Counter and Network Density Based Detection and Prevention Scheme of DOS Attack in MANET

(IJCSNT) International Journal of Communication Systems and Network Technologies
ISSN Number: 2053-6283
Volume 3, Issue No. 2, 86–96
©The Author(s) 2014
https://journals.mirlabs.in/index.php/ijcsnt
10.18486/ijcsnt/3.2.035
IJCSNT

Mamta Jha[1], Rajesh Singh[2], S.S. Dhakad[3]

Abstract
This paper presents the denial of service attack in MANET using a threshold value. In our approach, the node broadcasts the packets and then finds out the neighbors'. then it checks the degree of each successive neighbor and checks for a threshold value. If value is greater than the value clearly distinguishes between sparse and dense network. After waiting for random no. of slots the counter check is done which decides whether to terminate the process or not and continue ddos attack in manet in each network. It is better than the previous methods.

Keywords
DOS, SMURF, IGMP, ICMP.

Received: 12 April 2014; **Revised:** 29 June 2014; **Accepted:** 20 August 2014;
Published: 30 August 2014;

[1,2,3]Dept of Computer Science & Engineering, NITM, Gwalior, Madhya Pradesh, India.

Corresponding author:
Email: mamtajhamam@gmail.com

Introduction

In the present time internet has revolutionized every aspect of computer technology and communication world. The technological advancement began with early research on packet switching and the ARPANET. The Internet was created in 1969 to provide an open network for researchers[1]. Unfortunately, with the growth of the Internet, the attacks to the Internet have also increased incredibly fast. The widespread need and ability to connect machines across the Internet has caused the network to be more vulnerable to intrusions. Every year a large number of vulnerabilities go unreported.

A Mobile Ad hoc Network (MANET) is a[2] collection of wireless nodes that creates a temporary network without any centralized administration. MANETs have a decentralized architecture and lack of centralized control. In such network each node is free to move independently in any direction and will therefore change in it's like with other node and changes it frequently. Security of Mobile Ad hoc Networks (MANETs) has been a lot of scope in the research community. Due to open nature of network, dynamic changing topology MANET is easily vulnerable to various attacks. In addition, other issues also contribute to its vulnerability, such as the open architecture, shared radio channels, and limited resources, etc. Without a clear network boundary, it is extremely difficult to develop and understand ad hoc security strategy for MANETs. In MANET there are various Kinds of attacks like black hole attack, worm hole attack, sink hole , Sybil attack, Denial of service attack and Gray hole attack.

Denial of Service (dos)

A denial of service (DoS) attack is characterized[3] by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources. Examples of denial of service attacks include:

- Attempts to "flood" a network, thereby preventing legitimate network traffic.
- Attempts to disrupt connections between two machines, thereby preventing access to a service.
- Attempts to prevent a particular individual from accessing a service.
- Attempts to disrupt service to a specific system or person[3].

DDOS Attack

Denial-of-Service attack is an attempt that makes the network resource and machine unavailable to the intended users[5]. The attacks occur when the services is blocked by another user intentionally. This type of attack doesn't cause any damage to the data but it does not provide the required resource[4]. DDoS attack is a mass of compromised systems, which attacks a single target that causes denial-of–service for the users in targeted system.

As shown in Figure 1, DDoS attacks consist of following components:

i. Real Attacker

ii. Master hosts or handlers are capable of handling multiple agents.

iii. Zombie hosts that generate packets.

iv. Target host or Victim.[4].

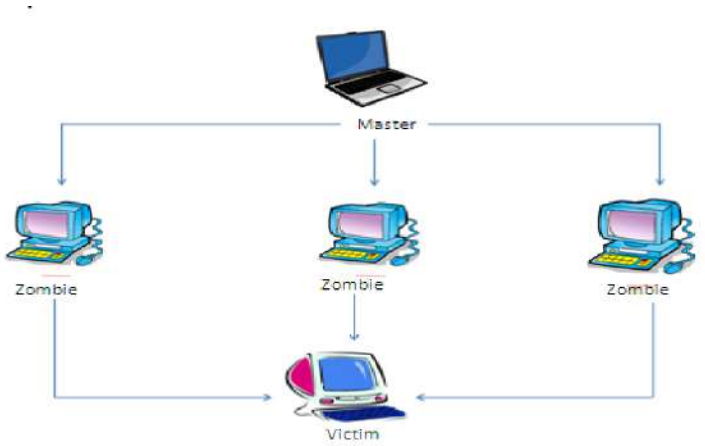

Figure 1. DDoS attack[2]

Types OF DDOS Attacks

SYN FLOODING:

This is the most important attack occur during the three-way handshake. In three-way handshake client request a new connection by sending SYN packet server ACK sends back to client. Finally client acknowledged with ACK. If attack occur numerous SYN packet to victim. It makes open numerous connections and responds to them, and third step of the hank-shake will not perform. That makes unable to open new connections. This Because of queue is filled with full of half-way TCP request. This flooding does not targeting specific operating system. It attacks any system that support TCP[6] .

SMURF ATTACK:

Cause of Smurf attack is flooding of ICMP echo-request echo-reply. Direction of packet is to IP broadcast address from remote location to generate DoS attack. Most of time attacker generate forged echo request using spoofed IP address, i.e. it is intended to victim machine, and attacker hide its identity. The intermediate node can't identify whether it is original or not. So intermediate node immediately reply that make flood on the victim machine[6].

UDP FLOOD ATTACK:

This is the second most popular attack. Main idea of this attack is to exploit UDP services. These attacks slowly down/congested the network. In this attack attacker sends to random port of victim. After receiving that packet victim system is try to find which application is waiting on the destination. But actually no

application running on that port.AZ large number of UDP packet are received by the victim, it make infinite number of loop goes between the Two UDP services [6].

ICMP DOS ATTACK:

In this attack Attacker simply forging the notification message. Attacker could use either Time exceed and or Destination unreached that cause immediately drop the connection Eg. Ping of Death, ICMP PING flood attack, ICMP nukes attack [6].

PING OF DEATH:

In this attack, attacker sends large number of malicious ping to computer. In this case large IP packet is split in multiple IP packets. In ping death scenario receiver ends up with packet size greater than 65,535when reassembled and over flow on allocated memory with numerous packets [3].

LAND ATTACK:

It consist stream of the TCP SYN packet both source and destination have same IP address and port number. Some implementations are impossible to handle this type of attacks completely. The main cause of this attack the operating system repeatedly go into the loop try to resolved repeated connection itself [6].

MAIL BOMB:

It is bandwidth-based flood attack. The attacker node sends large volumes of mail to mail-server causing it to deny services to legitimate user [6].

DNS AMPLIFICATION ATTACK:

Attacker use publically accessible open DNS server to flood a target system with DNS response traffic. The crucial technique consists of an attacker sending a DNS name lookup to an open DNS server with source address spoofed to be target's address. Attacker submits more requests to zone as possible to maximize the effect [6].

IGMP ATTACK.:

Cause this attack is to Flood the network with random IGMP messages. It makes overload on the network. It is the type of hacking attack. Main idea this attack is to reduced broadband and memory usage. But it is useful for multimedia broadcast application [6].

SQL SLAMMER:

.It is one computer worm that causes the denial of service on some internet host. Dramatically slow down internet traffic. It exploits buffer overflow vulnerability in SQL server and MSDE code [6].

Literature Review

Rutvij H. Jhaveri [7] present survey of common Denial-of-Service (DoS) attacks on network layer namely Gray hole attack, Wormhole attack, Black hole attack and which are serious threats for MANETs. We

will also discuss some suggested solutions to detect and prevent these attacks. MANETs have unique characteristics like, limited resources, dynamic topology, lack of centralized administration and wireless radio medium; as a result, they are unprotected to different types of attacks in different layers of protocol stack. Each node in a MANET is proficient of acting as a router. Routing is one of the features having various security concerns.

Yinghua Guo[8] presents a detailed investigation of the flooding attack in MANET which is particularly vulnerable to flooding attacks. To avoid being recognized, attackers usually recruit multiple accomplices to dilute attack traffic density of each attack source, and use the address parody technique to challenge attack tracing. we design two flow based detection features, and apply the increasing sum algorithm on them to effectively and accurately detect such attack.

Hwee-Xian Tan[9] studies the vulnerability of MANETs to DDoS attacks and provide an overview of constant filtering, which is commonly used as a security mechanism against DDoS attacks in wired networks. Also propose a structure for statistical filtering in MANETs to combat DDoS attacks.

Buchegger and Boudec[10] suggest that despite the fact that networks only function properly if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate. They propose a protocol, called CONFIDANT, which aims at detecting and isolating misbehaving nodes, thus making misbehavior unattractive. Here misbehaving nodes are excluded from forwarding routes. It includes a trust manager to evaluate the level of trust of alert reports. But it is not clear how fast the trust level can be adjusted for compromised node especially if it has a high trust level initially[11].

Trust Evaluation method[13] provides an effective security mechanism based on data protection and secure routing. But it relies on global information and hence the reaction time is more. It would be preferable to reduce the reaction time.

Li Zhao et.al[12] have proposed Multipath Routing Single path transmission (MARS) scheme to mitigate adverse effects of misbehavior. This scheme combines multipath routing and single path data transmission with end-to-end feedback mechanism to provide more comprehensive protection against misbehavior from individual or cooperating misbehaving nodes.

Mukesh Kumar[14] a technique is proposed that can prevent a specific kind of DDoS attack named flood attack which Disable IP Broadcast. MANET has no clear line of defense so it is accessible to both malicious attackers and legitimate network users. In the presence of hostile nodes, one of the main Challenges in MANET is to design the robust security solution that can prevent MANET from various DDoS attacks. Individual mechanisms have been proposed using various cryptographic techniques to countermeasures these attacks against MANET.

Proposed Algorithm

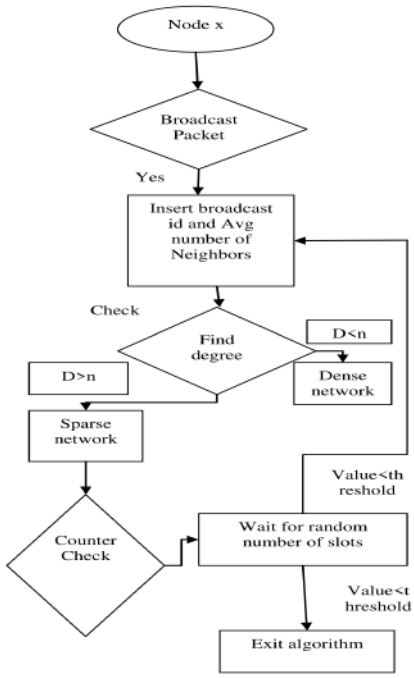

Figure 2. Proposed algorithm

Experimental Results

The metrics used are simulated as under
END TO END DELAY

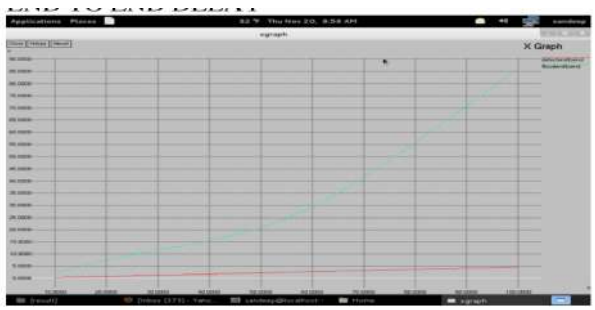

Figure 3. End to end delay

Throughput

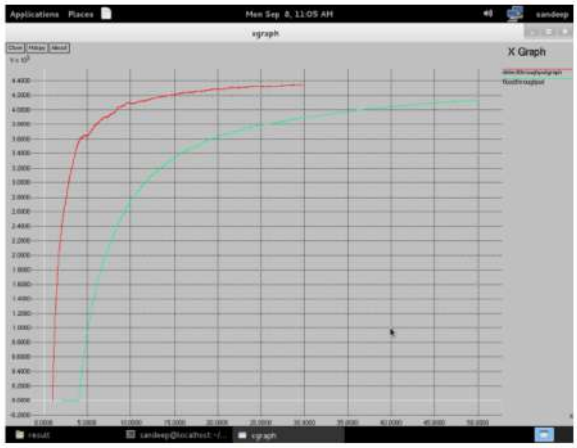

Figure 4. Throughput

Packet delivery ratio

Figure 5. Packet delivery ratio

Send packet

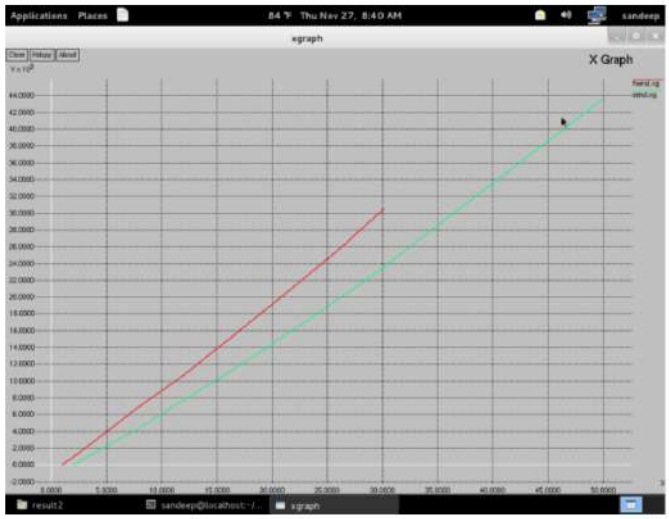

Figure 6. Send packet

Receive packet

Figure 7. Receive packet

Forward packet

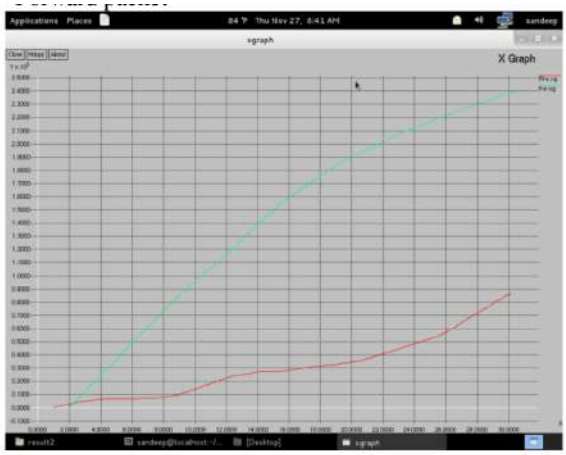

Figure 8. Forward packet

Drop packet

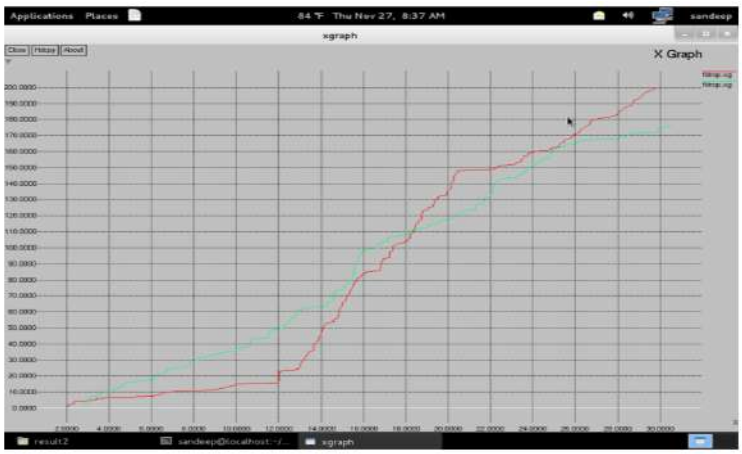

Figure 9. Drop packet

Control overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

Packet Delivery Ratio: The packet delivery ratio (PDR) of a network is defined as the ratio of total number of data packets actually received and total number of data packets transmitted by senders.

Normalized Path Discovery: Normalized path discovery is defined as the number of RREQ packets generated per data packet.

End-to-End Delay: The End-to-End delay is defined as the difference between two time instances: one when packets generated at the sender and the other, when packet I received by the receiving application.

Conclusion

In our paper , Dos attack is checked and according to the density of the network counter check is done which decide whether to further continue the process or not. In simulation work the performance metrices like Control overhead, Packet Delivery Ratio, Normalized Path Discovery, End-to-End Delay, show lesser dos attack which helps to make the network efficient. There by enhancing network performance.

References

[1] CERT. Cert statistics, 2007. http://www.cert.org/stats/cert_stats.html. (Accessed on: May 28, 2007).

[2] Gupt GK and Singh J. Truth of d-dos attacks in manet 2010; 10(15 (Ver. 1.0)).

[3] Gupta GK and Singh J. Truth of d-dos attacks in manet. *Global Journal of Computer Science and Technology* 2010; 10(15 (Ver. 1.0)).

[4] Garg D. Ddos mitigation techniques-a survey. International Journal of Advances in Computer Networks and its Security.

[5] Denial-of-service attack. http://en.wikipedia.org/wiki/Denial-of-service_attack.

[6] Kuriakose D and Praveena V. A survey on ddos attacks and defense approaches. *International Journal of Innovative Research in Computer and Communication Engineering* 2013; 1(8).

[7] Jhaveri RH. In *Second International Conference on "Advanced Computing & Communication Technologies"*. 2012.

[8] Guo Y, Gordon S and Perreau S. This full text paper was peer reviewed at the direction of ieee communications society subject matter experts for publication in the wcnc 2007 proceedings. In *WCNC 2007 proceedings*. 2007.

[9] Tan HX and Seah WKG. In *Second International Conference on Embedded Software and Systems (ICESS'05)*.

[10] Buchegger S and Boudec J. Performance analysis of the confidant protocol. In *Proc. Int'l Symp, Mobile Ad Hoc Networking and Computing*. 2002.

[11] Huang Y and Lee W. A cooperative ids for adhoc network security of adhoc and sensor networks. *ACM* 2003; : 135–145.

[12] Zhao L and Delgado-Frias JG. Mars: Misbehavior detection in ad hoc networks. In *Proceedings of IEEE GLOBECOM*. pp. 941–945. 2007.

[13] Yan Z and Zhang P. Trust evalution based security solution in adhoc network. Pp. 1-14.

[14] Kumar M and Kumar N. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)* 2013; 2(7). July 2013, ISSN 2319–4847.