Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detection and Prevention of DDOS Flooding Attack in MANET

Vibha Tripathi, Mayuresh Kanher
Department of CSE, GITS GwaliorDepartment of CSE, GITS Gwalior,
Madhya Pradesh, India

Abstract— ThisMobile ad hoc network (MANET) is an example of mobile wireless communication. MANET is infrastructure less network due to dynamic mobile network can be established in any circumstances. Network in MANET is composed of mobile nodes that are self-configured, multi-hop connected through wireless links. Each node is free and changes their position randomly. Denial of service (DoS) attack is one of major security attack in MANET. In this kind of attacks, a group of attacker or single attacker tries to gain access to network in terms of interrupting valid user to serve by an application running on a mobile node. In Denial of service (DoS) flooding attack become a major threat to internet reliability. By DoS Flooding a large volume of attack traffic is generated. The DoS Flooding attack defense is significantly difficult due to the fact that internet lacks accountability at network layer. In this work present the detection and prevention of DoS Flooding attack in MANET. In propose work we calculate the trust of node on the basis of their behavior and on the basis of trust, reputation is calculated. If reputation value is minimum to threshold, then all node blocks this node for particular times and after some time listens this node, if receiving RREQ by this node get RREP so node increase its trust by one. Detection and prevention of Flooding attack can be done by use of proposed algorithm. For implementation we have used network simulator (NS2). We compared result in terms of packet delivery ratio, end to end delay, throughput and routing overhead. text.

Keywords— MANET, DDoS, Floodingattack, Pdr.

I. INTRODUCTION

Ad hoc network refers to a network connection built for a single session and does not require a wireless base station and a router, it is a temporary network association made for some particular reason like for sending date from one device to other. If the network is set up for a long period of time, then it is just a plain old local area network.website.

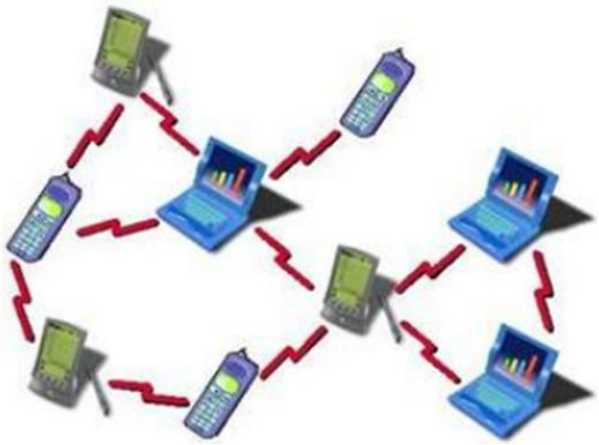

Figure 1.1: Ad hoc Network

The mobile ad-hoc network is an integration of more than one wireless nodes and have the capacity of transferring data to one another without any kind of help due to the integration of the nodes changing with time because of the mobility of nodes, entry of new nodes and flight of nodes. Hence, productive routing protocols are needed for these nodes to communicate. Quick and unusual topological changes, wireless network dynamic nature, mobility of nodes and restricted battery power raise numerous difficulties in making up a routing protocol. Because of huge challenges in planning a routing protocol for MANET, various developments recently focusing on giving ideal solution for routing. Thus, an ideal routing protocol that can cover the greater part of the user requirements or applications and additionally adapt up to the stringent conduct of the wireless medium is constantly alluring. Ad hoc nodes are devices to have the capacity to identify the existence of other such devices in order to permit data sharing and communication. Besides that, it ought to additionally have the capacity to distinguish type of relating attributes and services. Due to the mobility of nodes the amount of wireless nodes will change, routing data additionally changes to follow changes in the connectivity of links. Henceforth, the topology of the network is a great deal is dynamic and the adjustments are frequently unusual as contrasted with the settled type of actual wired networks[1].

II. CHARACTERISITICS OF ADHOC NETWORK

For designing or suggesting solutions for MANETs following features can be considered.

- Distributed operation is one of the features of MANET because in ad hoc network every device works individually and there is no machine or centralized administrator to deal with this network, instead this job is conveyed among all working nodes. Every device works with an alternate device in collaboration to accomplish functions like routing and security[2].
- As compared to wired network MANET has lower bandwidth capacity. MANETs can encounter an issue of lower bandwidth capacity and bit error rate because node to node link path are utilized by many nodes in the network[3].
- An alternate characteristic of MANET that could be utilized is energy as a part of mobile nodes. As all mobile nodes will get their energy from the battery, which is a constrained asset, whatever energy the portable nodes have, it must be utilized proficiently.

III. DDOS ATTACK

Distributed denial of Service attacks usually occurs in MANETS or in wireless networks. It is an attack where multiple systems comprised together and target a single system causing a denial of service (DoS) [4, 5]. The target node is flooded with the data packets that system shutdowns, thereby denying service to legitimate users. A Denial of Service (DoS) attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system. 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. Or in another way we can say that a Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The services under attack are those of the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims." The use of secondary victims in a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack while remaining anonymous since the secondary victims actually perform the attack making it more difficult for network forensics to track down the real attacker[6].

IV. LITERATURE REVIEW

Kreibich et al. [5] propose to use packet symmetry to curtail DoS attack trace. Their observation is that during a DoS attack, an attacker host sends out a large amount of trace while receives little incoming trace. Therefore, if each access router shapes each host's trace to keep a relatively low ratio of outgoing trace over incoming trace, DoS attack trace will be significantly curtailed. However, the threshold ratio is difficult to set, because legitimate applications may also result in a high ratio of outgoing trace over incoming trace. An ideal DoS mitigation scheme should be able to identify and drop attack trace as early as possible, but this goal is often difficult to achieve, especially when attack trace cannot be distinguished from legitimate trace or those who can identify attack trace do not ask to stop the attack trace.

Song et al. [6] propose two packet marking schemes better than those in: one requires fewer attack packets to reconstruct the attack path, and the other allows authenticating router markings such that a compromised router cannot forge the markings of other routers. Yaar et al. [7] propose FIT, a mechanism that is still based on probabilistic packet marking but can reconstruct the attack path with even fewer attack packets. Khan et al. [8] and Zhou et al. [11] give overview of challenges of DoS attack on MANET. Bin et al.[9]demonstrated how Distributed DoS (DDoS) attacks can be detected at an early stage. Chen et al. [10] explainedStatefull DDoS attacks and targeted filtering. Siris et al. [11] and Abraham et al. [12] have proposed a method ofdefence against DDoS attack by using provider based deterministic packet marking and IP spoofing defence.Here, we are discussing two types of DDoS attacks i.e. Malicious Packet Dropping based DDoS attack and FloodingBased DDoS attack [11]. The Malicious Packet Dropping based DDoS attack has the aim of attacking the victim nodein order to drop some or all of the data packets sent to it for further forwarding even when no congestion occurs. Thesecond type of DDoS attack is based on a huge volume of attack traffic, which is known as a Flooding-based DDoS.

V. PROPOSED WORK

Mobile ad-hoc network gain popularity now days. MANET is easily cope up with attack due its infrastructure and flexibility to accommodate with others nodes, security is main concern for MANET there are several attack by which network is effected and performance of network is degrade. Flooding attack is one of the most security threats for MANET because intruder node generate worthless packet to misuse the bandwidth or resources of network. Existing work have problem that it calculate the reputation value on the basis of RREP packet if any node in deafness and other node wants to communicate with this node and it generate RREQ again and again so reputation value goes to zero or this node blacklisted forever, existing work defending this attack, to overcome this problem we propose a Reputation based flooding detection and prevention technique. In our proposed work, we are searching a cluster head in the cluster network. A node become cluster head if it have RREP for RREQ of source and also this node announce its one hop neighbor. Initially all nodes in the network have trust value which is 1 and after seeing their behavior of trust will be decrease or increase. After this we calculate their reputation on the basis of trust value, if reputation of nodes less than threshold value so black list this node for some time interval. After a time interval, we are approaching again to this node which is

in the black list queue and seeing again is there any RREQ messages generate, if again RREQ generate then we check we get RREP for this RREQ or not if we receive RREP then unblock this node or increase trust by one otherwise black list this node for a random time.

Proposed Algorithm
Step1: initialize network
Step2: select cluster head
If ((energy of node > all) &&(speed is low))
{
Node become cluster head
}
Else
{ journal node }
Step3: calculate trust
If (receive RREP){ trust+2}
Else {decrease trust}
Step4: calculate reputation
If (trust=>threshold){ reputation+2}
Else
{ reputation -1}
Step5: if(reputation<0.5) {
Block the node for some time and listen this node after some interval
Else {
Node in network}
Step6: end

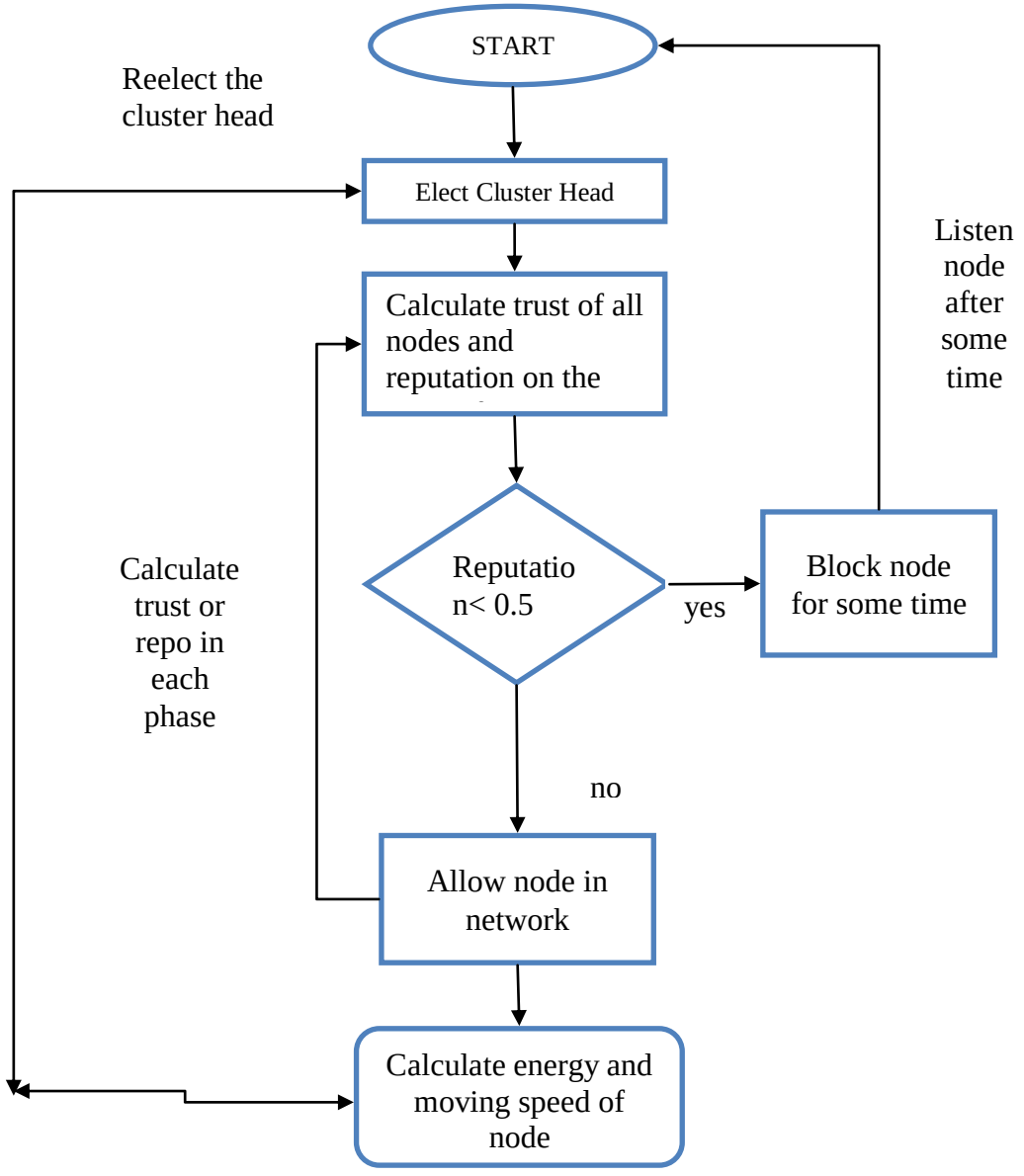

Fig 1: Block diagram of proposed work

VI. RESULT ANALYSIS

A. S Packet delivery ratio:

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as:

PDR= S1÷ S2

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source.

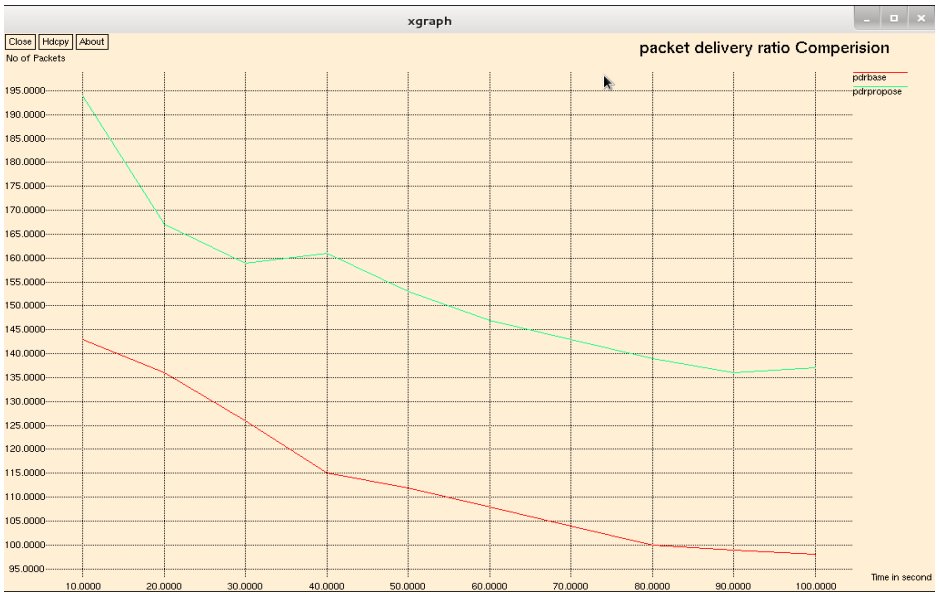

Fig 2: Comparison between base (red) and Proposed (green) values in PDR.

As shown in fig.2 when the simulation start minimum packet delivery ratio is 136 and highest is 195 of proposed algo. And other end previous work minimum packet delivery ratio is 98 and highest is 143 with increase in time . On the basis of comparative results we easily say that our propose work is a novel approach.

B. End to End Delay:

It is defined as delay of time taken for a packet transmits over network from particular source to destination.

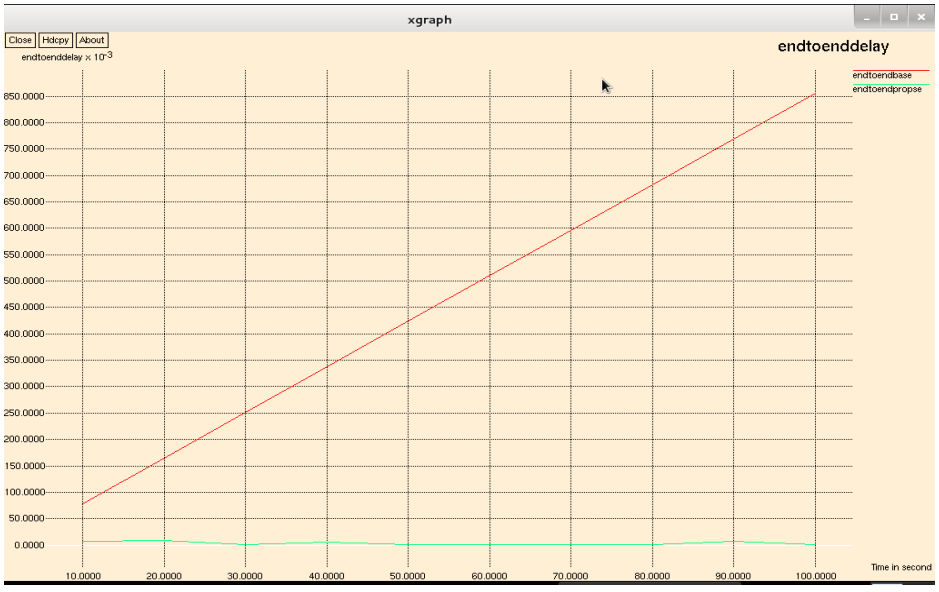

Fig 3 shows the comparison between base and proposed values in end to end delay.

When simulation starts the delay of proposed work is 60 and goes to maximum value 850, and the value of base work start with 0and maximum value up to 0 with increased time.

C. Throughput:

It is defined as the total number of packets delivered over the total simulation time. The throughput comparison shows that the three algorithms performance margins are very close under traffic load of 50 and 100 nodes in MANET scenario and have large margins when number of nodes increases to 200. Mathematically, it can be defined as:

Throughput= N/1000

Where N is the number of bits received successfully by all destinations.

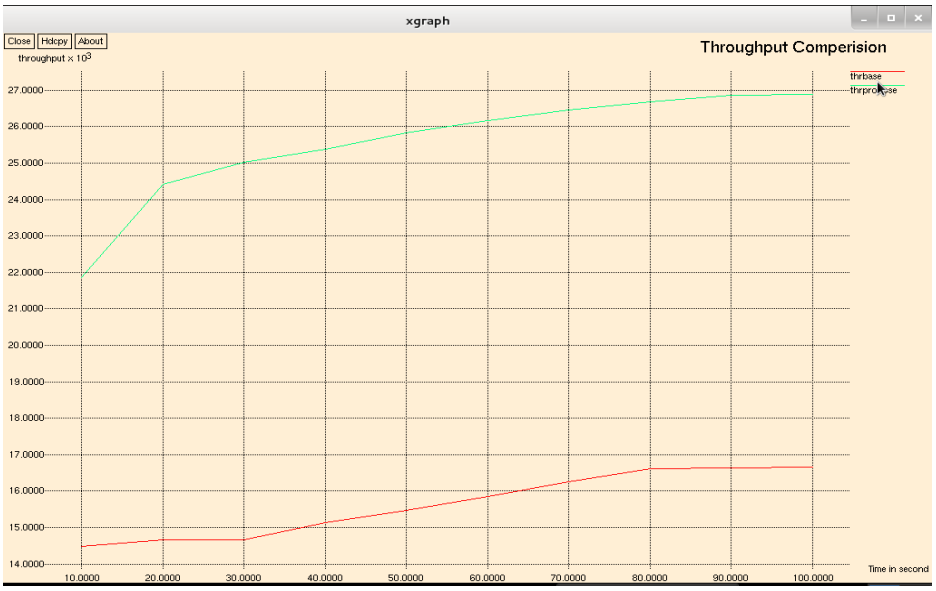

Fig 4: Comparison between base (red) and Proposed (green) values in Throughput.

Fig 4 shows the comparison between base and proposed values in throughput. When simulation starts the throughput of proposed work is 22 and goes to maximum value 27, and the value of base work start with 14 and maximum value up to 15 with increased time. In this way previous work is not good in real time scenario.

D. Routing overhead:

Routing overhead refers to the metadata and network routing knowledge sent through an application, which uses a portion of the available bandwidth of communications protocols. This additional information, making up the convention headers and application-particular data is alluded to as overhead, since it doesn't add to the substance of the introduction. Protocol overhead can be expressed as a percentage of non-application bytes (protocol and frame synchronization) divided by the total amount of bytes in the data.

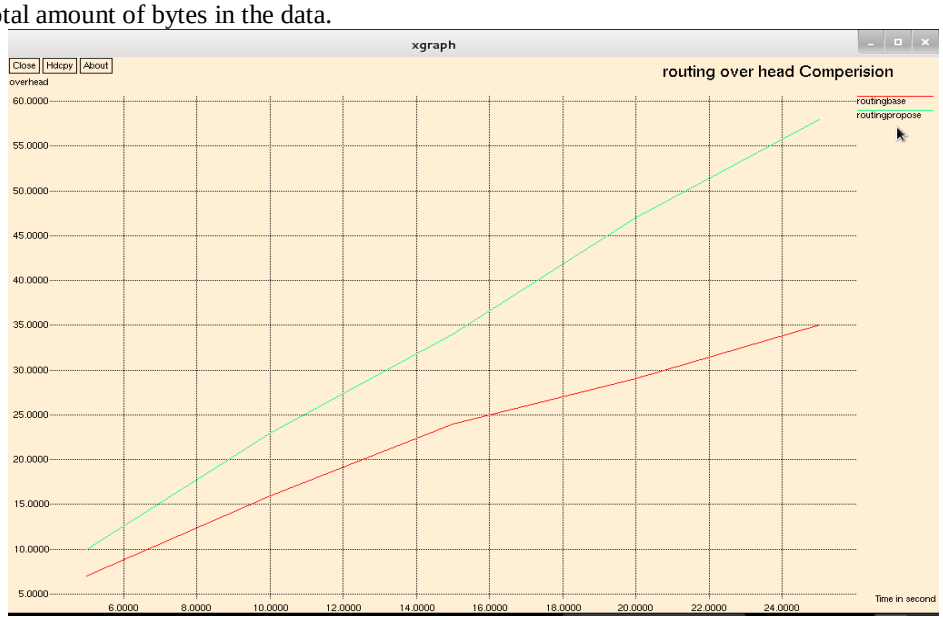

Fig 5: Comparison between base and proposed values in routing overhead.

Fig.5 shows the comparison of routing overhead. When simulation start the proposed value is 10 and increased up to 57, where as the values of base work is 7 and reached up to 30 with increased time.

VII. CONCLUSIONS

DoS flooding attacks are difficult to mitigate partly because of the lack of account ability in the network layer of the current Internet. In this paper, we proposed a reputation & trust-based incentive mechanism for detecting and preventing DoS attacks in MANETs. The DoS Flooding attack defense is significantly difficult due to the fact that internet lacks accountability at network layer. In this thesis we present the detection and prevention of DoS Flooding attack in MANET. In propose work we calculate the trust of node on the basis of their behavior and on the basis of trust, reputation is

calculated. If reputation value is minimum to threshold, then all node blocks this node for particular times and after some time listens this node, if receiving RREQ by this node get RREP so node increase its trust by one. Detection and prevention of Flooding attack can be done by use of proposed algorithm. For implementation we have used network simulator (NS2). We compared result in terms of packet delivery ratio, end to end delay, throughput and routing overhead.In future work implement the detection and prevention technique of flooding attack with different routing protocols to check the performance of routing protocols with other.

REFERENCES

[1] Bathi Srikanth "Detecting Selfish Nodes in MANETs" National Institute of Technology Rourkela, Odisha, 769 008, India June 2014.

[2] Arvind Sharma "Comparative Analysis Of Low Rate Denial Of Service Attack In Manets" Computer Science And Engineering Department Thapar University Patiala – 147004 July 2013.

[3] Yau, P-W & Mitchell, CJ, "Security vulnerabilities in ad hoc networks," Proceedings of ISCTA 2003, 7th International Symposium on Communications Theory and Applications, July 2003.

[4] Liu, S, "Surviving Distributed Denial-of-Service Attacks," IEEE Computer, vol.11,no.5, pp.51-53,Sep.2009.

[5] Z. Duan, X. Yuan, and J. Chandrashekar. Constructing Inter-Domain Packet Filters to Control IP Spoo_ng Based on BGP Updates. In IEEE INFOCOM, 2006.

[6] A. Yaar, A. Perrig, and D. Song. FIT: Fast Internet Traceback. In Proc. of IEEE Infocom, 2005.

[7] Shafiullah Khan et al, "Denial of Service Attacks and Challenges in Broadband Wireless Networks," InternationalJournal of Computer Science and Network Security, Vol. 8, No. 7, pp. 1-6, July 2008.

[8] Xiao Bin et al, "A novel approach to detecting DDoS Attacks at an Early Stage," The Journal of Supercomputing,Springer, Volume 36, Number 3, June 2006 , pp. 235-248(14).

[9] Shigang Chen et al, "Stateful DDoS attacks and targeted filtering," Journal of Network and ComputerApplications, Volume 30, Issue 3, August 2007, pp. 823-840.

[10] Xiaobo Zhou et al, "Distributed denial-of-service and intrusion detection," Journal of Network and ComputerApplications, Volume 30, Issue 3, August 2007, pp. 819- 822.

[11] Vasilios A. Siris et al, "Provider-based deterministic packet marking against distributed DoS attacks," Journal ofNetwork and Computer Applications, Volume 30, Issue 3, August 2007, pp. 858-876.

[12] Yaar Abraham et al "StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP SpoofingDefense," IEEE Journal on Selected Areas in Comunications 24, no. 10 (October 2006): 1853-1863.

