Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detection and Prevention Algorithms of DDOS Attack in MANETs

Geetika, *Naveen Kumari*
Punjabi University Regional Center for Information Technology and Management, Mohali, Punjab, India

Abstract*— Security is a weak link of network systems. The malicious usage and attacks have caused tremendous loss by impairing the functionalities of the computer networks.. In an attempt to enhance security in MANETs many researchers have suggested and implemented new improvements to the protocols and some of them have suggested new protocols. Existing MANET routing protocols, such as Ad Hoc On-Demand Distance Vector Routing Protocol (AODV), do not provide enough security defense capacity. Distributed Denial of Service (DDoS) attack has become a major problem to networks. In this paper, we introduce Bottom-up approach, New Cracking algorithm,Prevention algorithm using IDS node for detecting and controlling DDoS attack.

Keywords*— MANET, Flooding attack, DDoS attack, Bottom Up, New Cracking Algorithm, IP Traceback.

I. INTRODUCTION

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.A **mobile ad hoc network** (**MANET**) is a self-configuring infrastructureless network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. [20] **Distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a machine or network resource unavailable to its intended users.[19]. MANET is a distributed system that comprises wireless mobile nodes that can freely and dynamically self-organize into arbitrary, temporary, and ad hoc network topologies, allowing seamless interconnections without pre-existing communication infrastructure and central administration. Due to its unique characteristics, MANET is vulnerable to various security threats, and it is particularly susceptible to the DDoS attack.[4]

Security Challenges & Issues Of Manets

- MANETs use wireless media for transmission, which introduces security flaws to the networks. Basically any one with the proper equipment and knowledge of the current network topology and the protocols may obtain access to the network. Both active and passive attacks such as impersonation, eavesdrop-ping, message redirection, and traffic analysis, can be per-formed by an adversary. [10]
- In specific scenarios, MANET nodes may be scattered over a large area. Some nodes or network components may be un-monitored or hard to monitor, and exposed to the physical attacks.[2]
- Because MANETs do not have any central authority, this is a major barrier to security. The security mechanisms employed in wired networks, such as Public Key Management, Node Authentication, and Determination of Node Behavior, are in fact very difficult to achieve without any central administration.
- Ad hoc networks are highly dynamic in nature. Node joins and departures are not predictable. Moreover, network topology is always changing in Ad Hoc networks. [3]

MANET VULNERABILITIES:

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

Lack of centralized management: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network.

Resource availability: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

Scalability: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

Dynamic topology: Dynamic topology and changeable nodes Membership may disturb the trust relationship among nodes. The

trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

Limited power supply: The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

Bandwidth constraint: Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

Adversary inside the Network: The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.

No predefined Boundary: In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node. The attacks include Eavesdropping impersonation; tempering, replay and Denial of Service (DoS) attack.[10]

Some specific DDoS types are listed below

- *SYN Flooding.* The attack uses the weakness of the TCP handshake. It sends an abundance of TCP SYN packets to the victim. The victim opens a lot of TCP connections and responds with ACK. But the attacker does not finish the hand-shake, which, in result, causes the half-open TCP connections to overflow the victim's incoming queue. SYN Flooding does not target specific Operating System, so it may attack any system supporting TCP protocol .

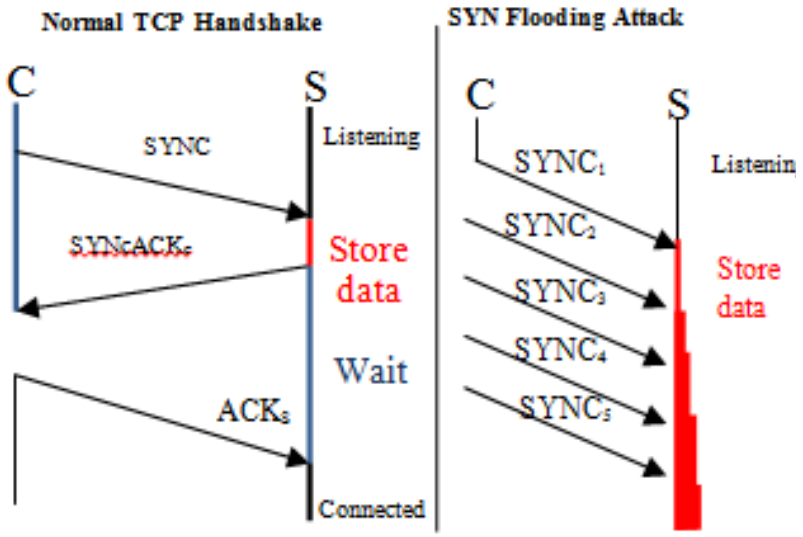

Fig. 1- SYN Flooding Attack [8]

- *Ping of Death*: The attacker sends the victim oversized IP packets, which contain more than 65,536 bytes. It may cause the victim machine to crash.[4]
- *Process Table* :The attacker sends an abundance of uncom-pleted connections to the victim server. The victim will create a new process for each connection until it cannot serve any more requests.
- *Smurf Attack* :The attacker sends the broadcast address an abundance of Internet Control Message Protocol (ICMP) "echo-request" packets, which has the victim's IP as the source address. The victim will be flooded with ICMP "echo-reply" packets . [7]
- *SSH Process Table* : The attacker overflows the SSH daemon in the victim system. It is similar to the process table attacks.
- *TCP Reset*: The attacker listens the traffic for the "tcpconnection" requests to the victim. Once such a request is found, the attacker sends a spoofed TCP RESET packet to the victim and obliges it to stop the TCP connection [9].
- *Teardrop:* The attacker creates a stream of IP fragments with their offset field overlapped. The victim may crash when trying to reassemble these malformed fragments [8].
- *UDP Packet Storm* :The attacker spoofs a start packet and builds a connection between two victim nodes, which provide a type of UDP output services (such as "chargen" or "echo") to generate numerous traffic into the network [16].

DDOS ATTACKS IN MANETS :

Distributed denial of Service attacks usually occurs in MANETS or in wireless networks. It is an attack where multiple systems comprised together and target a single system causing a denial of service (DoS). The target node is flooded with the data packets that system shutdowns, thereby denying service to legitimate users.The services under attack are those of the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims." [1]Current MANets are basically vulnerable to two different types of DDoS attacks:

- *Active DDoS attack* is an attack when misbehaving node has to bear some energy costs in order to perform the threat
- Passive DDoS attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly [14].

Nodes that perform active DDoS attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive DDoS attacks with the aim of saving battery life for their own communications are considered to be selfish [13] [1]. The attacks are classified as :

Modification Attack :Modification is a type of attack when an unauthorized party not only gains access to but tampers with

an asset.

Impersonation Attacks : As there is no authentication of data packets in currentadhoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing.

Fabrication Attacks **:**Fabrication is an attack in which an unauthorized party not only gains the access but also inserts counterfeit objects into the system. [2].

ATTACK DETECTION METHODS IN MANET:

Profile-based detection

Profile-based detection is also known as behaviour-based detection. Profile-based detection defines a profile of normal behaviour and classifies any deviation of that profile as an anomaly. The assumption of this type of detection is that attacks are events distinguishable from normal legitimate use of system resources. Although this type of anomaly detectors are able to detect novel attacks, they are prune to high false positive rate due to the difficulty of clear segmentation between normal and abnormal activities and the use of insufficient or inadequate features to profile normal behaviours.

Specification-based detection

Specification-based detection defines a set of constraints that describe the correct operation of a program or protocol and monitors the execution of the program with respect to the defined constraints. It has been show that specification-based techniques live up to their promise of detecting known as well as unknown attacks, while maintaining a very low rate of false positives. Since, the increasing popularity of wireless networks to that of wired networks, security is being considered as a major threat in them. Wireless network exposes a risk that an unauthorized user can exploit and severely compromise the network. There can be different possible attacks in wireless network viz., active and passive attacks. So there is a need for secured wireless system to analyze and detect number of attacks.[1,17]

II. Review f Existing DDOS Defense Techniques

Bottom-up-Detection and Prevention Techniques-

This detection scheme is divided into 3 phases:

Phase–I : Quality Reduction Based Attacks

When an attacking host send SYN(k) packet for new connection to victim server victim server allocates memory for that host and sends SYN/ACK to that attacker consumes one sequence number and waits to receive for ACK from attacking host. This state is called half open connection state.

More and more requests will accumulate and fill up the memory buffer at server side. Attacker send large number SYN packets with spoofed source IP for preventing services to be granted to other legitimate requests. Therefore, no new request, including legitimate requests, can be processed and the services of the system are disabled.

Phase–II Bottom- up Approach for detection of TCP SYN Flood Attack

The detection algorithm needs the capability to detect any newly starting attacks not relating to the current happening ones. Also, if the extracted data characteristics cannot match any signatures, those packets will be regarded as normal network traffic and the detection system ignores them. The whole detection process continues recursively till detection been terminated.

Phase–III Prevention

Window-based Control for Normal Half Open Connection:

In this approach we proposed a window limit per resource or per traffic aggregate. This allows us to control how a certain resource can be consumed by a traffic class at any given time. After this limit is reached, incoming requests or packets seeking this resource are dropped or delayed at the QOS regulator until the server sends some kind of indication that an earlier request from this traffic class has freed its resources. When this happens, more flows or requests can be admitted. The windows limit quantifies the resource availability.

TTL-based Packet Filtering Approach for Abnormal Half Open Connection:

Filtering all packets having a certain TTL value would result in the filtering of legitimate as well as attack packets. Hence, our TTL-based rate-limit scheme includes rules for distinguishing normal from spoofed packets. It does this by observing TCP three-way handshake behaviors. During a normal three way handshake procedure, Syn(k), Ack(k + 1) + Syn(j) and Ack(j +1) can be captured at the victim side.[4]

LPN DDoS Attack Mitigation Strategies -

Local Protection Node(LPN) protects the victim node of a DDoS attack. The LPN node filters all the attacking packages in the traffic whose destination is the victim. In addition, the LPN recognizes the source IP addresses corresponding to the malicious traffic, and an Attack Notification Message (ANM) is sent to the victim node. The ANM includes the source IP addresses of involved malicious attack agents. Then, the victim node broadcasts an Attack Information Message (AIM) packet towards the remote protection node (RPN). With the information in AIM, the RPN nodes filter off all the malicious packets at the source side. This mechanism aims to recover the service for destination protection node and to tell every other node to drop the RREQ from the malicious node. After doing this, the malicious nodes cannot send out traffic or build a route.[5]

Clustering Based Prevention Techniques –

In this clustering technique the reputation and score value of nodes to elect a cluster head and when a Cluster-Head is subjected to DDoS attack this would have manifolds consequences as the Cluster Heads form a virtual backbone and may be used to maintain routing states information & route packets to nodes in their cluster. The architecture worked in three phases namely as

Phase I: Reputation and Score Based Cluster Creation And Cluster Head Selection

Phase II: presents mentioning of some of DDoS attacks like message bombing and cache poisoning, their detection strategies

Phase III: presents a control frame packet format which can be used as a line of defense mechanism to control and mitigate from DDoS attacks over a Reputation and score based MANET.[12]

Detection Algorithm using IDS node –

In this algorithm firstly we create an IDS node in which we set AODV as a routing protocol. Then after the creation, our IDS node check the network configuration and capture lode by finding that if any node is in its radio range and also the next hop is not null, then capture all the information of nodes. Else nodes are out of range or destination unreachable. With the help of this information IDS node creates a normal profile which contains information like type of packet, in our case (protocol is AODV, pkt type TCP, UDP, CBR), time of packet send and receive and threshold. After creating normal profile and threshold checking is done in the network i.e. if network load is smaller than or equal to maximum limit and new profile is smaller than or equal to maximum threshold and new profile is greater than or equal to minimum threshold then there is no any kind of attack present. Else there is an attack in the network and find the attack. For doing it compare normal profile with each new trace value i.e. check packet type, count unknown packet type, arrival time of packet, sender of packet, receiver of packet. And after detection of any anomaly in that parameters then block that packet sender node . The proposed mechanism eliminates the need for a centralized trusted authority which is not practical in ADHOC network due to their self organizing nature. It protects the network through a self organized, fully distributed and localized procedure. It can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks.[11]

New Cracking Algorithm –

In this algorithm a procedure is made to tackle the continuous problems occur in the internet services. To avoid the continous logon to a particular web site, this algorithm maintains a status table. In that it keeps the IP addresses of current users and their status. If the particular IP address has been signed on for a first time, it makes the status as genuine user. For 2, 3, 4 it marks as Normal user. For the fifth time it makes the particular IP address status as Attacker. In the time calculations we are only consider 5 times. User wish to server increase the time depends up on the application. After that, the user cannot allow get the service of that particular web site. The service is denied to that particular IP address. The basic idea behind the proposed system is to isolate and protect the web server from huge volumes of DDoS request when an attack occurs. Also a DDoS defense system for protecting the web services is also proposed. When a DDoS attack occurs, the proposed defense system ensures that, in a web related server information are managed without corruption. This newly designed system that effectively gives the availability of web services even during severe DDoS attacks. Our system is practical and easily deployable because it is transparent to both web servers and clients and is fully compatible with all existing network protocols.[15]

IP Traceback Algorithm -

IP traceback is the ability to find the source of an IP packet without relying on the source IP field in the packet, which is often spoofed. This algorithm can trace the source (zombies) of the attack up to its local administrative network. IP traceback scheme based on information metrics can effectively trace all attacks until their own LANs (zombies). In conclusion, our proposed information metrics can substantially improve the performance of low-rate DDoS attacks detection and IP traceback over the traditional approaches. DDoS attacks detection metric is combined with IP traceback algorithm and filtering technology together to form an effective collaborative defense mechanism against network security threats in Internet. In hop-by-hop IP tracing, the more hops the more tracing processes, thus the longer time will be taken. In order to convenience for IP traceback algorithm analysis, we classify two types of traffic as local traffic and forward traffic. The local traffic of is the traffic generated from its LAN , the forward traffic of is the sum of its local traffic and the traffic forwarded from its immediate upstream routers. This information metrics can substantially improve the performance oflow-rate DDoS attacks detection and IP traceback over the traditional approaches.[16]

III. Conclusion

There is an alarming increase in the number of DDoS attack incidents. Not only, DDoS incidents are growing day by day but the technique to attack, botnet size, and attack traffic are also attaining new heights. Effective defense measures needed to prevent and mitigate these attacks is the current need of the hour. In this paper, we introduce techniques for detecting and controlling flooding and DDoS attacks in MANET. They have most of the problems of wired networks and many more due to their specific features: dynamic topology, limited resources, lack of central management points. First, we have presented specific vulnerabilities of this new environment. Then we have surveyed the attacks that exploit these vulnerabilities and the possible proactive and reactive solutions proposed in the literature. Attacks are classified into passive and active attacks at the top level. Then various Preventive measures are discussed in order to mitigate the effects of DDOS attack in MANET. To conclude, MANET security is a complex and challenging topic.

References

[1] J. Mirkovic, and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *Computer Journal of ACM SIGCOMM*,vol. 34, no. 2, pp. 39- 53, Apr. 2004.

[2] J. Mirkovic, "D-WARD: source end defense against distributed denial of service attacks," Ph.D. thesis,University of California,2003.

[3] K. Sivakumar, Dr. G. Selvaraj,"Overview of various Attack in MANET and Countermeasures for Attack", *International Journal of Computer Science and Management Research*, Vol 2 Issue 1, January 2013.

[4] Laxmi Bala, A.K. Vatsa, "Quality based Bottom-up-Detection and Prevention Techniques for DDOS in MANET",*International Journal of Computer Applications*, Volume 55– No.2, October 2012.

[5] Minda Xiang,Yu Chen,Wei-Shinn Ku, Zhou Su, " Mitigating DDoS Attacks using Protection Nodes in Mobile Ad Hoc Networks", Dept. of Computer Science & Software Engineering, Auburn University, Auburn, AL 36849.

[6] Mohan K Mali, Pramod A Jadhav, " Review of DDoS and Flooding Attacks in MANET", *International Journal of Emerging Technology and Advanced Engineering*, Volume 3, Issue 5, May 2013.

[7] Maha Abdelhaq, Sami Serhan, Rred Alsqour and Rosilah Hassan (2011) *IEEE sponsored International Conference on Electrical Engineering & Informatics*.

[8] Michael R. Lyu and Lorrien K.Y. Lau (2000) 24*th International Computer Software and Applications Conference* 116-121.

[9] M. Robinson, J. Mirkovic, M. Schnaider, S. Michel, and P. Reiher, "Challenges and principles of DDoS defense," *Computer Journal of ACM SIGCOMM*, vol. 5, no. 2, pp. 148-152, 2003.

[10] Priyanka Goyal, Vinti Parmar, Rahul Rishi, "Vulnerabilities, Challenges, Attacks, Application",*International Journal of Computational Engineering & Management*, Vol. 11, January 2011.

[11] Prajeet Sharma,Niresh Sharma,Rajdeep Singh," A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network", *International Journal of Computer Applications*,Volume 41– No.21, March 2012.

[12] Rizwan Khan , A. K. Vatsa, "Detection and Control of DDOS Attacks over Reputation and Score Based MANET", *Journal of Emerging Trends in Computing and Information Sciences*, VOL. 2, NO. 11, October 2011.

[13] T. Peng, C. Leckie, and K. Ramamohanarao,"Survey of network based defense mechanisms countering the DoS and DDoS problems," *Computer Journal of ACM Computing Surveys*, vol. 39, no. 1,pp. 123-128, Apr. 2007.

[14] T. Roebuck. (2005) Crime-research.org, "Network security: DoS vs. DDoS attacks," [Online].Available: http:// www.crime-research.org/articles/network-security-dos-ddos-attacks.

[15] V.Priyadharshini, Dr.K.Kuppusamy, " Prevention of DDOS Attacks using New Cracking Algorithm", *International Journal of Engineering Research and Applications*,Vol. 2, Issue 3, May-Jun 2012, pp.2263-2267.

[16] Wang H., Zhang D. and Shin K. Delectating syn flooding attacks, *in IEEE infocom.*

[17] Washington.edu, "A DNS reflection attack on register.com," [Online]. Available: http:// www.staff.washington.edu/dittrich/misc/ ddos/

[18] Yang Xiang,Wanlei Zhou, "Low-Rate DDOS Attack Detection and Traceback with New Information Metrics", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, VOL. 6-NO. 2, JUNE 2011.

[19] https://en.wikipedia.org/wiki/Denial-of-service_attack

[20] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network

