Kumar Rai ,Rajiv Ranjan Tewari and Saurabh Kant Upadhyay, Different Types of Attacks on Integrated MANET-Internet, International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), pp 265-274

[3] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, IEEE Wireless CommunicatioOctober 2007 , pp. 85−91

[4] Yi-an Huang and Wenke LeeE. Jonsson et al. (Eds.): Springer-Verlag Berlin Heidelberg 2004RAID 2004, LNCS 3224, pp. 125–145, 2004..

[5] Kavuri Roshan1 , K.Reddi Prasad2 , Niraj Upadhayaya3 & A.Govardhan4, International Journal of Computer Science & Information Technology (IJCSIT) Vol 4, No 3, June 2012, pp. 25-34

[6] YihChun Hu , Adrian Perrig, David B. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network routing Protocols; September 19, 2003, San Diego, California, USA.

[7] Panagiotis Papadimitratos, Zygmunt J. Haas; Secure Link State Routing For Mobile Ad Hoc Networks

[8] Adnan Nadeem , Michael Howarth ; Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs

[9] Ujwala D. Khartad & R. K. Krishna; Route Request Flooding Attack Using Trust based Security Scheme in , International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248-9738 Volume-1, Issue-4, 2012;pp 27-33

[10] Shishir K. Shandilya, Sunita Sahu; A Trust Based Security Scheme for RREQ Flooding Attack in MANET; International Journal of Computer Applications (0975 – 8887) Volume 5– No.12, August 2010,pp 4-8

[11] D.karun Kumar Reddy ,et al, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 5, October,pp-228-

237

[12] A Study of MANET: Characteristics, Challenges, Application and Security Attacks; Aarti et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(5), May - 2013, pp. 252-257

[13] Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review ;Gagandeep, Aashima, Pawan Kumar ;International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012

[14] Survey of different types of attack and prevention scheme ,Sitesh kumar sinha Krishna kumar pandey Mukesh kumar sahu; International Journal of Computer Technology and Electronics Communication ISSN 2320 – 0081,pp-19-24

[15] Sapna Choudhary, Alka Agrawal ; Threshold Based Intrusion Detection System for MANET using Machine Learning Approach, International Journal of Advance Electrical and Electronics Engineering (IJAEEE), ISSN (Print): 2278-8948, Volume-3 Issue-1, 2014,pp-1-6