Towards DoS Attack Prevention based on Clustering Architecture in Mobile IP Communication

Sazia Parvin[1], Sohrab Ali[2], Jaipal Singh[1],
Farookh Hussain[1], Song Han[1]

[1]Digital Ecosystems & Business Intelligence Institute
Curtin University of Technology, Australia
sazia.parvin@postgrad.curtin.edu.au,
{J.Singh, Farookh.Hussain, Song.Han}@cbs.curtin.edu.au

[2]CSE Department
Dhaka University, Bangladesh
milon_csdu707@yahoo.com

***Abstract*-Mobile IP communication, like wired communication and mobile ad hoc networking, is vulnerable to Denial-of-Service (DoS) attacks. In this paper, we propose using a lightweight packet filtering technique in different domains and base stations to reduce/eliminate the threat of DoS attacks on mobile IP networks. The proposed technique will be able to detect and filter out any suspected packets containing spoofed IP address created by DoS attackers. The results of our experiments indicate that our proposed technique can significantly reduce the effect of DoS attacks and improves performance of mobile IP communication.**

I. INTRODUCTION

The ubiquitous nature of mobile computing, brought by the proliferation of mobile phones and wireless networks, is being felt in all spheres of our lives. Users nowadays want to be always connected and they require computing devices such as laptops, PDAs and smart phones to be connected to the Internet. Business users are relying more on wireless networks due to the lower infrastructure costs and the flexibility it brings to employees. While mobile users can easily stay connected through the Internet, the mobile workforce requires more reliable and secure connectivity to the office network.

Mobile IP [1] was introduced to provide seamless and transparent network connectivity while the user is physically moving between network access points or base stations. Since mobile IP is an extension of the IP protocol, it has the same robustness and scalability of the protocol. However, mobile IP is also vulnerable to security exploits affecting the wired Internet as well as some new exploits in a mobile environment.

This paper aims to solve one of the main problems currently faced by businesses, namely denial of service (DoS) attacks on their organizational resources. DoS attacks are an ongoing issue in fixed networks and a lot of work has been done for preventing or mitigating this attack in wired communication. A fuzzy-based inference mechanism is used to infer a soft boundary between anomalous and normal behaviors using multiple detection engines [17].

DoS prevention and mitigation is now a very important issue in mobile communication as mobile devices have much lower resources, both in terms of bandwidth and processing power, compared to fixed network devices. A DoS attack will temporarily cause the mobile user to lose connectivity to the network, thus reducing productivity and possible loss of revenue. For example, a mobile sales force that is unable to access the organization sales server will not be able to complete a sale. This problem is further exacerbated in small and medium enterprises (SME) since they lack the resources to quickly recover from a DoS attack. As this is such an important problem, we have designed a better solution for detecting and preventing DoS attack in Mobile IP communication.

The rest of the paper is organized as follows. Section II presents a brief overview of mobile IP, DoS attack scenarios and existing research on mitigating these DoS attacks in mobile communications. Section III provides a detail design of our proposed solution. Section IV presents simulation analysis of the proposed solution. Section V concludes this paper.

II. RELATED WORK

A. Mobile IP Architecture

Mobile IP is an open standard supporting data transmission in a mobile network using the IP protocol. It allows a mobile node to seamlessly continue receiving data when the node changes its point of attachment to the Internet. For this purpose, some additional components and control messages are required as explained below.

978-1-4244-4649-0/09/$25.00 ©2009 IEEE

Mobile Node (MN): A network host that can change its point of attachment from one network to another without changing its home IP address.

Corresponding Node (CN): A network host that communicates with a mobile node over the Internet. This node can be either fixed or mobile.

Home IP Address: A globally unique IP address that is used to identify a mobile node over the Internet. This address does not change during the communication session with a CN.

Care-of-Address (CoA): A temporary IP address given to a mobile node while it is connected to a foreign network.

Home Agent (HA): An agent located in the mobile node's home network that maintains the mobile node's current location information and tunnels any packets that are addressed to the mobile node (Home IP address) to its current location on the network (CoA).

Foreign Agent (FA): An agent that provides a care-of-address to the mobile node in a foreign network. The FA is the end point of the tunnel between the home agent and the mobile node and will deliver the tunneled packets from the corresponding node to the mobile node in a foreign network.

Mobile IP not only maintains session continuity for network applications by retaining its home IP address, but also presents a consistent IP address to others so that users are constantly reachable by applications. The operations of Mobile IP are provided in [1].

B. DoS Attack Scenarios in Mobile IP Networks

Mobile IP raises some new security issues and vulnerabilities, particularly from attacks that deny the user from accessing network resources (denial of service). This is due to the fact that the communicating device is mobile and must transmit/receive data from one network point to another.

A DoS attack [2, 3] is any event that diminishes a network's capacity to perform its expected function. These attacks are launched against server resources or network bandwidth by preventing authorized users from accessing resources. They pose threats to larger websites such as Amazon and eBay. The effect of these attacks varies from temporarily blocking service availability to permanently distorting information in the network. DoS attacks can target a client computer or a server computer. For example, an attack may target a system by exhausting limited mobile node resources such as wireless bandwidth, storage space, battery power, CPU, or system memory. Networks and applications can be attacked by modifying routing information or changing system configuration, thereby directly attacking data integrity.

The most common type of DoS attack occurs when adversaries flood a large amount of bogus data to interfere or disrupt the service on the server [4]. A DoS attack takes one of the two forms: (a) An attacker floods nuisance packets (e.g. TCP SYN flooding) or (b) an attacker somehow precludes packets from flowing between two nodes.

This attack prevents or inhibits the normal use or management of communication facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g. the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

In the case of Mobile IP, when an attacker manages a bogus registration of a new CoA for a legitimate mobile node or generates a bogus registration request specifying its own IP address as the CoA for a mobile node, a DoS attack can occur. This can lead to disconnection of the legitimate mobile node from the network and unauthorized snooping of all traffic to the mobile node by the attacker.

An attacker can overflow the access server by launching a flooding attack. It is possible because the IP addresses of the HA and the MN are not hidden in the registration message. An example of such an attack is TCP/IP SYN attack [5]. This attack typically attempts to flood a target with traffic to waste network bandwidth or server resources. The DoS attacks that target resources can be grouped into three broad scenarios.

The first attack scenario targets storage and processing resources. This is an attack that mainly targets the memory, storage space, or CPU of the service provider. Consider the case where an attacker continuously sends an executable flooding packet to its neighborhoods to overload the storage space and exhaust the memory of those nodes. This prevents the nodes from sending or receiving packets from other legitimate nodes.

The second attack scenario targets energy resources, specifically the battery power of the service provider. Since mobile devices operate by battery power, energy is an important resource in mobile IP communication. An attacker may continuously send a bogus packet to a node with the intention of consuming the victim's battery energy and preventing other nodes from communicating with the node.

The third attack scenario targets bandwidth. Consider the case where an attacker located between multiple communicating nodes wants to waste the network bandwidth and disrupt connectivity. The malicious node can continuously send packets with spoofed IP addresses, thereby overloading the network. This consumes the resources of all neighbors that receive the packets, thus overloading the network, which results in performance degradations.

Firewall offers some level of protection, in that they can be programmed to drop all packets from a known attacking host, but it's easy for the attacker to simply put a different source IP address in each packet by using IP spoofing technique. We need to apply some filtering technique to

identify and filter the suspected or unwanted packets which contains spoofed IP addresses.

An attacker can also make use of other network devices (zombies) to launch an attack. This version of DoS attack is called Distributed Denial of Service (DDoS) attack and is more severe than a DoS attack. In a DDoS attack, an attacker launches an attack upon the target victim in a coordinated fashion.

A combination of different DoS and DDoS attack scenarios is shown in figure 1, reproduced from [2]. Here routers, attackers, victims, domains and hosts are denoted by R, A, V, D and H respectively. The attacker A1 launches an attack on the victim V. A1 spoofs IP address of host H5 from domain D5. Another attacker A3 uses hosts H3 as a reflector to attack V.

C. *Methods to Prevent DoS Attacks in Mobile IP Networks*

Mobile IP raises new security issues for wireless network and there is comparatively higher probability (compared with wired network) of being attacked by hostile opponents. T. Braun and M. Danzeisen [6] proposed a solution to provide security to Mobile IP using IP Sec and called it Secure Mobile IP (SecMIP). J. Zao and M. Condel [16] used IP Sec ESP protocol in Mobile IP to protect against both passive and active attacks. MIP-IPSec tunnel is established between MN-HA, HA-FA and FA-MN to fulfill the security requirements. V. Gupta and G. Montenegro [8] proposed some enhancements to basic Mobile IP protocol so that authorized users can access network that is protected by firewalls or some combinations of source filtering routers or the network, which are using private address space for security reasons. A. Inoue, M. Ishiyama, A. Fukumoto and T. Okamoto [9] proposed to modify Mobile IP protocol with IP Sec and called it Secure Mobile IP protocol. Here secure Mobile IP is implemented on gateway servers and mobile hosts. A new protocol for securing binding update messages

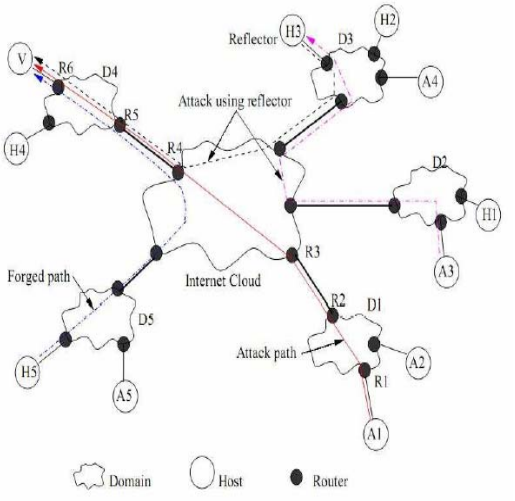

Fig. 1. Different scenarios for DoS attacks

of mobile IP communication has been proposed by employing key cryptosystems that is digital signature and Diffie-Hellman key exchange algorithm [10].

DoS and DDoS attacks were classified in [7]. These attacks pose unpredictable threats to the Internet infrastructure and Internet-based business [11]. Some methods to prevent DoS attacks in Mobile IP communication have been proposed but they did not show any performance evaluation as well as consider any DDoS attacks [12]. Denko *et al.* [5] proposed a DoS attack prevention scheme in mobile ad hoc network's using reputation based incentive scheme. Anderson *et al.* [13] proposed TVA system, Packet Passport system and StopIt system for limiting DoS attack in wired communication. DDoS Attack Traceback and Mitigation System (DATMS) are proposed to trace the DDoS attack sources based on network performance monitoring [14]. A packet filter controller which adapts to queue length is proposed to mitigate the DDoS attack in this paper. The work on preventing DoS attacks in mobile devices using Mobile IP is very limited and a new approach is proposed in this paper for use in mobile networks.

III. DESIGN OF PROPOSED SOLUTION

When a network becomes highly dynamic, it becomes too complex to detect and prevent DoS attack. So, an acceptable approach is to divide a large network into small and manageable groups and implement security mechanisms in each group in a distributed manner. We propose to divide a large network into some hierarchical structures. Firstly, we will divide the network into domains. Then, each domain can be divided into clusters which consist of one or more wired or mobile node or base station. We argue that, if we can manage and secure each cluster efficiently, we can secure each domain and thus the whole network becomes secured and manageable. This is basically a distributed approach where each domain or cluster is independent. Figure 2 in [12] shows our proposed domain-based clustering architecture.

We present the following advantages for hierarchical structures. First, this approach is scalable. The performance of the security mechanisms would not degrade when the network scales. Second, each cluster can be controlled

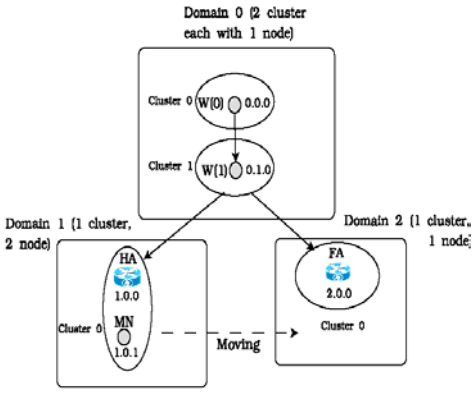

Fig. 2. Clustering Architecture of mobile IP communication.

independently. That means, the security mechanisms in a cluster lying in the more dynamic portion of a large network may not match with that of a cluster lying in a comparative static portion. Third, detecting an attacker becomes easier in a clustered architecture as it provides localized information. Fourth, this localized and distributed feature reduces storage, processing and communication overhead, thereby optimizing network bandwidth utilization.

After dividing a large network into hierarchical structure we propose two techniques, (i) Filtering in Domain Base Station Router, and (ii) Queue Monitoring in Base Station Node. Each of these techniques is described in details below.

A. *Filtering in Domain Base Station Router*

In each domain there is an edge or periphery router through which each packet within the domain has to pass through to get to another domain. We propose to filter the malicious packets in each domain's periphery router before the packets are sent to the mobile node. This approach uses ingress/egress filtering to stop DoS attacks from entering or leaving a domain.

Basically foreign agents act as the periphery router in a domain. When a mobile node is visiting a foreign network and registers with the FA, the FA will keep track of the addresses associated with that mobile node using a caching mechanism. After registration, if the mobile node wants to attack any node outside its current domain by spoofing the source address, the domain periphery router will detect and filter that packet as the spoofed address is unknown to itself. If the FA receives a packet for the MN with a source address different than the tunneled HA address, it will filter that packet as it assumes it is a DoS attack.

Although caching requires some memory in the domain periphery router, we argue that, it would not be a performance issues because for each node very small memory would be needed.

B. *Queue Monitoring in Base Station Node*

Our second proposition is to protect the HA from forwarding DoS attacks to the MN. If the HA is under DoS attack, it will be overloaded by attacking packets. Most of the HA resources will be consumed by the fake packets. As a result, legitimate nodes will be barred from communicating with the MN. In this situation, we propose to monitor the queue and set its size in an adaptive manner. We propose to limit the queue size in case of sudden increase of tiny packets (like TCP SYN packets) in the queue. This is because sudden increase of such packets raises the probability of a DoS attack. So, dropping packets in this case would reduce the effect of the attack.

We propose to measure the queue in the basis of small (near to size of TCP SYN packets) packets at the HA regularly. Once this value goes over a predefined level, the queue size would be limited by an adaptive value considering other bigger size packets in the queue. This indicates that we only want to filter the suspicious packets, not any one of the data packets. This is important as the FA will not filter out packets from HA. Thus eliminating suspicious packets at the HA will prevent DoS attacks at the foreign network.

The problem with this approach is, some applications use small packets, which may also be dropped in this filtering. To save these packets we propose to drop packets in the event of sudden and large increases of small packets in the queue. We argue that, the applications that use small packets do not send packets at a very high rate.

IV. IMPLEMENTATION AND ANALYSIS

A. *Simulation Environment*

We created Mobile IP simulation environments in ns-2 [15]. We created a wired-cum-wireless topology through which we can exchange packets between a wired and wireless domain via a base-station. We make the following assumptions for the simplicity of simulation:

(a) Each mobile node in the network has a unique ID and can join or leave the network freely.

(b) Each packet is of equal size, although packet may vary in size according to their contained data. Packet sending rates are also constant.

(c) Initially, all nodes have equal computational and storage capability.

B. *Scenario 1: Filtering in the queue of Home Agent*

As said earlier, filtering in the queue of the HA can significantly reduce the effect of DoS attack. For example, in case of TCP SYN flooding attack, an attacking node starts the three way handshaking phase, but does not complete the phase. The size of the packets in handshaking phase is very small. However, the HA will observe a sudden

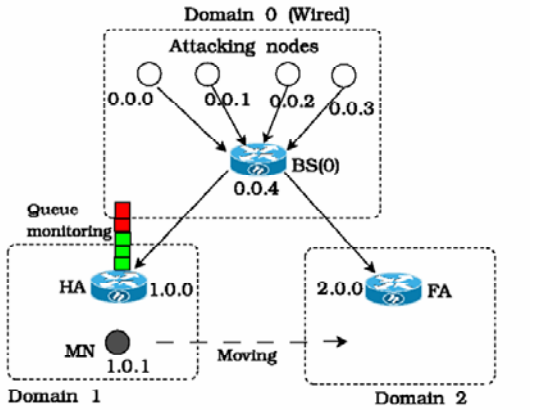

Fig. 3. Monitoring queue in the HA

increase of TCP SYN packets in its queue.

In figure 3, we simulate four malicious nodes simultaneously attacking a mobile node under the base station which is its home agent. We used constant bit rate (CBR) applications to simulate TCP SYN flooding attack

TABLE I
SIMULATION PARAMETERS FOR SCENARIO 1

Parameters	Values/Ranges
Packet Size	40 Bytes
Transport agent	TCP
Application	CBR
Number of Domains	3
Number of Clusters	4
Simulation Time	60 s

where packet size is 40 bytes. The parameters used in this simulation is shown in table 1. In ns-2 there are many parameters to express the status of a queue such as queue size in bytes, queue size in no. of packets, the entrance and departure of packets etc.

In our approach, we filter the queue in the HA by limiting the queue size to four and observe the effects of queue size on DoS attacks. In this simulation, we dropped 63 TCP SYN packets and thus the effect of the attack is reduced at the HA node.

In figure 4, we observed some high fluctuations in queue size (measured in no. of packets). The peak values indicate the sudden presence of huge no. of small packets which is a sign of DDoS attack. The peak values rose close to 15 in this figure.

In figure 5, we observed the queue status while it is being filtered by limiting the queue size to an adaptive value, in our case it was set to 4. Limiting the queue size results in some packets drops which were certainly used for DDoS attack here. In this simulation we found by analyzing the trace file of the simulation that 63 malicious packets were dropped using this filtering technique

C. *Scenario-2: Filtering in Domain Base Station Router*

In figure 6, there is a wired domain consisting of two wired nodes in two clusters with hierarchical addresses 0.0.0 and 0.1.0 respectively. Home Agent (HA) and Foreign Agent (FA) are two base station nodes in two other different domains. There are five roaming mobile nodes (MN)

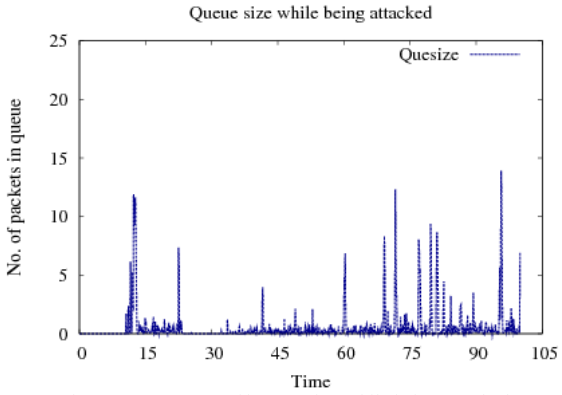

Fig. 4. Queue status of base station while being attacked

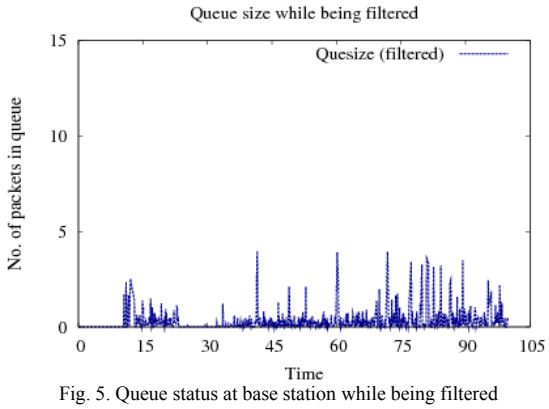

Fig. 5. Queue status at base station while being filtered

marked as green, which move between their home agent and foreign agent. There are five TCP flows from each of these five nodes where a node in the wired domain of address 0.0.0 is the destination for all. As the five sources move out from the domain the HA to the domain of FA, the packets destined for the wired node is redirected by its HA to the FA as per Mobile IP protocol definitions.

When the five MN reach the FA, they first get registered. In our simulation scenario some of the sources become malicious (marked as red) and use spoofed addresses to attack the wired node.

In our proposed solution, we cache the addresses of each node at the FA and when the MNs start using spoofed IP addresses, those packets from unknown sources are dropped at the FA. Although this mechanism consumes some memory of the FA, it can significantly reduce the DoS attack in the very early stage.

We use the simulation parameter described in table 2 for scenario 2 and compare result between filtering and without filtering techniques. In figure 7, a comparison is shown with and without this filtering technique applied. We observe that, after the filtering technique is applied, the number of packets forwarded by the FA is reduced significantly. This is because the packets sent by the MNs with spoofed addresses are identified and dropped. Here it is noticeable that, using this filtering technique, packets will be dropped proportionally with the increase or decrease with the number of attacking nodes.

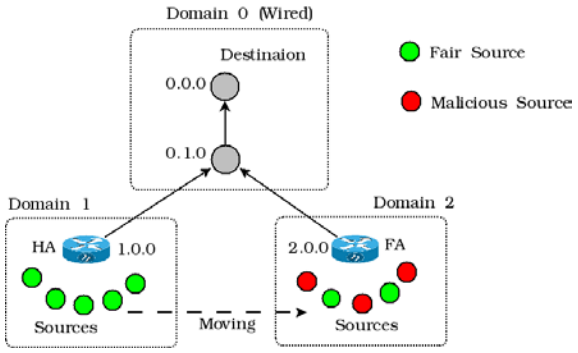

Fig. 6. Simulation with filtering in the domain periphery router

TABLE II
SIMULATION PARAMETERS FOR SCENARIO 2

Parameters	Values/Ranges
Speed of mobile nodes	20 m/s
Packet Size	1000 Bytes
Transport agent	TCP
Application	FTP
Node Numbers	100
Domain Numbers	4 - 5
Number of Clusters	5 - 10
Simulation Time	60 s

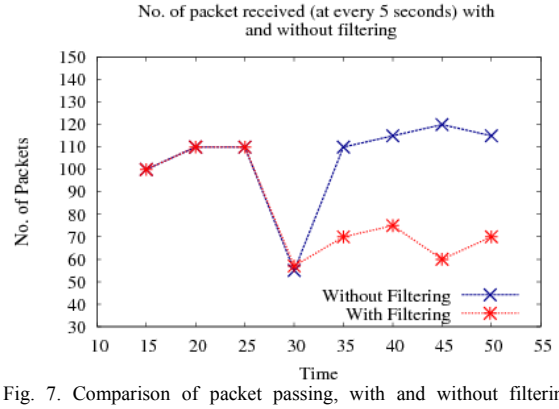

Fig. 7. Comparison of packet passing, with and without filtering technique applied

V. CONCLUSION AND FUTURE WORKS

Denial of service attacks in mobile IP communication is now considered as one of the most severe attacks. The detection and prevention of these attacks is more difficult in case of mobile IP communication than in their wired counterparts as the node is not fixed to a particular network. In this paper, we proposed a technique for detecting and preventing DoS attacks in mobile IP communication. We proposed to apply a filtering and queue monitoring technique at the vulnerable points of the mobile IP communication, namely the foreign agent (FA) and home agent (HA). We observed that our proposed architecture can reduce the effect of DoS and DDoS significantly. We intend to test the use of our techniques against other types of DDoS attacks in future work.

REFERENCES

[1] C. Perkins (eds.), "IP mobility support for IPv4 " in *RFC 3344*: IETF, August 2002.

[2] A. Habib, M. H. Hafeeda, and B. Bhargava, "Detecting service violation and dos attacks," in *Proc. of the 10th Annual Network and Distributed System Security Symposium (NDSS)*, California, USA, 2003.

[3] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of service attacks at the MAC layer in wireless ad hoc networks," in *Proc. of the Military Communications Conference (MILCOM)*, California, USA, 2002, pp. 1118-1123.

[4] S.Tritilanunt, "Protocol engineering for protecting against denial-of-service attacks," PhD Thesis: Faculty of Information Technology, Queensland University of Technology, 2009.

[5] M. K. Denko, "Detection and prevention of denial of service (DoS) attacks in mobile ad hoc networks using reputation-based incentive scheme," *Journal of Systemics, Cybernetics and Informatics,* Vol. 3, No. 6, 2006.

[6] M. Danzeisen and T. Braun, "Access of mobile IP users to firewall protected vpns," in *Workshop Mobile Communication over Wireless LAN at Informatik* Vienna, Austria, 2001, pp. 562-567.

[7] S. Han, E. Chang, L. Gao,T. Dillon, "Taxonomy of Attacks on Wireless Sensor Networks", in *the Proceedings of the 1st European Conference on Computer Network Defence (EC2ND), Springer Press.*

[8] V. Gupta and G. Montenegro, "Secure and mobile networking," *Mobile Networks and Applications,* Vol. 3, No. 4, 1998, pp. 381-390.

[9] A. Inoue, M. Ishiyama, A. Fukumoto, and T. Okamoto, "Secure mobile IP using IP security primitives," in *Proc. of the 6th IEEE workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, USA, 1997, pp. 235-241.

[10] R. H. Deng, J. Zhou, and F. Bao, "Defending against redirect attacks in mobile IP," in *Proc. of the 9th ACM conference on Computer and Communications Security*, USA, 2002, pp. 59-67.

[11] T.Gamer, "Distributed detection of large-scale attacks in the internet," in *Proc. of the ACM Conference on Emerging Networking Experiments and Technologies*, Madrid, Spain, 2008.

[12] S. Parin, S. Ali, S. Han and T. Dillon , "Security against DoS Attack in Mobile IP Communication", *in the proceedings of 2nd ACM International Conference on Security of Information and Networks, by ACM, 2009.*

[13] X. Yang, D. Wetherall, and T. Anderson, "A DoS-limiting network architecture," *ACM SIGCOMM Computer Communication Review,* Vol. 35, No. 4, 2005, pp. 241-252.

[14] W.Su, T.Lin, C.Wu, J.Hsu, and Y.Kuo, "An on-line DDoS attack traceback and mitigation system based on network performance monitoring," in *Proc. of IEEE conference on Advanced Communication Technology*, Korea, 2008, pp. 1467-1472.

[15] The VINT Project, "The network simulator ns-2," Available from: http://www.isi.edu/nsnam/ns/.

[16] J. K. Zao and M. Condell, "Use of IP sec in mobile IP," in *Internet Draft draft-ietf-mobileip-ipsec-use-00*: IETF, November 1997.

[17] X.D. Hoang, J. Hu, and P. Bertok, "A Program based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference," *Journal of Network and Computer Applications, Elsevier, 2009.*