ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 1, No.7 , January 2014
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Mobile IP Issues and Their Potential Solutions: An Overview

Aatifah Noureen[1], Zunaira Ilyas[1],Iram Shahzadi[1], Muddesar Iqbal[1], Muhammad Shafiq[2], Azeem Irshad[3]

[1]Faculty of Computing and Information Technology
University of Gujrat,Gujrat, Pakistan

[2]Department of Information and Communication Engineering
Yeungnam University, Gyeongsan, South Korea

[3]Department of computer science and software engineering
International Islamic University, Islamabad, Pakistan

{atifanoureen, zunaira.ilyas,}@gmail.com,
iramshahzadi013@yahoo.com
m.iqbal@uog.edu.pk,shafiq.pu@gmail.com
irshadazeem2@gmail.com@gmail.com

Abstract

A typical Internet protocol (IP)could not address the mobility of nodes and was only designed for fixed networks where the nodes were improbable to move from one location to other. An ever-increasing dependence on network computation makes the use of portable and handy devices,inevitable. Mobile IP protocol architecture was developed tomeet such needs and support mobility. Mobile IPlets the roving nodes to establish an uninterrupted connection towards internet without altering the IP address whilemoving to another network.However, Mobile IP goes through several issues like ingress filtering, triangle routing, handoff and Quality of service problems etc. In this paper we discuss few of those with their possible solutions. That resolves these problems, reduce the unnecessary load from the network and enhance the efficiency. Some security threats on mobile and their solutions are also focused to secure the communicationduring mobility.

Keywords: *Mobile IP, Triangle routing, Ingress filtering, binding updates and COA.*

1. Introduction

1.1 Mobile Internet Protocol (Mobile IP)

In standard IP routing, a problem occurs when a mobile node roams through multiple access points.It has to reinstate the connection each time with changing in its IP address due to which the lively session of the nodes was dropped and response time of the network is increased [1]. A novel technology which satisfies the requirement for smooth connection is Mobile IP; a mobility support open standard Protocol suggested by the Internet Engineering Task Force (IETF) in November 1996. That makes it possible for the moving nodes to maintain an un-interrupted connection towards internet without altering the IP address while shifting to another network [2]. The primary reasons that persuading the need of Mobile IP; making available a scalable, translucent as well as a safe alternative [3]. In Mobile IP a host node possesses two addresses at a time, one for the home network; permanent address and other for the foreign network which is short-lived and just legitimate at a particular foreign network [4]. Every roving node is recognized through its home address irrespective of its present location over the internet. When the node is far away to home network it owed a care-of address to determine its existing location [5].

1.2 Functional components of mobile IP:

The integral componentsbelong to the mobile architecture are as follow:

- Mobile Node (MN)
- Home Agent (HA)
- Foreign Agent (FA)
- Correspondent Node (CN)
- Home Agent Address
- Care-of-Address (CoA)
- Home Network
- Foreign Network
- Tunneling

These architectural components are conferred below:

Mobile Node (MN): Any device which software facilitates network roaming. A node using the Mobile IP that moves in different IP subnets. A permanent (home address) IP address is allotted to this node which defines the destination of all its packets. Other nodes use only home IP address to send packets, regardless of node's physical location.

Home Agent (HA): A router within home network that delivers packets to the Mobile Node and in charge to intercept packets whenever the mobile node is connected to an overseas network. The home agent is liable for sending these packets to the mobile node.

Foreign Agent (FA): A router in foreign network to which mobile node is connected. A foreign network router designed to use for Mobile IP. A mobile node having a 'foreign agent care-of address' all packets are passed on through this node. The mobile node possibly uses a foreign agent for registration in the distant network. [6]

Correspondent Node (CN): Any host with which mobile node communicates. It is a communicating host with the mobile node. This can be placed on the foreign network, home network, or any other place holding potential to send packets to the mobile node's home network.

Home Agent Address: IP address of the device within its home network.

Care-of-Address (CoA): IP address of the device when it is working in a foreign network. The address used by mobile node for communication purpose while it is not away from home network. When the mobile node is using foreign agent's IP address as its care-of address it is named as foreign agent care-of address, and a collocated care-of address is used when network interface of the mobile node is provisionally allocated an IP number on the foreign network [7].

Home Network: The subnet which communicates to the home address of the mobile node and the home agent. It is sighted as the "home" spot of connection for mobile node.

Foreign network: The network in which the Mobile Node is currently existent, away from its Home network.

Tunneling: The encapsulating process foran IP packet in a further IP packet to route it at a place other than the one defined in the destination field originally. Prior to promoting it to a suitable router, when a packet is accepted by home agent, it encapsulatesthat packet into a new packet, setting the mobile node's care-of address in the new target/destination address field. The path that is pursued by the new packet is known as the tunnel. [5]

1.3 Architecture:

In Figure 1 exemplifies the simple architecture of mobile IP scenario.

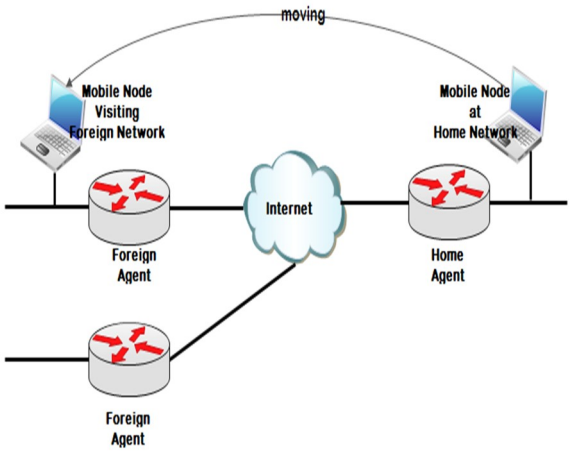

Figure 1: Architecture of Mobile IP

1.4 How mobile IP Works

Whenever a mobile node goes far away from its home network it listens for advertisement by FAandtake care-of-address via a foreign agent then the mobile node records its existing position with the Foreign Agent and Home Agent (***Agent Discovery and Registration***). Packets are delivered to the home address of the mobile node are resented by the home agent over the tunnel towards the care of address in the foreign agent (***Encapsulation***). Then the foreign agent passes the packets to the mobile node on its home address (***De-capsulation***). Every time a node shifts to a network it needs to obtain a new care-of address. A mobility agent at home network preserves ***mobility binding table*** where as a foreign agent sustains the ***visitor list.*** [1, 8]

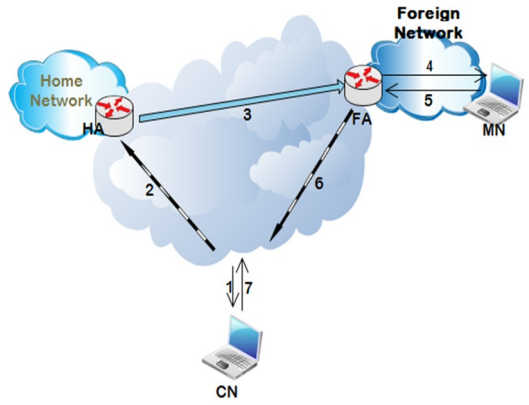

Figure 2: Working of Mobile IP

2. Issues in mobile IP:

These are the transitional issues of mobile IPv4 to Mobile IP v6:

- Ingress Filtering
- Intra-Domain Movement Problem
- Triangular Routing Problems
- Handoff Problem
- Quality of Service Problem
- Fragility problem

2.1 Ingress Filtering problem

Ingress Filtering [9] is an approach carried out by the firewall enabled systems to ensure that the particular packets are truly from the network that they are declaring, if the IP address is not same as the network these packets are discarded. If the mobile node transmits packets using a Home Address rather than Temporary Care of Address when it is in foreign network then packets are declined by the program which supports Ingress Filtering.This problem occurs when both nodes (sender and receiver) belongs to same home network [10]. The whole process is shown in Figure 3.

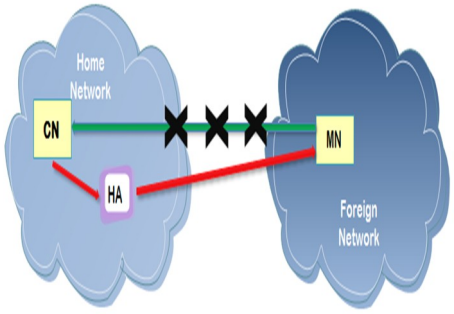

Figure 3: Ingress filtering

2.2 Triangle routing problem

Another aspect [11] is that when mobile node is in foreign network the corresponding node is not aware of its care of address, it transmits a packet to the home address of the mobile node which sends it to the foreign agent which further delivers it to the mobile node, on the other side the mobile node communicates directly with the corresponding node.

Packets are usually sent efficiently both to and from the mobile node but when corresponding node sends packet towards mobile node they have to follow a longer route as compared to optimum. Since the both transmission directions have used distinct paths, creates ***"triangle routing"*** problem which decreases network efficiency and places an unwanted load on the networks [4, 1, 6]. However Figure 4 illustrates triangle routing problem scenario in more simple fashion.

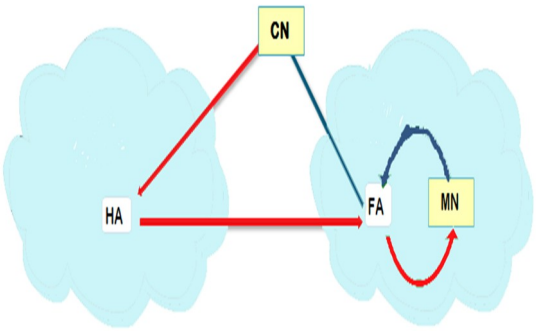

Figure 4: Triangle Routing

2.3 Handoff Problem

Handoff problem occurswhen mobile node switches from its current foreign agent to another[12]. Since, home agent is not aware of the change of the position of the mobile node so it tunnels packets to its old foreign agent till it receives the news registration request from the mobile node. Thus packets are lost during the hand off and as a result communication between corresponding node and mobile node does not occur successfully [13].

2.4 Intra-Domain Movement Problem

When mobile node changes its position frequently within a domain and hand off occurs again and again, a large number of messages are created in network which decreases the effectiveness of the network [14].

2.5 Quality of service Problem

As mobility is the vital ability of telecom wires networks, besides this phenomenon some other management issues are also led to be address, sinceYong Fenghighlighted themas,due to mobility, unpredictable bandwidth, inadequate network resources and increasing error rate it is tough to offer QoS in mobile environment [15].

2.6 Fragility problem

It is simple and easy to configure a single home agent but it has also a drawback of fragility. As if the home agent stops working the mobile node also come to be unapproachable [16].

3. ViableSolutions

The most possible solutions of given problems,so far proposed by the experts, discussed for single glance overview, are as follow:

3.1 Solution of Ingress FilteringProblem

For Mobile IP, ingress filtering triggers/creates massive problems.Ingress filtering limitations may be improved through an approach named as ***reverse tunneling***. In Reverse Tunneling foreign agent receives packet from the mobile node encapsulate it and transmit it towards home agent, then the home agent de-capsulate it and further send it to the corresponding node. [10]In this manner now we have always topologically **truthful** addresses however it probably raises the delay, congestion of the packets [5].Figure 5 illustrates the whole process of reverse tunneling.

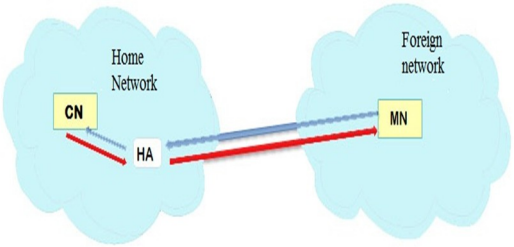

Figure 5: Reverse Tunneling

Reverse tunneling enables the reception of packets on home network is free from firewall blockage but it negatively affects the efficiency and safety of the mobile IP because of inside subnets direct link[17].

3.2 Solutions of Triangle Routingproblem

To tackle the triangle routing problem, many protocols are planned like forward tunneling and binding cache, bidirectional route optimization, the smooth handoff technique, a virtual home agent and SAIL.

3.2.1 Route optimization

Charles Perkins and David Jhosan presented this protocol in 2000 and it is used in IP Version 6. Route optimization mobile IP work as it tells the new care of address to corresponding Nodes. Nevertheless the communication would be much more reliable if correspondent node is aware of care of address of the mobile node and directly sends the packets directly to the mobile node at current location without detouring by the home network [6, 2].Correspondent node can be aware of the care-of address of the mobile node as the moving node tells by itself or a home agent transmits a binding update message to the correspondent node when forwarding the packet towards the foreign agent. The correspondent node then constructs an entry in the binding cache for further communication[3]. since a mobile node shifts to another foreign agent, the foreign agent will maintain a binding cache of the new care-of address, forward packets towards mobile node which has moved from its network and also transmits a Binding Warning message to aware the home agent about the movement of the node [1]. Handling of triangular routing by route optimization mobile IP is effective but in a complex manner. Regular updating is shared by all of the nodes that are connected [17].

3.2.2 Reverse Routing

Reverse Routing is proposed by Peifang Zhou and Oliver W. Yang as a substitute to Route optimization mobile IP. Mobile node deliver packet to its home network and while moving to foreign network, it gets care of address. At the next step mobile node send registration message to the corresponding node that contain its home network address as well as care of address. Then the corresponding node updates its routing table, and all the further communication from mobile node to corresponding node takes place according to updated binding table. It is simpler then Router optimization as it relay on one message [17].

3.2.3 Location Registers (LR)

In this method the corresponding node first create link to the database named as home location register (is a database bridging information of mobile home IP address and care of address). And the mobile node always uses home location register for registration purpose, when the mobile node is on home network HLR takes responsibility of identity mapping and when its location changes to home network, it register its care of address assigned it by foreign network similar to mobile IP. When corresponding nodes want to communicate message at first check the database of Home location registration and confirm the mobility binding and deliver data directly to mobile node care of address. Correspondent node has to update its binding database before its registration lifetime expires. Mobile node upholding lists of its all corresponding nodes that deliver packet during its existing registration life time and While it shift to new place it share binding update to entire active CN's [18]. It reduces the cost because it does not require the home address and foreign address but it create burden on corresponding node in form of mobility and ways of interaction with home LR [17].

3.2.4 Virtual Home Agent

In this scheme idea of virtual home agent is presented. Virtual home agent [19] behaves like a real home agent. Whenever a mobile node moves to a foreign network it has assigned a virtual home address against its permanent home address for a session period. During the session the corresponding node send messages to the virtual home agent which further tunnels them towards the mobile node. This protocol supports transparency as the corresponding nodes are not aware of mobility. All the sessions are just for a short period of time and after that mobile node can change its virtual home agent which makes sure that every time mobile node is near to its virtual home agent [20].

3.2.5 Surrogate HA

To resolve resolves triangle routing problem idea of surrogate home agent (SHA) is presented. Surrogate home agent exist two levels above the permanent home agent. When a mobile node goes far away from its home network, it takes care of address from foreign agent and registers it with its home agent which further shares it with SHA. When the corresponding node sends packets they are tunneled to SHA rather than permanent home agent than SHA forwards them towards mobile node current location. As compare to Original mobile IP this technique decrease the transmission time, handoff delay, packet loss, and registration time But it has some limitations as it only provide better results whenever corresponding node is above the SHA otherwise not. It is just supportive in the inter-network. [21]

3.2.6 Other Possible Solutions

Many other protocols has been also proposed so far to solve the triangle routing problem as forward tunneling and binding cache [3], bidirectional route optimization [22], the smooth handoff technique [20], a virtual home agent [21], and a port address translation based route optimization scheme [4].

3.3 Solution of Hand off problem

The transmission overall performance during the mobile node handoff relies on three factors: re registration, mobile test, and fundamental interaction with the above layer protocol [13]. Getting local registration via the layered Mobile IP [23] is a method that helps in decreasing the wait time for re-registration and enhances the handoff functionality of Mobile IP. Original FA notification is also a solution to reduce packets loss by using the buffer memory [13].

3.4 Solution of intra domain movement Problem

Many protocols are designed to reduce problem of intra domain movement like TeleMIP, Cellular IP, and HAWAII. They can resolve the problems of frequently handoff and consequently decreases packet loss and hand off delay [14].

3.5 Solution of quality of serviceproblem

To solve end to end Quality of service problem in mobile IP combination of (DiffServ) differentiate service and (RSVP) resource reservation protocol is used [15].

3.6 Solution of Fragility problem

Multiple home agents rather than single one are used to solve the fragility issues. If one HA break down there are others who can took the responsibility to route the data packets towards mobile node [16].

4. Mobile IP Threats

Mobility leads to a number of different kinds of threats that might have different effects on the protection of the protocol. Though MIPv6 have many advance features against MIPv4. It uses IPsec protocol to provide security but still it has some loop holes for security threats. Few of them are described here.

4.1 Spoofing Binding Updates

If binding updates are not attested / authenticated, an attacker between the mobile node and corresponding node can spoofs all the binding update messages. It captures the messages and can alter the home address/CoA in it and then deliver them to corresponding node [24].Thus communication between mobile node and corresponding node cannot do successfully and packets are transmitted to an unwanted node.

4.2 Attacks against secrecy and integrity

Attacker can bust the integrity and privacy between mobile node and corresponding node as by sending the false binding message to the corresponding node. It inserts its own CoA in the field of the spoofed Binding message. When this particular message is send to corresponding node it will revise its binding cache and start out communication. In this way an attacker can able to see and alter the packets that are for the mobile node [25].

4.3 Basic Denial of Service Attacks

If the attacker spoofs the binding update and resends a registration request to a home address using own CoA. In this manner the attacker will get all the packets that fail entire connection with mobile node [14].

Bombing CoA with unwanted data

Sometimes the attacker places false CoA in the binding update and reroute the packets to any other targeted node. The purpose behind that is to bomb the targeted node with undesired packets. This could be possible when attacker understands about the large data stream involving both nodes [26]. This is a very serious attack because targeted node cannot recognize the attacker and could not do any think to avoid.

4.4 Replaying and Blocking Binding Updates

In this type of attacks the attacker captures the binding update message and holds the previous location of the mobile node. When the MN roves to a new place then it send that binding update to the corresponding node on the behalf of mobile node and reroute the packets on the previous spot. In that manner an attacker can stop binding updates for MN at its current position till the CN cache entry exhales [25].

4.5 Replay attacks

Sometimes attacker can spoof and store a copy of true registration request and use it later by registering false CoA for the MN.The temporal effects, are also need to be focused to tackle replay attacks.

4.6 Eavesdropping

In this type of attacks an attacker silently listen the traffic between MN and CN and gather important

information. Sometimes it just alters the messages and sometimes makes its independent communication to both MN and CN on the behalf of each other. Both MN and CN's are unaware of this and believe that they are communicating directly on a secure link [27].

5. Possible Solutions forPotential Threats

These are the possible solutions proposed by the researchers as countermeasures:

5.1 Message Authentication

Whenever corresponding node receive the binding update message, Mobile IP system architecture shouldauthenticate it to proceed. Following are some authentication techniques likely to be considered for this.

5.1.1 Use of Public Key Infrastructure (PKI)

Use of public key infrastructure is a typical method for authentication but in mobile IPv6 it is difficult to use a single PKI on the internet. [24]

5.1.2 Use of Cryptographically Generated Addresses

Cryptographically generated addresses are another method of authentication. In this technique mobile node's public key is hashed in the 2nd half of the HA. The key makes 62-64 bits of IP address which make it hard for an attacker to discover the key of the particular address. But there is only 62-64 bits of address so attacker can find the key by matching through error and trial methods. [25] Bombing attacks does not prevent by the Use of Cryptographically Generated Addresses.

5.1.3 Return Routability Tests

Return routability tests are also used to authenticate the binding updates and prevent bombing attacks. Two types of tests are used one for home address and other for CoA. Whenever the corresponding node gets a binding update message deliver a secret key to the home agent which it further tunnels towards mobile node, on the other hand the corresponding node also deliver another data packet with 2nd key at the CoA. The mobile node utilizes these two keys for the authentication of binding updates messages. [26] These tests confirm the home address and care of address efficiently but may result as the base of many other harasses [24].

5.2 Solution of Replay attacks

To avoid replay attacks the identification field is produced as it enables the home agents to figure out about the next value.

5.3 Solution of Eavesdropping

MIPv6 uses IPsec for security purpose, it authenticate and encrypt all IP packet during the communication session. Packets exchanged during communication are secured using IPSec but there is no security procedure exists for this kind of attacks [27].

6. Conclusion

Mobility can be considered as amajorinnovationin communication technologiescontributing valuein user's life style. This ability in telecom environment comes in to existence by the invention of Mobile IP. Mobile IP is a protocol that permits mobile system user to shift from one place to another keeping permanent IP address without getting the communicating session terminated. However, this capability also bears technicalissues and security concerns as presented by the researchers. This Paper takes into account thesechallenges besides possible security concerns faced by the mobile IPtill now. Since the index of their possible solutions tosecurethe Mobile IPcommunication architecture and process by reducingthenetworkoverhead and maximization of network performance is also discussed for single glance overview.

References:

[1] Redi, J., and P. Bahl. Mobile ip: (1998). A solution for transparent, seamless mobile computer communications.Fuji-Keizai's Report on Upcoming Trends in Mobile Computing and Communications.

[2] Girgis, Moheb R., Tarek M. Mahmoud, Youssef S. Takroni, and Hassan S. H.(2010). Performance evaluation of a new route optimization technique for mobile IP. arXiv preprint arXiv:1004.0771.

[3] Chandrasekaran, Janani. Mobile ip: Issues, challenges and solutions. (2009). PhD diss., Master's thesis, Department of Electrical and Computer Engineering Rutgers University.

[4] Raj S. B., Daljeet K., and Navpreet K. Mobile IP:(2013). A Study, Problems and their Solutions. International Journal of Scientific Research.

[5] Kumar, Ranjeeth. (2003) MSIP: a protocol for efficient handoffs of real-time multimedia sessions in mobile wireless scenarios. PhD diss., Indian Institute of Technology, Bombay.

[6] Nada, Fayza. (2007). Performance Analysis of Mobile IPv4 and Mobile IPv6. Int. Arab J. Inf. Technol. 4, no. 2: 153-160.

[7] Siozios, Kostas, PavlosE, and AlexandrosK.(2006). Design and Implementation of a Secure Mobile IP Architecture.

[8] Stoica, Adrian. (2007).A Review on Mobile IP Connectivity and its QoS.International Journal of Multimedia and Ubiquitous Engineering.

[9] Perkins, Charles. (2002). IP mobility support for IPv4.IETF RFC 3344,

[10] Doja, M. N., and Ravish S. (2012).Analysis of Token Based Mobile IPv6 and Standard Mobile IPv6 using CPN Tool. International Journal 2,vol no. 7

[11] Wu, Chun H., AnnT., Cheng, ShaoT. Lee, JanM. H., and DerT. L. (2002). Bi-directional route optimization in mobile ip over wireless lan. In Vehicular Technology Conference, 2002. Proceedings. VTC 2002-Fall. IEEE 56th, vol. 2, pp. 1168-1172.

[12] Ayani, Babak. (2002).Smooth handoff in mobile IP. PhD diss., Master's thesis, Department of Microelectronics and Information Technology at KTH University of California,

[13] Minhua Y., Yu L.Huimin Z.(2003). Handover Technology in Mobile IP. Telecommunication Technology.

[14] Min S., ZhiminL. (2003). Mobile IP and Its Improved Technologies. Telecommunications Science

[15] Yong Feng, FangweiLi. (2003).QoS Guarantee over Mobile IP.

[16] Nada, Fayza A.(2006).On using Mobile IP Protocols. Journal of Computer Science 2, Volno. 2

[17] Mahmood, Sohaib. (2004). Triangle Routing in Mobile IP. Lahore University of Management Sciences, Pakistan. http://suraj. lums. edu. pk/-cs678s04/2004% 20ProjectslFinals/Group04.pdf.

[18] Jan, R., Thomas R., Danny Y., Li F. C., Charles G., Michael B., and Mitesh P. (1999). Enhancing survivability of mobile Internet access using mobile IP with location registers. In INFOCOM'99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol. 1, pp. 3-11.

[19] Gao, Qiang, and Anthony Acampora. (2000), A virtual home agent based route optimization for mobile IP. In Wireless Communications and Networking Conference. WCNC. IEEE, vol. 2, pp. 592-596.

[20] Wang, Nen-Chung, and Yi-Jung Wu. (2006). A route optimization scheme for mobile IP with IP header extension. In Proceedings of the 2006 international conference on Wireless communications and mobile computing, pp. 1247-1252. ACM.

[21] Kumar, C., N. Tyagi, and R. Tripathi. (2005). Performance of Mobile IP with new route optimisation technique. In Personal Wireless Communications, ICPWC. 2005 IEEE International Conference on, pp. 522-526. IEEE.

[22] Zhu, Zhenkai, Ryuji Wakikawa, and Lixia Zhang. (2011). SAIL: A scalable approach for wide-area IP mobility. In Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, pp. 367-372. IEEE.

[23] Gustafsson Eva, Jonsson Annika, Perkins Charles E.(2003). IETF Internet Draft. Mobile IPv4 Regional Registration.

[24] Aura, Tuomas. (2004). Mobile IPv6 SecurityIn Security Protocols,. Springer Berlin Heidelberg,pp. 215-234.

[25] Aura, Tuomas, and JariA. (2002).MIPv6 BU attacks and defenses. Work in Progress

[26] Arkko, Jari, Vijay D., and Francis D. (2004).Using IPsec to protect mobile IPv6 signaling between mobile nodes and home agents.

[27] Barbudhe K Vishwajit, Barbudhe K Aumdevi. "Mobile IPv6:Threats and Solution." International journal of application or innovation in engineering and management. (2013).

Aatifah Noureen is a research scholar under the enrollment of MS (IT) program in University of Gujrat, Pakistan since 2013.She enrolled at the University of Gujrat in 2008 as she realized her interests in computing and technology and received her BS degree in Information Technology from University of Gujrat in 2012.Her research interest includes networking performance issues in mobile computing.

Zunaira Ilyasis a student of MS (IT) in University of Gujrat, Pakistan since 2013. She did BS (IT) from the same university in 2012. Her research interest spans the area of mobile ad-hoc networks.

Iram Shahzadi is a research scholar in University of Gujratsince 2013. She receives her B.Sc and MSc degrees from University of The Punjab, Pakistan in 2002and 2008 respectively. She is serving as a lecturer at Govt. Margazar College for women, Gujrat since 2009.Her research interests are QoS of packet radio networks for real communication.

Dr. Muddesar Iqbal has done Ph.D. from Kingston University UK in the area of Wireless Mesh Networks in 2009. He has been serving as Associate Professor in Faculty of computing and Information technology, University of Gujrat, Pakistan, since 2010. He won an Award of Appreciation from the Association of Business Executive (ABE) UK for tutoring the prize winner in Computer Fundamentals module. He also received Foreign Expert Certificate from State Administration of Foreign Experts. He is the authors of numerous papers within the area of wireless networks. He is also the approved supervisor for Ph.D. studies of Higher Education Commission of Pakistan.

Mr. Muhammad Shafiq is the Ph.D. scholar in department of Information and Communication Engineering, Yeungnam University, South Korea. He did Master of Science in Computer Science (MSCS) degree from UIIT, PMAS Arid Agriculture University Rawalpindi, Pakistan in 2010. He also received the degree of Master in Information Technology (M.I.T) from The University of Punjab in 2006. He served as visiting lecturer in the Federal Urdu University, Islamabad, Pakistan, for the period of one year since 2009.He has been serving as Lecturer in Faculty of Computing and Information Technology, University of Gujrat, Pakistan since 2010. He has published more than 10 research papers within the field of information and communication technology, at national and international level. His research interests span the area of QoS issues, resources and mobility management in mobile ad-hoc networks.

Azeem Irshad has been doing Ph.D from International Islamic University, Islamabad, after completing MS-CS from PMAS Arid Agriculture University Rawalpindi and is currently serving as visiting lecturer in AIOU. He has published more than 10 papers, in national and International Journals and proceedings. His research interests include NGN, IMS security, MANET security, merger of Ad hoc networks with other 4G technology platforms, multimedia over IP and resolving the emerging wireless issues.