Mobile Information Systems 8 (2012) 127–152
DOI 10.3233/MIS-2012-0135
IOS Press

A methodology to counter DoS attacks in mobile IP communication

Sazia Parvin[a,*], Farookh Khadeer Hussain[b] and Sohrab Ali[c]
[a]*Digital Ecosystems and Business Intelligence Institute, Curtin University, Perth, Australia*
[b]*School of Software, Faculty of Engineering and Information Technology, University of Technology, Sydney, Australia*
[c]*The People's University of Bangladesh, Dhaka, Bangladesh*

Abstract. Similar to wired communication, Mobile IP communication is susceptible to various kinds of attacks. Of these attacks, Denial of Service (DoS) attack is considered as a great threat to mobile IP communication. The number of approaches hitherto proposed to prevent DoS attack in the area of mobile IP communication is much less compared to those for the wired domain and mobile ad hoc networks. In this work, the effects of Denial of Service attack on mobile IP communication are analyzed in detail. We propose to use packet filtering techniques that work in different domains and base stations of mobile IP communication to detect suspicious packets and to improve the performance. If any packet contains a spoofed IP address which is created by DoS attackers, the proposed scheme can detect this and then filter the suspected packet. The proposed system can mitigate the effect of Denial of Service (DoS) attack by applying three methods: (i) by filtering in the domain periphery router (ii) by filtering in the base station and (iii) by queue monitoring at the vulnerable points of base-station node. We evaluate the performance of our proposed scheme using the network simulator NS-2. The results indicate that the proposed scheme is able to minimize the effects of Denial of Service attacks and improve the performance of mobile IP communication.

Keywords: Security, communication, mobile IP, DoS, DDoS, attack, filtering, monitoring

1. Introduction

In the last few years, demands for mobile computing have increased noticeably with the increasing use of powerful hand-held communicating wireless devices such as cell phones, i-pod, PDAs, laptops etc. Remarkable progress in the areas of mobile computing has streamlined our communication. In spite of having worldwide Internet access, it is not expectable to reap all the benefits until secure communication over the communication channel is ensured. There are different kinds of security threats in current wireless networks. Palmieri et al. [35] proposed a new active third party authentication, authorization and security assessment strategy for next generation wireless mobile networks. Algorithms are proposed in [15] to quantify the trust between all parties of 3G-WLAN including cellular and IP technologies integrated networks to secure user authentication in wireless networks.

Providing security for Mobile IP communication is a complex process because of its inherent dynamic characteristics like frequent changes in the point of attachment, absence of central administration etc. Various kinds of attacks on Mobile IP Communication can disrupt normal functioning. Among all these attacks, Denial of Service (DoS) is a difficult problem and becomes an increasing threat to the current Internet [34].

*Corresponding author. E-mail: sazia.parvin@postgrad.curtin.edu.au.

The main target of Denial of service (DoS) attack is to consume a server's resources such as network bandwidth, computing power, main memory, disk bandwidth etc. This results in either limited or no resources being left to process further upcoming requests from legitimate clients. Thus, a DoS attack can paralyze any user, site or server in the Internet. There is another category of DoS attack which is known as Distributed Denial of Service (DDoS) attack, where many malicious users simultaneously attack the same site/server. As a result, the impact of the attack on that node is much more severe. Therefore, DDoS is often considered as one of the worst possible attacks in the current Internet [34]. DoS might be a great threat in the ubiquitous medical sensor networks [14] by changing the patient's data. Delot et al. [11] proposed a data management solution for event exchange in vehicular networks to avoid dangerous/undesirable situations where DoS might be a great threat. A general solution is proposed to protect the system against DoS attack by filtering DoS attack requests at the possible earliest point before they use much of the server's resources [31]. A considerable amount of work has been done to prevent DoS attacks on wired networks. In contrast, however, there has been little research focused on Mobile AdHoc Networking. However, DoS attack is now considered to be a great threat to Mobile IP communication. In this work, we have proposed a new technique to prevent DoS attack in Mobile IP communication. We propose two techniques in this paper: (i) packet filtering technique in the domain periphery router and base station for discarding the suspected packets sent by the DoS attackers by (ii) queue monitoring technique to mitigate the effect and damage by DDoS attack in the vulnerable points of the network.

1.1. Objectives and motivation

Today's world is enjoying tremendous advantages thanks to the advancement in the area of mobile computing. Mobile IP uses one of the technology which can support of various mobile data and wireless networking related applications. Users can enjoy abundant seamless roaming and fast feasible application anywhere at any time by using mobile IP. Moreover, users can get continuous access to the Internet through Mobile IP. Hence, ensuring security services for Mobile IP has now become a major challenging issue of researchers. There are different kinds of attacks in Mobile IP communication which can disrupt its normal communication. Denial of Service (DoS) attack is one of the greatest threats to today's Internet [34]. A DoS attack is capable of harming any user or server connected to the Internet. You et al. [49] proposed fast mobile IPv6 security by minimizing an involvement of the authentication server. A huge amount of work [11,17,21,25] has been done to prevent or mitigate this type of attack. But most of this work has been done for wired communication, while some relates to mobile adhoc Networking. Providing security mechanisms against DoS attack for Mobile IP communication is an outstanding research issue. Although some works have enhanced the security for Mobile IP communication, most provide only a general solution and do not address the problem clearly. They do not provide the security requirements of the applications and do not adequately address specific attacks. Therefore, in this paper, we propose a solution to counter DoS attack in Mobile IP communication.

1.2. Problem statement

Recently, Mobile IP has received closer attention in areas of both research and application. The application of Mobile IP is increasing day-by-day. Mobile IP devices are vulnerable to attacks because of their dynamic nature. Most of the current researchers pay attention how to increase the network efficiency in mobile IP Environment. A great deal of research has been done to overcome this problem [33,39, 46]. Therefore, there are quite a number of proposals proposed in [33,39,46] which can show high

performance through route optimization. Providing security in Mobile IP using the firewall concept has been proposed in many research proposals. That is, the Mobile IP users can securely access a firewall-protected network. Much work has been done to provide security to Mobile IP using IP Sec. Original Mobile IP protocol provides some general security services which gives some protection to mobile IP communication. However, there still exist numerous threats that cannot be prevented by current general security services. Much work has been done to remove the inefficiencies of existing security protocols for mobile IP communication, but little has been done to protect mobile IP communication from specific attacks like DoS attack [4]. It is difficult to mitigate DoS attack in Mobile IP communication due to the following problems:

- A very little research has been done to mitigate DoS attacks in the Mobile IP communication. Little research has been carried out to compare and categorize different types of DoS attacks and find defense mechanisms.
- There is no effective defense mechanism against DoS attack in Mobile IP communication as well as no guideline for the selection of defense mechanism.
- Existing solutions and defense mechanisms have been evaluated based on assumptions and according to limited criteria.

1.3. Aim of this work

The main goal of this work was to analyze the effect of Denial of Service attack on mobile IP communication and provide a reliable solution for ensuring security against this attack. Our aim is to use a packet filtering technique for discarding the suspected packets sent by the DoS attackers. We are also interested in monitoring the queues in the vulnerable points of the network to mitigate the effect and damage caused by DDoS attack.

1.4. Scope of this work

There are different ways to ensure security against Denial of Service attack. We can detect the suspected packets related to DoS attack and discard those packets before the attack occurs. We can do this at the important points of the network. Sometimes we cannot detect the attacks before they occur. In these cases, we have to mitigate the amount of damage done during the attack. As a precaution, we can also mark every packet going through the network routers by keeping track of its previous source and next destination. When a packet is detected as a suspicious packet, we can trace it back to its original source following the marked paths. Thus, we can detect the real attacker. Possible approaches for ensuring security against Denial of Service attack are as follows:

1. DoS attack detection and prevention
2. Mitigating the amount of damage while being attacked
3. Back-tracking and packet marking for detecting the attacker

Our work focuses on the first two approaches. The third approach has been omitted here.

2. Major contributions

The major contributions of this paper is to analyze the effects of Denial of Service attack on mobile IP communication in detail. We propose here packet filtering techniques in different domains and base

stations of mobile IP communication to detect suspicious packets and by using these techniques we can improve the performance. If any packet contains a spoofed IP address which is created by DoS attackers, the proposed scheme can detect this and then filter the suspected packet. The main contribution of this paper is:

- We filter the domain periphery router and base station to mitigate the effect of Denial of Service (DoS) attack.
- We monitor the queue at the vulnerable points of base-station node to minimize the Denial of Service attack.
- We evaluate the performance of our proposed scheme using the network simulator NS-2 and show that our proposed scheme is able to minimize the effects of Denial of Service attacks and improve the performance of mobile IP communication.

3. Related works

Mobile IP produces new security threats for wireless networks and there is a comparatively higher chance being attacked by hostile opponents in comparison to wired network due to their wireless media. In the following sections we highlight different works related to ensuring the security of mobile IP communication.

3.1. Sec MIP

Torsten Braun and Marc Danzeisen [5] proposed Secure Mobile IP (SecMIP) to provide security to Mobile IP using IP Sec. In their work [5], they proposed the way in which a Mobile node access the network securely. Each Mobile Node needs to authenticate itself using IP Sec if it wants to traverse the firewall. Therefore, a secure IP Sec tunnel is established between the firewall and the Mobile Node for the communication. The functionalities of this tunnel and working principles are fully described step by step in this paper [5]. SecMIP is implemented and a performance result is also presented in this work. The main advantage of this solution is that it does not require the introduction of any new protocols or the modification of any existing protocol. But the problem of this proposition is that if a Mobile Node wishing to transfer data to a correspondent node, it must send it via the Home agent [5]. So, there is a chance of traffic increment in the network as a MN cannot securely transfer data to a correspondent node directly. The authors in [19] proposed an effective method for measuring the accuracy of IP multicast based multimedia transmission and the main focus of this method is to find the accuracy and the complexity of the user model describing user movement in the network.

3.2. Use of IP Sec in mobile IP

John K. Zao and Matt Condel [51] used IP Sec ESP protocol in Mobile IP to defend against both passive and active attacks. In this approach, the security requirements are fulfilled by establishing a MIP-IPSec tunnel between MN-HA, HA-FA and FA-MN. Some modifications have been proposed to Agent advertisement and to the registration of request messages. The authors in [29] proposed a Diffie-Hellman key based authentication scheme that utilizes the low layer signaling to exchange Diffie-Hellman variables and allows mobility service provisioning entities to exchange mobile node's profile and ongoing sessions securely.

3.3. Secure mobile networking

Vipul Gupta and Gabriel Montenegro [22] proposed some enhancements to the basic MobileIP protocol so that authorized users can access a network that is protected by some combinations of source filtering routers or the network such as firewalls, which are using private address space for security reasons. The use of private addresses is quite challenging to Mobile IP because the Mobile node cannot use its home address to communicate with a correspondent node while outside its protected network. The concept of a secured Mobile IP presented in this paper [22] is able to solve the security problems of Mobile IP in an efficient and successful way, but it requires the introduction of new protocols. The authors in [10] proposed a novel secure and efficient ID-based mobile IP registration protocol in Mobile IP networks by considering performance while providing the security. The authors in [30] proposed a general analytical model through Authentication, Authorization, and Accounting (AAA) framework architecture which is able to protect incoming messages from malicious attackers in Mobile IP. The authors in [42] proposed an agent-based model to find the issues of intrusion detection in cluster based mobile wireless ad hoc network environment and evaluated how agent based approach facilitates flexible and adaptable security services. Ciou et al. [9] proposed an effective and efficient handover key management and authentication scheme during handover by speeding up the handover process through Diffie-Hellman key exchange scheme in order to increase the security level for mobile stations (MSs).

3.4. Secure mobile IP protocol

Atsuhi Inoue, Masahiro Ishiyama, Atsushi Fukumoto and Toshio Okamoto [26] proposed to modify Mobile IP protocol with IP Sec. Datagram entering the network and exiting the visiting network both are securely processed using IP Sec. Here, secure Mobile IP is implemented on gateway servers and Mobile Nodes for evaluation purpose. In this approach, a mobile node with IP Sec processing capability is called a Secure Mobile Node (SMN) and a firewall with IP Sec processing capability is called a Security Gateway (SGW). It is recommended to place SGW between the inside network and the Internet. But the organization can also place SGW inside it's network to protect of the specific division of the network. A dynamic gateway discovery has beeb proposed to select the best location for a specific SGW and also a communication model showed the details for traversing of SGW using IP Sec.

3.5. Securing binding update message

A new protocol is proposed to secure binding update messages and protect against redirect attacks [13]. This protocol uses public key cryptosystems which is based on digital signature and Diffie-Hellman key exchange algorithm. Chang et al. [7] designed the proper technical measures ('Software Tamper Resistance') for mobile game service to minimize its vulnerability by using cryptography techniques. There are two existing protocols proposed by the IETF Mobile IP working group. They analyzed the weakness of these existing protocols and generated the report. The authors in [7] mentioned secure key negotiation as a challenging issue for the successful deployment of mobile IPv6. In their work, they analyzed and showed the performance of optimal binding-management-key refresh interval in mobile IPv6 networks. Chen et al. [8] a novel authentication scheme to ensure the security of the transmitted messages against known attacks by integrating fingerprint biometrics, related cryptology and a hash function mechanism and this scheme requires a low implementation cost.

3.6. Mobile IP security system

John Zao, Stephen Kent, Joshua Gahm, Gregory Troxel, Matthew Con-dell, Pam Helinek, Nina Yuan and Isidro Castineyra [50] designed and implemented Mobile IP Security System (MoIPS) using a public

key system for route optimization. According to their approach, all the hosts and mobile agents must use MoIPS certificates with a view to authenticate the Mobile IP control messages. Public key technology can efficiently meet the requirements of key management. It is mentioned in [27] that the X.509 PKI uses two types of certificates: Certificate of Mobile IP Control Message Authentication (MoIPS Certificates) and Certificates for IP Security Services (IP Sec Certificates). There are many solutions for ensuring the security in Mobile IP. Most of the solutions are general and do not focus on specific attacks. Some research has also been done on the detection and prevention of DoS attacks, but most of them are for either wired communication or mobile ad hoc networking. We discuss several of these works below.

3.7. DoS attack detection approaches

Most of detection approaches rely on finding the malicious party who has created a DoS attack and subsequently made damage [23]. However, identifying and tracking the real attacker is not a easy task. The authors in [23] mentioned two possible reasons: (i) the attacker spoofs the source IP address of the attacking packets and (ii) the Internet is stateless, which makes a sense that whenever a packet goes through a router, the router does not store any information (or traces) about that packet.

IP trace back

Yang Xiang and Wanlei Zhou [47] proposed a protection system against DoS attack by a large scale IP Traceback method. They named their system FDPM (Flexible Deterministic Packet Marking). IP Traceback can identify IP packets of their sources without any prior information about the source address field of the IP header. This technique is extremely beneficial for identifying the sources of the attackers and taking appropriate actions against them. This proposition is applicable for wired networks.

ICMP trace back

Bellovin [2] proposed the idea of ICMP Traceback messages. In this approach, every router use one sampling technique for each forwarded packets with a very low probability and reports to the base station by sending an ICMP Traceback message while packets are passed through the network from the attacker to the victim. An ICMP Traceback message carries the information about the previous and next hop addresses of the router, timestamp, portion of the traced packet, and authentication information [2]. The most challenging thing of this approach is that the attacker makes the victim confused by sending many false ICMP Traceback messages. Barros [1] proposed a modification to the ICMP Traceback messages to figure out the Distributed DoS (DDoS) attacks by reflector.

Packet marking

Burch and Cheswick [3] proposed to discover some path information into the header of the packets instead of routers sending separate messages for the sampled packets. This marking technique is deterministic or probabilistic. In the deterministic marking technique, all packets are marked by every router marks. The major drawback of the deterministic packet marking is that the packet header increment is proportional to the number of hops increment on the path. In probabilistic packet marking (PPM) technique, it encodes the path information of every packet into a small possible fraction. It is assumed that a huge amount of packet traffic rush towards the victim during a flooding attack. Therefore, many of these packets will be marked at routers by packet marking technique during their travel from the source to the victim. The marked packets which contains enough information will be able to provide enough information to trace the network path from the victim to the source during the network travel.

3.8. DoS attack prevention approaches

We discuss here some DoS attack preventive approaches. The goal of these approaches are to identify the attacked packets and discard them from the network before they attack the victim. We examine several packet filtering approaches [10,12,36,48] that are able to detect the attack packet and discard them from the network.

Reputation based incentive scheme

Denko et al. [12] proposed a DoS attack prevention scheme using a reputation-based incentive scheme which works fine in mobile ad hoc networks. With this proposed mechanism, the reputation of all nodes in this network will be updated based on their behavior (good or malicious). They examined their technique on both active and passive DoS attack and claimed their technique will motivate the nodes in the ad hoc network to prevent both types of DoS attacks.

DoS limiting network architecture

TVA system, Packet Passport system and StopIt system are proposed in [48] for limiting DoS attack in wired communication. Traffic Validation Architecture (TVA) is short-term authorization technique. In this TVA technique, senders will stamp their authorization on received packets whenever they will receive from receivers. The Packet Passport system is a piece of authentication information embedded into an IP packet that authenticates the source IP address. StopIt is a packet filtering system that blocks the undesired traffic it receives.

Ingress filtering

Ingress routers can filter the incoming packets to a network domain. These filters has the capability to verify the identity of packets entering into the domain. Farguson and Senie [10] proposed Ingress filtering which can filter the incoming packets by dropping any traffic with an IP address that does not match a domain prefix connected to the ingress router.

Egress filtering

The concept behind an egress filter [6] is that only packets with one's network source address should be leaving one's network. In computer networking, egress filtering is a technique which can monitor and restrict the flow of information from one network to another. Router or firewall of a networks can always examine the TCP/IP packets that are being sent out of the internal. Packets that do not meet security policies, are denied by the egress filter. Egress filtering ensures the presence of the unauthorized or malicious traffic in the internal network. The idea is to permit only those packets from trusted hosts to leave your network [18].

Route-based filtering

Route-based filtering is proposed by Park and Lee [36] which can filter out spoofed IP packets based on route information. In this system, every router keeps track of the incoming and outgoing paths of each packet. When a packet is detected as malicious, then its route from sender to receiver is marked as dangerous. In future, packets coming from that route would be blocked. Qadri et al. [41] mentioned that the lack of centralized routing and network resource management becomes an obstacle fore video streaming within a VANET.

As we can see from a comprehensive review of the existing literature review, we represent a meta-literature analysis in the Table 1:

Table 1
Literature review

Packet filtering techniques	Proposed schemes	Outcomes	Shortcomings
Reputation Based Incentive Mechanism [12]	Reputation Based Incentive Scheme	They proposed reputation-based incentive mechanism for encouraging nodes to cooperate both in resource utilization and preventing DoS attacks [12]	The approach is only used for clustering architecture in MANETs in a localized or distributed manner
Traffic validation Architecture [48]	Traffic validation Architecture	They proposed the design and evaluation of TVA, a network architecture that limits the impact of Denial of Service (DoS) floods from the outset	The approach works for wired communication
Ingress filtering [10]	Ingress filtering techniques	This mechanism can drop any traffic with an IP address that does not match a domain prefix connected to ingress router [10]	This approach works for Internet Service Providers and the Internet community
Egress filtering [6]	Egress filtering technique	Packets that do not meet security policies are now allowed to leave-they are denied "egress" [6]	This approach is only to permit those packets from trusted hosts to leave own network [18].
Route based filtering technique [36]	Route-based distributed packet filtering technique [36]	Every router keeps track of the incoming and outgoing paths of each packet.	This approach is suitable for Internet-based system.

Clearly, from a comprehensive review of the existing body of literature and the meta-literature analysis on mobile IP, we can conclude that (a) there has been significant research and advances made in the area of mobile IP security (b) there is no-method to counter the DoS attacks in Mobile IP.

4. Methodology to counter DoS attack

It is too complex to detect and prevent DoS attack in a dynamic network such as wireless sensor networks, mobile ip networks. So, its easier to divide a large network into small and manageable groups and implement security mechanisms in each group in a distributed manner instead of thinking the whole network [37]. For this purpose, here we follow the same hierarchical architecture which we already proposed in [37]. More specifically, we propose to first divide the network into domains. Then each domain can be divided into clusters, each of which consists of one or more wired or mobile nodes or base station. We argue that, if we can manage and secure each cluster efficiently, we can in turn secure each domain and thus the whole network becomes secure. This is basically a distributed approach where each domain or cluster is independent.

Clustering architecture is a distributed and scalable architecture for monitoring and securing the networks.

There are other benefits of clustering architecture as stated in [12]. Clustering architecture can monitor the network continuously and detect the attack in the network. After that, it provides prevention mechanism based on the attacker's characteristics. So, this architecture can minimize the network bandwidth by reducing storage and communication overhead. The Fig. 1 shows the clustering architecture of a network:

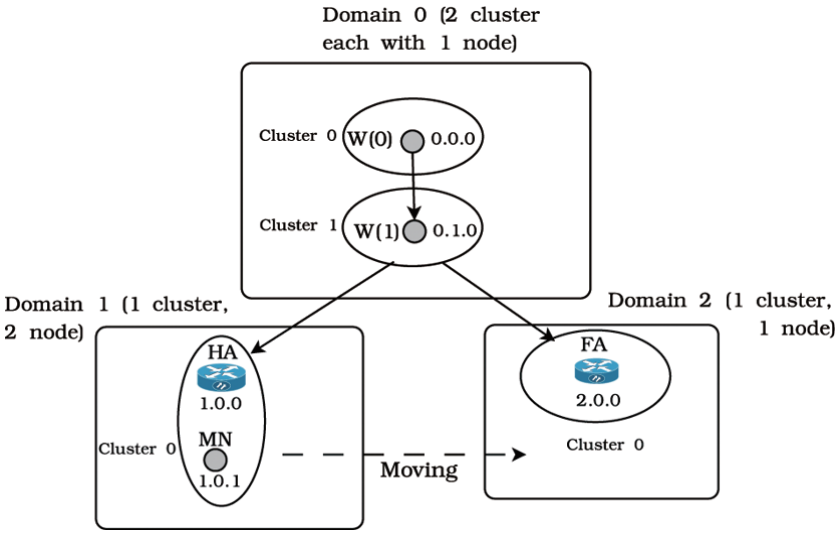

Fig. 1. Clustering architecture of mobile IP communication.

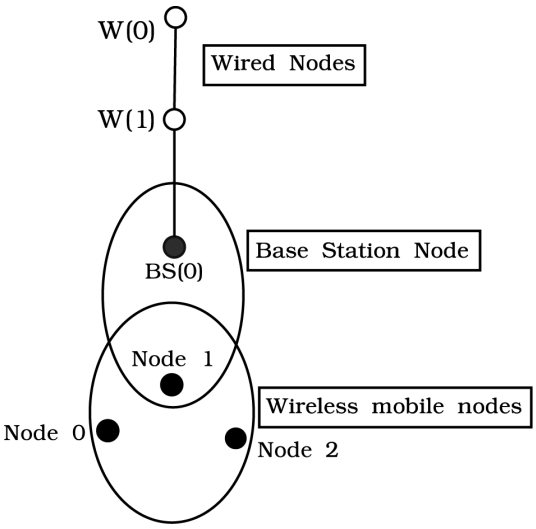

Fig. 2. Topology for wired cum wireless scenario.

Figure 2 shows a wired-cum-wireless topology through which we can exchange packets between a wired and wireless domain through using a base-station. But at any time a mobile node can roam outside the domain of its base-station and be still in a communication link so that it can receive any packets which is destined for it [12]. That is why we have extended the Mobile IP support in this wired-cum-wireless scenario.

Figure 3 shows a wired domain. This domain has 2 wired nodes, named as W0 and W1. In this architecture, We have 2 base-station nodes, Home Agent (HA) and Foreign Agent (FA) respectively. In this architecture, W1 is connected to HA and FA. There is a roaming mobile node called Mobile Node (MN) that moves between the communication range of its home agent (HA) and foreign agents (FA). A TCP flow will be set up between any node (e.g. W0) and MN. According to the architecture, when a MN

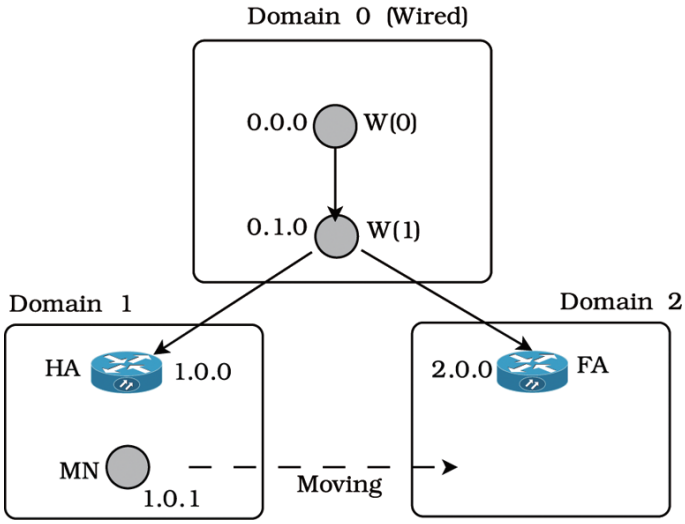

Fig. 3. Topology for Mobile IP simulation.

moves out from the domain of its HA, into the domain of FA, if any packet is sent to the MN during this time interval, the packet will be automatically redirected to the FA by its HA as per definitions of mobile IP.

In the above architecture, we have set up one as wired domain (denoted by 0) and 2 as wireless domains (denoted by 1 and 2 respectively). According to the clustering architecture shown above, the addresses of two wired nodes are 0.0.0 and 0.1.0. The first section of the address represents the domain number, the second section represents the cluster number and the third section is the node number. In the first wireless domain (domain 1) we have a base-station, HA and mobile node MN, in one single cluster. So their addresses are represented as 1.0.0 and 1.0.1 respectively. And for the second wireless domain (domain 2) we have a base-station, FA with an address of 2.0.0. However, when the MN moves into the domain of FA, the packets originating from a wired domain and destined for MN will reach to as per definitions of Mobile IP protocol. The above figure depicts a basic structure of a Mobile IP communication network which may have a huge number of domains. Each domain may contain a different number of clusters and each cluster can contain a different number of nodes.

We present here the following advantages of our proposed hierarchical structure to securing the network.

First, this approach is scalable, because here we are dividing the whole network into several sub-networks and managing and securing them separately.

Second, each domain or cluster can be controlled independently. That means that the security mechanisms in a cluster lying in the more dynamic portion of a large network may not match that of a cluster lying in a comparatively static portion.

Third, the detection of an attacker becomes easier in clustering architecture as it provides localized information. On the other hand, attacker detection is much more complex in a large network with a flat hierarchy.

Fourth, this localized and distributed feature reduces storage, processing and communication overheads, thereby optimizing network bandwidth utilization.

After dividing a large network into a hierarchical structure, we propose three types of filtering techniques. These are:

1. Filtering in the Domain Periphery Router
2. Filtering in the Base-station
3. Queue Monitoring in Base-station Node

Each of these techniques is described in detail below.

4.1. Filtering in the domain periphery router

According to [37], there is an edge or periphery router in each domain, through which each packet within the domain has to pass when going to another domain. In this proposed method, we propose filtering technique in the domain periphery router with a view to filter the malicious packets. Basically, home agents or foreign agents act as the periphery routers in a domain. According to [37], when a mobile node is in a foreign network and wants to register with its home agent via its foreign agent, then the foreign agent would keep track of the addresses associated with that mobile node using a caching mechanism. After registration, when the mobile node wants to attack any node outside its current domain by spoofing the source address, then the domain periphery router will detect and filter that packet as the spoofed address is unknown to itself. When the mobile node tries to attack from its home network, then the home agent will block the packet which contains addresses outside of this network or which is unknown to the home agent. Here we use the concept of egress filtering because egress filtering is used to filter the packets leaving a network [6].

IF packet's source address is within domain's address
THEN forwards the packet
ELSE discard the packet

4.2. Filtering in the base station node

According to our proposal in [37], 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 as described in [37]:

- 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

4.3. Queue monitoring in base station node

This scheme is for preventing Distributed Denial of Service (DDoS) attack. When a node of any domain is under DDoS attack, its corresponding base-station will be overloaded by the attacking packets. Most of the resources of the base-station will be consumed by the attacking packets. As a result, fair

nodes will be barred from services. In this case, we propose to monitor the queue and define its size for setting up in an adaptive manner. More specifically, we consider here the case of sudden increase of tiny packets (like TCP SYN packets) in the queue. It is stated in [38] that a sudden increase of such packets raises the probability of a Denial of Service attack. So, dropping packets in this case would reduce the effect of the attack. In this way we can save the base-station node and its mobile nodes from DDoS attack. Here we use the concept of ingress filtering because ingress filtering is used to filter the packets entering a network.

We propose to regularly measure the queue on the basis of small (near to size of TCP SYN packets) packets at the base-station nodes. Then we set up a predefined level of the queue size. When the queue size of the packets increases to above a predefined level, the queue size will be limited by an adaptive value considering other bigger size packets in the queue. This indicates that we need to filter only the suspicious packets, not any one of the data packets.

As described earlier in [37], the problem with this approach is that some applications use small packets, which may also be dropped during this filtering process. To save these packets, we propose to drop packets in case of a sudden and large increase of small packets in the queue. We argue that the applications that use small packets do not send packets at a very high rate.

5. Simulation and result analysis

Network Simulator 2 [16,20], is used as the simulation tool in this paper. We have created simulation environments and conducted a performance evaluation using the network simulator NS-2 [16,20], as it provides the wide range of features and it has an open source code that can be modified and extended. 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 at any time and should still continue to receive packets which is destined for it. That is why we have implemented the Mobile IP protocol with that wired-cum-wireless scenario. At first we have implemented the DoS attack scenario without protection in this Mobile IP environment. After that, we have simulated the scenario by applying filtering technique in the domain periphery router and in the base station node. Finally, we simulated the queue monitoring in the base-station node as a part of our proposed scheme. Then we compared the performance of the simulation results.

6. Description of the simulations

We have undertaken all the simulations required for this work, dividing this process into four steps:

1. Creating a wired-cum-wireless scenario
2. Running Mobile IP in the wired-cum-wireless topology
3. Implementation of mobile IP communication with Denial of Service attack
4. Implementation of mobile IP communication with proposed technique

All of these steps are described below:

6.1. Creating a wired-cum-wireless scenario

In this section, we have simulated a mixed scenario consisting of a wireless and a wired domain. In this scenario, data is exchanged between the mobile and non-mobile nodes. As we set up a mixed scenario,

so we have 2 wired nodes, W(0) and W(1), connected to our wireless domain consisting of 3 mobile nodes (nodes 0, 1 and 2) via a base-station node, BS. Here, base-station nodes actually act as gateways between wireless and wired domains and allow packets to be exchanged between the two types of nodes. Figure 2 shows the topology for this example.

The DSDV Ad hoc routing protocol is used here. Also, we defined TCP and CBR connections between the wired and wireless nodes. For mixed simulations, here we used hierarchical architecture for routing in order to route packets between wireless and wired domains. The routing information for wired nodes is based on connectivity of the topology. This connectivity information between the nodes is used to generate the forwarding tables in each wired node. Because of the dynamic properties, wireless nodes do not follow the concept of "links". In a wireless topology, packets are routed using their ad hoc routing protocols which can generate a forwarding tables by exchanging routing queries among its neighbors. So in this paper, we use base-stations as gateways between the two domains in order to exchange packets among these wired and wireless nodes. We set up hierarchical topology structure based on different domain and clusters. Next we setup tracing for the simulation for both wired and wireless domains as described in [20].

Next, we created the wired, wireless and base-station nodes. We set up the simulation environment by the help of [20]. Base station should have a different wired routing mechanism for configuring the Routing ON and OFF as it will act as gateway between wired and wireless domains. All other node config options used for the base-station remain the same for mobile node. Also, the BS(0) node is assigned as the base-station node for all the mobile nodes in the wireless domain, so that all packets originating from mobile nodes and destined for outside the wireless domain, will be forwarded by mobile nodes to their assigned base-station. Note that it is important for the base-station node to be in the same domain as the wireless nodes. According to [44], all packets originating from the wired domain, and destined for a wireless node, will reach the base-station which then uses its ad hoc routing protocol to route the packet to its correct destination. Thus, in a mixed simulation involving wired and wireless nodes, it is necessary to:

1. turn on hierarchical routing [20].
2. create separate domains for wired and wireless nodes; there may be multiple wired and wireless domains to simulate multiple networks [20].
3. have one base-station node in every wireless domain, through which the wireless nodes may communicate with nodes outside their domain [20].

Note that traffic flow for mobile nodes is not as yet supported in nam [20]. In trace file, we see traces for both wired domain and wireless domain (preceded by "WL" for wireless). Also note that the node-ids are created internally by the simulator and are assigned in the order of node creation. Actually, here we set up the simulation environment by the help of NS-manual [20].

6.2. Running mobile IP in the wired-cum-wireless topology

We run our simulation by the help of [20]. In the first scenario, we have created a wired-cum-wireless topology and have exchanged 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 for it. In other words, it is necessary to extend mobile IP support in this wired-cum-wireless scenario. For this Mobile IP scenario, we have the same wired domain consisting of 2 wired nodes, W0 and W1. In addition we have 2 base-station nodes named Home Agent (HA) and Foreign Agent (FA) respectively. The wired node W1 is connected to HA and FA as shown in the figure below. There is a

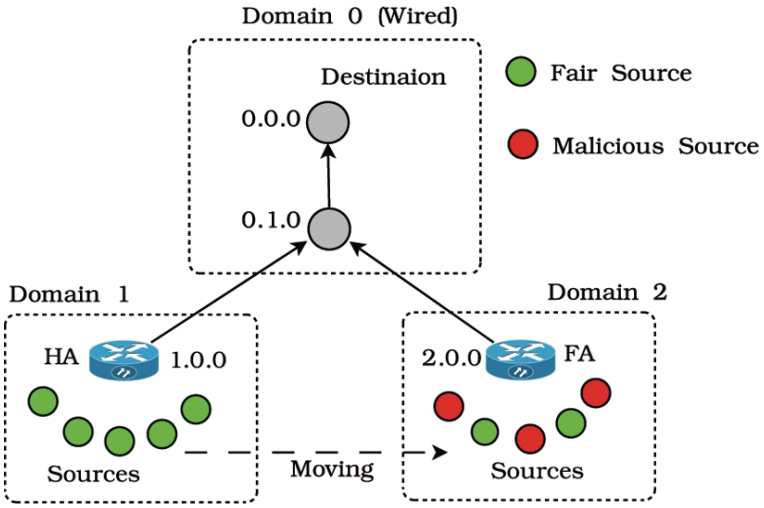

Fig. 4. Simulation of Mobile IP with DoS attack.

roaming mobile node called Mobile Node (MN) that moves between its home agent and foreign agents. We set up a TCP flow between W0 and MN. As MN moves out from the domain of it's HA, into the domain of FA, the packets destined for MN is redirected by its HA to the FA as per mobile IP protocol definitions. In the Fig. 4 the topology described above is shown.

In this topology, we have one wired domain (denoted by 0) and 2 wireless domains (denoted by 1 and 2 respectively). The wired node addresses remain the same, 0.0.0 and 0.1.0. In the first wireless domain (domain 1) we have base-station, HA and mobile node MN, 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, in the simulation, the MN will move into the domain of FA and the packets originating from a wired domain and destined for MN will reach it as a result of the Mobile IP protocol. Wired nodes will be created as done earlier. However, in place of a single base station node, a HA and FA will be created. Note here that in order to turn on the mobile IP flag, we have configured the node structure accordingly using option mobile IP ON.

Next, we have created the Mobile Node (MN) as follows. We have to turn off the option wired Routing (used for creation of base-station nodes) before creating mobile nodes. Also, the HA is set up as the home-agent for the Mobile Node. The MN has an address called the care-of-address (COA). Based on the registration/beacons exchanged between the MN and the base-station node (of the domain the MN is currently in), the base-station's address is assigned as the MN's COA. Thus in this simulation, the address of the HA is assigned initially as the COA of MN. As MN moves into the domain of FA, its COA changes to that of the FA. We can see from the nam output that, initially the TCP packets are handed down to MN directly by its HA. As MN moves away from HA domain into the domain of the FA, we find the packets destined for MN, being encapsulated and forwarded to the FA which then decapsulates the packet and hands it over to the MN.

6.3. Implementation of mobile IP communication with denial of service attack

Scenario-1: Simulation of Mobile IP with DoS attack

In this scenario as shown in Fig. 4, 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

Table 2
Simulation parameters for scenario 1

Parameters	Values/Ranges
Speed of mobile nodes	20 m/s
Packet size	1000 Bytes
Transport agent	TCP
Application	FTP
Number of nodes (max)	100
Number of domains	4–5
Number of clusters	5–10
Simulation time	60s

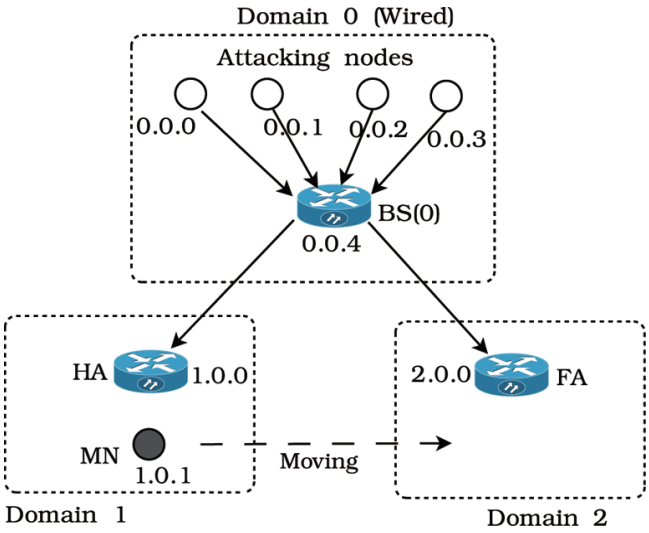

Fig. 5. Simulation of Mobile IP with DDoS attack.

(FA) are two base-station nodes in two other different domains. There are five roaming mobile nodes 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 are redirected by its HA to the FA as per mobile IP protocol definitions.

When the five sources 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 of address 0.0.0.

The parameters used to implement this scenario are given in Table 2 below:

Scenario-2: Simulation of Mobile IP with DDoS attack

For the second attack scenario (DDoS attack) we have modified Domain 0 of the topology described above slightly. The modified topology is shown in Fig. 5.

Figure 5, wired nodes connected to BS (0) simultaneously send packets to the Mobile Node (MN) of domain 1. All these packets go to the MN through the base-station (HA) of domain 1. All these packets simultaneously overflow the queue of HA. Hence, the 4 nodes act as malicious nodes and try to consume network resources of the base station node (HA). So they are interrupting normal communications

Table 3
Simulation parameters for scenario 2

Parameters	Values/Ranges
Packet size	40Bytes
Transport agent	TCP
Application	CBR
Number of domains	3
Number of clusters	4
Simulation time	60s

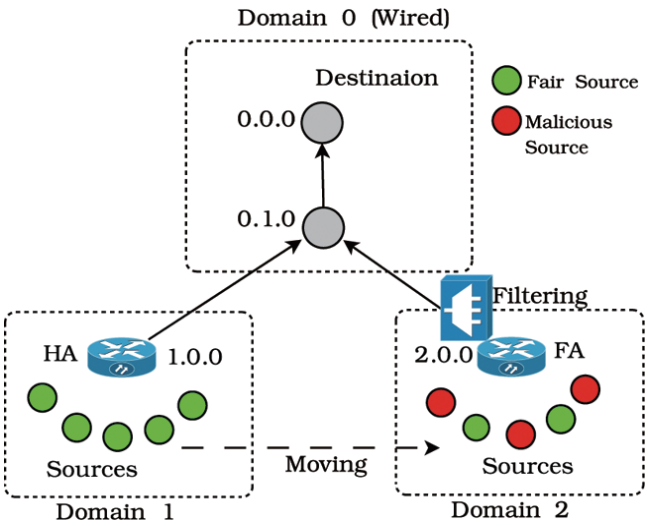

Fig. 6. Simulation with filtering in the domain periphery router.

through the base station node (HA). When fair nodes try to communicate with the base-station node HA or with the mobile node (MN), they cannot access services because of the attack on the base station

The parameters used for the simulation of this scenario are given in Table 3.

6.4. Implementation of Mobile IP communication with proposed technique

To protect against Denial of Service attack we have implemented a packet filtering technique in two vulnerable positions of the Mobile IP communication network, first in the domain periphery router and then in the base station node of the mobile node which is the receiver of the packets.

6.4.1. Filtering in the Domain periphery router

According to our proposed solution, we cache the addresses of each node at base-station (FA) and when they start using spoofed IP addresses, those packets from unknown sources to the base-station (FA) are dropped as shown in Fig. 6. Although this mechanism consumes some memory of the base station, it can significantly reduce the chance of DoS attack at a very early stage.

The parameters used to implement this scenario are given in Table 4.

6.4.2. Filtering in Base-station node

In this proposal we consider the case, 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

Table 4
Simulation parameters for filtering in domain periphery router

Parameters	Values/Ranges
Speed of mobile nodes	20 m/s
Packet size	1000 Bytes
Transport agent	TCP
Application	FTP
Number of nodes (max)	100
Number of domains	4–5
Number of clusters	5–10
Simulation Time	60s

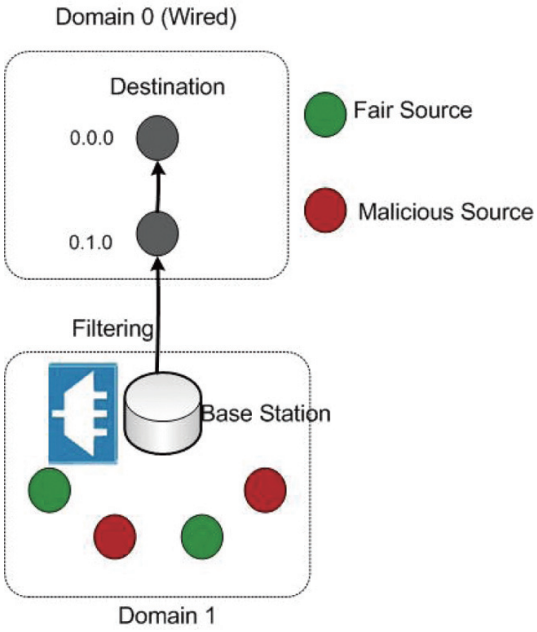

Fig. 7. Filtering in the base station node.

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 which will pass through the base station in the network as shown in Fig. 7.

The parameters used for the simulation of this scenario are given in Table 5 below:

6.4.3. Filtering in the base-station node by monitoring the queue

As stated earlier, filtering in the queue of an appropriate node can significantly reduce the effect of DoS attack. For example, in the case of a TCP SYN flooding attack, many attacking nodes start from the three way handshaking phase, but do not complete the phase. The size of the packets in the handshaking phase is very small. However, when many malicious nodes start a TCP SYN flooding attack on a mobile node, the base-station of that node observes a sudden increase of TCP SYN packets in its queue.

Table 5
Simulation parameters for filtering in base station node

Parameters	Values/Ranges
Simulation area	900 × 900 m
Speed (m/s)	1 m/s to 20 m/s
Packet rate	5 packets/ s
Packet size	128 Bytes
Traffic source	CBR
Pause time	60s
Routing protocols	DSDV and Mobile Ip
Number of nodes	80–100
Number of domains	2–3
Number of clusters	3–4
Transmission range	400 m
Simulation time	250 s

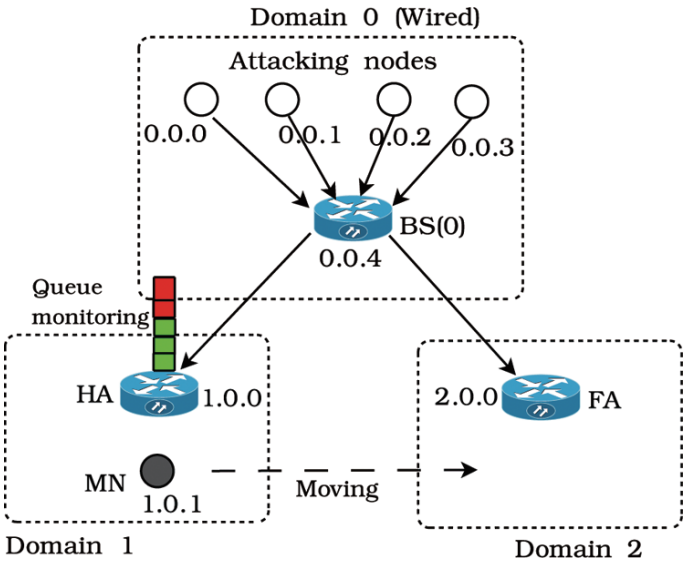

Fig. 8. Monitoring queue in the base station node.

In this scenario, four malicious nodes begin simultaneously attacking a mobile node under the base-station which is its home agent.

Figure 8 shows the simulation scenario of monitoring the queue in the mobile host's base station. According to our proposition, we filter the queue in the base-station by limiting the queue size to four and observe the queue status. In this simulation, we could drop 63 TCP SYN packets and thus the effect of the attack is reduced at the base-station node. It is obvious that this type of queue filtering can also be applied to the foreign agent. Hence, it is also possible to prevent the attack while the target node is moving from his home agent to the foreign agent.

The parameters used for the simulation of this scenario are given in Table 6 below:

Here we have used constant bit rate (CBR) applications to simulate a TCP SYN flooding attack where packet size is 40 bytes. In ns2, there are many parameters to express the status of a queue such as queue size in bytes, queue size in number of packets, the entrance and departure of packets etc. Here, we measured the queue of the base-station by number of packets.

Table 6
Simulation parameters for queue monitoring in the base station node

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

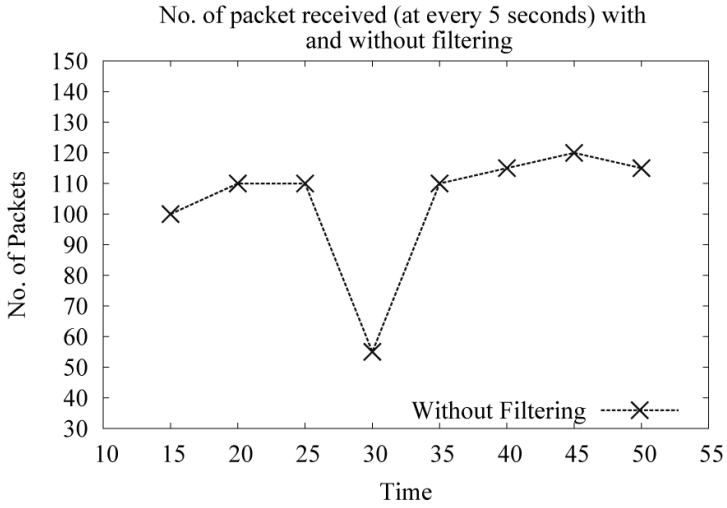

Fig. 9. Without applying the filtering technique.

6.5. Experimental result analysis

We make the following assumptions for the simplicity of simulation:

6.5.1. Comparison for filtering in the domain periphery router:

Figure 9 shows the resulting graph after simulating the Mobile IP communication without applying our proposed filtering technique in the domain periphery router. Implementation of this scenario is described in scenario-1 of section 3.1. From this graph we see the number of packets leaving the periphery router (FA) of domain 2. In this figure, there is a great fall in the curve at the time 25–35. When the Mobile Node (MN) moves away from its home agent, it loses its previous registration with the home agent. Before registering with the foreign agent, for an amount of time it deserves no registration at all. At this time, all the packets destined for the mobile node are dropped. For this reason, there is a great decline in the graph.

Figure 10 shows the resulting graph after simulating the Mobile IP communication by applying our proposed filtering technique in the domain periphery router. Implementation of this scenario is described in step 1 of section 5.3. We applied packet filtering in the base-station (FA) of the domain. The mobile nodes come to the foreign network and are registered with the base-station (FA). After that, some malicious packets are dropped by the periphery router (FA) of domain 2. From the graph, we can see that after registration with a foreign agent, the number of outgoing packets is less compared to that of the previous graph.

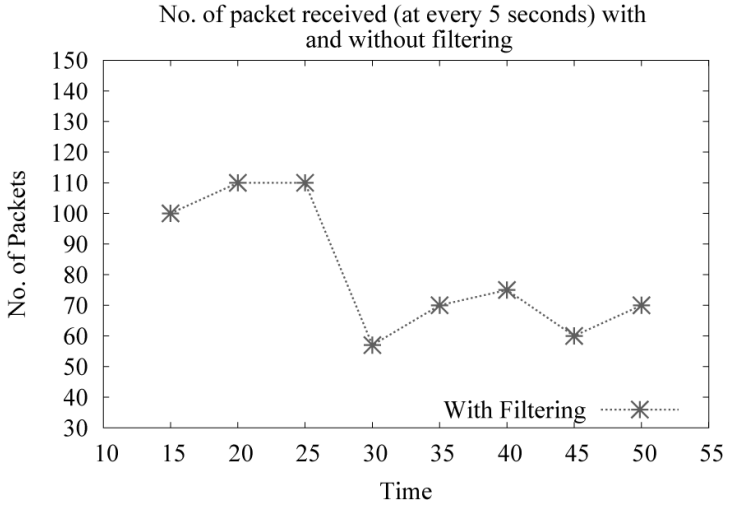

Fig. 10. With applying the filtering technique.

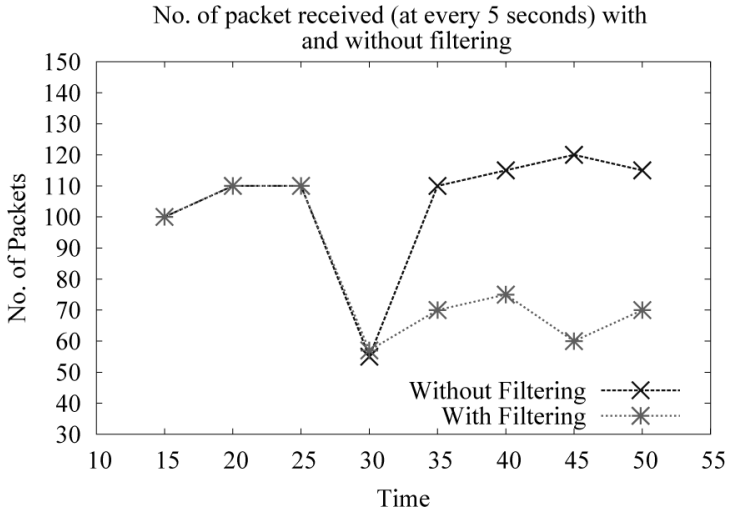

Fig. 11. Comparison of packet passing, with and without filtering technique applied.

A comparison of the above two graphs, that is with and without applying the filtering technique, is shown in Fig. 11.

Here we observe that, after the filtering technique was applied, the number of packets passed is reduced significantly. This is because the packets sent by the nodes 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 in the number of attacking nodes.

6.5.2. Comparison for filtering in the base station node

In our simulation the home agent router of the domain 1 is considered as the base station node and the mobile node connected to this base station is under attack.

Figure 12 shows that our system will exhibit better performance for malicious node detection rate if

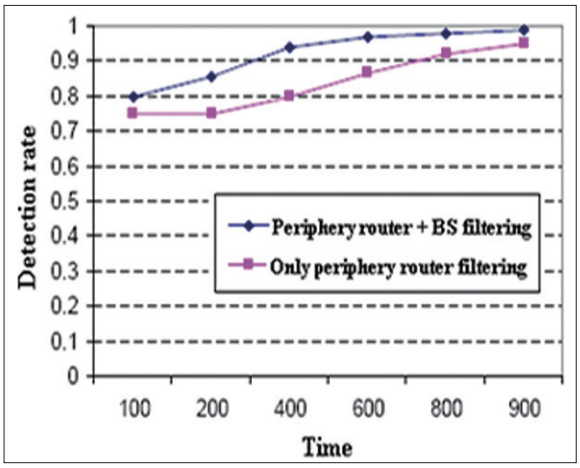

Fig. 12. Time Vs detection rate.

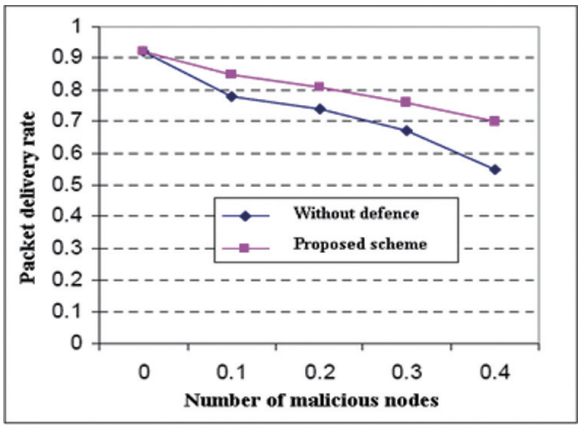

Fig. 13. Packet delivery Vs malicious nodes.

we use base station filtering and the periphery router filtering rather than using only periphery router filtering.

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. Figure 13 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 14 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.

Figure 15 shows the comparison between our proposed scheme and scheme without defense. Here the output shows the detection rate, packet delivery rate and overhead. This figure shows the summary of our proposed scheme. From this figure, we get that if we apply both periphery router and base station filtering, the detection rate increases than the only periphery filtering scheme. Our proposed scheme shows better packet delivery against malicious nodes and low communication overhead which is desirable.

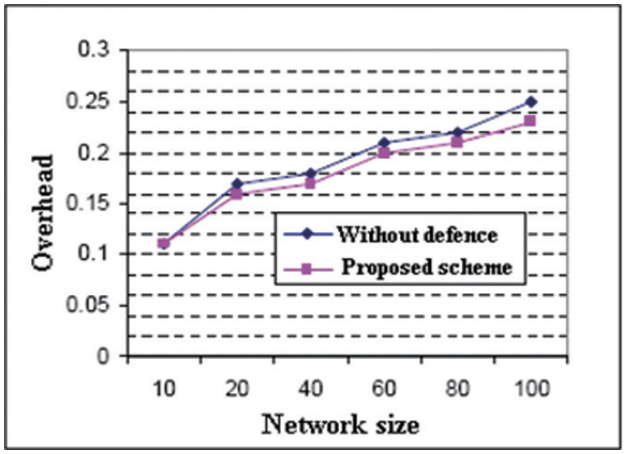

Fig. 14. Network size Vs overhead.

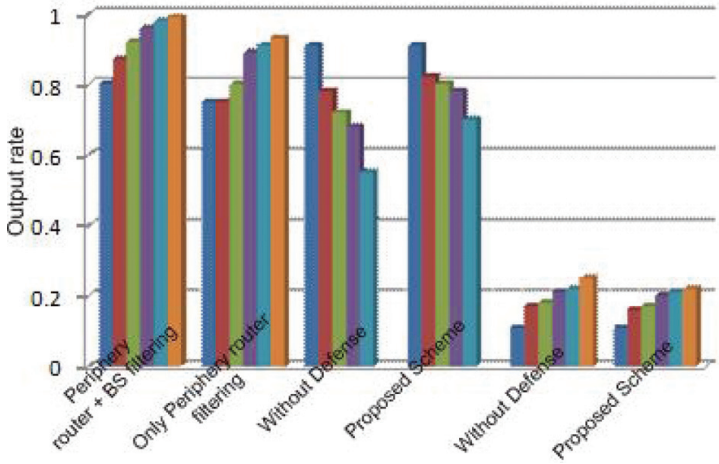

Fig. 15. Without defense vs. proposed scheme.

6.5.3. Comparison for queue monitoring in the base station node

In this section we show that queue status of base station while being monitored and while being attacked.

Figure 16, we observe that, some high fluctuations in queue size (measured in terms of number of packets). The peak values indicate the sudden presence of huge number of small packets which is a sign of DDoS attack. The peak values rose to almost 15 in this figure.

Figure 17 is the resulting graph after applying our proposed queue monitoring technique in the base station node. In this simulation the queue of the home agent router of domain 1 is monitored because it is attacked as a victim by the attackers.

Here we observe the queue status of the base-station node 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 used for DDoS attack here. In this simulation, we found by analyzing the trace file of the simulation, that 63 malicious packets are dropped after using this filtering technique.

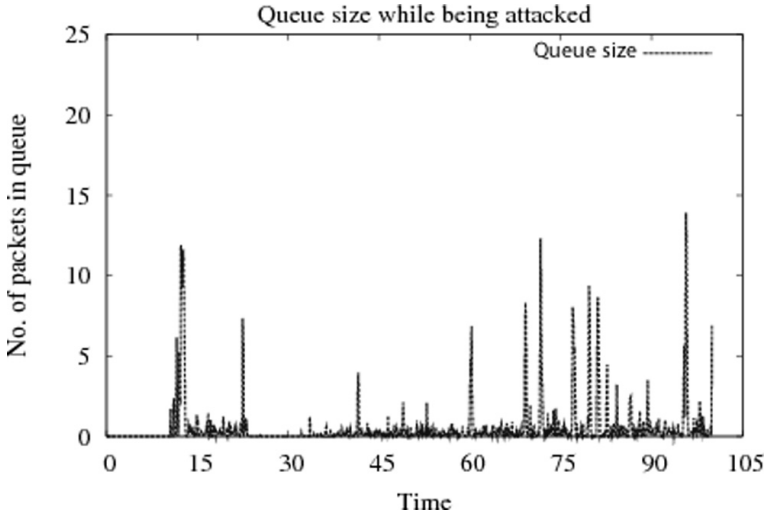

Fig. 16. Queue status of base station while being attacked.

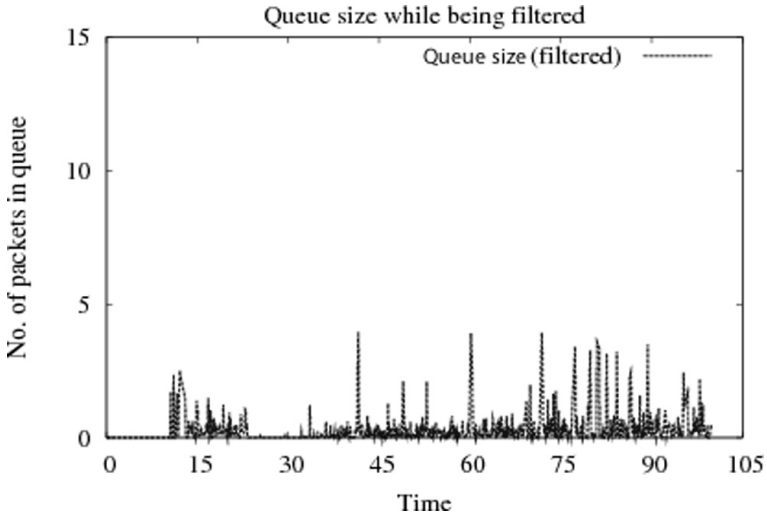

Fig. 17. Queue status at base station while being filtered.

6.5.4. Comparison with other schemes

In this section, we compare our proposed schemes with others. Analysis and comparisons are made among the approaches that belong to an identical technique category which ensures security by mitigating DoS attack in Mobile IP communication. Zao et al. [50] proposed a public-key based security schemes for mobile IP but this scheme increases communication overhead like all other conventional PKI techniques whereas we showed our proposed scheme is low in communication overhead. Park et al. [36] proposed route-based packet filtering technique for preventing DDoS attack but this approach is suitable only for internet based system whereas our scheme is suitable for all mobile IP systems. Ferguson et al. [17] proposed ingress filtering technique but this approach only works for Internet Service Providers and for internet based community whereas our approach works for all mobile IP based communication. Like other scheme, our proposed scheme has some shortcomings as our scheme only works for cluster-based

Table 7
Comparison between our scheme and other schemes

Proposed schemes	Techniques	Shortcomings
Public key based secure mobile Ip [50]	Public key management techniques	Like all other conventional PKI techniques, it increases communication overhead
Route based filtering approach [36]	Route based distributed packet filtering technique	This approach is only suitable for internet based system
Ingress filtering to [10] mitigate DoS attack	Ingress filtering techniques	This approach works for Internet Service Providers and for internet based community
Our proposed schemes	Filtering and queue monitoring techniques at base station	It only works for clustering architecture

architecture. A comprehensive comparison between our scheme and other's schemes are shown in Table 7.

7. Conclusion and future works

Denial of Service attack in mobile IP communication is considered to be one of the most severe attacks. The detection and prevention of this attack is more difficult in cases of mobile IP communications than in their wired counterparts. In this paper, we proposed a technique for detecting and preventing DoS attacks in mobile IP communication. We propose to use packet filtering techniques that work in different domains and base stations of mobile IP communication to detect suspicious packets and to improve the performance. If any packet contains a spoofed IP address which is created by DoS attackers, our scheme can detect this and then filter the suspected packet. The proposed system can mitigate the effect of Denial of Service (DoS) attack by applying three methods which are elaborately described in this work: (i) by filtering in the domain periphery router (ii) by filtering in the base station and (iii) by queue monitoring at the vulnerable points of base-station node. We proposed to apply a packet filtering technique at the vulnerable points of the Mobile IP network. We used the network simulator NS-2 for simulating and evaluating the performance of our proposed system. We observed that the performance of our proposed system is better than the system without any protection. We also observed that our proposed technique can significantly reduce the effect of DoS and DDoS attacks.

References

[1] C. Barros, A proposal for ICMP traceback messages. Internet Draft http://www.research.att.com/lists/ietfitrace/2000/09/msg00044.html, Sept. 18, 2000.
[2] S.M. Bellovin, M. Leech and T. Taylor, ICMP traceback messages. Obsolete Internet draft, February 2003.
[3] H. Burch and B. Cheswick, Tracing anonymous packets to their approximate source, *Proceedings of the 14th USENIX conference on System administration*, 2000.
[4] T. Braun and M. Danzeisen, Secure mobile IP communication, *In Conference on Local Computer Networks* (2001), 586–593.
[5] T. Braun and M. Danzeisen, Access to Mobile IP Users to Firewall Protected VPNs, *Proceedings of Workshop on Wireless Local Networks at the 26th Annual IEEE Conference on Local Computer Networks*, 2001.
[6] C. Brenton, What is Egress Filtering and How can I Implement it?. Published by the SANS Institute, June 13, 2011.
[7] H.B. Chang, H.J. Kwon and J.G. Kang, The design and implementation of tamper resistance for mobile game service, *Mobile Information System* **6**(1) (2010), 85–105.
[8] C.L. Chen, Design of a secure RFID authentication scheme preceding market transactions, *Mobile Information Systems* **7**(3) (2011), 201–216.

[9] Y.F. Ciou, F.Y. Leu, Y.L. Huang and K. Yim, A handover security mechanism employing the Diffie-Hellman key exchange approach for the IEEE802.16e wireless networks, *Mobile Information Systems* **7**(3) (2011), 241–269.
[10] L. Dang, W. Kou, H. Li, J.Z hang, X. Cao, B. Zhao and K. Fan, Efficient ID-based registration protocol featured with user anonymity in mobile IP networks, *IEEE Transactions on Wireless Communications* **9**(2) (2010), 594–604.
[11] T. Delot, S. Ilarri, N. Cenerario and T. Hien, Event Sharing in Vehicular Networks Using Geographic Vectors and Maps, *Mobile Information Systems* **7**(1) (2011), 21–44.
[12] 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* **3**(4) (2005), 1–9.
[13] R.H. Deng, J. Zhou and F. Bao, Defending against redirect attacks in mobile IP, *Proceedings of the 9th ACM Conference on Computer and Communications Security* (2002), 59–67.
[14] I. Doh, J. Lim and K. Chae, Distributed authentication mechanism for secure channel establishment in ubiquitous medical sensor networks, *Mobile Information Systems* **7**(3) (2011), 189–200.
[15] A. Durresi, M. Durresi and B. Barolli, Secure authentication in heterogeneous wireless networks, *Journal of Mobile Information Systems* **4**(2) (2008), 119–130.
[16] K. Fall and K. Vardhan, ns notes and documentation, available from http://www-mash.cs.berkeley.edu/ns/, 1999.
[17] P. Ferguson and D. Senie, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2827, BCP 38, 2000.
[18] H.L. Flanagan and G.P.A. Version, Egress filtering-keeping the Internet safe from your systems. April 30, 2001. Available at SANS Institute. http://rr.sans.org/sysadmin/egress.php.
[19] P. Fulop, S. Imre, S. Szabo and T. Szalka, Accurate mobility modeling and location prediction based on pattern analysis of handover series in mobile networks, *Journal of Mobile Information Systems* **5**(3) (2009), 255–289.
[20] M. Greis, Tutorial for the Network Simulator NS, available online (11.08.2004), http://www.isi.edu/nsnam/ns/tutorial.
[21] V. Gupta, S. Krishnamurthy and M. Faloutsos, Denial of service attacks at the MAC layer in wireless ad hoc networks, *Proceedings of IEEE MILCOM Conference* (2002), 1118–1123.
[22] V. Gupta and G. Montenegro, Secure and mobile networking, *Journal of Mobile Networks and Applications – Special issue: mobile networking in the Internet* **3**(4) (1998), 381–390.
[23] A. Habib, M. Hefeeda and B. Bhargava, Detecting service violations and DoS attacks, *Proceedings of Internet Society Symposium on Network and Distributed System Security*, 2003.
[24] A.A. Hamidian, A study of internet connectivity for mobile ad hoc networks in ns-2, *Published by Department of Communication Systems, Lund Institute of Technology, Lund University*, 2003.
[25] L.T. Heberlein and M. Bishop, Attack class: Address spoofing, *Proceedings of the 19th National Information Systems Security Conference* (1996), 371–377.
[26] A. Inoue, M. Ishiyama, A. Fukumoto and T. Okamoto, Secure mobile IP using IP security primitives, *Proceedings Sixth IEEE workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises* (1997), 235–241.
[27] R. Islam, Enhanced security in Mobile IP communication, *PhD thesis, Stockholm University*, 2005.
[28] C. Jin, H. Wang and K.G. Shin, Hop-count filtering: an effective defense against spoofed DDoS traffic, *Proceedings of the 10th ACM Conference on Computer and Communications Security* (2003), 30–41.
[29] H. Kim and J.H. Lee, Diffie-Hellman key based authentication in proxy mobile IPv6, *Journal of Mobile Information Systems* **6**(1) (2010), 107–121.
[30] P. Lin, S.M. Cheng and W. Liao, Modeling Key Caching for Mobile IP Authentication, Authorization, and Accounting (AAA) Services, *IEEE Transactions on Vehicular Technology* **58**(7) (2009), 3596–3608.
[31] L. Liu, A Client-Transparent Approach to Defend Against Denial of Service Attacks, *Proceedings of 25th IEEE Symposium on Reliable Distributed Systems* (*SRDS 06*), 2006.
[32] G. Montenegro, Reverse tunneling for Mobile IP, revised. 2001.
[33] P. Nikander, J. Arkko, T. Aura, G. Montenegro and E. Nordmark, Mobile IP version 6 (MIPv6) route optimization security design, *Proceedings OF THE IEEE Vehicular Technology Conference* (2003), 2004–2008.
[34] P. Owezarski, On the impact of DoS attacks on Internet traffic characteristics and QoS, 14th International Conference on Computer Communications and Networks, ICCCN 2005, 17–19 Oct. 2005, pp. 269–274.
[35] F. Palmieri, U. Fiore and A. Castiglione, Automatic security assessment for next generation wireless mobile networks, *Mobile Information Systems* **7**(3) (2011), 217–239.
[36] K. Park and H. Lee, A proactive approach to distributed DoS attack prevention using route-based packet filtering, *Proceedings of ACM SIGCOMM Conference*, 2001.
[37] S. Parvin, S. Ali, S. Han and T. Dillon, Security against DOS attack in mobile IP communication, *Proceedings of the 2nd International Conference on Security of Information and Networks* (2010), 152–157.
[38] S. Parvin, S. Ali, J. Singh, H. Hussain and S. Han, Towards DoS Attack Prevention based on Clustering Architecture in Mobile IP Communication, *Proceedings of IEEE IECON* (2009), 3183–3188.
[39] C.E. Perkins and D.B. Johnson, Route optimization for mobile IP, *Cluster Computing* **1**(2) (1998), 161–176.
[40] C.E. Perkins, Mobile IP: Design Principles and Practices, *Addison-Wesley*, 1997.

[41] N.N. Qadri, M. Altaf, M. Fleury and M. Ghanbari, Robust video communication over an urban VANET, *Mobile Information Systems* **6**(3) (2010), 259–280.
[42] B.M. Reshmi and S.S. Manvi, Bhagyavati. An agent based intrusion detection model for mobile ad hoc networks, *Journal of Mobile Information Systems* **2**(4) (2006), 169–191.
[43] Security aspects of Mobile IP. SANS Institute 2001, as part of the information security reading room.
[44] D. Strom and S.R. Room, The Packet Filter: A Basic Network Security Tool. September 2000, Available at http://www.giac.org/paper/gsec/131/packet-filter-basic-network-security-tool/100197.
[45] G. Tuquerres, M.R. Salvador and R. Sprenkels, Mobile IP: security and application, *Telematics Systems and Services*, 1999.
[46] C.H. Wu, A.T. Cheng, S.T. Lee, J.M. Ho and D.T. Lee, Bi-directional route optimization in mobile IP over wireless LAN, *Proceedings of IEEE 56th Vehicular Technology Conference*, 2002.
[47] Y. Xiang and W. Zhou, A defense system against DDOS attacks by largescale IP traceback, *Proceedings of third International Conference on Information Technology and Applications*, 2005.
[48] X. Yang, D. Wetherall and T. Anderson, A DoS-limiting network architecture, *Proceedings of the 2005 conference on Applications, Technologies, Architectures, and Protocols for Computer Communications* **35**(4) (2005), 241–252.
[49] I. You, J.H. Lee, Y. Hori and K. Sakurai, Enhancing MISP with Fast Mobile IPv6 Security, *Mobile Information Systems* **7**(3) (2011), 271–283.
[50] J. Zao, S. Kent, J. Gahm, G. Troxel, M. Condell, P. Helinek, N. Yuan and I. Castineyra, A public-key based secure Mobile IP, *Journal of Wireless Networks* **5**(5) (1999), 373–390.
[51] J.K. Zao and M. Condell, Use of IPSec in mobile IP. 1997, 381–390.

Sazia Parvin received her MS degree in Computer Engineering from Korea Aerospace University in 2008. Presently she is a PhD student at Digital Ecosystems and Business Intelligence Institute, Curtin University, Australia. Her research interests include security in wireless communications and networking. She is a lecturer at Department of Computer Science and Engineering in Dhaka University, Dhaka, Bangladesh.

Farookh Khadeer Hussain received the Bachelor of Technology degree in computer science and computer engineering; the M.S. degree in Information Yechnology from the La Trobe University, Melbourne, Australia; and the Ph.D. degree in Information Systems from Curtin University of Technology, Perth, Australia, in 2006. He is currently a Research Fellow with the Digital Ecosystems and Business Intelligence Institute (DEBII), Curtin University, Perth, Australia. His areas of active research are trust, reputation, trust ontologies, data modeling of public and private trust data, semantic web technologies and industrial informatics. He works actively in the domain of making informed business decisions (business intelligence) through the use of trust and reputation technology. He is interested in the application of trust and reputation as a technology, as a business analysis and intelligence tool, and the applications of trust and reputation to various domains.

Sohrab Ali received his Bachelor and MS degree from Computer Science and Engineering department in Dhaka University. Presently he serving as a lecturer in People's University in Dhaka, Bangladesh. His research interests include security in wireless communications and networking.