Security against DoS Attack in Mobile IP Communication

Sazia Parvin
University of Dhaka
Computer Science and Engineering Department
saziap@yahoo.com

Shohrab Ali
University of Dhaka
Computer Science and Engineering Department
milon_csdu707@yahoo.com

Song Han
DEBII Institute
Curtin University of Technology
song.han@cbs.curtin.edu.au

Tharam.S.Dillon
DEBII Institute
Curtin University of Technology
Tharam.Dillon@cbs.curtin.edu.au

ABSTRACT
As like as wired communication and mobile ad hoc networking, mobile IP communication is also vulnerable to different kinds of attack. Among different kinds of attack Denial-of-Service (DoS) is a great threat for mobile IP communication. In this paper we proposed to imply a lightweight packet filtering technique in different domains and base stations of mobile IP communication. If there is any packet containing spoofed IP address created by DoS attackers, our scheme can detect and then filters the suspected packets. We evaluated the performance of our proposed scheme using ns-2. The results indicate that our proposed scheme can significantly reduce the effect of DoS attacks and improves performance of mobile IP communication.

Categories and Subject Descriptors
C.2. [COMPUTER-COMMUNICATION NETWORKS]: Security and Protection- General.

General Terms
Security

Keywords
Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Mobile Node (MN), Mobile Host (MH), Home Agent (HA), Foreign Agent (FA), Correspondent Node (CN), Care-of-Address (COA).

1. INTRODUCTION
Today' world is enjoying the tremendous advancement in the area of mobile computing. It ensures much speed and ease in every sphere of our life. Demands for mobile computing are also emerging as smaller PCs, PDAs and Mobile phones become more commonly used. Although we have worldwide Internet access, we cannot expect to take all benefit from Internet until we can ensure confidential access to Internet in anytime and from anywhere in the world. It is the promise of the Mobile IP that the user can enjoy seamless roaming and transparent application while away from their home. Mobile IP is a protocol to support continuous access to Internet. Providing secure communication service has now become a major concern of the related researchers. Security mechanisms for attacks on mobile or wireless networks include packet filtering techniques, encryption, key management, authentication, and routing [1-5, 8, 10, 16-18]. Securing Mobile IP is a difficult task, made of by its inherent characteristics such as frequently changing its point of attachment, no central administration and its dynamic nature. But security support is the most necessary thing for mobile computing environments. There are different kinds of attacks in Mobile IP Communication which can disrupt the normal communication of Mobile IP. Among all the attacks, Denial-of-Service (DoS) attack has become an increasing threat to the reliability of the internet. A huge amount of work has been done for preventing or mitigating this attack. But most of these works have been done for wired communication. DoS attack is also a great threat for Mobile IP Communication. Although some works have been done for enhancing the security for Mobile IP communication, most of the works provide a general solution. They do not provide the security requirements of the applications and don't cope with specific attack. So we proposed a general solution for detecting and preventing DoS attack in Mobile IP communication in this paper.

The reminder of this paper is as follows: we present the brief overview of mobile IP communication in section 2. Section 3 represents different kinds of attacks including DoS attack. We introduce several related works in section 4. We proposed our desired solution to imply a lightweight packet filtering technique of mobile IP communication in section 5. The performance analysis and discussion are presented in section 6. In section 7, we conclude this paper with future works.

2. MOBILE IP
2.1 Overview
Mobile IP is an open standard approved by the Internet Engineering Steering Group (IESG) in June 1996 and published as a proposed standard by the Internet Engineering Task Force (IETF) in November 1996 in order to support mobility. Mobile IP allows users to keep the same IP address, enjoy similar Internet

connectivity and safety while roaming between IP networks. A seamless delivery of information to its destination can be provided by Mobile IP. Basically Mobile IP is a modification to IP that allows the nodes to continue to receive datagram when the user changes the computer's point of attachment to the Internet. For this purpose some additional control messages are involved that allow the IP nodes to manage their IP routing table reliably. During the development of Mobile IP, scalability was considered, as a dominant factor so that in future a high percentage of the nodes attached to the Internet will have the capability of mobility.

2.2 Architecture of Mobile IP

Mobile IP introduces the following new functional entities that are given below:

Mobile Node: A host or router that may change its point of attachment from one network to another without changing its IP address is called a mobile node. It can continue to communicate with other nodes at any location using its IP address.

Home Agent: A home agent is a router on the mobile node's home network that maintains current location information for the mobile node and forwards the packets that are addressed to the mobile node to its current point of attachment on the network, when it is away from home.

Foreign Agent: The Foreign Agent is a router on a mobile node's visited network and functions as the point of attachment for the Mobile Node when it is away from home, delivering packets from the Home Agent to the Mobile Node.

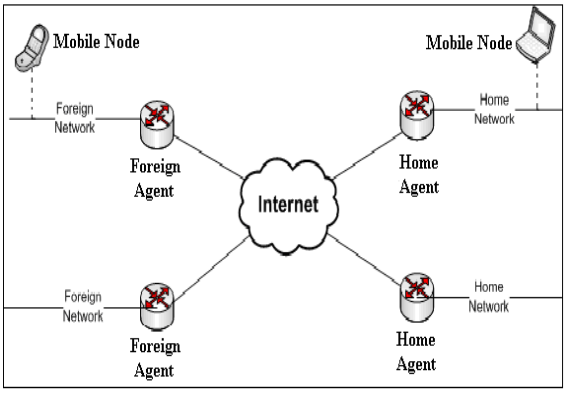

Figure 1. Mobile IP components and their relationships.

2.3 How Mobile IP works

Mobile IP uses two IP addresses: a fixed home address and a care-of-address (COA) that changes at each new point of attachment. When a mobile node moves from its home network to a foreign network, it waits for an advertisement from or sends a solicitation message to the foreign agent on the foreign network informing its presence. The mobile node thus obtains a COA, which is either dynamically assigned or is associated with its foreign host. The home address is static and is used for identifying TCP connections. The home address makes it possible that the mobile node is continually able to receive data on its home network. On the other hand, COA indicates the network number and it changes at each new point of attachment with respect to the network topology [1].

The protocol of Mobile IP can be best described with the cooperation of three separable mechanisms discussed below:

Agent Discovery: A mobile node discovers its home and foreign agents in the discovery phase.

Registration: A mobile device registers its COA with its home agent and foreign agent in the registration phase.

Tunneling: A tunnel is set up to route packets from the home agent to the foreign agent and finally to the mobile node.

3. DoS ATTACK SCENARIOS

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. 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 wireless resources such as 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.

A simple delimitation of Denial-of-Service (DoS) attack is 'A bad guy preventing a good guy from accomplishing work done'. Actually, a DoS attack takes one of the two forms:

- A bad guy floods nuisance packets (TCP SYN flooding) or

-The bad guy somehow precludes packets from flowing between two nodes.

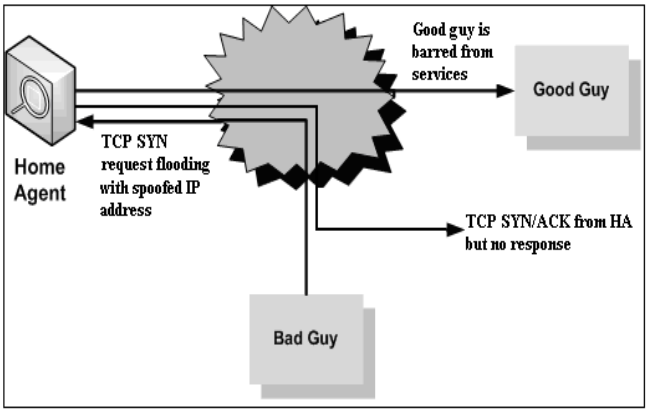

Figure 2. TCP SYN flooding DoS attack Scenario.

In the case of Mobile IP, when a bad guy somehow manages a bogus registration of a new COA for a particular 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 and can raise some problems:

-The actual mobile node is no longer connected.

-The bad guy can see all the traffic going to actual mobile node.

-All packets sent by correspondent nodes would be tunneled by home agent to the bad guy.

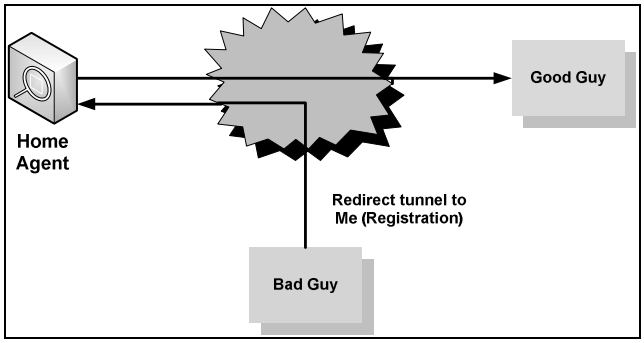

Figure 3. Redirecting tunnel DoS attack.

In this attack an attacker can overflow the access server. It is possible because the sensitive IP addresses of the HA and the MN are not hidden in the registration message. Unlike a privacy attack, where an adversary is trying to gain access to information it is not allowed to see, a DoS attack involves an adversary trying to keep you from accessing information or resources you have every right to access. This attack does harm for two systems:

-The destination targeted system

-The system which is actually using the spoofed address in the global routing system.

DoS attacks are potentially devastating to the victim. 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 a node continuously sends an executable flooding packet to its neighborhoods and to overload the storage space and exhaust the memory of that node. This prevents the node 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. A malicious node 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 bogus source IP addresses of other nodes, thereby overloading the network. This consumes the resources of all neighbors that communicate, overloads the network, and results in performance degradations.

In this case, firewall offers some level of protection. 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. So, in this paper, we applied some filtering techniques to filter the suspected packets in order to protect against DoS attacks.

4. RELATED WORKS

Currently Mobile IP is gaining popularity for its attractive features and applications. 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. Braun *et al.* [4] proposed a solution to provide security to Mobile IP using IP Sec. Considering a VPN or a secured network protected by a firewall, the way in which a Mobile Node can securely access this network is proposed in [4]. In order to traverse the firewall the Mobile Node has to authenticate itself using IP Sec. Zao *et al.* [5] used IP Sec ESP protocol in Mobile IP to protect against both passive and active attacks. They also proposed to add some modifications to agent advertisement and to registration request messages. Gupta *et al.* [6] proposed MobileIP 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. Secure Mobile IP protocol has been proposed to modify Mobile IP protocol with IP Sec in [7]. Datagram going into the network and going out the visiting network both are securely processed using IP Sec. Here secure Mobile IP is implemented on gateway servers and mobile hosts. In most the above works some general security measures such as cryptography, authentication etc are used to reduce the threats against mobile IP communication. But they didn't focus on specific attack. Security attacks and mechanisms for mobile or wireless networks through encryption, key management, authentication, routing, and packet filtering techniques have been proposed in many research papers [1-5, 8, 10, 17-20]. Some researches also have been done for detecting and preventing DoS attack, but all of them are for wired communication or mobile ad hoc networking. Xiang *et al.* [9] proposed a defense system against DoS attack by large scale IP Trace back. Denko *et al.* [18] proposed a DoS attack prevention scheme in mobile ad hoc network's using reputation based incentive scheme. In this proposed mechanism, the reputation of all nodes in the add hoc network will be updated based on their behavior (good or malicious). Xiaowei Yang, David Wetherall and Tom Anderson [11] proposed TVA system, Packet Passport system and StopIt system for limiting DoS attack in wired communication. Traffic Validation Architecture (TVA) is short-term authorization that senders obtain from receivers and stamp on their packets [11]. The Packet Passport system is a piece of authentication information embedded into an IP packet that authenticates the source IP address [11]. StopIt is a packet filtering system to block the undesired traffic it receives [11].

5. DESIGN OF PROPOSED SOLUTION

Detecting and preventing DoS attacks is difficult in highly dynamic and large networks. Hence, it is necessary to divide these networks into small and manageable groups and implement security mechanisms in each group in a distributed manner. In this paper, at first we divided the whole network into some

domains. Then we divided each domain into some clusters. Each cluster contains one or more wired or mobile node. Clustering provides a distributed and scalable architecture for network monitoring and topology control. Clustering architecture also provides a localized attack detection and prevention mechanism through continuous monitoring and information exchange. This localized and distributed feature also reduces storage and communication overhead, thereby optimizing network bandwidth utilization. The figure below shows the clustering architecture:

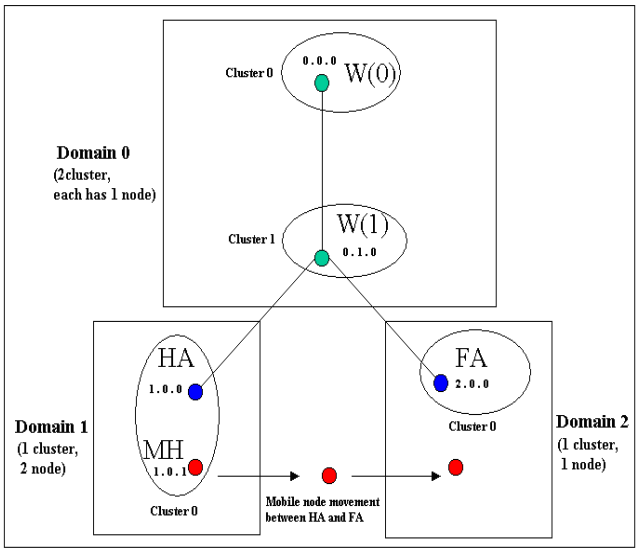

Figure 4. Clustering Architecture of mobile IP communication.

We have created a wired-cum-wireless topology through which we can exchange packets between a wired and wireless domain via a base-station. But a mobile node may roam outside the domain of its base station and should still continue to receive packets destined to it. Actually we have extended the mobile IP support in a wired-cum-wireless scenario.

In the above picture there is a wired domain consisting of 2 wired nodes, W0 and W1. We have 2 base-station nodes and call them Home Agent (HA) and Foreign Agent (FA) respectively. The wired node W1 is connected to HA and FA as shown in the figure 4. There is a roaming mobile node called Mobile Host (MH) that moves between its home agent domain and foreign agent domain. A TCP flow will be set up between any node (e.g. W0) and MH. As MH moves out from the domain of it's HA, into the domain of FA, the packets destined for MH is redirected by it's HA to the FA as per mobile IP protocol definitions.

In the above topology we have one wired domain (denoted by 0) and 2 wireless domains (denoted by 1 & 2 respectively). Hence the addresses of two wired nodes are 0.0.0 and 0.1.0. In the first wireless domain (domain 1) we have a base-station, HA and mobile node MH, in the same single cluster. Their addresses are 1.0.0 and 1.0.1 respectively. For the second wireless domain (domain 2) we have a base-station, FA with an address of 2.0.0. However when the MH will move into the domain of FA, the packets originating from a wired domain and destined to MH will reach it as a result of the Mobile IP protocol. The above figure is a basic structure of mobile IP communication network. This network may contain a huge number of domains; each domain may contain different number of clusters and each cluster can contain a different number of nodes.

We have created a wired-cum-wireless topology through which we can exchange packets between a wired and wireless domain via a base-station. But a mobile node may roam outside the domain of its base station and should still continue to receive packets destined to it. Actually we have extended the mobile IP support in a wired-cum-wireless scenario.

In the above picture there is a wired domain consisting of 2 wired nodes, W0 and W1. We have 2 base-station nodes and call them Home Agent (HA) and Foreign Agent (FA) respectively. The wired node W1 is connected to HA and FA as shown in the figure. There is a roaming mobile node called Mobile Host (MH) that moves between its home agent and foreign agents. A TCP flow will be set up between any node (e.g. W0) and MH. As MH moves out from the domain of it's HA, into the domain of FA, the packets destined for MH is redirected by it's HA to the FA as per mobile IP protocol definitions.

In the above topology we have one wired domain (denoted by 0) and 2 wireless domains (denoted by 1 & 2 respectively). Hence the addresses of two wired nodes are 0.0.0 and 0.1.0. In the first wireless domain (domain 1) we have a base-station, HA and mobile node MH, in the same single cluster. Their addresses are 1.0.0 and 1.0.1 respectively. For the second wireless domain (domain 2) we have a base-station, FA with an address of 2.0.0. However when the MH will move into the domain of FA, the packets originating from a wired domain and destined to MH will reach it as a result of the Mobile IP protocol. The above figure is a basic structure of mobile IP communication network. This network may contain a huge number of domains; each domain may contain different number of clusters and each cluster can contain a different number of nodes.

Filtering in Domain Periphery Router:

In each domain there is an edge or periphery router through which each packet within the domain has to pass for going to another domain. In the above figure-4, the node W(1) is the periphery router for domain 0. So our proposed scheme will imply filtering technique in that node. If any malicious node from domain 0 wants to attack a mobile node outside that domain with spoofed IP address then the periphery router will detect and discard that suspected packet. The periphery router would check:

IF packet's source address is within domain's address

THEN forwards the packet

IF packet's source address is anything else

THEN discard the packet

Filtering in the Base Station Node:

If the attacker resides inside the same domain of the victim, then the edge or periphery router could not detect the attacking packet. That's why we have proposed an additional filtering technique in the Base Station node (HA or FA) to which the mobile nodes are connected. Basically the base station nodes (HA or FA) in mobile IP communication are the main targets of the attackers, because the mobile nodes get services from these base stations. So detecting and preventing attacks in the base station nodes is very important. In our proposed scheme the base station node will filter a packet if one of the following events occurs:

- If the base station's router queue overflows
- If there are many packets from same domain or same cluster, because the attacker nodes at first take help from the neighbor for attacking any target.
- If most of the bandwidth of the network is consumed by DoS attackers, then the network will be congested. If the network gets congested then incoming packets should be discarded for the time beings.

5. IMPLEMENTATION AND ANALYSIS

Assumptions

We make the following assumptions for the proper operation of the proposed architecture:

(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, although a node may have more resources than others during the communication process.

5.1 Simulation Environment:

We have done the performance evaluation using NS2 [12, 14, 15, 17]. At first we have implemented the DoS attack scenario without protection. After that we have simulated the scenario with applying filtering technique in the periphery routers only, then with our full proposed scheme. Then we compared the performance results. Simulation performance metrics and simulation parameters are given below:

Table 1. Simulation Parameters

Parameters	Values/Ranges
Simulation area	1000m x 1000m
Speed (m/s)	1 m/s to 20 m/s
Packet Rate	5 Packets / s
Packet Size	128 Bytes
Traffic Source	CBR
Pause Time	Uniformly distributed in 0-50 s
Routing Protocols	DSDV and Mobile IP
Number of Nodes (max)	100
Number of Domains	4 - 5
Number of Clusters	5 - 10
Transmission Range	300 m
Simulation Time	250 s

5.2 Performance Metrics

The performances of simulation were measured using the following metrics:

-Packet delivery ratio: Defined as the ratio of the total number of packets received by destinations and the total number of packets sent by a source.

-Routing and Communication overhead. Defined as the number of instructions and packets needed to maintain the entire network.

-Misbehaving nodes detection rate. Defined as the ratio of the total number of malicious node detected and the total number of malicious node in the network

-Network Size. Defined as the total area of the network.

5.3 Comparison of Simulation Results

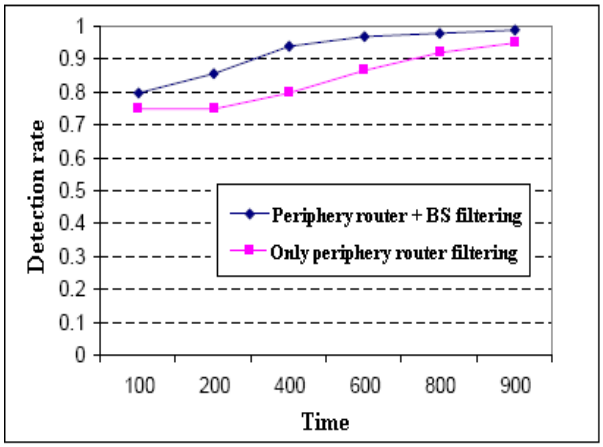

Figure 5. Time Vs Detection rate.

The above figure-5 shows that our system will exhibit better performance for malicious node detection rate if we use base station filtering and the periphery router filtering rather than using only periphery router filtering

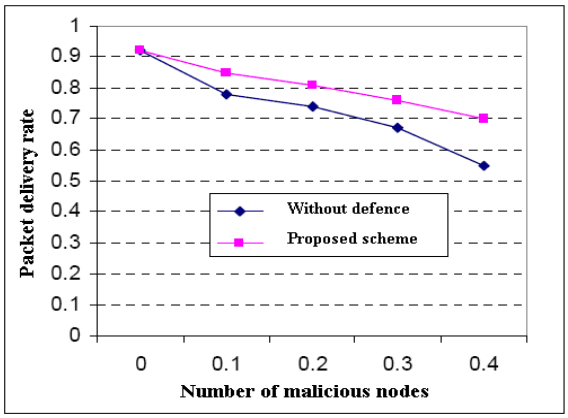

Figure 6. Time Vs Detection rate.

If number of misbehaving nodes increases then the packet delivery ratio will decrease due to attack in the servers and network resources consumed by the attackers. The above figure-6 shows that if our proposed scheme is applied then the packet delivery ratio will increase slightly in spite of the presence of DoS attack.

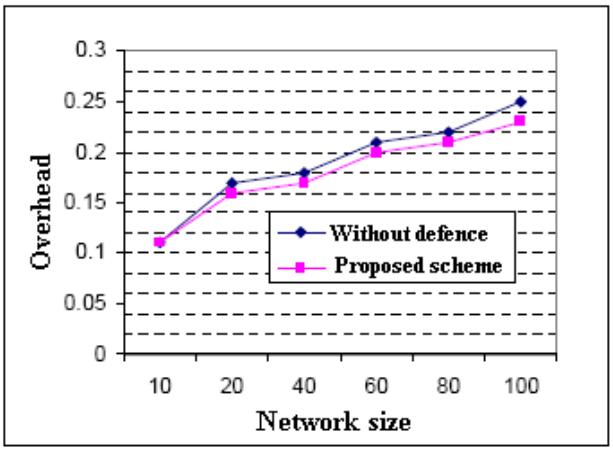

Figure 7. Network size Vs overhead.

The above figure-7 shows that, as the network size increases the total overhead increases. When our proposed scheme is applied the overhead is relatively lower due to the use of clustering architecture.

6. CONCLUSION AND FUTURE WORK

DoS attack in mobile IP communication is serious, and the detection and prevention of this attack is difficult than in their wired counterparts. In this paper, we proposed packet filtering technique for detecting and preventing DoS attack in mobile IP communication. We proposed to apply a packet filtering technique at the vulnerable points of the mobile IP communication to check the suspicious packet. We used the network simulator ns-2 for simulating the performance of our proposed system. We observed that our proposed scheme showed better performance for the protection of system in comparison with system without filtering. In future we want to analyze the effect of Distributed Denial-of-Service (DDoS) in mobile IP communication.

7. REFERENCES

[1] Nikander, P., Arkko, J., Aura, T., Montenegro, G., "Mobile IP version 6(MIPv6) Route Optimization Security Design", Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th volume 3, Issue, 6-9 Oct. 2003 Page(s): 2004 – 2008.

[2] Habib, A., Hafeeda, M.H, and Bhargava, B.,"Detecting Service Violation and DoS Attacks", In Proc. of Network and Distributed System Security Symposium (NDSS), 2003.

[3] Gupta,V., Krishnamurthy, S., and Faloutsos, M.,"Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks", In Proc. of MILCOM, 2002.

[4] Braun, T., and Danzeisen, M., "Access to Mobile IP Users to Firewall Protected VPNs", Workshop on Wireless Local Networks at the 26th Annual IEEE Conference on Local Computer Networks (LCN'2001).

[5] Zao, J.K., M. Condell, "Use of IP Sec in Mobile IP", Mobile IP Internet Draft, draf-itef-mobileip-ipsec-use-0 0.txt, November 1997.

[6] Gupta,V., Montenegro,G., "Secure Mobile Networking, Mobile Networks and Applications", Volume 3 , Issue 4 (1998) table of contents,Special issue: mobile networking in the Internet, Pages: 381 - 390.

[7] Inoue,A.,Ishiyama, Fukumoto, A., and Okamoto, T., "Secure Mobile IP using IP Security Primitives", IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1997, PP: 235-241.

[8] Deng, R.H., Zhou,J., Bao,F., "Defending Against Redirect Attacks in Mobile IP", Proceedings of the 9th ACM conference on Computer and Communications Security, November 2002.

[9] Denko, M.K.,"Detection and Prevention of DoS Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme", Systemics, Cybernetics and informatics, Volume 3- Number 4.

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

[11] McCanne, S., and Floyd, S., Network Simulator, http://www.mash.cs.berkley.edu/ns/.

[12] Greis,M.,"Marc Greis's Tutorial", http://www.isi.edu/nsnam/ns/tutorial/index.html.

[13] Han, S., Tian, B., He, M., Chang, E., "Efficient Threshold Self-healing Key Distribution with Sponsorization for Infrastructureless Wireless Networks", IEEE Transactions on Wireless Communications, Vol. 8, No. 4, pp. 1876-1887.

[14] Chung, J., and Claypool, M., NS by Example, http://nile.wpi.edu/NS/

[15] Altman, E., and Jimenez, T., "NS Simulator for beginners",http://wwwsop.inria.fr/maestro/personnel/Eitan.Altman/ns.html.

[16] Han, S., Dillon, T.S., Chang, E., Tian, B., "Secure web services using two-way authentication and three-party key

establishment for resource delivery", Journal of Systems Architecture, Vol. 55, no. 4, 233-242, 2009, Elsevier.

[17] The ns Manual, http://www.isi.edu/nsnam/ns/ns-documentation.htmll

[18] Yang, X., Wetherall, D., and Anderson, T., "A DoS-limiting Network Architecture", ACM SIGCOMM Computer Communication ,Volume 35 , Issue 4 (October 2005) ,2005,Pages: 241 - 252.