Volume 5, Issue 4, April 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review of DoS Attack and Defence Scheme in Manet

Lovely
CSE & Kurukshetra University, Kurukshetra,
Haryana, India

Abstract— ***Mobile Ad-hoc network is the network comprised of wireless nodes. It has basically no infrastructure i.e. the connections are established without any centralized administration. A mobile ad hoc network (MANET) is a spontaneous network that can be established with no fixed infrastructure.***

Aim of DOS attack is to overload the server's bandwidth and other resources. A DDoS attack is a severe form of DOS which uses multiple machines to prevent the legitimate use of a service. A bandwidth depletion and resource depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. The research objective is the prevention of existing attack and defense mechanisms .

Keywords— DDoS, Denial of service, Wireless mobile adhoc network, security attacks, defensive mechanisms.

I. INTRODUCTION

Mobile Ad hoc Network (MANET) [15] comprises autonomous mobile nodes that dynamically and arbitrarily form multi-hop communication facilities to attack, Denial of Service (DoS) attack, selfish misbehaving, etc.. make up for the absence of fixed infrastructure. Securing communication in MANET is a challenging issue. Firstly, traditional security mechanisms used in infrastructure networks may be inapplicable to MANET due to its unique characteristics: unreliability of wireless links, the absence of a certification authority, dynamically changing topology and the lack of a centralized observation or management point. Secondly, for the same reason, MANET suffers from a wide range of threats and attacks: impersonation attack, black-hole.

1.1 FLOODING ATTACK IN MANET

The flooding attack [15] is the most common attack found in manet. The aim of the flooding attack is to fatigue the network resources such as bandwidth and to consume a node's resources or to disrupt the routing operation to degrade the network performance. This leads to a kind of Denial-of- Service (DoS) attack, wastage of bandwidth, wastage of node's processing power and exhaustion of node's battery power as well as a performance. Most of the network resources are wasted in trying to generate the routes to the destination that do not exist. The Route Request Flooding Attack (RRFA) is a denial-of service attack which aims to flood the network with a large number of RREQs to non-existent destinations in the network. In this attack, the spiteful node will generate a thousands of RREQs, into the network until the network is saturated with RREQs and unable to transmit data packets. In RREQ flooding attack the attacker select random IP addresses depending on knowledge about scope of the IP address in the network.

1.2 EFFECTS OF FLOODING ATTACK

Flooding Attack reduce the performance of reactive routing protocols [15] and affect a node in the following ways:

I. Degrade the performance in buffer:

The buffer used by the routing protocol may overflow since a reactive protocol has to buffer data packets during the route discovery process. Furthermore, if a large number of data packets originating from the application layer are actually beyond reach, authentic data packets in the buffer may be replaced by these unreachable data packets.

II. Degrade the performance in wireless interface:

the buffer used by the wireless network interface card may overflow due to the large number of RREQs to be sent. Similarly, genuine data packets may be dropped if routing packets have priority over data packets.

III. Degrade the performance in RREQ packets:

Since RREQ packets are broadcast into the entire network, the growing number of RREQ packets in the network results in more MAC layer collisions and consequently, overcrowding in the network as well as delays for the data packets. Higher level protocols which is sensitive to round trip times and congestion in the network will be affected.

IV. Degrade the performance in lifetime of Manet:

RRFA can reduce the lifetime of the network through useless RREQ transmissions as well as additional overheads of authenticating a large number of RREQs, if used.

1.3 DOS ATTACK

Denial of Service (DoS) attack [13] uses one computer to flood a server with packets. Aim of this attack is to overload the server's bandwidth. A DDoS attack is a severe form of DOS which uses multiple machines to prevent the legitimate use of a service. It is an active attack and powerful technique to attack Internet resources. It adds to the many-to-one dimension to the DoS problem. Making the prevention and mitigation schemes for them are more complicated. DDoS is composed as shown in Fig.1. First attacker build a network of nodes which are used to initiate the attack. The nodes called zombies which allow them to carry out attacks under the control of the attacker. The zombies are devided into two parts masters and slaves. The attacker motivates the masters to start the attack, the masters then motivate the slaves to start the attack. The slaves flood the victim.

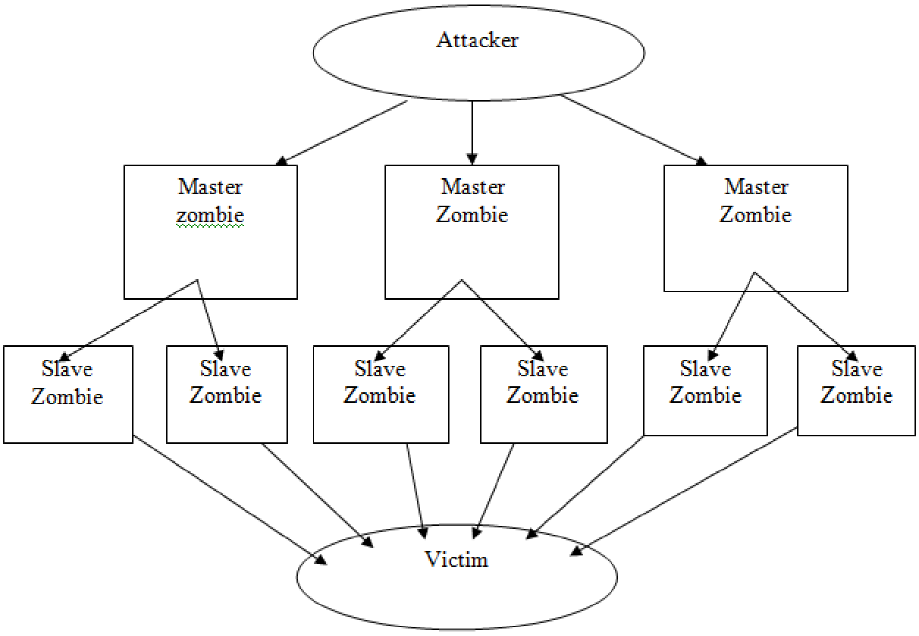

Fig. 1.Block diagram of DDOS attack [13]

1.4 DDoS ATTACKING PATTERNS AND DEFENSE SCHEME

Overview of IEEE 802.11 DCF

The Distributed Coordination Function (DCF) of IEEE 802.11 specifies the use of CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to reduce packet collisions in a network [8]. A node with a packet to transmit picks a back off value I which is chosen uniformly randomly from the set {0, 1, . . .CW} where CW denotes the size of the contention window, and then transmits the packet after waiting for I idle time slots. Nodes exchange Request to Send (RTS) and Clear to Send (CTS) packets to reserve the channel before transmission [8]. Both RTS and CTS packets contain a duration field to indicate the time required for utilizing the channel to complete the data transmission. RTS or the CTS are required to adjust their Network Allocation Vector (NAV), which specifies for how long the node should defer transmissions on the channel. If a transmission is unsuccessful (by the lack of CTS for RTS or ACK for the DATA sent), the value CW of is doubled and the lost packet is retransmitted. The maximum number of retransmissions of RTS is always set to 7 and that of DATA to 4. On the other hand, if the transmission is successful, the host resets its CW to minimum value CW min, There are additional idle times between frames, such as DIFS (Distributed Inter Frame Space) and SIFS (Short Inter Fame Space).

1.5 ATTACKING PRINCIPLES

In wireless networks [8], the main competing resource is the channel, which is shared by wireless nodes with only one node having access at a time. Unlike wired networks in which channel congestion is always the result of increased rate of competing flows at the bottleneck link, congestion in MANETs may also be due to the aggregation of mobile nodes. If the attacking nodes aggregate with high density near the victim nodes, the attacking nodes may occupy the channel in the most of the time. Another reason of potential attacking is the current routing protocols or intermediate nodes in MANET have not provided traffics control mechanisms, such as traffics filter, traffics allocation and Quality of Services. According to the analysis , radios that are sufficiently distant from each other can transmit data concurrently. The total number of data packets that can be simultaneously transmitted for one hop increases linearly with the total area of the ad-hoc network. If the node density is constant, then the total one-hop capacity is O(n) where n denotes the total number of nodes in the network. As the network grows in size, the number of hops between the source and destination nodes may also increase. The average path length grows with the spatial diameter of the network, which is proportional to the square root of the area, i.e., O(pn). Therefore, the total end-to-end capacity is roughly O(n/pn) and the end-to-end throughput available to each node is O(1/pn). To simplify the analysis, given n nodes in the interference range, each node has a probability of 1/n to access the channel. Of the n nodes there are m attacking nodes, so each victim node only has a probability of $(1 - m/n)$ to access the channel.

1.6 FOUR ATTACK TYPES

Based on the characteristics of MANETs and the MAC protocol [8], we describe in this subsection different DDoS attack patterns and hence different attack types. In our discussions, we adopt the basic assumption that the general requirements for information security in MANET have been satisfied.Instead, our focus is on the network security aspect of MANETs. We are particularly interested in attack patterns that are sophisticated attacks designed by expert adversary and cannot be detected easily. Actually many other simple attacks are included in our modelled attacking patterns as follows. Let the set of all nodes in a MANET be S : {N1,N2, . . .Nn}, the set of attacking nodes be Sa : {Na1,Na2, . . .Nan} with Sa _ S, and the set of victim nodes be Sv : {Nv1,Nv2, . . .Nvn} with Sv _ S − Sa. In the context of DDoS, the attacking nodes include the active attacking nodes and the passive zombie nodes that are compromised by the active attacking nodes or are controlled by them to become their slaves. Here we simply refer to all of them as attacking nodes. The attacking nodes cause chaos in the channel by sending packets arbitrarily. To prevent them from being detected, they continuously change the packet size and time as well as the sending and receiving nodes. In essence, the attacking nodes complete for the channel aggressively and occupy it for a long time. As a consequence, the channel is always in a saturated state and hence the victim nodes essentially enter into a DoS status. The purpose of this attack is to consume network bandwidth and produce traffic overhead in a smart way using low attacking cost.

The direct outcome of such attack is the reduction of quality of service of the channel and localized congestion near the victim nodes. In what follows, we discuss four different attack types based on the different attacking patterns:

Pattern 1: Pulsing Attack:

A single attacking node Nai 2 Sa sends packets to a randomly selected victim node Nvi 2 Sv, with a random sending period T and a random packet size Pi.

Pattern 2: Round Robin Attack:

Multiple randomly selected attacking nodes Nai1,Nai2 . . .Nain 2 Sa send packets in sequence in a round robin manner to randomly selected victim nodes Nvj1,Nvj2 . . .Nvjn 2 Sv, with a random sending period Ti and a random packet size Pi.

Pattern 3: Self-Whisper Attack:

Two randomly selected nodes Nap ,Naq in Sa send packets to each other with a random sending period Ti and a random packet size Pi.

Pattern 4: Flooding Attack:

Multiple randomly selected attacking nodes send packets to a single victim node with a random period Ti and a random packet size Pi. The purpose of the attack is to force the victim node to decrease its communication with other nodes and eventually enter into a DoS status.

II. LITERATURE SURVEY

A. TAXONOMIES OF COUNTERMEASURES.

The authors David Karig and Ruby Lee in 2001 proposed [1] that Distributed Denial of Service (DDoS) attacks have become a large problem for users of computer systems connected to the Internet. DDoS attackers takes secondary victim systems using them to wage a coordinated large-scale attack against primary victim systems. when new countermeasures are developed to prevent or mitigate DDoS attacks, then attackers are developing new methods to circumvent these new countermeasures.In this paper, we describe about the DDoS attack models and propose taxonomies to characterize the scope of DDoS attacks, and the countermeasures are also available. These taxonomies provides similarities and patterns in different DDoS attacks,gives more generalized solutions to countering DDoS attacks and new derivative attacks.

B. DISTRIBUTED FRAMEWORK FOR DEFENDING DOS ATTACKS.

The author Rocky K. C. Chang in 2002 proposed [2] that the behavior of DoS attacks while they are affecting the stability’s of computer systems as well as exploit a distributed framework which will monitor, detect, and prevent DoS attacks. This framework includes several distributed monitors implemented at the critical components and a management center which is used to detect and prevent DoS attacks.

C. DDOS ATTACKS AND DEFENSE MECHANISMS.

The authors Christos Douligeris, Aikaterini Mitrokotsa in 2003 investigate [3] that Denial of Service (DoS) attacks constitute one of the major threats and among the hardest security problems in today Internet. a DDoS attack can easily exhaust the computing and communication resources of its victim within a short period of time. there are many defense mechanisms have been proposed to combat these attacks. for DDoS problem this paper presents a structural approach by developing a classification of DDoS attacks and DDoS defense mechanisms. the important features of each attack and defense system category are described and advantages and disadvantages of each proposed scheme are outlined. The goal of the paper the prevention of existing attack and defense mechanisms, so that a better understanding of efficient and effective algorithms, techniques and procedures to degrade these attacks may be developed.

D. USING TARGET CUSTOMER BEHAVIOR.

The authors Srikanth Kandula, Dina Katabi, Matthais Jacob and Arthur Berger in 2005 proposed [5] that, DDoS attacks also are growing in equal proportion. Sharing of information is being carried out by means of server and client. The client requests for the data from the server and the server provides the response for the client-request. Here the client can degrade the server performance by sending continuous or anomaly requests. The result is the server performance becomes degraded. This paper discusses how can we prevent the performance from degradation using some algorithm proposed in the methodology. In this work the blocking is done using a different mechanism based on the category of the client.

E. RoQ DDoS ATTACK IN MANET

The authors Ren and Dit-Yan Yeung in 2007 proposed [8] that Reduction of Quality (RoQ) attack is a new style of Distributed Denial of Service (DDoS) attack. The good put and delay performance of TCP or UDP flows are very sensitive to such RoQ attacks. In this paper, we study about congestion-based RoQ DDoS attacks in mobile ad-hoc networks. we also study about the attacking principles based on analysis of the network capacity and classify these attacks into four categories: 1st is pulsing attack, 2nd is round robin attack, 3rd is self-whisper attack, and 4th is flooding attack. We then propose a defense scheme that includes both the detection and response mechanisms. The detection signals uses the frequency of receiving RTS/CTS packets, frequency of sensing a busy channel, Through extensive ns2 net- work simulations, we demonstrate the existence of high good put and delay jitters under the pulsing attack mode. Increase in delay (by 110 times under five attacking flows) and decrease in good put (to 77% under five attacking flows) can be observed especially when more attacking flows occurs..

F. DDoS ATTACK IN WIRELESS AD HOC NETWORKS

The author S.A.Arunmozhi proposed [9] that The wireless ad hoc networks are highly vulnerable to distributed denial of service(DDoS) attacks because of its unique characteristics. These attacks reduce the quality of service (QoS) to end systems gradually rather than refusing the clients from the services completely. In this paper, we discussed about the DDoS attacks and proposed a defense scheme to improve the performance of the ad hoc networks. Our defense mechanism uses the medium access control (MAC) layer information to detect the attackers. when the attackers are identified, then all the packets will be blocked. The network resources are available to the legitimate users. we proved that our proposed system improves the network performance.

G. WIRELESS MANET

The author Prajeet Sharma in 2012 proposed [10] that Wireless Mobile ad-hoc network (MANET) is an emerging technology and have great strength to be applied in critical situations like battlefields and commercial applications. MANET has no infrastructure, with no any centralized controller exist and also each node contain routing capability, In MANET each device can independently move in any direction. So most important challenges in wireless mobile ad-hoc networks face today is security. MANETs are a type of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. Ad hoc contains a sensor network so the problems is facing by sensor network is also faced by MANET. There are many security attacks in MANET and DDoS (Distributed denial of service) is one of them. with these parameters and many more also we build secure IDS to detect this kind of attack. In this paper we discussed about attacks on MANET and DDOS also and provide the security against the DDOS attack.

H. USING NEW CRACKING ALGORITHM

The author V.Priyadharshini in 2012 proposed [11] that In the modern computer world, Some interrupts may occur on the local system or network based systems. Without security measures our data might be subjected to an attack. One common method of attack involves sending enormous amount of request to server or site and server will be unable to handle the requests and site will be offline for some days or some years depends upon the attack called distributed denial of service attack. In this paper a new cracking algorithm is implemented to stop that DDOS attacks. In our algorithmic design a practical DDOS defense system that can protect the availability of web services during severe DDOS attacks. The proposed system identifies whether the number of entries of client exceeds more than five times to the same sever, then the client will be saved as a attacker in blocked list and the service could not be provided. So our algorithm protects legitimate traffic from a huge volume of DDOS traffic when an attack occurs.

I. IP BROADCAST USING DISABLE TECH.

The author Mukesh kumar in 2013 proposed [14] that Ad-hoc network is the network comprised of wireless nodes. It has no any infrastructure which is self configured. MANET is accessible to both legitimate network users and malicious attackers. one of the main purpose in MANET is to design the robust security solution that can prevent MANET from various DDOS attacks. different cryptographic techniques have been proposed to countermeasures these attacks against MANET. These techniques are not suitable for MANET resource constraints, because they introduced heavy traffic load to exchange. Therefore ad hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions. Distributed Denial of Service (DDoS) attacks has also become a problem for users of computer systems connected to the Internet. In this paper, a technique is used that can prevent a specific kind of DDoS attack. The scheme is distributed in nature it has the capability to prevent Distributed DoS (DDoS) attack. The performance of the scheme in a series of simulations shows that the proposed scheme provides a better solution than existing schemes.

J. A NOVEL SOLUTION TO NULLFY DDoS ATTACK

The author Ranju in 2014 proposed [15] that Distributed Denial of Service (DDoS) attacks in the networks needs to be prevented or handled if it occurs, as soon as possible. DoS attacks is difficult due to their properties such as dynamic attack rates, big scale of botnet , various kinds of goals, etc. Distributed Denial of Service (DDoS) attack is hard to deal with because when the traffic is coming at a different rate from disseminated sources. DDoS attack creates more problems if it occurs in wireless network because of the properties of ad hoc network. There- fore, it is better to prevent the distributed denial of service attack rather than allowing it to occur and then taking the necessary steps to handle it. In this paper the author proposed to handle DDoS attacks in mobile ad hoc networks (MANETs).

TABLE

AUTHOR	YEAR	PREVENTION & DETECTION TECH.	FINDINGS
David Karig and Ruby Lee [1].	In 2001	Taxonomies of Attacks, Tools and Counter-measures	DDoS attacks make a networked system or service unavailable to legitimate users.
Rocky K. C. Chang [2].	In 2002	distributed framework used to detect and defend DoS attacks	Author proposed a distributed framework which could be used to detect and prevent DoS attacks.
Christos Douligeris , Aikaterini Mitrokotsa [3].	In 2003	defense mechanisms are used for better understanding of DDoS attacks	Author tried to achieve a clear view of the DDoS attack problem and find more effective solutions to the problem.
Srikanth Kandula, Dina Katabi [5].	In 2005	Prevention of attacks using target customer behaviour	Authors proposed an efficient method-ology to prevent the attack on server performance and to improve the reliability on the clients.
Wei Ren and Dit-Yan Yeung [8].	In 2007	Reduction of quality(ROQ) is a new style used for distributed denial of service (DDoS)	congestion-based RoQ DDoS attacks in MANETs and detection scheme that monitors three MAC layer signals and a response scheme based on ECN marking.
S. A. Arunmozhi [9].	In 2011	bandwidth depletion attack	Author discussed the DDoS attacks and proposed a defense scheme to mitigate the attack in wireless ad hoc networks.

III. CONCLUSION

Denial of service attack uses a distributed framework which could be used to detect and prevent the legitimate use of service. Different techniques of DoS attack in MANET have been review. Aim of this attack is tried to achieve a clear view of the DDoS attack problem and find more effective solution to the problem. DDoS attack make a networked system or service available to legitimate users and uses multiple machines for prevent the resources and gives a defense scheme to mitigate the attack in wireless Adhoc networks.

REFERENCES

[1] David Karig and Ruby Lee, “Remote Denial of Service Attacks and Countermeasures,” Princeton University Department of Electrical Engineering Technical Report CEL2001-002, Oct 2001.

[2] Rocky K. C. Chang, “Defending against flooding-based distributed denial of service attacks: a tutorial,” IEEE Communication Magazine, vol. 40, no. 10, pp. 42-51, Oct. 2002.

[3] Christos Douligeris , Aikaterini Mitrokotsa “DDoS attacks and defense mechanisms: classification and state-of-the-art” Department of Informatics accepted 13 october 2003.

[4] Stephen M. Specht “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures” *International Journal of Advanced Research in Computer Science and Software Engineering* Sep. 2004.

[5] Srikanth Kandula, Dina Katabi, Matthais Jacob and Arthur Berger, “Surviving Organized DDoS Attacks that Mimic Flash Crowds”, NSDI'05 Proceedings of the 2^{nd} conference on Symposium on Networked Systems Design & Implementation, 2005, Vol.2.

[6] Zhenhai Duan, Xin Yuan and Jaideep Chandrashekar, “Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates”, 25th IEEE International Conference on Computer Communications. Proceedings 2006.

[7] Kamanshis Biswas and Md. Liakat Ali; Security Threats in Mobile Ad Hoc Network; Master Thesis; Thesis no: MCS- 2007:07; March 22, 2007.

[8] Wei Ren and Dit-Yan Yeung "Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks" International Journal of Network Security, Vol.4, No.2, PP.227-234, Mar. 2007.

[9] S.A.Arunmozhi "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.

[10] Prajeet Sharma " A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network" International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012.

[11] V. Priyadharshini " Prevention of DDOS Attacks using New Cracking Algorithm" Vol. 2, Issue 3, May-Jun 2012, pp.2263-2267.

[12] Kaspersky (2012). Kaspersky Internet Security & Anti-virus. http://www.kaspersky.com/. Russian Federation.

[13] A.Anna lakshmi " Defending MANETs against the DDoS Attacks" International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 9, September 2012.

[14] Mukesh kumar "DETECTION AND PREVENTION OF DDOS ATTACK IN MANET'S USING DISABLE IP BROADCAST TECHNIQUE" International Journal of Application or Innovation in Engineering & Management (IJAIEM). Volume 2, Issue 7, July 2013.

[15] RANJU "A Novel Solution to Nullify DDOS Attack in MANET" Vol. 2, Issue VI, June, 2014.