Secure and Fast Mobility Schemes for IP Multimedia Subsystem (IMS)

Submitted by

Shireen Tahira

56-FBAS/PhD-CS/F09

Supervisor

Prof Dr. Muhammad Sher

Department of Computer Science and Software Engineering

Faculty of Basic and Applied Sciences

International Islamic University, Islamabad

2017

ABSTRACT

This is the era of modern mobile technology that provides users to access different networks at any time and any where according to their situations and requirements. User Equipments (UEs) are designed to switch between different Access Networks (ANs) e.g. from WiMax to 3G or from Wifi to LTE. IP Multimedia Subsystem (IMS) promises a framework that provides services to all types of ANs. In 2020, 5G is promised to be on scene, and IMS is a candidate to provide its features to this as well. One of the features of IMS is to provide Quality of Service (QoS) to users. Due to mobility of user, UE handovers from one AN to another. This handover requires disconnection from current AN and then connection to a new. This leads to de-registration of UE in IMS and registration in IMS again after handover. In LTE-femtocell heterogeneous networks, handovers tend to occur more due to the decrease in the size of cells. Registration phase in IMS handles user's registration along with its authentication and authorization. This phase establishes IPSec Security Associations (SAs) between UE and entry point of IMS i.e. Proxy-Call Session Control Function (P-CSCF). If a UE handovers to new AN while having a session with a Corresponding Node (CN) then it has to undergo long process of registration, authentication authorization and establishment of IPSec SAsin IMS before resuming its session with CN. Meanwhile user of UE experiences delay in media disruption time and packet loss. The servers of IMS along with UE suffer the communication overhead. In other words QoS gets affected due to handover of UE to new AN. As one of the promises of IMS is to provide good QoS to users then there is a strong need to minimize media disruption time , loss of packets and communication overhead.

This thesis proposes a complete framework for mobility issues in IMS that resulted from UE's handover to new AN. It proposes two schemes for providing solution to the problems of sub phases of registration in IMS after handover. The first scheme caters with UE's registration with new IP address and P-CSCF, UE's authentication, UE's authorization and transfer of IPSec SAs to new P-CSCF in a secure manner. Second scheme deals with the establishment of new IPSec SAs between UE and new P-CSCF after handover with reduced number of messages and within SIP capabilities. We give solution for these issues by avoiding de-registration before

handover. Our scheme FIM (**F**ast **I**MS **M**obility) sends a proposed subsequent request from UE instead of conventional request to IMS servers that does not undergo the long phase of registration. Instead it gives a solution to do only necessary things needed after handover Proposed scheme caters registration with new IP address of UE and P-CSCF that takes care of authentication and authorization as well. FIM also transfers IPSec SAs from old server to new. For the establishment of new IPSec SAs, second proposed scheme EMSA (**E**fficient **M**echanism for **S**ecurity **A**ssociations) uses proposed subsequent request and response. It establishes IPSec SAs between UE and IMS after negotiating necessary parameters. Both schemes use already running protocols of IMS. The overhead of new protocol integration is avoided.

We analyzed the media disruption time, number of commands and packet loss of proposed scheme FIM theoretically as well as on a test bed developed by using an open IMS core (i.e. FOKUS) and compared the results with existing schemes. Transmission delay, processing delay and queuing delay of the establishment of IPSec SAs for our proposed scheme EMSA are also calculated theoretically and the results are compared with the old schemes. On the developed testbed we compared the delay and packet loss of EMSA with IMS scheme. Overall our proposed schemes FIM and EMSA outperform than existing schemes in terms of minimizing number of messages, media disruption time, packet loss and signaling delay.

CHAPTER 1

1. INTRODUCTION

This chapter gives the introduction of the IP multimedia subsystem and its important servers, Session Initiation Protocol, reference points between servers and user identities. Handover issues due to mobility of UE and the area of the research are also explained. In this chapter we raised the research questions and mentioned proposed solutions of the problems.

1.1. Next Generation Mobile Networks

The next generation of mobile networks (NGMN) consists of different technologies e.g. WiMAX [6], Wifi [8], LTE [7], VoLTE [50], VoWiFi [62] and 5G [63]. New appliances are equipped with the advanced features that facilitate user to roam freely. User can switch from one network to another due to any reason. One of the reasons could be the good signal strength of new network. But other reason could be the mobility of user from one area to another area where the coverage of old network is not present. Mobility of UE that leads to its handover from one network to another [10] must be facilitated by the networks as it has become a need of the era. It is user's demand to experience good quality of service (QoS) during mobility. Good QoS [64] is met when there is less media disruption and less packet loss.

These networks are expected to get services by IP multimedia subsystem (IMS) [1]. IMS framework is developed by 3gpp. IMS development is a collaborative work of two organizations. One of them is a leading organization related to cellular standards i.e. 3GPP [4] and other one is a leading organization for Internet standards i.e. Internet Engineering Task Force (IETF). IETF developed the basic technology and specifications of protocols. Whereas, 3GPP developed its framework and also integrated the protocols

so that it can get the capabilities of mobile systems. These capabilities could be roaming, Quality of Service (QoS) and charging [2].

1.2. IP Multimedia Subsystem (IMS)

Third generation (3G) networks have a packet-switched domain [65] that provides IP access to the Internet. IMS is the element in 4G architecture [66] that provides cellular access to the internet services and it is expected to be a part of 5G [61] as well. The main problem in using packet switched domain is that it doesn't provide a best service with QoS. There is no surety if the user gets the required amount of bandwidth that he/she needs for an application [2].

One of the features of IMS is to provide QoS to user. IMS does session establishment with Corresponding node (CN) in a way that it negotiate QoS so that user can have the required quality. So the IMS could be defined as a global and access independent architecture that facilitates users to get various types of multimedia services by using internet protocol.

The Session Initiation Protocol (SIP) as defined in RFC 3261 [3] is the application-layer control (signaling) protocol in 3GPP IMS networks for creating, modifying, and terminating sessions with one or more users. These sessions include multimedia calls between mobile users, telephone calls to the (Public Switched Telephone Network) PSTN, multimedia calls to users in the Internet, multimedia distribution, and multimedia conferences. SIP invitations can carry session descriptions that allow users to agree on a set of compatible media types.

Every user in the IP Multimedia Subsystem will have one or more public user identities. The public user identities are used by any user for requesting communications to other users. The public user identity takes the form of a SIP URL. A public user identity has to be registered either explicitly or implicitly (registered and de-registered simultaneously) before the identity can be used to originate IMS sessions or terminating IMS sessions can

be delivered to the user. A user can register several public user identities. The user can also register several IP addresses with a public user identity.

IMS entities can be divided into six categories [2].

1. Session management and routing family (CSCFs);
2. Databases (HSS, SLF);
3. Services (application server, MRFC, MRFP);
4. Interworking functions (BGCF, MGCF, IMS-MGW, SGW);
5. Support functions (PCRF, SEG, IBCF, TrGW, LRF);
6. Charging.

Figure 1.1 shows the handover scenario where UE disconnects from an old AN and connects to new one. It gets de-registered from IMS and gets registered in IMS after handover.

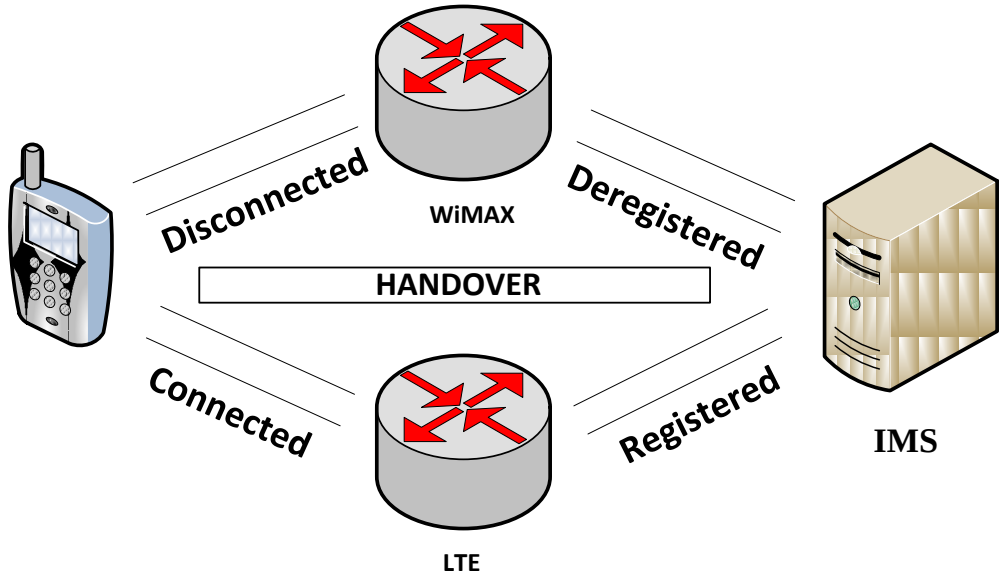

Figure 1.1: Handover Scenario

Few of the above entities those are in scope of this thesis are discussed below. These include CSCFs, Databases and SCC-AS.

1.2.1. Call Session Control Functions (CSCF)

There are four types of Call Session Control Functions (CSCF):

1. Proxy-CSCF (P-CSCF)
2. Serving-CSCF (S-CSCF)
3. Interrogating-CSCF (I-CSCF)
4. Emergency-CSCF (E-CSCF)

Each CSCF is responsible for its own specific tasks. P-CSCF, I-CSCF and S-CSCF are responsible for registration and session establishment and form the SIP routing machinery. These three CSCFs are defined below.

1.2.1.1. Proxy Call Session Control Function (P-CSCF)

Very first point of contact in IMS is P-CSCF. UE sends the SIP signaling traffic to the P-CSCF [11]. In a similar manner, P-CSCF sends the SIP signaling traffic that is being terminated to the UE. Four different tasks are appointed to the P-CSCF: SIP compression [14], IPSec security association, interaction with Policy and Charging Rules Function (PCRF) [12] and emergency session detection.

Being a text-based signaling protocol, the SIP protocol has larger message sizes as compared to the binary-encoded protocols. This is because the SIP protocol has a large number of headers and header parameters, along with the extensions and information related to security. If the UE requires compressed signaling messages, the P-CSCF would have to compress the messages for speedy session establishment [13]. Some of the responsibilities of the P-CSCF include maintaining Security Associations (SAs) and protecting the confidentiality and integrity of the SIP signaling. This occurs during the registration of the SIP as the UE and P-CSCF negotiate IPSec SAs. Integrity and confidential protection is applied to SIP signaling after registering the P-CSCF. The application of policy and charging control by an operator signals the P-CSCF to relay session and media-related information to the PCRF. The information that the PCRF

receives is used to develop the authorized IP QoS information and the rules that will be further delivered to the access gateway (e.g. GGSN [15]).

1.2.1.2. Interrogating Call Session Control Function (I-CSCF)

All connections destined to the subscribers of a network contact I-CSCF. Three different tasks are allocated to the I-CSCF:

1. It obtains the name of next hop from HSS e.g. S-CSCF or application server.
2. It assigns the S-CSCF based on the capabilities received from HSS.
3. It routes requests to next hop i.e. assigned S-CSCF or application server.

1.2.1.3. Serving Call Session Control Function (S-CSCF)

S-CSCF is the brain of IMS. It is responsible for doing registration processes, storing service profiles, making decisions to route and maintaining session states. A request sent by user goes to S-CSCF. S-CSCF downloads the authentication data from HSS. Based on this authentication data S-CSCF generates a challenge and sends to UE. When UE fulfills the challenge, S-CSCF accepts the authentication and registers it.

1.2.2. Databases

IMS architecture contains two databases: Home Subscriber Server (HSS) and Subscription Locator Function (SLF).

HSS is the main storage of data for all subscribers and service related data. The data stored in HSS includes user identities i.e. public user identity and private user identity, registration information, service triggering information and access parameters [17].

SLF resolves the address of HSS for I-CSCF, S-CSCF and AS. It resolves the address of HSS that keeps the subscriber's data for the user identity in a situation where more than one HSS are deployed by the operator of the network.

1.2.3. SCC-AS

After handover UE loses its session with the corresponding node, therefore 3gpp proposed an entity i.e. Service centralization and continuity application server (SCC-AS) [5] in order to continue session. When UE is completely registered with S-CSCF, then S-CSCF gets this UE registered in SCC-AS. It is part of the session between UE and CN. After handover, when UE gains new IP address, this SCC-AS is contacted to carry on the session between UE and CN. This ensures service continuity but the delay resulted in getting new IP address is still a problem. Also the issues related to new P-CSCF and handover latency are not resolved by this.

1.3. IMS Reference Points

IMS reference points between registration related entities are described in this section. Gm, Mw and Cx reference points are discussed below.

1.3.1. Gm Reference Point

Any UE that connects to IMS goes by Gm reference point. All the SIP messages that come from UE destined to IMS are transported by Gm. Similarly messages coming from IMS destined to UE go through Gm.

1.3.2. Mw Reference Point

The Mw reference point links the CSCF servers in IMS. Mw reference point is responsible for registration, session and transaction procedures.

1.3.3. Cx Reference Point

In order to fetch data from HSS or save data in HSS by CSCF servers is done through Cx reference point. The protocol that runs here is Diameter. The procedures include location management, user authentication and user data handling.

1.4. Identification

This section explains the identifiers of the users of UE in IMS i.e. public user id (IMPU) and private user id (IMPI).

1.4.1. Public User Identity

Public user identity (IMPU) is user's identity used for requesting communication with other nodes. It is used for initiating and receiving sessions from other networks. The requirements imposed by IMS [18, 19] for IMPU are:

1. The IMPU will be in the form of SIP Uniform Resource Identifier (URI) or tel URL i.e. telephone uniform Locator.
2. One of the IMPU must be stored in IP Multimedia Services Identity Module (ISIM).
3. UE will not be able to modify IMPU in ISIM.
4. Before starting any session, IMPU must be registered in IMS.
5. Before terminating any session, IMPU must be registered in IMS.

1.4.2. Private User Identity

The private user identity (IMPI) is provided by the home network operator. It is a unique identity used within the home network [18]. In fact it identifies the user's subscription rather than the user's identity. That is why it is used for authentication of user. Requirements imposed by IMS for IMPI are [18, 19]:

1. IMPI will take the form of Network Access Identifier (NAI) [16].
2. IMPI will be included in all registration processes.
3. IMPI will be authenticated during registration of user.
4. S-CSCF must store IMPI on registration and termination.
5. IMPI will not be used for SIP messages' routing.
6. The IMPI will be stored in ISIM and allocated to user permanently. It will be valid till the termination of user's subscription in home network.

7. UE will not be able to modify the IMPI in ISIM.
8. The HSS must need to store the IMPI.
9. IMPI will optionally be the part if charging records.

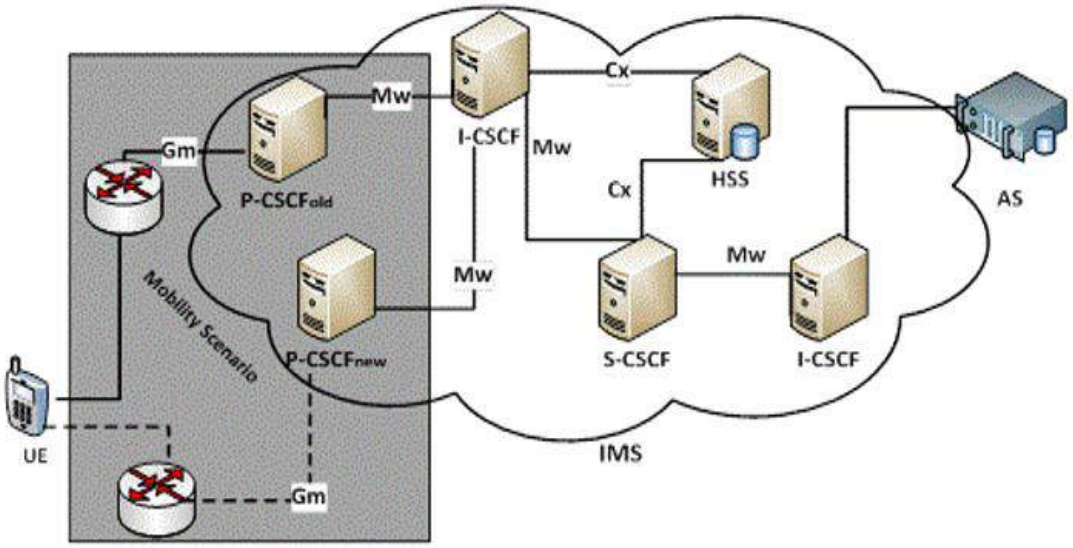

Figure 1.2: Mobility handover Scenario in IMS

When UE changes its point of attachment, it gets de-registered from its old P-CSCF. On getting connected to new point of attachment it registers in P-CSCF again. This P-CSCF may be the old one or may be the new one. Figure 1.2 shows the mobility handover scenario in IMS along with its main servers where UE connects to new P-CSCF shown by dotted line.

1.5. Problem Statement

New ubiquitous mobile devices have more than one option for the users to switch between different access networks so that they can have a continuous flow of internet data. While moving from one place to another, a user can switch to another available network by performing either horizontal or vertical handover. It takes time for a mobile device to get connected to new access network and then to get registered in IMS after a handover. If a device is in a session with a Corresponding Node (CN) before handover then it may experience poor QoS i.e. delay in media disruption and loss of packets.

Due to handover, the User Equipment (UE) gains new IP address in new AN and registers to a new P-CSCF in IMS. The main protocol of IMS is SIP that doesn't give solution to the "change of IP address" issue of UE after handover. In literature, researchers gave solutions to integrate MIPv6 with IMS to solve the issue of new IP address of UE after handover. MIPv6 is a protocol that gives the solution for mobility issues on layer 3. Integration of MIPv6 in IMS is problematic that is explained in [22]. It also causes more media disruption time and number of messages.. There is a need to resolve the issue of "change in IP address" of UE within SIP so that the overhead of new protocol integration in IMS can be avoided. In literature, delay of handover is proposed to reduce by integrating other protocols in IMS e.g. FMIPv6 and MIH. FMIPv6 has same integration issues and it is meant to reduce delay at layer 3. Similarly MIH gives a mobility solution at layer 2. As IMS is a framework for different kinds of next generation networks, there is a need to have solution for change of IP address of UE and handover delay within IMS registration phase. Registration phase of IMS is coupled with authentication and authorization of UE. We have realized that there is a strong need to give solution for registration of UE with new IP address in IMS along with authentication and authorization of UE in IMS after handover. There is a need to securely transfer IPSec SAs to new P-CSCF after handover as well. This needs to be done with reduced media disruption time, less number of commands and packet loss.

In every Registration UE and P-CSCF establish IPSec SAs (Security Associations) with each other after negotiating security parameters. To our knowledge there is no method to establish IPSec SAs between UE and new P-CSCF after handover by negotiation of security parameters i.e. algorithms, mechanisms and supported ports between two entities. In literature context transfer based solutions are proposed after handover. Such solutions do not provide the facility to negotiate security parameters between UE and new P-CSCF. There is a need to give solution for establishment of IPSec SAs between UE and new P-CSCF after handover that reduces delay and number of messages within SIP capabilities.

1.6. Research Questions

Research questions of this thesis are as follows:

1. How to reduce no. of messages in registration, authentication, authorization and SA establishment after handover?
2. How to handle new IP address of UE after handover?
3. How to handle if P-CSCF is changed after handover?
4. How to transfer of IPSec SAs to new P-CSCF
5. How to do IMS part efficiently in case of mobility?
6. How to establish IPSec SAs between UE and new P-CSCF after handover.

1.7. Research Objectives

There is a need of a complete new framework for mobility scenarios that handles registration, authentication, authorization and transfer of IPSec SAs from old P-CSCF to new P-CSCF. The registration of UE in IMS must be done with the changed IP address of UE that is obtained in new AN. After handover the P-CSCF could not be the old one so this scheme must cater the registration with new P-CSCF also the IPSec SAs must be transferred to new P-CSCF. Authentication and authorization phases along with registration phase should be carried out. All of these phases need to be done with in IMS i.e with already running SIP protocol.

Establishment of IPSec SAs between UE and new P-CSCF need to be done after handover. Negotiation of security parameters and transfer of key to new P-CSCF need to be done in a secure manner. This should be done within SIP capabilities.

All above issues are needed to be done in less number of messages and with improved QoS.

Figure 1.3 shows the research scope of our thesis

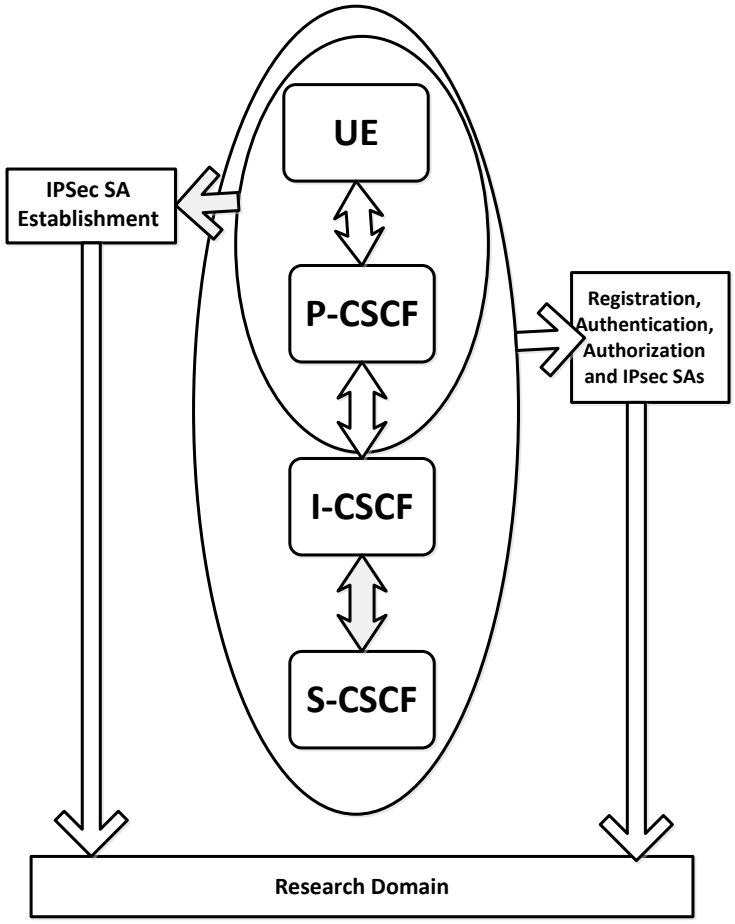

Figure 1.3: Research Scope

1.8. Research Domain

Our thesis research domain is forked into two in terms of handover of UE. First one is the registration, authentication and authorization of UE with new IP address in IMS. It also includes the transfer of IPSec SAs to new P-CSCF after handover. It involves UE, P-CSCFs, I-CSCF and S-CSCF. Second part is the establishment of IPSec SAs between UE and new P-CSCF after handover. It involves UE and P-CSCFs. This can be shown in figure 1.3. These two areas are more elaborated in figure 1.4.

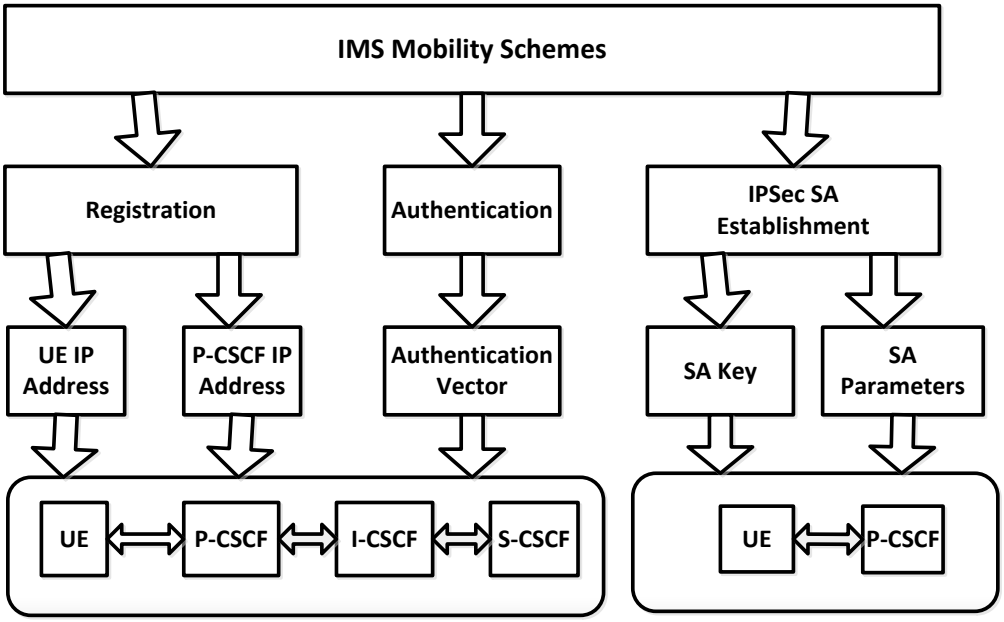

Figure 1.4: Proposed Framework for issues after handover

1.9. Thesis organization

Thesis includes five chapters. Chapter one gives the introduction that what the problem is. What is the area of research and what are the objectives and goals of research. Chapter two gives the related work of schemes proposed for similar problems. Chapter three covers the scheme "FIM" proposed to deal with registration phase along with authentication and authorization. It also gives the proposed methodology along with results. Chapter four gives a scheme for establishing IPSec SAs, its evaluation and results. Chapter five is about the conclusion and future work. Figure 1.5 shows the thesis outline.

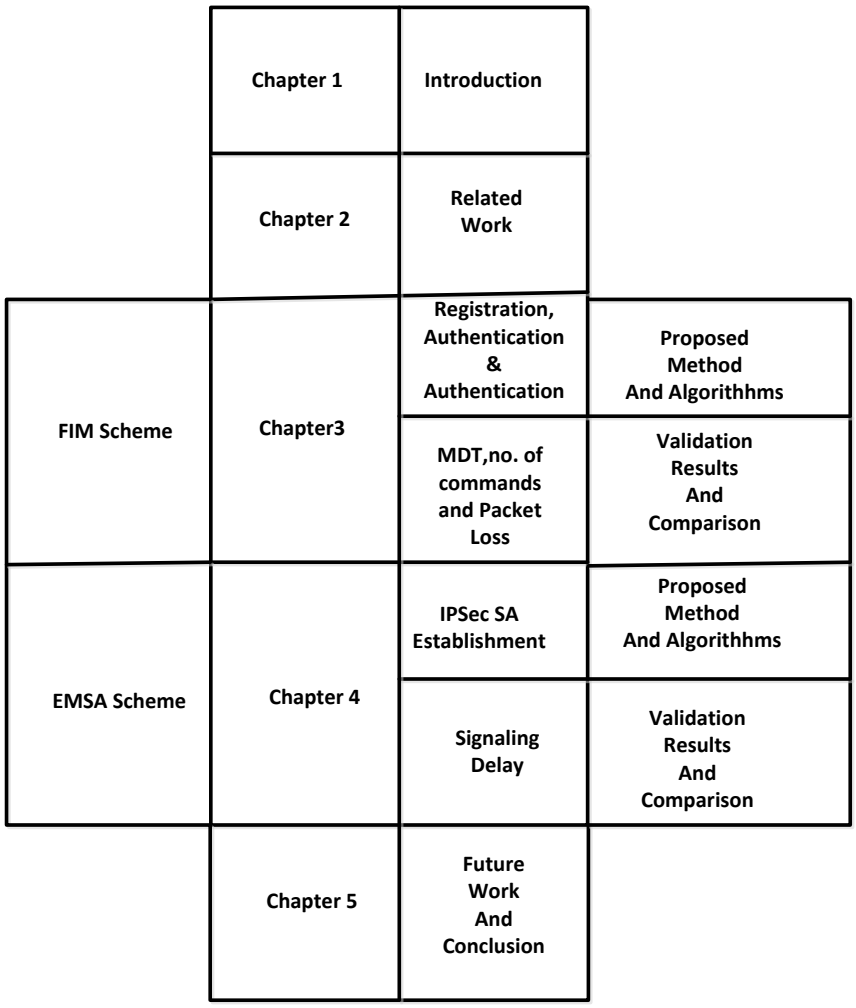

Figure 1.5: Thesis Organization

CHAPTER 2

2. RELATED WORK

2.1. Background

This section deals with the background knowledge of IMS phases that involves with handover. It explains that how UE gets de-registered from IMS and then re-registers in IMS again. The authentication and authorization phases are also defined here. During de-registration, IPSec SAs also drops between UE and old P-CSCF. Then on registering again how IPSec SAs are established between UE and P-CSCF after handover in standard IMS procedure.

2.1.1. De-Registration

UE can be de-registered from its home network in IMS. De-registration could be user initiated or network initiated. In case of user initiated de-registration, UE sends REGISTER request with expire value equals to zero in "Contact" header to P-CSCF. P-CSCF further sends it to I-CSCF. I-CSCF asks the HSS for the S-CSCF address that was assigned to the user by sending UAR (User Authorization Request). HSS gives I-CSCF the address of S-CSCF by sending UAA (User Authorization Answer). And finally the REGISTER request reaches to S-CSCF. Here UE gets de-registered. S-CSCF sends a 200 OK response back to UE with expire value equals to zero. Figure 2.1 shows the user initiated de-registration process whereas figure 2.2 shows the network initiated de-registration process.

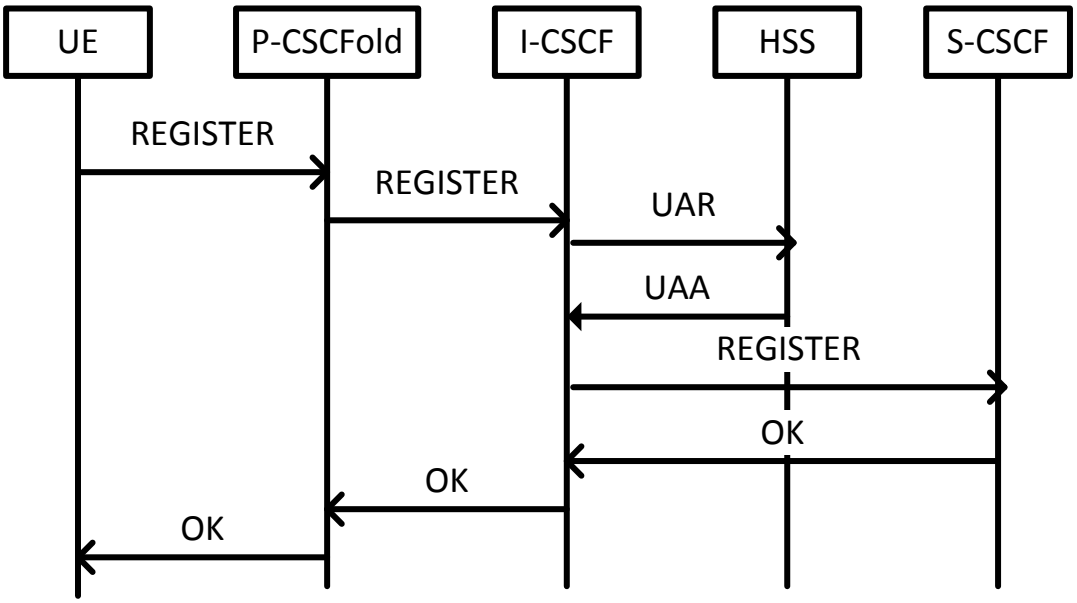

Figure 2.1 User Initiated De-Registration in IMS

In network initiated de-registration, S-CSCF sends a Notify to old P-CSCF and UE. It notifies that due to any reason system is de-registering UE. Figure 2.2 shows the network initiated de-registration phase. After handover to new AN, UE gains a new IP address by GGSN. Then GGSN notifies the HSS with the new pair of MSISDN/IP address. HSS initiates a de-registration phase here according to TR 33.878.

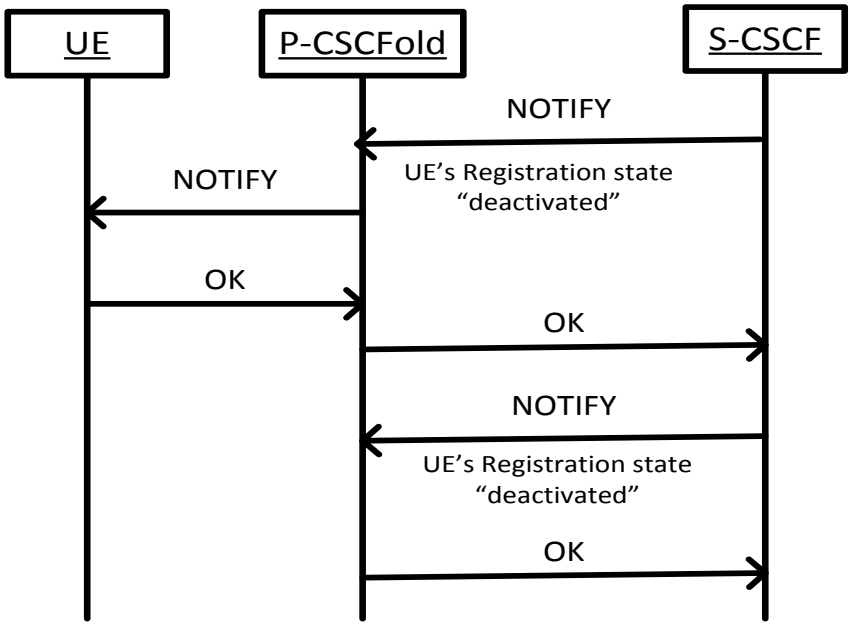

Figure 2.2 Network Initiated De-Registration in IMS

2.1.2. Registration

When user gets registered to IMS, it enters in it through P-CSCF. In the registration process shown in figure 2.3, a REGISTER [4] request is sent to the P-CSCF. This request is processed by P-CSCF and then IP address of I-CSCF is resolved. I-CSCF contacts the HSS for the selection of S-CSCF and gets its name by UAA and UAR messages. After selecting it, the REGISTER request is sent to S-CSCF from I-CSCF. S-CSCF sends MAR (Multimedia Authentication Requests) to HSS for authentication Vectors (AVs) of this UE. HSS sends AVs by MAA (Media Authentication Answer) to S-CSCF. Then if the S-CSCF doesn't find out the authorization of user, it challenges the UE by sending (401) Unauthorized response. The UE calculates a response and sends the REGISTER request again. S-CSCF compares the RES with XRES. On the true match of RES with XRES, UE is authenticated. S-CSCF sends Server Assignment Request (SAR) to HSS to inform the allocation of S-CSCF. HSS sends Server Assignment Answer (SAA) to S-CSCF. Registration is complete when (200) OK response is sent back to the UE from S-CSCF. After handover to new AN, UE has to undergo this registration phase once again.

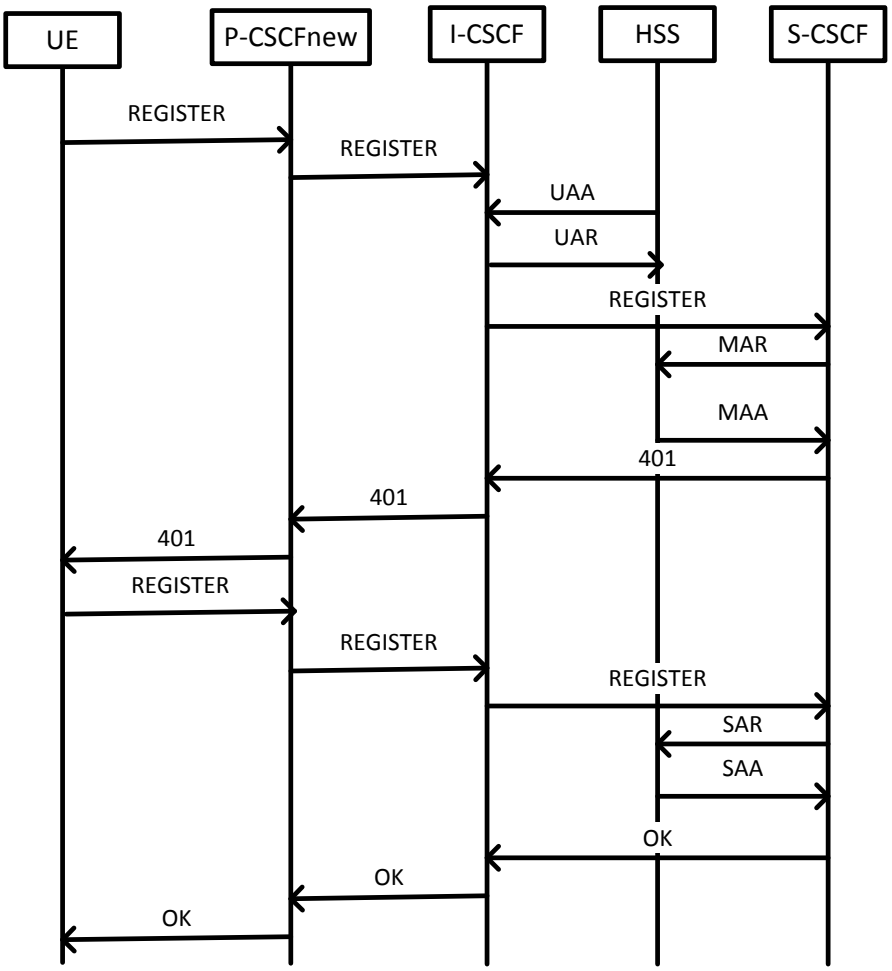

Figure 2.3 Registration in IMS

2.1.3. Authentication

Registration and authentication processes are coupled in IMS. Figure 2.4 shows the authentication phase. It is carried out by the help of a shared secret and a sequence number (SQN). Shared secret and SQN is known by HSS and ISIM application on the universal integrated circuit card (UICC) card in UE. When first REGISTER request is sent from UE to S-CSCF, S-CSCF downloads the Authentication Vector (AV) from the HSS for this UE. AV includes following vectors:

1. A random challenge (RAND)
2. The expected result (XRES)
3. The network authentication token (AUTN)

4. The integrity key (IK)
5. The ciphering key (CK)

S-CSCF performs authentication by the help of these AV parameters without knowing shared secret and SQN. S-CSCF sends (401) Unauthorized response back to UE along with these AV parameters. UE calculates the result (RES) based on RAND and the shared secret. Now UE sends second REGSITER request to S-CSCF along with authentication challenge response (RES). S-CSCF compares this RES with XRES. If it is verified then S-CSCF treats the UE authenticated. And the registration process completes in this way. This registration phase along with authentication is carried out once again when UE handovers to new AN.

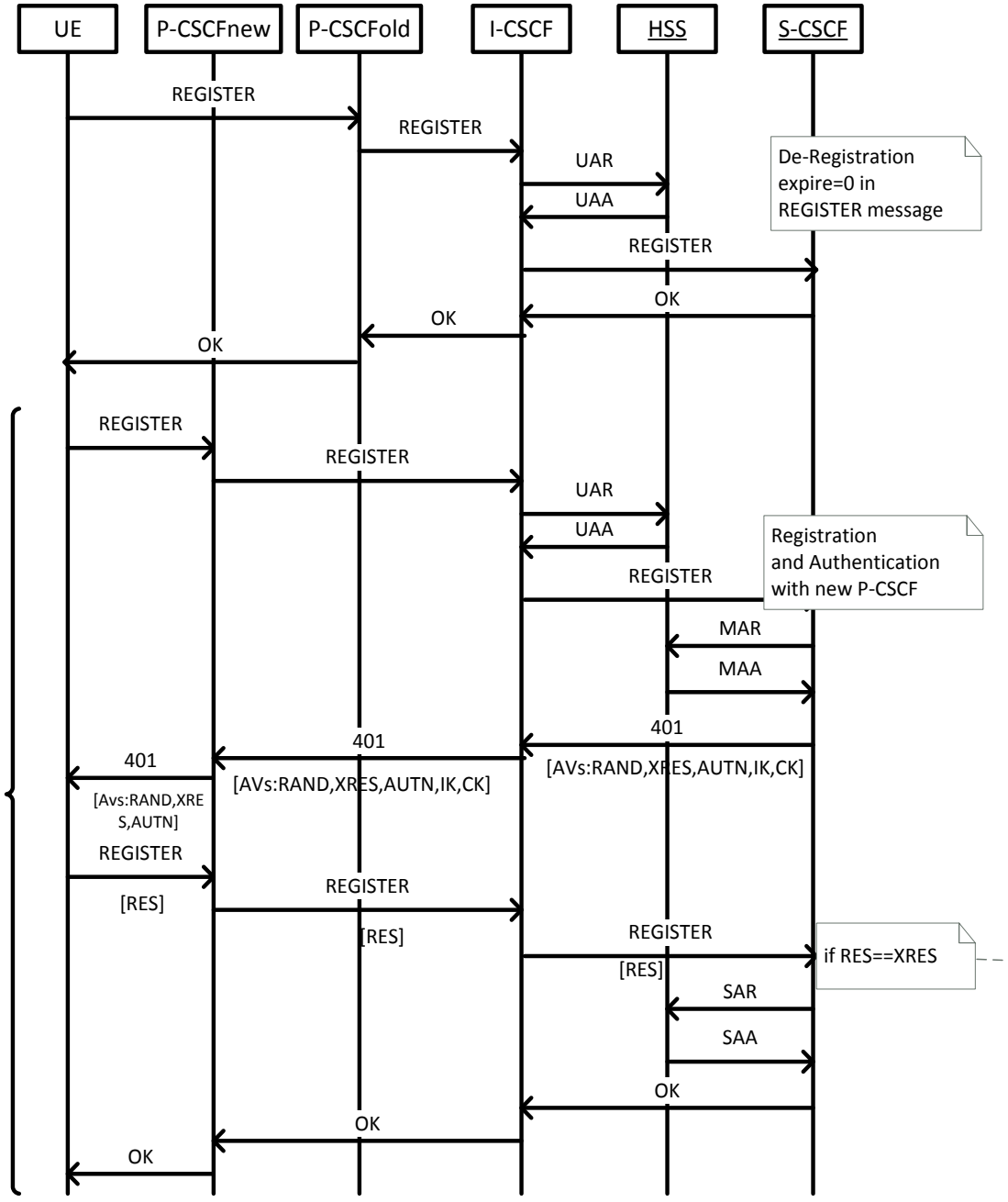

Figure 2.4 Authentication process inside registration

2.1.4. Authorization

Authorization is assured between UE and P-CSCF. P-CSCF receives REGISTER request from UE. But initially P-CSCF is not sure whether this request is coming from the UE or not. UE and P-CSCF establishes IPSec SAs after initial REGISTER and(401) response. The second REGISTER request goes from this established IPSec tunnel. In this way P-CSCF is sure that the request is coming from authorized UE. The P-CSCF puts "yes" to "integrity-protected" filed in Authorization header of REGISTER request as shown in figure 2.5. After handover UE has to undergo this phase as well.

```
REGISTER sip:home1.fr SIP/2.0
Authorization: Digest username = "user1@home1.ims,
                realm = "home1.ims",
                nonce=A34cm+vghfgfgh, algorithm = AKAv1-MD5,
                uri=sip:home1.ims",
                response="76875675645645765fgdgfdgf8979878978789",
                integrity-protected="yes"
```

Figure 2.5 REGISTER request with Authorization

2.1.5. Routing-related headers in REGISTER message

REGISTER message is sent from UE to S-CSCF through P-CSCF and I-CSCF. Some of its headers needed for routing are described below.

Via header is used by each SIP entity that puts its IP address in it during routing of requests.

Route header is used by each entity that puts the IP address of next hop during routing of requests.

Path header is used by P-CSCF which adds its IP address in it during REGISTER request that is sent to S-CSCF.

Service-Route header contains IP address of S-CSCF that is calculated during REGISTER request routing for the routing of initial request.

Figure 2.6 shows the REGISTER message. Once a UE is registered, it could send an initial request such as INVITE to the corresponding node in order to establish a session with it. The UE loads the IP address of its P-CSCF and S-CSCF in *Route* header of INVITE request. It gets these addresses from *path* and *service-route* headers respectively that were set during registration process [8].

```
REGISTER sip:home1.fr SIP/2.0
Via: SIP/2.0/UDP [5555::1:2:3:4];branch=0uetb
Route: sip:[5555::a:f:f:e];lr
Max-Forwards: 70
From: <sip:user@home1.fr>;tag=pohja
To: <sip:user@home1.fr>
Contact: <sip:[5555::1:2:3:4]>;expires=600000
Call-ID:ahdkhskd4984jeij
CSeq: 20 REGISTER
Content-Length: 0
```

Figure 2.6 REGISTER message

2.2. IPSec Security Associations

Security Association (*SA*) is a relationship between two entities that describes the way in which communication is going to be secure. It includes the authentication and encryption algorithms they agree on. Two *SAs* are used for bidirectional flow of data, one is for receiving and other is for sending purpose. Figure 2.7 shows the *IPSec SAs* establishment between two nodes.

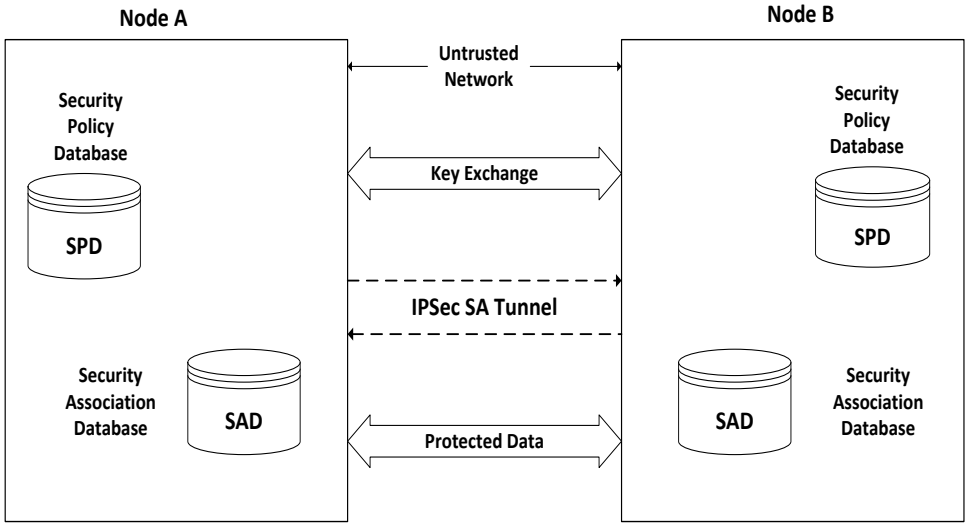

Figure 2.7 Establishment of IPSec SAs between 2 nodes

IPSec [40, 69] provides confidentiality and integrity at third layer with the help of two protocols i.e. Authentication Header (AH) [41] and Encapsulating Security Payload (ESP) [42] and through using a symmetric key. IPSec SAs (security associations) are established between two nodes for secure exchange of data. SAs operate in transport mode where only packet's payload is encapsulated and tunnel mode where the entire packet is encapsulated. Key exchange could be done by IKE [43] or without IKE i.e. manual keying. IMS uses IPSec SAs on Gm interface between UE and P-CSCF. Security mechanisms used in IMS is ipsec-3gpp [44] whereas there are number of security mechanism used for VoIP networks i.e. IPSec-ike, ipsec-man, digest and TLS [67]. Transfer of security associations during handover is a hot issue [68] found in survey.

During registration phase in IMS, IPSec SAs are established between UE and P-CSCF. This IPSec SAs are used to protect integrity of two entities. There are 4 messages used for registration and authentication phase. During this process, IPSec SAs are also established between UE and new P-CSCF.

2.1.6. IPSec SAs between UE and P-CSCF

The Security Associations are established by negotiating security parameters and algorithms in Register request. It uses three headers namely security-client, security-

server and security-verify. IPSec SAs are established after successful authentication of UE. It shows that SAs between UE and P-CSCF are established when process of registration and authentication completes.

One of the SAs is established between the UE's client port and P-CSCF's server port. And second SA is established between the P-CSCF's client port and UE's server port. Traffic flows in both direction. The UE and P-CSCF use the same two REGISTER requests for negotiations of IPSec parameters those used for registration and authentication. The UE adds a Security-Client header field in REGISTER request. UE adds security mechanism, authentication and encryption algorithm in this header those supported by itself. UE also adds its client port from that it will send requests and server ports on which it will receive responses. Figure 2.8 shows a REGISTER request with security-client header. It shows that UE supports digest and IPsec-3gpp as security mechanisms and HMAC SHA 1-96 [45] algorithms for IPSec encryption and protection. Protected client port and protected server port used from its end for IPSec SAs and SPIs related to these ports are also mentioned.

```
REGISTER sip:home1.fr SIP/2.0
Via: SIP/2.0/UDP [5555::1:2:3:4];branch=0uetb
Route: sip:[5555::a:f:f:e];lr
Security-Client: digest, IPsec-3gpp; alg=hmac-sha-1-96;
                 spi-c=23456789 ;spi-s=12345678
                 ;port-c=2468; port-s=1357
Contact: <sip:[5555::1:2:3:4]:1357>;expires=600000
```

Figure 2.8 Register Request with security-client

Then the P-CSCF adds a Security-server header to the 401 response that is going to UE. P-CSCF adds the security mechanisms, authentication and encryption algorithms that it supports. P-CSCF adds q-value to each mechanism that shows the preference. Figure 5.2 shows 401 Response with security-server header. This 401 response is coming from S-

CSCF that has Authentication Vectors (AVs). P-CSCF obtains and removes integrity and encryption keys (IK and CK) from (401) response. IK is the key that is used for SAs establishment. SAs are now ready to be used and the next REGISTER request goes over these SAs. Figure 2.9 shows 401 response along with security-server and WWW-Authenticate headers [2].

```
SIP/2.0 401 Unauthorized
Security-Server: tls ;q=0.2, IPsec-3gpp; q=0.1;alg=hmac-sha-1-96
                 ;spi-c=98765432 ; spi-s=87654321
                 ;port-c=8642 ; port-s 7531
WWW-Authenticate: Digest realm="home1.fr",
                  nonce=A#$GGRTREGFG, algorithm=AKAv1-MD5,
                  ik="0123456789poiuytewqasdfghjkjhgfvb"
                  ck="987654321aasdfghjjjjklkjhghjkjhghhh"
```

Figure 2.9 401 Response Message

This second REGISTER request from UE contains a header security-verify that contains the parameters of security-client and security-server to P-CSCF i.e. the mechanisms, the authentication algorithm, the encryption algorithm, SPIs and port numbers. The SAs' establishment will be completed when UE is authenticated. It happens when UE gets a 200 response from S-CSCF. Lifetime of SAs is 4 minutes when the process of registration and authentication is going on. After successful completion of authentication, lifetime is set to the time of registration of UE plus 30 seconds. The time of registration of UE is in *contact* header in (200) Ok response. Figure 2.10 shows the establishment of SAs during IMS registration and authentication process.

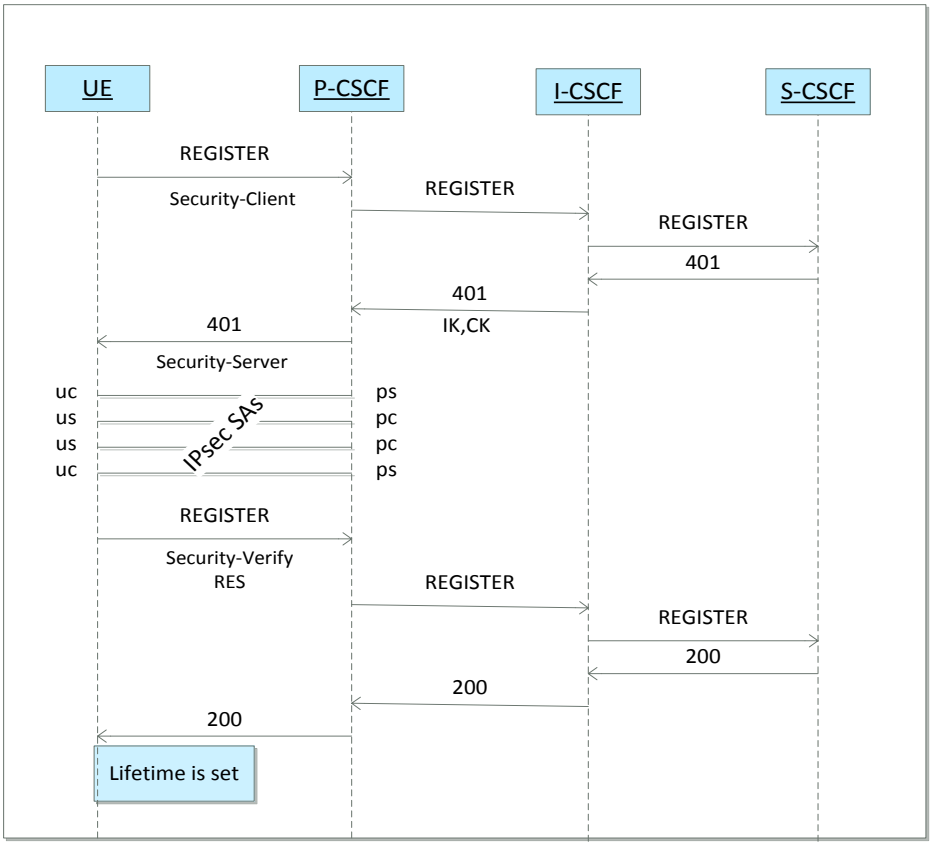

Figure 2.10 IMS Registration and SA establishment

2.1.7. De-Registration and SA drop

When UE changes it's AN, it gets de-registered from IMS. Due to de-registration, the IPSec SAs that were previously established between UE and old P-CSCF also dropped. Figure 2.11 shows the phase of de-registration and drop of SAs.

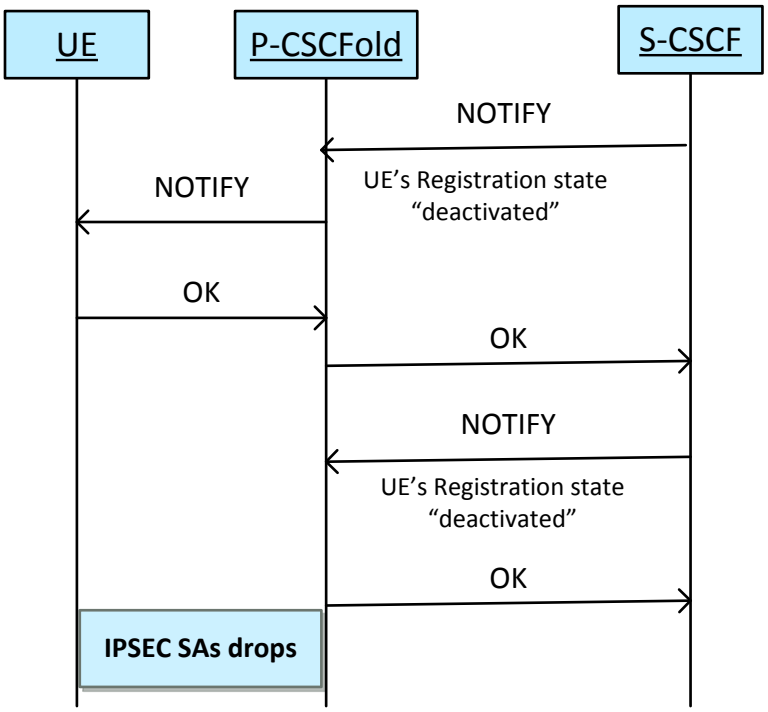

Figure 2.11 De-Registration and SA drop

2.1.8. Context Transfer Protocol based Approach

In CXTP [46] approaches, new P-CSCF request old P-CSCF to transfer context of SAs. Old P-CSCF transfers the SAs context to new P-CSCF. New P-CSCF acknowledges to old P-CSCF about the transfer of SAs. IMS registration phase is still done for the registration of UE. Figure 2.12 shows CXTP in IMS scenario.

Most common methods in literature are using context transfer protocol to transfer the SAs from old P-CSCF to new P-CSCF. We will explain the context transfer protocol approach here firstly with IMS. In coming sections we will discuss the transmission delay, processing delay and queuing delay.

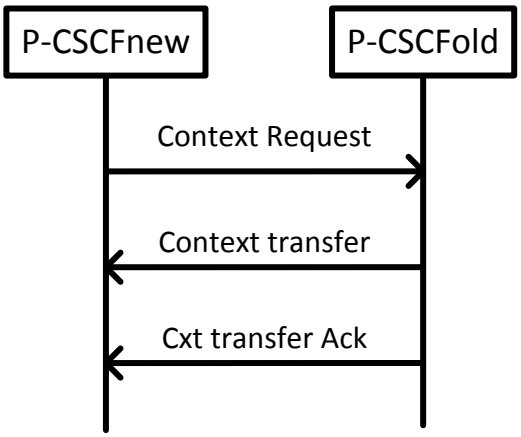

Figure 2.12 Context transfer between old P-CSCF and new P-CSCF

2.2. Related Schemes

In this section, we have reviewed the different schemes for handover scenarios and related functionalities for IMS. Related schemes are discussed under different categories including media disruption time (MDT) reducing schemes where the related schemes target to reduce the disruption time during the handover process. It is further sub divided into new protocol inclusion based schemes, context transfer, pre-processing and simultaneous processing based schemes. After that change in IP address based schemes are discussed. Moreover, packet loss improvement and reduction in commands based schemes are also discussed. These schemes also target to minimize latency of handover phase by integrating mobility protocols with IMS. Few techniques proposed to reduce number of messages for registration and session establishment phase in order to reduce latency caused by handover as discussed in following section.

Due to mobility, UE changes its P-CSCF that leads to drop of IPSec SAs between UE and old P-CSCF. Researchers gave the solution for this problem as well that is discussed in this chapter. Researchers suggested reducing message signaling for UE registration in IMS that is also important to reduce latency.

2.3. Change of IP address of UE

Change of IP address of UE happens when it disconnects from current access network and connects to new access network. As SIP doesn't cater this issue, the schemes proposed in [20-22] suggested integrating MIP in IMS.

MIPv6 [24] is a layer 3 protocol that hides the mobility of UE to upper layers. It assigns and hides the care of address (CoA) and keeps the record in Home Agent (HA). it always shows home address (HoA) of UE to the upper layers. Change of IP address of UE is handled by this approach but there are integration issues mentioned in [23].

2.2. MDT reducing schemes

MDT minimization is really important issue in mobility scenarios. It effects quality of service (QoS) in any way. Many techniques proposed solution to reduce delay of handover. FMIPv6 [25] is suggested to integrate in IMS instead of MIPv6 as it reduces layer 3 delay already. The schemes proposed in [26][27] utilized FMIPv6 protocol to reduce the media disruption delay at layer 3..

In literature we have found out that different solutions are proposed to reduce media disruption time caused by handover in IMS.

2.2.1. Context Transfer based Schemes

K. Larsen et al. [28] proposed a technique to reuse the information and states of session in old P-CSCF. This scheme transfers this context from old P-CSCF to new P-CSCF. In this way handover delay is reduced.

The scheme introduced by T. Renier et al. [29] uses a novel type of Packet Data Protocol (PDP) context which is a combination of primary and secondary PDP context. This new PDP context is used for signaling as well as data flow. This scheme utilizes AuthToken that comes from old Policy Decision Function (PDF) at which the user was attached before mobility. AuthToken is added to the new type of PDP context request in order to

transfer all resources allocation context. The request is sent to old PDF, it recognizes the AuthToken and searches its database for the ongoing session's states, user's profile and authorized QoS levels in the user's old network. The authors suggested using MIPv6 to quickly inform the corresponding node about the user's new location. In this way packets will not be lost. Number of messages is reduced thus reducing the latency. To secure the transfer of AuthToken, encryption and timestamps are suggested by the authors.

There are two schemes presented to transfer context to support seamless handover and two schemes to transfer context for QoS parameter negotiations by Farahbakhsh et al. [26]. These schemes are either predictive or reactive for FMIPv6 handovers. In predictive schemes, due to FMIPv6 and Neighbor Discovery (ND) [25], user knows in advance that towards which router it will move, it anticipates the transfer to the new access router. The mobile node sends a Move-notify message to its P-CSCF that contains the address of new router, the id of context to be transferred for seamless handover. Now the tunnel is established between new access router and old access router, new P-CSCF requests old P-CSCF for QoS parameter negotiations. The context of QoS parameters are sent to new P-CSCF and new access router. Here authors utilized movement anticipation, tunneling and transfer of context for reducing handover latency as well as QoS parameters. Here context transfer is running simultaneously with FMIPv6 handover procedure. Whereas in reactive schemes both for seamless handover and QoS parameter negotiations, mobile node handovers before requesting context transfer. After handover to the new router, the procedure of context transfer is done. Results showed that predictive schemes are faster than the reactive schemes. Equation (1) shows its predictive scheme where 4 messages are exchanged between *UE* and old *AR* ($4T_{UEtoARo}$). One message is sent to old P-CSCF from *UE* ($T_{UEtoPold}$). Two messages are exchanged between old *AR* and new *AR* ($2T_{ARotoARn}$). One message is sent from *UE* to new *AR* ($T_{UEtoARn}$). Two messages are exchanged between *UE* and *HA* ($2T_{HA}$). Four messages are exchanged between *UE* and *CN* ($4T_{UEtoCN}$). Two messages are exchanged between *UE* and new P-CSCF ($2T_{UEtoPnew}$). Equation (2) shows MDT_{RM} for reactive mode where $T_{PoldtoS}$ is the message between old P-CSCF and S-CSCF.

$$MDT = 4T_{UEtoARo} + T_{UEtoPold} + 2T_{ARotoARn} + T_{UEtoARn} + 2T_{HA} + 4T_{UEtoCN} + 2T_{UEtoPnew} \quad (1)$$

$$MDT_{RM} = 2T_{UEtoARo} + 3T_{UEtoPnew} + T_{UEtoARn} + 2T_{ARotoARn} + 3T_{PoldtoPnew} + 2T_{PoldtoS} + 2T_{PoldtoS} + 2T_{HA} + 4T_{UEtoCN} \quad (2)$$

2.2.2. Simultaneous Switching based Schemes

Thanh et al. [30] proposed to integrate mSCTP with IMS. Authors of this technique believed that MIPv4 and MIPv6 provide mobility but due to higher signaling cost and handover delay, it lacks session continuity. mSCTP is an extension of SCTP, which has a feature of multi-home. mSCTP has an added feature in it that can add, delete or modify the IP address of UE while connection is active. mSCTP supports session continuity but it lacks location awareness which is necessary for QoS parameters' negotiations. IMS has policy based QoS model that can handle this. This paper proposed a scheme to place an mSCTP based proxy between mobile node and corresponding node. And the session is not direct between them, instead it is divided into two TCP/UDP data sessions i.e. one between UE and proxy and other one is between proxy and CN. UE should have mSCTP support. The whole interaction between CN, proxy and UE is handled by IMS overlay. IMS is responsible for call initiation, location management and QoS control. On UE handover to another network, UE establishes a new mSCTP connection to the proxy over IMS domain 2. While the old leg of connection with the previous network is still active. UE changes the QoS parameters of new mSCTP connection according to the QoS level of new network and request required codecs for this from the proxy. A new SWITCH SIP method is proposed to switch fast back and forth between these two connections. This reduced handover latency once the second leg of connection is established but takes time to establish this second leg of connection.

2.2.3. Proactive Selection based Schemes

The scheme proposed by Manabu Ito et al. [31] has a solution for QoS control for IMS mobility scenario. A service centralization and continuity application server (SCC AS) is standardized in 3GPP [20] for service continuity. When a UE registers itself with IMS, the S-CSCF notifies the UE's registration to SCC AS. For service continuity after handover, an INVITE message is sent to SCC AS. In standard handover procedure [20] communication between UE and CN doesn't start until UE gets new IP address and service continuity procedure is complete. This technique adds QoS control by reducing media disruption time for a handover procedure that is based on standard [5]. Firstly, this technique proactively obtains the new IP address for UE in new network and completes the service continuity procedure before switching to the new network. Secondly it gives a mechanism to select the best network that provides the required resources. UE establishes a tunnel with the router of new network and starts its communication with CN through this tunnel. If the new network does not provide the required resources then the SCC AS may fail to re-establish the session with CN until best network is found. A policy and charging rules function (PCRF) is helpful in giving the information of resources of access networks. Before switching to new network, UE sends a request to the router of new network to stop sending the packets and instead buffer them. After switching to new network, the buffered media from the router is sent to UE. UE starts its communication immediately with CN, so no packet loss is caused. This method needs to extend the messages specified in FMIPv6 according to the requirements. Authors concluded that the media disruption delay is approximately equal to handover delay by applying this method.

2.2.4. Re-registration Avoidance based Schemes

Shun-Ren Yang et al. [32] proposes a QoS reservation model that reserves resources in advance at neighboring IMS networks. This paper also gives a solution for IMS mobility that is based on the concept of SIP multicast [33]. The leaves of the multicast tree are locations for which reservation model proposed in this approach will reserve resources. The authors preferred SIP multicast routing because it's easy to be implemented rather than MIP tunneling. Also it avoids re-registration and it is fast to switch the route. The reservation model reserves bandwidth in the current network as well as in geographically

adjacent neighboring IMS networks. It proposes three classes of reservation: *Conventional Reservation (CR)* reserves resources in the current IMS network. The packets are travelling actually on the CR link to the CN. *Predictive Reservation (PR)* reserves resources on the neighboring leaves of multicast tree from the mobile node (source). The data doesn't flow on PR links. *Temporary Reservation (TR)* uses inactive bandwidth which is reserved by other data flows. As soon as UE enters into the IMS network, then it has the right to use PR links if it has reserved it. And any other temporary usage of inactive bandwidth should be stopped. The advantage of this technique is to avoid re-registration without using MIP tunneling.

Another approach by Nazari et al. [34] proposed a solution to minimize handover delay by eliminating the delay of registration. There is a server HOS (Handover Server) in the proposed PRIME architecture. With the help of MIH[35] protocol HOS enables the UE to get mobility information and then it pre registers with the new network in IMS and gets a new IP address. The HOS acts as a proxy and forwards the authentication messages between the UE and the authentication server in the new network. On detecting a suitable BS, UE pre-registers with the AN. Due to pre-registration delay is minimized when handover happens.

2.2.5. Simultaneous Data Flow based Scheme

P. Bellavista et al. [37] proposes a framework where a module predicts the network on which UE handovers its connection. It keeps the flow on old network also starts signaling on new network. Another module is to handle QoS issue on new network.

In the framework for handover in IMS known as IHMAS (IMS-compliant Handoff Management Application Server). IHMAS gives solution for session continuity and adaptation of QoS parameters for new network where the mobile node handovers. IHMAS consists of three components i.e. VHP (Vertical Handover predictor), ASSC (Application server for service continuity) and AMG (Adaptation media gateway). VHP is used for handover decision to best network and it is placed in mobile node. VHP predicts the new network where the UE will handover and it starts signaling with this new network while keeping the flow over old network. ASSC is deployed at home

network of mobile node and AMG is an application layer media gateway that is responsible for dynamic adaptation of QoS parameters on new network where UE will handover. ASSC keeps the information of CN. That is why during handoff it receives all the handoff related messages and after handoff on receiving INVITE message, it starts QoS parameter adaptation process by contacting AMG. AMG has the knowledge of QoS level of new network, it transfers the session from old network to new network after modifying the QoS parameters according to target network.

2.2.6. New Protocol inclusion based schemes

The FMIPv6 is developed for reducing layer 3 delay [25] that is recommended to be integrated with IMS to reduce handover delay [26][27]. In MIP based mobility solution for IMS handover, two messages are exchanged between UE and AR-old for router solicitation/advertisement. Two messages are exchanged between UE and Home Agent (HA) for Binding Update (*BU*) and BU Acknowledgment (*BU-Ack*). Similarly two messages are exchanged between *UE* and *CN* for *BU* and *BU-Ack*. Then standard REGISTRATION phase is carried out via new P-CSCF.

A cross layer architecture has been proposed for handover from LTE to WiMAX by integrating MIP and SIP protocols [51]. It uses EPC (Evolved Packet Core) as the core network and IMS to provide multimedia services and manage sessions. The Delay (D) for a handover from LTE to WiMAX is given in equation (3). In this equation, a sub element D_{MIP} is calculated using equation (4) by calculating the delay time of agent solicitation/advertisement for BS of WiMAX and registration request and reply with *HA* to identify the new P-CSCF and S-CSCF. The time T_{UEtoCN} is calculated for *BU* and *BU-Ack* messages that are exchanged between *UE* and *CN*.

$$D = D_{MIP} + D_{SIP} + D_{HSS} \quad (3)$$

$$D_{MIP} = 2T_{UEtoBS} + 2T_{UEtoHA} + 2T_{UEtoCN} \quad (4)$$

Equation (5) explores the calculation of D_{SIP} for non cross layer architecture that involves the delay time taken for the registration request and response messages between *UE* and

S-CSCF. It also involves delay time for 3 re-invite messages between *UE* and *CN* i.e. REINVITE, OK and ACKNOWLEDGMENT. Equation (6) shows the D_{SIP_CL} for cross layer scenario.

$$D_{SIP} = 2T_{UEtoS} + 3T_{UEtoCN} \quad (5)$$

$$D_{SIP\_CL} = 2T_{HAtoS} + 3T_{UEtoCN} \quad (6)$$

In this case, D_{HSS} is the delay consumed by S-CSCF to update HSS about new location of *UE*. In this scheme registration of *UE* with S-CSCF is shown in 2 messages but it does not explain the authentication, establishment of SAs with new P-CSCF and integrity protection issues.

2.3. IPSec SAs Establishment

In following techniques proposed in literature for IPSec SAs transfer or re-establishment are discussed.

2.3.1. SA Context Transfer based Schemes

K. Larsen et al. [28] gives the solution to transfer IPSec SAs by transferring context from old P-CSCF to new P-CSCF. After registration to new P-CSCF, old P-CSCF sends context transfer request to new P-CSCF. Old P-CSCF transfers the key used for IPSec SAs establishment. In this way SAs are migrated from old P-CSCF to new P-CSCF.

According to E. Prince et al. [38], when handover occurs, instead of re-registering new P-CSCF get context information from old P-CSCF. Authors suggested transferring this context in SIP body instead of using a whole new protocol. During Context transfer key used for SAs is transferred to UE's new IP address. UE sends a special message to new P-CSCF in order to authorize the user, hence it reduces handoff delay n packet loss.

2.3.2. Early SA Establishment based Schemes

Nazari et al. [34] and Nazari et al. [36] do pre-registration with IMS. UE uses MIH protocol to get mobility information and gets registered in target network and IMS. As UE gets new IP address, it establishes SAs with the new P-CSCF. Here delay to establish SAs is reduced by pre-registering in new AN and IMS.

Bongkyo Moon [39] gives a method to establish SAs when UE is handing over from wifi to 3G. UE sends its IP address in 3G network before actual handover through wifi link. This IP address is used for SAs establishment in advance thus reducing delay.

Scheme proposed for pre-authorization (SCTM) by [52] for the handover between *LTE* and *WIMAX*. It suggests transferring context of *IPSec SAs* from old *P-CSCF* to new *P-CSCF* before moving to new *AN*. The mobility information is obtained with the help of MIH protocol. This scheme reduces re-authorization messages from 22 to 10. It calculated the handoff delay as equation (7):

$$D_{IMS-Auth} = D_{T-Auth} + D_{P-Auth} + D_{Q-Auth} \quad (7)$$

$D_{T\text{-}Auth}$ is transmission delay, $D_{P\text{-}Auth}$ is processing delay and $D_{Q\text{-}Auth}$ is queuing delay.

[39] gives a method to establish *SAs* when *UE* is handing over from wifi to *3G*. When *UE* pre registers in *3G* while still connected to *WiFi*, then the *IP* address sent to *CN* is the old one i.e. *UE*'s *IP* address on *WiFi*. So the *CN* establishes *SAs* on this *IP* address. Rather it must establish *SAs* on new *IP* address obtained at *3G*. In order resolve this *IP* mismatch problem [39] gives a method to *SA* establishment in such schemes where a handover occurs from *WiFi* to *3G*. It adds new SIP headers to resolve the *IP* address mismatch problem for *SAs* by indicating the destination *IP* address of *UE* in its SIP messages. Author considers the queuing delay and transmission delay to find delay of IMS.

2.4. Minimization of number of commands

K.Larsen et al. [28] proposed a scheme in order to reduce number of SIP messages for registration and invite (for session) in order to reduce handoff latency. It proposes to reuse the information about user and session states in CSCF servers. This technique claims to reduce number of messages from 15 to 4. Thus it reduces signaling cost of messages. It transfers the context from old P-CSCF to new P-CSCF, which contains the information of the user and state of session that was going on before user changed the network.

2.5. Packet Loss Evaluation

Bagubali [53] analyzed and evaluated the IMS based integration architecture proposed in [51] for WiMax/LTE handover. It is found out that the cross layer architecture is better than the non cross layer architecture by evaluating packet losses and other parameters [53]. Equation (8) is used by [54] to calculate packet loss where Ti_{ad} is agent advertisement signal, G is downlink packet transmission rate, D is handoff delay and Nm is the number of handovers during a session.

$$\text{Packet Loss} = \left[\left(1/(2 * \text{Ti}_{\text{ad})}\right) + \text{D}\right] * \text{G} * \text{Nm} \quad (8)$$

2.6. Chapter Summary

In this chapter IMS mobility schemes are discussed. Different researchers gave solutions on different mobility areas those are summed up in this chapter. Different researchers evaluated their schemes on a number of metrics. We categorized the areas as registration with new of IP addresses, authentication, integrity Protection and establishment of IPSec SA establishment. Evaluation metrics are categorized as media disruption time, number of commands, packet loss, signaling delay and authorization delay.

CHAPTER 3

3. FAST IMS MOBILITY SCHEME

In this chapter we introduced a framework for registration/authentication phase as well as authorization of UE when it changes its AN and then contacts IMS. This phase covers transfer of IPSec SAs to new P-CSCF as well in a secure manner. The scheme proposed to carry out all these phases is discussed here along with the algorithms and protocol.

3.1. Introduction

A UE that handovers to different ANs and then contacts IMS, undergoes a process of Registration. Registration phase is coupled with authentication. In this chapter we discussed the two processes along with another process that is authorization. Authorization is also a part of registration phase. These three processes took 6 messages in standard IMS method when UE changes its AN. We reduced the number of commands to carry out these three processes after handover. These reduced messages cover registration, authentication and authorization. The proposed framework managed to reduce media disruption time, number of messages/commands and packet loss. In this chapter these three evaluation metrics are also discussed.

3.2. Proposed Scheme

We have proposed a **F**ast **I**MS **M**obility (FIM) scheme where a flag is maintained to ensure that no de-registration in IMS occurs if it is enabled during handover. The value of flag is set according to the state of *UE*, either it is having a session with a *CN* previously

or not. The flag ensures that no de-registration in IMS occurs if it is enabled. This is done due to the fact that *UE* has not intentionally terminated from *AN* because it is still in a session with *CN*. So it shows that *UE* is terminated from *AN* for handover process only and it is going to get registered in IMS again. We have recommended that after layer 3 handover and discovery of new P-CSCF, *UE* should transmit a new subsequent request for handover to S-CSCF for replacing old IP address of *UE* with new one. Similarly, IP address of old P-CSCF is also replaced. It also initiates to transfer *IPSec SAs* to new P-CSCF in a secure manner using authentication. In this way four messages of REGISTER request are reduced to 2 messages. Similarly it reduces number of commands by eliminating the need of network initiated de-registration.

3.3.1 Phases of Proposed Scheme and Algorithms

In our scheme, the communication begins when *UE* transmits a proposed subsequent HANDOVER request to old P-CSCF. After that, *UE*'s registration/authentication process begins at S-CSCF to proceed with the connectivity of new P-CSCF along with credentials. In next phase, IPSec SAs are forwarded by the S-CSCF to new P-CSCF that exchanges the confirmation messages for the running call session. Finally the old P-CSCF removes the IPSec SAs from itself as illustrated in four phases in figure 3.1.

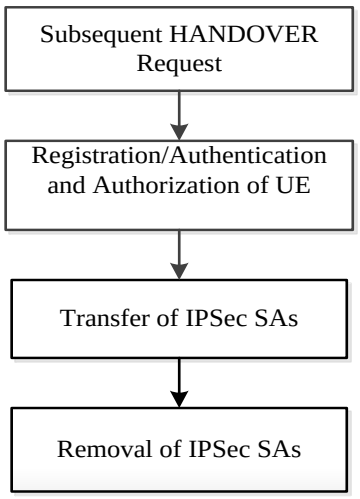

Figure 3.1 Phases of FIM Scheme during handover

In first phase, *UE* transmits a subsequent HANDOVER request with its new IP address in *Contact* and IP address of P-CSCF in *discovered-CSCF* parameter in header as shown below. In this scenario, a new *sessionContinued* flag is introduced to keep status of session between *UE* and *CN*. When a *UE* establishes a session with *CN* then *sessionContinued* flag gets enabled. On cancellation of session, this flag gets disabled. In this case, if the flag is not set then REGISTER request will be sent to old-CSCF as illustrated in pseudoCode 1. *UE*'s disconnection from an *AN* leads to de-registration from IMS. Our scheme protects against de-registration due to *sessionContinued* flag. In this way all the related data of *UE*'s registration is not deleted from the IMS servers and *UE*. After layer 3 mobility, *UE* discovers a P-CSCF that is either new one or the same one at previous location. Here instead of starting registration phase our scheme sends HANDOVER request to S-CSCF via old P-CSCF as described above. The HANDOVER request utilizes a routing header i.e. service-route. In this way P-CSCF doesn't need to contact I-CSCF for S-CSCF's address. So the I-CSCF doesn't contact HSS that results in no *Cx* commands for our scheme.

Subsequent HANDOVER request
HANDOVER sip:home1.fr.SIP/2.0 *Via: SIP/2.0/UDP [5555::1:2:3:4];branch=0uetb* *Route:sip:[5555::a:f:f:e];lr* *Max-Forwards: 70* *From: sip:user@home1.fr;tag=pohja* *To:sip:user@home1.f* *Contact: sip:[5555::1:2:3:4};expire=600000* *discovered-CSCF:sip[6666::d:e:e:f]* *TIPSecSAs: tls;q=0.2,IPSec3gpp;q=0.1;alg=hmac-sha-1-96; spi-c=9865432;spi-s=8764321;port-c=8642;port-s=7531* *Authorization: Digest username="user1@home1.ims, Response="083493483927jdhfjshfj"* *Call-ID:ahedew23398fk* *CSeq: 20 HANDOVER*

Content-Length:0

pseudoCode 1: Session handling at UE

```
IF sessionContinued == true then
  Construct method = HANDOVER
  Route "HANDOVER" to old P-CSCF
ELSE
  Route "REGISTER" to old P-CSCF
ENDIF
```

In second phase, *UE* connects to new *AN* and then verifies that if the status of sessionContinued flag is enabled then instead of sending REGISTER request to IMS, *UE* constructs HANDOVER request. *UE* integrates its new IP address in *via* and *Contact* headers. *UE* places IP address of new P-CSCF in a new proposed header *discovered-CSCF* in HANDOVER message. *UE* forwards this HANDOVER request to old P-CSCF that forwards it to S-CSCF where new values from *Contact* and *discovered-CSCF* headers are saved. IP address of new P-CSCF is copied to *path*. Now S-CSCF is able to forward request destined for *UE* towards new P-CSCF. In this way, *UE* gets registered in IMS. *UE* and HSS keep a shared secret and sequence number. In *UE*, it is saved in ISIM application on universal integrated circuit card (UICC). In the initial register request of standard IMS scheme, S-CSCF downloads Authentication vectors (AVs) for *UE*. AVs contain random challenge (RAND) and expected response (*XRES*) along with integrity key (IK), cipher key (CK) and authentication token (AUTN). S-CSCF sends these AVs to *UE* in initial request's response i.e. 401. *UE* calculates *RES* with the help of shared secret and RAND. This *RES* is like a password [2] and used for authentication. In our proposed scheme, due to no de-registration, *RES* and *XRES* are not lost and used for authentication during HANDOVER phase. When S-CSCF receives HANDOVER it compares the received *RES* with *XRES* and then save the new IP address of *UE* and IP address of P-CSCF as illustrated in pseudoCode 2. In other scenario, when the method is not HANDOVER then complete registration process is performed including user RES verification in the reply of "Unauthorized" message. During registration *UE* and P-CSCF establishes *IPSec SAs* used for integrity protect/authorization. Our scheme sends HANDOVER request through old P-CSCF where *IPSec SAs* are saved in a header. In this way our scheme handles registration, authentication and authorization in two messages.

pseudoCode 2: Authentication at S-CSCF

```
SCSCF receives request
IF  method=="HANDOVER"
  IF RES == XRES & integrity-protected ==
true then
    IMPU_IPaddress = Contact;
    P-CSCF_IPaddress = Path;
    IF P-CSCFold != P-CSCFnew then
      Route "HANDOVER" to P-CSCFnew
    ENDIF
 ELSEIF method == "REGISTER"
   IF RES != XRES then
     Create User-challenge( );
     route(Service-Routes);
     reply("401", "Unauthorized - Challenging
UE");
   ELSEIF RES == XRES then
     Set -status == "200"
    Route "OK" to ICSCF
   ENDIF
  ENDIF
ENDIF
```

In third phase, the old P-CSCF receives message from *UE* and compares that if the received request is HANDOVER then add *IPSec SAs* to HANDOVER message in *TIPSecSAs* header. It adds the IP address of new P-CSCF to *path* header and set *Integrity-Protected* to yes in HANDOVER request. Old P-CSCF doesn't send *IPSec SAs* to new P-CSCF directly because there is no *IPSec SAs* established between these two entities. In our scheme *IPSec SAs* are transferred from old P-CSCF to S-CSCF. S-CSCF first compares *RES* with *XRES* and then transfers the received *IPSec SAs* to new P-CSCF. This is only done when the newly discovered P-CSCF is not the old one (before handover). In this way no new protocol is used to transfer *IPSec SAs*. The transfer is done within the handover phase proposed by our scheme. In fourth phase, S-CSCF transmits "OK" message to old P-CSCF. As in our scheme there is no de-registration, the old P-CSCF removes *IPsec SAs* from itself after sending "OK" message to *UE* as illustrated in pseudoCode 3. It is only needed when newly discovered P-CSCF is the new one. The registration after handover is presented in a visual manner in figure 3.2 by sequentially exploring above four phases.

pseudoCode 3: IPsec SAs handling at old P-CSCF

```
PCSCFold receives request
IF method == "HANDOVER" then
    Add IPSec SAs to T-IPSecSAs
   Path = discoveredP-CSCF;
   Integrity-Protected = “yes”;
   Route to S-CSCF
ELSEIF method == ”REGISTER”
   route "REGISTER" to ICSCF
   IF status == "401"
      STATE Remove CK, IK
   ELSE
     STATE reply("500","P-CSCF Error on
    Removing CK, IK");
  ENDIF
ENDIF

IF status == "200" then
   Route “OK” to UE
ENDIF

IF P-CSCFold != P-CSCFnew
   Delete IPSec SAs
ENDIF
```

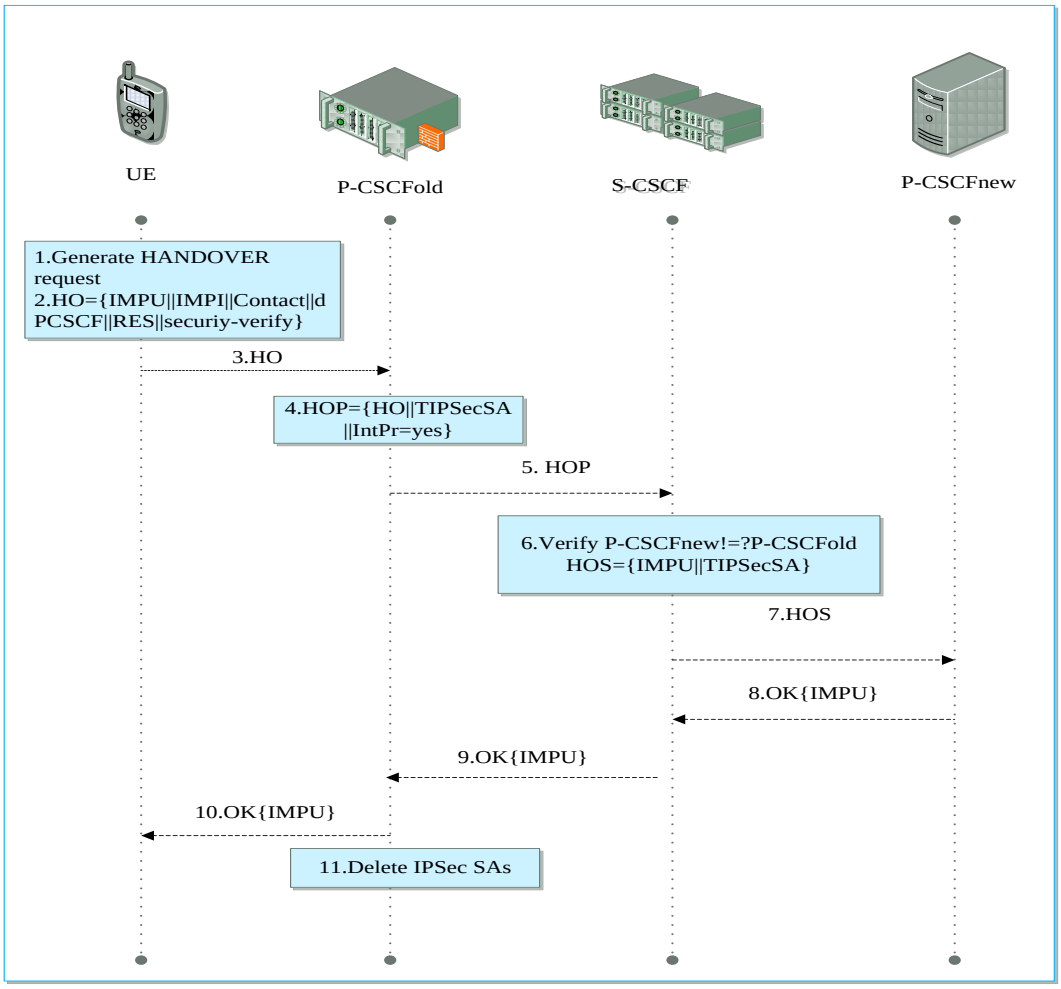

Figure 3.2 Proposed Flow for FIM Scheme

3.3. Protocol of Fast IMS Mobility (FIM) Scheme

Protocol for FIM scheme is given below. It shows the steps of proposed registration phase after handover to new AN in IMS. A proposed subsequent request HANDOVER is used here.

$$
\begin{aligned}
&1.\ If\ sessionContinued == true\\
&2.\ UE \rightarrow PCSCFold : Handover\{IMPU||Contact||dPCSCF||RES\}\\
&3.\ PCSCFold \rightarrow SCSCF : Handover\ \{IMPU||Contact||Path||RES||\\
&IntPr = yes\}\\
&4.\ SCSCF \rightarrow PCSCFold : 200\ \{IMPU\}\\
&5.\ if\ PCSCFnew\ != PCSCFold\\
&6.\ SCSCF \rightarrow PCSCFnew : Handover\{IMPU||TIPSecSA\}\\
&7.\ PCSCFnew \rightarrow SCSCF : OK\{IMPU\}
\end{aligned}
$$

8. $PCSCFold \rightarrow UE : 200\{IMPU\}$
9. $else\ if\ sessionContinued == false$
10. $UE \rightarrow PCSCFold : Notify\ \{IMPU||State\}$
11. $PCSCFold \rightarrow UE : Notify\ \{IMPU||State\}$
12. $UE \rightarrow PCSCFold : OK\{IMPU\}$
13. $PCSCFold \rightarrow SCSCF : OK\ \{IMPU\}$
14. $SCSCF \rightarrow PCSCFold : Notify\{IMPU||State\}$
15. $PCSCFold \rightarrow SCSCF : 200\{IMPU\}$
16. $UE \rightarrow PCSCFnew : Register\{IMPU||Contact\}$
17. $PCSCFnew \rightarrow ICSCF : Register\{IMPU||Contact\}$
18. $ICSCF \rightarrow HSS : UAR\{IMPU\}$
19. $HSS \rightarrow ICSCF : UAA\{SCSCF\ name\}$
20. $ICSCF \rightarrow SCSCF : Register\ \{IMPU\}$
21. $SCSCF \rightarrow HSS : MAR\{IMPU\}$
22. $HSS \rightarrow SCSCF : MAR\{AVs: RAND, IK, CK, XRES, AUTN\}$
23. $SCSCF \rightarrow ICSCF : 401\ \{AVs: RAND, IK, CK, XRES, AUTN\}$
24. $ICSCF \rightarrow PCSCFnew : 401\ \{AVs: RAND, IK, CK, X\ RES, AUTN\}$
25. $PCSCFnew \rightarrow UE : 401\ \{AVs: RAND, XRES, AUTN\}$
26. $UE \rightarrow PCSCFnew : Register\ \{IMPU||RES||IntPr = yes\}$
27. $PCSCFnew \rightarrow ICSCF : Register\ \{IMPU||RES\}$
28. $ICSCF \rightarrow SCSCF : Register\ \{IMPU||RES\}$
29. $SCSCF \rightarrow HSS : SAR\ \{IMPU\}$
30. $HSS \rightarrow SCSCF : SAA\ \{Assigned\ SCSCF\ name\}$
31. $SCSCF \rightarrow ICSCF : 200\ \{IMPU\}$
32. $ICSCF \rightarrow PCSCFnew : 200\ \{IMPU\}$
33. $PCSCFnew \rightarrow UE : 200\ \{IMPU\}$
34. $End\ if$

Steps 1 – 8: If *UE* finds the status of sessionContinued flag enabled then instead of initiating registration phase it starts handover phase. *UE* sends handover request to old P-CSCF with its new IP address in Contact header and IP address of P-CSCF in discovered-CSCF header. Old P-CSCF copies the IP address of new P-CSCF in path header and forwards the handover request to S-CSCF after setting Integrity-Protected field as "yes". For authentication *RES* is coming from *UE* to S-CSCF. On successful match of *RES* with *XRES*, S-CSCF replaces UE's old IP address with new IP address from *Contact* header. S-CSCF sends *IPSec SAs* to new P-CSCF in handover request when *RES* successfully matches with *XRES*.

Steps: 9-16: If the *sessionContinued* flag is disabled then usual network initiated de-registration takes place S-CSCF sends a *Notify* for de-registration to UE through old P-

CSCF. *UE* sends OK response to S-CSCF through old P-CSCF. S-CSCF sends a *Notify* of de-registration to old P-CSCF and old P-CSCF sends OK response to S-CSCF.

Steps 17-24: After de-registration, *UE* sends the REGISTER request to newly discovered P-CSCF. That forwards it to I-CSCF. I-CSCF finds a suitable S-CSCF for this *UE*. The S-CSCF finds this request form unauthorized *UE*. It generates Authentication Vectors and challenges the UE.

Steps 25-34*: UE* calculates *RES* from a shared secret and *RAND* received in 401 response. Till now IPSec SAs are also established between *UE* and P-CSCF_new. Integrity protected is set as "yes" in this message. Request is forwarded to I-CSCF that finds assigned S-CSCF. S-CSCF compares *RES* with *XRES*. If both are equal then *UE* is authenticated and get registered in IMS.

3.4. MEDIA DISRUPTION TIME AND PACKET LOSS

Fast schemes are needed for handover scenarios in IMS. In this section we will discuss the evaluation metrics for our scheme of registration, authentication, authorization and transfer of IPSec SAs to new P-CSCF proposed in previous section. Here we show that our scheme is better than standard method of registration in IMS and other methods proposed in literature. Proposed method enables IMS to reduce media disruption time, number of commands and packet loss.

We have reduced *MDT* between two entities after handover from one *AN* to another *AN*. *MDT* is confined by reducing delay and cost of the registration phase in IMS in a case where the two entities are already in a session with each other. Similarly we proposed to reduce number of *Gm*, *Mw* and *Cx* commands. Our proposed scheme handles authorization of *UE* and transfers *IPSec SAs* during registration phase. It handles all this with low latency in media disruption time as given in equation (1) where $E = \{UE, PCSCF, ICSCF, HSS, SCSCF\}$ is the set of entities, x is the number of messages between two entities, $T(E_i, E_j)$ is delay time taken by the message between entities $E_i \; to \; E_j$ where $i = \{1,2,3,4\}$ and $j = i + 1$.

$$minimize\ MDT = \sum x.T(E_i, E_j) \quad (1)$$

Schemes [51], [38] and [55] use re-INVITE request after handover where 3 messages are exchanged between *UE and CN*. In MIP based schemes and FIM scheme, re-INVITE method is considered for correct comparison. In standard IMS method, there is no scheme for handover so INVITE method is used.

For minimizing number of commands, if we consider $S = \{PCSCF, ICSCF, SCSCF\}$ is the set of IMS servers and $H = \{HSS\}$ is the set of database. y is the number of *Mw* commands, $i = \{1,2\}$. Then number of *Mw* commands is needed to be minimized as given in equation (2). It calculates sum of Mw commands needed from P-CSCF to I-CSCF and from P-CSCF to S-CSCF. Equation (3) calculates sum of *Cx* commands needed from I-CSCF to HSS and from I-CSCF to HSS where z is the number of *Cx* commands, then minimization of Cx commands.

$$minimize\ Mw\ signaling\ cost = \sum y.(S_i, S_{i+1}) \quad (2)$$

$$minimize\ Cx\ signaling\ cost = \sum z.(S_{i+1,} H) \quad (3)$$

U = {UE} and *k* is the number of *Gm* commands, then the minimization of *Gm* commands is given in Eq. 4 that calculates the sum of Gm commands needed from P-CSCF to *UE*.

$$minimize\ Gm\ commands = \sum k.(S_i, U) \quad (4)$$

In handover scenarios, there is no method for change of IP address in IMS. In literature, researchers proposed methods for change of IP address by proposing MIPv6 integration with IMS. Researchers suggested using a fast protocol i.e. FMIPv6 instead of MIPv6. FMIPv6 does Address Configuration (AC) before handover to reduce layer 3 handoff delay of MIPv6. Instead of comparing results of our technique with MIPv6 and FMIPv6 separately, we will consider a standard MIP-IMS technique for the comparison. In this way researchers can have an idea from the results that our proposed method is better than both.

3.5. MIP-IMS Technique Evaluation

Basic MIP-IMS technique can be taken from Farahbakhsh et al. [26]. This approach can be explained in the figure 3.3. UE gets disconnected from its old AN and connects to new AN

then P-CSCF de-registers UE from IMS. After connecting to new AN and obtaining new IP address i.e. known as Care of Address (CoA), UE registers in IMS again. An entity called Home Agent (HA) is involved in this scheme that binds CoA with Home Address (HoA) of UE with it. Binding Update is also sent to CN for direct communication. MIP based handover in IMS gives solution for change of IP address in IMS, however it causes delay in media disruption time.

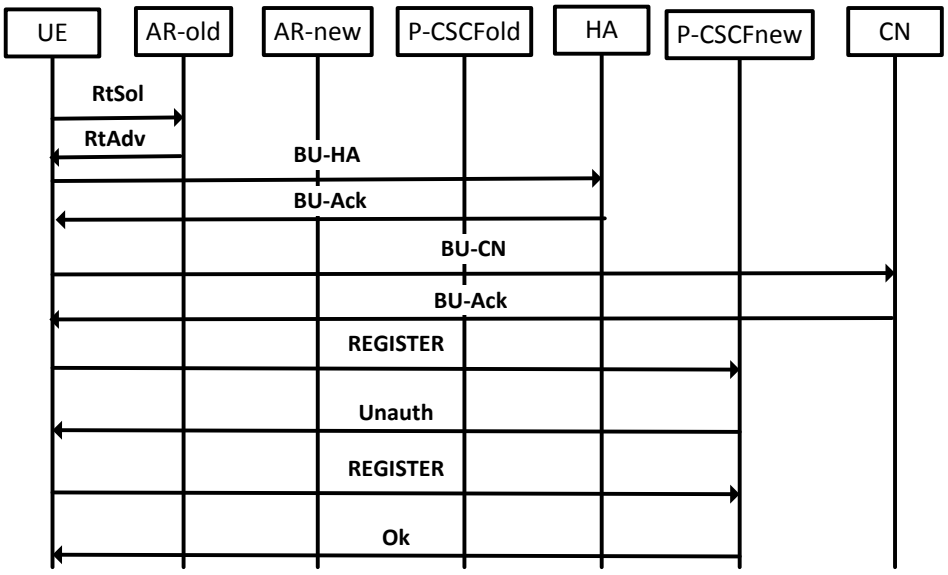

Figure 3.3: MIP-IMS handover scenario

3.5.1. Media Disruption Time

MDT for this scheme is calculated using equation (5) taken from scheme [28] and [51]. In this equation, T_{HA}+T_{UEtoCN} represents the time taken for sending binding update to *CN* and *HA*.

$$MDT_{MIP} = 2T_{UEtoARn} + 2T_{HA} + 5T_{UEtoCN} + 4T_{UEtoP} + 4T_{PtoS} + 6T_{CSCFtoHSS} \quad (5)$$

The time for sending binding update to CN and HA is $T_{HA} + T_{UEtoCN}$ [26].

3.5.2. Number of Commands

Number of SIP commands in case of MIP-IMS based handovers is shown in table 3.1

calculated according to Eq. 2, Eq. 3 and Eq. 4. As the number of handovers increase, SIP commands i.e. Mw, Gm and Cx increase in effect. UE has to undergo de-registration and then registration again in IMS. So the total number of commands are counted including de-registration and registration phases.

Table 3.1: Number of Commands of MIP-IMS handovers

No. of Handovers	Mw Commands	Cx Commands	Gm Commands
1	6	6	6
5	30	30	30
10	60	60	60
500	3000	3000	3000
1000	6000	6000	6000

3.6. Standard IMS handover Evaluation

In standard IMS handover scenario, UE undergoes de-registration when it disconnects from AN_{old}. On connecting to AN_{new}, it gets registered again in IMS. Media disruption time and number of commands are shown below for standard IMS handover scheme.

3.6.1. Media Disruption Time

De-registration from IMS and disconnection from AR_{old} go parallel. So de-registration time will not affect media disruption time. Following expression shows the media disruption time for IMS handover scenario.

$$MDT = 2T_{UEtoAR} + 4T_{UEtoP} + 4T_{PtoS} + 6T_{CSCFtoHSS} + 8T_{UEtoCN} \quad (5)$$

3.6.2. Number of Commands

Signaling cost is shown in table 3.2 according to Eq. 2, Eq. 3 and Eq. 4 for standard IMS

handover scenarios. Mw, Cx and Gm commands are calculated and shown in table below.

Table 3.2: Number of Commands for IMS based handover

No. of Handovers	Mw Commands	Cx Commands	Gm Commands
1	6	6	6
5	30	30	30
10	60	60	60
500	3000	3000	3000
1000	6000	6000	6000

3.7. Proposed Scheme Evaluation

Our proposed scheme (FIM) needs no de-registration. FIM does registration in 2 messages instead of 4. Following subsections show media disruption time and signaling cost for FIM scheme.

3.7.1. Media Disruption Time

We have evaluated our results by creating three handover scenarios in order to get accurate results. First scenario is *SP* (Same P-CSCF), second scenario is *OFP* (Other Far P-CSCF) and third scenario is *ONP* (Other Near P-CSCF). The handover scenarios are explained as follows.

) SP: A handover scenario where a *UE* disconnects from *AN* and then connects to a new *AN* but it gets attached to IMS with the same P-CSCF after handover. *MDT* for *SP* scenario is shown in equation 6.

) OFP: After handover to new *AN*, *UE* connects to a P-CSCF that is not the P-CSCF to which it was connected before handover. The new P-CSCF is physically located far than old P-CSCF. Such a scenario is called *OFP*. *MDT* calculated for *OFP* scenario is shown in equation 7.

c) ONP: A scenario where *UE* connects to new P-CSCF that is different than the old P-CSCF (before handover). And the distance of new P-CSCF is physically less than the old P-CSCF from *UE*. *MDT* calculated for *ONP* is shown in equation 7.

The MDT for proposed scheme FIM is calculated using equation (6) for *SP* scenario and in equation (7) for *OFP* and *ONP* handover scenarios.

$$MDT_{SP} = 2T_{UEtoARn} + T_{UEtoPold} + T_{PoldtoS} + 3T_{UEtoCN} + T_{PnewtoUE} \quad (6)$$

$$MDT_{OFP\_ONP} = 2T_{UEtoARn} + T_{UEtoPold} + T_{PoldtoS} + 2T_{StoPnew} + 3T_{UEtoCN} + T_{PnewtoUE} \quad (7)$$

Where T_{UEtoAR} is the time taken for the exchange of messages between UE and AR_{new}. T_{UEtoP} is the time for messages' exchange between UE and P-CSCF. T_{PtoS} is the time for exchange of messages between P-CSCF and S-CSCF. Time taken by CSCF servers and HSS database is denoted by $T_{CSCFtoHSS}$. Whereas T_{UEtoCN} is the time taken by UE and CN for exchange of messages.

3.7.2. Number of Commands

Number of commands are significantly reduced in FIM for Mw, Cx and Gm commands calculated according to Eq. 2, Eq. 3 and Eq.4. Table 3.3 shows the signaling cost for FIM scheme.

Table 3.3: Number of Commands of FIM scheme

No. of Handovers	Mw Commands	Cx Commands	Gm Commands
1	2	0	2
5	10	0	10
10	20	0	20
500	1000	0	1000
1000	2000	0	2000

3.8. Numerical and Test bed Results

To evaluate *MDT*, we set $T_{UEtoRAN}$ = 10ms as in [56] and [57] and $T_{UEtoARo}$ = 11ms, $T_{ARotoARn}$ = 5ms, $T_{UEtoPold}$ = 15ms, $T_{PoldtoPnew}$ = 7ms, $T_{PoldtoS}$ = 10ms as in [26]. We considered internet delay as 100ms and T_{HA} = 116ms, T_{UEtoCN} = 128ms and T_{HAtoCN} = 114ms as in [26]. We assumed $T_{UEtoARn}$ = 10ms, $T_{PnewtoUE}$ = 16ms and $T_{StoPnew}$ = 12ms. *MDT* versus delay between *UE* and new *AR* is obtained for three handover scenarios including *SP*, *OFP* and *ONP*. It can be seen that for IMS standard scheme, *MDT* is increasing with a high rate. In figure 3.4 for SP scenario, for a delay of 30ms the *MDT* values are 338ms, 408ms and 80ms for IMS, MIP-IMS and FIM respectively where FIM requires the lowest *MDT*. It is also observed that when delay is increased three times i.e. 90ms then *MDT* values are 458ms, 528ms and 122ms for IMS, MIP-IMS and FIM respectively that shows that the FIM scheme is better than both other schemes. In figure 3.5 for *OFP* scenario, for a delay of 30ms the *MDT* values are 338ms, 440ms and 169ms for IMS, MIP-IMS and FIM respectively where FIM outperforms by consuming the lowest MDT. It is also observed that when the delay is increased three times i.e. 90ms then *MDT* is 458ms, 596ms and 229ms for IMS, MIP-IMS and FIM respectively that proves the dominance of FIM over preliminaries.

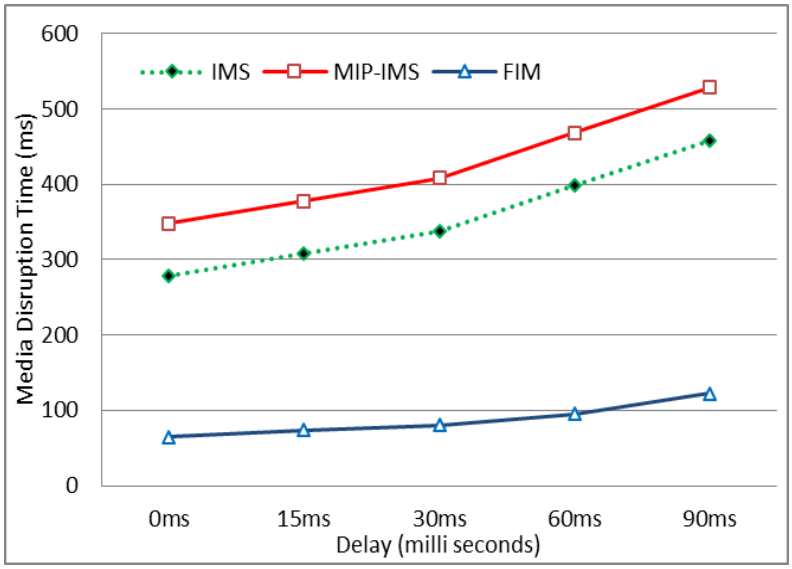

Figure 3.4. MDT versus delay between UE and AR for SP

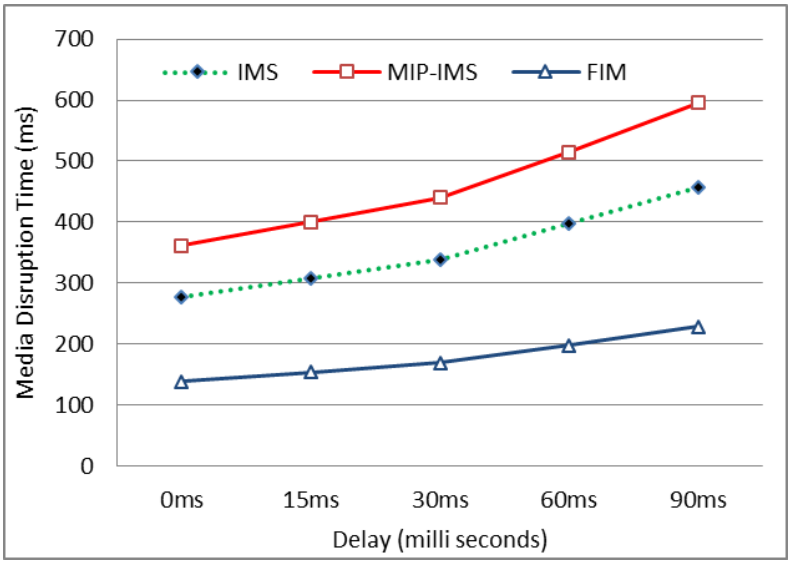

Figure 3.5. MDT versus delay between UE and AR for OFP

In figure 3.6 for ONP scenario, for a delay of 30ms the *MDT* values are 338ms, 408ms and 100ms for IMS, MIP-IMS and FIM respectively where FIM outperforms by consuming the lowest disruption time. It is also observed that when the delay is increased three times i.e. 90ms then MDT is 458ms, 528ms and 135ms for IMS, MIP-IMS and FIM respectively that proves the dominance of FIM over preliminaries.

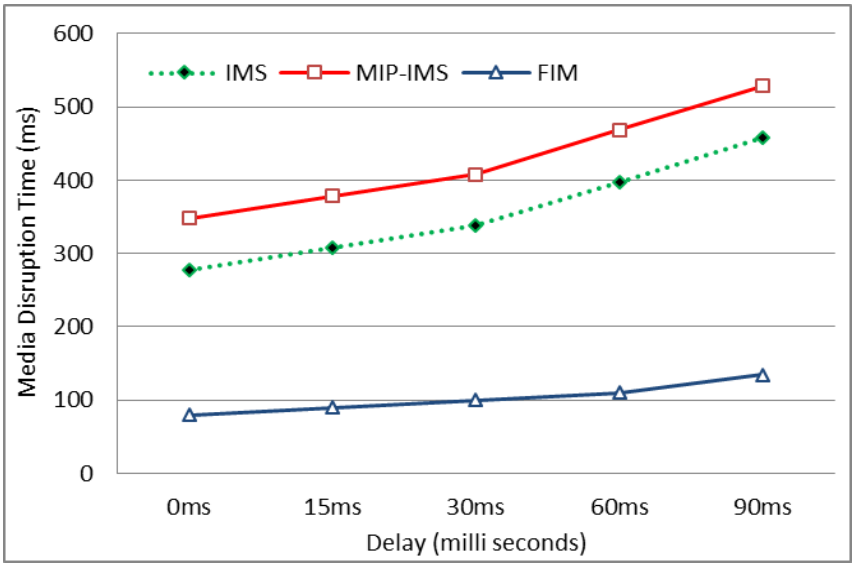

Figure 3.6 Media Disruption Time Versus delay between UE and ARn in ONP

Figure 3.7 elucidates that in *SP*, for a delay=40ms, *MDT* values are 468ms, 578ms and

110ms for MIP-IMS, IMS and FIM respectively. Results prove the dominance of our proposed FIM scheme over preliminaries. For a 4 times increase in delay i.e. 160ms due to some congestion scenarios the *MDT* values are 1428, 1778ms and 300ms for MIP-IMS, IMS and FIM respectively. It explores that existing schemes endure an abrupt change in *MDT* values as compared to a steady increase in proposed FIM scheme. In *SP* case, proposed scheme FIM reduces 71% than IMS scheme and it reduces 83% *MDT* than MIP-IMS scheme. Figure 3.8 elucidates that in case of *OFP*, the *MDT* values at 40ms delay are 468, 609 and 234 for IMS, MIP-IMS and FIM methods respectively. It is evident that our proposed scheme is better than other two schemes in reducing *MDT*. It is also observed that when the delay is 4 times i.e. 160ms the *MDT* values are 1428ms, 1831ms and 704ms for IMS, MIP-IMS and FIM schemes respectively. It explores that our proposed scheme is faster than the other two schemes. In case of *OFP*, FIM reduces 50% as compared to IMS scheme and it reduces 61% than MIP-IMS scheme.

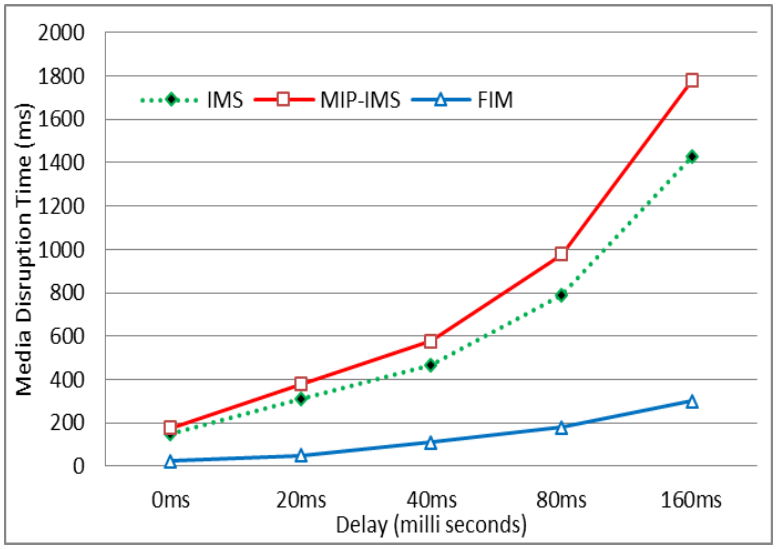

Figure 3.7 MDT versus delay between UE and CN for SP

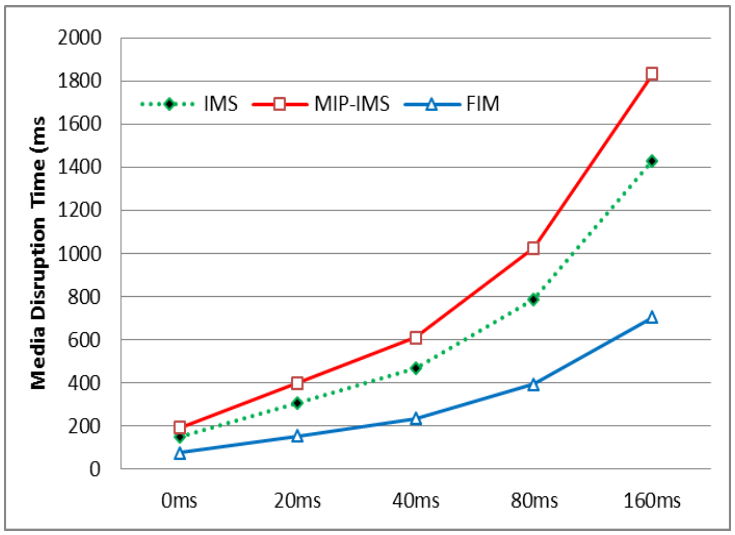

Figure 3.8 MDT versus delay between UE and CN in OFP

Figure 3.9 elucidates that in case of *ONP*, for a delay of 40 milli seconds (ms) the *MDT* values are 468ms, 578ms and 140ms for MIP-IMS, IMS and FIM scheme respectively. Results are evident to elaborate the dominance of our proposed FIM scheme over preliminaries. It has been observed that for a 4 times increase in delay i.e. 160ms due to some congestion scenarios the *MDT* values are 1428, 1778ms and 400ms for MIP-IMS, IMS and FIM scheme respectively. It explores that existing schemes endure an abrupt change in *MDT* values as compared to a steady increase in proposed FIM scheme. In *ONP* case, proposed scheme FIM reduces 71% *MDT* than IMS scheme and it reduces 77% *MDT* than MIP-IMS scheme.

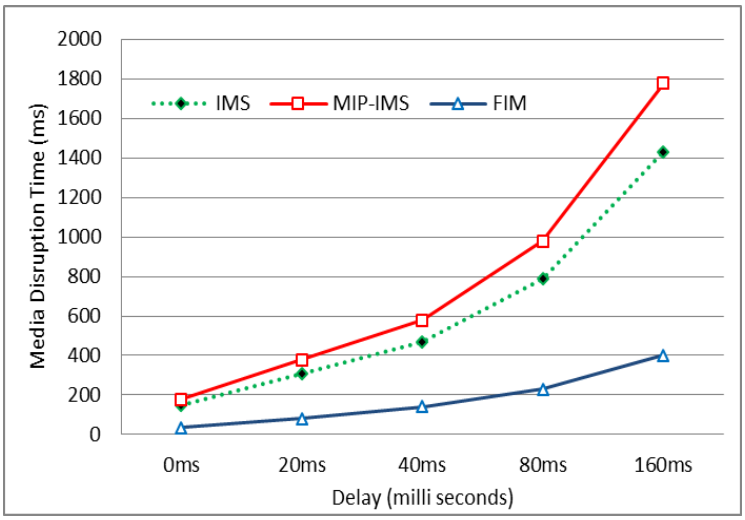

Figure 3.9 MDT versus delay between UE and CN ONP

Figure 3.10 shows the *MDT* versus delay between UE and new P-CSCF. It elucidates for a delay of 24 milli seconds (ms) the *MDT* values are 356ms, 463ms and 178ms for MIP-IMS, IMS and FIM respectively. Results are evident to prove dominance of FIM scheme over preliminaries. It has been observed that for a 3 times increase in delay i.e. 96ms due the *MDT* values are 644, 838ms and 322ms for MIP-IMS, IMS and FIM scheme respectively. In this case, proposed scheme FIM reduces 50% *MDT* than IMS scheme and it reduces 61% *MDT* than MIP-IMS scheme.

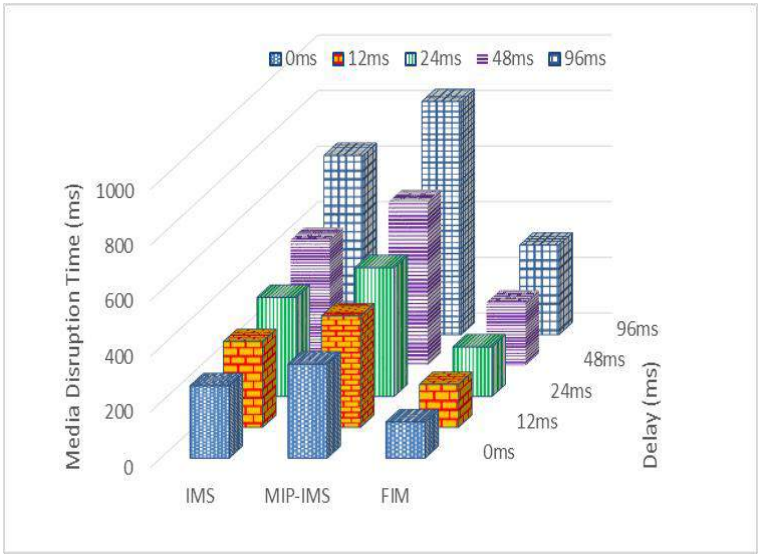

Figure 3.10 MDT versus delay between UE and new P-CSCF

The proposed FIM scheme is analyzed by performing several experiments on a test bed setup as illustrated in figure 3.11. The IMS entities HSS, P-CSCFs, I-CSCF and S-CSCF are developed on a workstations i.e. Intel core i3 with 1.7 GHz and 4 GB RAM. Open IMS core [58] is used for the implementation of these entities. It is connected through IP network with four *AN*s where each one has a router and 802.11g WLAN Access Point (*AP*). *UE* and *CN* are android phones, with 1 GB RAM and 1.2 GHz, connect to *AN* through WLAN *AP*. For MIP-IMS scheme a router is deployed that maps the HoA with CoA i.e. it acts as HA. The four simulated *ANs* has *SSID 1, SSID 2, SSID 3* and *SSID 4* respectively. We have taken a number of handovers to get the results that show how the MDT is reduced by our scheme. While *UE* is in session with *CN*, it disconnects from *SSID 1* and connects to *SSID 2*. *UE* then registers in IMS and sends INVITE to *CN* for session establishment. MDT of FIM is

compared with MIP-IMS [28],[51] and standard IMS [1] schemes and it is found out that FIM scheme reduces more *MDT* than other two schemes.

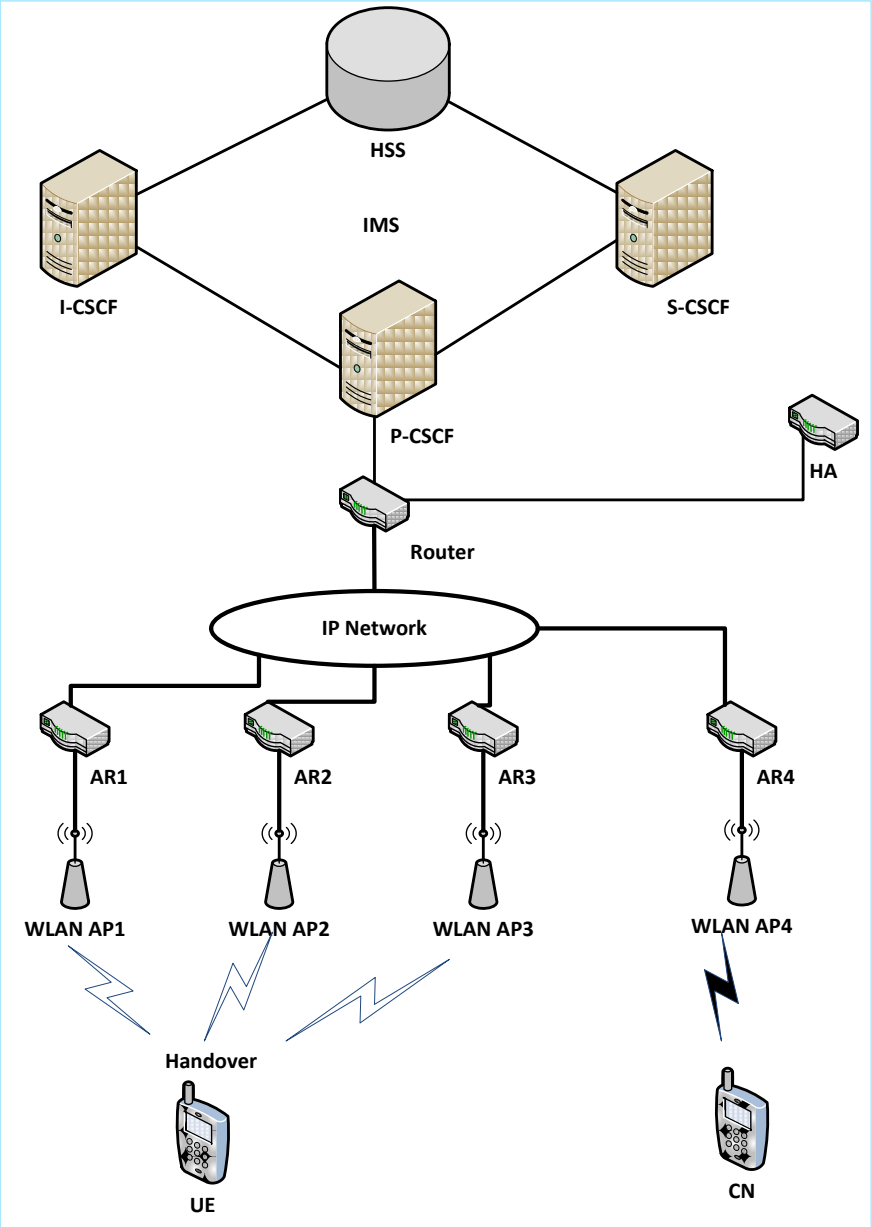

Figure 3.11 Experimental model setup for Test bed using IMS

Table 3.4 shows the evaluation parameters for our test bed.

Table 3.4 Evaluation parameters for Test bed

Test bed Setup	
Parameters	***Values***
Network Servers	P-CSCF, I-CSCF, S-CSCF, HSS
Servers' Physical Type	Wired Physical
UEs' Physical Type	Wireless Physical
Antenna Type	Omni Antenna
Parameter Variations	
Delay	0 – 90 milliseconds
Number of Hops	1 – 5
Number of Handovers	1 – 10

In test bed shown in figure 3.11, the *UE* detects that signals of *AP1* are weak and it connects to *AP2* that has strong signals. Both entities are in a VoIP session and exchanging RTP (real-time transport protocol) packets encoded with G.711 codec at 20ms interval from each other. UE monitors the signaling strength of *APs* for handover. When the exponential smoothing value of the strength ($S_t = aS_{t-1} + (1-a)a_t, 0 \leq a \leq 1$) goes below the threshold value then *UE* connects to *AP* with strong signal strength. Where a_t is signaling strength of *AP* at time *t* and S_t is the result at time *t* and a = 0.5 in the experiment as in [27]. In a number of experiments we altered the number of routers between *ANs*, *UE* and *CN* in order to vary number of hops. We considered the SP, OFP and ONP cases for our experiments. Figures 3.12 and 3.13 show the *MDT* vs. the number of hops between *UE* and new *AR* in case of SP and *OFP*. Figure 3.12 shows MDT for IMS, MIP-IMS and FIM for SP handover scenario. For 3 hops, MDT is 364ms, 438ms and 119ms for IMS, MIP-IMS and FIM schemes respectively. It can be seen in figure 3.13 that our proposed scheme reduces more *MDT* than IMS and MP-IMS schemes for OFP case . For 3 hops between UE and new AR, our scheme gives 189ms of MDT whereas MDT for IMS is 378ms and for MIP-IMS, MDT is 540ms.

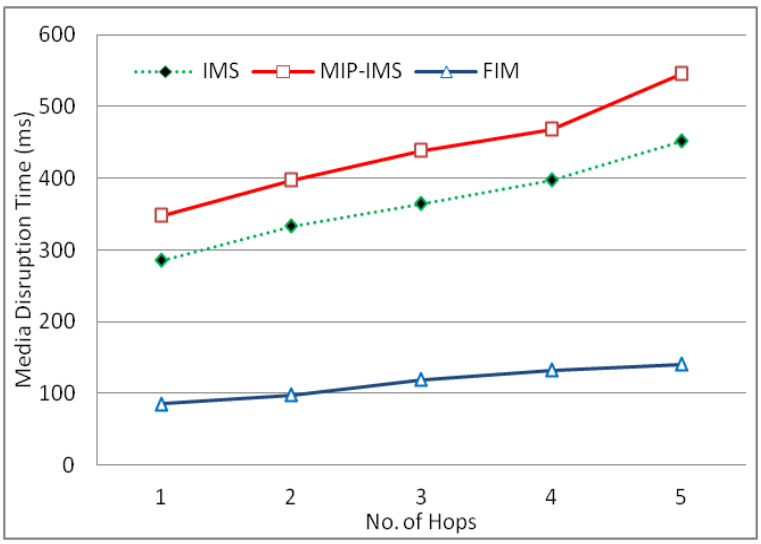

Figure 3.12 MDT Vs No. of Hops between UE and New AR are presented for SP

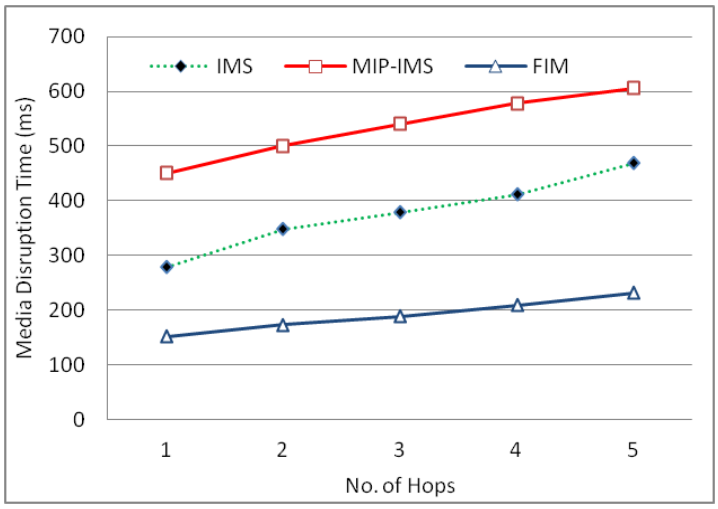

Figure 3.13 MDT Vs No. of Hops between UE and New AR are presented for OFP

In figure 3.14 for ONP scenario, for 3 hops, the *MDT* values are 357ms, 432ms and 122ms for IMS, MIP-IMS and FIM respectively where FIM consumes the lowest disruption time. It is also observed that when number of hops are increased to 5 then MDT is 476ms, 567ms and 155ms for IMS, MIP-IMS and FIM respectively that proves the dominance of FIM over preliminaries. Figure 3.15 elucidates that in *SP*, for 3 hops between UE and CN, *MDT* values are 497ms, 598ms and 140ms for MIP-IMS, IMS and FIM respectively. Results prove the dominance of our proposed FIM scheme over preliminaries.

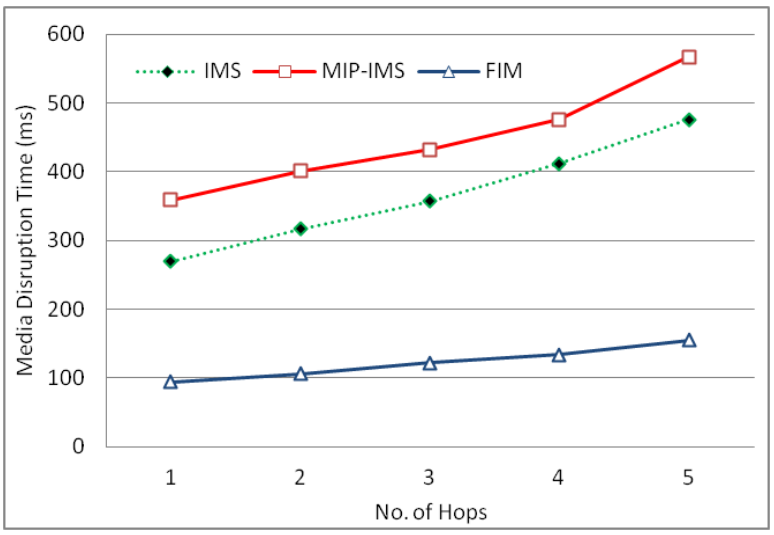

Figure 3.14 MDT Vs No. of Hops between UE and New AR for ONP

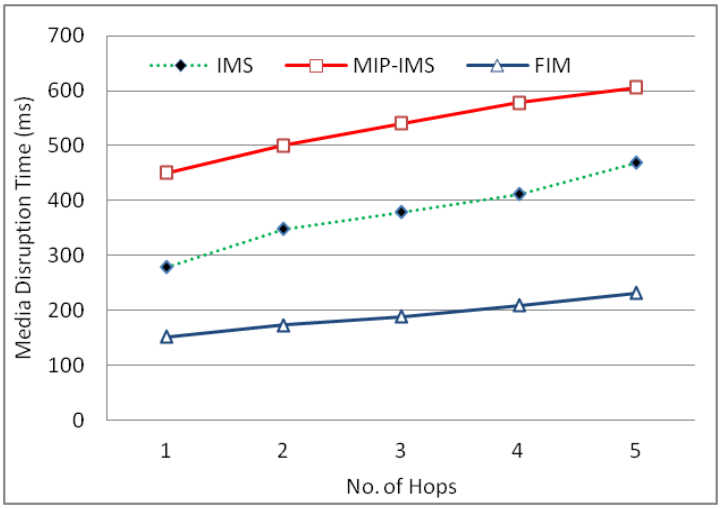

Figure 3.15 MDT Vs No. of Hops between UE and CN for SP

Figure 3.16 elucidates that in case of *OFP*, the *MDT* values at 3 number of hops are 501ms, 678ms and 287ms for IMS, MIP-IMS and FIM methods respectively. It is evident that our proposed scheme is better than other two schemes in reducing *MDT*. Figure 3.17 elucidates that in case of *ONP*, for 3 hops between UE and CN, the *MDT* values are 418ms, 544ms and 121ms for MIP-IMS, IMS and FIM scheme respectively. Results are evident to elaborate the dominance of our proposed FIM scheme over preliminaries.

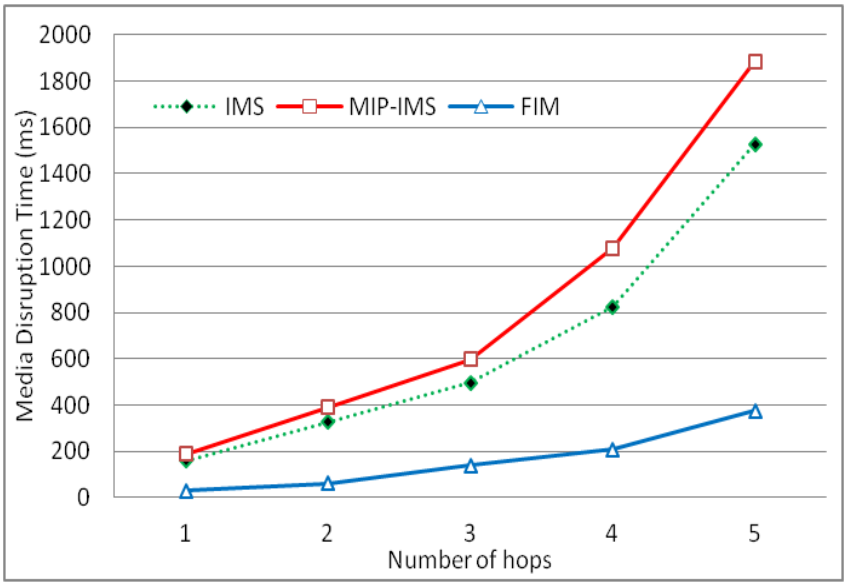

Figure 3.16 MDT Vs No. of Hops between UE and CN in OFP

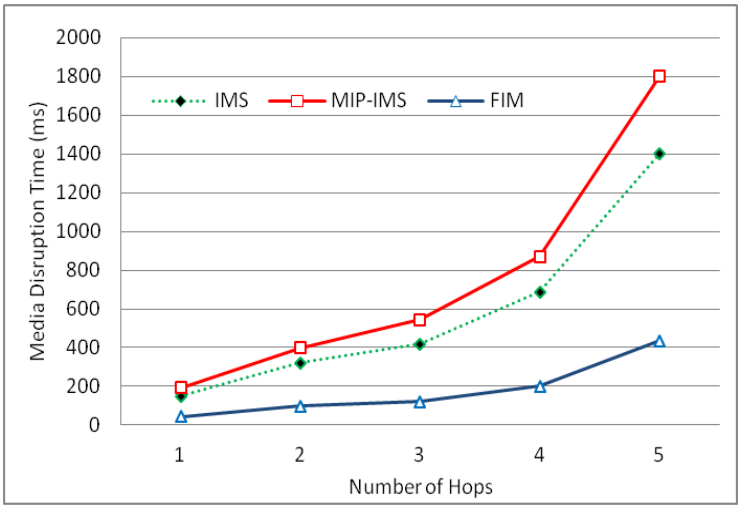

Figure 3.17 MDT Vs No. of Hops between UE and CN in ONP scenarios

3.9. Analysis of Results

Table 3.5 shows the results of the dominance of proposed scheme over IMS and MIP-IMS schemes in terms of percentage. It shows the results of numerical analysis and testbed experiments. It proves that our scheme is better in reducing *MDT* time than other two schemes when delay and number of hops are altered between UE and new AR as well as between UE and CN. It is observed that in case of ONP, MDT is lesser than OFP. MDT is even lesser in case of SP.

Table 3.5 Improvement of FIM scheme over other schemes

Delay & Hops b/w	Scenarios	SP		OFP		ONP	
	Schemes	Numerical	Testbed	Numerical	Testbed	Numerical	Testbed
UE to ARn	IMS	76%	67%	50%	50%	71%	65%
	MIP-IMS	81%	72%	61%	65%	77%	71%
UE to CN	IMS	71%	71%	50%	42%	71%	71%
	MIP-IMS	83%	76%	61%	57%	77%	77%

Figure 3.18 elucidates the values of *Gm, Mw* and *Cx* are 60, 60, 60 respectively for 10 handovers in case of IMS and MIP-IMS methods. In comparison, values for our proposed scheme are significantly low i.e. 20, 20 and 0 respectively. Our scheme completely removes the need for *Cx* commands.

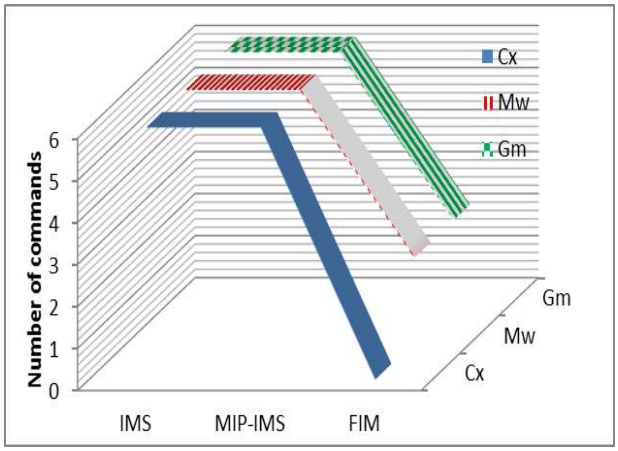

Figure 3.18 Number of *Cx, Mw* and *Gm* commands

3.10. Packet Loss

We have set G = 50 pkts/sec as used by [59]. On a constant handover delay, we have measured loss of packets for IMS, MIP-IMS and FIM. Packet loss is directly proportional to delay of handover [54] and it can be observed from the figure 3.19. For a handover loss of packets are 44400 bytes, 57600bytes and 22200bytes for IMS, MIP-IMS and FIM schemes respectively. It is observed that proposed scheme FIM decreases the packet loss 50% than IMS scheme and 61% than MIP-IMS scheme.

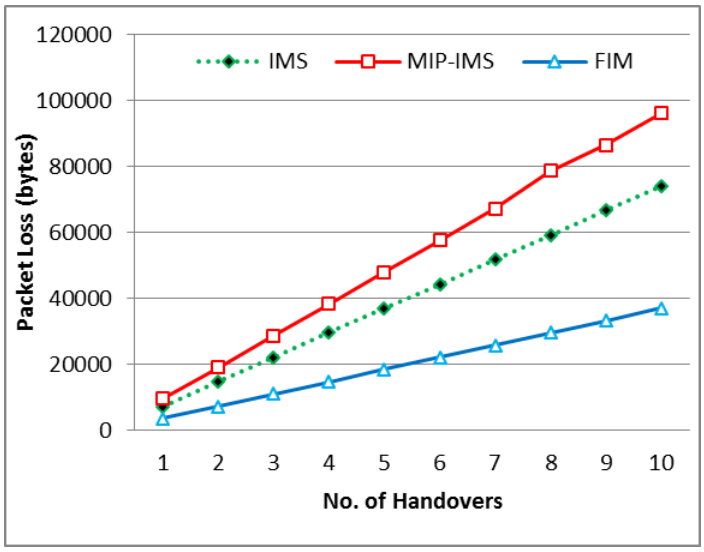

Figure 3.19 Number of handovers vs and Packet Loss

3.11. SIP Session Delay

To test the delay of our proposed scheme (FIM) for SIP messages, an experiment is run after handover. The delay time of SIP session is captured by using Wireshark [70]. Figure 3.20 shows the time of SIP session that confirms the reduction of delay.

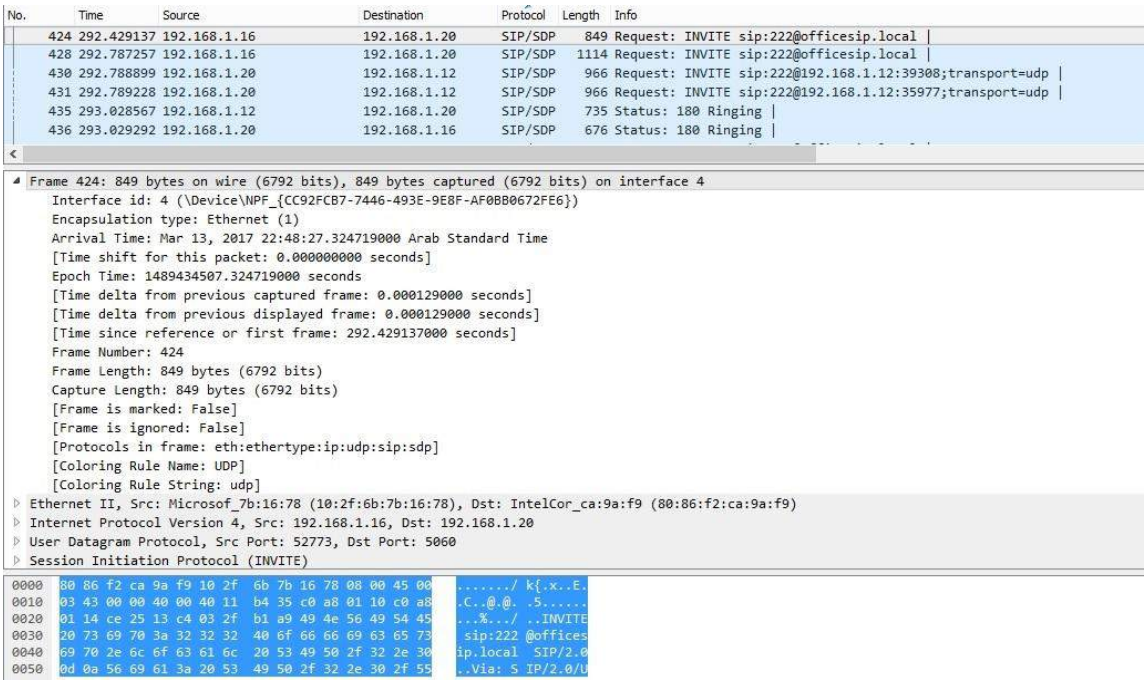

Figure 3.20 Analysis of FIM using Wireshark

3.12. Chapter Summary

In this chapter we have offered a complete method for registration with its sub phases (authentication, authorization and transfer of IPSec SAs) in IMS in case of handover. Our method reduces media disruption delay, number of commands of Cx, Gm and Mw. It also reduces number of packet loss thus making it efficient and secure. Our proposed method proposed a subsequent request HANDOVER and enables a flag when UE was in session with a CN before handover. With the help of this special flag, de-registration is eliminated because system considers that UE may get registered again in IMS. So the process must be fast because UE is in session with a CN and delay should be minimized. Due to no de-registration, parameters for authentication and authorization are stored in system. So registration process is also reduced to 2 messages.

We showed the results for our proposed scheme used for handover scenarios in IMS. We evaluated results of our scheme based on 3 parameters.
Schemes compared are as follows:

1. Standard IMS
2. MIP-IMS Schemes
3. FIM Schemes

Evaluation metrics:

1. Media disruption time
2. Number of Commands.
3. Packet loss

In next chapter we will discuss the second phase of our research i.e. establishment of IPSec SAs between UE and new P-CSCF after handover. Signaling delay of proposed scheme and comparison of results with other schemes will also be explained.

CHAPTER 4

4. EFFICIENT MECHANISM FOR SECURITY ASSOCIATIONS

4.1. Introduction

Security architecture of IMS is driven by 3GPP and 3GPP2 security standards. SIP [3] is an application protocol that is also used for *IPSec SAs* establishment between *UE* and IMS during registration. IMS security is necessary in terms of confidentiality, integrity and authentication. *UE* should be the authorized one because IMS is responsible for the charging as well. *UE*'s identity fraud can be protected if *UE* is authorized in IMS. *IPSec SAs* are established between *UE* and IMS in order to ensure that the interface between these two entities (Gm interface) is secured. Otherwise the attacks by some methods are possible [60] e.g. attack by the BYE method, CANCEL method and REGISTER method.

In this chapter, the proposed scheme for the establishment of IPSec SAs between UE and new P-CSCF is discussed. We will explain the signaling delay caused by the process of SA establishment during handover. We will discuss the transmission delay, processing delay and queuing delay separately. The common methods used for handling SAs incase of mobility will be defined and their results for signaling delays will be compared with standard IMS method and with our proposed method. In this chapter we will evaluate signaling delay caused by Context transfer protocol based approaches, the standard IMS handoff and our proposed scheme for giving solution to IPSec SAs establishment when UE is in mobility.

4.2. Proposed Method

The main problem during re-authorization after handover is that *SA* establishment is dependent on registration process in IMS. After handover, it causes delay because whole

procedure of registration and *SA* establishment is repeated along with authentication. Schemes proposed to reduce this delay by transferring context of *IPSec SAs* from old P-CSCF to new P-CSCF so that process of *SA* establishment can be reduced. But it is not always valid as the *SAs* are established between *UE* and P-CSCF after negotiating security parameters. There is a need for a scheme where *SAs* must be negotiated between *UE* and new P-CSCF after handover instead of transferring the context from old P-CSCF to new P-CSCF. In SCTM [52], context is transferred from old P-CSCF to new P-CSCF before actual handover in order to save time. However, there is no negotiation of *SA* establishment between *UE* and new P-CSCF.

We present "**E**fficient **M**echanism for **S**ecurity **A**ssociation" (EMSA) during re-authorization where *IPSec SAs* are established between *UE* and new *P-CSCF*. It introduces a flag "sessionContinued" to prevent network initiated de-registration phase. If a *UE* is already in a session with the Corresponding Node (*CN*) before the switch over to new network, then this flag turns on. Otherwise it is turned off. It reduces latency of re-authorization phase after mobility by avoiding the "de-registration" in case the flag is enabled. A subsequent request *EMSA-R* along with a response message *EMSA-OK* is proposed in our scheme. In the re-authorization phase it establishes *IPSec SAs* between *UE* and new *P-CSCF* in less number of messages that reduces signaling delay, *VHO* delay and packet loss. There is no context transfer and no new mobility protocol is needed in our scheme. Within the SIP capabilities it reduces signaling delay and latency of handover caused by *IPSec SA* establishment. Our scheme is compared with other schemes by a test bed and numerical analysis as well that yields the efficiency of our scheme over existing solutions.

We have explored that as per our study there is no specific solution given for the efficient and secure establishment of *IPSec SAs* between *UE* and new *P-CSCF* with the help of SIP solely. During handover scenarios, *UE* has to be transferred from one *AN* to the another with less delay to have a good QoS. Our scheme gives a mechanism to establish *IPSec SAs* after handover in a secure manner.

In EMSA, *EMSA-R* and *EMSA-OK* messages in SIP are proposed for the negotiation of parameters and transferring key with less number of messages to reduce delay. *EMSA-R* and *EMSA-OK* are shown in table 4.1. *EMSA-R* is a subsequent request that is why it doesn't traverse *I-CSCF* to know *S-CSCF*. Thus it reduces number of messages as well.

Table 4.1 SIP message format for EMSA

EMSA-R
EMSA-R sip:home1.fr.SIP/2.0 *Via: SIP/2.0/UDP [5555::1:2:3:4];branch=0uetb* *Route:sip:[5555::a:f:f:e];lr* *Max-Forwards: 70* *From: sip:user@home1.fr;tag=pohja* *To:sip:user@home1.f* *Contact: sip:[5555::1:2:3:4};expire=600000* *dPCSCF:sip[6666::d:e:e:f]* *sec-client:tls;q=0.2,IPSec3gpp;q=0.1;alg=hmac-sha-1-96;* *spi-c=9865432;spi-s=8764321;port-c=8642;port-s=7531* *Authorization:* *Digest username="user1@home1.ims,* *Response="083493483927jdhfjshfj"* *Call-ID:ahedew23398fk* *CSeq: 22 EMSA-R* *Content-Length:0*
EMSA-OK
EMSA-OK sip:home1.fr.SIP/2.0 *Via: SIP/2.0/UDP [5555::5:6:7:8];branch=0uetb* *From:sip:user@home1.f* *To: sip:user@home1.fr;tag=pohja* *Sec-verify:tls;q=0.2,IPSec3gpp;q=0.1;alg=hmac-sha-1-96;* *spi-c=9865432;spi-s=8764321;port-c=8642;port-s=7531* *WWW-Authenticate:ik="1232dskfdjfhfj4545kjvk";* *ck="jdshfsdjfh4535345kdfdkgjf"* *Call-ID:ahedew23398fk* *CSeq: 22 EMSA-OK*

Content-Length:0

4.2.1. Phases of Proposed Scheme and Algorithms

Our solution reduces delay for the establishment of *IPSec SAs* after handover by reducing the steps to transfer keys and negotiation of security mechanisms, algorithms and ports. Figure 4.1 elucidates the phases for EMSA.

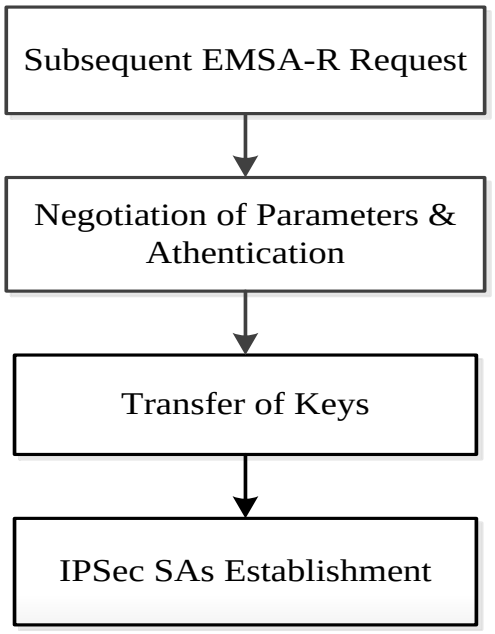

Figure 4.1 Phases of EMSA during handover

In first phase, *UE* generates *EMSA-R* subsequent request due to the status of sessionContinued flag i.e. "enabled". The *sessionContinued* flag is introduced to prevent de-registration of *UE* from IMS when it handovers to new *AN*. It gets disabled when *UE* cancelled a session with *CN* otherwise it is enabled to show that *UE* is still in a session and disconnected from *AN* for handover purpose only. In this way network initiated de-registration is avoided and states of *UE* registration is maintained in *UE* and IMS servers i.e. *RES* (response), keys and *IPSec SAs* between *UE* and old *P-CSCF*. *UE* sends *EMSA-R*

request to old *P-CSCF* along with the *RES* and *IP* address of new *P-CSCF*. This request is encapsulated in already established *IPSec SAs* between *UE* and old *P-CSCF*.

EMSA-R At UE

```
IF sessionContinued == true then
  Construct method == EMSA-R
  Route “EMSAm-R” to old P-CSCF
Route “EMSA-R” to newP-CSCF
ELSE
  Route “REGISTER” to old P-CSCF
ENDIF
```

EMSA-R at old P-CSCF

```
PCSCFold receives request
IF method == "EMSA-R"      THEN
     Via =  discoveredP-CSCF;
     Integrity-Protected = “yes”;
    Route “EMSA-R” to S-CSCF
ELSE  IF  method  ==  “REGISTER”
THEN
        Via = P-CSCFold;
        Integrity-Protected = “no”;
 route "REGISTER" to ICSCF
ENDIF
IF status == "401" THEN
   STATE Remove CK, IK
ELSE
  reply("500","P-CSCF Error Rem CK,
IK");
ENDIF
IF status == "200" THEN
       Route “OK” to UE
       Savelocation()
ELSE
       reply("500","P-CSCF   Error   on
location");
ENDIF
IF status == "408" THEN
       reply("504","Server Time-Out");
ENDIF
ENDIF
```

In second phase, negotiation of security parameters and algorithms starts *UE* sends *EMSA-R* to new *P-CSCF* along with *RES* and *security-client* headers. *Security-client* header contains security parameters like algorithms, server and client ports at *UE*. This negotiation

completes when new *P-CSCF* sends its security parameters in security-verify header to *UE* in *EMSA-OK* response.

EMSA-R at new P-CSCF

```
PCSCFnew Receives Request
IF method == "EMSA-R" THEN
Save IPSec Parameters
ELSEIF method == REGISTER THEN
Route "REGISTER" to I-CSCF
IF status == "401" THEN
STATE Remove CK, IK
ELSE
reply("500","P-CSCF Error Rem CK,
IK");
ENDIF
```

In third phase, *S-CSCF* receives *EMSA-R* request from old *P-CSCF*. Due to *RES, S-CSCF* knows the authenticity of *UE*. *EMSA-R* contains the information of new *P-CSCF* that is sent to *S-CSCF*. Old *P-CSCF* doesn't put its own *IP* address in *Via* header rather it adds the *IP* address of newly discovered *P-CSCF*. In this way the response comes back to new *P-CSCF* instead of old *P-CSCF*. *UE* has the keys already before any handover. *S-CSCF* sends the response *EMSA-OK* with keys in *WWW-Authenticate* header to new *P-CSCF*. New *P-CSCF* saves the keys before sending response *EMSA-OK* to *UE*.

EMSA-R at S-CSCF

```
SCSCF receives request
IF  method=="EMSA-R"
  IF RES == XRES & integrity-protected
== true then
    Route "EMSA-OK" to new P-CSCF

ELSEIF method == "REGISTER"
   IF RES != XRES then
      Create User-challenge( );
      route(Service-Routes);
     reply("401", "Unauthorized -
Challenging UE");
  ELSEIF RES == XRES then
     Set -status == "200"
    Route "OK" to ICSCF
  ENDIF
 ENDIF
```

ENDIF

In forth phase, new *P-CSCF* saves the keys from *S-CSCF* and forwards the *EMSA-OK* response to *UE* after adding security mechanism, algorithms and ports in *security-server* header. *IPSec SAs* are established between *UE* and new *P-CSCF* now. After that *security-verify* will be used to encapsulate every message sent between *UE* and new *P-CSCF*. Lifetime is sent to *UE* in *EMSA-OK* response by adding 30 seconds in *UE*'s Registration lifetime taken from *contact* header.

EMSA-OK at new P-CSCF
IF status == "EMSA-OK" *STATE Remove CK,IK* *STATE Put security-verify* *Route "EMSA-OK" to UE* *ELSE* *reply("500","P-CSCF Error on saving location");* *ENDIF*

Figure 4.2 explores the establishment of *IPSec SAs* after handover in a visual manner where step are explained as follows.

Steps (1) – (5): *UE* prepares *EMSA-R* request, add public and private ids of *UE* along with *RES* and sends it to old P-CSCF. *UE* adds *security-client* header to EMSA-R and sends this request to new P-CSCF for negotiation of security parameters.

Step (6) – (11): Old P-CSCF forwards *EMSA-R* to S-CSCF that prepares *EMSA-OK* response, adds keys after authentication and sends the response to new P-CSCF due to address in *Via* header. New P-CSCF saves the keys that came from S-CSCF. It forwards *EMSA-OK* to UE along with *security-server* header that contains security parameters. In this way *SAs* are established between *UE* and new P-CSCF.

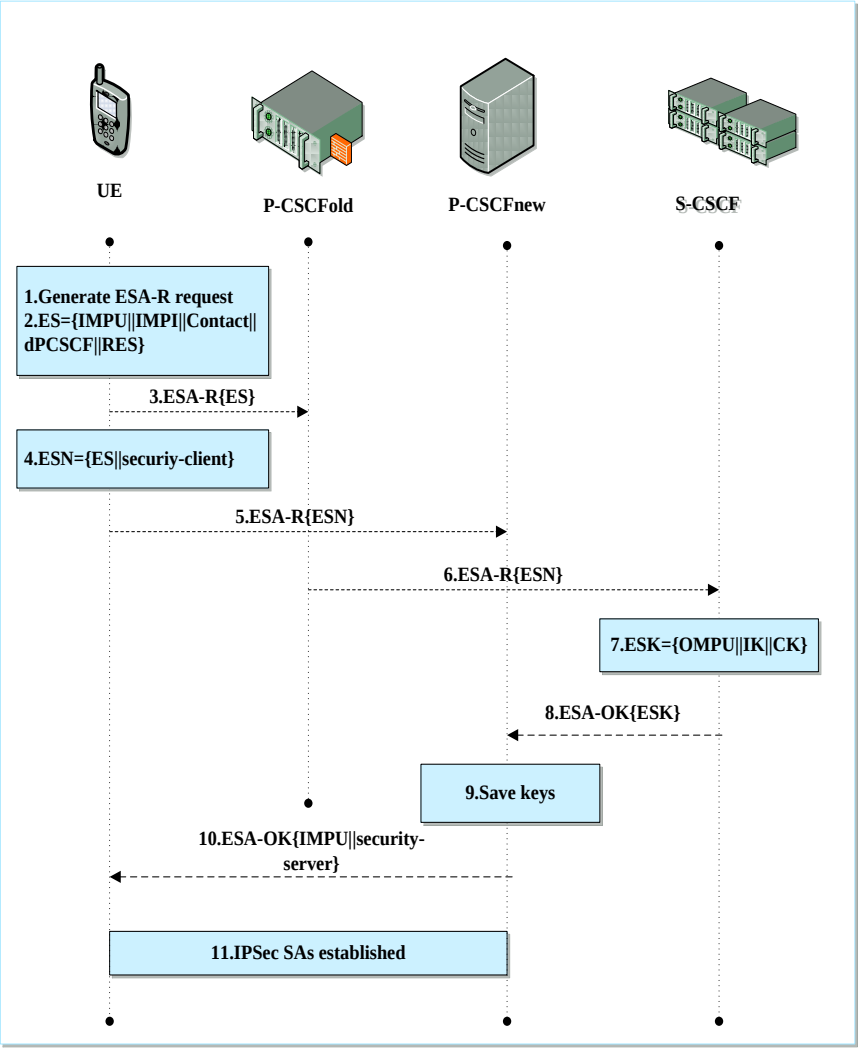

Figure 4.2 Proposed Scheme for SA Establishment

4.3. Signaling Delay

In this section we analyze the signaling delay in the establishment of IPSec SAs during mobility. We have considered transmission, processing and queuing delay for the analysis. We have focused on the delay caused by IMS/SIP IPSec SAs establishment when UE switches from one network to another. This will enable researchers to implement IMS with NGMN real time environment. We have compared the results of standard IMS scheme for re-authorization, SCTM [52] and our proposed scheme in this

chapter. It shows that our scheme is better than in reducing transmission delay, processing delay and queuing delay. Our scheme is better in reducing number of messages and packet loss as well.

Delay in IMS signaling for SA establishment is calculated according to (1):

$$D_{IMS} = D_{Transm} + D_{Process} + D_{Queue} \quad (1)$$

4.3.1. Transmission Delay

Transmission delay of SIP messages can be found with the help of following expression [47].

$$T_t = \mathrm{D} + (\mathrm{k}-1)\tau + \mathrm{Tr}(1) \times \left(\frac{(1-\mathrm{p_r})(1-(2\mathrm{p_r})^{\mathrm{N_m}}}{(1-{p_r}^{N_m})(1-2p_r)} - 1 \right) \quad (2)$$

here *D* denotes the end-to-end propagation delay, k denotes the number of frames in UDP datagram, τ is the inter frame time, pr is probability of retransmission of packet, maximum number of transmissions in SIP is denoted by Nm. (that is 7), and initial value of retransmission timer is denoted by Tr (1) that gets doubled, according to SIP protocol, after each retransmission.

In case of IMS total transmission delay without RLP is as follow.

$$\mathrm{D_T} = 4 \times \mathrm{T_t} \quad (3)$$

In case of SCTM total transmission delay in IMS without RLP is given as,

$$\mathrm{D_T} = 4 \times \mathrm{T_t} \quad (4)$$

In our proposed approach (EMSA) total transmission delay in IMS without RLP is,

$$\mathrm{D_T} = 3 \times \mathrm{T_t} \quad (5)$$

4.3.2. Processing Delay

The number of messages a node receives is the node's processing delay. Equation 6 shows the total processing delay in IMS when UE undergoes the handover and establishes IPSec SAs again. Equation 7 shows the total processing delay in SCTM scheme. Equation 8 shows the total processing delay on IMS entities for SA establishment proposed by our scheme (EMSA).

For standard IMS

$$D_{P_{IMS}} = 2d_{UE} + 4d_{Pn} + 4d_{I-CSCF} + 4d_{S-CSCF} + 6d_{HSS} \quad (6)$$

For SCTM

$$D_{P_{SCTM}} = d_{UE} + 2(d_{P_{new}} + d_{p_{old}} + d_{I-CSCF} + d_{S-CSCF}) + d_{HSS} \quad (7)$$

For our Proposed Scheme (ESA)

$$D_{P_{EMSA}} = d_{UE} + 2d_{Pnew} + d_{Pold} + d_{S-CSCF} \quad (8)$$

Figure 4.4 elucidates that for 1000 number of users that handovers to new *AN*, the processing delay in milliseconds is 28000ms for IMS re-authorization and 16000ms for SCTM scheme whereas it is 5000ms for our proposed EMSA. Proposed solution EMSA shows that processing delay is significantly less than other approaches as number of users increase. One of the reasons is that EMSA prevents the processing delay of de-registration phase on entities. Similarly for 1700 number of users that handovers to new *AN*, the processing delay is 47600ms, 27200 and 8500ms for IMS, SCTM and EMSA schemes respectively. EMSA shows 82% improvement than conventional IMS re-authorization and 68% improvement than SCTM in case of decreasing processing delay when number of users increase.

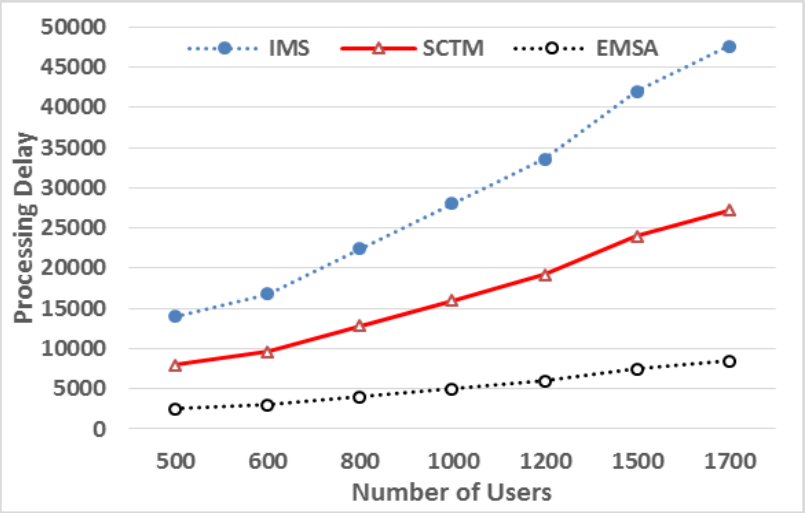

Figure 4.3: Processing Delay Vs No. of Users

4.3.3. Queuing Delay

We compute the queuing delay on IMS entities during SA establishment. This delay is due to queuing of packets at the nodes. Total queuing delay is the sum of queuing delay on UE, P-CSCF, I-CSCF and S-CSCF based on waiting time formulae. M/M/1 queuing model is used for calculating the delay on UE and CSCF servers because they do dedicated jobs. Figure 4.5 shows the queuing model for analyzing queuing delay in our scheme ESA.

According to M/M/1 queuing model for UE and CSCF servers, the queuing delay estimates at UE and CSCF servers [48] are given as,

$$D_{UE} = \frac{1}{\mu_{UE} - \lambda_{UE}} \quad (9)$$

$$D_{P-CSCF} = D_{S-CSCF} = D_{I-CSCF} = \frac{\rho_s}{\lambda(1 - \rho_s)} \quad (10)$$

In the analysis, the arrival rate of SIP message at CSCF (λ) is considered as $\lambda < \mu$ [49] and the service rate (μ) is 4×10^{-4}. The server load on CSCF (ρs) is given as λ / μ [49].

$$D_{ASN-GW} = D_{SGSN} = \frac{\rho_s}{\lambda(1-\rho_s)} \quad (11)$$

Queuing delay at gateway to *WIMAX* (D_{ASN-GW}) and queuing delay at gateway to *LTE* (D_{SGSN}) is given in equation (11).

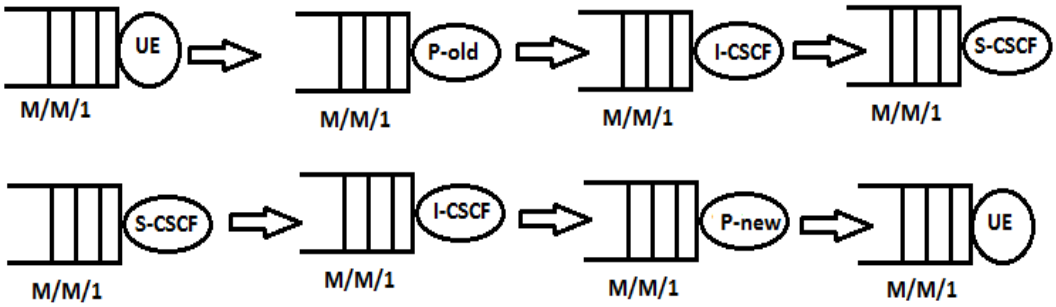

Figure 4.4: Queuing model for analyzing the IMS queuing delay for SA establishment in proposed scheme

For standard IMS, total queuing delay is as follows.

$$D_{Q_{IMS}} = 2D_{UE} + 4(D_{P_{new}} + D_{I-CSCF} + D_{S-CSCF}) + 6D_{HSS} \quad (12)$$

For SCTM, queuing delay can be found as,

$$D_{Q_{SCTM}} = D_{UE} + 2(D_{Pnew} + D_{Pold} + D_{HSS} + D_{I-CSCF} + D_{S-CSCF} \quad (13)$$

For Proposed Scheme EMSA, queuing delay can be calculates as,

$$D_{Q_{EMSA}} = 1D_{UE} + 2D_{Pnew} + 1D_{Pold} + 1D_{S-CSCF} \quad (14)$$

Figure 4.6 elucidates the queuing delay at old *P-CSCF* versus SIP messages arrival rate at old *P-CSCF*. For the SIP messages arrival rate of 0.00025ms at old *P-CSCF*, the queuing delay is 13332ms, 26664ms and 6666ms for IMS, SCTM and EMSA schemes respectively. The queuing delay at old *P-CSCF* in conventional IMS re-authorization scheme is less than SCTM scheme due to de-registration. Whereas our proposed scheme avoids de-registration at all and it also establishes *IPSec SAs* in lesser number of messages so it shows less queuing delay at old P-CSCF than conventional IMS and SCTM schemes. In this case our scheme shows 50%

improvement than conventional IMS re-authorization scheme and 75% improvement than SCTM scheme. Figure 4.7 elucidates the queuing delay at new *P-CSCF* versus arrival rate of SIP messages at new *P-CSCF*. For SIP messages arrival rate of 0.00025ms at new *P-CSCF*, the queuing delay is 26664ms for IMS scheme and 13332ms for both SCTM and EMSA schemes. In this case our scheme shows 50% improvement than IMS scheme.

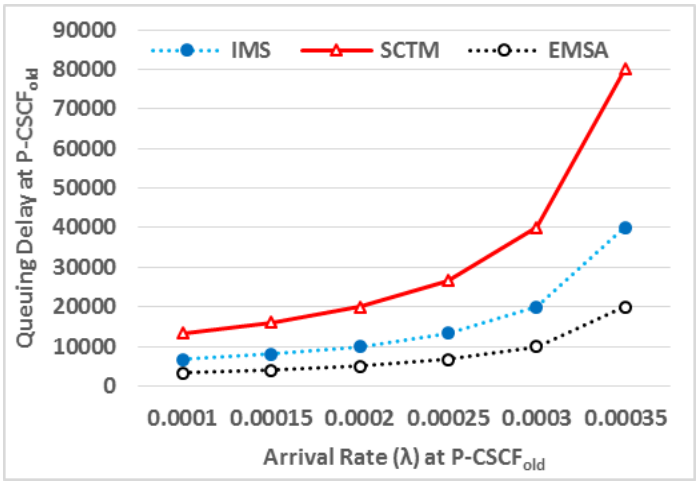

Figure 4.5 Queuing Delay vs Arrival Rate at old P-CSCF

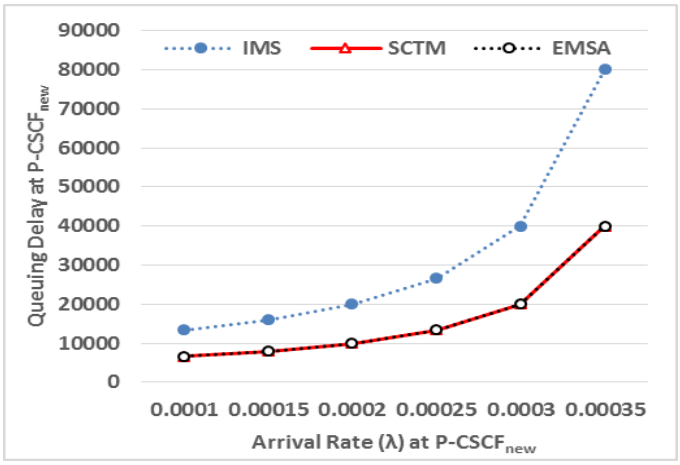

Figure 4.6 Queuing Delay vs Arrival Rate at new P-CSCF

Figure 4.8 elucidate queuing delay on *S-CSCF* when SIP messages arrival rate increases for IMS, SCTM and EMSA schemes. It illustrates that for the arrival rate of 0.0003ms on *S-CSCF*, the queuing delay is 80000ms ,60000ms and 10000ms for IMS, SCTM and EMSA schemes respectively. The queuing delay doubles on *S-CSCF* i.e. 160000ms, 120000ms and

20000ms for IMS, SCTM and EMSA schemes respectively when arrival rate of SIP messages is 0.00035ms. EMSA scheme shows improvement of 87% than IMS scheme and 83% improvememnt than SCTM scheme. Our scheme EMSA shows such good results because it also reduces the queuing delay at S-CSCF caused by de-registration. Figure 4.9 shows the results of queuing delay at *I-CSCF* versus arrival rate of SIP messages at *I-CSCF*. Our scheme shows no queuing delay at *I-CSCF* because of proposed subsequent request *EMSA-R, UE* doesn't need to traverse *I-CSCF*. Whereas for arrival rate of 0.0002ms at *I-CSCF* the queing delay is 20000ms and 10000ms for IMS and SCTM schemes. Our scheme EMSA reduces this delay 100%.

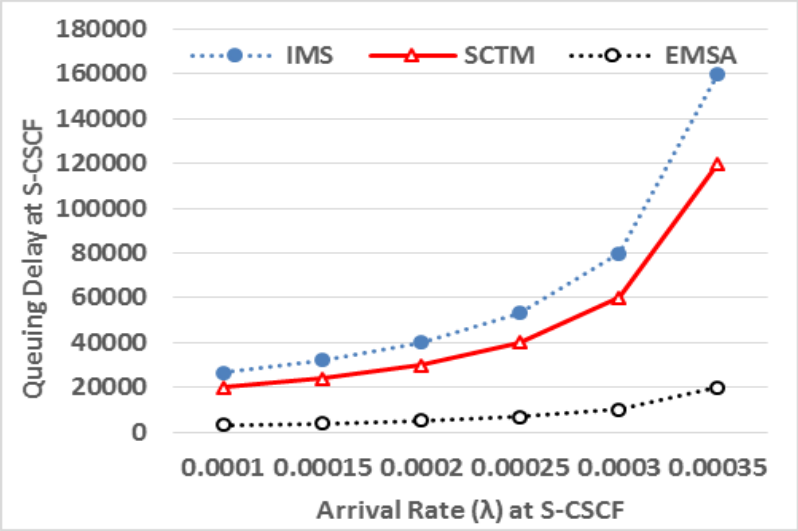

Figure 4.7 Queuing Delay Vs Arrival Rate at S-CSCF

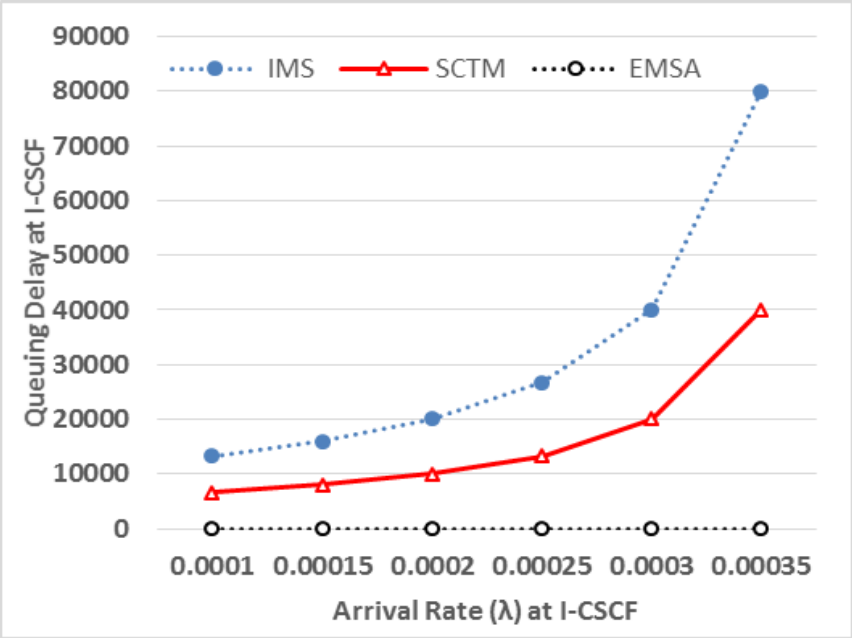

Figure 4.8 Queuing Delay Vs Arrival Rate at I-CSCF

4.4. Results and Analysis

We have setup a test bed for IMS by implementing related servers as illustrated in figure 4.10 and a number of experiments are performed. [58] is used to implement IMS entities on workstations Intel core *i* 3 1.7 GHz with *RAM* is 4 GB connected with four *ANs* through *IP* network. *UE* is an android phone with one GB RAM that connects to *AN* via *WLAN AP* and is in session with another android phone. During experiments, *UE* is first connected to AR_1 and on getting weak signals from AR_2, it disconnects from AR_1 and connects to AR_2 and then it re-authenticates with IMS. We have measured the delay for IMS [2] and our EMSA. *UE* and *CN* were in a VoIP session and exchanging *RTP* (real-time transport protocol) packets encoded with G.711 codec at 20ms interval from each other. *UE* observes the signaling strength of *APs* for handover. When the exponential smoothing value of the strength ($E_t = gE_{t-1} + (1-g)g_t, 0 \leq g \leq 1$) goes below the threshold value then it connects to *AP* that has strong signal strength. Where a_t is *AP*'s signaling strength at time *t* and E_t is the result at time *t* and g = 0.5 in the experiment as in [27]. In a number of experiments we altered the number of routers to vary delay between *UE* and *CN* to get the results of the schemes. Table 4.1 shows the evaluation parameters for test bed.

Table 4.2 Evaluation parameters for Test bed

Parameters	*Values*
Network Servers	P-CSCF, I-CSCF, S-CSCF, HSS
Servers' Physical Type	Wired Physical
UEs' Physical Type	Wireless Physical
Antenna Type	Omni Antenna
Delay	0 – 90 milliseconds
Number of Hops	1 – 10
Number of Handovers	1 – 10

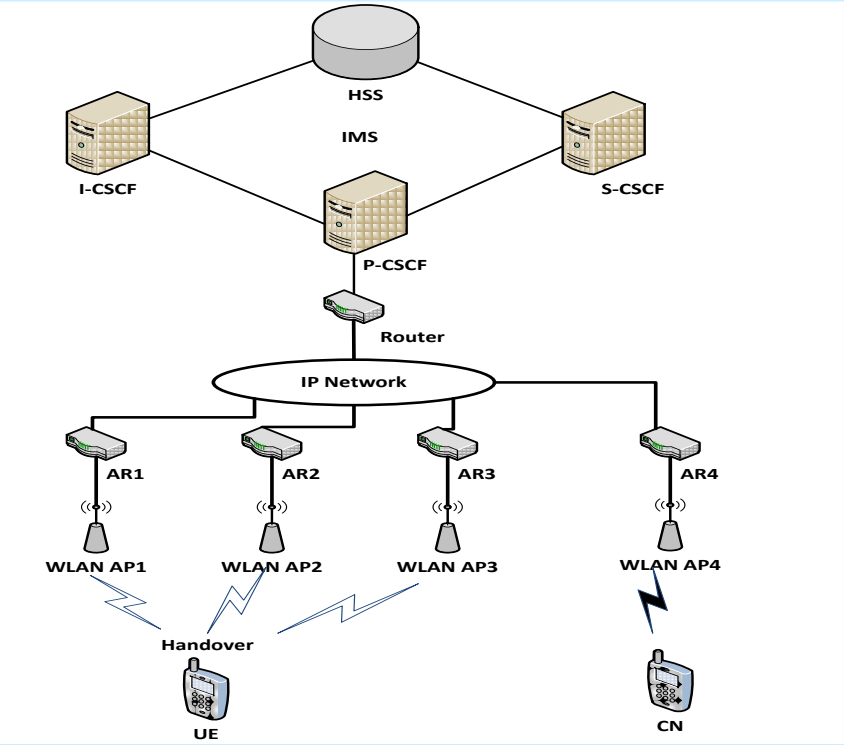

Figure 4.9 Testbed Setup for EMSA Evaluation

We have analyzed signaling delay for establishment of *IPSec SAs* during handover by considering transmission, processing and queuing delay. Signaling delay is measured for IMS [2], SCTM [52] and EMSA scheme. Delay in IMS signaling is sum of transmission delay D_{Transm}, processing delay $D_{Process}$ and queuing delay D_{Queue}.

4.5. Total IMS Authorization Delay

The authorization delay for IMS is a total of transmission delay, processing delay and queuing delay as given in equation (15). In [2], the number of messages exchanged for the establishment of *IPSec SAs* between *UE* and new *P-CSCF* is 22. In SCTM [52], number of messages exchanged for the IMS authorization procedure is 10. In our proposed scheme the number of messages to establish *IPSec SAs* between *UE* and new *P-CSCF* is 5. Figure 4.11 elucidates the number of messages for IMS, SCTM and EMSA scheme.

$$D_{IMS-Auth} = D_{T-Auth} + D_{P-Auth} + D_{Q-Auth} \quad (15)$$

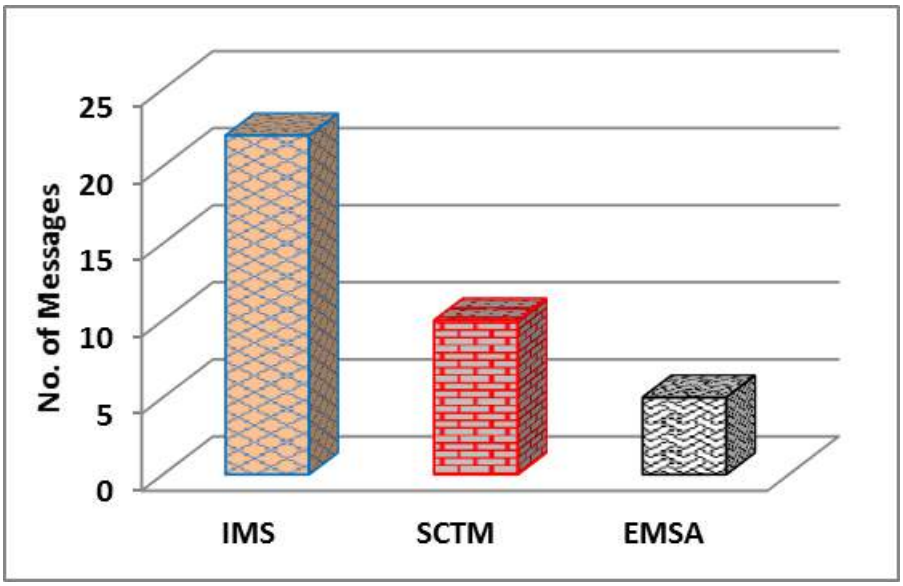

Figure 4.10 Number of messages for re-authorization

4.6. Handover Latency and Packet Loss

Figure 4.12 elucidates the authorization delay versus number of handovers. Plenty of were carried out in order to test the authorization delay for conventional IMS scheme and proposed EMSA scheme. It shows an authorization of 8800ms for IMS scheme whereas 3600ms authorization delay for EMSA scheme for a handover. Approximately on average our proposed scheme shows an improvement of 59% in reducing this delay than IMS scheme. Figure 4.13 elucidates the packet loss for IMS and EMSA schemes. For a number of

handovers packet loss was observed and it shows an improvement of 50% by EMSA scheme in reducing packet loss than conventional IMS scheme. For example when for a handover packet loss was 51800 bytes in IMS scheme then it was 25900 bytes for EMSA scheme.

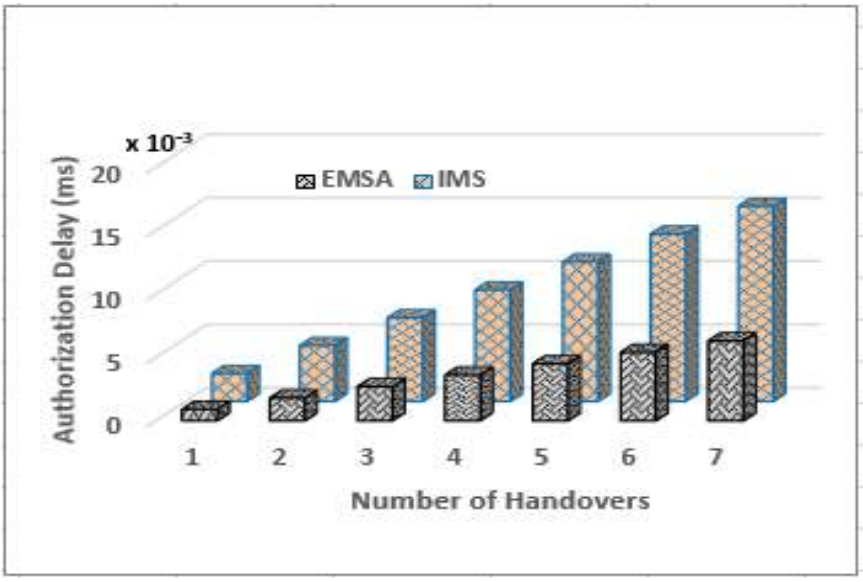

Figure 4.11 Number of handovers vs Delay time

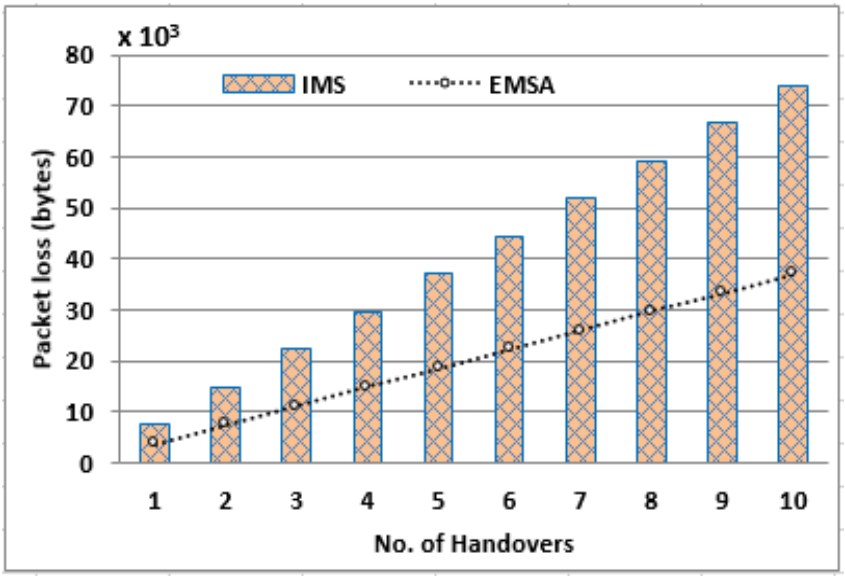

Figure 4.12 Number of handovers vs Packet Loss

4.7. Chapter Summary

In this chapter we defined a mechanism to establish IPSec SAs between UE and P-CSCF when UE handovers to new AN. This method ensures authorization and authentication of UE as well. In this chapter it is explained that how the key is transferred and security parameters are negotiated for SA establishment.

Our proposed method reduces the signaling delay as well as it reduces number of messages. Authorization delay, packet loss, transmission delay, processing delay and queuing delay are calculated for following schemes:

1. Standard IMS scheme
2. SCTM
3. Our proposed scheme (EMSA)

Also a test bed implementation is described to find out the results. Comparisons of schemes are also done in this chapter.

CHAPTER 5

5. Conclusion and Future Work

5.1. Contributions

In our research we have proposed a complete framework for mobility scenario in IMS for registration that covers authentication, authorization, authorization, transfer of IPSec SAs to new P-CSCF and establishment of IPSec SAs with new P-CSCF. These issues are addressed by our two proposed schemes namely FIM and EMSA.

For a UE to be connected to any Access Network, it is a must to be registered in IMS. In case of mobility, UE changes its Access Network and gets de-registered from IMS. On connecting to new Access Network UE gets registered again in IMS. The process of de-registration and registration in IMS causes higher delay, more number of commands and packet loss.

In IMS after handover there is no solution when the UE changes its IP address. In literature survey we found out that for this problem researchers have proposed MIPv6 and one of its versions i.e. FMIPv6 to be a part of mobility in IMS scenarios. We have found out in our research that there are integration issues of MIPv6 with IMS. In our research we found out that no one gave the solution to change of IP address of P-CSCF. In our proposed scheme we gave solution to both the changes in IP addresses i.e. change of IP address of UE and change of IP address of P-CSCF. We have not proposed to integrate any new protocol instead we suggested to do it within SIP capabilities. For registration of new IP addresses, authentication, integrity protection and transfer of IPSec SAs to new P-CSCF, we proposed a subsequent request HANOVER. Our solution is not only secure but it also reduces VHO delay in order to achieve minimum MDT and packet loss. Our solution also reduces number of commands in between the IMS servers.

We observed that after handover, there is a need for re-negotiation of IPSec SAs between UE and new P-CSCF. For this purpose we introduced subsequent request/response i.e. EMSA-R and EMSA-OK. This not only reduces number of commands but it also manages to establish SAs with less transmission delay, processing delay, queuing delay, authorization delay and packet loss.

In literature survey we have found out that delay is reduced by transferring context from old P-CSCF to new P-CSCF. This is used to transfer IPSec SAs as well. For this purpose mostly CXTP (Context Transfer Protocol) is proposed in literature. This is an overhead to integrate a new protocol. Our solution used no new protocol for reducing delay and IPSec SAs establishment problem.

For reducing signaling cost or number of messages, researchers proposed to do context transfer. Our solution reduces number of messages by not doing any context transfer from old P-CSCF to new P-CSCF or by integrating any new protocol.

Our solution compared our results with MIP based solution and context transfer based solutions. We have also compared our results with standard methods of IMS. We have found out that our results are better than all of them. We have concluded that MIP and CXTP base methods give overhead of adding or taking help from new protocols. Because integrating MIP and CXTP doesn't avoid standard registration phase. Our scheme addressed these problems in general:

1. Change of IP address of UE
2. Change of IP address of P-CSCF
3. Re-establishment of SAs with new P-CSCF
4. Number of commands
5. Vertical Handover Delay
6. Signaling delay
7. Packet loss

Hence it is analyzed that handover is an important issue and it needs to be handled within IMS phases instead of integrating new protocols. New protocols come with an

overhead of integration as well as complexity of the process. Our scheme gives a complete solution for mobility by slight changes within the process of registration.

5.2. Future Work

In order to achieve good quality of service (QoS) between UE and CN, there should be less delay and less packet loss. We have given solutions to registration phase and its sub phases of IMS along with establishment of IPSec SAs after handover. In future it is a need to work on session establishment phase between UE and CN after handover. Number of messages should be reduced for INVITE message for mobility scenario. Session establishment phase must be proposed that reduces signaling delay and packet loss as well.

References

[1] Miikka Poikselka, Georg Mayer, " The IMS: IP Multimedia Concepts and services, third edition". John Wiley and Sons, 2009.

[2] G. Camarillo and M. A. Garcia-Martin, "The 3G IP Multimedia Subsystem (IMS):Mergining the Internet and the Cellular Worlds". WILEY, 2006.

[3] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. RFC 3261: SIP: Session Initiation Protocol, 2002.

[4] 3rd Generation Partnership Project. 3GPP TS 24.229: Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3.

[5] 3GPP: IP Multimedia subsystem (IMS) Service Continuity; Stage 3 (Release 9), TS 24.237 V9.1.0, 3rd Generation Partnership Project (3GPP) (2009).

[6] Etemad, Kamran. "Overview of mobile WiMAX technology and evolution."*Communications magazine, IEEE* 46.10 (2008): 31-40.

[7] Zhang, Chenghui, Sirikiat Lek Ariyavisitakul, and Meixia Tao. "LTE-advanced and 4G wireless communications [Guest Editorial]."*Communications Magazine, IEEE* 50.2 (2012): 102-103.

[8] Ophir, Lior, Yigal Bitran, and Itay Sherman. "Wi-Fi (IEEE 802.11) and Bluetooth coexistence: issues and solutions." *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on.* Vol. 2. IEEE, 2004.

[9] Haukka, Tao, Aki Niemi, and Gabor Bajko. "Method and system for authentication in IP multimedia core network system (IMS)." U.S. Patent Application No. 10/369,497.

[10] Chiang, Wei Kuo, and Wen-Yen Chang. "Mobile initiated network executed SIP-based handover in IMS over heterogeneous accesses." *International Journal of Communication Systems* 23.9-10 (2010): 1268-1288.

[11] Ohta, Masataka. "Overload protection in a SIP signaling network." *Internet Surveillance and Protection, 2006. ICISP'06. International Conference on.* IEEE, 2006.

[12] Corici, Marius Iulian, Fabricio Carvalho De Gouveia, and Thomas Magedanz. "A network controlled QoS model over the 3GPP system architecture evolution." *Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on.* IEEE, 2007.

[13] Munir, Arslan. "Analysis of SIP-based IMS session establishment signaling for WiMax-3G networks." *Networking and Services, 2008. ICNS 2008. Fourth International Conference on.* IEEE, 2008.

[14] Jin, Haipeng, and A. C. Mahendran. "Using SigComp to compress SIP/SDP messages." *Communications, 2005. ICC 2005. 2005 IEEE International Conference on.* Vol. 5. IEEE, 2005.

[15] Ghribi, Brahim, and Luigi Logrippo. "Understanding GPRS: the GSM packet radio service." *Computer Networks* 34.5 (2000): 763-779.

[16] Aboba, B., and M. Beadles. "RFC 2486: The network access identifier, January 1999." *Status: PROPOSED STANDARD.*

[17] 3GPP TS 23.002, "Network Architecture," rel. 5, v. 5.6.0, http://www.3gpp.org/, Mar. 2002.

[18] 3GPP TS 23.228 V6.10.0 (2005-06). IP multimedia subsystem.

[19] 3GPP, "Numbering, addressing and identification", 3GPP TS 23.003 v10.0.0, December 2010.

[20] S. Faccin, P. Lalwaney, and B. Patil, "IP Multimedia Services: Analysis of Mobile IP and SIP Interactions in 3G Networks," *IEEE Communications Magazine*, pp. 113–120, Jan. 2004.

[21] X. Chen, J. Rinne, J. Wiljakka, and M. Watson, "Problem Statement for MIPv6 Interactions with GPRS/UMTS Packet Filtering," *IETF*, Jan. 2006.

[22] Renier, Thibault, et al. "Mid-session macro-mobility in IMS-based networks." *Vehicular Technology Magazine, IEEE* 2.1 (2007): 20-27.

[23]T. Renier et al, "MIPv6 Operations in IMS-based Networks," *Proceedings of WPMC'06*, Sept. 2006.

[24]D. Johnson, C. Perkins, J. Arkko, RFC 3775 Mobility Support in IPv6, IETF, June 2004.

[25] Koodli, R.: Mobile IPv6 Fast Handovers, RFC 5568, Internet Engineering Task Force.

[26] Farahbakhsh, R and Movahhedinia, N: Two Fast Handover Solutions for the IMS Handover in the Presence of Mobile IPv6 by Using Context Transfer Procedures. International Conference on Innovations in Information Technology, 2008 (IIT 2008), pp. 568-572 (online), DOI:10.1109/INNOVATIONS.2008.4781677 (2008).

[27] Manabo Ito, Satoshi Komorita, Yoshinori Kitatsuji, Hidetoshi Yokota, "IMS based Fast Session Handover With Available Network Resources Discovery of Access Network", Journal of information processing, Vol.20 no.1 308-318 (Jan 2012).

[28] K.Larsen, E. Matthiesen, H-P. Schwefel, G. Kuhn, "Optimized Macro Mobility within the 3GPP IP Multimedia Subsystem", in the proceedings of ICWMC'06, July 2006.

[29] T. Renier, H. Fathi, H.-P. Schwefel, G. Kuhn, and R. Prasad. Enhanced MIP-based mid-session macro handover for ims-controlled stateful applications. WPMC2007, 2007.

[30] Thanh, N.H., Hang, L.T., Van Yem, V., Thu, N.Q., Dung, N.X., Multimedia Session Continuity with Context-Aware Capability in IMS-based Networks Proceedings of IEEE Sixth International Symposium on Wireless Communication Systems 2009 (ISWCS'09), September 7-10, 2009, Siena-Tuscany, Italy

[31] Manabo Ito, Satoshi Komorita, Yoshinori Kitatsuji, Hidetoshi Yokota, "IMS based Fast Session Handover With Available Network Resources Discovery of Access Network", Journal of information processing, Vol.20 no.1 308-318 (Jan 2012).

[32] Yang, Shun-Ren, and Wen-Tsuen Chen. "SIP multicast-based mobile quality-of-service support over heterogeneous IP multimedia subsystems." *Mobile Computing, IEEE Transactions on* 7.11 (2008): 1297-1310.

[33] Yang, X. and Agarwal, A. Multicast Mobility in SIP Layer. *IEEE Vehicular Technology Conference*, 2004.

[34] Nazari, A., But, J., Branch, P., & Vu, H. PRIME: Preregistration for IMS mobility enhancement. *IEEE international conference on multimedia and expo, pp,* (2012). 920–924.

[35] IEEE, "IEEE Standard for Local and metropolitan area networks – Media Independent Handover Services," *IEEE Standard 802.21*, 2009.

[36] Nazari, Abolfazl, et al. "UPTIME: an IMS-based mobility framework for next generation mobile networks." *Wireless Networks* 20.7 (2014): 1967-1979.

[37] P. Bellavista, A. Corradi, L. Foschini, An IMS vertical handoff solution to dynamically adapt moble multimedia services, in: Computers and Communications, ISCC 2008, IEEE Symposium on 6-9 July 2008.

[38] Edward, E. Prince, and V. Sumathy. "Performance analysis of a context aware cross layer scheme for fast handoff in IMS based integrated WiFi–WiMax networks." *Pervasive and Mobile Computing* 17 (2015): 79-101.

[39] Bongkyo Moon, "Fast and Secure Session Mobility in IMS-based Vertical Handover Scenario", International Journal of Multimedia and Ubiquitous Engineering Vol.9, No.9 (2014), pp.171-188.

[40] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. RFC 2401, Internet Engineering Task Force, November 1998.

[41] S. Kent and R. Atkinson, "IP Authentication Header (AH)", Internet Engineering Task Force, RFC 2402, November 1998.

[42] "IP Encapsulating Security Payload (ESP)", Internet Engineering Task Force, RFC 2406, November 1998.

[43] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)", Internet Engineering Task Force, RFC 2409, November 1998.

[44] "Security Mechanism Agreement for the Session Initiation Protocol (SIP)", Internet Engineering Task Force, RFC 3329, January 2003.

[45] "The Use of HMAC-SHA-1-96 within ESP and AH", Internet Engineering Task Force, RFC 2404, November 1998.

[46] J. Loughney, M, Nakhjiri, C. Perkins, and R. Koodli, "Context Transfer Protocol (CXTP)," Internet Engineering Task Force, RFC 4067 (Experimental), July 2005.

[47] H. Fathi, S. Chakraborty, and R. Prasad, "Optimization of SIP session setup delay for VoIP in 3G wireless networks," *IEEE Trans. Mobile Computer*, vol. 5, no. 9, Sep. 2006, pp. 1121-1132.

[48] L. Kleinrock, QUEUING SYSTEMS vol. I: Theory, Wiley, New York, 1975

[49] Banerjee, Nilanjan, et al. "Analysis of SIP-based mobility management in 4G wireless networks." *Computer communications* 27.8 (2004): 697-707.

[50] Gautam, Sumit, and Durga Prasad Sharma. "Solution to Reduce Voice Interruption Time during Handover of VoLTE Call in Enhanced Single Radio Voice Call Continuity." *Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on*. IEEE, 2015.

[51] N. Akkari, "An IMS-based integration architecture for WiMax/LTE handover," *Computer Networks*, vol. 57, no. 18, pp. 3790-3798, 2013

[52] E. Edward, "A Context Transfer Model for Secure Handover in WiMAX/LTE Integrated Networks," International Journal of Mobile Computing and Multimedia Communications (IJMCMC), pp. 56-74, 2014.

[53] A. Bagubali, V. Prithiviraj and P. Mallick, "Performance analysis of IMS based LTE and WIMAX integration architectures," *Alexandria Engineering Journal,* vol. 55, p. 3229–3238, 2016.

[54] Munasinghe, S. Kumudu and J. Abbas, "Analytical Modeling of IMS based Interworking in Heterogeneous Mobile Data Networks," in *Proceedings of International Conference on Signal Processing and Communication Systems*, Gold Coast,Australia, 2007.

[55] E. Prince, "A novel seamless handover scheme for WiMAX/LTE heterogeneous networks," *Arabian Journal for Science and Engineering,* vol. 41, no. 3, pp. 1129-1143, 2016.

[56] J. Kempf, "Problem Description: Reasons for Performing Context Transfers Between Nodes in an IP Access Network.," IETF RFC 3374, 2002.

[57] Pérez-Costa, Xavier, T.-M. Marc and H. Hannes, "A Performance comparison of mobile IPv6, hierarchical mobile IPv6, fast handovers for mobile IPv6 and their combination," *IEEE. Mobile Comp. Commu. Rev,* p. 5–19, 2003.

[58] Magedanz, Thomas, W. Dorota and K. Karsten, "The IMS playground@ FOKUS-an open testbed for generation network multimedia services.," in *Testbeds and Research Infrastructures for the Development of Networks and Communities, 2005. Tridentcom 2005. First International Conference on. IEEE.*, 2005.

[59] Cai, Lin, X. Yang and W. M. Jon, "VoIP over WLAN: Voice capacity, admission control, QoS, and MAC," *International Journal of Communication Systems.* vol. 19, no. 4, pp. 491-508, 2006.

[60] Belmekki, Elmostafa, B. Mostafa and B. Abdelhamid, "Enhances security for IMS client," in Next Generation Networks and Services (NGNS), IEEE, 2014.

[61] M. Abu-Lebdeh, S. Jagruti, G. Roch and W. Constant, "Cloudifying the 3GPP IP multimedia subsystem for 4G and beyond: A survey," *IEEE Communications Magazine* vol. 54, no. 1, pp. 91-97, 2016

[62] Ngongang, Serge Fabrice Mbianda, Navid Tadayon, and Georges Kaddoum. "Voice over Wi-Fi: feasibility analysis." *Advances in Wireless and Optical Communications (RTUWO), 2016.* IEEE, 2016.

[63] Chagh, Youssef, Zouhair Guennoun, and Youness Jouihri. "Voice service in 5G network: Towards an edge-computing enhancement of voice over Wi-Fi." *Telecommunications and Signal Processing (TSP), 2016 39th International Conference on.* IEEE, 2016.

[64] Ali, Muntadher Alshaikh, Amir Esmailpour, and Nidal Nasser. "Traffic density based adaptive QoS classes mapping for integrated LTE-WiMAX 5G networks." *Communications (ICC), 2017 IEEE International Conference on.* IEEE, 2017.

[65] Tu, Guan-Hua, et al. "New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks." *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.* ACM, 2016.

[66] Haddar, Imane, Brahim Raouyane, and Mostafa Bellafkih. "Generating a service broker framework for service selection and SLA-based provisioning within network environments." *Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on.* IEEE, 2017.

[67] Voznak, Miroslav. "Speech bandwith requirements in IPsec and TLS environment." *WSEAS International Conference. Proceedings. Recent Advances in Computer Engineering.* No. 13. WSEAS, 2009.

[68] Ala-Laurila, Juha, Harri Hansén, and Juha Salvela. "Transfer of security association during a mobile terminal handover." U.S. Patent No. 6,587,680. 1 Jul. 2003.

[69] Doraswamy, Naganand, and Dan Harkins. *IPSec: the new security standard for the Internet, intranets, and virtual private networks*. Prentice Hall Professional, 2003.

[70] Chappell, Laura A. *Wireshark network analysis: the official Wireshark certified network analyst study guide*. Protocol Analysis Institute, Chappell University, 2010.