Efficient Security Associations Establishment Using IPSec in IMS after Handover in NGMN

Shireen Tahira[1], Ata Ullah[2], Humaira Ashraf[3], Muhammad Sher[3]

[1] Department of Computer Science and Engineering, Air University, Pakistan.
[2] Department of Computer Science, National University of Modern Languages, Pakistan.
[3] Department of Computer Science and Software Engineering, International Islamic University, Pakistan.
shireentahira381@gmail.com, aullah@numl.edu.pk, humairaashraf12@yahoo.com, m.sher@iiu.edu.pk

Abstract

Next generation mobile networks allow smart phones to constantly switch and handover its networks to access internet for multimedia applications. To avail multimedia services, IP Multimedia Subsystem (IMS) is a 3gpp based framework for all types of networks. UE has to register with IMS where it first contacts to P-CSCF for establishing IPSec Security Associations (SA). During handover to a new network, de-registration from IMS is imposed that results in expiring IPSec SAs with old P-CSCF. UE has to establish new IPSec SAs with new P-CSCF that causes more signaling delay due to more number of messages. This paper presents a novel solution to establish SAs in IMS after handover where a flag is used to block de-registration until expiry. IPSec SAs are negotiated by reducing steps of re-authorization without appending new protocol in IMS. We tested our scheme on a test bed and compared the results with existing IMS re-authorization schemes. Our approach dominates the preliminaries in reducing transmission delay, processing delay and queuing delay as well as VHO delay and packet loss.

Keywords: IMS, Handover, IPSec Security Associations (SAs), Delay, Packet loss

1 Introduction

Next Generation Mobile Networks (NGMN), include mobile devices that are equipped with more than one interfaces in order to connect to different networks, i.e. WiMAX, Wifi, UMTS, LTE and in future 5G. Voice over Wi-Fi (VoWiFi) is emerging today as 5G technology. Its requirements are not complete yet but until 2018, 3gpp is planning to gather them to produce a standard [1]. Service control layer of NGMN is handled by IP Multimedia Subsystem (IMS) [2] that is developed by 3GPP. It provides QoS (Quality of Service), charging and integration of different services to these NGMNs. A WiMAX-3G convergence provides QoS for IMS to manage real time trafiic during mobility and reduces delay [3]. Due to handover from one network to another, *UE* (User Equipment) has to register in IMS again [4].Security architecture of IMS is driven by 3GPP and 3GPP2 security standards. SIP [5] is an application protocol that is also used for *IPSec SAs* establishment 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 [6] like BYE, CANCEL and REGISTER methods. Two *SAs* are bidirectional for receiving and sending [4] like *UE*'s client port to P-CSCF's server port where second *SA* is from the P-CSCF's client port to *UE*'s server port. Figure 1 illustrates the *IPSec SAs* establishment between two nodes. It provides confidentiality and integrity between two entities by negotiating security parameters and algorithms in *Register* request.

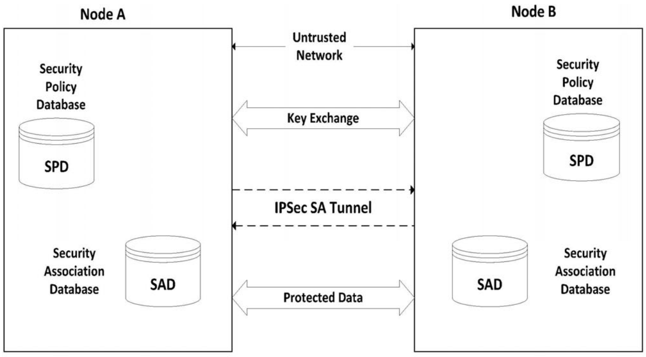


Figure 1. Establishment of IPSec SAs between 2 nodes

The main problem during re-authorization after handover is that after switching to a new network, *UE* has to go under the process of *IPSec SAs* establishment again in re-authorization. It takes more signaling delay to establish *IPSec SAs* during registration phase that leads to more packet loss, increased handover latency and more number of messages. Different schemes reduced this delay by transferring context of *IPSec SAs* from old P-CSCF to new P-CSCF but it is not always valid as the *SAs* are established between *UE* and P-

*Corresponding Author: Shireen Tahira; E-mail: shireentahira381@gmail.com

DOI: 10.3966/160792642019032002005

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 with less signaling delay.

This paper presents **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 *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 is proposed in our scheme. In 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. In our scheme, no need for context transfer and no new mobility protocol is required. It reduces signaling delay and latency of handover caused by *IPSec SAs* establishment. Our scheme is compared with other schemes to ensure dominance of our scheme.

This paper is sectioned as follows. Section 2 provides system model and problem statement. Section 3 consists of related work. Section 4 explores the proposed solution. Section 5 explains about results and analysis of EMSA using testbed scenario. Section 6 concludes our work.

2 System Model

In this section we describe important entities of IMS that interact after the handover. *UE* first discovers P-CSCF as all requests and responses are traversed through P-CSCF including *IPSec SAs* messages. I-CSCF routes the requests to appropriate S-CSCF and it also has an interface with the HSS. S-CSCF is the central node of IMS to download user profile from HSS which is central database for user-related data. Figure 2 elucidates the entities of IMS along with two *AN*s for handover scenario. After handover to new *AN2*, *UE* is attached to new P-CSCF by new *IPSec SAs* establishment.

During *SA* establishment, the *UE* and P-CSCF use the two REGISTER requests for registration and authentication. *UE* adds a *security-client* header field in REGISTER request containing security mechanism, authentication, encryption algorithm, client and server ports. Similar parameters are added by P-CSCF in *security-server* header to the 401 response along with a *q-value* to show preference. P-CSCF obtains and removes integrity and encryption keys (*IK* and *CK*) from 401 response. *IK* is used for *SAs* establishment. *SAs* are now ready to be used and next REGISTER request goes over these *SAs* as illustrated in Figure 3.

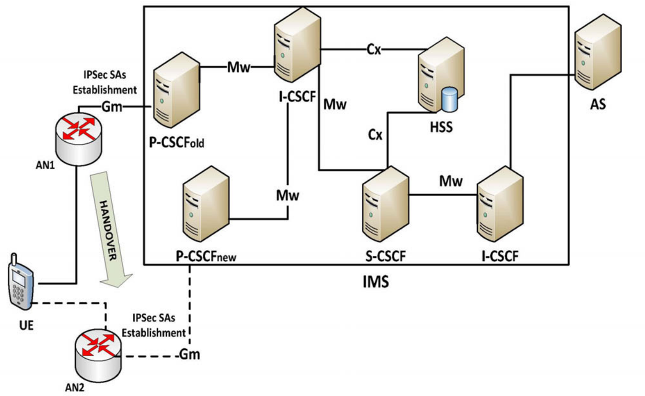


Figure 2. IMS architecture and handover

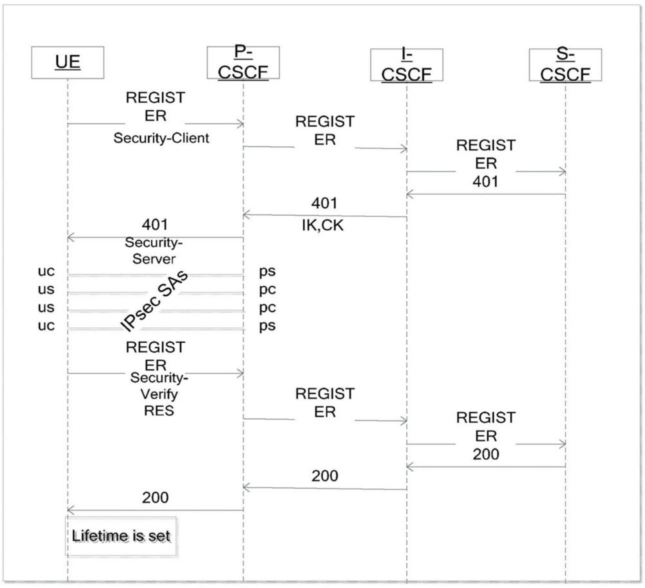


Figure 3. IMS registration and SA establishment

3 Related Work

A number of existing schemes reduce delay after handover in authorization phase. In existing solutions, it is suggested to transfer context of *SAs* or transfer the context within SIP. Moreover, early re-authorization was also explored to get connection request in advance. Following schemes show different approaches to reduce latency of *SA* establishment after handover.

3.1 Context Transfer with CXTP

UE has to establish *SAs* again by negotiating parameters and algorithms after handover when it gets registered in IMS. Larsen et al. has proposed to transfer *IPSec SAs* by transferring context from old P-CSCF to new P-CSCF. After that old P-CSCF sends context transfer request to new P-CSCF followed by the secret key for *IPSec SAs* establishment [7]. Most of the solutions utilized context transfer protocol (CXTP) [8]. It exchanges a number of extra messages that also causes delay.

3.2 Context Transfer in SIP and Early Re-authorization

Edward has proposed Secure Context Transfer Model (SCTM) [9] using pre-authorization 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 Access Network (*AN)*. Mobility information is obtained using MIH protocol. It reduces re-authorization messages from 22 to 10. It measures handoff delay as given in equation (1) where D_T_{Auth} is transmission delay, D_P_{Auth} is processing delay and D_Q_{Auth} is queuing delay.

$$D\_IMS_{Auth} = D\_T_{Auth} + D\_P_{Auth} + D\_Q_{Auth} \qquad \textbf{(1)}$$

In [10], a fast handoff is presented where new P-CSCF transfers context information using SIP header from old P-CSCF instead of re-registration. Key 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. It reduces handoff delay and packet loss whereas our proposed scheme reduces number of messages as well.

During pre-registration with IMS in [11-13], *UE* uses MIH protocol [14] to get mobility information and register in target network and IMS. As *UE* gets new IP address, it establishes *SAs* with new P-CSCF that reduces delay. During handover from WiFi to *3G* [15], *UE* pre-registers in 3G where *CN* establishes *SAs* on IP address used by *UE* on WiFi. After handoff, UE gets new IP address for SIP messages. A few schemes perform pre-processing by either exploiting MIH protocol or MIPV6 [16] and FMIPv6 [17] protocols. *IPSec* [18] provides confidentiality and integrity at third layer using Authentication Header (*AH*) [19] and Encapsulating Security Payload (*ESP*) [20]. *IPSec SAs* are established for secure exchange of data using IKE [21] key. Security mechanisms in IMS is ipsec-3gpp [22] whereas there are number of security mechanism used for VoIP networks incuding *IPSec-ike*, *ipsec-man*, *digest* and *TLS.*

3.3 SA Update with Minimum Number of Messages

Cheng and Chen have proposed to update *SAs* after handover with minimum number of messages [23]. It utilizes already stored *RES* to match it with *XRES* in IMS server for authentication in order to avoid the phase of authentication. For authorization phase it sends the new IP address and ports to IMS that is updated in servers. It reduces number of messages to update *SA*. However in our scheme we proposed to negotiate and establish new *SAs* between *UE* and new P-CSCF in less number of messages. In literature, we identified that mostly *IPSec SAs* are handled using context transfer from old P-CSCF to new P-CSCF. Schemes [9-11] do it within SIP header during pre-registration by knowing the new *AN* in advance due to MIH. Key for *IPSec SAs* is transferred i SIP during pre-registration. Cheng and Chen [23] suggest updating *SAs* with minimum number of messages. As SIP is solely running for registration according to *3gpp* so we suggested our solutions within the scope of SIP. Another thing in *IPSec SAs* establishment is the negotiations of security parameters between *UE* and P-CSCF. As per our study, we are the first one to solve it.

4 Proposed Solution

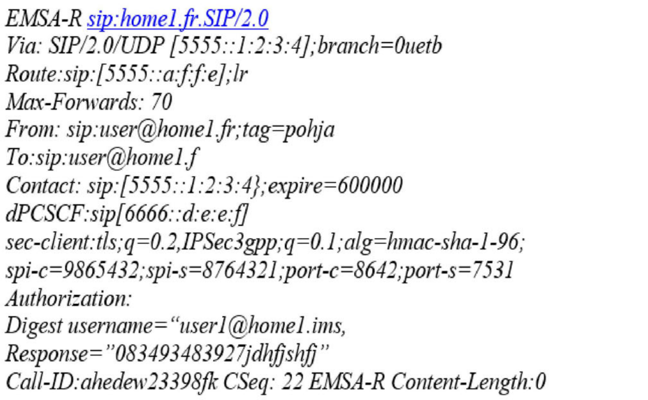
This section explains our proposed scheme that handles the re-authorization process when users are moving in an area and handovers to a new network. We have explored that as per our study there is no specific solution given for the efficient and secure establishment of *IPSec SAs* between *UE* and new 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. The notations used in the proposed solution EMSA are listed in Table 1.

Table 1. List of notations

Notation	Description
UE	User Equipment
AN	Access Network
QoS	Quality of Service
EMSA-R	Request Message
IPSec SAs	IPSec Security Associations
R_{ES}	Calculated response
CSCF	Call Session Control Function

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* shown in Table 2 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 2. SIP message format for 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
```

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 elucidates the phases for EMSA.

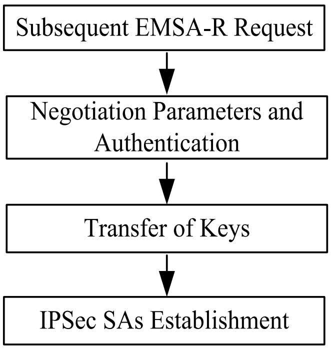
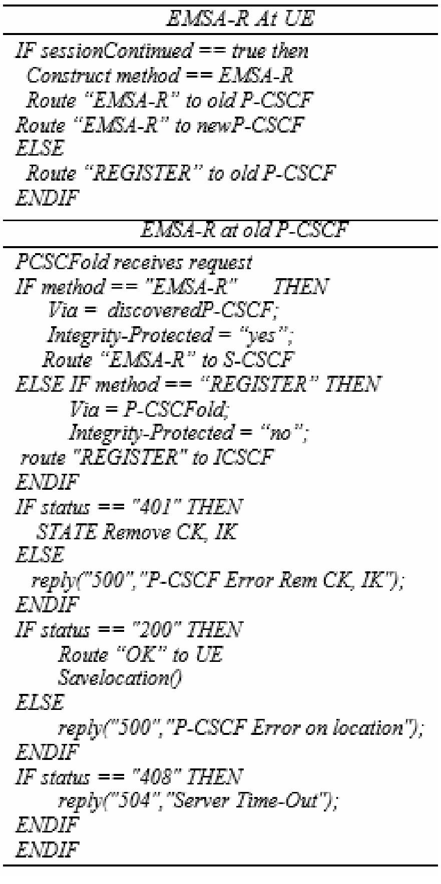

Subsequent EMSA-R Request
Negotiation Parameters and Authentication
Transfer of Keys
IPSec SAs Establishment

Figure 4. 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. Network initiated de-registration is avoided and states including *R*ES, keys and *IPSec SAs* between *UE* and old P-CSCF of *UE* registration is maintained at *UE* and IMS entities. *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*.



EMSA-R At UE

```
IF sessionContimued == true then
  Construct method == EMSA-R
  Route "EMSA-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* is 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.

Figure 5 explores *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.

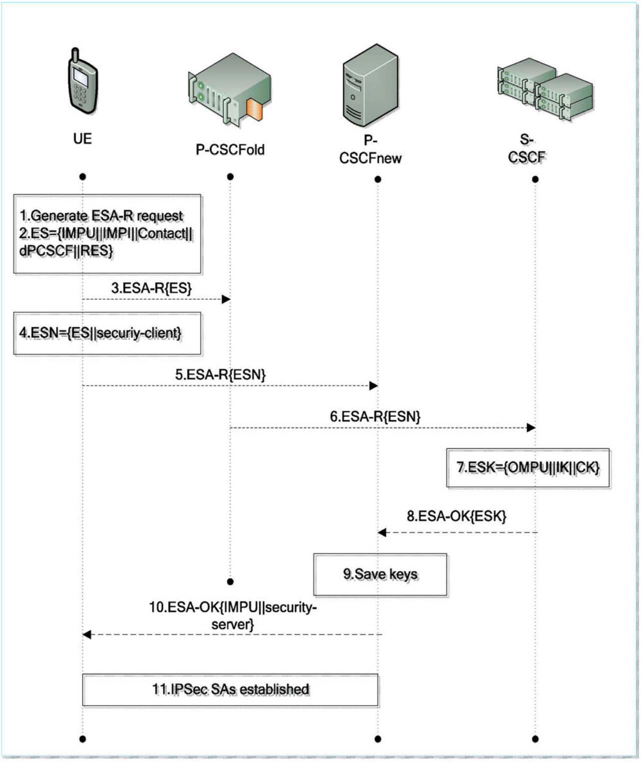


Figure 5. Proposed scheme for SA establishment

5 Results and Analysis

We have setup a testbed for IMS by implementing related servers as illustrated in Figure 6 and a number of experiments are performed. FOKUS [24] is used to implement IMS entities on workstations connected with four *ANs* through *IP* network. *UE* is an android phone 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. *UE* and *CN* in VoIP session, exchange *RTP* packets encoded with G.711 at 20ms interval. *UE* switches to nearing AP when signaling strength $(E_t = \mathcal{G}E_{t-1} + (1-g)g_t, 0 \le \mathcal{G} \le 1)$ goes below the threshold as in [25]. Table 3 shows the evaluation parameters for test bed.

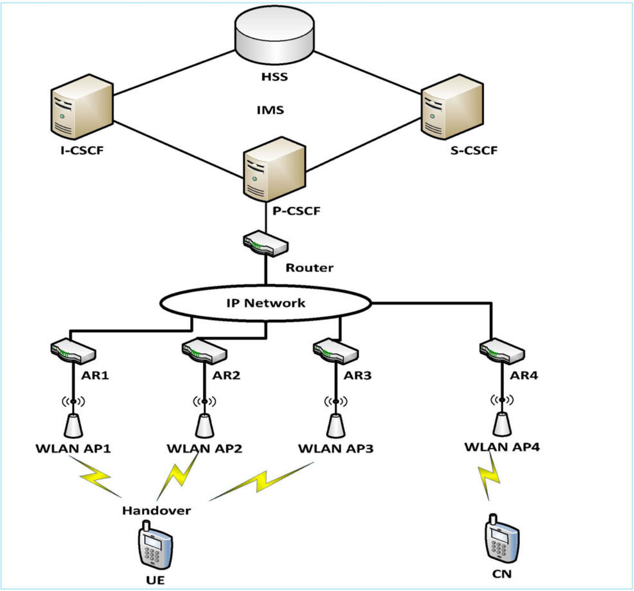


Figure 6. Testbed setup for EMSA evaluation

Table 3. 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

5.1 Transmission Delay

Transmission delay of SIP messages as given in equation (2) [26] where *D* denotes the end-to-end propagation delay, *k* denotes the number of frames in *UDP* datagram, *τ* is the inter frame time, p_r is probability of retransmission of packet, maximum number of transmissions in SIP is denoted by N_m. (that is 7), and initial value of retransmission timer is denoted by *Tr* (1) that gets doubled (according to SIP) after each retransmission. In case of IMS [4] and SCTM [9], total transmission delay without *RLP* is $4 \times \boldsymbol{T_t}$. Transmission delay of EMSA without *RLP* is $3 \times T_t$.

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

5.2 Processing Delay

The number of messages a node receives is the node's processing delay. Equation (3) shows the total processing delay in IMS when *UE* undergoes the handover and establishes *IPSec SAs* again. Equation (4) shows the total processing delay in IMS when *UE* undergoes the handover and does re-authorization with *SCTM* scheme. Equation (5) shows the total processing delay on IMS entities for *SA* establishment proposed by our scheme EMSA.

$$D_{P_{IMS}} = 2d_{UE} + 4d_{P_n} + 4d_{I-CSCF} + 4d_{S-CSCF} + 6d_{HSS} \quad \textbf{(3)}$$

$$D_{P_{SCTM}} = d_{UE} + 2(d_{P_{new}} + d_{P_{old}} + d_{I-CSCF} + d_{S-CSCF}) + d_{HSS} \quad \textbf{(4)}$$

$$D_{P_{EMSA}} = d_{UE} + 2d_{P_{new}} + d_{P_{old}} + d_{S-CSCF} \quad \textbf{(5)}$$

Figure 7 elucidates that for 1000 number of users that handover to new *AN*, the processing delay in milliseconds is 28000ms for IMS re-authorization and 16000ms for SCTM whereas it is 5000ms for our proposed EMSA. 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.

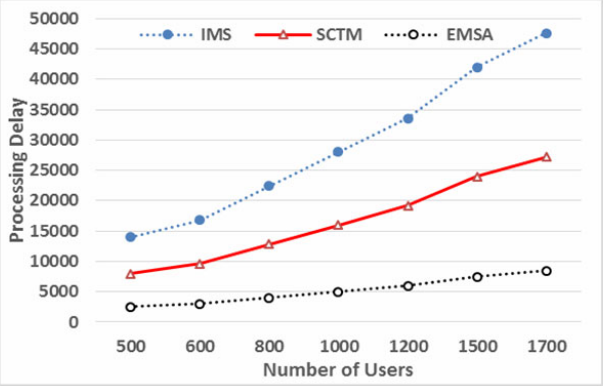


Figure 7. Processing delay vs. number of users

5.3 Queuing Delay

Delay is due to queuing of packets at the nodes where total delay is sum of delay on *UE*, *P-CSCF, I-CSCF* and *S-CSCF* based on waiting time. According to *M/M/1* queuing model [15], the queuing delay at *UE* $D_{UE} = 1/(\mu_{UE} - \lambda_{UE})$. In case of CSCF servers, the queuing delay is calculated using equation (6).

$$D_{P-CSCF} = D_{S-CSCF} = D_{I-CSCF} = \frac{\rho_s}{\lambda(1-\rho_s)} \quad \textbf{(6)}$$

The expression for D_{CN} is derived from the non-preemptive priority based *M/G/I* queue [27] given in equation (7) where μ_{CN} is processing rate of SIP messages at *CN*, ρ_s is load at *CN*, ρ_n is load of non SIP messages at *CN* and R = $\lambda_n X_1$ + $\lambda_{CN} X_{CN}$ / 2. Moreover, X_1 and X_{CN} are the second moments of μ_n and μ_{CN} and λ_n and λ_{CN} are the arrival rate of non-SIP and SIP messages at *CN* respectively.

$$D_{CN} = \frac{\frac{1}{\mu_{CN}}(1-\rho_n-\rho_s)+R}{(1-\rho_n)+(1-\rho_n-\rho_s)} \quad \textbf{(7)}$$

$$D_{ASN-GW} = D_{SGSN} = \frac{\rho_s}{\lambda(1-\rho_s)} \quad \textbf{(8)}$$

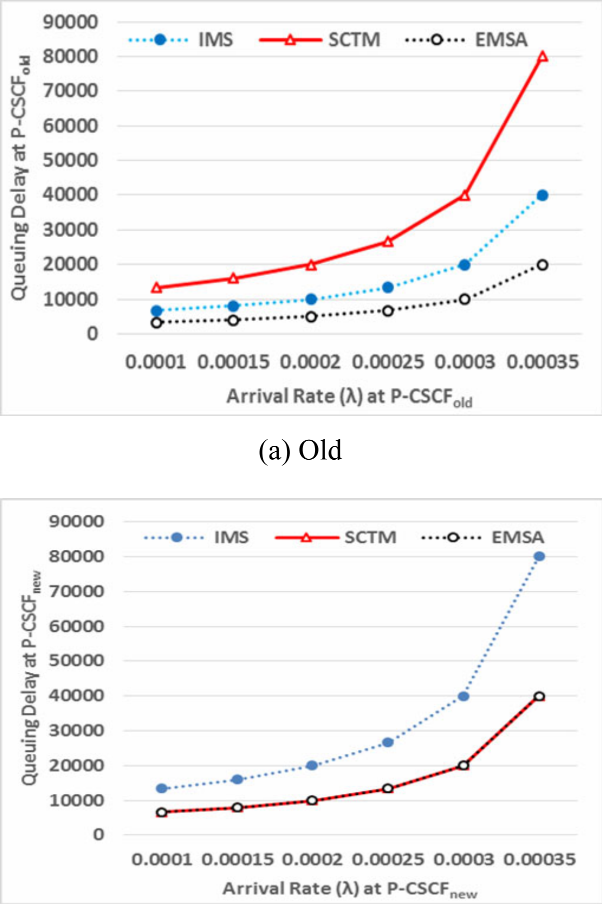
Queuing delay at gateway to WIMAX (D_{ASN-GW}) and at gateway to LTE (D_{SGSN}) is given in equation (8). Arrival rate of SIP message at CSCF (λ) is considered as λ< μ and service rate (μ) is 4×10^{-4}. Server load on CSCF (ρs) is given as λ/ μ [28]. Total queuing delays for IMS, SCTM, EMSA are given in equation (9), (10) and (11) respectively.

$$D_{Q_{IMS}} = 2D_{UE} + 4(D_{P_{new}} + D_{I-CSCF} + D_{S-CSCF}) + 6D_{HSS} \quad \textbf{(9)}$$

$$D_{Q_{SCTM}} = D_{UE} + 2(D_{P_{new}} + D_{P_{old}} + D_{HSS} + D_{I-CSCF} + D_{S-CSCF}) \quad \textbf{(10)}$$

$$D_{Q_{EMSA}} = 1D_{UE} + 2D_{P_{new}} + 1D_{P_{old}} + 1D_{S-CSCF} \quad \textbf{(11)}$$

Figure 8(a) elucidates queuing delay as 13332ms, 26664ms and 6666ms for IMS, SCTM and EMSA respectively for the SIP messages arrival rate of 0.00025ms at old P-CSCF. EMSA is 50% and 75% better than IMS and SCTM respectively. Figure 8(b) elucidates the queuing delay at new P-CSCF versus arrival rate of SIP messages at new P-CSCF. EMSA shows 50% improvement over IMS.

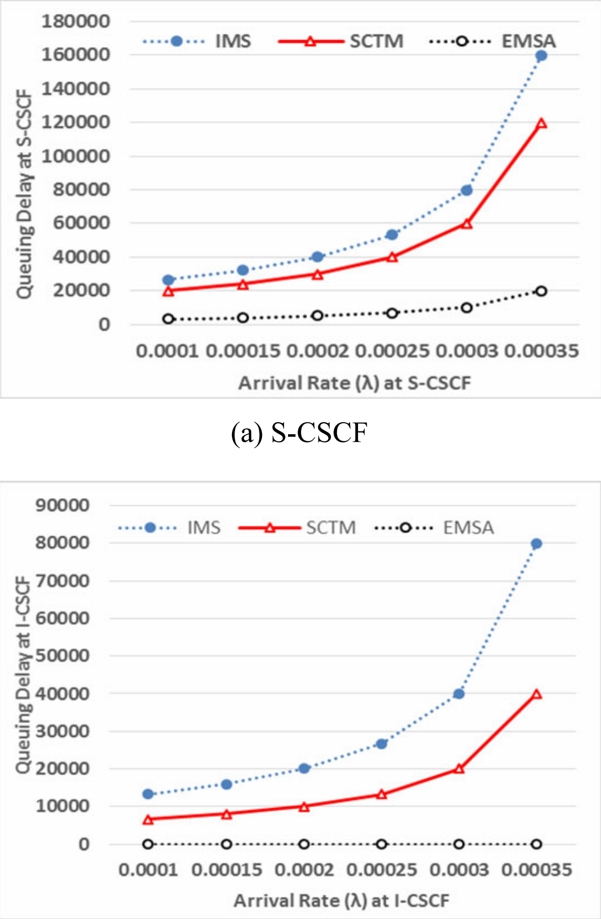


(a) Old

(b) New P-CSCF

Figure 8. Delay vs. arrival rate

Figure 9(a) elucidate that queuing delay is 80000ms ,60000ms and 10000ms for IMS, SCTM and EMSA schemes respectively for the arrival rate of 0.0003ms on S-CSCF wheras it doubles at 0.00035ms. EMSA scheme shows improvement of 87% than IMS and 83% as compared to SCTM. Figure 9(b) elucidates that for arrival rate of 0.0002ms at I-CSCF the queing delay is 20000ms and 10000ms for IMS and SCTM schemes. Our scheme shows no queuing delay at I-CSCF because of proposed subsequent request *EMSA-R, UE* doesn't need to traverse I-CSCF.



(a) S-CSCF

(b) I-CSCF

Figure 9. Delay vs Arrival Rate

5.4 Total IMS Authorization Delay

The authorization delay for IMS is a total of transmission delay, processing delay and queuing delay as given in equation (12). In [4], the number of messages exchanged for the establishment of *IPSec SAs* between *UE* and new P-CSCF is 22. In SCTM [9], 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 10 elucidates the number of messages for IMS, SCTM and EMSA scheme.

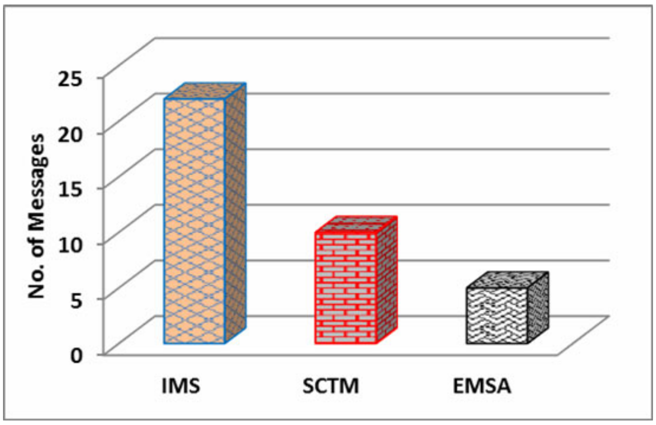


Figure 10. Number of messages for re-authorization

$$D_{IMS-Auth} = D_{T-Auth} + D_{P-Auth} + D_{Q-Auth} \qquad (12)$$

5.5 Handover Latency and Packet Loss

Figure 11 elucidates the authorization delay versus number of handovers. It shows an authorization of 8800ms for IMS scheme whereas 3600ms authorization delay for EMSA scheme for a handover. Approximately EMSA reduces 59% delay than IMS. Figure 12 elucidates that for number of handovers, packet loss shows an improvement of 50% when a handover packet loss was 51800 bytes in IMS scheme then it was 25900 bytes for EMSA scheme.

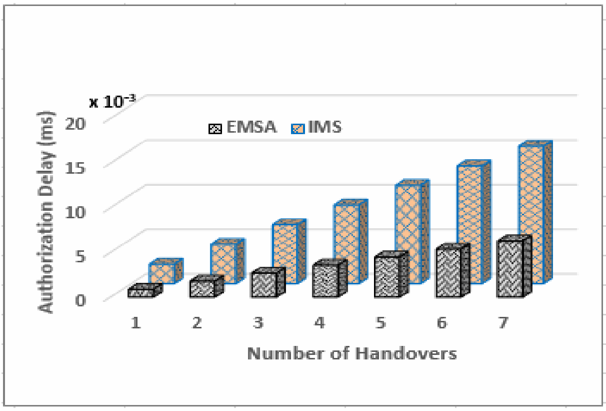


Figure 11. Number of handovers vs Delay time

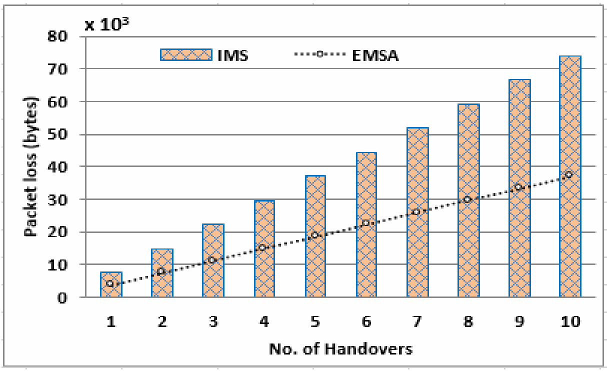


Figure 12. Number of handovers vs Packet Loss

6 Conclusion

This paper explores to establish *IPSec* SAs for re-authorization purpose after handover. It resolves the problem of frequent re-registration with complete steps. It caused more transmission, processing and queuing delays. Our work reduces the communication overhead and hence saving energy consumption. Moreover, we have discussed the delay caused by the process of establishing *SAs* after mobility. Our EMSA achieves 82% and 68% improvement as compared to conventional IMS and SCTM respectively for decreasing processing delay. In case of reducing queuing delay at old and new P-CSCF, our scheme achieves 50% improvement over IMS and 75% improvement over SCTM. For queuing delay at S-CSCF, the EMSA achieves 87% and 83% improvement as compared to IMS and SCTM respectively. In future 5G and 5G Xhaul [29] networks need more solutions for efficient establishment of sessions between UE and CN as small cells cause more handovers to happen.

References

[1] C. Youssef, G. Zouhair, J. Youness, Voice Service in 5G Network: Towards an Edge-computing Enhancement of Voice over Wi-Fi, *International Conference on Telecommunications and Signal Processing*, Vienna, Austria, 2016, pp. 116-120.

[2] M. Poikselkä, G. Mayer, *The IMS: IP Multimedia Concepts and Services*, John Wiley and Sons, 2013.

[3] G. Vijayalakshmy, G. Sivaradje, Convergence of WiMAX-3G QoS Architecture with IMS Signaling Analysis, *Journal of Internet Technology*, Vol. 16, No. 3, pp. 443-452, May, 2015.

[4] G. Camarillo, M.-A. García-Martín, *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds*, John Wiley and Sons, 2007.

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

[6] E. Belmekki, M. Bellafkih, A. Belmekki, Enhances Security for IMS Client, *International Conference on Next Generation Networks and Services (NGNS)*, Casablanca, Morocco, 2014, pp. 231-237.

[7] K. L. Larsen, E. V. Matthiesen, H.-P. Schwefel, G. Kuhn, Optimized Macro Mobility within the 3GPP IP Multimedia Subsystem, *International Conference on Wireless and Mobile Communications*, Bucharest, Romania, 2006, pp. 82-82.

[8] J. Loughney, M. Nakhjiri, C. Perkins, R. KoodliJ, *Context Transfer Protocol (CXTP)*, RFC 4067, July, 2005.

[9] E. P. Edward, A Context Transfer Model for Secure Handover in WiMAX/LTE Integrated Networks, *International Journal of Mobile Computing and Multimedia Communications*, Vol. 6, No. 3, pp. 56-74, July, 2014.

[10] E. P. Edward, 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*, Vol. 17, pp. 79-101, February, 2015.

[11] E. P. Edward, A Novel Seamless Handover Scheme for WiMAX/LTE Heterogeneous Networks, *Arabian Journal for Science and Engineering*, Vol. 41, No. 3, pp. 1129-1143, December, 2016.

[12] A. Nazari, J. But, P. Branch, H. Vu, PRIME: Preregistration for IMS Mobility Enhancement, *IEEE International Conference on Multimedia and Expo*, Melbourne, VIC, Australia, 2012, pp. 920-924.

[13] A. Nazari, P. Branch, J. But, H. Vu, UPTIME: An IMS-based Mobility Framework for Next Generation Mobile Networks, *Wireless Networks*, Vol. 20, No. 7, pp. 1967-1979, October, 2014.

[14] O. Khattab, O. Alani, A Survey on Media Independent Handover (MIH) and IP Multimedia Subsystem (IMS) in Heterogeneous Wireless Networks, *International Journal of Wireless Information Networks*, Vol. 20, No. 3, pp. 215-228, June, 2013.

[15] B.-K. Moon, Fast and Secure Session Mobility in IMS-based Vertical Handover Scenario, *International Journal of Multimedia and Ubiquitous Engineering*, Vol. 9, No. 9, pp. 171-188, September, 2014.

[16] D. Johnson, C. Perkins, J. Arkko, *Mobility Support in IPv6*, No. RFC 3775, June, 2004.

[17] R. Koodli, *Mobile IPv6 Fast Handovers*, RFC 5568, July, 2009.

[18] K. Seo, *Security Architecture for the Internet Protocol*, RFC 4301, December, 2005.

[19] S. Kent, *IP Authentication Header*, RFC 4302, December, 2005.

[20] S. Kent, *IP Encapsulating Security Payload (ESP)*, RFC 4303, December, 2005.

[21] D. Harkins, D. Carrel, *The Internet Key Exchange (IKE)*, RFC 2409, November, 1998.

[22] J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, T. Haukka, *Security Mechanism Agreement for the Session Initiation Protocol*, RFC 3329, January, 2003.

[23] S.-Y. Cheng, W.-E. Chen, A Fast SA Update Mechanism for Secure SIP/IMS Mobility in Integrated UMTS-WLAN Networks, *International Conference on Complex, Intelligent, and Software Intensive Systems*, Taichung, Taiwan, 2013, pp. 281-286.

[24] T. Magedanz, D. Witaszek, K. Knuettel, The IMS Playground@ FOKUS-An Open Testbed for Generation Network Multimedia Services, *Tridentcom 2005-International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities*, Trento, Italy, 2005, pp. 2-11.

[25] I. Manabo, K. Satoshi, K. Yoshinori, Y. Hidetoshi, IMS based Fast Session Handover with Available Network Resources Discovery of Access Network, *Journal of Information Processing*, Vol. 20, No. 1, pp. 308-318, January, 2012.

[26] H. Fathi, S. S. Chakraborty, R. Prasad, Optimization of SIP Session Setup Delay for VoIP in 3G Wireless Networks, *IEEE Transactions on Mobile Computing*, Vol. 5, No. 9, pp. 1121-1132, September, 2006.

[27] L. Kleinrock, *Queueing Systems Volume I*, John Wiley and Sons, 1975.

[28] N. Banerjee, W. Wu, K. Basu, S. K. Das, Analysis of SIP-based Mobility Management in 4G Wireless Networks, *Computer Communications*, Vol. 27, No. 8, pp. 697-707, May, 2004.

[29] V. Sharma, I. You, F.-Y. Leu, M. Atiquzzaman, Secure and Efficient Protocol for Fast Handover in 5G Mobile Xhaul Networks, *Journal of Network and Computer Applications*, Vol. 102, pp. 38-57, January, 2018.

Biographies

Shireen Tahira did her BSCS in 2002, MSCS in 2005 from IIUI Pakistan. She did Ph.D. in 2017 from IIUI Pakistan. She is Assistant Professor at Department of Computer Science and Engineering, Air University, Islamabad. Her areas of interest include NGN, Handover, security and IMS.

Ata Ullah did BSCS and MSCS in 2005 and 2007 from COMSATS and Ph.D. (CS) from IIUI Pakistan in 2016. He is Assistant Professor at Department of CS at NUML Islamabad since 2008. His areas of interests are WSN Security, IoT, NGN and VoIP.

Humaira Ashraf is Assistant Professor at IIUI, Pakistan. Now she is working at IIUI, Islamabad since 2016. She did Ph.D. in 2017 from IIUI. Her areas of interest include NGN, Network Security, IMS, VOLTE and VoIP.

Muhammad Sher is Professor at IIUI, Pakistan. He did Ph.D. from TU Berlin, Germany. He has 26 years' experience and supervised 90 research projects at graduate, M.Phil and Ph.D. level. His areas of research are Information Security, NGN and WSN.