Journal of Information Security, 2013, 4, 165-179
http://dx.doi.org/10.4236/jis.2013.43019 Published Online July 2013 (http://www.scirp.org/journal/jis)

A Novel Solution to Handle DDOS Attack in MANET

Meghna Chhabra[1], Brij Gupta[1*], Ammar Almomani[2]
[1]School of Computing Science & Engineering, Galgotias Universiy, Greater Noida, India
[2]Faculty of Computing and Information Technology, North Jeddah Branch, King Abdulaziz University, Jeddah, Saudi Arabia
Email: *gupta.brij@gmail.com

Received May 30, 2013; revised June 30, 2013; accepted July 8, 2013

ABSTRACT

Distributed Denial of Service (DDoS) attacks in the networks needs to be prevented or handled if it occurs, as early as possible and before reaching the victim. Dealing with DDoS attacks is difficult due to their properties such as dynamic attack rates, various kinds of targets, big scale of botnet, etc. Distributed Denial of Service (DDoS) attack is hard to deal with because it is difficult to distinguish legitimate traffic from malicious traffic, especially when the traffic is coming at a different rate from distributed sources. DDoS attack becomes more difficult to handle if it occurs in wireless network because of the properties of ad hoc network such as dynamic topologies, low battery life, multicast routing, frequency of updates or network overhead, scalability, mobile agent based routing, and power aware routing, etc. Therefore, it is better to prevent the distributed denial of service attack rather than allowing it to occur and then taking the necessary steps to handle it. This paper discusses various the attack mechanisms and problems due to DDoS attack, also how MANET can be affected by these attacks. In addition to this, a novel solution is proposed to handle DDoS attacks in mobile ad hoc networks (MANETs).

Keywords: DDoS Attack; MANET; AODV; DSR; Flooding Attack; Botnet

1. Introduction

In view of the increasing demand for wireless information and data services, providing faster and reliable mobile access is becoming an important concern. Nowadays, not only mobile phones, but also laptops and PDAs are used by people in their professional and private lives. These devices are used separately for the most part that is their applications do not interact. Sometimes, however, a group of mobile devices form a spontaneous, temporary network as they move closer. This allows us to share information in the form of documents, presentations even when we are on the move or in a meeting [1]. This kind of spontaneous, temporary network referred to as mobile ad hoc networks (MANETs) sometimes just called ad hoc networks or multi-hop wireless networks, play an important role in our present life and will continue to help us in near future.

A mobile ad hoc network (MANET) is a spontaneous network that can be established without any fixed infrastructure or a topology. This means that all its nodes behave as routers and take part in its discovery and maintenance of routes *i.e.* nodes within each other's radio range communicate directly via wireless links, while those that are not in each other's radio range use other nodes as relays. Its routing protocol has to be able to manage with the new difficulties that an ad hoc network creates such as nodes mobility, limited power supply, quality of service, bandwidth issues, changing topology and security issues. These challenges set new requirements on MANET routing protocols and make them more vulnerable to attacks [2].

Ad hoc networks have a wide array of military and commercial applications. They are ideal in situations where installing an infrastructure network is not possible or when the purpose of the network is too transient or even for the reason that the previous infrastructure network was destroyed. Because of its ad hoc infrastructure, decentralized and dynamic topology, loopholes such as limited bandwidth, limited memory and limited battery power, it is very hard to achieve security. There are many solutions exist which cope up against loopholes and provide security up to a certain level in wired network but these solutions are not always suitable for wireless environment. Therefore ad-hoc network has its own issues and challenge over security, which cannot be tackled by the available wired security mechanism.

*Corresponding author.

In MANETs, all the participating nodes are involved in the routing process. Since conventional routing protocols are designed for predefined infrastructure networks, which cannot be used in mobile ad hoc networks, so the new classes of routing protocols, *i.e.* ad hoc routing protocols were designed to accomplish the requirement of less infrastructure ad hoc network. In comparison to guided and unguided media, most of the traditional applications do not provide user level security schemes based on the fact that physical network wiring provides some level of security. The routing protocol sets the upper limit to security in any packet network. If routing is misdirected, the entire network will be paralyzed. This problem makes ad hoc networks more complex as the routing usually needs to trust on the trustworthiness of all nodes that are participating in the routing process [3].

One of the recent and biggest cyber attacks has been reported on Netflix, this is because broadband router has been subverted and "Digital N-bombs" slows the Internet worldwide. The attackers were throwing so much of the digital traffic that popular site like Netflix have reportedly disrupted access. Mathew Prince, chief executive of CloudFlare, one of firms dealing with "nuclear bombs" said it's easy to cause so much damage. Spamhaus, an anti-spam organization, was hit by a wave of digital traffic that knocked its website offline.

Spamhaus's work is believed to have launched the massive DDoS, attack to bring down to bring down the anti-spam group. The attackers sent a series of data requests to DNS severs, which help to direct web traffic around the world. After receiving legitimate requests (as these servers are accessed by authorized users), the servers responded by sending the required data to Spamhaus, which could not deal with the information that suddenly arrived. The attack was so large that it began clogging up the DNS servers, which in turn slowed down the Internet worldwide. The congestion was so heavy that it overwhelmed the DNS routers [4]. A flood of request to view a site at the same time will exceed its capacity-stopping it from loading. Spamhaus greater capacity turning to CloudFlare, spread traffic over larger bandwidth. However the attackers began targeting their attacks so they would be concentrated. Hence, the connection slowed down.

Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks. Distributed Denial of Service (DDoS) attacks has also become a problem for users of computer systems connected to the Internet. A DDoS 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 [5].

Rest of the paper is organized as follows: Section 2 describes related work, Section 3 presents over of DDoS attacks, Section 4 describes MANET overview, Section 5 describes proposed prevention scheme, and finally, Section 6 concludes the paper and discusses some future work.

2. Related Work

In paper [6], Lu Han describes that the wireless ad hoc networks were first unfolded in 1990's. 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 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.

Kamanshis Biswas in [7] mentioned that Mobile Ad Hoc Network (MANET) is 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 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 network 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 has become a main concern to provide secure communication.

Andrim Piskozub in [8] gives main types of DoS attacks which flood victim's communication channel bandwidth, is carried out their analysis and are offered methods of protection from these attacks. The DDoS attacks are considerably more effective than their DoS-counterparts because they allow performing such attacks simultaneously from several sites, that makes this attack more efficient and complicates searches of attacker. 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 indicated system-victim. This paper also describes various countermeasures that should be taken to prevent the network from DDoS attack.

Xianjun Geng in [9] describe that the notorious, crippling attack on e-commerce's top companies in February 2000 and the recurring evidence of active network scan-

ning, 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.

In [10], Vicky Laurens *et al.* 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 machines 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.

In [11] Stephen M. Specht describe that Distributed Denial of Service (DDoS) attacks have 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 new countermeasures that are developed to prevent or mitigate DDoS attacks, attackers are constantly developing new methods to cheat on these new countermeasures.

This paper 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 in his paper [12], mention 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 census is monitored to classify normal and abnormal behavior. 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. 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.

In [13], the authors introduced a dynamic DoS attack, the one which can be characterized by exploiting the node mobility, dynamic power control, and compromised nodes to launch new DoS attacks dynamically. The authors have discussed static and dynamic DoS attacks. The DoS attacks launched on data link layer and on the layer above it, *i.e.* network layer is called as static DoS attack. Malicious nodes may be able to move around the entire network, to adjust transmission power dynamically, or even launch DoS attacks by compromising their cooperative neighbors.

In [14], the authors proposed a model to characterize the DDoS flooding attack and its traffic statistics. Also, they proposed an analytical model for looking for specific patterns of the attack traffic, aiming to check if there is an anomaly in the traffic and whether the attack is the DDoS attack and to find out the time when the attack is launched. The main aim of flooding attack is to paralyze the entire network by inserting overwhelming attack traffic (e.g. RREQ broadcasting) into the MANET. The advantage of this method is to detect DDoS attacks more effectively by traffic pattern identification proposed in their work.

In [15], the authors proposed a system which consists of a client detector and a server detector for producing warning of a DDoS attack. The client detector uses a Bloom filter-based detection scheme to generate accurate detection results and it consumes minimal storage and computational resources. Its main task is to monitor the TCP control packets entering and leaving a network. The detection scheme is developed from a modified hash table. The server detector, in an active state, assists the warning by sending requests to legitimate hosts. With the help of client detectors, a server detector can detect an upcoming DDoS attack at an early stage.

Antonio Challita in [16] describe different types of DDoS attacks, present recent DDoS defense methods and

propose a unique approach to handle DDoS attack. Based on common defense principles and taking into account a number of DDoS attacks, the author find out several defense methods and categorize them according to several 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, heavy traffic is checked before being passed to its destination node, thus preventing congestion in the network. This method is simple to integrate, requires no association between nodes, causes no overhead, and adds 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 lesser cost.

Mobile ad hoc networks are expected to be widely used in the near future. However, they are vulnerable to various security issues because of their dynamic characteristics. Malicious flooding attacks are the lethal attacks on mobile ad hoc networks. These attacks can severely occlude an entire network. To defend against these attacks, the authors propose a novel defence 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 security attacks in MANETs can be categorized as active attacks and passive attacks.

- Active Attack is an attack when attacker node has to bear some energy costs in order to perform the threat. Nodes that perform active attacks with the aim of causing harm to other nodes by causing network outage are considered as malicious.
- Passive Attacks are mainly with the purpose of saving energy selfishly. Nodes that cause 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, Lack of Cooperation, Denial of Service attack, and distributed denial of service attack. A number of proposals have been given by different researchers to handle these attacks but none crossed the benchmark because of dynamic characteristics of the MANET. A perfect solution needs to be proposed to handle the attacks and prevent the sensitive data of the user from mishandling.

Most ad hoc routing protocols are vulnerable to two categories, called external attacks and internal attacks. Internal attacks are initiated and executed by authorized node in the network, where as external attacks are performed by the node that they are not authorized to participate in the network. Another classification of attacks is related to protocol stacks, for instance, network layer attacks and some network layer attacks [17] are listed below in **Table 1** [18].

3. DDoS Attack Overview

3.1. DDoS Attack Components

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 kills the victim network of resources such as bandwidth, computing power, etc. The victim becomes unable to provide services to its legitimate clients and network performance is greatly affected. In brief, as the name suggests, the service to a legitimate user is being denied of the service by a malicious users by sending a large number of unwanted packets on a network or a single computer. 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. 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 agents are usually installed on host computers. These attacker agents or the secondary victims affect both the target and the host computers [19-22].

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

Table 1. Various network layer attack.

Type of Attack	Description
Wormhole	Tunneling the packets using private high speed network.
Byzantine	Selectively drop packets by making routing loops, forwarding packets through non-optimal paths with compromised nodes.
Rushing	Quickly forwards the control messages to gain access to the network.
Resource consumption	It injects the packets to get more network resource.
Location disclosure	Attacker discloses the privacy of a network by knowing the location of a node.
Blackhole	Drops the packets by sending false route reply messages to the route request.

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 DDoS attack components and procedure is shown in **Figure 1**. The following steps take place during a distributed attack [2,19]:

- The real attacker sends an "execute" message to the control master program.
- The control master program receives the "execute" message and propagates the command to the attack daemons under its control.
- Upon receiving the attack command, the agent machines begin the attack on the victim.

3.2. 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 [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 changes 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].

3.3. DDoS Attack Taxonomy

There are a wide variety of DDoS attacks [22]. Two types of DDoS attacks 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**.

3.3.1. Bandwidth Depletion Attacks

A Bandwidth Depletion Attack is designed to flood the

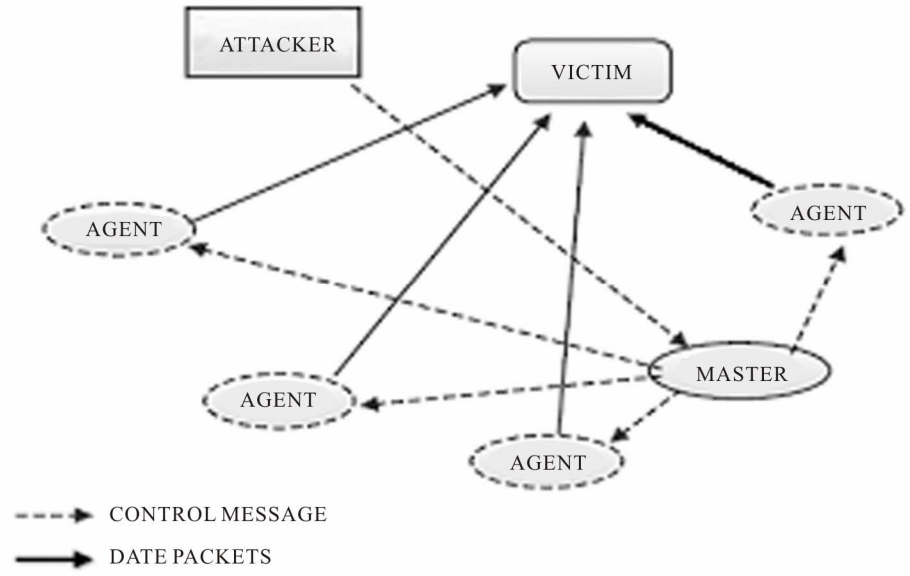

Figure 1. DDoS attack components.

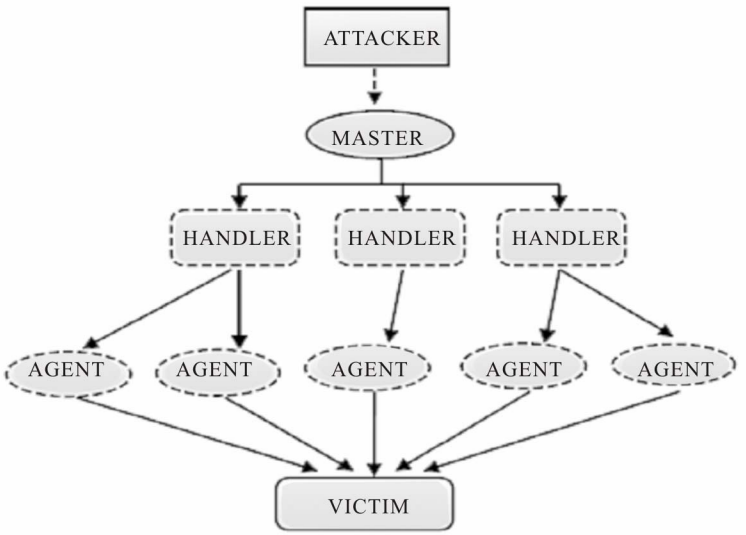

Figure 2. Typical DDoS architecture (the agent handler model).

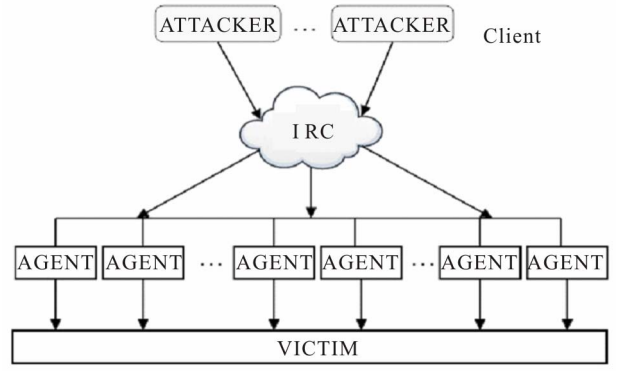

Figure 3. Architecture of IRC based DDoS attack.

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].

1) Flood Attacks

In a *flood attack*, zombies send a large volume of traffic to a victim system, so as to congest the victim system's network bandwidth with IP traffic. The victim system slows down, crashes, or suffers 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 requested 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 around 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].

2) 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 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. The attacking packets are typically ICMP ECHO REQUESTs, which are packets (similar to a

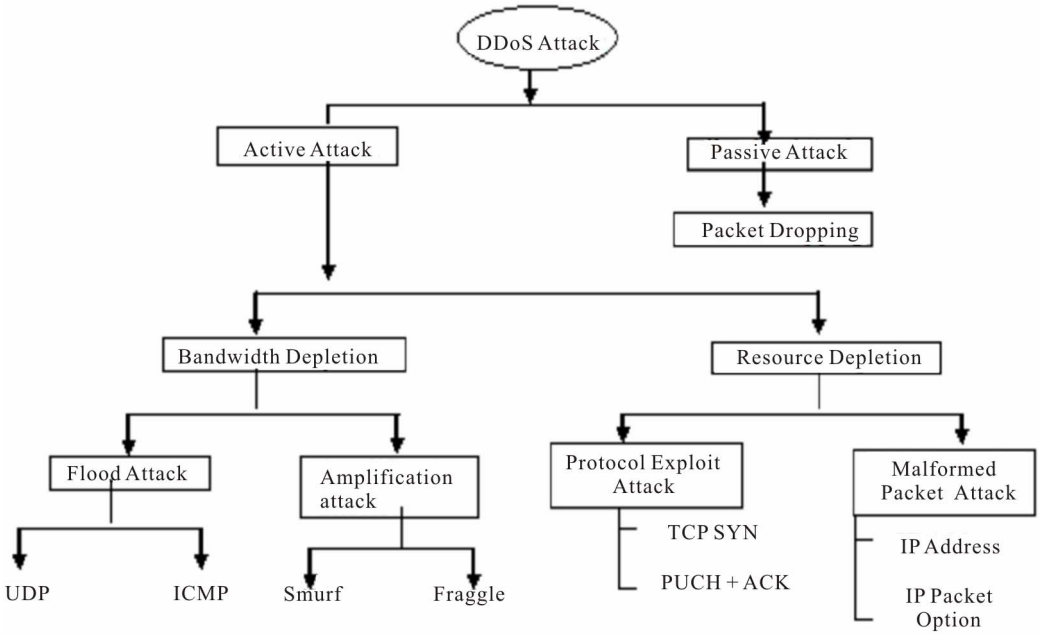

Figure 4. DDoS attack taxonomy.

"ping") that request the receiver to generate an ICMP ECHO REPLY packet [31]. The amplifier sends the ICMP ECHO REQUEST packets to all of the systems within the broadcast address range, and each of these systems will return an ICMP ECHO REPLY to the target victim's IP address. This type of attack amplifies the original packet tens or hundreds of times [32].

Another example is the DDoS *Fraggle attack*, where the attacker sends packets to a network amplifier, using UDP ECHO packets [33]. There is a variation of the Fraggle attack where the UDP ECHO packets are sent to the port that supports character generation, with the return address spoofed to the victim's echo service creating an infinite loop [34]. The UDP Fraggle packet will target the character generator in the systems reached by the broadcast address. These systems generate a character to send to the echo service in the victim system, which will send an echo packet back to the character generator, and the process repeats. This attack can generate more bad traffic and cause more damage than a Smurf attack.

3.3.2. Resource Depletion Attacks

A Resource Depletion Attack is an attack that is designed to tie up the resources of a victim 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 [35].

1) Protocol Exploit 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 so as to tie up the server's processor resources, and hence prevent the server from responding to the requests from legitimate user. 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 are 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 resources, and is unable to respond to legitimate users [35].

In a *PUSH + ACK attack*, the attacking agents send TCP packets with the PUSH and ACK bits set to one. These triggers 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 incoming packets and the victim system will eventually crash.

2) 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 [2,35].

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 options* 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].

3.4. 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 so as to drop some or all of the data packets for further forwarding even when there is no congestion in the network, is known as Malicious Packet Dropping-based DDoS attack [36]. 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 a HTTP response packet after receiving a 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 [37].

Problems Due to DDoS Attacks:

- DDoS attack is an attempt to make a computer resource inaccessible to its legitimate users.
- The bandwidth of the Internet and a 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.
- Gradual increase in the number of fake emails received due to DDoS attacks.

4. Mobile Ad Hoc Network (MANET) Overview

4.1. MANET Overview

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 forwarding 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 among the nodes [38].

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 military applications possible with ad hoc networks. Even the technology was initially developed for the military applications. In such situations, the ad hoc networks having self-organizing capability can be effectively used where other technologies either fail or cannot be deployed effectively. 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 network where nodes are usually associated with someone. 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.

Mobile Adhoc Network Usage and Characteristics: MANETs have a number of characteristics and challenges which are as follows [39]:

- *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 a MANET.
- *Bandwidth-constrained*, *variable capacity links*: Wireless links will continue to have considerably lower capacity than their hardwired counterparts. Also, 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 a 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 possibility of different attacks should be carefully considered.

Security goals for MANET: 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:

- *Availability*: 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.
- *Confidentiality*: 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.
- *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.
- *Authentication*: 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.
- *Non-repudiation*: Ensures that the originator of a message cannot refuse sending this message. This attribute is useful when trying to detect isolated compromised nodes.

4.2. Manet Routing Protocols

The routing protocols in ad hoc networks may be categorized as proactive routing protocols, reactive routing protocols, and hybrid routing protocols [40].

- 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) [41].
- 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 shows the categorization of various mobile ad hoc network routing protocols and their subtypes [42].

4.3. Overview of AODV Routing Protocol

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol [43,44] is built on the Dynamic Destination Sequenced Distance-Vector (DSDV) algorithm. AODV is a betterment of DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, and does not maintain a complete list of routes as in the DSDV algorithm [43]. AODV is classified as a pure on-demand route finding system, since nodes that are not on a selected path do not maintain routing information nor do they participate in the routing

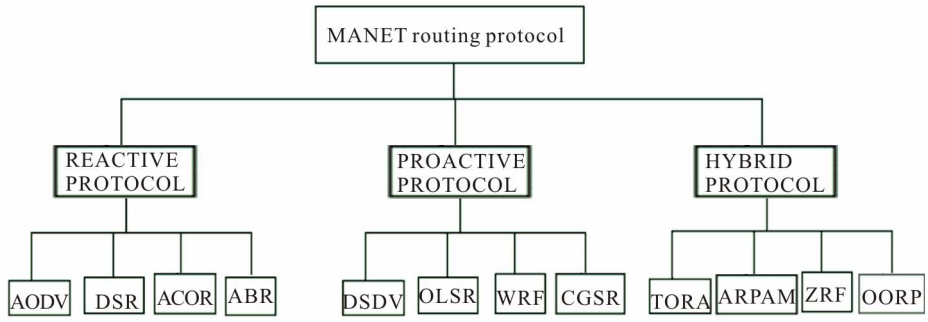

Figure 5. MANET routing protocols.

table maintenance. In general, the operations in AODV can be classified into two phases: the route construction phase and the route maintenance phase. The main work in route construction phase is to create a route from source node to destination node while in route maintenance phase, the main work is to rebuild a route between source and destination nodes since the previous found route may be broken due to the nodes movement.

In the route construction phase, when a source node wants to send packets to a destination node and there is no valid route between the source node and the destination node, the source node commences a path discovery process to locate the destination node. The source node will broadcast a route request (RREQ) packet to explore a route to the destination. AODV uses the destination sequence number to ensure that all routes are loop-free and contain the most recent route information [43].

During the route discovery process, each intermediate node that gets the RREQ packet will again broadcast this packet to its neighbors. The duplicate copies of the same RREQ message that is received by an intermediate node will be discarded. Once the RREQ reaches the destination or an intermediate node with a fresh route to the destination is located, the destination or the intermediate node will send a route reply (RREP) packet back to the source along the reverse routing path [42].

Figure 6 shows the process of route discovery in AODV. In **Figure 6(a)**, the source node broadcast RREQ packet to its neighbor, and so on, while in **Figure 6(b)**, the destination node send the RREP packet back to the source node.

Advantages:

- The main advantage of this protocol is that routes are established on demand or as when needed and destination sequence numbers are used to check the freshness of the route in the network.
- The connection setup delay is less. Another advantage of AODV is that it creates no extra traffic for communication along existing links.
- Thirdly, distance vector routing is simple, and doesn't require much memory or calculation.

Disadvantages:

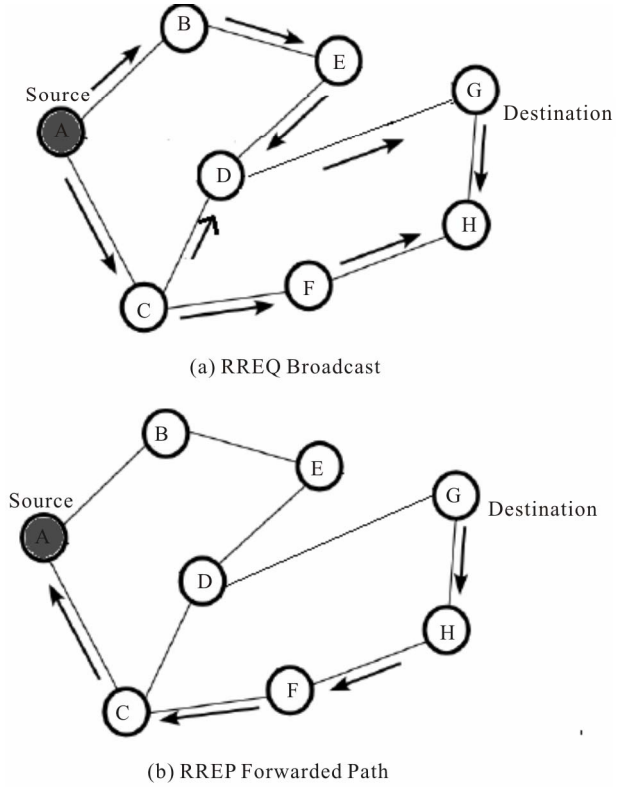

Figure 6. AODV route discovery.

- AODV requires more time to establish a connection as before sending data packets, route to the destination is searched and the initial communication to establish a route is heavy.
- Other disadvantages of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries.
- Thirdly, multiple RREP packets in response to a single RREQ packet can lead to heavy control overhead.

4.4. Flooding Attacks in MANET

The Flooding attack procedure was proposed in [45].

Flood attacks occur when a network or service becomes incapable of providing service to its clients, thereby causing incomplete connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually tries to fill the host's memory buffer thereby not accepting further connections, which causes a Denial of Service attack. To reduce congestion, the protocol has already adopted some methods which are briefly described as follows.

1) Firstly, the number of RREQ that a node can originate per second is limited. Secondly, after broadcasting a RREQ packet, the initiator node will wait for a ROUTE REPLY. If a route is not received within round-trip milliseconds, the node may try again to discover a route by broadcasting another RREQ; until it reaches a maximum of retry times at the maximum TTL value. Time intervals between repeated attempts by a source node at route discovery for a single destination must satisfy a binary exponential back off. The first time a source node broadcasts a RREQ, it waits until the round-trip time for the receiving the ROUTE REPLY (RRPEP) packet [45-48].

2) But for the second RREQ, the time to wait for the ROUTE REPLY should be calculated according to a binary exponential backoff, by which the waiting time now becomes twice of round trip time.

3) Thirdly, The RREQ packets are broadcasted in an incremental ring to reduce the overhead caused by flooding the whole network. At first, the packets are flooded in a small area confined by a small starting time-to-live (TTL) in the IP headers. After RING TRA-VERSAL TIME, if no ROUTE REPLY is received, the forwarding area is enlarged by increasing the TTL by a fixed value.

The procedure is repeated until a ROUTE REPLY is received which means that a route has been found. In the flooding attack, the attack node violates the above rules to exhaust the network resources. Firstly, the attacker will produce many IP addresses which do not exist in the networks if he knows the scope of the IP addresses in the networks. As no node can return ROUTE REPLY packets for these ROUTE REQUESTs, the reverse route in the nodes' route table will be conserved longer than normal. If the attacker cannot get the scope of IP addresses in the network, he can just choose random IP addresses. Secondly, the attacker successively originates mass RREQ messages with these void IP addresses as destination and tries to send excessive RREQ without considering the RREQ RATELIMIT, that is, without waiting for the ROUTE REPLY or waiting a round-trip time. Besides, the TTL of RREQ is set up to a maximum at the beginning without using an expanding ring search method. Under such attack, the whole network will be full of RREQ packets from the attacker. The communication bandwidth and other node resources will be exhausted by the flooded RREQ packets. For example, the storage of route table is limited. If the large amounts of RREQ packets are arriving in a very short time, the storage of the route table in the node will be used up soon so that the node cannot receive new RREQ packets any more [45-47]. **Figure 7** shows the flooding attack mechanism in MANET.

4.5. Effect of Flooding Attacks

Flooding Attack can seriously degrade the performance of reactive routing protocols and affect a node in the following ways. This was proposed in [48].

4.5.1. Degrade the Performance in Buffer

The buffer used by the routing protocol may exceed the limit since a reactive protocol needs to buffer data packets when the RREQ packets are being sent by the source node. Also, if a large number of data packets originating from the application layer are actually unreachable, genuine data packets in the buffer may be replaced by these unreachable data packets, based on the buffer management scheme used.

4.5.2. Degrade the Performance in Wireless Interface

Depending on the design of the interface of wireless network, the buffer used by the wireless network interface may overflow due to the large number of RREQs sent in the route discovery process. Similarly, genuine data packets may be dropped if routing packets have higher priority over data packets.

4.5.3. Degrade the Performance in RREQ Packets

Since RREQ packets are broadcasted into the entire network, the increased number of RREQ packets in the network leads to more collision in MAC layer and thereby congestion in the network and delays for the data

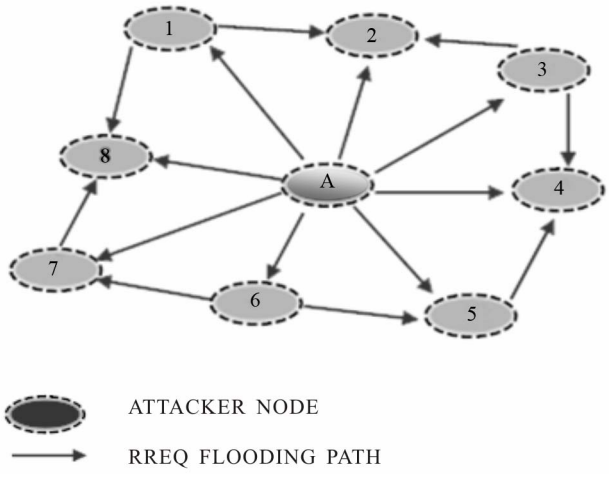

Figure 7. The RREQ flooding attack.

packets. Protocols like TCP that is sensitive to round trip times and congestion in the network gets affected.

4.5.4. Degrade the Performance in Lifetime of MANET

Since MANET nodes are likely to be power and bandwidth constrained, useless RREQ packets transmission can reduce the lifetime of the network also incurring additional overheads of authenticating a large number of RREQs. The following metrics can be used to evaluate the performance of flooding attack.

- 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 maximum throughput that the network can support. The metric characterizes both the completeness and correctness of the routing protocol.
- Average delay: Average of delay incurred by all the packets which are successfully transmitted.
- Throughput: Average number of packets per second X packet size.
- Average number of hops: Total length of all routes divided by the total number of routes.

5. Proposed Prevention Technique

A broadcast is a data packet that is to be delivered to multiple hosts. Broadcasts can be done at the data link layer and the network layer. Packets that are broadcasted at data-link layer are sent to all hosts attached to a particular physical network whereas the packets that are broadcasted to network layer are sent to all hosts attached to a particular logical network.

Since, broadcast packets are destined to all hosts; the goal of the router is to control unnecessary proliferation of broadcast packets. Cisco routers support two kinds of broadcasting, the directed broadcast and the flooded one. In a directed broadcast, a packet is sent to a specific network or series of networks, whereas a flooded broadcast is a packet meant for every network or for every node in the network [36].

Taking the example of flooding broadcast which cause DDoS attack. A nasty type of DDoS attack is the Smurf attack, which is made possible mainly because of the network devices that respond to ICMP echoes sent to broadcast addresses. The attacker node sends a large amount of ICMP traffic to a broadcast address and uses a victim's IP address as the source IP so the replies from all the devices that respond to the broadcast address will flood the victim. The surprising part of this attack is that the attacker uses a low-bandwidth connection to kill a high-bandwidth connection. The amount of traffic sent by the attacker is multiplied by a numeric value equal to the number of hosts behind the router that reply to the ICMP echo packets.

The attacker sends a number of ICMP echo packets to the router at 128 Kbps. The attacker, before sending them, modifies the packets by changing the source IP to the IP address of the victim's computer so replies to the echo packets will be sent to that address [36]. The destination address of the packets is a broadcast address of the so-called bounce site. If the router is (mis-) configured to forward these broadcasts to hosts on the other side of the router all this host will reply. That would mean N × 128 Kbps of ICMP replies will revert back to the victim's system, which would effectively disable its 512 Kbps connection. Besides the target system, the ***intermediate*** router is also a victim, and thus also the hosts in the bounce site. A similar attack that uses UDP echo packets instead of ICMP echo packets is called a Fraggle attack [36].

IP Broadcast is used in AODV routing Protocols to broadcast RREQ packets on all the nodes in the network. Flood attack occurs because of initiating lots of RREQ packets in the network so that network becomes congested and no bandwidth is available to send packets. Hence, we need to keep a check on the number of the RREQs which are broadcast to all nodes.

We put a threshold value on the number of packets, which can be sent by a node and if a node exceeds the threshold value then it will be considered as an attacker node.

In the detection technique, each node comes into processing. For each attack, the node that runs the corresponding detection rule is the "monitoring" node, and the node whose behavior is being analyzed (*i.e.*, the possible attacking or misbehaving node) the "monitored" node. The monitoring node is a 1-hop neighborhood of the "monitored" node. For Flooding, only the attack type, but not the attacker, can be identified by a monitoring node.

The monitoring node will send a "Hello" packet to its next neighborhood node, *i.e.* the monitored node and will wait for its reply. If it does not get reply within the set interval then the node being monitored is flooded node that is the victim node. Later, the id of this node will be disabled and the entry of victim node will be deleted from the routing tables of all nodes. After finding the nodes, we handle it by finding the path in which attack is being executed and sum up the broadcast ids whose effect will be nullified. Code for the technique will be implemented in neighbor management function, Get Broadcast ID function and finalize function of aodv.pc file. **Figure 8** describes the procedure of the proposed model in the form of a flow chart.

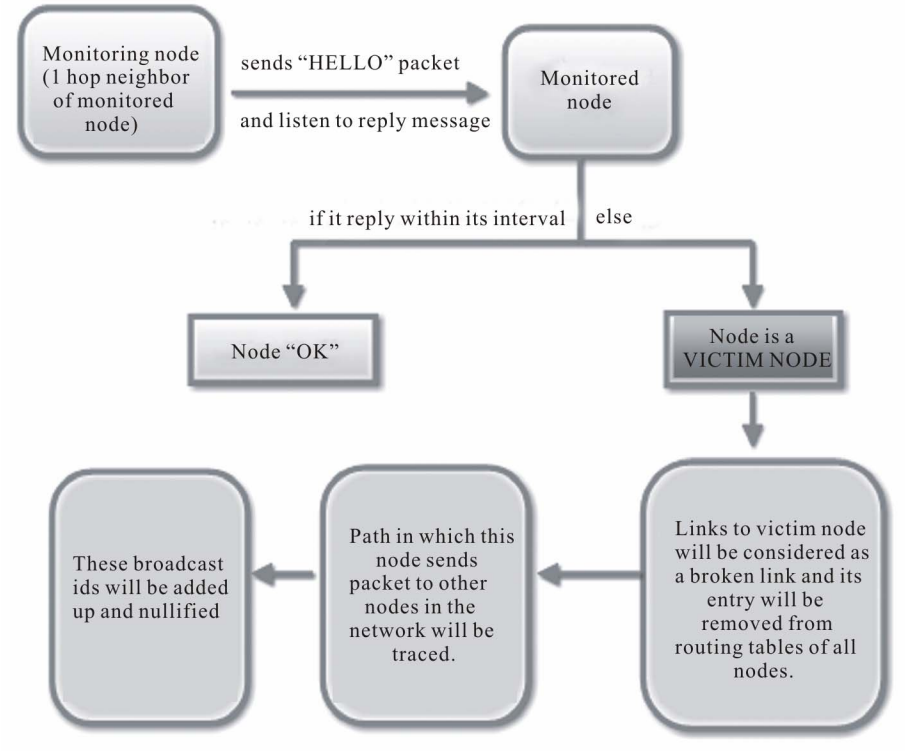

Figure 8. Proposed model for DDoS attack prevention.

6. 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 the lack of a trusted centralized authority and limited resources. There is an urgent need to develop a scheme to handle DDoS attack in mobile ad hoc network. 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. In addition to this, a novel solution is proposed to handle DDoS attacks in mobile ad hoc networks (MANETs).

REFERENCES

[1] C. S. R. Murthy and B. S. Manoj, "Ad-Hoc Wireless Networks Architectures and Protocols," Prentice Hall Communications Engineering and Emerging Technologies Series, 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] S. Taneja and A. Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks," *International Journal of Innovation, Management and Technology*, Vol. 1, No. 3, 2010, ISSN: 2010-0248.

[4] D. Lee, "Global Internet Slows after Biggest Attack in History," 2013. http://www.bbc.co.uk/news/technology-21954636

[5] B. B. Gupta, R. C. Joshi and M. Misra, "Defending against Distributed Denial of Service Attacks: Issues and Challenges," *Information Security Journal*: *A Global Perspective*, Vol. 18, No. 5, 2009, pp. 224-247.

[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] K. Biswas and Md. Liaqat Ali, "Security Threats in Mobile Ad-Hoc Network," Master Thesis, Blekinge Institute of Technology, Blekinge, 2007.

[8] A. Piskozub, "Denial of Service and Distributed Denial of Service Attacks," *Proceedings of the International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science*, Lviv-Slavsko, 18-23 February 2002, pp. 303-304.

[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] 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.

[11] S. M. Specht, "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures," *ISCA* 17*th*

International Conference on Parallel and Distributed Computing Systems, San Francisco, 15-17 September 2004, pp. 543-550.

[12] Q. M. Li, "On the Effectiveness of DDoS Attacks on Statistical Filtering," *INFOCOM* 2005, 24*th Annual Joint Conference of the IEEE Computer and Communications Societies*, Miami, 13-17 March 2005, pp. 1373-1383.

[13] F. Xing and W. Y. Wang, "Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks," *Military Communications Conference*, *MILCOM* 2006, Washington DC, 23-25 October 2006, pp. 1-7.

[14] Y. H. Guo and M. Simon, "Network Forensics in MANET: Traffic Analysis of Source Spoofed DoS Attacks," Fourth International Conference on Network and System Security, Melbourne, 1-3 September 2010, pp. 128-135. doi:10.1109/NSS.2010.45

[15] B. Xiao, W. Chen and Y. Xian, "A Novel Approach to Detecting DDoS Attacks at an Early Stage," *The Journal of Supercomputing*, Vol. 36, No. 3, 2006, pp. 235-248.

[16] A. Challita, M. El Hassan, S. Maalouf and A. Zouheiry, "A Survey of DDoS Defense Mechanisms," *FEA Student Conference*, 2004. http://webfea-lb.fea.aub.edu.lb/proceedings/2004/SRC-ECE-39.pdf

[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* 16*th 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] J. Lo, *et al*., "An IRC Tutorial," 1997. http://www.irchelp.org/irchelp/irctutorial.html#part1

[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. doi:10.1145/505659.505664

[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 Bandwidth 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] P. J. Criscuolo, "Distributed Denial of Service Trinoo, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht, CIAC-2319," Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev.1, Lawrence Livermore National Laboratory, Livermore, 2000.

[29] S. Bellovin, M. Leech and T. Taylor, "ICMP trace back messages," Internet Draft: draft-ietf-itrace-01.txt, Work in Progress, 2001.

[30] 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.

[31] TFreak, 2003. www.phreak.org/archives/exploits/denial/smurf.c

[32] Fed CIRC, "Defense Tactics for Distributed Denial of Service Attacks," Federal Computer Incident Response Center, Washington DC, 2000.

[33] TFreak, "fraggle.c," 2003. www.phreak.org/archives/exploits/denial/fraggle.c

[34] M. J. Martin, "Router Expert: Smurf/Fraggle Attack Defense Using SACLS," Networking Tips and Newsletters, 2002.

[35] 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.

[36] 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.

[37] 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.

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

[39] A. Nayyar "Enhanced Anomaly Detection IDS-Based Scheme for Dynamic MANET On-Demand (DYMO)

Routing Protocol for MANETS," *International Journal of Computer Science and Mobile Computing*, Vol. 2, No. 4, 2013, pp. 384-390.

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

[41] 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.

[42] C. E. Perkins, E. M. Belding-Royer and S. R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," 2*nd IEEE Workshop on Workshop Mobile Computing Systems and Applications*, New Orleans, 25-26 February 1999, pp. 90-100.

[43] S. Saraeian, F. Adibniya, M. G. Zadeh and S. A. Abtahi, "Performance Evaluation of AODV Protocol under DDoS Attacks in MANET," *World Academy of Science*, *Engineering and Technology*, Vol. 45, 2008, p. 501.

[44] G. S. Tomar, T. Sharma, D. Bhattacharyya and T.-H. Kim, "Performance Comparision of AODV, DSR and DSDV under Various Network Conditions: A Survey," 2011 *International Conference on Ubiquitous Computing and Multimedia Applications*, Daejeon, 13-15 April 2011, pp. 3-7.

[45] C. CenGen, "Allocations for Mobile Ad Hoc Network (MANET) Protocols," IANA, Marina del Rey, 2009.

[46] P. Ning and K. Sun, "How to Misuse AODV: A Case Study of Inside Attacks against Mobile Ad-Hoc Routing Protocols," *Proceedings of the* 2003 *IEEE Workshop on Information Assurance United States Military Academy*, West Point, New York, 18-20 June 2003, pp. 60-67.

[47] M. Y. Dangore and S. S. Sambare, "A Survey on Detection of Blackhole Attack Using AODV Protocol in MANET," *International Journal on Recent and Innovation Trends in Computing and Communication*, Vol. 1, No. 1, 2013, pp. 55-61.

[48] M. B. Guddhe and M. U. Kharat, "Core Assisted Defense against Flooding Attacks in MANET," 2009. http://www.nsnam.org

