ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Research Article

A STUDY AND AN ANALYSIS TO MITIGATE DISTRIBUTED DENIAL OF SERVICE ATTACKS IN MOBILE AD-HOC NETWORK

Karthikeyan Thyagarajan*, Arunkumar Thangavelu
School of Computing Science and Engineering, VIT University, Vellore-14, Tamil Nadu, India.
Email:tknvlr@gmail.com

Received on 12-05-2016 *Accepted on 05-06-2016*

Abstract

Mobile ad hoc networks (MANETs) are dynamic mobile networks that can be formed in the absence of any pre-existing communication infrastructure. In addition to node mobility, a MANET is characterized by limited resources such as bandwidth, battery power, and storage space. The underlying assumption in MANETs is that the intermediate nodes cooperate in forwarding packets. However, this assumption does not hold in commercial and emerging civilian applications. MANETs are vulnerable to Denial of Service (DoS) due to their salient characteristics. In this paper, a resource pricing mechanism is proposed for mitigating DDoS attacks. DDoS attacks committed by selfish and malicious nodes were investigated. Our scheme motivates nodes to cooperate and excludes them from the network only if they fail to do so. We evaluated the performance of our scheme using NS-2 simulator and the packet delivery ratio, the routing and communication overhead, and misbehaving node detection in a discrete event-simulation environment. The results indicate that the resource pricing mechanism can significantly reduce the effect of DDoS attacks and improve performance in MANETs.

Keywords: Ad-hoc Networks, Mobile Networks, Distributed Denial of Services, DDoS, Security, Botnet.

Introduction

A DDoS attack [1, 2] is any event that diminishes or eliminates a network's capacity to perform its expected function. These attacks are launched against server resources or network bandwidth by preventing authorized users from access ingresources. They pose threats to larger websites such as Amazon and eBay. The effect of these attacks varies from temporarily blocking service availability to permanently distorting in formation in the network. DoS attacks can target a client computer or a server computer. For example, an attack may target a system by exhausting limited wireless resources such as bandwidth, storage space, battery power, CPU, or system memory. Networks and applications can be attacked by modifying routing information or changing system configuration, thereby directly attacking data integrity. DoS attack packets may use spoofed IP addresses, and can occur indifferent forms including buffer overflow, TCP SYN flooding, Smurf, or Viruses. For example, in TCP SYN flooding, an attacker sends multiple connection requests to a victim, exhausting all of the victim's resources and preventing use by legitimate users. The emergence of new low detection rate DoS attacks, such as low-rate TCP-targeted DoS attacks [8], brings new challenges to the network services.

In MANETs, nodes act as both routers and ordinary nodes. Due to dynamic network topology and lack of centralized infrastructure, network security has brought a new challenge to networking communities. Unlike traditional networks, MANETs are more vulnerable to DoS attacks due to limited resources that force nodes to be greedy in resource utilization. When there is no cooperation, activities of even a small number of nodes may significantly decrease the performance of the network. For example, a misbehaving node that discards any packets passing through it can result in repeated retransmissions, which in turn cause network congestions. Also, a wireless link does not provide the same protection for data transmissions as does its wired link counter-part. Hence, any user or receiver within the transmissions range can eavesdrop or interfere with data packets or routing information. Battery power is another critical resource for mobile nodes. If the battery power has been used up due to malicious attacks such as the sleep deprivation attack, the victim will not be able to provide network services. Since all nodes can be mobile, changes in network connectivity and resource availability also expose a network to various attacks. This calls for detection and prevention of attacks in the network. Some intrusion prevention measures, such as cryptograph and authentication, can reduce the threats against MANETs. However, these mechanisms either cause greater overhead and latency or cannot defend against malicious internal nodes. The deployment of a Public Key Infrastructure (PKI) requires certification authority, but such an entity must always be available. Most current research on MANET, [3, 4] security focuses mainly on secure routing. Enforcing cooperation among nodes is one of the strategies for tackling security and improving MANET performance. Popular web-based services such as Amazon and eBay use reputation rating systems for buyers and sellers to rate each other; however, this mechanism relies on a centralized server to store and manage data. In eBay's reputation system, buyers and sellers can rate each other after each service, and the overall reputation of a participant is computed as the sum of these ratings over a period of months. The central location that provides reputation information is usually a server with high computational and storage capability.

Although MANETs are based on the fundamental assumption[5, 6] that the nodes will cooperate in providing services or sharing available resources, non-cooperation is a critical problem when deploying these networks for civilian applications. Lack of cooperation in MANETs can be a result of misbehaving nodes or lack of sufficient resources. Misbehaving nodes can either be malicious or selfish. Selfish nodes are nodes that participate in the network to maximize their own benefit by using network resources while saving their own resources. Malicious nodes directly attack a network by disrupting its normal operation. The absence of a trusted third party in ad hoc networks necessitates the development of protocols for collecting, storing, and distributing reputations. Enhancing cooperation among nodes in the network can help in detecting and mitigating DoS attacks caused by the misbehaving nodes.

Classification of Mobile Ad-Hoc networks and Attack Scenarios

Based on the composition of nodes that form a network, ad hoc networks can be classified into two main categories, cooperative and non-cooperative. In the first category, cooperative, nodes form networks based on common goals to achieve certain objectives. Examples are networks that can be formed in emergency relief operations, collaborative data processing, military applications, entertainment, and conference sessions. In this scenario all members of the group have common objectives, and therefore they cooperate. In the second category, a network is formed to establish communication in civilian environments. There is no reason for mutual cooperation. While the nodes in a network used by the soldiers in a battlefield or disaster recovery area can be assumed to cooperate, there is no good reason to assume that networks formed by civilians with diverging goals and interests will cooperate. Such a network can be formed by a group of people who want to communicate by establishing a temporary networking environment. Each user’s objective is usually to maximize his own benefit, and hence the network may suffer from misbehaving nodes that may want to save theirown resources while using other nodes for packet forwarding. Itseems appropriate to use a mechanism that encourages cooperation in non-cooperating networks to improve network performance.

Non-cooperation in MANETs occurs due to misbehaving nodes [7, 8] and lack of resources in non-misbehaving nodes. In the non-cooperation due to misbehaving nodes scenario, nodes fail to cooperate due either to malicious behaviour or selfishness to maximize their own benefits. In non-cooperating scenarios, anode may promise to forward a packet but fail to do so, or may not be willing to forward packets to save its resources. In both scenarios, network services can be degraded due to lack of cooperation among the nodes. We consider this type of non-cooperation in our study. In the non-cooperation due to lack of resources scenario, nodes fail to cooperate due to lack of sufficient resources. This resource shortage may occur as a result of wireless network characteristics (limited memory, bandwidth, or energy) or environmental conditions (unreliable connectivity or network load). This category of non-cooperative behaviour is called reasonable non-cooperation. The main issue that requires attention here is load balancing, which is required to distribute the network load equally among the nodes.

DoS Attack Scenarios

The DoS attacks that target resources can be grouped into three broad scenarios. The first attack scenario targets Storage and Processing Resources. This is an attack that mainly targets the memory, storage space, or CPU of the service provider. Consider the case where a node continuously sends an executable flooding packet to its neighbourhoods and to over load the storage space and deplete the memory of that node. This prevents the node from sending or receiving packets from other legitimate nodes. Neighbourhood watch and monitoring can prevent the occurrence of such events by gradually excluding such malicious nodes. The second attack scenario targets energy resources, specifically the battery power of the service provider. Since mobile devices operate by battery power, energy is an important resource in MANETs. A malicious node may continuously send a bogus packet to a node with the intention of consuming the victim's battery energy and preventing other nodes from communicating with the node. The use of localized monitoring can help in detecting such nodes and preventing their consequences. he third attack scenario targets bandwidth. Consider the case where an attacker located between multiple communicating nodes wants to waste the network bandwidth and disrupt connectivity. The malicious node can continuously send packets with bogus source IP addresses of other nodes, there by overloading the network. This consumes the resources of all neighbours that communicate, overloads the network, and results in performance degradations. Such attacks can be prevented based on the reputation information exchanged among the involved nodes or the cluster head. We attempt to prevent both selfish and malicious nodes from degrading network performance by providing incentives to encourage cooperation and punishing nodes that do not cooperate.

Non-cooperative nodes in MANETs can degrade network performance through security threats including DoS attacks. Stimulating cooperation is an important measure in defending against attacks generated by misbehaving nodes. Attacks can be either active or passive. Active attacks can modify data, disrupt network operation, or disable services, while passive attacks do not alter data but fail to cooperate in providing services such as routing and packet forwarding. Active attacks on network routing include flooding, modifying routing information, providing false route requests and replies, attracting unexpected traffic, hiding error messages, and fabricating false error messages.

Passive attacks include packet dropping to conserve resources. These abnormal node behaviours result in performance degradation and cause denial of service attacks, packet losses, longer delays, and low throughput. The effect of DoS attacks on MANETs can be serious, and the prevention and detection of these attacks is more difficult than in their wired counterparts. Like other networks, the security requirements in ad hoc networks include services such as availability, authentication, non-repudiation, confidentiality, integrity, and access control. The limited processing and storage capability, bandwidth, and battery power of mobile devices prevent the implementation of complex algorithms in tackling attacks against MANETs. Moreover, due to the absence of a central entity for security management, unreliable links, and frequent membership changes, attacks from internal nodes are difficult to detect or prevent using existing security mechanisms. Due to the absence of a fixed infrastructure for key management, centralized monitoring is impossible in MANETs. Reputation-based incentives can help in establishing more cooperative behaviour among non-cooperative nodes. A suitable security management system in this environment is a distributed mechanism where each node maintains local information, thereby incurring lower communication and computation overhead. We use clustering architecture to provide a localized monitoring mechanism to detect malicious nodes and improve the scalability of the proposed mechanism.

The Rest of the paper is organized as follows: Section 2 describes related work; Section 3 presents Overview of DDoS attacks. Section 4 describes Overview of MANET, Section 5 deals with the Various Defense Mechanisms, Section 6 describes about the proposed defense method, Section 7 discusses the performance evaluation based on simulation experiments, and Section 8 presents Results and Discussion and Section 9 Concludes the paper.

Related Work

Lu Han [6] describes that the wireless ad-hoc networks were first unfolded in 1990s. Mobile ad-hoc networks have been widely researched for many years. Mobile ad hoc networks are collection of two or more devices equipped with wireless communications and networking capability The Wireless ad hoc Networks do not have a gateway rather every node can act as the gateway. Although, lots of research is done in this field, but the question is often raised, whether the architecture of mobile ad-hoc networks is a fundamental flawed architecture.

Antonio Challita, Mona El Hassan, Sabine Maalouf and Adel Zouheiry [7] describe different types of DDoS attacks, present recent DDoS defense methods as published in technical papers, and propose a novel approach to counter DDoS. Based on common defense principles and taking into account the different types of DDoS attacks, this paper survey defense methods and classify them according to several criteria. This paper proposes a simple-to-integrate

DDoS victim based defense method, Packet Funneling, which aims at mitigating an attack's effect on the victim. In this approach, heavy traffic is funnelled before being passed to its destination node, thus preventing congestion at the nodes access link and keeping the node on-line. This method is simple to integrate, requires no collaboration between nodes, introduces no overhead, and adds slight delays only in case of heavy network loads. The proposed packet funneling approach promises to be a suitable means of coping with DDoS traffic, with easy integration at minimal cost in Framework for Statistical Filtering against DDoS Attacks in MANETs Hwee-Xian Tan and Winston K. G. Seah [8] describes that A DDoS (Distributed Denial-Of- Service) attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated. There are many proposed methods in the literature which aim to alleviate this problem; such as hop-count filtering, rate-limiting and statistical filtering. However, most of these solutions are meant for the wired Internet, and there is little research efforts on mechanisms against DDoS attacks in wireless networks such as MANETs. This paper gives information about the vulnerability of MANETs to DDoS attacks and provide an overview of statistical filtering, which is commonly used as a security mechanism against DDoS attacks in wired networks and then propose a framework for statistical filtering in MANETs to combat DDoS attacks. This paper also simulates some DDoS attacks in MANETs without any filtering mechanisms to explore and understand the effects of such attacks on the performance of the network.

In Defeating Distributed Denial of Service Attacks Xianjun Geng and Andrew B. Whinston [9] describes that the notorious, crippling attack on e-commerce top companies in February 2000 and the recurring evidence of active network scanning a sign of attackers looking for network weaknesses all over the Internet are harbingers of future Distributed Denial of Service (DDoS) attacks. They signify the continued dissemination of the evil daemon programs that are likely to lead to repeated DDoS attacks in the foreseeable future. This paper gives information about network weaknesses that DDoS attacks exploit the technological futility of addressing the problem solely at the local level, potential global solutions, and why global solutions require an economic incentive framework.

On the effectiveness of DDoS Attacks on Statistical Filtering Qiming Li, Ee-Chien Chang and Mun Choon Chan [11], describes that Distributed Denial of Service (DDoS) attacks pose a serious threat to service availability of the victim network by severely degrading its performance. There has been significant interest in the use of statistical-based filtering to defend against and mitigate the effect of DDoS attacks. Under this approach, packet statistics are monitored to classify normal and abnormal behaviour. Under attack, packets that are classified as abnormal are dropped by the filter that guards the victim network. This paper gives the effectiveness of DDoS attacks on such statistical-based filtering in a general context where the attackers are “smart”. We first give an optimal policy for the filter when the statistical behaviours of both the attackers and the filter are static. Next, this paper considers cases where both the attacker and the filter can dynamically change their behavior, possibly depending on the perceived behavior of the other party. This paper observes that while an adaptive filter can effectively defend against a static attacker, the filter can perform much worse if the attacker is more dynamic than perceived.

Kamanshis Biswas [12] mentioned that Mobile Ad Hoc Network (MANET) was a collection of communicating devices or nodes that wish to communicate without any fixed infrastructure. The nodes in MANET themselves are responsible for dynamically finding out other nodes in the network to communicate. Although an ad-hoc network is used for commercial uses due to their certain unique characteristics, but the main challenge is the vulnerability to security attacks. A number of challenges like dynamic network topology, stringent resource constraints, shared wireless medium, open peer-to-peer net-work architecture, etc., are posed in MANET. As MANET is widely spread for the property of its Capability in forming temporary network without any fixed infrastructure or centralized topology, security challenges have become a leading concern to provide secure communication.

Andrim Piskozub [13] gives principal types of DoS attacks, which flood victim’s communication channel band-width, is carried out their analysis and are offered methods of protection from these attacks. The DDoS attacks are considerably more effective than their DoS counter parts because they allow performing such attacks simultaneously from several sites that make this attack more efficient and complicate searches of an attacker. The attacker uses the client program, which, in turn, interacts with the handler program. The handler sends commands to the agents, which perform actual DoS attacks against an indicated system-victim. This paper also describes various countermeasures that should be taken to prevent the net- work from DDoS attack.

Xianjun Geng [4] describe that the notorious, crippling attack on e-commerce’s top companies in February 2000 and the recurring evidence of active network scanning, a sign of attackers looking for network weaknesses all over the Internet, are harbingers of future Distributed Denial of Service (DDoS) attacks. They signify the continued dissemination of the evil daemon programs that are likely to lead to repeated DDoS attacks in the foreseeable future. This paper gives information about the weaknesses in the network that DDoS attacks exploit the technological futility of addressing the problem solely at the local level.

Vicky Laurens et al[15], describe that due to financial losses caused by Distributed Denial of Service (DDoS) attacks; most defense mechanisms have been deployed at the network where the target server is located. This paper believes that this paradigm should change in order to tackle the DDoS threat in its basis: thwart agent machine's participation in DDoS attacks. Paper consists of developing an agent to monitor the packet traffic rate (outgoing packets/incoming packets). The deployment is based upon characterizing TCP connections; normal TCP connections can be characterized by the ratio of the sent packets to the received packets from a given destination. The result shows that the traffic ratio values usually give larger values at the beginning of the run when there are not enough packets to make a decision that whether or not the traffic is legitimate. A low value for threshold allows for faster detection of attack, but also increases the false-positives.

Stephen M. Specht [16] describes that Distributed Denial of Service (DDoS) attacks has become a large problem for the systems connected to the Internet. DDoS attackers take control over secondary victim systems and use them to launch a coordinated large-scale attack against primary victim systems. As a result of fresh counter measures that are developed to prevent or mitigate DDoS attacks, attackers are constantly developing brand new methods to cheat on these unused countermeasures. This paper also gives us information about DDoS attack models and proposed taxonomies to characterize the DDoS attacks, the software attacking tools used, and the possible countermeasures those are available. The taxonomy shows the similarities and patterns in different DDoS attacks, including new derivative attacks. It is essential, that as the Internet and Internet usage expand, more comprehensive solutions and countermeasures to DDoS attacks be developed, verified, and implemented more effectively and precisely. Thus, this paper describes that DDoS attacks make a networked system or service unavailable to legitimate users. These attacks are an annoyance at a minimum, or can be seriously damaging if a critical system is the primary victim. Loss of network resources causes economic loss, work delays, and loss of communication between network users. Solutions must be developed to prevent these DDoS attacks.

Qiming Li [17] mentions that Distributed Denial of Service (DDoS) attacks posed a serious threat to service availability of the victim network by severely degrading its performance. There has been significant interest in the use of statistical-based filtering to defend against and mitigate the effect of DDoS attacks. Under this approach, packet census is monitored to classify normal and unusual behavior. Under attack, packets that are classified as unusual are dropped by the filter that guards the victim network. This paper gives the effectiveness of DDoS attacks on such statistical-based filtering in a general context where the attackers are smart. They first give an optimal policy for the filter when the statistical behaviors of both the attackers and the filter are static. Next, this paper considers cases where both the attacker and the filter can dynamically change their behavior, possibly depending on the perceived behavior of the other party.

Antonio Challita [7] describes different types of DDoS attacks, present recent DDoS defense methods and proposed a unique approach to handle DDoS attack. Based on common defense principles and taking into account a number of DDoS attacks, the author finds out many defense methods and categorizes them according to a number of criteria. This paper proposes a simple-to integrate DDoS victim based defense method, Packet Funneling, whose main aim is to mitigate the effect of attack on the victim. In this approach, massive traffic is checked before being passed to its destination node, thus preventing congestion in the network. This method is simple to integrate, re- quires no association between nodes, causes no overhead, and adds delays only in case of massive network loads. The proposed packet funnelling approach promises to be a suitable means of coping with DDoS traffic, with easy integration at lesser cost.

Malicious flooding attacks are the lethal attacks on mobile ad-hoc networks. These attacks can severely occlude an entire network. To defend against these at- tacks, the authors propose a novel defense mechanism in mobile ad-hoc networks. The proposed scheme increases the number of legitimate packet processing at each node and thus improves the end-to-end packet delivery ratio.

From the above literature survey, it is being concluded that the most of the works carried out in DDoS defense has concentrated either individually on Prevention or Detection. So there is no technique where integration of these approaches is available. So aresource pricing approach is being present to defense against DDoS attacks in MANET’s.

Overview of Distributed Denial of service Attacks

A DDoS (Distributed Denial-Of-Service) attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated. The distributed format adds the “many to one” dimension that makes these attacks more difficult to prevent. A distributed denial of service attack is composed of four elements, as shown in Figure 1.First, it involves a victim, i.e., the target host that has been chosen to receive the brunt of the attack. Second, it involves the presence of the attack daemon agents. These are agent programs that actually conduct the attack on the target victim. Attack daemons are usually deployed in host computers. These daemons affect both the target and the host computers. The task of deploying these attack daemons requires the attacker to gain access and infiltrate the host computers. The third component of a distributed denial of service attack is the control master program. Its task is to coordinate the attack. Finally, there is the real attacker, the mastermind behind the attack. By using a control master program, the real attacker can stay behind the scenes of the attack. The following steps involved during a distributed attack:

1. The real attacker sends an “execute” message to the control master program.

2. The control master program receives the “execute” message and propagates the command to the attack daemons under its control.

3. Upon receiving the attack command, the attack daemons begin the attack on the victim.

A distributed denial of service attack is composed of four elements. First, it involves a victim, i.e., the target host who has been chosen to receive the brunt of the attack. Second, it involves the presence of the attack daemon agents. These are agent programs that actually conduct the attack on the target victim. Attack agents are usually installed on host computers. These attacker agents or the secondary victims affect both the target and the host computers [19-22].

Distributed Cooperative Architecture of DDoS Attacks

Before real attack traffic reaches the victim; the attacker must communicate with all its DDoS agents. Therefore, there must be control channels present in between the agent machines and the attacker machine. This cooperation between the two requires all agents to send traffic based on the commands received from the attacker.

The attack network consists of the three components: attacker, agents, and control channels. In attack, networks are divided into three types: the agent-handle model, the Internet Relay Chat (IRC) based model and the reflector model [20, 23].

The agent-handler model consists of three components: attacker, handlers, and agents. Figure 2 illustrates the typical architecture of the agent handler model. The main attacker sends control messages to the previously compromised agents through a number of handlers, guiding them to produce unwanted traffic to send it to the victim [2].

The only difference between the architecture of IRC- based model, and the agent-handler model is in the former case. An IRC communication channel is used to connect the main attacker to agent machines [23, 24], which is shown in Figure 3.

In the attack network architecture of the reflector model, the reflector layer creates a major difference from the basic DDoS attack architecture. In the request messages, the agents change the source address field in the IP header to the victim's address and thus replace the real agents' addresses. Then, the reflectors will in turn generate response messages to the victim.

As a result, the flooding traffic that finally reaches the victim computer or the victim network is not from a few hundred agents, but from a million reflectors. An exceedingly diffused reflector based DDoS attack raises the bar for tracing out the real attacker by hiding the attacker behind a large number of reflectors [24].

DDoS Attack Taxonomy

There is a wide variety of DDoS attacks [22]. There are two types of DDoS attacks, they are: Active and passive attack. Packet dropping is a type of passive attack in which node drops some or all of data packets sent to it for further forwarding even when no congestion occurs.

There are two main classes of DDoS attacks: bandwidth depletion and resource depletion attacks. The classification of various DDoS attacks is shown in the Figure 4.

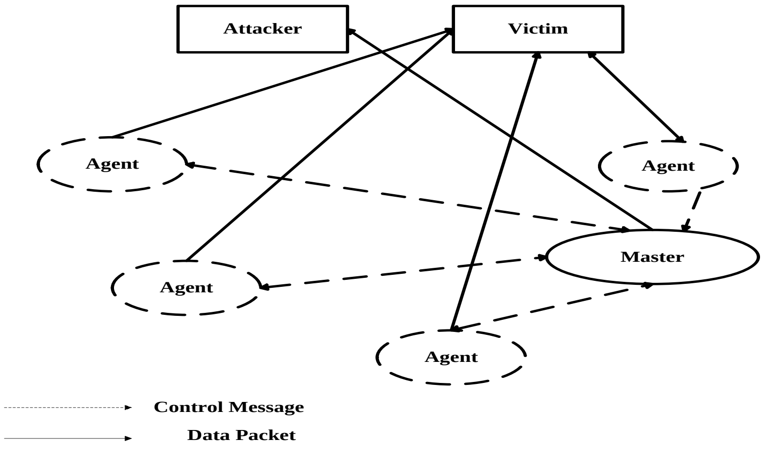

Figure 1: DDoS attack components.

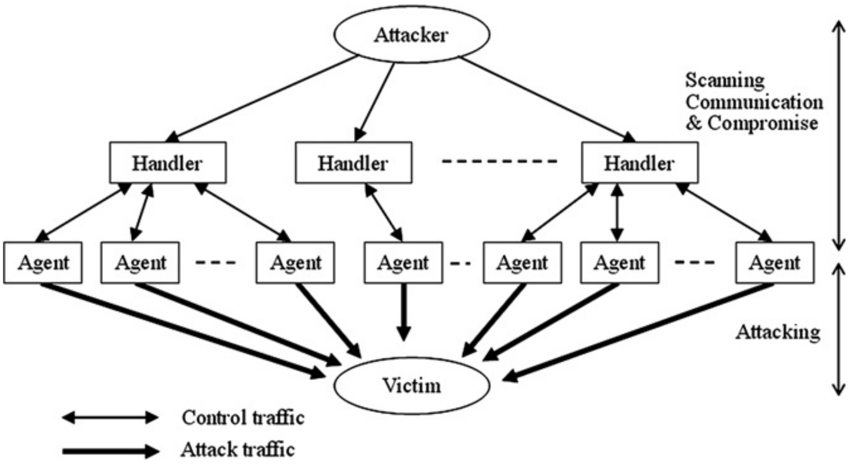

Figure 2: Typical DDoS architecture (the agent handler model).

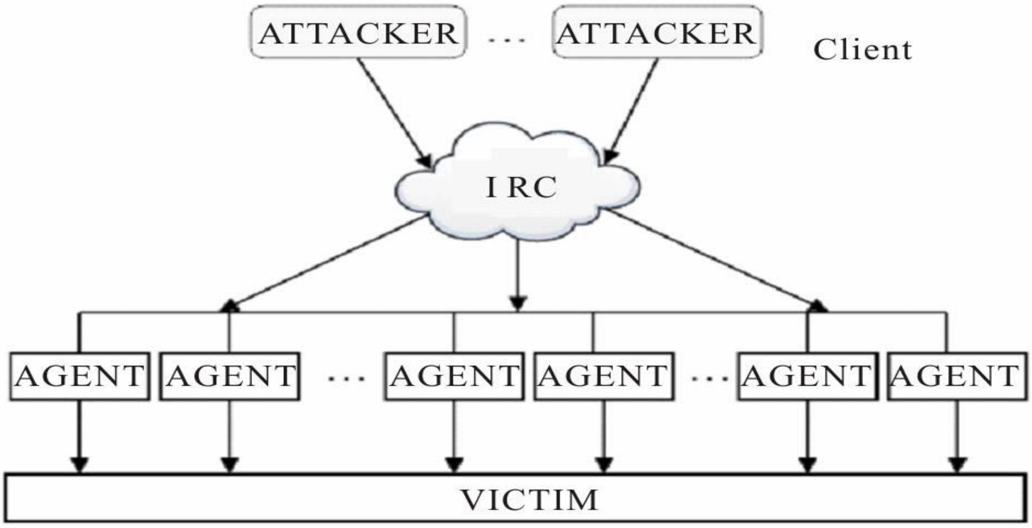

Figure 3: Architecture of IRC based DDoS attack.

Bandwidth Depletion Attacks

A Bandwidth Depletion Attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the primary victim. Bandwidth depletion attacks can be characterized as flood attacks and amplification attacks [25, 26].

Flood Attack

In a flood attack, zombies send a large volume of traffic to a victim's system, to congest the victim systems network bandwidth with IP traffic. The victim systems slow down, crashes, or suffer from saturated network bandwidth, thereby preventing access by an authorized user. Flood attacks can be launched using both UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol) packets [27].

In a UDP Flood attack, a large number of UDP packets are sent to either random or specified ports on the victim system. The victim system tries to process the incoming data to determine which applications have re- quested data. If the victim system is not having any applications on the targeted port, it will send an ICMP packet to the sending system indicating a ‘destination port unreachable’ message [28].

Often, the attacking DDoS tool will also spoof the source IP address of the attacking packets. This helps the secondary victims in hiding their identity since return packets from the victim system are not sent back to the zombies, but are sent back to the spoofed addresses. UDP flood attacks may also fill the bandwidth of connections located on the victim system.

An ICMP flood attack is initiated when the zombies send a huge number of ICMP_ECHO_REPLY packets (“ping”) to the victim system. These packets flag the victim system to reply to this message, and the combination of traffic saturates the bandwidth of the victim’s network connection. During this attack, the source IP address of the ICMP packet may also be spoofed [29, 30].

Amplification Attacks

In amplification attack the attacker or the zombies send messages to a broadcast IP address, using this to cause all systems in the subnet reached by the broadcast address to send a reply to the victim system. The broadcast IP address feature is found on most routers; when a sending system specifies a broadcast IP address as the destination address, the routers replicate to send the broadcast message directly, or use the agents to send the broadcast message to increase the volume of attacking traffic. If the attacker decides to send the broadcasting message directly, this attack helps the attacker with the ability to use the systems within the broadcast network as zombies without any need to install any agent software [2]. A DDoS Smurf attack is a type of an amplification attack where the attacker sends packets to a network amplifier, with the return address changed to the victim’s IP address.

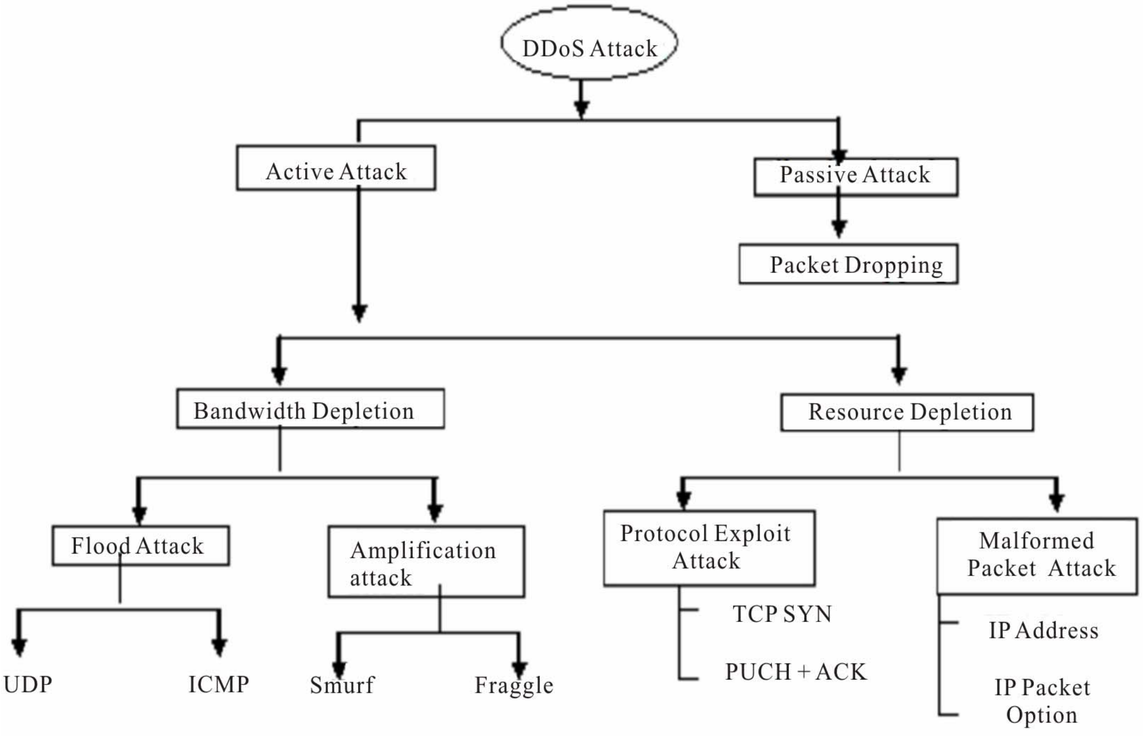

Figure 4: DDoS attack taxonomy.

Resource Depletion Attacks

A Resource Depletion Attack is an attack that is designed to tie up the resources of a victim's system making the victim unable to process legitimate requests for service. DDoS resource depletion attacks involve the attacker sending packets that misuse network protocol communications or are malformed. Network resources are tied up so that none are left for legitimate users [31, 34].

Protocol exploits Attacks

We give two examples, one misusing the TCP SYN (Transfer Control Protocol Synchronize) protocol, and the other misusing the PUSH + ACK protocol.

In a DDoS TCP SYN attack, the attacker gives instructions the zombies to send tons of TCP SYN requests to a victim server to tie up the server's processor re- sources, and hence prevent the server from responding to the requests from legitimate users. The TCP SYN attack exploits the three-way handshake between the sending machine and the receiving machine by sending a huge number of TCP SYN packets to the victim system with changed source IP addresses, so the victim system responds to a non requesting system with the ACK + SYN. When a large volume of SYN requests is being processed by a server and none of the ACK + SYN responses are returned. The server eventually runs out of the computing resources such as the processor and memory re- sources, and is unable to respond to legitimate users [31].

In a PUSH + ACK attack, the attacking agents send TCP packets with the PUSH and ACK bits set to one. These trigger in the TCP packet header instruct the victim system to unload all data in the TCP buffer and send an acknowledgement message when complete. If this process is repeated with a number of agent machines, the receiving system cannot process the large volume of in- coming packets, and the victim system will eventually crash.

Malformed Packet Attacks

A malformed packet attack is an attack where the attacker instructs the zombies to send incorrectly formed IP packets to the victim system in order to crash it. There are at least two types of malformed packet attacks [2, 31].

In an IP address attack, the packet contains the same source and destination IP addresses. This can confuse the victim system and can cause it to crash. In an IP packet option's attack, a malformed packet may randomize the optional fields within an IP packet and set all quality of service bits to one so that the victim system must use additional processing time to analyze the traffic. If this attack is multiplied, it can exhaust the processing ability of the victim system [2, 33].

DDoS Attack Mechanism

As one of the major security problems in the current Internet, a denial-of-service (DoS) attack always attempts to prevent the victim from serving legitimate users. A distributed denial-of-service (DDoS) attack is a DoS attack which relies on multiple compromised hosts in the network to attack the victim. There are two types of DDoS attacks. The First type of DDoS attack aims at attacking the victim node to drop some or all the data packets for further forwarding even when there is no congestion in the network, is known as Malicious Packet Dropping-based DDoS attack [32].

The second type of DDoS attack is based on a huge volume of attack traffic, which is known as a Flooding-based DDoS attack [36].

A flooding-based DDoS attack tries to clog the victim's network bandwidth and other resources with real-looking but unwanted IP data. As a result of which, the legitimate IP packets cannot reach their destination node.

To amplify the effects and hide real attackers, DDoS attacks can be run in two different distributed and parallel ways. In the first one, the attacker compromises a number of agents and manipulates the agents to send attack traffic to the victim node. The second method makes it even more difficult to determine the attack sources because it uses reflectors.

For example, a Web server can be reflector because it will return an HTTP response packet after receiving an HTTP request packet. The attacker sends request packets to servers and fakes victim's address as the source address. Therefore, the servers will send back the response packets to the real victim. If the number of reflectors is large enough, the victim network will suffer exceptional traffic congestion [33].

Issues in DDoS Attacks

DDoS attack is an attempt to make a computer resource inaccessible to its legitimate users.

- The bandwidth of the Internet and an LAN may be consumed unwontedly by DDoS, by which not only the intended computer, but also the entire network suffers.
- Slow network performance (opening files or accessing web sites) due to DDoS attacks.
- Unavailability and inability to access a particular web site due to DDoS attacks.

  Why out-dated anti-DDoS solutions that base their protection on rate limitation methods cannot address this challenge. Because the rate limit mechanism is based on a pre-defined, static threshold of traffic and has two main drawbacks:

- It does not mitigate attacks until the attack traffic reaches the predefined threshold. This results in slow detection of attacks or failure to detect attacks below the threshold.
- Once the rate based mechanism starts to mitigate suspected traffic, it impacts the quality of experience for all users, including legitimate ones. Not every increase in traffic rate is a result of an attack; there are other cases,

such as flash crowd events, that look like attacks to out-dated anti-DDoS solutions. As a result, the solution can mistakenly block legitimate traffic.

It is clear that out-dated anti-DDoS solutions cannot distinguish properly between attackers and legitimate users. Advanced DDoS mitigation solutions deploy more sophisticated methods, such as behavioural analysis or challenge-response mechanisms to deal with this challenge.

Behavioural Analysis

Behavioural analysis follows application transactions and builds an understanding of the application in order to distinguish between legitimate and malicious users. A baseline application behaviour is defined after considering both the amount and frequency of events.

During an attack, data is gathered and compared to the baseline behavior model. If a suspicious behavior is detected, a deeper inspection process is triggered, which analyses application-level parameters and resolves whether the suspicious behavior is a result of a legitimate burst of application traffic or a result of a malicious application abuse.

For example, a PDF file in a certain website is normally downloaded 10 times per hour. If the same file is downloaded 1000 times per hour, an attacker may be involved, so further security measures must be taken.

Challenge Response

A challenge response (C/R) mechanism sends challenges to suspicious sources and based on the response, determines if the source is a Bot or a real user. An example of a challenge response mechanism is CAPTCHA, which requires the user to type letters and/or digits from a distorted image that appears on the screen. The CAPTCHA test prevents unwanted internet bots from accessing websites, since a normal human can easily read the CAPTCHA, while the bot cannot process the image letters.

To use the C/R mechanism, an attack mitigation system launches a series of queries to the source of a request in question, and according to the responses received, it decides whether to send an additional, more sophisticated challenge, or flag the source as a malicious user. C/R mechanisms use automated processes, and require no human intervention from the mitigation system or from the source. The intelligent usage of a C/R mechanism and network behavioral analysis can almost completely eliminate false positives, guaranteeing an excellent quality of experience for legitimate users.

In summary, anyone can rate limit the traffic to a specific application and prevent floods on the applications, but this will result in denying the service from your legitimate users, which was the original objective of the attackers. Only advanced anti-DDoS solutions can successfully distinguish between attackers from legitimate users during an attack and guarantee proper service to online customers.

The following areas are of a particular concern as we look towards 2012 planning for attacks:

1. Real-Time Protection against Volumetric Attacks

According to Wikipedia, volumetric attacks are defined as the following, “attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.” 2011 has seen a dramatic rise in the growth of these attack types and even more ominous is the procurement of more capable ‘weapon systems’ or new application-based tools from which attacks can be launched.

The following is a list to consider when making certain you are covering your basis in this category:TCP SYN floods, TCP SYN+ACK floods, TCP RESET floods, TCP Fragment floods, UDP floods, ICMP floods, IGMP floods and Packet Anomalies

2. Application Layer (L7) Availability Protections

Malware is morphing in scale, scope and delivery payloads. It has managed to renew itself as a top concern related to protecting your organization in 2012 and has emerged as an imminent threat to Organizational Availability. In fact, attackers have shifted away from mass distribution of a small number of threats to micro distribution of large families of threats. These new strains of malware consist of millions of distinct threats that mutate as they spread rapidly. In this category, the following is a list of attacks worthy of considering when choosing protection mechanisms for your enterprise:Real-time protection against: Bot-originated and direct application attacks, HTTP GET page floods,HTTP POST floods, DNS query floods and Brute Force Attacks (HTTP, Telnet, POP3, IMAP, etc.,)

3. Service Denials & Behavioral Protections

Trusted Web sites are the focus of a large portion of malicious activity. As more and more users go online to take advantage of Web 2.0 applications-like social-networking sites, blogs, and wikis — authors of ‘hacking and cracking’ software are right behind them, opening up yet another front in the constant cat-and-mouse game between security defenses and hackers.

These threats will become increasingly important with younger workforces who are proficient with these tools. To thwart these attack types consider very strong protections against these categories of attacks or threats: HTTP servers, web vulnerability scans, Brute force, Application Brute force and Application scans.

IPS & Reputation Services

The continued high volume of Hacktivist attacks underscored the importance of various signature prevention technologies to prevent proper exploitation of an evolving tool landscape. In fact, the heavy reliance on tools as part of Hacktivist attacks have ironically exposed the over-reliance on the perimeter model of deployed security devices without IPS technologies on the VERY edge.

Most DDoS Providers do not rely on signatures and frequently fail to uncover newly developed attack tools, and most IPS providers suggest deployments of their tools to deep in the infrastructure for them to be meaningful to stop attacks at the perimeter. The following is a shopping list of things to consideration when procuring IPS & Reputational Management solutions to prevent perimeter attacks:

Signatures Protection against: Application Vulnerabilities and exploits, Web, Mail, DNS, databases, VoIP, OS Vulnerabilities and exploits, Microsoft, Apple, Unix based, Network Infrastructure Vulnerabilities, Switches, routers and other network elements vulnerabilities, Worms, Bots, Trojans and Drop-points, Spyware and Protocol Anomalies.

Network scanning and malware propagation Protections

As mentioned above in the Application-focused problem of bots and malware, the very same categorical problem exists at the network layer, however this time it is as equally as important to protect the internal environment as well as the external in real time. The following is a list of network protection considerations: UDP spreading worms detection, TCP spreading worms detection,High and low rate network scans, Scanning/spreading pattern identification and Infected source identification.

RISE OF THE AVAILABILITY VULNERABILITIES

The following are the solid reasons to test your organization for these risks, in order to provide DDoS protection:

1. Validate the strength of your perimeter-protection security to availability attacks.

Scores of new tools have been released and used lately – do you test for these new releases? Tools such as LOIC, RUDY, RefRef, Slowloris, etc., are not listed on the common vulnerability exposure (CVE) register as they are tools. Yet most companies don’t know if these new ‘weapon systems’ can pierce their current defenses.

2. Improve security of critical architectures.

Knowing where the holes are in your current architecture allows you to adopt remediation procedures that close them. Radware helps you tighten security by identifying gaps and recommending solutions.

3. Strengthen your response capability for security attacks.

By highlighting areas of improvement, you can greatly enhance the quality of event response plans.

4. Increase the effectiveness of security initiatives.

Can you bring someone to justice if you undergo an attack? Gain valuable insight into your organization's security posture and ensure the highest levels of readiness.

5. Test your current incident detection methods.

The information security threats to an organization revolve around the following problems:Real-Time Protection against Volumetric Attacks, Application Protections Against Application Layer (L7) Outages, Behavioral Protections (e.g., non-signature based) Protecting Critical Servers and Services, Signature-based (IPS) & Reputation Services Coverage and Quality and Effectiveness of from existing malware propagation and scanning Protection tools.

OVERVIEW OF MOBILE AD-HOC NETWORK (MANET)

Security issues in MANET

We know that a Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predetermined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Now-a-days, Mobile ad hoc network (MANET) is one of the recent active fields and has received marvellous attention because of their self-configuration and self-maintenance capabilities. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks.

A mobile ad-hoc network (MANET) consists of a number of mobile hosts to carry out its basic functions like packet forwarding, routing, and service discovery without the help of an established infrastructure. Each node of an ad-hoc network depends on another node in for- warding a packet to its destination, because of the limited range of each mobile host's wireless transmissions. An ad-hoc network uses no centralized administration. This ensures that the network will not stop its functioning just because one of the mobile nodes moves out of the range of the others. Because of the limited transmitter range of the nodes, multiple hops need to cooperate to reach other nodes. Every node in an ad-hoc network must be willing to forward packets to other nodes. Thus, every node acts both as a host and as a router. The topology of ad-hoc networks varies with time as nodes move in and out of the network. This topological instability requires a routing protocol to run on each node to create and maintain routes between the nodes [34].

Mobile Ad-hoc Networks' Usages: Wireless ad-hoc networks are mainly used in areas where a wired network infrastructure cannot fit in due to reasons such as cost or convenience. It can be very quickly deployed to support emergency requirements, connectivity on the go, short- term needs, and coverage in undeveloped areas. Any day-to-day application such as electronic email and file transfer can be considered to be easily deployable within an ad-hoc network environment.

In addition to this, there is no need to focus on the wide range of warlike applications possible with ad-hoc networks. Even the technology was initially developed for the warlike applications. In such situations, the ad-hoc networks having self-organizing capability can be efficiently used where other technologies either fail or cannot be deployed efficiently. Some well-known ad-hoc network applications are:

Collaborative Work: For some business environments, the need for collaborative computing is sometimes more important outside office environments than inside. Moreover, it is often the case where people really need to have meetings to cooperate and exchange information on a project.

Crisis-Management Applications: These arise as a result of natural disasters where the entire communications infrastructure is disordered and restoring communications quickly is essential. By using ad-hoc networks, it becomes easy and quick to establish a communication channel than required for wired communications.

Personal Area Networking and Bluetooth: A personal area network (PAN) is a short-range, localized net- work where nodes are usually associated with some- one. These nodes could be attached to a pulse watch, belt, and so on. In such scenarios, mobility is only a major consideration when interaction among several PANs is the main issue.

For analyzing the security of wireless mobile ad-hoc networks, we need certain parameters. The basic parameters for a secure system are: Availability, Confidentiality, Authentication, Integrity, Non-repudiation and Scalability.

Challenges in Manets

MANETs face challenges in secure communication. For example the resource constraints on nodes in ad hoc networks limit the cryptographic measures that are used for secure messages. Thus it is susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Mobile nodes without adequate protection are easy to compromise. An attacker can listen, modify and attempt to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network. Static configuration may not be adequate for the dynamically changing topology in terms of security solution. Various attacks like DoS (Denial of Service) can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information. Lack of cooperation and constrained capability is common in wireless MANET which makes anomalies hard to distinguish from normalcy. In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, and absence of central authorities, distribution cooperation and constrained capability.

MANET Usage and Characteristics

Dynamic topologies: Nodes are free to move anywhere in the network. Thus, the network topology changes randomly and rapidly at unpredictable times, which is the main characteristic of an MANET.

Bandwidth-constrained variable capacity links: Wireless links will continue to have considerably lower capacity than their hardwired counterparts. In addition, the actual throughput of wireless communications, after calculating for the effects of multiple accesses, multipath routing, noise, and interference conditions, is lesser than a radio’s maximum transmission rate.

Energy-constrained operation: The nodes in an MANET may depend on batteries or other exhaustible means for their energy. For these nodes, an important optimization criteria system design may be energy saving.

Security: Mobile wireless networks are highly prone to physical security threats because of its hop by hop routing, multipath routing and dynamically changing topology. Therefore, an increase in the possibility of different attacks should be carefully considered.

Security attacks in MANET

The security attacks in MANETs can be categorized as active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. Various types of attacks in MANETs are: Modification, Impersonation, Fabrication, Eavesdropping, Replay, Denial of Service, Malicious Software and Lack of Cooperation. Denial of Service attack is described below. Network Protocol Stack Based Attack Classification Attacks could also be classified according to the target layer in the protocol stack Security is an important issue for ad-hoc networks, especially for the more security sensitive applications used in military and critical networks.

An ad-hoc network can be considered secure if it holds the following attributes:

1. Availability: It ensures that the network manages to provide all services despite denial of service attacks. A denial of service attack can be launched at any layer of an ad-hoc network. On the physical and media access control layer a malicious user can employ jamming in order to interfere with signals in the physical layer. On the network layer, a malicious user can disrupt the normal operation of the routing table in various ways that are presented in a following section. Lastly, on the higher layer, a malicious user can bring down high-level services such as the key management service.

2. Confidentiality: It ensures that certain information is never disclosed to unauthorized users. This attribute is mostly desired when transmitting sensitive information such as military and tactical data. Routing information must also be confidential in some cases when the user’s location must be kept secret.

3. Integrity: Guarantees that the message that is transmitted reaches its destination without being changed or corrupted in any way. Message corruption can be caused by either a malicious attack on the network or because of radio propagation failure.

4. Authentication: It enables a node to be sure of the identity of the peer with which it communicates. When there is no authentication scheme, a node can masquerade as some other node and gain unauthorized access to resources or sensitive information.

5. Non-repudiation: It ensures that the originator of a message cannot refuse to send this message. This attribute is useful when trying to detect isolated compromised nodes.

Overview of MANET Routing Protocols

Figure 5 shows the various Mobile Ad-Hoc Networks Routing Protocols and their subtypes. The routing protocols in ad-hoc networks may be categorized as proactive routing protocols, reactive routing protocols, and hybrid routing protocols [35]. Proactive Routing Protocols are those protocols, in which the routes are maintained to all the nodes, including those nodes to which packets are not sent. An example of proactive routing protocols in ad-hoc networks is Optimized Link State Routing Protocol (OLSR). Reactive Routing Protocols are those protocols in which the route between the two nodes is constructed only when the communication occurs between the two nodes. Such type of routing protocols is Ad hoc On Demand Distance Vector Routing Protocol (AODV) and Dynamic Source Routing Protocol (DSR) [36]. Hybrid Routing Protocols are those protocols in which the combined approach of proactive routing and reactive routing are used for the route generation between the nodes. The Zone Routing Protocol (ZRP) is such a hybrid reactive/proactive routing protocols.

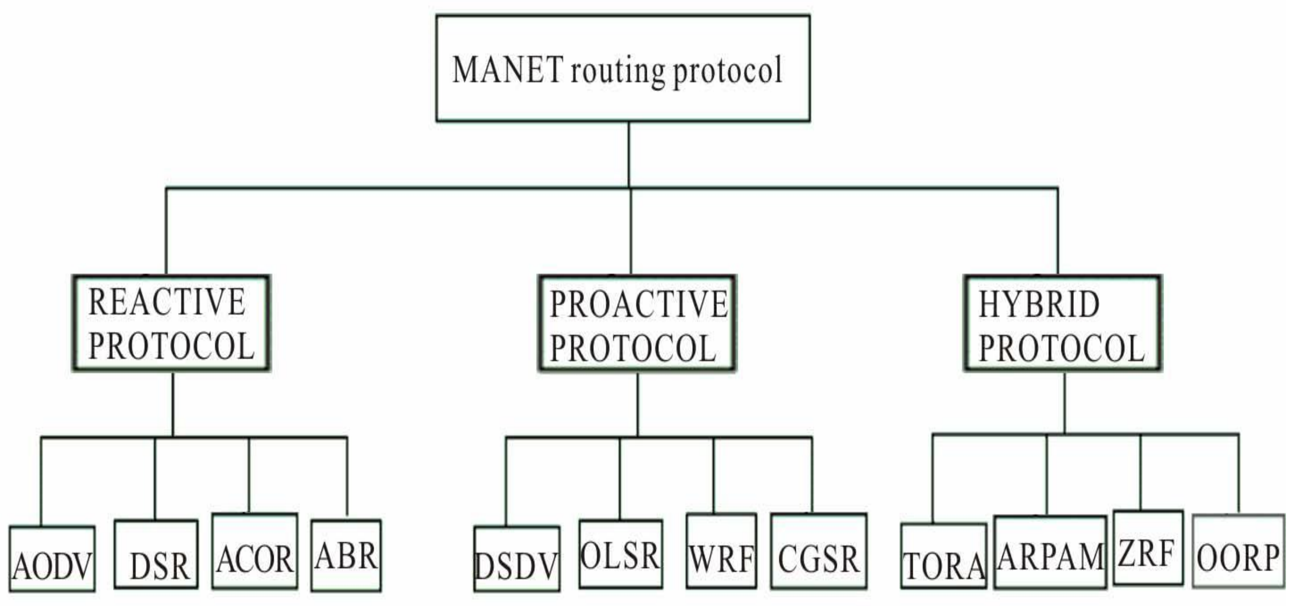

Figure 5: Various MANET Routing Protocols and their subtypes.

Degrade the Performance in Lifetime of MANET

The following metrics can be used to evaluate the performance of flooding attack:

1. Packet loss rate: The ratio of the number of packets dropped by the nodes divided by the number of packets originated by the application layer continuous bit rate (CBR) sources. The packet loss ratio is important as it describes the loss rate that can be seen by the transport protocols, which in turn affects the maxi- mum throughput that the network can support. The metric characterizes both the completeness and correctness of the routing protocol.
2. Average delay: Average of delay incurred by all the packets, which are successfully transmitted.
3. Throughput: Average number of packets per second X packet size.
4. Average number of hops: complete length of all routes divided by the total number of routes.

Various Existing Defense Mechanisms

The different defense mechanisms for DDoS attacks are classified into two categories: local and global. As the name suggests, local solutions can be implemented on the victim computer or its local network without an outsider's cooperation.

Global solutions, by their very nature, require the cooperation of several Internet subnets, which typically cross company boundaries.

Local Solutions

Protection for individual computers falls into these areas:

1. Local Filtering
2. The timeworn short-term solution is to try to stop the infiltrating IP packets on the local router by installing a filter to detect them. The stumbling block to his solution is that if an attack jams the victim's local network with enough traffic, it also overwhelms the local router, overloading the filtering software and rendering it inoperable.
3. Changing IPs
4. A Band-Aid solution to a DDoS attack is to change the victim computer's IP address, thereby invalidating the old address. This action still leaves the computer vulnerable because the attacker can launch the attack at the new IP address. This option is practical because the current type of DDoS attack is based on IP addresses. System administrators must make a series of changes to domain name service entries, routing table entries, and so on to lead traffic to the new IP address. Once the IP change which takes some time is completed, all Internet routers will have been informed, and edge routers will drop the attacking packets.
5. Creating Client Bottlenecks
6. The objective behind this approach is to create bottleneck processes on the zombie computers, limiting their attacking ability. Examples of this approach include RSA Security Corp. Client Puzzles: RSA‟s Client Puzzles algorithm requires the attacking computer to correctly solve a small puzzle before establishing a connection.

   Solving the puzzle consumes some computational power, limiting the attacker in the number of connection requests it can make at the same time. Turing test: Software implementing this approach requires the attacking computer to answer a random question before establishing the connection.

Global Solutions

Clearly, as DDoS attacks target the deficiencies of the Internet as a whole, local solutions to the problem become futile. Global solutions are better from a technological standpoint. The real question is whether there is a global incentive to implement them.

Improving the Security of the Entire Internet: Improving the security of all computers linked to the Internet would prevent attackers from finding enough vulnerable computers to break into and plant daemon programs that would turn them into zombies.

Using Globally Coordinated Filters: The strategy here is to prevent the accumulation of a critical mass of attacking packets in time. Once filters are installed throughout the Internet, a victim can send information that it has detected an attack, and the filters can stop attacking packets earlier along the attacking path, before they aggregate to lethal proportions. This method is effective even if the attacker has already seized enough zombie computers to pose a threat.

Tracing the Source IP Address: The goal of this approach is to trace the intruders‟ path back to the zombie computers and stop their attacks or, even better, to find the original attacker and take legal actions. If tracing is done promptly enough, it can help to abort the DDoS attack. Catching the attacker would deter repeat attacks. However, two attacker techniques hinder tracing:

- IP spoofing that uses forged source IP addresses, and
- The hierarchical attacking structure that detaches the control traffic from the attacking traffic, effectively hiding attackers even if the zombie computers are identified.

Proposed Defense Method

General Observations about DDoS Attacks

Denial-of-service attacks create shortages of are source such as bandwidth or computing cycles through the creation of an artificial demand. They work because the "cost" of the transaction falls overwhelmingly on the server. Sophisticated DDoS attacks also can be virtually in distinguishable from genuine overload (at least at the time of the attack) due to the limitations of the information available and the kinds of analysis possible in real-time. A mechanism is necessary to transfer a corresponding burden to the requesting client and to control the damage that any single client can cause. This characterization suggests that an economics-based approach to establish a"market place" for the services may provide a fairer allocation of resources, provided that the currency's availability can be effectively allocated by the service provider to its customers (and kept away from its detractors).To make services more robust against a DDoS attack, we propose the following combination of strategies:

1. Increase the barrier to entry by using a pricing-based scheme in which the price of entry varies with the load level. This will throttle the machines used in the attack, thereby forcing the attacker to employ (orsubvert) a larger number of machines.

2. Use a differentiated model. Provide prioritized access to classes of users; though a DDoS attack will raise the price so high that lower priority classes get locked out, higher priority clients can still access the service. Allocating a priority mechanism to desirable clients is

Key.

3. Use a dynamic, differential pricing mechanism to penalize clients that are responsible for a load on the server. This typically requires flow monitoring and isolation capabilities in line with those of Diffserv.

None of these strategies are sufficient in isolation —situations can be defined where each may contribute to increasing the availability of the network services.

Types of Micro-payments

Micro-payments can provide a useful side benefit by providing a uniform means of resource accounting, pricing, and arbitration. Micro-payment mechanisms must not impose an undue performance penalty − in the absence of an attack, the performance should be nearly comparable to a system that does not use the payment mechanisms. There is prior work on how pricing can be used to influence consumer behavior, how to integrate pricing mechanisms with OS and network resource management mechanisms. In this paper, we instead focus on how pricing strategies can be used to mitigate DDoS, and improve overall service survivability.

Fungible vs. Non-fungible Micro-payments

There have been a number of digital payment and micro-payment schemes proposed to support digital exchanges. These have been primarily proposed to support digital commerce, but some researchers have also looked at the use of payment schemes as a means of mitigating denials of service. They therefore have low latency with respect to coordination with external servers; however the validation process typically requires significant computation or memory usage overhead for the server itself. As a result, high integrity cash-like payment schemes may not be compatible with fielded servers. Many of the alternative fungible payment schemes are analogous to a check or credit card transaction and require some type of on-line verification of payment − a server must connect online with a bank and verify the creditworthiness of the requester. On-line verification is susceptible to high latency and provides an alternative critical path target for DoS.

Scrip-based systems are an attempt to reduce the latency of verification by making the verification a purely local operation on the server. Clients obtain a quantity of scrip from network scrip brokers using one of the high-overhead bulk-payment schemes geared for larger expenditures. Millicent allows a server to give a clientchange (which the client may later redeem with their broker). The server sets a computational task to the client that must be solved before server resources are expended on the client's task. To be useful, the task must be computationally hard to solve, but a solution must be simple to verify e.g., factoring a large number-the size of the number is determined by the prices of the service, which in turn reflects the load (demand) on the server.

Convertible vs. Non-convertible Currencies

A non-convertible currency scheme has a limited scope where it can be used and cannot be exchanged for other types of currency. A convertible currency on the other hand can be exchanged for other types of currency. The former is useful to permit priority access to specific resources for a particular subset of known potential users (e.g. a military squadron). The latter has advantages in situations requiring high priority access for a dynamically changing subset of potential users drawn from a general population.

Dynamic Resource Pricing as Discriminants

As the logical next step, we implement a dynamic pricing strategy that can favor good user behavior and discriminate against aggressive adversarial behavior. In our model, we have a time-varying price function for each service. The price function relates the price of the service to supply, demand and other factors. Each user has a utility function that determines how much they are willing to pay for a unit of a given service as well as how many units they will consume at a given price at any given time. The cumulative effect of the utility functions drives the overall demand for the service. Furthermore, the spending behavior can be monitored in a distributed fashion for anomalies. Selection of one particular user behavior over another occurs due to interplay of the price and utility curves. While the idea of using pricing to mold user behavior is known, our approach extends this idea to discriminate against adversarial behavior.

Price-based Service Quality Differentiation and Survivability

We have discussed how different pricing function scan be used to select different kinds of user behavior, thereby protecting against some classes of attacks. A single price function is unlikely to provide sufficient service quality differentiation necessary to satisfy a wide range of user requirements. Furthermore, a single pricing function is unlikely to protect the system against all forms of attack. Therefore we propose to partition and isolate the available resources among various service classes. For example, in the case of a network router, weighted fair queuing can be used to partition resources. Resources can also be isolated using VPNs. Server resources can similarly be partitioned and isolated among service classes by using OS prioritized scheduling techniques and by virtual OS techniques respectively. We hypothesize that the survivability of the system can be further enhanced by associating different partitions with different discriminants (pricing functions) that are robust against different classes of attacks. With this approach, a successful resource depletion attack will not

only require more resources, but also the simultaneous aunch of different forms of attack for each service class. Possible extensions of this strategy include dynamic policy iteration that progressively improves robustness against a larger class of attacks or a randomized policy iteration that makes it harder for the adversary to guess the pricing function and determine efficient attack strategies.

System Architecture - Figure 6 illustrates the operational architecture for the Mb SQD system. The Mb SQD system employs a distributed architecture with three distinct features:

1. Deployment of resource brokers at network boundaries

MbSQD will use stateful packet filters and/or application proxies to control resource utilization at the logical boundaries of user subnets(on either the provider's or the client's sites). This architecture has the following advantages:

a) The operation of client and server applications will not be affected by the deployment of the traffic control system; in fact, both clients and servers may not be aware of its presence except due to apparent changes in network through put and device performance. No modification of end node protocols and applications is necessary.

b) The architecture may be used to control the utilization of both network and information resources including network throughput, server capacity, information access and device usage. The brokers may be installed at the border gateways of autonomous systems if they are intended to be used for inter-domain traffic control, or they can be placed at the "choke points" of server access if they are used to control information access and/or device usage.

c) Price-based resource management can be made mandatory in order to obtain the highest priority access privileges.

2. Employment of client-side defined price and purchase decision functions

MbSQD achieves rapid control of resource utilization by relying on the interactions between the dynamic pricing of resources and the autonomic purchase decisions made by individual clients. By employing different pricing functions, MbSQD can favor the clients that exhibit desired behaviors or use certain forms of purchase decision functions. This behavioral discrimination is a unique feature of the dynamic pricing scheme.

3. Operation with TCP-integrated payment protocols

MbSQD uses a three-message handshake protocol to initiate service request and conduct payment transaction; it also uses two-message handshakes topay for continuous resource use. The initial payment protocol can be readily integrated with the TCP connection establishment, and the renewal hand shakes can be "piggy-backed" onto TCP data segments as options. The protocols are also designed to support different forms of payments including scrip and proof-of-work. A micro-payment infrastructure will be needed in order to use scrip.

In the remaining parts of this section, we will examine the three essential components of MbSQD: the resource brokers that are installed at the boundary gateways, the business logic that implements the price and the purchase decision functions, and the payment protocol that enables the business transactions.

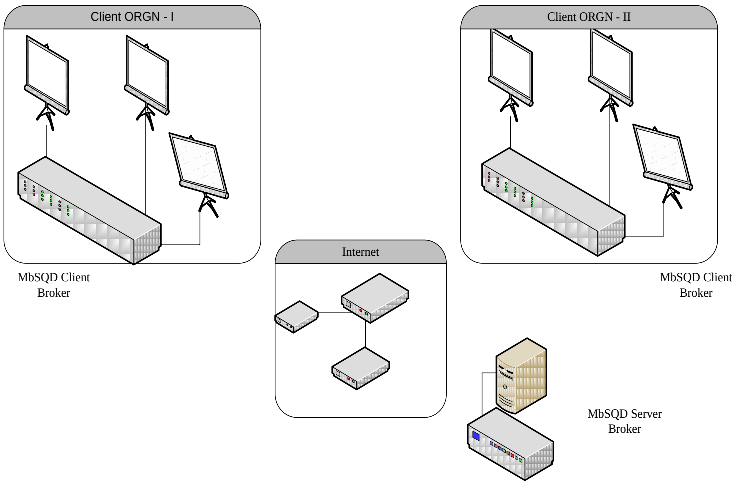

Figure 6: MbSQD Operational Architecture.

Resource Brokers

The MbSQD resource brokers are to be installed in gateways at the boundary of Internet sub-networks, where they can function as application proxies or packet filters. The brokers determine whether data grams going to and from certain IP addresses using specific transport protocols and port numbers should be passed or discarded. Functionally, the resource brokers may be the proxies of application clients or servers. The server and client brokers enable passage of data grams based resource prices and budgetary considerations. Operationally, each broker consists of two sets of components that either operate on data or control flows.

Server vs. Client Brokers

The client brokers function as proxies of the client applications that run on the end hosts. The client brokers submit the requests for services — specified in terms of server IP addresses, transport protocols and port numbers— to the server broker on behalf of the client applications, make the purchase decision when the server brokers reveal the current prices of the services and conduct the transaction in order to establish passages for the traffic. The server brokers, on the other hand, function as proxies of the server applications that provide specific services. The brokers determine the dynamic prices of the services based on several traffic parameters that are monitored continuously. They also work with the client brokers to conduct the payment transactions and control the client-server traffic flows.

Subscription Types

Currently, four general subscription types are implemented in MbSQD

a) Subscriptions in Packets: subscriptions are offered to customers on a per packet basis. The service provider defines a maximum number of packets the client can send or receive; once the quota has been met, the subscription expires and the client must pay for additional service.

b) Subscriptions in Seconds: subscriptions are sold in seconds of connection time. When the connection duration has elapsed, the subscription expires and customers must purchase a new subscription. A time based subscription may be used in conjunction with another subscription type to create a hybrid subscription type. For instance the subscriptions may be sold in terms of number of packets, but a client must send or receive the packets within a certain period of time. Such a hybrid type may be useful discourage clients from “squatting” on a connection.

c) Subscriptions in Connections: a client pays for a connection that lasts for an indeterminate duration. This subscription type may be combined with a time based subscription to simulate leasing of a resource.

d) Subscriptions in Bytes: a client may also purchase a subscription based on the number of bytes sent to or from a server.

Purchase Decision Functions

At the client brokers, interacting with the resource prices are the purchase decision functions, which determine whether to purchase the subscriptions by making required payments.

The decision functions can employ sophisticated strategies based on the market observables and other parameters supplied by the clients.

The simplest decision function might only specify a price ceiling for each client.

Micro-payment Protocols

MbSQD employs a three-message handshake to perform the payment transactions. The handshakes provide a framework protocol that can be used to support different forms of micro-payment including scrip and computational proof-of-work. It can also be made compatible with various micro-payment infrastructures.

EXPERIMENTAL SETUP FOR PROPOSED DEFENSE METHOD

We investigated the behaviors of MbSQD broker architecture and traffic management mechanisms by conducting a series of simulation experiments using public-domain discrete-event network simulator, NS-2. In the experiments, a fixed set of legitimate clients was programmed to request the service offered by a single server. Their requests were mingled with much larger number of requests initiated by the rogue clients that were subverted to instigate DDoS attacks. Client and server brokers, deployed at the boundaries of the sub-networks that contain the clients and the servers, relayed the service requests of both “good” and “bad” clients. Both client and server brokers could operate in an active or an inactive mode. In the inactive mode, the brokers behaved like ordinary firewalls or routers. When activated, client and server brokers could control the traffic flowing through them by matching the IP data grams with the connections established between the brokers. The data grams were passed if they could be matched with one or more of the established connections and discarded otherwise. In each run, we observed the progress of two DDoS attacks – one with and the other without the use of MbSQD. Control parameters, such numbers of rogue clients and traffic characteristics, were changed between experimental runs.T he goal of the experiments was to investigate the effectiveness of MbSQD architecture in mitigating the DDoS attacks. The degree of effectiveness was inferred from the following two sets of observations:

1. A comparison between the number of subverted clients required to launch two similar DDoS attacks that cause compatible levels of performance degradation with and without the activation of MbSQD brokers;

2. A comparison of the residual level of services

available to the fixed set of legitimate clients in the two similar DDoS attacks with and without MbSQD brokers.

Results

We performed three sets of experiments that were designed to study the behaviors of MbSQD system in response to three different kinds of DDoS attacks:

1. TCP-SYN Attacks: in these experiments, the rogue clients flood the server with SYN packets with forged source IP addresses in order to overwhelm the server with half-opened TCP connections;

2. Server Flooding Attacks: in these experiments, the rogue clients flood the server with frequent and long TCP connections uploading large amount of data to the server; this set of experiments were also designed to examine the effects of using computational proof-of-work as a method of payments offered by the clients;

3. Server Draining Attack: in these experiments, therogue clients initiate frequent TCP connections downloading large amount of data from the server(e.g. an HTTP server). This set of experiments also examines the effects of using fungible payments as a means of payments.

Metrics of Proposed Defense Method

In this section we describe the parameters used in the simulations. The performance simulation environment used is based on NS-2, a network simulator that provides support for simulating multi-hop wireless networks. General parameters for Experimental Setup are shown in Table 1.

Table 1: General Parameters for Experimental Setup of Proposed Defense Method.

Sl.No.	Parameter	Value	Description
1	Number of Nodes	0-50	Network Nodes
2	Terrain Range	(1500,1500)	X,Y dimension of motion in m
3	Bandwidth	5 Mbps	Bandwidth of nodes
4	Simulation Time	0-20 Second’s	Simulation Duration
5	Placement of Nodes	Uniform	Node placement Policy
6	Mobility	Random	Randomly change the direction
7	Mobility Time	0-25 m/s	Mobility of Nodes
8	Traffic Model	CBR	Constant bit rate protocol
9	MAC Protocol	CSMA	MAC Protocol
10	Routing Protocol	AODV Modified	Routing protocol

Performance Metrics

1) Misbehaving Nodes
2) Network Size
3) Pause Time

4) Simulation Time were investigated using the following 4 Metrics:

- Average Packet Delivery ratio
- Selfish node detection rate
- Routing and Communication Overhead.
- Misbehaving nodes detection rate.

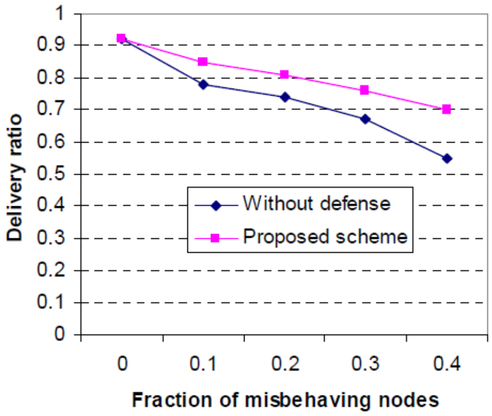

Figure 7: Delivery Ratio as a Function of Misbehaving Nodes.

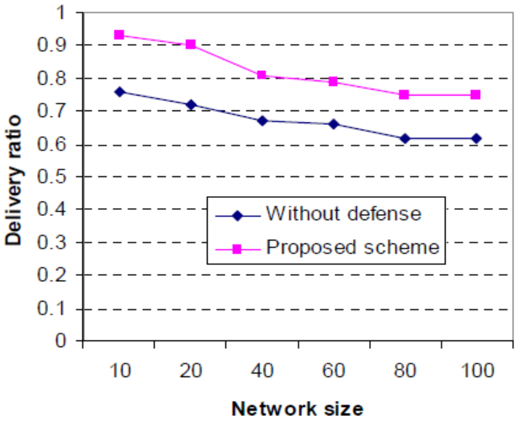

Figure 8: Packet Delivery Ratio as a Function of Network Size.

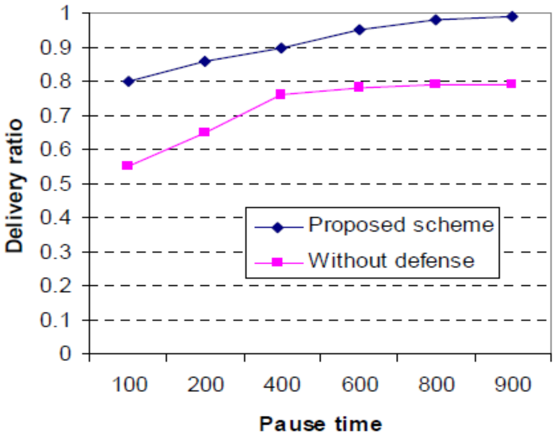

Figure 9: Delivery Ratio as a Function of Pause Time.

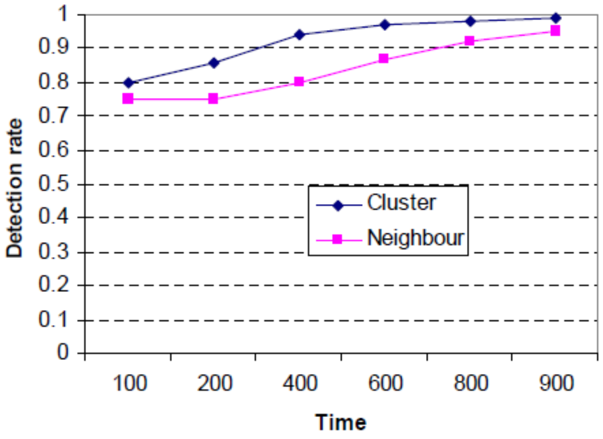

Figure 10: Detecting Misbehaving Node Rate as a Function of Time.

The following performance metrics are compared.

1. Packet Delivery Ratio (PDR): It is the ratio of the number of packets actually delivered without duplicates to the destinations versus the number of data packets supposed to be received. This number represents the effectiveness and throughput of a protocol in delivering data to the intended receivers within the network. Number of successfully delivered legitimate packets as a ratio of number of generated legitimate packets.

PDR = Total Number of packets Sent / Total Number of packets Received

2. Number of Collisions: In a network, when two or more nodes attempt to transmit a packet across the network at the same time, a packet collision occurs. When a packet collision occurs, the packets are either discarded or sent back to their originating stations and then retransmitted in a timed sequence to avoid further collision. Packet collisions can result in the loss of packet integrity or can impede the performance of a network. This metric is used to measure such collisions in the network. Using the NS-2 simulator, the effect of DDoS attacks is measured with respect to different number of attackers.

Results and Discussion

Effect of Proposed Defense Method on PDR with Different Number of Attackers

By using this defense method PDR increases up to 19.56% as compared to the PDR of existing defense method.

Effect of Proposed Defense Method on Number of Collisions with Different Number of Attackers

By using this defense method the number of collisions decreases up to 45.6% as compared to the collisions of existing defense method.

Lessons learned

We made the following observations from the simulation experiments:

• Pushing costs back onto clients appears to be effective for mitigating server-based DDoS attacks. Specifically, MbSQD does show promise for maintaining control of client-server traffic flows over the Internet.

• Proof-of-work methods are effective for elimination of spoofed requests or flooding via a limited number of machines.

• Different client behaviors can be discriminated by different server pricing strategies. Service Brokers can work to favor certain traffic behaviors in the range of various scenarios.

• The choice of a pricing function will have a very strong effect on the effectiveness of MbSQD.

Conclusion

Mobile Ad-hoc Network is an infrastructure less network due to its capability of operating without the support of any fixed infrastructure. Security plays a vital role in MANET due to its applications like battlefield or disaster-recovery networks. MANETs are more vulnerable compared to wired networks due to the lack of a trusted centralized authority and limited resources. There is an urgent need to develop a scheme to handle DDoS attack in the mobile ad-hoc network. In this paper we have discussed the various the attack mechanisms and problems due to DDoS attack, also how MANET can be affected by these attacks. In this paper, we have explored the application of dynamic pricing mechanisms in mitigating DDoS attacks. We have prototyped the proposed defense method using the NS-2 simulator. The various simulation results shows that the proposed architecture mitigates DDoS attacks effectively than the existing methods.

References

1. C. S. R. Murthy and B. S. Manoj, “Ad-Hoc Wireless Net- works Architectures and Protocols,” Prentice Hall Com- munications Engineering and Emerging Technologies Se- ries, Pearson Education, Upper Saddle River, 2004.
2. S. K. Sarkar, T. G. Basavaraju and C. Puttamadappa, “Ad-Hoc Mobile Wireless Networks: Principles, Protocols, and Applications,” Auerbach Publications, Boca Raton, 2008.
3. L. Garber, “Denial-of-service attacks rip the internet,” IEEE Comput., vol. 33, Apr. 2000.
4. C. Douligeris, and A. Mitrokotsa, “DDoS attacks and defense mechanisms: classification and state-of-the-art,” Computer Networks, 2004, pp.643–666.
5. Li-Chiou Chen, Thomas A. Longstaff, and Kathieen M. Carley, “Characterization of defense mechanisms against distributed denial of service attacks,” Computer & Security 23, 2004, pp.665-678.

6. B. Han, H. H. Fu, L. Lin and W. Jia, “Efficient Construction of Connected Dominating Set in Wireless Ad Hoc Networks,” IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, Fort Lauderdale, 25-27 October 2004, pp. 570-572.
7. Antonio Challita, Mona El Hassan, Sabine Maalouf and Adel Zouheiry; A Survey of DDoS Defense Mechanisms; Department of Electrical and Computer Engineering American University of Beirut; {asc04,mhe03,sem05,atz00}@aub.edu.lb.
8. Hwee-Xian Tan and Winston K. G. Seah; Framework for Statistical Filtering Against DDOS Attacks in MANETs; Proceedings of the Second International Conference on Embedded Software and Systems; 2005 IEEE.
9. X. J. Geng and A. B. Whinston, “Defeating Distributed Denial of Service Attacks,” IT Professional, Vol. 2, No. 4, 2000, pp. 36-41. doi:10.1109/6294.869381.
10. A Novel Solution to Handle DDOS Attack in MANET - Meghna Chhabra, Brij Gupta, Ammar Almomani - Journal of Information Security, 2013, 4, 165-179.
11. Q. Li, E-C. Chang and M. C. Chan; On the Effectiveness of DDoS Attacks on Statistical Filtering; Proceedings of the 24th Annual Conference of the IEEE Communications Society (INFOCOM 2005), Miami; Mar 13-17, 2005.
12. K. Biswas and Md. Liaqat Ali, “Security Threats in Mobile Ad-Hoc Network,” Master Thesis, Blekinge Institute of Technology, Blekinge, 2007.
13. A. Piskozub, “Denial of Service and Distributed Denial of Service Attacks,” Proceedings of the International Conference on Modern Problems of Radio Engineering, Tele- communications and Computer Science, Lviv-Slavsko, 18-23 February 2002, pp. 303-304.
14. Xianjun Geng and Andrew B. Whinston; Defeating Distributed Denial of Service Attacks; February 2000.
15. V. Laurens, “Detecting DDoS attack traffic at the Agent Machines,” Canadian Conference on Electrical and Computer Engineering, CCECE’06, Ottawa, 7-10 May 2006, pp. 2369-2372.
16. S. M. Specht, “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures,” ISCA 17th International Conference on Parallel and Distributed Computing Systems, San Francisco, 15-17 September 2004, pp. 543-550.
17. P. Joshi, “Security Issues in Routing Protocols in Manets at Network Layer,” Procedia Computer Science, Vol. 3 2011, pp. 954-960. doi:10.1016/j.procs.2010.12.156.

18. K. S. Madhusudhananaga Kumar and G. Aghila, “A Survey on Black Hole Attacks on AODV Protocol in MANET,” International Journal of Computer Applications, Vol. 34, No. 5, 2011, pp. 23-30.

19. E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah and R. Alfaris, “Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art,” International Journal of Computer Applications, Vol. 49, No. 7, 2012, pp. 24-32.

20. B. B. Gupta, M. Misra and R. C. Joshi, “FVBA: A Combined Statistical Approach for Low Rate Degrading and High Bandwidth Disruptive DDoS Attacks Detection in ISP Domain,” Proceedings of 16th IEEE International Conference on Networks (ICON-2008), New Delhi, 12-14 December 2008, pp. 1-4. doi:10.1109/ICON.2008.4772654

21. A. Srivastava, B. B. Gupta, A. Tyagi, A. Sharma and A. Mishra, “A Recent Survey on DDoS Attacks and Defense Mechanisms”, Proceedings of the First International Conference on Parallel, Distributed Computing Technologies and Applications (PDCTA-2011), Tirunelveli, 23-25 September 2011, pp. 570-580.

22. B. B. Gupta, R. C. Joshi and M. Misra, “ANN Based Scheme to Predict Number of Zombies Involved in a DDoS Attack,” International Journal of Network Security (IJNS), Vol. 14, No. 1, 2012, pp. 36-45.

23. Karthikeyan Thyagarajan and Arunkumar Thangavelu, “An integrated defense approach for distributed denial of service attacks in mobile ad-hoc network”, International journal of applied engineering research – ISSN 0973-4562 Volume 11, Number 7 (2016) pp 4898-4910.

24. V. Paxson, “An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks,” ACM SIGCOMM Computer Communication Review, Vol. 31, No. 3, 2001, pp. 38-47.

25. R. Guo, G. R. Chang, R. D. Hou, Y. H. Qin, B. J. Sun, A. Liu, Y. Jia and D. Peng, “Research on Counter Band-width Depletion DDoS Attacks Based on Genetic Algorithm,” Third International Conference on Natural Computation, ICNC 2007, Haikou, 24-27 August 2007, pp. 155-159,.

26. H.-J. Kim, R. B. Chitti and J. S. Song, “Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks,” Journal of Information Processing Systems, Vol. 7, No. 1, 2011, pp. 137-150.

27. U. 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), Vol. 1, No. 4, 2012, p. 27.

28. H. X. Tan, "Framework for Statistical Filtering against DDoS Attacks in MANETs," Second International Conference on Embedded Software and Systems, Xi'an, 16-18 December 2005, 8 pp.

29. A. Mishra, B. B. Gupta and R. C. Joshi, "A Comparative Study of Distributed Denial of Service Attacks, Intrusion Tolerance and Mitigation Techniques," European Intelligence and Security Informatics Conference, EISIC 2011, 12-14 September 2011, pp. 286, 289.

30. Y. Chaba, Y. Singh and P. Aneja, "Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET," Journal of Networks, Vol. 4, No. 3, 2009, pp. 178-183.

31. S. A. Arunmozhi and Y. Venkataramani, "DDoS Attack and Defense Scheme in Wireless Ad Hoc Networks," International Journal of Network Security & Its Applications, Vol. 3, No. 3, 2011, 6 pp.

32. A. Sun, "The Design and Implementation of Fisheye Routing Protocol for Mobile Ad Hoc Networks," Master Thesis, Massachusetts Institute of Technology, Cambridge, 2002.

33. P. Misra, "Routing Protocols for Ad Hoc Mobile Wireless Networks," 2006. http://www.cse.wustl.edu/~jain/cis788-99/adhoc_routing/

34. D. Johnson, D. Maltz and J. Broch, "DSR the Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," In: C. E. Perkins, Ed., Ad Hoc Networking, Addison-Wesley Longman Publishing Co., Inc., Boston, 2001, pp. 139-172.

Corresponding Author:
Karthikeyan Thyagarajan*,
Email: *tknvlr@gmail.com*