Research Journal of Applied Sciences, Engineering and Technology 7(10): 2033-2039, 2014
DOI:10.19026/ajfst.7.496
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: June 25, 2013 Accepted: July 19, 2013 Published: March 15, 2014

Research Article

An Efficient Scheme to Prevent DDoS Flooding Attacks in Mobile Ad-Hoc Network (MANET)

Meghna Chhabra and B.B. Gupta
School of Computing Science and Engineering, Galgotias Universiy, Greater Noida, India

Abstract: The purpose of this study is to understand the flaws of existing solutions to combat the DDoS attack and a novel scheme is being provided with its validation to reduce the effect of DDoS attack in MANET Environment. As Internet users are increasing day by day, it is becoming more prone to attacks and new hacking techniques. People are accessing information and communicating with each other on the move. Mobile Ad-hoc Network (MANET) is responsible for this rapid change in the lives of people. With the emergence of technology, where people communicate or share important documentations on the go with the help of laptops, PDAs, notebooks, smart phones etc., the loopholes in the Internet security have also increased and they are becoming more difficult to handle due to the characteristics of MANET 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. The network is becoming more prone to attacks like DDoS, byzantine, resource consumption, blackhole, grayhole, etc. Therefore, there is an urgent need to look into the security issues to allow authorized users to access the information available on Internet without any risk. In this study, a novel scheme is proposed which deals with suppressing the influence of the attack. The effectiveness of the approach is validated with simulation in GloMoSim, integrated with parsec compiler, on a windows platform.

Keywords: ARPANET, DDoS attacks, flooding attack, GloMoSim, MANET

INTRODUCTION

Today, Internet has revolutionized every aspect of the computer and communications world (Leiner *et al*., 2007). The technological evolution began with early research on packet switching and the ARPANET. The Internet was created in 1969 to provide an open network for researchers (CERT, 2007a). Unfortunately, with the growth of the Internet, the attacks to the Internet have also increased incredibly fast. The widespread need and ability to connect machines across the Internet has caused the network to be more vulnerable to intrusions. According to (CERT, 2007a) a mere 171 vulnerabilities were reported in 1995 which boomed to 8064 in the year of 2006. Already, the number for the same for merely the first quarter of 2007 has gone up to 2,176. Apart from these, a large number of vulnerabilities go unreported each year.

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 (Chhabra *et al*., 2013). Its routing protocol has to be able to manage with the new difficulties that an adhoc network creates such as nodes mobility, limited power supply, quality of service, bandwidth issues, changing topology and security issues which make MANET more vulnerable to attacks and security issues.

A Denial of Service (DoS) attack is commonly characterized as an event in which a legitimate user or organization is deprived of certain services, like e-mail or network connectivity, that they would normally expect to have (CERT, 2007b; Houle *et al*., 2001). DoS attacks inject maliciously designed packets into the network to deplete some or all of these resources.

Distributed Denial of Service (DDoS) attacks has also become a problem for users of computer systems connected to the Internet. The attack power of a Distributed DoS (DDoS) attack (Lau *et al*., 2000) is based on the massive number of attack sources instead of the vulnerabilities of one particular protocol. DDoS attacks, which aim at overwhelming a target server with an immense volume of useless traffic from distributed and coordinated attack sources, are a major threat to the stability of the Internet (Elnoubi *et al*., 2011). Distributed Denial of Service (DDoS) attacks pose an immense threat to the Internet and many defines mechanisms have been proposed to combat the problem. Attackers constantly modify their tools to bypass these security systems and researchers in turn modify their approaches to handle new attacks

Corresponding Author: B.B. Gupta, School of Computing Science and Engineering, Galgotias University, Greater Noida, India

(Mirkovic *et al*., 2004). The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated (Gupta *et al*., 2009).

The number and assortment of both the attacks as well as the defense mechanisms is monstrous. Though an array of schemes has been proposed for the detection of the presence of these attacks, characterization of the flows as normal or malicious, identifying the source(s) of the attacks and mitigating the effects of the attacks once they have been detected, still there are loopholes in the defense system against DDoS attacks.

Various DDoS attacks against high-profile websites such as yahoo, CNN Amazon and E Trade in early 2000, series of attacks on GRC.Com in May, 2001 (CERT, 2007b) and my doom virus attack on SCO website in Feb. 2003 demonstrate how devastating DDoS attacks are and how defenseless the Internet is under such attacks. As proof of these disturbing trends, a 2004 FBI/CSI survey concluded that DDoS attacks were the number one cause for financial losses resulting from cyber crime. The services of these websites were unavailable for hours or even days as a result of these attacks (Gupta *et al*., 2009). A recent DDoS attack reported was on Netflix and Spamhaus in March 2013 caused a great harm to these organizations.

The mobile ad hoc networks have several salient characteristics, such as Dynamic topologies, Band width-constrained, variable capacity links, Energy-constrained operation, Limited physical security (Douligeris and Mitrokotsa, 2004). Due to these features, mobile ad hoc networks are particularly vulnerable to denial of service attacks launched through compromised node (Chhabra *et al*., 2013). In this study, a novel scheme is proposed which deals with suppressing the influence of the attack. The effectiveness of the approach is validated with simulation in GloMoSim, integrated with parsec compiler, on a windows platform.

Overview of DoS and DDoS attack: A DoS attack can be described as an attack designed to render a computer or network incapable of providing normal services to its legitimate users. It is considered to take place only when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user. Therefore, as defined by Weiler (2002), it includes any of the following attempts (Gupta *et al*., 2008):

- To inhibit legitimate network traffic by flooding the network with useless traffic
- To deny access to a service by disrupting connections between two parties
- To block the access of a particular individual to a service
- To disrupt the specific system or service itself

The main aim of such attacks is to prevent the victim either from the benefit of a particular service (in case of client being victim) or from providing its services to others (in case of server being victim) (GloMoSim, Year).

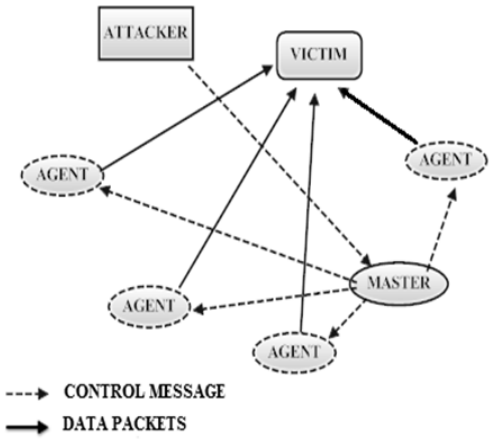

Fig. 1: DDoS attack components

Distributed Denial-of-Service (DDoS) attack can usually cause more significant damage than DoS attack by performing attack from many compromised machines. A DDoS attack has two phases named deployment and attack. A DDoS program must first be deployed on one or more compromised hosts before an attack is possible. A DDoS attacker uses many computers to launch a coordinated DDoS attack against one or more targets. This attack is launched indirectly through many compromised computing systems by sending a stream of useless aggregate traffic meant to explode victim resources. As a side effect, these attacks frequently create network congestion on the way from a source to the target, thus disrupting normal Internet operations (Mirkovic *et al*., 2004). Figure 1 shows the DDoS attack method and components. Intruder can perform DDoS attack either as flooding attack or as logical attack (Gupta *et al*., 2009).

In flooding DDoS attack, massive amount of legitimate looking data packets are sent to victims, with the aim of reducing legitimate users' bandwidth, thereby preventing authorized users from accessing a service. Logical attack uses a specific feature of the protocol or the application installed at the target machine so as to consume an excess amount of its resources. The main motives behind DDoS attack could be criminal, commercial, or ideological in nature (Saraeian *et al*., 2008).

Popular DDoS attacks: Today, DoS and the DDoS attacks are one of the latest threats to the users, organizations and infrastructure of the Internet. In these attacks, the main aim of the attacker is to clog up the chosen resources at the victim, by sending a high volume of seemingly legitimate traffic.

Although a large variety of DDoS attacks is reported and is possible, some of them have been more popular with the attackers:

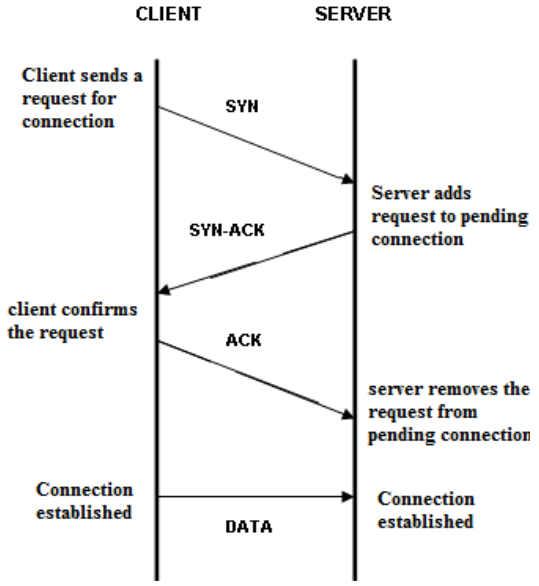

Fig. 2: TCP 3-way handshaking

Algorithm
Detect Dos Attack (S, D) /* S is the source node and D is the Destination Node */
Step-1 As the transmission begins it will search for all the intermediate nodes and send HELLO packet on to it.
Step-2 If (the intermediate node failed to forward the Hello Message to the next node),
{Again call the detection algorithm}
Step-3 It will check the RESPONSE time for the intermediate node.
Step-4 If (Response Time> Hop Time +Threshold)
{The Attacker Node is detected. Update Neighbour Node Table and Routing Table for the Intermediate Nodes}
Step-5 Return.

Fig. 3: Proposed detection technique for DDoS attack

- **TCP SYN flooding attack:** A TCP session Schuba *et al*. (1997) starts with negotiation of session parameters, such as SYN or SYN/ACK, between the client and the server. This is done by the 3-way handshake illustrated in the Fig. 2.
  During SYN flood attacks, the attacker sends SYN packets with source IP addresses that do not exist or are not in use (Wang *et al*., 2002). During the 3-way handshake, when the server puts the request information into the memory stack, it will wait for the confirmation from the client that sends the request. Before the request is confirmed, it will remain in the memory stack. Since the source IP addresses used in SYN flood attacks are non-existent, the server cannot receive confirmation packets for requests created by the SYN flood attack (Kavisankar and Chellappan, 2011). Thus, more and more requests will accumulate and fill up the memory stack. Therefore, no new request, including legitimate requests, can be processed and the services of the system are disabled.
- **ICMP flooding attack:** An Internet Control Message Protocol (ICMP) flooding attack (Schuba *et al*., 1997) comprises of a stream of ICMP ECHO packets generated by the attackers and aimed at the victim. The victim replies to each ICMP request, consuming its CPU and network resources. The Smurf Attack (Alomari *et al*., 2012) is a reflector attack. The attacker directs a stream of ICMP ECHO requests to broadcast addresses in intermediary networks, spoofing the victim's IP address in their source address fields. A multitude of machines then reply to the victim, overwhelming its network.
- **UDP flooding attack:** During this attack (Schuba *et al*., 1997), the victim is flooded by numerous UDP packets that overwhelm its network bandwidth. UDP does not have flow control mechanism. Also, unlike TCP, UDP does not have a negotiation mechanism before setting up a connection (Ihsan *et al*., 2011). Therefore, it is easier to spoof UDP traffic without being noticed by the victim.

METHODOLOGY

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 (Chhabra *et al*., 2013).

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, where as a flooded broadcast is a packet meant for every network or for every node in the network (Chaba *et al*., 2009; Chhabra *et al*., 2013).

IP Broadcast is used in AODV routing Protocols to broadcast packets on all the nodes in the network. Flood attack occurs because of initiating lots of 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 packets which are broadcast to all nodes (Chhabra *et al*., 2013).

Proposed detection technique for DDoS attack: For each attack, the node that runs the corresponding detection rule is "monitoring" node and the node whose behavior is being analyzed the "monitored" node. The nodes between the source and the destination, i.e., the intermediate nodes will be analyzed. For the DDoS attack, the monitoring node is a 1-hop neighborhood of the "monitored" node. Both the attack type and the

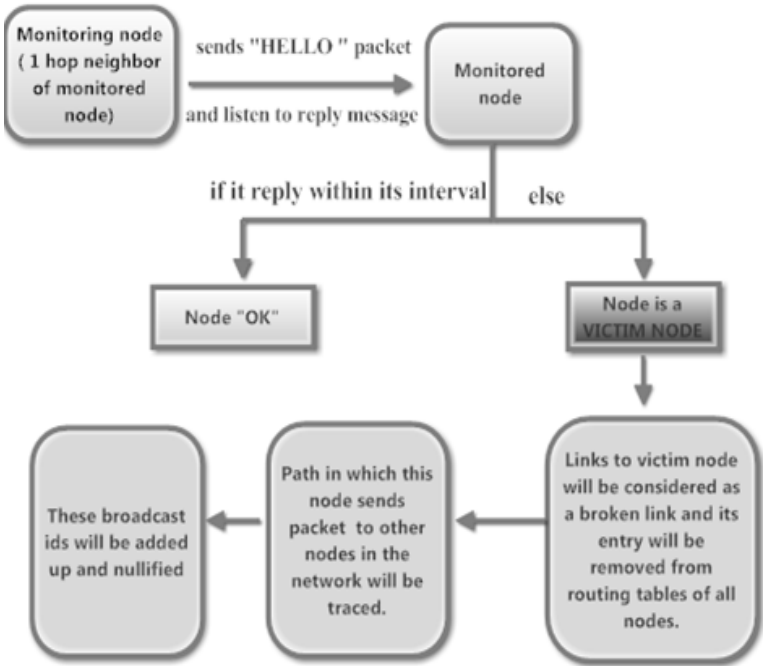

Fig. 4: Proposed prevention scheme for DDoS attack

attacker cannot be identified because the monitoring node can overhear traffic within its 1-hop neighborhood. For Flooding, only the victim node, but not the attacker, can be identified by a monitoring node. Proposed detection technique for DDoS attack is shown in Fig. 3.

Proposed prevention technique for DDoS attack: Proposed technique to implement prevention mechanism is by disabling IP broadcast. IP Broadcast is used in AODV routing Protocols to broadcast packets on all the nodes in the network. Flood attack occurs because of initiating lots of packets in the network so that network becomes congested and no bandwidth is available to send packets.

The monitoring node will send a "Hello" packet to its next neighborhood node, i.e., the monitored node and will listen for its reply message. 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. In this way the attack is being prevented. The code for the technique will be implemented in neighbor management function, get broadcast ID function and finalize function of aodv. pc file.

The proposed prevention scheme can be understood easily with the help of a flowchart as given in the Fig. 4. This shows the complete flow of the proposed methodology. The scheme works effectively and efficiently in case of flooding attack in the network and can suppress the effect of the DDoS attack to a considerable level which is shown by the effect of proposed methodology on throughput, number of collisions and packet delivery ratio when attack takes place as shown in the next section.

Performance metrics: The following quantitative metrics are to be used to evaluate the performance of D Do Sattacks and their prevention techniques under different combinations in the fixed mobile ad hoc network:

- **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:

$$\text{PDR} = \frac{Total\ Number\ of\ packets\ sent}{Total\ Number\ of\ packets\ Received}$$

- **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

Table 1: Simulation parameter

Parameter	Value	Description
Number of nodes	0-50	Network nodes
Terrain range	(1200, 1200)	X,Y dimension of motion in m
Bandwidth	2 Mbps	Node's bandwidth
Simulation time	15-20 m	Simulation duration
Node-placement	Uniform	Node placement policy
Mobility	Random waypoint	Mobility of nodes
Traffic model	CBR	Constant bit rate protocol
MAC protocol	802.11	MAC protocol used
Routing protocol	AODV	Routing protocol used

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.

- **Throughput:** Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps) and sometimes in data packets per second or data packets per time slot.

Experimental setup: This section describes the parameters used in the simulations. The simulation environment used is based on GloMoSim. GloMoSim is a scalable simulator that is designed especially to large wireless networks. It supports thousands of nodes, using parallel and distributed environment (GloMoSim). Table 1 contains various simulation parameters used for simulations.

The simulated environment consists of 50 wireless mobile nodes roaming in 1200×1200 m as shown in Table 1. Nodes were placed uniformly in the given area. MAC protocol 802.11 with AODV routing protocol is used which helps node to route their packets to correct destination. 2 Mbps bandwidth was considered for maximum of 20 min of simulation time. Constant bit rate protocol was used to define the traffic flow in the simulation.

RESULTS AND DISCUSSION

In this section, we will study the effect of DDoS attack on various performance measures, i.e., packet delivery ratio, number of collisions, throughput. Attack is performed using varied number of attackers. Performance of the system is compared when system is in normal condition i.e., no attack, under flooding DDoS attack with no prevention scheme and when proposed prevention scheme is used.

Effect of attack on packet delivery ratio when attack is performed with varied number of attackers: In this section, we will study the effect of DDoS attack on packet delivery ratio. Attack is performed using varied number of attackers. Performance of the system is compared when system is in normal condition i.e., no attack, under flooding DDoS attack with no prevention scheme and when proposed prevention scheme is used.

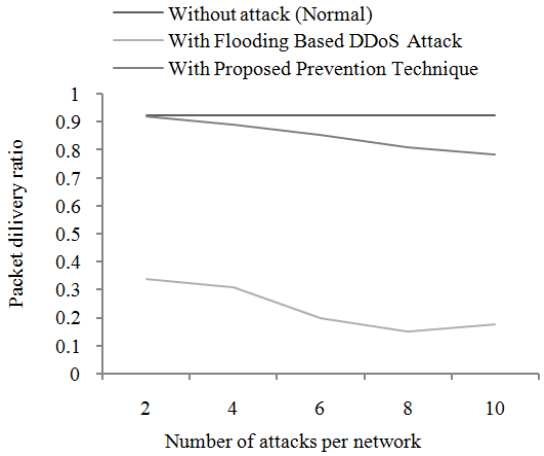

Fig. 5: Effect of attack on PDR with varying number of attackers

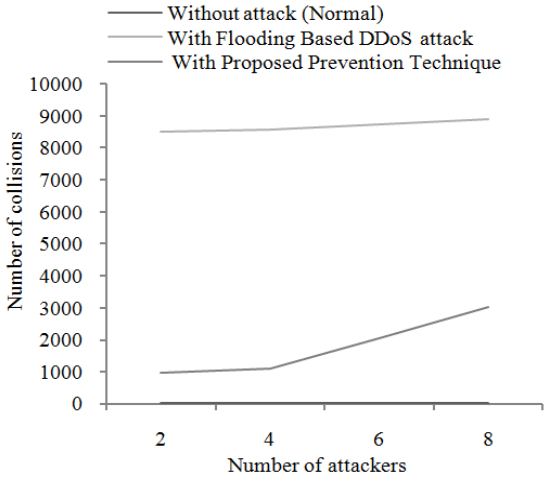

Fig. 6: Effect of attack on the number of collisions in the network with varying number of attackers

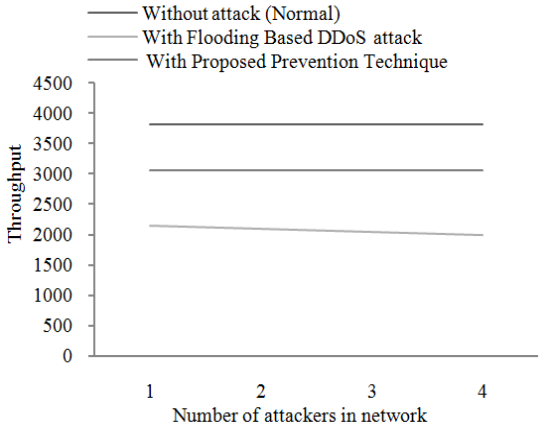

Fig. 7: Effect of attack on throughput with varying number of attackers

It can be seen from the Fig. 5 that the proposed technique can easily mitigate the effect of DDoS attack in MANET.

Effect of attack on number of collisions when attack is performed with varied number of attackers: In this section, we will study the effect of DDoS attack on number of collisions. Attack is performed using varied number of attackers. Performance of the system is compared when system is in normal condition i.e., no attack, under flooding DDoS attack with no prevention scheme and when proposed prevention scheme is used. It can be seen from the Fig. 6 that the proposed technique can easily mitigate the effect of DDoS attack in MANET.

Effect of attack on throughput when attack is performed with varied number of attackers: In this section, we will study the effect of DDoS attack on throughput. Attack is performed using varied number of attackers. Performance of the system is compared when system is in normal condition i.e., no attack, under flooding DDoS attack with no prevention scheme and when proposed prevention scheme is used. It can be seen from the Fig. 7 that the proposed technique can easily mitigate the effect of DDoS attack in MANET.

Advantages of the proposed scheme:

- The proposed scheme incurs no extra overhead, as it makes minimal modifications to the existing data structures and functions related to blacklisting a node in the existing version of pure AODV.
- Also, the proposed scheme is more efficient in terms of its resultant routes established, resource reservations and its computational complexity.
- If more than one malicious node collaborates, they too will be restricted and isolated by their neighbors. Thus the scheme successfully prevents DDoS attacks.

CONCLUSION AND RECOMMENDATIONS

Detection and Prevention of DDoS attacks are part of an overall risk management strategy for an organization. Each organization must identify the most important DDoS risks and implement a cost-effective set of defense mechanisms against those attack types causing the highest risk for business continuity. Studies and news about real-life DDoS attacks indicate that these attacks are not only among the most prevalent network security risks, but that these attacks can also block whole organizations out of the Internet for the duration of an attack. The risk from DDoS attacks should not thus be underestimated, but not overestimated, either. In this study, a novel scheme is proposed which deals with suppressing the influence of the attack. The effectiveness of the approach is validated with simulation in GloMoSim, integrated with parsec compiler, on a windows platform.

Scope for future work: In future, the framework can be evaluated for:

- Detection mechanism implemented in the thesis detect only victim node not the attack type. So, we plan to implement a new detection mechanism which not only detect attacking node but also attack type.
- In our study, we have implemented only one attack mechanism for DDoS attack. But there are lots more DDoS attack types which have greater impact on network performance are yet to be implemented and we plan to implement them in future.
- In our study, we have implement prevention technique for flooding attack. Prevention scheme for packet dropping is not implemented and we plan to find and implement prevention scheme for packet dropping based DDoS attack.

REFERENCES

Alomari, E., M. Selvakumar, B.B. Gupta, K. Shankar and A. Rafeef, 2012. Article: Botnet-based Distributed Denial of Service (DDoS) attacks on web servers: Classification and art. Int. J. Comput. Appl., 49(7): 24-32.

CERT, 2007a. Statistics. Retrievedform: http://www. cert. org/stats/cert_stats.html. (Accessed on: May 28, 2007).

CERT, 2007b. Denial of Service Attacks. Retrieved form: http://www.cert.org/tech_tips/denial_of_ service. html, oct. 1997, (Accessed on: May 28, 2007).

Chaba, Y., Y. Singh and P. Aneja, 2009. Performance Analysis of disable IP broadcast technique for prevention of flooding-based DDoS attack in MANET. J. Networks, 4(3): 178-183.

Chhabra, M., B.B. Gupta and A. Almomani, 2013. A novel solution to handle DDoS attack in MANET. Int. J. Inf. Secur., 4(3): 165-179.

Douligeris, C. and A. Mitrokotsa, 2004. DDoS attacks and defense mechanisms: Classification and state-of-the-art. Elsevier Sci. Direct Comput. Networks, 44: 643-666.

Elnoubi, S., W. Abdallah and M.M.M. Omar, 2011. Minimum bit error rate beam forming combined with space-time block coding using double antenna array group. Int. J. Comput. Sci. Inform. Secur., 9(5).

GloMoSim, Year. GloMoSim: Global Mobile Information Systems Simulation Library. Retrieved form: http://pcl.cs. ucla.edu/projects/glomosim.

Gupta, B.B., M. Misra and R.C. Joshi, 2008. An ISP level solution to combat DDoS attacks using combined statistical based approach. J. Inform. Assurance Secur., 2: 102-110.

Gupta, B.B., R.C. Joshi and M. Misra, 2009. Defending against distributed denial of service attacks: Issues and challenges. Inform. Secur. J. Global Perspective, 18(5): 224-247.

Houle, K.J., G.M. Weaver, N. Long and R. Thomas, 2001. Trends in denial of service attack technology. Technical Report Version 1.0, CERT Coordination Center, Carnegie Mellon University 2001. Retrieved form: http://www.cert.org/ archive/ pdf/DoS_trends.pdf. (Accessed on: May 28, 2007).

Ihsan, Z., M. Yazid Idris, K. Hussain, D. Stiawan and K.M. Awan, 2011. Protocol share based traffic rate analysis for UDP bandwidth attack. Comm. Com. Inf. Sc., 251: 275-289.

Kavisankar, L. and C. Chellappan, 2011. CNoA: Challenging number approach for uncovering TCP SYN flooding using SYN spoofing attack. Int. J. Network Secur. Appl., 3(5).

Lau, F., S.H. Rubin, M.H. Smith and L. Trajkovi, 2000. Distributed denial of service Attacks. Proceedings of IEEE International Conference on Systems, Man and Cybernetics. Nashville, TN, USA, pp: 2275-2280.

Leiner, B.M., V.G. Cerf, D.D. Clark, R.E. Kahn, L. Kleinrock, D.C. Lynch, J. Postel, L.G. Roberts and S. Wolff, 2007. Internet Society: Histories of the Internet-a Brief History of the Internet. Version 3.32. Retrieved form: http://www.isoc.org/ internet/ history/brief.shtml. (Accessed on: May 28, 2007).

Mirkovic, J., J. Martin and P. Reiher, 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Comput. Commun. Rev., 34(2): 39-53.

Saraeian, S., A. Fazllolah, G.Z. Mohammad and A.A. Seyed, 2008. Performance Evaluation of AODV Protocol under DDoS Attacks in MANET. Proceeding of World Academy of Science, Engineering and Technology, 45: 501.

Schuba, C.L., I.V. Krsul, M.G. Kuhn, E.H. Spafford, A. Sundaram and D. Zamboni, 1997. Analysis of a denial of service attack on TCP. Proceeding of the IEEE Symposium on Security and Privacy, pp: 208-223.

Wang, H., D. Zhang and K.G. Shin, 2002. Detecting SYN flooding attacks. Proceeding of the 21th Annual Joint Conference of the IEEE Computer and Communications Societies, (INFOCOM), 3: 1530-1539.