February 2010

Master's Degree Thesis

Secure Roaming of Mobile Devices in Residential Network

Graduate School of Chosun University

Department of Information and Communication Engineering

Roja Kiran Basukala

Secure Roaming of Mobile Devices in Residential Network

February 25, 2010

Graduate School of Chosun University

Department of Information and Communication Engineering

Roja Kiran Basukala

Secure Roaming of Mobile Devices in Residential Network

Advisor: Dong-You Choi

This thesis is submitted to Chosun University in partial fulfillment of the requirements for a Master's Degree

October 2009

Graduate School of Chosun University

Department of Information and Communication Engineering

Roja Kiran Basukala

Roja Kiran Basukala's
Master's Degree Thesis
Approval

Committee Chairman Prof. Jong-An Park (인)

Committee Member Prof. Seung-Jo Han (인)

Committee Member Prof. Dong-You Choi (인)

November 2009

Graduate School of
Chosun University

Table of Contents

List of Figures

List of Tables

Acronyms

3DES:	Triple Data Encryption Standard
AC:	Alternating Current
AH:	Authentication Header
A/V:	Audio/Visual
CA:	Corresponding Agent
CD:	Compact Disc
CN:	Corresponding Node
CoA:	Care-of-Address
DHCP:	Dynamic Host Control Protocol
DoS:	Denial of Service
DES:	Data Encryption Standard
DVD:	Digital Versatile Disk
ESP:	Encapsulating security Payload
FA:	Foreign Agent
HA:	Home Agent
HAN:	Home Area Network
HMAC:	Hash based Message Authentication Code
HMAC-MD5:	Hash based Authentication Code Message Digest Algorithm 5
IP:	Internet Protocol
IPSec:	Internet Protocol Security
IETF:	Internet Engineering Task Force
IT:	Internet Technology
LAN:	Local Area Network
MAC:	Message Authentication Code
MN :	Mobile Node
RF:	Radio Frequency
RG:	Residential Gateway

RSA:	Rivest, Shamir and Adleman's algorithm
PC:	Personal Computer
PDA:	Personal Digital Assistant
SMN:	Secure Mobile Node
SRG:	Secure Residential Gateway
SBG:	Security Border Gateway
SA:	Security Association
TCP:	Transmission Control Protocol
UDP:	User Datagram Protocol
UPNP:	Universal Plug and Play
VPN:	Virtual Private Network
WAN:	Wide Area Network
WLAN:	Wireless Local Area Network

초 록

주택 네트워크에서 모바일 장치의 로밍 보안

Roja Kiran Basukala
지도교수: 최동유
정보통신공학과
조선대학교 일반대학원

주택 네트워크는 사용자의 편리하고 안전한 일상생활을 위해 전기적인 장치들과 접속을 하고 정보들을 수집한다. 주택 네트워크는 시간과 장소에 구속받지 않고 댁내에서 무선, 이더넷, 블루투스 그리고 RF 등의 각종 통신망 서비스와 광대역 연결을 통해 인터넷에 접속할 수 있는 복합 기술이다. 유비쿼터스가 발달함에 따라 더 많은 장치들이 무선화 되고 대부분 장치들이 로밍되어 질것이다. 로밍 장치는 사용자의 일상생활에서 개인적인 정보를 전달하기 때문에 주거 네트워크는 로밍 기기와 상호 작용시에 반드시 보안을 필요로 한다. 본 논문에서 제한한 모바일 IP 프로토콜은 모바일 IP와 IP 보안이 신뢰성 있는 외부 에이전트와 관계없이 주택 네트워크 통합과 로밍 보안을 제공하며, 주택 네트워크 로밍 보안은 IP 보안과 주거 네트워크 게이트웨이 등 모든 가정용 기기에 사용

할 수 있으며 모바일 장치의 end to end 보안을 책임진다. 또 한, 제안한 안전한 모바일 IP 프로토콜은 외부 네트워크에서 모바일 주거 장치의 로밍 보안을 보장한다.

ABSTRACT

Secure Roaming of Mobile Devices in Residential Network

Roja Kiran Basukala
Advisor: Prof. Dong-You Choi
Department of Information and Communications Engineering
Graduate School
Chosun University

Residential Network is collection and connection of several electrical and electronic home appliances for convenient, comfortable and daily life of home users. It is the hybrid technology of wireless, Ethernet, Bluetooth and RF to the internet via broadband connection at home with various home network services regardless of device, time and place. For ubiquitous development, more devices will be wireless and most of them will be roaming. Since these roaming devices carry private information of daily life of residential users,

the interaction among the roaming devices of residential network must be secure. This thesis presents security of roaming devices of residential network using integration of Mobile IP and IP Security without the need to trust foreign agents. Moreover, it ensures end to end security of mobile devices of residential network with IP Security enabled in all residential devices including residential gateway. The proposed secure Mobile IP registration protocol in this thesis ensures the roaming security of mobile residential devices in foreign networks.

Ⅰ. Introduction

A. Research overview

Residential Network also known as Home network is a new IT technology environment for making an offer of convenient, safe, pleasant and blessed lives to people, making it possible to be provided with various home network services by constructing home network infrastructure regardless of devices, time and places [1]. This is achieved by the integrating existing Ethernet, wireless, power line and phone line technologies at residential gateway at home. The residential gateway is connected to the outside world with the public internet in order to access internet from home and to access home network from outside.

Currently, there is a worldwide trend towards ubiquitous home. Hence more and more devices in home network are wireless because of the ability to control or access networked devices from anywhere anytime inside or outside the residence. Emerging wireless home networking technologies in these devices include the 802.11 wireless LAN standard and low cost technologies such as Bluetooth and Home RF. Thus, several modern residential electronic devices like laptops, handheld computers and palm devices, cordless and

cellular phones, and MP3 players, etc. are exponentially added to residential networks.

In residential network system, security problems such as hacking, viruses, and exposure of personal information, traditional problems in network environments, still exist, and new security problems have developed because most of the devices connected with the network are quite simple [2]. Also the home network users are not skilled from security point of view. Moreover, data flow in home network contain our daily life private information; the necessity of protecting incoming and outgoing traffic from the internet and mobile devices has greatly emerged. If security mechanisms are not properly implemented in such hybrid networks, the internet and wireless part of home network could provide entry points for malicious entities [3]. A natural way to provide security to Mobile IP based network is to use the IP Security (IPSec) protocol suite. This thesis specially focuses on security of roaming devices of residential network. The integration of Mobile IP and IPSec along with a secure Mobile IP Registration protocol is proposed to ensure security of roaming devices in residential network.

B. Research objectives

Security is always a concern in any internetworking environment

these days and hence residential network is not an exception. Home network environment has security-weaknesses that are appeared in existing environment and additional security weaknesses, which is unique in home network environment, that are due to information appliances with lower computing performance [4].

Wireless part of residential network is less secure than wired because transmissions are sent "out in the open" where they can be intercepted. Hence malicious users can disrupt the wireless communication of residential network. For example, a malicious device could interfere with registration process, causing the datagrams intended for a mobile device to be diverted. Moreover, in a ubiquitous home, roaming enables a device to move from one residence to another [5]. While roaming, attackers can spoof packets transmitted over wireless links, hence mobile users must be authenticated safely.

Because the digital home network is connected to the Internet, the home will face even greater threats, not only from the same intruders, but also from a new class of Internet criminals who are likely to target private home networks, and the homes themselves, using Internet access to facilitate mayhem and mischief [6]. Home network users are not only multiple adults or teenage boys/girls but also guests, friends, hired employees, maintenance personnel etc. These outsiders may bring mobile devices or control points into the

home networks. Moreover the integration of wired and wireless technology has also made the possibility of unauthorized access by device included in neighbor home network.

Hence this thesis arose to maintain security of wireless, internet and Mobile IP communication in order to secure residential network. The main objectives of this thesis are listed as follows

1. To secure the wireless section of home network.
2. To secure the registration and communication of roaming devices.
3. To provide end-to-end security support between residential devices.
4. To provide security from internet attacks.

C. Thesis contributions

Home networks are considered as an infrastructure for the ubiquitous computing environments that provide computing and communication services at any time any where [7]. With the development of various mobile sensing technologies, remote control and ubiquitous infrastructure, a lot of researches and developments on home network technologies and services are actively on going. As home devices are being used in ubiquitous manner, security of wired and wireless home network devices has been an important

factor for home network security.

Hence, this thesis is motivated to explore an alternative for integrating Mobile Internet Protocol Version 4 with IP Security to secure IP Communications over the wireless links of Residential Networks. This thesis focuses on network layer security and provision of security services while roaming to a foreign network, without having trust to foreign network. A secure Mobile IP Registration protocol is proposed to secure Mobile IP registration processes and Mobile IP communication when a mobile node roams to a foreign network in which there is no need of trusting foreign networks. Additionally, we have provisioned end-to-end security for roaming residential devices of the home network with two IPSec tunnels.

Thus the main contributions of this thesis are as listed as follows

1. Integration of Mobile IP and IPSec to secure Mobile IP registration and communication without the need to trust foreign agents.
2. End-to-end security support for roaming residential devices with two IPSec tunnels via Residential Gateway.
3. Provision of security from internet attacks and wireless attacks.
4. Securing residential gateway and mobile nodes from internal and external attacks.

D. Thesis organization

The remainder of this thesis is organized in modular chapters. Chapter II overviews Residential network and its features. Chapter III discusses about Mobile IP and its problems in terms of security. Chapter IV explains about IPSec as a secure mechanism to protect security flaws in Mobile IP. In chapter V, some related works with integration of Mobile IP and IPSec is discussed and a secure Mobile IP Registration protocol is proposed for the integration of Mobile IP and IPSec in residential network along with some security analysis of proposed method. Chapter VI illustrates the simulation and results of proposed method. Finally this thesis is concluded in the last chapter with the wrapping text for summary of this research along with some future works.

II. Residential Network

Home Network is the collection of network elements that process, manage, transport and store information, enabling the connection and integration of multiple computing, control, monitoring, and communication devices in the home [8]. It is not an entirely new network system but the integrated technology of wired and wireless network for a variety of purposes – from connecting multiple personal computers for printer, file and Internet connection sharing, to networking home entertainment systems and home automation [9].

With the rapid development of IT technology and wider distribution of internet services through high-speed networks, home networking devices have emerged rapidly with various functions along with improved computing power and networking ability. Home network include consumer electronics devices such as televisions, VCRs, and CD players, as well as traditional home appliances such as a refrigerators, microwave ovens, washers and dryers, heating and air conditioning thermostats, home security systems, and home automation controls. Home network devices perform a sending/receiving function in connection with an external network through a home gateway, and the sending/receiving of information within the home is done through the home network. Home

information devices may be managed outside of the home, through the use of devices such as handsets, PDAs, and computers [6].

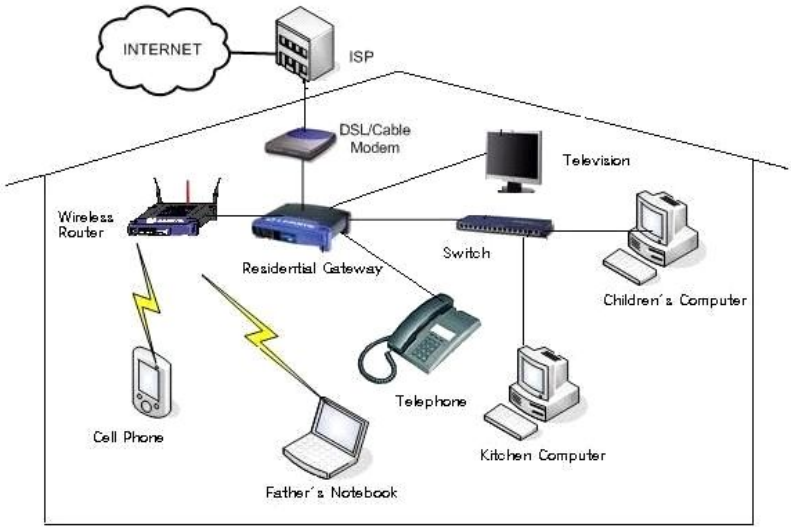

Figure 2.1 General residential network model

Currently home network supports broadband applications such as digital audio and video, and home automation functions such as home security, energy management, lighting, and remote control of appliances; these devices would be capable of being controlled from outside the home, through an access device such as a Residential Gateway (RG), using an "always on" Internet connection [6]. Figure 2.1 depicts the general residential network model which integrates power-line, Ethernet, wireless and phone-line technologies at the residential gateway which is connected to the outside world via

internet through broadband internet connection.

A. Residential gateway

The Residential Gateway is considered as heart of the home network since resides between the public network and the home network separating the Wide-Area Network (WAN) and the Home Area Network (HAN). It is always connected to the internet and hence is an always-on device. Thus it is the envisioned platform for hosting in-home applications as well as applications delivered by service providers. It inserts a control function between external networks and in-home networks and devices. It serves as a traffic cop function controlling and routing traffic so as to allow maximum use of all facilities [10]. It has server capability in order to realize the ingress function. Considering the requirements and the characteristics of the home gateway, dynamic access from outside the home has to be considered. There, the access can be from anywhere and from any land of node (e.g. PC, PDA or cellar phone) [11]. As the residential gateway separates the private home network from the public internet securing incoming and outgoing traffic to the residential gateway should be secured.

B. Home networking structure

Generally the home network technologies can be divided into two categories: WAN and HAN, the Residential area. The well known technologies exist over WAN as shown in figure 2.2 which is beyond the scope of this thesis. But in home area, there are a lot of standards and technologies working and providing services. The home area connect to the outside world through the residential gateway [12].

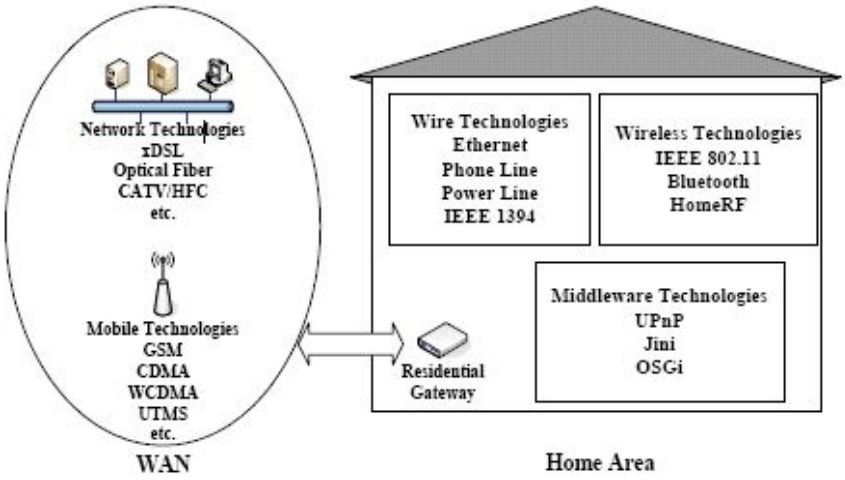

Figure 2.2 Home networking structure

C. Classifications of home networking technologies

Home network technologies can be classified into several parts:

wired network technologies, wireless network technologies and middleware technologies. The details of the middleware technologies is beyond the scope of this thesis.

1. Wired technologies

The physical circuit used to build home network covers wired technology. Some of the wired technologies applied in home area are briefly introduced in following section.

Ethernet: It is the most widely used network technology known as IEEE 802.3 standard. The Ethernet system requires new wiring like twisted-pair, coaxial cable, optical fiber etc. Several versions of Ethernet Standard exist in which most widely used version of Ethernet technology is 100Mbps twisted-pair.

Phoneline: This technology focuses on using the phone line to build physical network backbone for the home network. HomePNA is the most famous group developed in this technology. The transfer speed can reach 10Mbps. It connects home appliances like PCs, TV, fridge, DVD/CD/MP3 players to each other and to the internet. It supports up to 500 feet of phone wire between devices connected to RJ-11 jacks.

Powerline: It uses existing power and electric wiring in the home as a physical network layer. In every home, there are more AC/power sockets/outlets than phone jacks. It occupies about 4.5

to 21MHz band. HomePlug is the most famous group developed in this technology. The bit rate delivered to MAC layer by physical layer is about 10 Mbps but the greater the amount of electrical noise on the line limits practical transmission speeds to much lower values. Channel adaptation is required to achieve high data rates and reliability.

IEEE 1394: It is high speed peripheral standard ideal for audio and streaming video purposes in multimedia devices such as video camera and other high-speed device like hard disk drives and printers. Large amounts of data can be moved between computers and high-speed peripheral devices at data rates of 100, 200, 400 or 800 Mbps. There is no need to convert digital data into analog and tolerate a high loss of data integrity because of digital interface in this technology. However it requires new wiring and the cable length is limited to about 15 feet between devices.

2. Wireless technologies:

Wireless technologies use Radio frequency technologies to build the network connection. Some wireless technologies used in home network are briefly introduced below.

HomeRF: It is an open industry specification led by Home RF Working Group that allows PCs, peripherals, cell phone and other consumer devices to share and communicate data and voice in

home without laying new wires. This technology enables broad range of interoperable devices using RF anywhere in and around the house. Technically it offers low cost and voice support of along with TCP/IP support of 802.11 for data. It also includes support for data encryption.

IEEE 802.11: It is one of the most popular WLAN technologies in the world. The IEEE 802.11 standard works on 2.4GHz ISM band and transfer rate can reach 11Mbps. 802.11b and 802.11g can reach 54Mbps. The wireless communication ability, mobility and the high speed performance make this technology applied in home network. Radio or Infrared waves are used to transmit and receive data over air. It supports optional encryption modes for security with some shortcomings which has become a significant issue.

Bluetooth: It is an open specification that enables short-range wireless connections between desktop computers, notebook computers, computer devices, mobile phones, Personal digital assistants and other Bluetooth embedded devices. It operates in 2.4GHz globally. Though the theoretical data rate is 1 Mbps, the actual throughput observed is 400 to 700 Kbps. It also offers support for data encryption.

It is the wireless standards IEEE 802.11 and HiperLAN2 which will dominate replacing Ethernet which is dominating the fixed-line interconnect technology. Phoneline is not suitable due to the low

number of telephone socket outlets around the home. Powerline and Ethernet requires new wiring but is relatively low cost. Wireless technology requires no change to the infrastructure and is more flexible, although power levels must be kept low to be safe, limiting the range of the RF signal [13].

D. Home networking applications

A lot of intelligent appliances are appearing in the home environment. Intelligent home networking devices means devices or appliance systems in the home area or living environment which can be controlled, monitored or can offer ability of stream transmission via network. Users can query the appliances status and control them remotely through the user interface that appearing in web pages. Home network technology makes people's life have great improvement, makes the environment at home more convenient, safer and more efficient [12]. The applications of home networking technologies may be classified into following fields:

Home automation: It provides a centralized point for automation of home environment. Home networking technologies can help human to create a more confident living environment.

Home entertainment: This application take an advantage of A/V content feeds from the service provider in the internet or A/V

storage in the home area.

Networking communication: The home networking technologies provide network communication ability to each home appliance.

Security service: It can provide household status monitor service. Home user can monitor and control security service utilizing web user interface.

E. Home network security issues

Because of heterogeneous nature of several technologies, they poses new challenges concerning security. Some of the examples are:

- A wireless device is not confined by the walls of an apartment, so neighbors can monitor as well as intrude and use services they are meant to, like switching lights.
- The guests of the house may be granted to use home network with their own mobile devices.
- Broadband home networks are vulnerable to security threats from hackers due to always-on nature of the connection via Residential gateway.
- Denial of service attack vulnerability also needs to be addressed.

The first line of defense, such as a firewall or authentication client, is likely to be in the Residential Gateway (RG) or other access device; however, there needs other defense mechanisms required on user appliances or devices. It is important that the defenses in the RG and the defenses in the networked devices work in partnership; as these devices will generally come from different vendors, there is a need for a home network security standard that will implement interoperability of these security mechanisms, without undue burden on the homeowner [6].

III. Mobile IP

Mobile IP is a standard protocol that allows users to maintain nonstop connectivity with their home IP addresses regardless of the physical movement [14]. It is an on-going effort under IETF towards an Internet Standard that aims to support mobility within internet. It is proposed solution that operates at network-layer to address "node mobility problem" in current Internet Architecture. This protocol defines extension mechanisms on the top of existing IPV4 to allow transparent routing of IP datagrams between a Mobile Node (MN) and its Corresponding Node (CN), as it moves and changers its point of attachment on the Internet [15].

In Mobile IP, MN is allowed to use two IP addreses. The first one, called home address, is static and is mainly used to identify higher layer connections, e.g. TCP. The second IP address is Care-of-Address (CoA) used by MN when it is roaming into different network. The reason behind the CoA is for identification MN's new point of attachment with respect to network topology. The CoA can be achieved through a Dynamic Host Configuration Protocol (DHCP) server or via Foreign Agent (FA) in foreign networks. A network layer agent on home network called Home agent (HA) should be available to maintain an association between MN's home address and its current CoA. HA is responsible to

intercept any datagrams destined to MN's home address that reach home network. and redirect them to MN's CoA.

A. Mobile IP Protocol

The Mobile IP protocol can be described with following three steps.

1. Agent discovery

HA as well as FA periodically broadcasts agent advertisements at regular intervals. MN can also send a solicitation message to learn whether any agents are present. MN listens these advertisements and can decide whether it is in home network or foreign network by comparing the network portion of router's IP address obtained from these advertisements. If it is in foreign network, it proceeds to get CoA via FA or DHCP server.

2. Registration

After the MN gets CoA, it needs to register it with HA via FA or directly. This is initiated by a registration request sent by MN to HA. HA decides whether to accept or deny the request based on the parameters of the registration request. If it accepts the request it begins to associate the home address of MN with CoA, and

maintains this association until the registration lifetime expires. The triplet that contains the home address, care-of-address and registration lifetime is called binding for MN [16]. Figure 3.1 depicts the Mobile IP registration process.

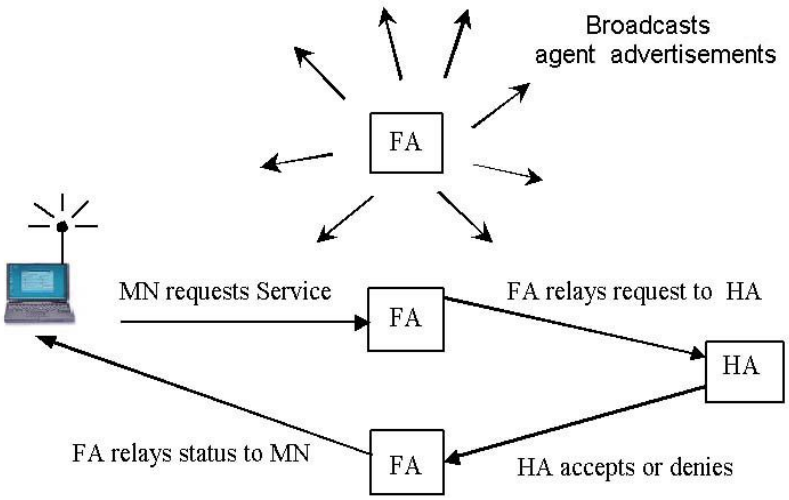

Figure 3.1 Mobile IP registration process.

3. Tunneling

When redirecting packets from the home agent to the mobile node, the default mechanism is to create a new IP header containing the mobile node's care-of address as the destination IP address. The new header encapsulates the original packet, making the previous header to be neglected when routing the packet to the mobile node. This type of encapsulation is called tunneling.

B. Mobile IP Security

In order to safeguard against various security risks, a limited number of provisions are available in Mobile IP. Authentication of Registration Request and Registration Reply messages can be used to prevent unauthorized devices from intercepting traffic. All mobile devices are required to support authentication and keys must be distributed manually as there is no automated system for key distribution. The default authentication method used is HMAC-MD5 [17].

1. Prevention from replay attacks

If a third party intercepts a datagram, hold onto it and re-sends it later on, then this type of attack is termed as replay-attack. The identification field used in Registration Request and Registration Reply messages is designed to prevent replay attacks. Since each request has a different identification number, nodes and agents can match up requests and replies and deny any data packets they receive that are repeated [17]. There are two main methods of replay protections to keep the identification field unique:

- Using timestamps
- Using random numbers

The mobile node and the home agent must agree on what method of replay protection to be used. The default method is using timestamps.

C. Security flaws in Mobile IP

Security is always a big concern for Mobile IP wireless networks. Mobile IP raises some security issues and attacks due to the wireless and roaming nature of mobile devices from one wireless network to another [16] [18].

1. Denial of service

Denial of Service (DoS) is defined as "A bad guy preventing a good guy from accomplishing work done". In Mobile IP, when a bad boy somehow performs registration of CoA for a real MN, DoS attack may occur with two probable problems.

- The real MN is disconnected
- The bad guy can see all traffic going to real MN.

For prevention of DoS attack, each MN and HA must share a SA to impose strong authentication on all registration messages that are exchanged during the registration process.

2. Replay attack

A malicious node somehow obtains a valid registration request, store it and then replay it to accomplish a forged CoA for a MN. It is already mentioned in above section about its prevention in Mobile IP. However, if an attacker somehow knows what should be the next value but it still impossible to insert it into the message because the messages are strongly authenticated.

3. Eavesdropping

This kind of attack occurs when a bad guy somehow manages to listen the traffic between the MN and HA. End-to-end encryption and Link-layer encryptions are the solutions to prevent this kind of attack.

4. Session hijacking

An attacker waits for a MN to register with its HA and then eavesdrop to see when something interesting happens. Then attacker transmits several unnecessary packets putting it out of action. In this way attacker hijacks the session and communicates with other node as if it is a valid node. This type of attack can be protected by End-to-End encryption and link layer encryption.

5. Flooding

This type of attack occurs if the attacker is the valid node of the network. The malicious node sends a legal registration request message to HA and claims that it has moved to a new location. Hence an intruder can redirect traffic intended to MN to a location of its choice.

The obvious solution when stronger assurances of privacy or authenticity are required is to make use of the IPSec.

IV. IPSec

IPSec is a collection of protocols, authentication and encryption /decryption mechanisms. It is a layer 3 protocol standard designed as an end-to-end mechanism for ensuring data security in IP based communications. It allows IP payloads to be encrypted and encapsulated in an IP header for secure transfer across the Internet [17]. It provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication. To implement IPSec, encryption keys are exchanged between communicating parties. These keys are used with encryption algorithms to encrypt and decrypt data. Symmetric algorithms are mostly used because of much higher performance.

The security services offered by IPSec are listed as follows[20]

- Access Control
- Connectionless Integrity
- Data origin authentication
- Rejection of Replayed packets
- Confidentiality
- Limited traffic flow confidentiality

A. Authentication header

The Authentication header (AH) is used to protect the authenticity and integrity of an IP packet with a keyed cryptographic hash value. It provides connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays [16]. Message Authentication Code (MAC) algorithm is used mostly in AH where the communicating parties share a secret key. Besides authentication, it also prevents from address spoofing attacks and replay attacks.

B. Encapsulating Security Payload

The Encapsulating Security Payload (ESP) transports encrypted IP packets ensuring confidentiality and optionally authenticity as well as integrity of the packet's payload. Unlike AH, the outer IP header is not protected. It provides confidentiality, data origin authentication, connectionless integrity and anti-replay service and limited traffic flow confidentiality. ESP supports nearly any kind of symmetric encryption. The default standard built into ESP that assures basic interoperability is DES. It may be applied alone or in combination with the AH in a nested fashion [16].

The following table 4.1 compares the security features of AH, ESP with encryption only and ESP with encryption plus authentication [19].

Table 4.1 Comparision of IPSec services derived from [19]

Security Services	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access Control	Yes	Yes	Yes
Connectionless Integrity	Yes	No	Yes
Data Origin Authentication	Yes	No	Yes
Rejection of replayed packets	Yes	Yes	Yes
Confidentiality	No	Yes	Yes
Limited Traffic Flow Confidentiality	No	Yes	Yes

These ESP and AH have been defined for use in two different modes:

C. Transport mode

In this mode, AH or ESP header is added to the IP payload. It is intended for use directly by communicating end-systems. It provides protection for upper layer protocols such as TCP and UDP segment or ICMP packet. ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header. AH in transport

mode authenticates the IP payload and selected portions of the IP header.

D. Tunnel mode

In this mode, the appropriate header is added to complete IP packet for its protection. A new IP header is created with the IP address of tunnel endpoint in destination address field. It is allowed to be used between end-systems or intermediate systems. ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header. AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header. The table 4.1 depicts the transport and tunnel modes of AH, ESP and ESP with Authentication [19].

Table 4.2 Tunnel mode and transport mode functionality from [19]

Mode/ IPSec Protocol	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outside header and outer IPv6 extension headers
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header	Encrypts entire inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header	Encrypts entire inner IP packet. Authenticates IP packet

To use these security mechanisms, some information like keys, algorithm parameters has to be exchanged between two communicating entities. Sharing of keys among communication parties is the fundamental thing for the proper functioning of the AH and ESP Protocol. The Internet Key Exchange (IKE) protocol has been defined so that the communication parties can negotiate security parameters and establish session keys to enable the setup of Security Association (SA) which is the key concept of IPSec. An SA is a oneway relationship between a sender and a receiver that affords security services to the traffic carried on it. If two-way secure exchange is needed then two SA is required. SAs can be established between end users, between security gateways and between end user and security gateway.

V. Integration of Mobile IP and IPSec in Residential devices

A. Related works

Much of the research work has been done integrating Mobile IP and IPSec to secure the Mobile IP communication.

Torsten Braun and Marc Danzeisen [20] proposed Secure Mobile IP (SecMIP) in which a MN can securely access network protected by a firewall with the establishment of a secure IP Sec tunnel between the firewall and the Mobile Node(MN). This solution ensures that it does not require to introduce any new protocols or to modify any existing protocol. The main problem of this model is that here only one direction is considered to create IPSec Tunnel and that is between MN node and home firewall. The CN cannot communicate with MN directly but through home firewall traversing long route. Also MN receives the collocated care-of-address from DHCP Server. But they also use foreign agent for IP Sec processing, and the FA has the capability of giving CoA to MN. So the use of DHCP Server can easily be omitted.

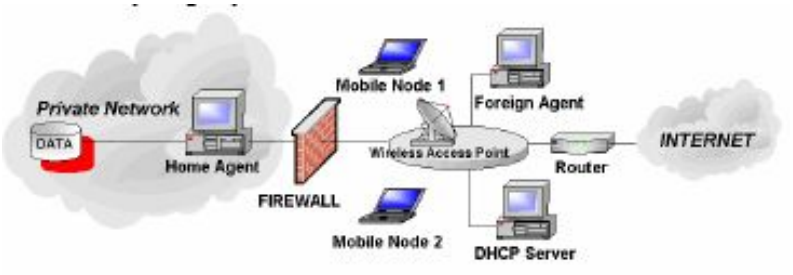

Figure 5.1 SecIP image scenario from [20]

John K. Zao and Matt Condel [21] proposed MIP-IPSec tunnel between MN-HA, HA-FA and FA-MN to fulfill the security requirements. It is proposed to add some modifications to Agent advertisement and to registration request messages. But establishment of MN-HA and MN-FA tunnels are expensive as they are not Mobile IP redirection tunnel. That's why they must be established separately. But HA-FA tunnel are very easy to establish just adding IP Sec protection to existing Mobile IP tunnel.

Atsuhi Inoue, Masahiro Ishiyama, Atsushi Fukumoto and Toshio Okamoto proposed Secure Mobile IP protocol with some modifications in Mobile IP protocol with IPSec [22]. Here secure Mobile IP is implemented on security gateway (SGW) and MNs. This SGW is placed between the inside network and the Internet. Dynamic gateway discovery is also proposed to locate a specific SGW and also a communication model is described that is how to traverse SGW using IP Sec. Finally current implementation status and the performance status is reported. The main problem of this

model is that when MN goes outside of an organization, they don''t protect routing information. Also MN has to maintain SAs with many SGWs. Since it has used DHCP server to obtain CoA to remove the involvement, there might be available address problem in foreign networks.

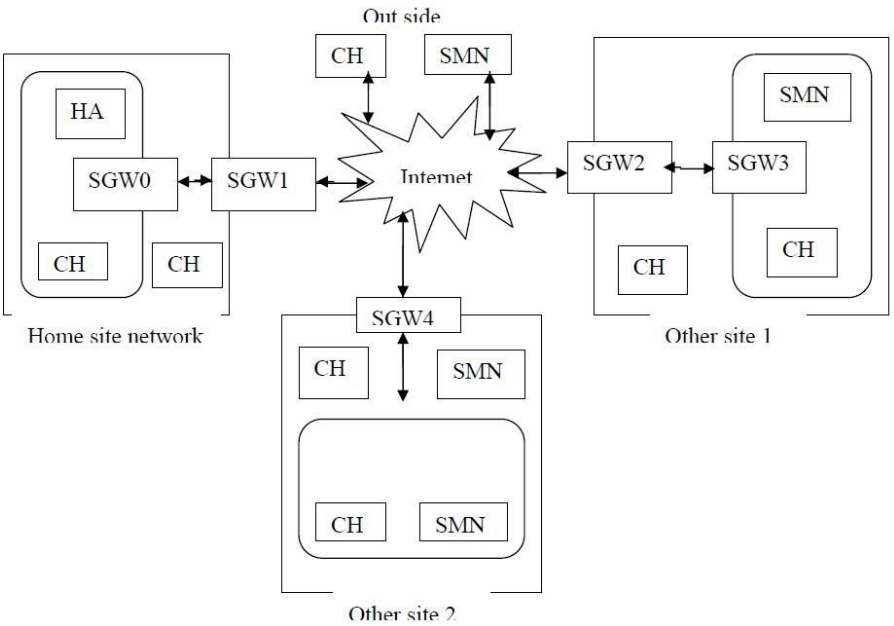

Figure 5.2 Secure Mobile IP protocol's framework derived from [22]

Rafiqul Islam [23] did a brief security survey on Mobile IP. Enhanced Security in Mobile IP Communication was also proposed by using IPSec where MN has to authenticate either the FA or the Firewall by IPSec functionality. He proposed a system to secure mobility support using Security Border Gateway(SBG) with the use

of IPSec, Ingress Filtering, and symmetric bi-directional route optimization. An addition of HA-CA tunnel in this protocol seems quite expensive. Also the SBGs are supposed to be administered by skilled administrators which is not possible for residential networks as the residential users may not have technical knowledge in maintaining security.

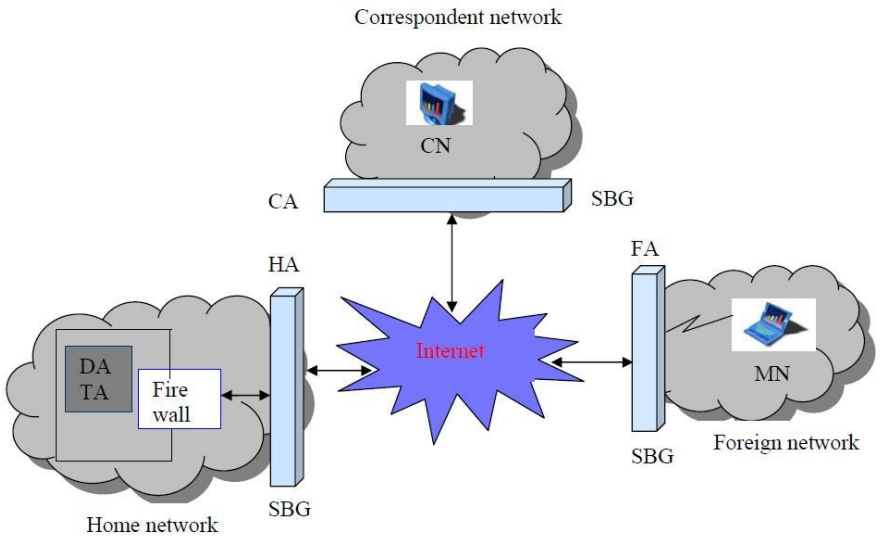

Figure 5.3 Framework for enhanced security in Mobile IP communication

B. Excluding FA in security

When we implement IPSec in any network, it is important to explore what sort of network entities should be enabled with IPSec to secure the whole network because a secret key should be shared

between those entities to create IPSec tunnel. As mentioned in [24] it is generally relatively easy to install a shared secret between MN and its HA, because these systems belong to the same residential network. A much more difficult task is to install a secret key between a MN and foreign networks. Foreign networks may or may not employ IP layer security. Furthermore, home network might not trust the foreign network to be involved in securing the roaming mobile node as explained in [24]. Moreover, a unique SA between MN and FA or HA and FA is required and every MN and HA should maintain SA with every FA it visits or may visit. The number of FAs MN may visit can not be predicted in advance because it may increase with increase in time. So, involvement of FA in security relationship with HA or MN is not scalable unless an efficient and secure key exchange mechanism is employed. [25] shows implementing IPSec in residential gateway and MNs is a good solution for devices with high mobility as high-roaming does not affect in security at all in this case as there is no overhead of maintaining security relationships with every residential networks. Since this thesis focussed on end-to-end security too, a study over conventional End-to-End Security with IPSec over Mobile IP which does not require FA to be trusted is performed.

C. End-to-end security support

MN and CN are IPSec enabled and hence the IP packets transmitted between MN and CN are encrypted end-to-end protecting wireless link between HA and FA. Though this integration seems secure in the sense that even if any malicious code is able to eavesdrop on the wireless link, it can only sniff encrypted packets [8]. Between the CN and MN an SA is maintained so that only MN and CN should keep the secret keys safely to avoid eavesdropping. However it is not possible for the MN to maintain SA with each CN with which it communicates. When the numbers of devices grow in residential network, the number of SAs in each MN will increase which leads a scalability problem. Hence this is not good solution of residential network technology where increase in residential devices is growing day by day because of ubiquitous nature.

D. Proposed security support for residential network

In order to achieve residential network security, implementation of IPSec in only residential network entities is kept in mind. Following this, only HA, RG, MN and wired devices of the residential network can be trusted. RG being the heart of the residential network connected to the outside world can also act as HA for

mobile IP operations. So both Mobile IP operations and IPSec are handled by RG if IPSec is implemented over it. Since this gateway is intended to use for security of residential network, we term it as Secure Residential Gateway (SRG). Residential MN maintains a single SA between itself and the SRG despite the location of mobile node. It is proposed to use IPSec tunnel mode running between RG and its MN. Unlike the proposed protocol in [26] FA is only responsible for agent discovery and relaying packets to SRG. Hence roaming MN is always protected hence it is termed as secure mobile node (SMN) in proposed protocol. This implementation allows IPSec to operate in a seamless manner when SMN roams. The SRG and SMN are both responsible for encryption, decryption operation of IPSec and also encapsulation and decapsulation operations of Mobile IP for secure Mobile IP Communication.

To achieve end-to-end security, the conventional end-to-end security tunnel form SMN to CN needs to be broken into 2 tunnels: between SRG and SMN; and between CN and SRG. So in this context SRG sets up an SA for each SMN in its network. Every SMN needs to maintain a single SA between itself and SRG in the residential network whether it is in home network or in foreign network. Every other wired or mobile node in residential network with which MN communicates is considered as CN in our proposed protocol assuming that the residential network communication is between residential

wired or mobile devices of the home network. The SRG is also responsible for Mobile IP registration and relaying messages to SMN's CoA. Any data packet from or to the SMN is secured by the IPSec tunnel between SRG and MN. So during roaming of SMN, all the data transmission over the wireless link is encrypted and also there is no need to re-establish an IPSec tunnel between SRG and SMN. The following figure 5.4 depicts steps in proposed protocol.

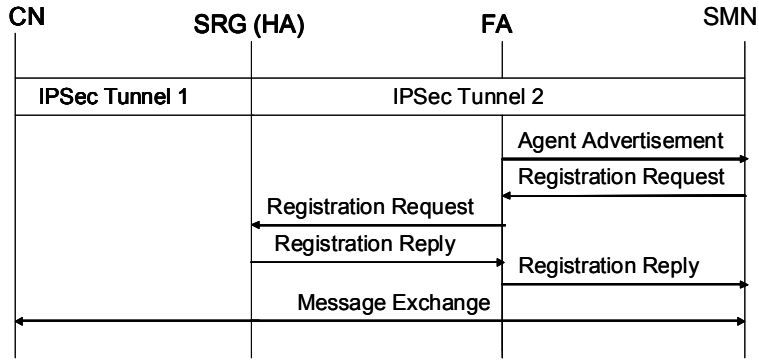

Figure 5.4: Proposed end-to-end security in Mobile IP communication

Firstly, the IPSec tunnel establishments from CN to SRG and SMN to SRG take place. These tunnels are established despite the location of SMN whether in home network or foreign network. When SMN visits a foreign residential network, it waits for an advertisement from or sends a solicitation message to the foreign agent informing its presence. The SMN hence obtains a care-of-address (CoA) from FA. Then it has to inform the home agent in residential network, i.e. SRG about the new IP address according to Mobile IP concept. So

SMN sends an encrypted registration request with care-of address info using UDP securely as follows.

1. Registration request

$MSG_{MR} = <IP_M, IP_R, LT, n_1, (K_{MR}, n_1, IP_M)K_{MR}>$

where,

M	The Mobile Node
R	The Residential Gateway of M
K_{AB}	Shared secret key between A and B
IP_A	The IP address of device A
N_i	Nonce i
MSG_{AB}	A message sent from entity A to entity B
<...>	Contents of the message
LT	Lifetime
()X	The contents of the parentheses are encrypted by the key X
P_A	Public key of A

The mobile forwards this encrypted registration message to the foreign agent and the foreign agent extracts the IP address of residential gateway where it has to transfer the encrypted packet.

The foreign agent here is only used for forwarding packets. It is not involved for security purposes of the registration messages and also for communication between roaming devise and the residential gateway. The foreign agent here is only involved for forwarding packets between mobile node and the secure residential gateway and also for ending agent solicitation messages to let the mobile node know that it has visited different network.

After the secure residential gateway receives the registration request from the foreign agent, it decrypts the encrypted registration information and confirms that the request is from its own mobile node as the secret key is only shared between the residential gateway and mobile node. Then it sends the registration as follows with a session key so use by the mobile node after the registration during that particular session.

2. Registration reply

$MSG_{RM} = <(K_{MR}, n_2, SK_{MR})K_{MR}>$

where,

SK_{AB} Session Key between A and B

The foreign agent upon receiving the registration reply from the secure residential gateway forwards to the destined mobile node and

mobile node decapsulates the packet with shared secret key and confirms the registration process is complete. It extracts the session key sent by the residential gateway in encrypted message and uses that key for the secure communication with residential gateway during that session. Hence the communication between the mobile node and the residential gateway is secured. The steps involved in proposed protocol is depicted in the figure 5.5.

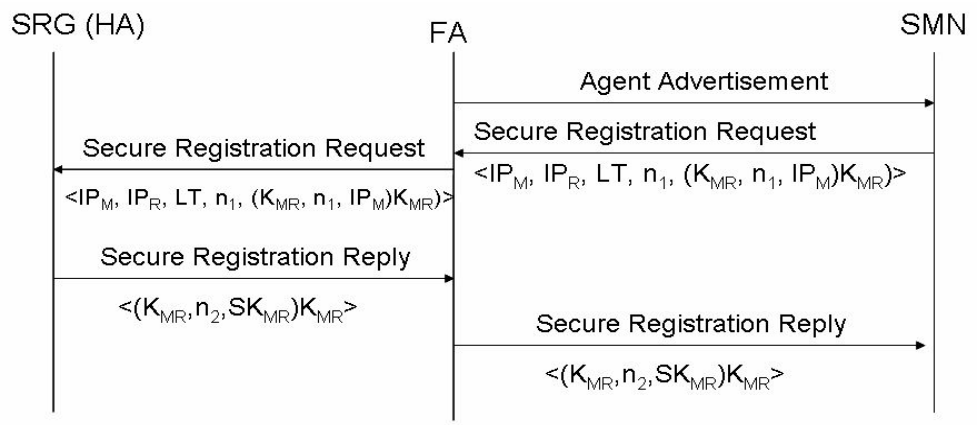

Figure 5.5: Message flow in proposed secure Mobile IP registration

All communications encrypted by SMN using IPSec will be sent to SRG. SRG being the endpoint of IPSec tunnel will decapsulate and decrypt IP packets. As it has to forward to CN, it will again encrypt the packet with CN's shared secret key so that the communication from SMN to SRG and SRG to CN is secure. Here SRG serves as endpoint for two IPSec tunnels with MN and CN. Every MN and CN are also responsible for encrypting and decrypting their packets too.

Similarly all the traffic from CN to SMN takes place securely in vice versa manner. Hence the end-to-end security from CN to SMN is ensured with multiple IPSec tunnels at SRG using the secure Mobile IP Registration Protocol to secure the Mobile IP Communication over the Residential network. This proposed secure Mobile IP Registration Protocol ensures security not only during Mobile IP registration but also after registration with session key being shared by SRG with SMN.

VI. Simulation Results and Security Analysis

A. Simulation

The simulation of roaming mobile device of residential network into foreign network was performed using opnet modeler version 14.5 [27] as shown in figure 6.1. The simulation was performed in two scenarios, CN_SMN and CN_SRG_SMN in order to compare the proposed security support with conventional end-to-end security support.

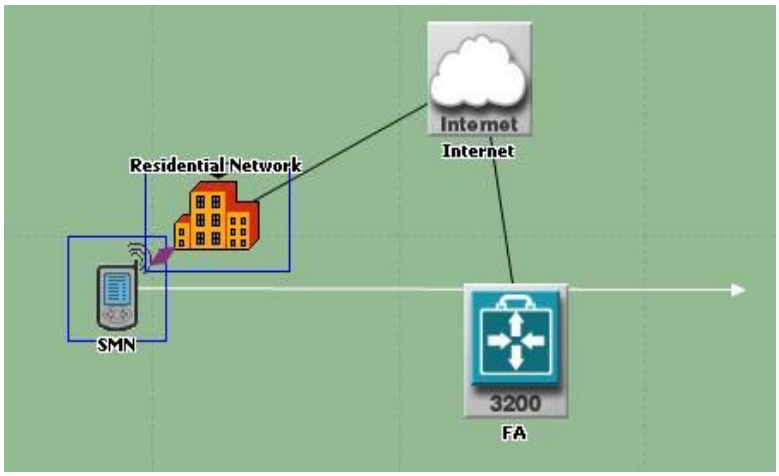

Figure 6.1 Simulation set up for roaming SMN of residential network

Both SMN and CN were configured with IPSec in transport mode

in CN_SMN scenario to reflect the conventional end-to-end security. Similarly, in CN_SRG_SMN scenario, two IPSec tunnels in tunnel mode were created between SMN and SRG; and between SRG and CN. As depicted in figure 6.1, the SMN roams from residential network to another network with foreign agent following the path of trajectory shown. In residential network the devices may be mobile or wired. CN was chosen as wired device connected to residential gateway through wired connection which communicates with the SMN despite the location of SMN in order to reflect since SMN is at home in order to reflect the feature of Residential network as shown in figure 6.2. The simulation was run for 15 minutes where the SMN which was communicating with CN in residential network roamed into foreign network at around 7 minutes and 30 seconds.

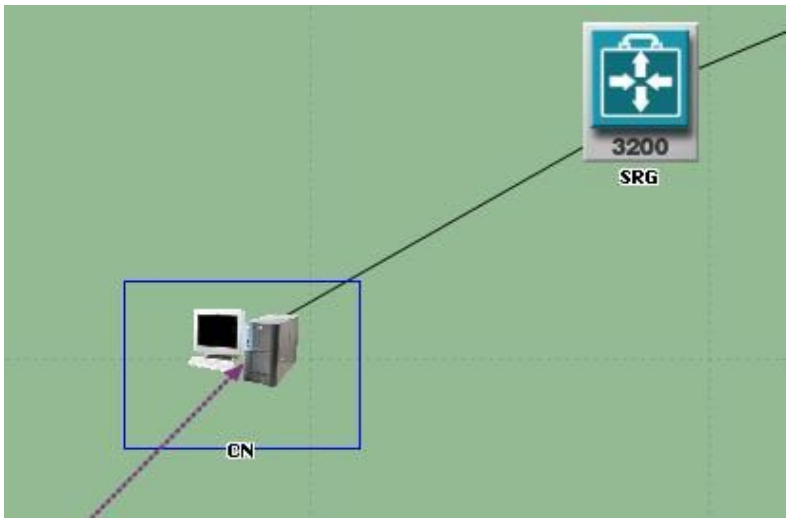

Figure 6.2 Residential network

The FA in figure 6.1 was used for broadcasting advertisement messages periodically, assigning CoA to roaming SMNs in its network and forward the messages sent by SMN and SRG. After getting CoA, SMN forwards Secure Registration Request to SRG using K_{MR} without having trust to FA. The foreign agent forwards the secure IP Registration Request packets received from SMN to SRG. SRG decapsulates the encapsulated packets using K_{MR} and based on the information retrieved it sends the Registration Reply encrypted with $K_{MR.}$ The FA again forwards the Secure Registration Reply to SMN. Using the SK_{MR} sent by SRG, both SRG and SMN can communicate securely over wireless links and internet. Similarly, using the secret key between CN and SRG, the messages between CN and SRG are encrypted making the communication a secure one. The simulation parameters set for security of residential network communication were set as shown in table 6.1 below.

Table 6.1. Simulation parameters

Authentication Algorithm	HMAC-MD5
Authentication Method	RSA Encrypted Nonces
Encryption Algorithm	3DES
IP Sec Protocol	ESP with authenication
SA Direction	Bidirectional
IKE Mode	Auto-negotiate

The HMAC-MD5 is the default authentication algorithm when using IPSec and hence used in the proposed protocol. RSA encrypted nonces are used to prevent form replay attacks. Both AH and ESP are used in bundle for authentication, encryption and confidentiality of data packets. The SA is maintained in both direction of tunnels. The 3DES is used as encryption algorithm because it is 3 times faster than the basic symmetric key encryption algorithm DES. As explained in chapter IV, the ESP protocol with authentication provides all security services offered by IPSec and hence implemented in the proposed protocol. The SA needs to bidirectional as this thesis focussed in implementing end-to-end security from CN to SMN via SRG and also from SMN to CN via SRG. The key distribution is not done manually in 손 proposed protocol and hence auto-negotiation feature is used while implementing IPSec in all residential devices for key distribution.

B. Results

In the proposed protocol SRG is overloaded with multiple tunnels. So the processing in SRG observed to see the effect of multiple IPsec tunnels. The processing power in SRG specially when SMN moved to foreign network was observed and found to be little higher

in proposed protocol than in conventional approach as depicted in figure 6.3.

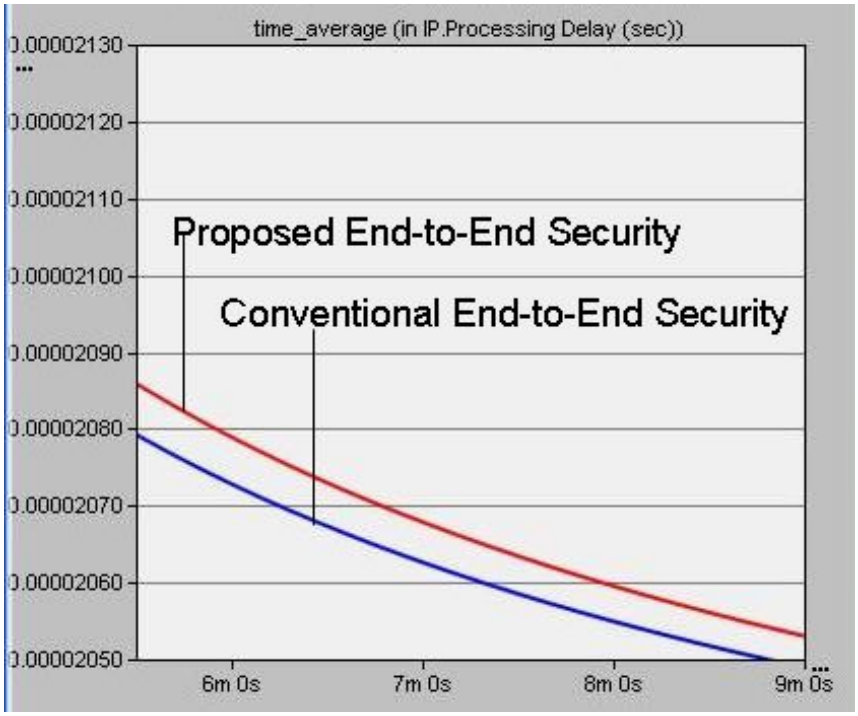

Figure 6.3 IP processing delay in SRG

The reason behind this due to the addition of IPSec encryption and decryption operations for 2 tunnels. However the increased delay was observed to was explored to be about 0.1 microsecond in proposed protocol due to high processing power of SRG. The more the number of residential devices, SRG has to maintain more security relationships with each residential device whether it is wired or wireless or mobile. This provision definitely overloads the

SRG with processing delay. Addition of security involves encryption and decryption methods and hence security incurs some processing time in every device which implements security and hence some delay is offered. Hence there is some kind of trade-off between security and processing delay in IPSec enabled devices and hence SRG is no option in our proposed security. As this thesis focussed on implementing security, the delay incurred is assumed to be tolerable. The increasing processing delay in SRG with more number of residential devices will be focussed in our future works with addtion of some QoS mechanims to decrease the processing delay in secure Mobile IP Communication in Residential Network.

The MAC delay in SRG is observed to be increased when SMN moved to foreign network in both scenarios as shown in figure 6.4. In proposed CN_SRG_SMN scenario, the link layer process is slower during the registration process due to the encryption and decryption of registration packets in SRG. However, the overall MAC delay in proposed scenario is always less in foreign network because of the short IPSec tunnels from SRG to SMN and from SRG to CN. Therefore the proposed protocol with end-to-end security apprach is better than the conventional end-to-end security approach is better than the conventional security approach. The breaking of long IPSec tunnel from SMN to CN into multiple tunnels showed improved SRG MAC delay. The additional multiple IPSec relationships of SRG with

SMN and CN has no effect in SRG MAC delay at all. Hence the proposed end-to-end security approach is better in terms of MAC delay in SRG.

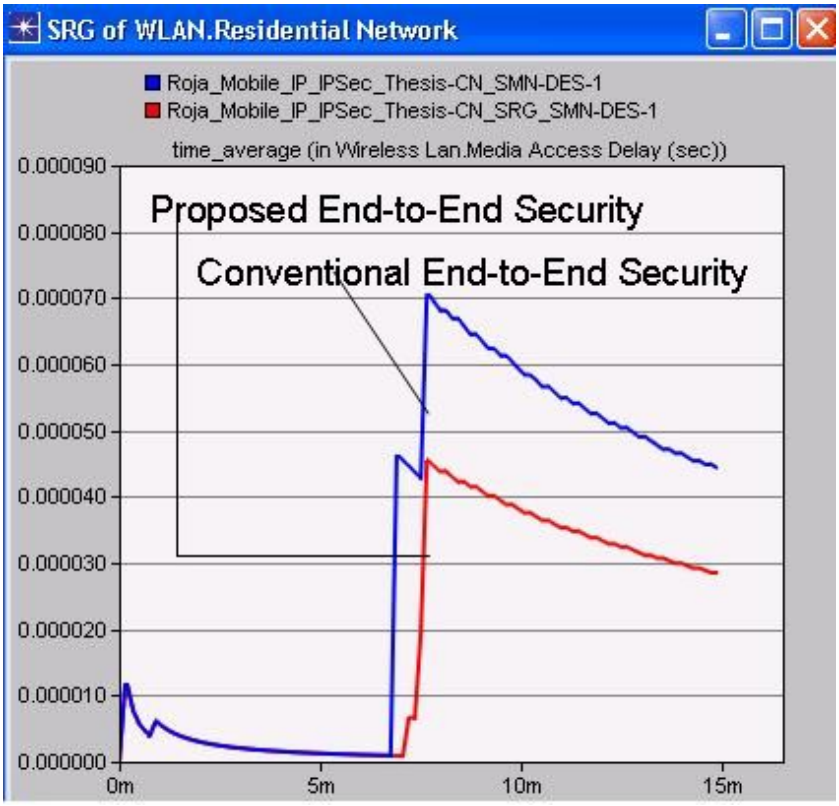

Figure 6.4 SRG MAC delay

The throughput in SMN is observed to be less in proposed scenario as shown in figure 6.5 because the long IPSec tunnel from SMN to CN is broken down into two shorter IPSec tunnels making SRG as the intermediate tunnel end-point to achieve end-to-end security. Hence encrypted communication from SMN to SRG results in

less throughput than in conventional approach from SMN to CN.

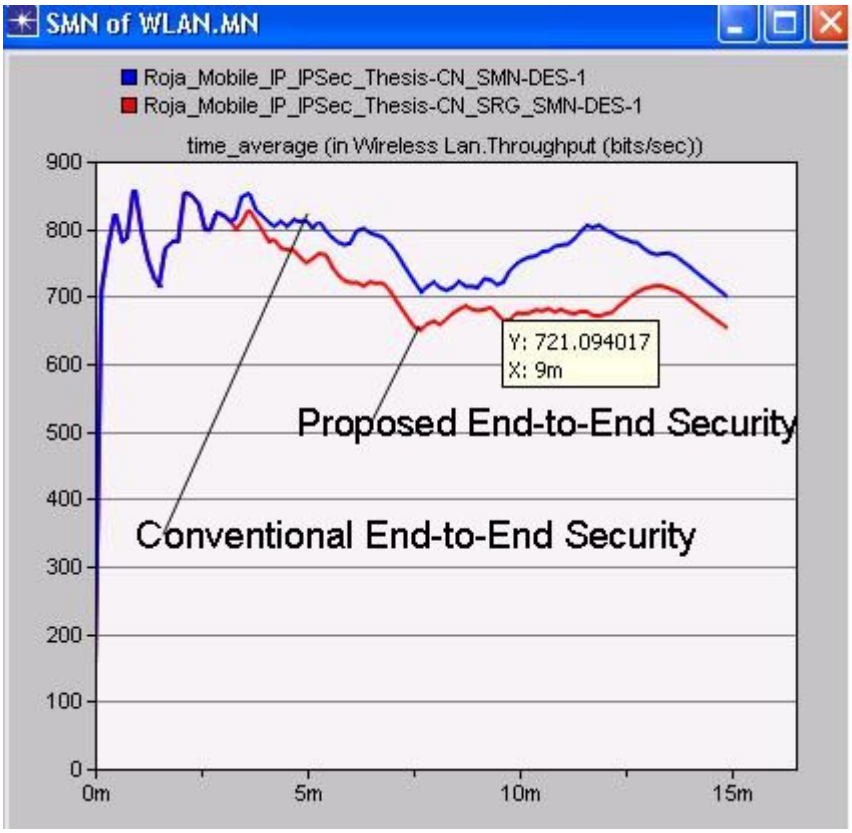

Figure 6.5 SMN throughput

The longer IPSec tunnel in conventional end-to-end security from CN to SMN has more throughput as the traffic is between CN and SMN only while in proposed protocol the overall traffic is flown from CN to SRG and finally to SMN and vice versa making the throughput load to be handled by theree important nodes. Hence the proposed protocol with end-to-end security approach is better than the

conventional end-to-end security approach is efficient in terms of throughput in roaming SMN in Mobile IP communication in Residential Network.

C. Security analysis of proposed scheme

As we have focused on securing mobile communication integrating IPSec with Mobile IP, the security benefits of the proposed protocol are briefly described below.

Scalability

This protocol does not require any security relationships between the residential network and any other foreign networks. So it can easily be extended to cover any number of networks. Hence this protocol seems to be scalable for residential devices roaming in any networks.

Efficiency

The protocol seems to be efficient in the sense that only two messages between the mobile node and residential gateway are involved and thus only the least amount of delay is incurred while establishing a connection at a new network. Furthermore, it exposes the network to the minimal increase in traffic.

Key Management

No secret keys are needed to be installed between the residential gateway and each foreign agent. Thus, key management becomes easier as compared to shared secret key management.

Integrity

Every registration message is encrypted and hence the resulting cipher text cannot be altered by any hackers. This ensures the integrity of messages reaching any destination.

Confidentiality

The proposed protocol sends the secret session key to the SMN to be shared and encrypted by their respective keys during a session. Hence this protocol maintains confidentiality too.

Authentication after Registration

The protocol authenticates not only during registration but also after registration since this protocol generates a new session key every time a new registration occurs. This session key acts as a shared authentication secret between the SMN and its SRG during session lifetime.

Ⅶ. Conclusion and Future Works

The implementation of IPSec in SMN and SRG is more secure as only the residential network's own devices are involved for its own private communication, the little delay incurred in processing of about 0.1 microseconds is not a concern for security. From the above simulation results and analysis, it is found that the proposed method is secure and efficient with less MAC delay and throughput. Hence using SRG as a tunnel end point for all the wired and mobile nodes in residential network is efficient and secure method than to protect with IPSec operations on separate HA nor FA. With IPSec enabled in mobile and wired devices of residential network, end-to-end security is achieved in proposed method taking the residential devices as CNs. However, the proposed Mobile IP Registration protocol can be used for CN beyond the residential network.

The simulation of the proposed secure Mobile IP registration protocol with end-to-end security with more number of mobile nodes to explore the effect of SRG processing delay with increase in number of mobile nodes is set for the future work. To reduce the overload in SRG, some QoS mechanisms will be used in future enhancements.

References

[1] G. W. Kim, D. W. Kim, J. H. Lee, J. B. Hwang, and J. W. Han, "Considerations on Security Model of Home Network", ICA0T2006, Feb. 20-22, 2006, pp. 109- 112

[2] Y. G. Jang, H. I. Choi, and C. K. Park, "Implementation of Home Network Security System based on Remote Management Server" on the proceedings of International Journal of Computer Science and Network Security (IJCSNS), VOL.7 No.2, Feb. 2007, pp. 267-274

[3] P. Krishnamurthy, and Joseph Kabara, "Security Architecture for Wireless Residential Networks", VTC 2000, pp. 1960-1966

[4] W. G. Lee, C. J. Char, S. K. Kim, M. Y. Kang, and J. K. Lee, " A Security Framework for Secure Home Networking in Ubiquitous Computing" on the proceedings of 2007 International Conference on Intelligent Pervasive Computing, pp. 394-397

[5] K. I. Chung, "Security Framework for Remote Access to Home Network" on the proceedings of 2006 International Conference on Hybrid Information Technology (ICHIT'06), Vol. 1, p.7

[6] S. G. Ungar, "Home Network Security" on the proceedings of IEEE Four International Workshop on Networked Appliances, Gaithersburg, Feb. 2002. pp. 41-48.

[7] M. H. Park, M. J. Beom, W. K. Park, Y. K. Jeong and E. H. Paik, "Implementation and Performance Evaluation of Hardware Accelerated IPSec VPN for the Home Gateway" on the proceedings of the 7th International Conference on Advanced Communication Technology,

ICACT 2005, pp. 1007-1010

[8] Z. Jiang, S. Kim, K. Lee, H. Bae, and S. Kim, "Security service framework for home network" on the proceedings of Computer and Information Science, 2005. Fourth Annual ACIS International Conference, Jeju, Korea, 14-16 July 2005, pp. 194-197

[9] P. Krishnamurthy, J. Kabara, and T. A. Amornkul "Security in wireless residential networks" , IEEE Transactions on Consumer Electronics, Vol. 48, No. 1, Feb. 2002, pp. 157-166

[10] C. R. Holliday, and P.E. ,"The Residential Gateway. A New Traffic Cop for the Home", New Telecom Quarterly, Technology Futures, Inc, 1996, pp. 24-29

[11] T. Saito, I. Tomoda, and Y. Takabatake, "Gateway Technologies for Home Network and Their Implementations" on the Proceedings of the 21st International Conference on Distributed Computing Systems, Apr. 2001, pp. 175-180,

[12] C. M. Chang and C. F. Liu, "The Study of Home Appliances Remote Control Based on OSGi" on the Proceedings of Int. Computer Symposium, Dec. 15-17, 2004, pp. 1134-1138

[13] J. G. Turnbull, "Introducing home area networks" BT Technology Journal , Vol 20, No 2, Apr. 2002, pp. 30-38

[14] C. S. In, Mobile IP Survey, 2006, www.cs.wustl.edu /~jain/cse574-6/ftp/mobile_ip.pdf

[15] Rathi S, and Thanushkodi K, "Performance Analysis of Mobile IP Registration Protocols", WSEAS Transactions on Computers, Issue 3, Volume 8, March 2009, pp. 538-548

[16] Torsten Braun, "Secure Mobile IP Communication" on the proceedings of the 26th Annual IEEE Conference on Local Computer Networks, 2001, p. 586

[17] TCP IP Guide, http://www.tcpipguide.com/

[18] S. Mink, F. Pahlke., G. Schafer, and J. Schiller., "Towards Secure Mobility 'Support for IP Networks", IEEE Publication, vol. 1, 21 August 2000, pp. 555-562

[19] William Stallings, "Cryptography and Network Security" Chapter 5, 4th edition, November 16, 2005

[20] T. Braun and Marc Danzeisen., "Access to Mobile IP Users to Firewall Protected VPNs" on the proceedings of Workshop on Wireless Local Networks at the 26th Annual IEEE Conference on Local Computer Networks, 2001

[21] J. K. Zao, and M. Condell, "Use of IP Sec in Mobile IP" Mobile IP Internet Draft, draft-ietf-mobileip-ipsec-use-0 0.txt, November 1997.

[22] A. Inoue, M. Ishiyama, A. Fukumoto and T. Okamoto. "Secure mobile IP using IP security primitives", IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1997, pp. 235 - 241

[23] Rafiqul Islam, "Enhanced security in Mobile IP Communication", Master of Science Thesis, Royal Institute of Technology, Stockholm University, Sweden, February 2005

[24] M. Barton, D. Atkins, J. Lee, S. N., D. Ritcherson, K. E. Tepe and K. D. Wong, "Integration of IP mobility and Security for Secure

wireless communication", Communications, 2002, ICC 2002, IEEE International Conference, Volume 2, pp. 1045-1049

[25] R. K. Basukala, D. Y. Choi, and S. J. Han, " A study on secure multi-home roaming in residential networks with IPSec", on the proceedings of the 8th KIIT IT based Convergence Service workshop and Summer Conference, 2009, June 12, p. E-17

[26] Dr. M. Mufti, and A. Khanum, "Design and Implementation of a Secure Mobile IP Protocol" on the proceedings of the Networking and Communication Conference, 2004. INCC 2004. International, 11-13 June 2004, pp. 53- 57

[27] Official Site of OPNET, http://www.opnet.com

Acknowledgement

This thesis is the outcome of two years of research work that has been carried out since I enrolled in Chosun University. It is my immense pleasure to humbly acknowledge my gratitude to the organizations as well as special people around me who were involved directly and indirectly in the preparation of this thesis.

Firstly I would like to convey my special gratitude to the **Institute of Information Technology Advancement** (IITA) under Ministry of Information and Communications, Republic of Korea for awarding me IITA Scholarship for financial support to study and to research in Korea. I am immensely indebted to **Chosun University** for waiving tuition fee and providing academic support to accomplish my study in Masters in Information and Communications Engineering.

I would like to express my deep and sincere gratitude to the Dean of College of Electronics and Information Engineering, **Prof. Seung-Jo Han** for his guidance, advice, and continuous support in Computer Network and Information Security (CNIS) Laboratory. I would like to show my gratitude to the Head of Department of Information and Communications Engineering, **Prof. Jong-An Park** for reviewing this thesis with precious suggestions. I gratefully owe special acknowledgement to my advisor **Prof. Dong-You Choi** for his sincere and continuous supervision, fruitful advice and excellent guidance in my research work throughout my entire course period. I extend sincere thanks to other professors in the Department f

Information and Communication Engineering for their encouragement during my study in Korea.

I am heartily thankful to **Dr. Binod Vaidya** for his supervision, advice, and guidance from the very early stage of this research. My special thanks goes to **Kishan Karmacharya, Anish Prasad Shrestha** and **Rakesh Shrestha** for the wonderful time we have spent together in Korea and supporting each other through sleepless nights of paper submission deadlines.

I appreciate the special support of **Dr. Sang Duck Lee and Han Kyoung-Heon** in editing this thesis and also for their immense help during my stay in Korea. Special thanks go to **Kyu-Jin Park**, **Seong-Jeong Yeop**, and **Ui-Hyoung Lim** for their tremendous help in laboratory activities and their personal help even in the days of my sickness. I cannot forget my roommates **Nana Kim**, **Meina Li** and **Young-Eun Jung** for their friendly love and care during my stay in dormitory and their special help in building my Korean language ability.

Finally, I am heartily indebted to my family and friends for their distant care, love and support throughout my studies. This thesis is specially dedicated to my father **Late Asha Kaji Basukala**, who had always been a source of inspiration in my life.

저작물 이용 허락서

학 과	정보통신공학과	학 번	20087735	과 정	석사
성 명	한글 로자 키란 바수카라 영문 Roja Kiran Basukala				
주 소	광주광역시 동구 서석동 조선대학교 전자정보공과대학 817호				
연락처	E-mail : rojakiran@hotmail.com				
논문 제목	한글 주택 네트워크에서 모바일 장치의 로밍 보안				
	영문 Secure Roaming of Mobile Devices in Residential Network				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건 아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함.
2. 위의 목적을 위하여 필요한 범위 내에서의 편집과 형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사 표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물 이용의 허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음.
7. 소속 대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의(○) 반대( )

2010년 2월 25일

저작자 : Roja Kiran Basukala (인)

조선대학교 총장 귀하