Journal of Information Systems and Communication
ISSN: 0976-8742 & E-ISSN: 0976-8750, Volume 3, Issue 1, 2012, pp.-310-314
Available online at http://www.bioinfo.in/contents.php?id=45

THE DDOS ATTACKS IN MANET- A REVIEW

KRISHAN KUMAR SALUJA[1] AND PARVEEN KAKKAR[2]

[1]Deptt. of Computer Science and Engineering, S.B.S.C.E.T Ferozepur, India.
[2]Deptt. of Computer Science and Engineering DAVIET, Jalandhar, India.
*Corresponding Author: Email- k.saluja@rediffmail.com, k.saluja@ieee.org, parveenkakkar@rediffmail.com.

Received: January 12, 2012; Accepted: February 15, 2012

Abstract- Security is a weak link of network systems. The malicious usage and attacks have caused tremendous loss by impairing the functionalities of the computer networks. Among all network attacks, Denial of Service (DoS) and Distributed DoS (DDoS) attacks are two of the most harmful threats to network functionality. Mobile Ad Hoc networks are even more vulnerable to these attacks. Existing MANET routing protocols, such as Ad Hoc On-Demand Distance Vector Routing Protocol (AODV), do not provide enough security defense capacity. AODV is inherently vulnerable to many attacks viz. authentication, availability, integrity & confidentiality attacks. Major research efforts have been taken to solve this problem. But most of the proposed solutions are not feasible or practical for the operating MANETs. Because some or all nodes of the MANETs are in a dispersal pattern, or the nodes could be possessed by individuals, it is difficult to apply a network-wide security upgrade. Not only operating MANETs but also any upcoming or planned MANETs face this problem. Various kind of DDoS attacks are identified & explored in different classifications viz Legitimate based, Interaction based & Network protocol stack based classification etc. Though an upcoming MANET can apply the up to date defense strategy, any unpredictable, unforeseen DDoS attack technique in the future can threaten the network and put it in the same situation of those operating unsafe MANETs.

Keywords- Denial of Service (DoS), Distributed Denial of Service (DDoS), Ad Hoc On-Demand Distance Vector Routing Protocol (AODV), MANET

Citation: Krishan Kumar Saluja and Parveen Kakkar. (2012) The DDoS Attacks in MANET- A Review. Journal of Information Systems and Communication, ISSN: 0976-8742 & E-ISSN: 0976-8750, Volume 3, Issue 1, pp.-310-314.

Introduction

A Mobile Ad Hoc Network (MANET) is a decentralized, self-organizing, and adaptive gathering of independent mobile nodes, which are communicating over wireless links. Each node is both a network user and a router. Because of the mobility of each node, the network topology may change frequently and be unpredictable. MANETs are attractive in military or civil situations where a rapid deployment and dynamic adaptation are required [1]. Comparing with wired networks, MANETs offer advantages such as mobility, flexibility, and no fixed infrastructure required, but there are more research challenges for Wireless networks

- The limited radio signal range requires a wireless node to stay within the network [2].
- The radio signal could be blocked or absorbed by some objects, and interfered or reflected by some others. The radio signals in the same band from the nearby nodes would collide each other. The range restriction and possible collisions makes packet loss more likely. Therefore, the bandwidth is often lower than that of a wired network. But some new standards (e.g. 802.11 Wi- Fi and 802.16 WiMAX) claim wireless bandwidth comparable to those of Ethernet [3].
- The mobile nodes have limited battery and computation power. Some power saving strategies may be applied. The nodes may listen to the receivers periodically; therefore, the nodes may not receive the signals in time. They may also need time to wake up and get ready for the communication. This may lead to high communication latency [4].
- Because of the mobility and flexibility of the nodes, it is re-

quired to quickly adapt to the change of the network topology and look up the specific node. A commercial MANET needs to implement a QoS solution for the traffic [5].
- Because of the mobility and the dynamic construction of the ad hoc nodes, one essential research topic of MANETs is about accurate and efficient service discovery, lookup and verification methods [7].

This paper highlights various security challenges & issues pertaining to the security of mobile Ad-Hoc networks. Various kinds of DDoS Attacks are identified & explored in different classifications viz Legitimate based, Interaction based & Classification of security attacks at different layers etc.

The rest of the paper is organized as follows. Section II focus on some security challenges & issues of MANET. Section III depicts identification of DoS & DDoS Attacks in MANET. Section IV depicts the classification of DDoS Attacks. Finally Section V concludes the paper

Security Challenges & Issues Of Manets

- MANETs use wireless media for transmission, which introduces security flaws to the networks. Basically any one with the proper equipment and knowledge of the current network topology and the protocols may obtain access to the network. Both active and passive attacks such as impersonation, eavesdropping, message redirection, and traffic analysis, can be performed by an adversary.
- In specific scenarios, MANET nodes may be scattered over a large area. Some nodes or network components may be unmonitored or hard to monitor, and exposed to the physical attacks.
- Because MANETs do not have any central authority, this is a major barrier to security. The security mechanisms employed in wired networks, such as Public Key Management, Node Authentication, and Determination of Node Behavior, are in fact very difficult to achieve without any central administration.
- Ad hoc networks are highly dynamic in nature. Node joins and departures are not predictable. Moreover, network topology is always changing in Ad Hoc networks. Therefore any static security mechanism will not be applicable in MANETs. In other words, security primitives must be dynamically adjusted to cope with the network. This is a daunting task.

There are many IP trace back schemes proposed for the internet e.g. link testing, logging etc. but these schemes are not applied to MANET directly because MANET has no fixed infrastructure. Each node works as an autonomous terminal, acting as both host and a router. Another is bandwidth is limited. Battery power is limited. Frequent change in the network topology when a node moves in and out in the topology. Mobile adhoc Network is an increasingly promising area with many of the practical applications. But, it is vulnerable to number of security attacks including the DoS (Denial of Service) attack due to its autonomous nature. In mobile adhoc networks various kinds of the DoS (Denial of Service) attacks are possible. In an ad hoc wireless network where wired infrastructures are not feasible, energy and bandwidth conservation are the two key elements presenting research challenges. Limited bandwidth makes a network easily congested by control signals of the routing protocol. Routing schemes developed for wired networks seldom consider restrictions of this type.

A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. In DoS actually what happens, the available Bandwidth is attacked with malicious traffic and then the original traffic is restricted to flow, which means that the bandwidth is hacked.

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System servers.

The most common DoS attacks are similar SYS flood, smurf, and UDP flood. Attackers routinely disguise their locations by using incorrect or spoofed source address.

A DoS attack can be perpetrated in a number of ways.

Denial-Of-Service (Dos) Distributed Denial-Of-Service Attacks (Ddos) In Manet

Among all the Internet attacks, DoS attacks are one of the most significant threats to network functionality. DoS attacks exhaust the network's resource of a specific Internet service or system so that the legitimate users lose the access to the resource. The first DoS attack case happened on Panix, the ISP (Internet Service Provider) of New York City area on September 6, 1996. According to the 2004 FBI Report on Cybercrime, the total reported costs of DoS attacks were over $26 million [7]. Denial of service was the top source of financial loss due to cybercrime in 2004 [7]. DoS attacks exploit the vulnerabilities of the network protocol architecture. They do not need complicated technology, and they are very easy for attackers to launch, but very hard for victims to prevent and track back. According to the attack trail, DoS attacks are classified as direct and reflected Types (Figure 1) [7].

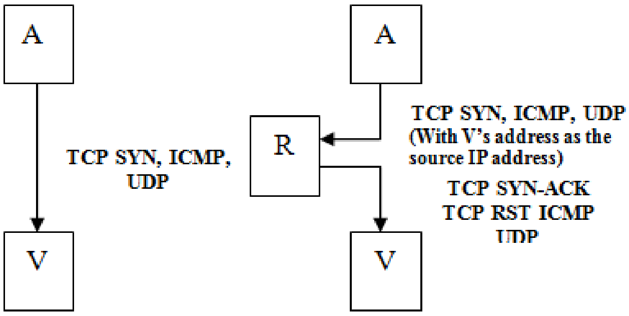
A
V
TCP SYN, ICMP, UDP
A
R
V
TCP SYN, ICMP, UDP (With V's address as the source IP address)
TCP SYN-ACK TCP RST ICMP UDP

Fig. 1- Direct & Reflected Attacks

Some specific DDoS types are listed below

- SYN Flooding. The attack uses the weakness of the TCP handshake. It sends an abundance of TCP SYN packets to the victim. The victim opens a lot of TCP connections and responds with ACK. But the attacker does not finish the handshake, which, in result, causes the half-open TCP connections to overflow the victim's incoming queue. SYN Flooding does not target specific Operating System, so it may attack any system supporting TCP protocol (Figure 2) [17].

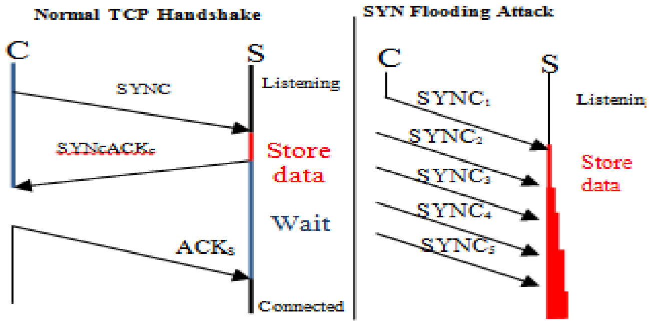

Fig. 2- SYN Flooding Attack

- Ping of Death The attacker sends the victim oversized IP packets, which contain more than 65,536 bytes. It may cause the victim machine to crash [18].
- Process Table The attacker sends an abundance of uncompleted connections to the victim server. The victim will create a new process for each connection until it cannot serve any more requests.
- Smurf Attack The attacker sends the broadcast address an abundance of Internet Control Message Protocol (ICMP) "echo-request" packets, which has the victim's IP as the source address. The victim will be flooded with ICMP "echo-reply" packets [19].
- SSH Process Table The attacker overflows the SSH daemon in the victim system. It is similar to the process table attacks.
- TCP Reset The attacker listens the traffic for the "tcpconnection" requests to the victim. Once such a request is found, the attacker sends a spoofed TCP RESET packet to the victim and obliges it to stop the TCP connection [17].
- Teardrop The attacker creates a stream of IP fragments with their offset field overlapped. The victim may crash when trying to reassemble these malformed fragments [15].
- UDP Packet Storm The attacker spoofs a start packet and builds a connection between two victim nodes, which provide a type of UDP output services (such as "chargen" or "echo") to generate numerous traffic into the network [18].

DDoS attacks first appeared in the summer of 1999. The victims were several high capacity commercial and educational websites [12]. The characteristics of Distributed Denial-of-Service (DDoS) are "WMD" (Wide, Massive, Dissemination). DDoS attacks are more powerful, leading to greater damage and easier to perform by Trojan horses, but harder to be prevented and traced back because of the numerous compromised civilian nodes. DDoS attackers user a group of compromised nodes (zombies) to carry on a "large-scale coordinated" attack against the target nodes, where compromised nodes are called the "secondary victims", and the target nodes are called the "primary victims". DDoS traffic stream is not unusually high near the attack sources, so it is hard to detect DDoS attacks in the early stages when the attack traffic is still close to the source. This characteristic provides a good concealment to the real attacker. DDoS traffic streams congest the victim node and often, the intermediate nodes ahead of the victim. This characteristic provides the maximum damage effect to the victim. The victim could be overwhelmed before it takes any defensive action, or the intermediate nodes ahead of the victim may be crashed and the victim will not receive any warning. There are many tools now on the Internet making a DDoS attack much easier to launch. These tools are classified as either Agent-Handler model or the IRC-based model. With Agent-Handler tools, such as Trinoo, Tribe Flood Network (TFN), and mstream and so on, an attacker can command the compromised nodes to generate a flooding attack (Figure 3). Stacheldraht combines the features of both Trinoo and TFN, and it encrypts the communication inside the attack system.

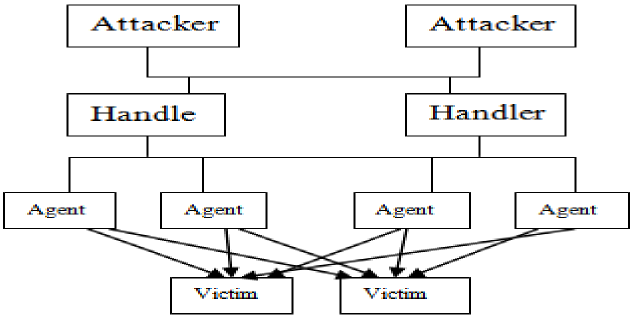

Fig. 3- Agent-Handler DDoS attack

IRC-based Botnet type tools have become popular to deploy DDoS attacks The Botnets are often an IRC program, which is installed on the compromised hosts by attackers. Eggdrop and Agobot are two well-known Botnet tools. The Agent-Handler commands have easily detectable patterns; while IRC based Botnets communication is more flexible and concealed. Except to launch the DDoS attacks, Botnets are also used to install Advertisement Addons to the web browsers, identity theft, spamming, and other malicious activities. To illustrate the danger of the Botnet, the Honey net project claims that they observed 226,585 unique IP addresses compromised to the Botnet attackers in only few months.

Classification Of Dos And Ddos Attacks In Manet's

Attacks on MANETs come in many varieties and they can be classified based on different aspects.

Legitimate Based Classification

According to the legitimate status of a node, an attack could be external or internal. The external attacks are committed by nodes that are not legal members of the network, while the internal attacks are from a compromised member inside the network. The internal attacks are not easy to prevent or detect. These attackers are aware of the security strategies, and are even protected by them. The internal attacks pose a higher threat to the network.

Interaction Based Classification

In terms of interaction, an attack could be passive or active. Passive attacks do not disrupt the communication. Instead, they intercept and capture the packets to read the information. On the other hand, active attackers inject packets into the network to interfere or interrupt the network communication, overload the network traffic; fake the legitimate node or package, obstruct the operation or cut off certain nodes from their neighbors so they cannot use the network services effectively anymore. DoS or DDoS are active attacks (Figure 4).

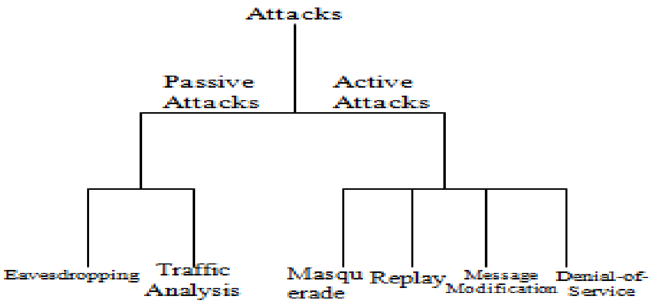

Fig. 4- Taxonomy of MANET Attacks

Classification of Security Attacks at Different Layers

Attacks could also be classified according to the target layer in the protocol stack (Figure 5).

Physical Layer Attacks

By targeting the physical layer of a wireless network or a wireless node, an attacker can easily intercept and read the message contents from open radio signals. An attacker can jam or interfere the communication by generating powerful transmissions to overwhelm the target signals. The jamming signals do not follow the protocol definition, and they can be meaningless random noise and pulse [13].

Link Layer Attacks

By targeting the link layer, an attacker can generate meaningless random packets to grab the channel and cause collision. In this situation, if the impacted node keeps trying to resend the packet, it will exhaust its power supply; the attacker can passively eavesdrop on the link layer packets; the link layer security protocol WEP is vulnerable too, the initialization vector (IV) flaw in the WEP protocol makes it easier for an attacker to launch a cryptanalytic type attack.

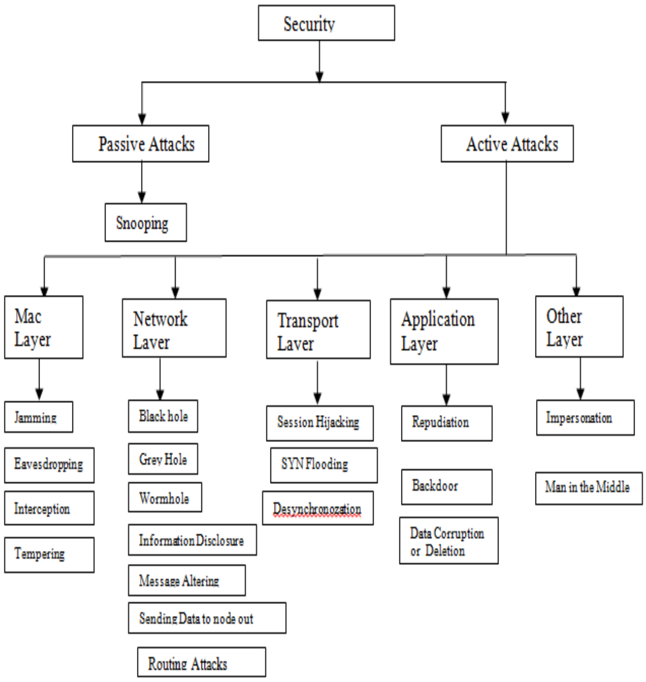

Fig. 5- Classification of Security Attacks at different layers

Network Layer Attacks

Coming along with many new routing protocols introduced to the MANETs, many new types of attacks were presented to target these specific protocols.

- Black hole attacks Distance-Vector type routing protocols. A black hole attacker responds to all RREQ with a shortest route RREP. After the attacker grabs the route, it may drop all the packets, or selectively forward some of the packets to hide the malicious nature. It is also the first step in the man-in -the-middle attacks[9] (Figure 6).Local Intrusion Detection security routing mechanism to Detect BHA(Black Hole Attack) over AODV (Ad hoc On Demand Distance Vector) MANET routing protocol. Cooperative black hole attacks over AODV are discussed in [19]

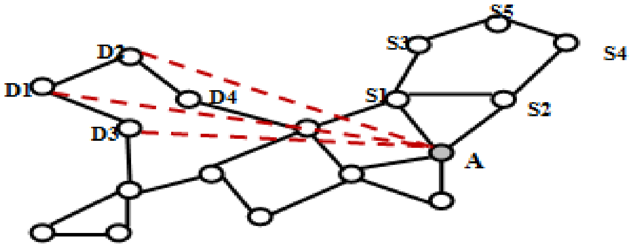

Fig. 6- Black Hole attack

Attacker A claims to have shortest route to D1, D2, and D3

- “Byzantine” attackers respond to the RREQ with wrong route information to disrupt or degrade the routing services, such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets.
- “Flooding” methods used by DoS and DDoS attackers in wired networks have the same effect on the MANET environment.
- “Location disclosure” attackers disclose the security-sensitive location information of nodes or the topology of the network.
- “Misdirection” attackers lead the packets to a wrong way and toward the victim. Similar to Smurf attacks.
- “Packet dropping” attackers disrupt the network communication, and they are very hard to detect. This type of attack is often working along with other attack methods to amplify the damage.
- “Resource consumption” or so-called “Sleep deprivation” attackers try to waste the power of the legitimate nodes by requesting excessive route discovery, forwarding useless packets to the victim node, or endlessly “dangling” useless packets between two distant attackers.
- “Rushing” attackers have more power and quicker links than legitimate nodes [19]. They may forward the RREQ and RREP faster. By this way, they are always involved in the routes (Figure 7).

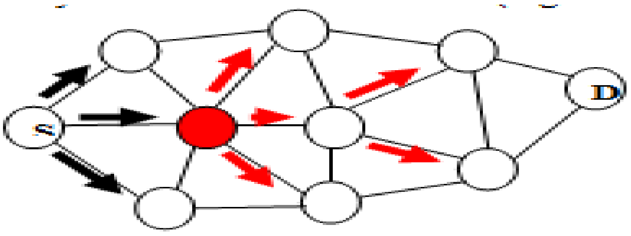

Fig. 7- Rushing Attack

- “Selfish” nodes use the network but do not cooperate. They save the battery life, CPU cycles, and other resources for their own packets. Though they do not intend to directly damage other nodes, the result is less damaging inefficient networking [19].
- “Spoofing” attackers impersonate a legitimate node to misrepresent the network topology to cause network loops or partitions.
- “Wormhole” attacker’s forward packets between each other by a tunnel instead of hop based routing method as defined by the protocol. Routing may be disrupted by tunneled routing control messages. Wormhole attacks are severe threats to MANET on-demand routing protocols [20]. Wormhole attack detection & prevention scheme which is based on a social science theory called the diffusion of innovations and serves all network nodes in detecting and preventing the attack even without prior interaction with malicious nodes. [20]. The attack could prevent the discovery of any route other than through the wormhole (Figure 8).

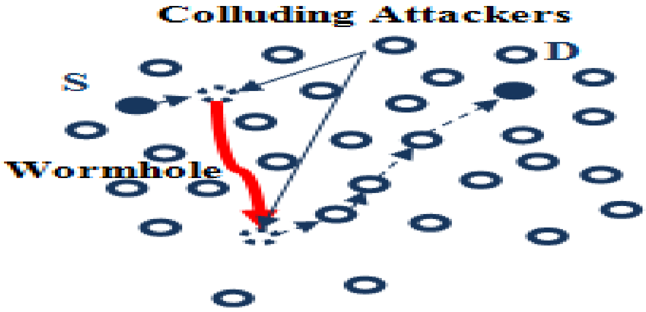

Fig. 8- Wormhole Attack

Wormhole attack defense strategies are often based on space or time relativity, such as geographical leashes, temporal leashes, or a graph theoretic approach.

Transport Layer Attacks

By targeting the transport layer, a “desynchronization” attacker can break an existing connection between two nodes by sending fabricated packets exceeding the sequence number to either node of the connection. It may result in letting the node keep sending retransmission requests for the missed frames. A “Session Hijacking” attacker impersonates the victim node and takes over the TCP session between the victim and the server.

Application Layer Attacks

By targeting on the application layer, a “Repudiation” attack is a threat to a business that relies on electronic traffic. Some examples are described in Other application layer attacks, such as viruses, worms, Trojans, spywares, backdoor, and data corruption or deletion, target either application layer protocols, such as FTP, HTTP, and SMTP, or applications and data files on the victims.

Conclusion

This paper reveals the security challenges & issues of Mobile Ad Hoc Networks (MANET). An attempt has been made to classify all the network attacks on the behalf of different classifications viz Legitimate Based, Interaction based and Network Protocol Stack based Classification. It is concluded that among all network attacks, Denial of Service (DoS) and Distributed DoS (DDoS) attacks are two of the most harmful threats to network functionality. Mobile Ad Hoc networks are even more vulnerable to these attacks. Existing MANET routing protocols, such as Ad Hoc On-Demand Distance Vector Routing Protocol (AODV), do not provide enough security defense capacity.

References

[1] Ricochet-Team (2003) *Internet Worms: Self-spreading Malicious Programs*.

[2] CERT (1988) *Computer Emergency Response Team*.

[3] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam and Erdal Cayirci (2002) *Computer Networks*, 38, 393-422.

[4] Jelena Mirkovic, Sven Dietrich, David Dittrich and Peter Reiher (2005) *Internet Denial of Service: Attack and Defense Mechanisms,* 400.

[5] Vern Paxson (2001) *Computer Communications Review*, 31(3), 38-47.

[6] Jonathan Lemon (2002) *Resisting SYN Flood DoS Attacks with a SYN Cache,* 89-97.

[7] Stephen Specht and Ruby Lee (2004) 17*th Int'l Conf. Parallel and Distributed Computing Systems*, 536-543.

[8] Jelena Mirkovic and Peter Reiher (2004) *SIGCOMM Computer Communication Review*, 34(2), 39-53.

[9] Ahsan Habib, Mohamed Hefeeda and Bharat Bhargava (2003) 10*th Annual Network and Distributed System Security Symposium,* 177-189.

[10]Mun Choon Chan, Yow-Jian Lin and Xin Wang (2000) *International Conference on Network Protocols*. *IEEE Computer Society.* 37-48.

[11]Duffield N.G., Lo Presti F., Paxson V. and Towsle D. (2001) *IEEE INFOCOM,* 915-923.

[12]Ahsan Habib, Maleq Khan and Bharat Bhargava (2004) *Journal of Computer and Telecommunications Networking* 44(2), 211-233.

[13]Steven Bellovin, Marcus Leech and Tom Taylor (2000) *ICMP Trace back Messages.*

[14]Kihong Park and Heejo Lee (2001) *IEEE INFOCOM* 338-347.

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

[16] Khor S.H. and Nakao A. (2008) *Over fort: Combating ddos with peer to peer ddos puzzle, in IEEE IPDPS*.

[17] Worldwide Infrastructure Security Report (2008) *http://asert.arbornetworks.com*.

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

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

[20] Marianne A. Azer, Sherif M. El-Kassas and Magdy S. El-Soudani (2010) *IEEE Computer Society*. 366-371.