# Efficient Certificate Based One-pass Authentication Protocol for IMS

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

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

## Abstract

IP Multimedia Subsystem (IMS) ensures quality voice and video transmission to users in next generation network. In IMS each user entering from another network like UMTS or Voice over LTE (VOLTE) or 5G has to authenticate itself. Due to unnecessary authentication, high signaling can result in congestion. This paper presents a Certificate based One-pass Authentication Protocol (COAP) that avoids duplicate authentication steps and achieve efficient authentication through the use of digital certificates. It restricts the repetition of full authentication until the certificate expires. We have also eliminated four messages during authentication by utilizing the existing credentials of UE shared earlier. Moreover, we have utilized backup servers during peak hours to reduce congestion, call termination and support more users. A testbed is setup to perform different experiments to validate performance of proposed and existing schemes. COAP achieves better bandwidth consumption, transmission cost, response time and signaling traffic load to reduce the congestion problem.

**Keywords:** Certificates, Authentication, IP multimedia subsystem, VOLTE, 5G

## 1 Introduction

Media applications are rapidly adding to web with a huge number of clients where IP-administrations are expected to satisfy client requests [1-2]. IMS is a system developed by Third Generation Partnership Project (3GPP) 2, 3GPP for the portable systems and UMTS. IMS supports versatile innovation over IP based foundation [3-4]. IMS design is used in offices for the administrations of clients and enhance hardware reusability through horintalization along with sessions. Two main components of IMS are; Call Session Control Function (CSCF) and Home subscriber server (HSS) [5] as shown in Figure 1. CSCF is the fundamental part of the IMS to deal with Session Initiation Protocol (SIP) flagging. It ensures registration, session administration and communicate with HSS.

Authentication is an essential procedure of IMS to permit legitimate clients to utilize IMS for multimedia services and administrations [6]. Next generation users will adopt IMS for accessing multimedia service [7] where CSCF servers transmit SIP messages to UEs [8]. For same clients, two-pass authentication procedure involves the rehashed confirmations. Moreover, multi-pass scenario is more challenging to secure against malicious clients. IMS servers could be influenced by congestion issue which is resolved by using stack adjusting procedures for SIP server [9]. Analysts infer that congestion can occur at any occasion during corruption of execution and refusal of administration tasks [10]. Schemes [11-15] result in security vulnerabilities.

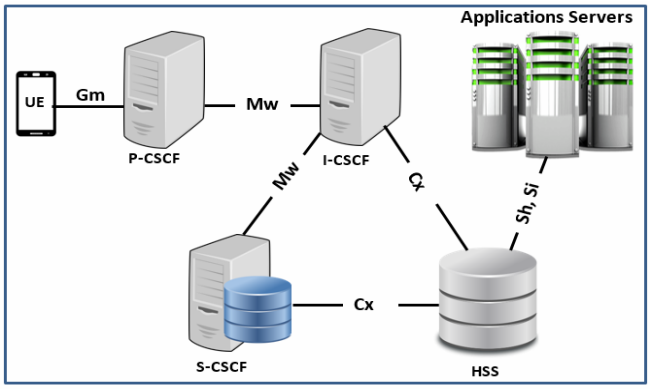



**Figure 1.** IMS architecture overview

This paper presents a Certificate based One-pass Authentication Protocol (COAP) that maintains a certificate to allow the UE for recurrent re-authentication without involving entire procedure for registration until the expiry of certificate. It reduces load over IMS servers during peak hours. We have also reduced four messages for authentication during first authentication including all steps for registration. It reduces communication cost and hence the congestion. Moreover, we have proposed to use instantaneous

*Corresponding Author: Ata Ullah; E-mail: aullah@numl.edu.pk
DOI: 10.3966/160792642019072004013

backup servers to handle more UE request that can be incorporated in the system during peak hours when congestion rises and influences to drop existing calls and block new ones. It also improves call drop ratio. We have setup a testbed to analyze bandwidth consumption, transmission time, response time and traffic load. Proposed COAP demonstrates the dominance over preliminaries.

The rest of paper is organized as follows: Section 2 explores the system model and problem statement. Related schemes are included in Section 3. The proposed COAP is explained in detail in Section 4. Results and analysis of proposed scheme are presented in Section 5 and Section 6 concludes our work.

## 2 System Model and Problem Scenario

An IMS based model is used where the authentication process initiates when UE communicates with enrollment system utilizing SIP. UE has the ability to initiate, translate and confirm SIP messages. P-CSCF is the principal server that handles verification requests from clients and process via other IMS entities. I-CSCF appoints a specific S-CSCF to the client by sharing user authentication request (UAR) and answer UAA. S-CSCF continues with further validation by sending confirmation test to client. S-CSCF exchanges message authentication request (MAR) and answer MAA with HSS and also notify 401 un-authorized message to UE to resend registration request to S-CSCF. After that, S-CSCF proceed with server authentication request (SAR) and answer SAA and then transmits OK message to UE for further communication. Figure 2 explains the registration process for IMS utilizing Authentication and Key Agreement (AKA) convention. COAP reduces messaging by eliminating exchange of MAR, MAA, un-authorized and register messages. It can be handled during exchange of SAR and SAA.

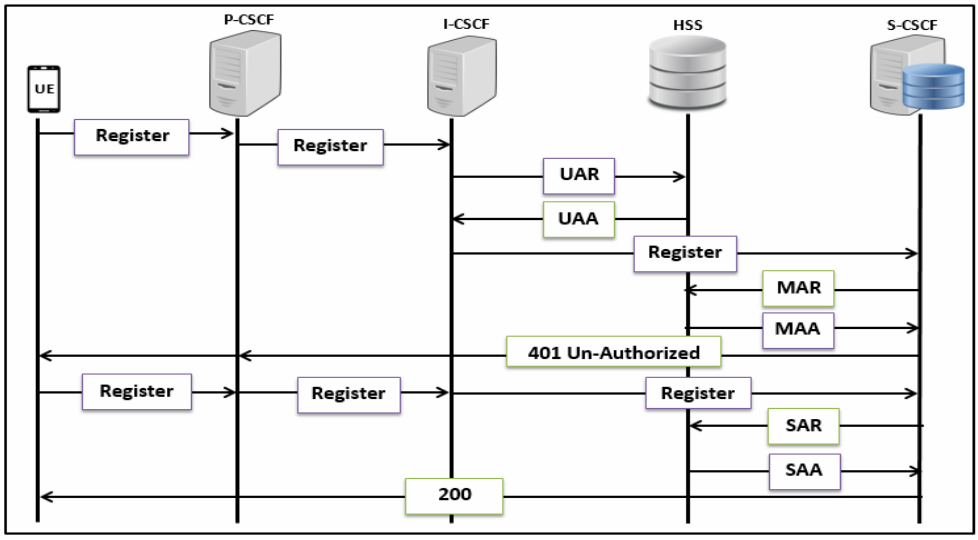



**Figure 2.** IMS Registration Process

The main problem during registration procedure is congestion when a large number of UEs that are user of UMTS, VOLTE and 5G send request for registration at IMS to avail multimedia services. UEs of different generation including 2G, 3G and 4G LTE, 5G are also supported by IMS that increases service set of users. During registration at IMS, each request initiated from UE exchanges 20 messages on different servers to successfully authorize a single UE. At peak time, IMS deals with congestion to serve a large set of users from different networks. It becomes more challenging when a number of re-registration requests are also served with complete process due to connection drop.

## 3 Related Work

This section explores review IMS authentication based schemes for registration and availing multimedia services.

### 3.1 One Pass Authentication Protocols

UMTS client needs to perform validation using IP Multimedia Private Entity ($IM_{SI}$) at first step and then verification with IP Multimedia Public Entity ($IM_{PI}$). After verification, consider a client Bob that pretends to be honest like Alice to utilize services of IMS on behalf of Alice's expense. Existing schemes attempted to keep away from this assault with the exception of IMS-AKA. LP [13] faces impermanent cheat attack that happens when SAR message is received by HSS whereas S-CSCF has not yet checked $IM_{PI}$. In enhanced one-pass IMS authentication (E-OIA), an intruder can attack before IMS validates actual sender [14]. Efficient authentication and key-agreement for IMS (EAKI) also presents a one-pass authentication mechanism. Other One-pass validation schemes are

presented in [11, 16] and [12] where S-CSCF performs the client's confirmation before the transmission of SAR message towards HSS.

Replay assaults are utilized for alteration. Conspire LP [13] is weak against replay assault [12]. Schemes [11], [14-16] have used time stamp and arrangement number as seed for random number. Schemes [12, 14] and [15] have proposed one-pass AKA. During one-pass validation [13], S-CSCF affirms $IM_{SI}$ and $IM_{PI}$ but UE does not verifies SCSCF. It causes an affirmation from fake CSCF as in [11, 15] and [16]. It demands period synchronization without security, which is hazardous to revive messages.

### 3.2 Low Congestion Authentication Protocol

MTCDs can exchange information of rejected requests that are not received. It affects clients' satisfaction. In case of huge requests and association preparation, it can perform verification before any correspondence. In [17], authentic workload information for base stations is considered to control the topographical clog in the ISP network. Time-based estimating plan is utilized to address blockage issue. One-time identity mechanism (O-TIM) obscures real identity of users by using commutative functions. It enables data exchange between users without pre-keying for authentication [18].

In [19], SIP based adaptive congestion aware procedure manages handover in heterogeneous networks. It significantly improves the QoS of VoIP users where signal strength was used as the trigger for handover decision. In [20], authentication and key establishment schemes are analyzed to verify the promising features of IMS. It involves pre-distribution of *Av* among the server-client system. Moreover, context-ID and elliptic curve–Diffie Hellman strategies are combined to guard against several attacks.

Internet of Things (IoT) is getting growing interest because it can encourage huge client accommodation. IoT precariously increments the utilization that may prompt to clog and server over-burden. To address this issue, an administration strategy for IoT activity in a virtualized IMS condition is presented that utilizes dynamic steering, SIP, and the proposed technique for administration through virtualized IMS [10]. QoS systems discuss about how different congestion based ideas could be connected [21]. Infonetics research has demonstrated that quantity of the versatile broadband memberships increased from 548.9 million in 2010 to 1.5 billion by late 2014 [22]. During busy hours, congestion happens administrative servers and more requests are processed. Numerous arrangements have been analyzed beforehand like expanding the entryways, ideal area of portals, and so forth. It considers a crossover work into a system that deals with the transient load on a work arrangement [23]. Due to open accessibility, IMS is vulnerable to SIP flooding attacks. Difference between the estimated distributions of SIP messages during training and testing phases can be measured using Kullback-Leibler divergence. If difference is larger, then it identifies SIP flooding attack [24].

## 4 Certificate- One Pass Authentication Protocol (COAP)

During a multimedia based communication on a slightly noisy channel or during busy hours, connections are dropped and re-authentication is mandatory for the UE. It causes congestion by serving recurrent authentication requests. UEs are unable to establish new calls and existing call sessions can also be terminated to reduce traffic load. Our scheme handles it in a better manner by maintaining certificates during first time authentication and then allow for recurrent Q authentications without performing all steps. It saves a large amount of messages to reduce chances of congestion. To further reduce congestion, we eliminate four messages that are handled in SAR and SAA by forwarding the UE's request received via P-CSCF and no need to challenge the 401 message. It increases the support for a large number of more UEs without congestion as compared to IMS AKA. The S-CSCF can verify the legitimate user for secure accessibility. In this scenario, the users with valid certificate can hold the re-authentication procedure for a certain amount before expiry. After the expiry, a new S_CSCF can allocate new certificate to the UE to access media services.

Authentication process begins when UE sends a request along with credentials to P-CSCF. In response, P-CSCF, I-CSCF, HSS and S-CSCF collaborates to complete certification process. P-CSCF can collaborate with P-CSCF2 that process the request via I-CSCF2 and S-CSCF2 and responds to HSS as shown in Figure 3. The protocol steps are visually illustrated in Figure 4. A list of notations used in COAP is provided in Table 1.

*Steps (1) – (7):* UE initiates a request containing $IM_{PI}$, $IM_{SI}$ values and random number *n* for registering to $PCSCF_1$. Using anomaly detection module, $PCSCF_1$ checks load to identify the attack scenario as per threshold. If condition is false then $PCSCF_1$ forwards request to $PCSCF_2$ otherwise forwards to $ICSCF_1$ as explored in step 3. $ICSCF_1$ checks whether $C_{header}$ is empty means no certificate or value of life time $L_T$ of certificate is equal to zero then it stores values of $IM_{PI}$ and $IM_{SI}$. It also updates random sequence number (*RSN*) to a maximum sequence number ($SN_{max}$). If condition is false then $ICSCF_1$ processes registration request. After that, $I\text{-}CSCF_1$ transmits UAR to HSS for acquiring details of $SCSCF_1$ that is available to serve requesting UE.

1.UE → PCSCF$_1$:Register{IM$_{PI}$ ||IM$_{SI}$||n}
2.PCSCF$_1$: IF threshold < attack value
3. PCSCF$_1$→ICSCF$_1$:Register{IM$_{PI}$||IM$_{SI}$||n}
4.ICSCF1: IF C$_{header}$="Empty" OR L$_T$ = 0 then
5. ICSCF$_1$ stores {IM$_{PI}$|| IM$_{SI}$, RSN≡ SN$_{max}$}
6. ELSE ICSCF$_1$: {Register} ENDIF
7.ICSCF$_1$→ HSS: Register {IM$_{PI}$} //UAR
8.HSS: Retrieves IM$_{SI\sim HSS}$ {(IM$_{PI}$)} using IM$_{PI}$
9.HSS → ICSCF$_1$: {IM$_{SI\sim HSS}$, SCSCF$_1$} //UAA
10.ICSCF$_1$: IF IM$_{SI}$ ≡ IM$_{SI\sim HSS}$ then
11. ICSCF$_1$ → SCSCF$_1$:{(Register)}
12.ENDIF
13.SCSCF$_1$ → HSS: {IM$_{PI}$} //SAR
14.HSS prepares A$_V$= {C$_K$, I$_K$, X$_{RES}$}
15.HSS stores SF$_{NAME}$
16.HSS → SCSCF$_1$: {A$_V$} //SAA
17.SCSCF$_1$: Certificate{IM$_{PI}$, SF$_{NAME}$, n, L$_T$}
18.SCSCF$_1$ → PCSCF$_1$: {A$_V$, Certificate}
19.PCSCF$_1$: saves{C$_K$, I$_K$}, PCSCF$_1$ → UE: {X$_{RES}$, Cert}
20.UE: IF RES≡ X$_{RES}$ then continue
21.SCSCF$_1$→ UE: {(Notify)}
22.UE→ PCSCF$_1$:{(Register)}
23.PCSCF$_1$→ ICSCF$_1$: Register: {IM$_{PI}$ || IM$_{SI}$ || n}
24.ICSCF$_1$: IF C$_{header}$ equals "Certificate"
25. ICSCF$_1$ → SCSCF$_1$: {Register}
26.SCSCF$_1$:IF UE$_{Cert}$ ≡ S$_{Cert}$ AND L$_T$ ≥ 1 then
27. SCSCF$_1$ → UE: 200 OK, L$_T$ = L$_T$-1
28. ELSE
29. SCSCF$_1$ → UE: invalid request
30. ENDIF
31. ENDIF
32.ELSE // IF threshold < attack value at step 2
33.PCSCF$_1$→PCSCF$_2$:Register:{IM$_{PI}$||IM$_{SI}$||n}
34.PCSCF$_2$→ICSCF$_2$:Register:{IM$_{PI}$||IM$_{SI}$||n}
Steps 35 onwards are like steps 4 – 31 on ICSCF$_2$ and PCSCF$_2$ in place of ICSCF$_1$ and PCSCF$_1$ respectively.

**Figure 3.** COAP steps for Registration

**Table 1.** List of Natation's for COAP

| Symbols | Description |
|---|---|
| $IM_{PI}$ | IP Multimedia Private Identity |
| $IM_{PU}$ | IP Multimedia Public Identity |
| $n$ | Random value |
| $VN$ | Visited network identifer |
| $SF_{Name}$ | SCSCF Name |
| $C_K$ | Cipher key |
| $I_K$ | Integrity key |
| $L_T$ | Certificate life time |
| $S_p$ | Improvement of COAP over AKA |
| $H_p$ | Expected cost for COAP |
| $\sigma_{IMSAV}$ | Transmission Cost for IMS with AVs |
| $\sigma_{IMS}$ | Transmission Cost for IMS without AVs |
| $\phi$ | Total authentication requests per S-CSCF |
| $\Gamma$ | Call rate per user for UMTS in IMS |
| T | Total no of MS |

*Steps (8) – (14):* HSS receives UAR and retrieves $IM_{SI\sim HSS}$ using $IM_{PI}$ and replies with UAA to $ICSCF_1$. After receiving UAA, $ICSCF_1$ compares $IM_{SI\sim HSS}$ newly received from HSS and $IM_{SI}$ value already received from UE. After comparison, $ICSCF_1$ transmits message to $S\text{-}CSCF_1$ for registration of UE. $SCSCF_1$ prepares SAR containing $IM_{PI}$ and transmits to HSS. Upon receiving SAR, HSS prepares an authentication vector ($A_V$) by using three parameters including expected response ($X_{RES}$), cipher key ($C_K$) and integrity key ($I_K$).

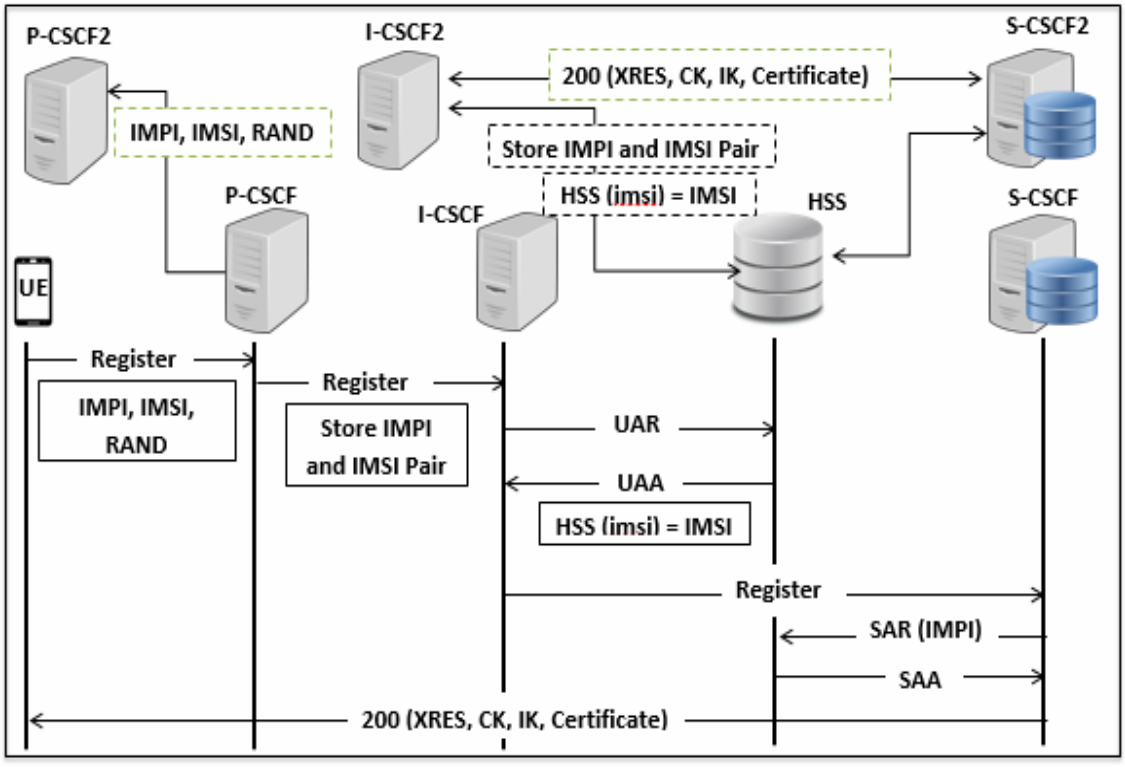



**Figure 4.** Authentication steps in COAP scheme

*Steps (15) – (21):* HSS saves SCSCF name $SF_{NAME}$. HSS further transmits SAA having $A_V$ to $SCSCF_1$ that creates a certificate using $IM_{PI}$, SCSCF name $SF_{NAME}$, random number $n$ and life time $L_T$ as given in step 17. $SCSCF_1$ forwards $A_V$ and certificate to $PCSCF_1$ that saves $C_K$ and $I_K$ whereas $X_{RES}$ and Certificate are transmitted to UE as illustrated in step 19. UE compares RES with $X_{RES}$ to verify authenticity of $SCSCF_1$ to continue with registration. $SCSCF_1$ can issues a Notify message to UE whenever needed to re-authenticate.

*Steps (22) – (28):* UE replies to $PCSCF_1$ by sending a request to register. $PCSCF_1$ prepares the message for forwarding register message to $ICSCF_1$ along with $IM_{PI}$, $IM_{SI}$ and $n$. $ICSCF_1$ compares that whether $C_{header}$ is equal to Certificate as illustrated in step 24. If the condition is true then $ICSCF_1$ forwards the register request to $SCSCF_1$ that further verifies that $UE_{Cert}$ is equal to certificate at $SCSCF_1$ represented as $S_{Cert}$ and secondly the value of $L_T$ is greater than 1. If the condition is true then $SCSCF_1$ transmits OK message towards UE. It decrement value of $L_T$ by 1 and update the previous value. Re-authentication by $SCSCF_1$, certificate from UE and OK message from $SCSCF_1$ as illustrated in Figure 5.

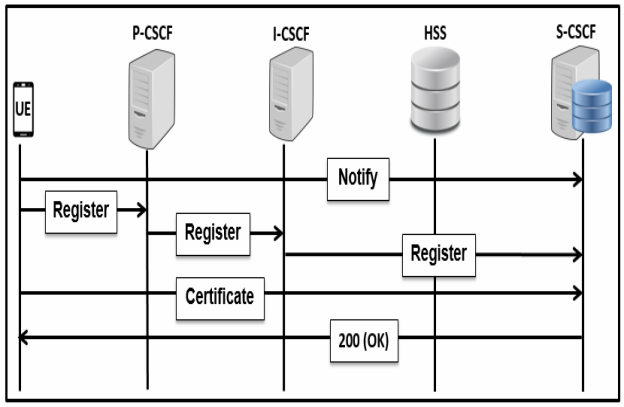



**Figure 5.** COAP for re-authentication

*Steps (29) – (34):* In case certificate at UE and $SCSCF_1$ represented as $UE_{Cert}$ and $S_{Cert}$ respectively are not equal then $SCSCF_1$ replies with an "invalid request" message to UE as illustrated in step 29. The else block executes when condition "*IF threshold < attack value"* at Step 2 is false and it temporarily acquires services of backup IMS entities. In this case, $PCSCF_1$ transmits register message $\{IM_{PI}||IM_{SI}||n\}$ to $PCSCF_2$ that further forwards it to $PCSCF_2$ as in step 34.

*More Steps:* Step 35 and onwards are similar to steps 4 to 31 that are executed for registration process initiated by UE. The main difference is that these steps are executed at $PCSCF_2$ and $ICSCF_2$ instead of $PCSCF_1$ and $ICSCF_1$. UE and HSS are same.

During the congestion in peak hour scenario, the SIP register message is forwarded to the P-CSCF server on the IMS network. Most of the mobile networks have no security equipment on the mobile network, conducting no abnormal SIP message check.

If an attacker exploits weakness of CSCF server and sends a forged SIP message, there is a high chance of security threat as the CSCF server will handle the traffic with the forged SIP message. SIP is a text-based message of which we can observe that only two register request are send from the user results into 20 messages within the network. Therefore if any emergency lunches bottle neck at CSCF it will highly effect IMS environment. Figure 6 elucidates that as load on $P\text{-}CSCF_1$ increases and the threshold value is violated which is implemented according to cumulative sum algorithm the load is shifted towards the backup servers i.e. $CSCF_2$ therefore, the congestion is avoided and many legitimate users are provided the services without delays and server crashes. Figure 7 illustrates visual flow of proposed COAP steps.

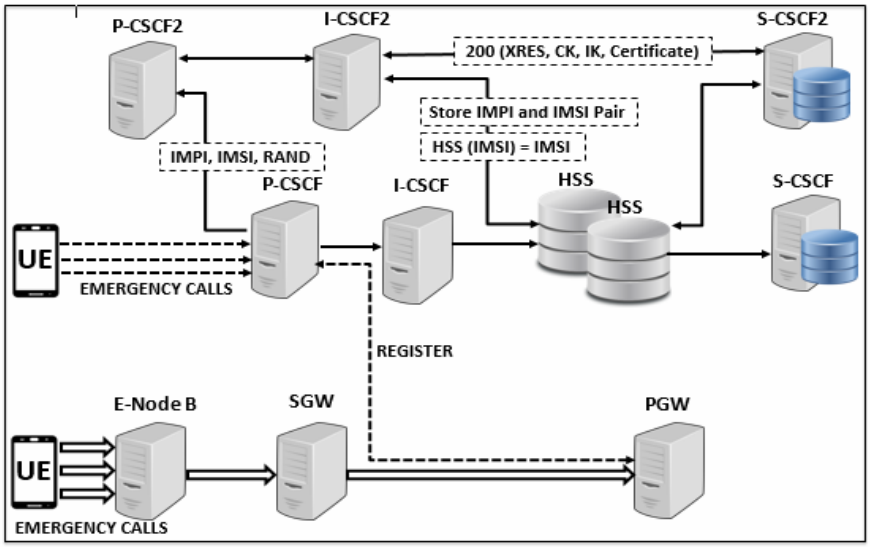



**Figure 6.** Congestion control in emergency scenarios

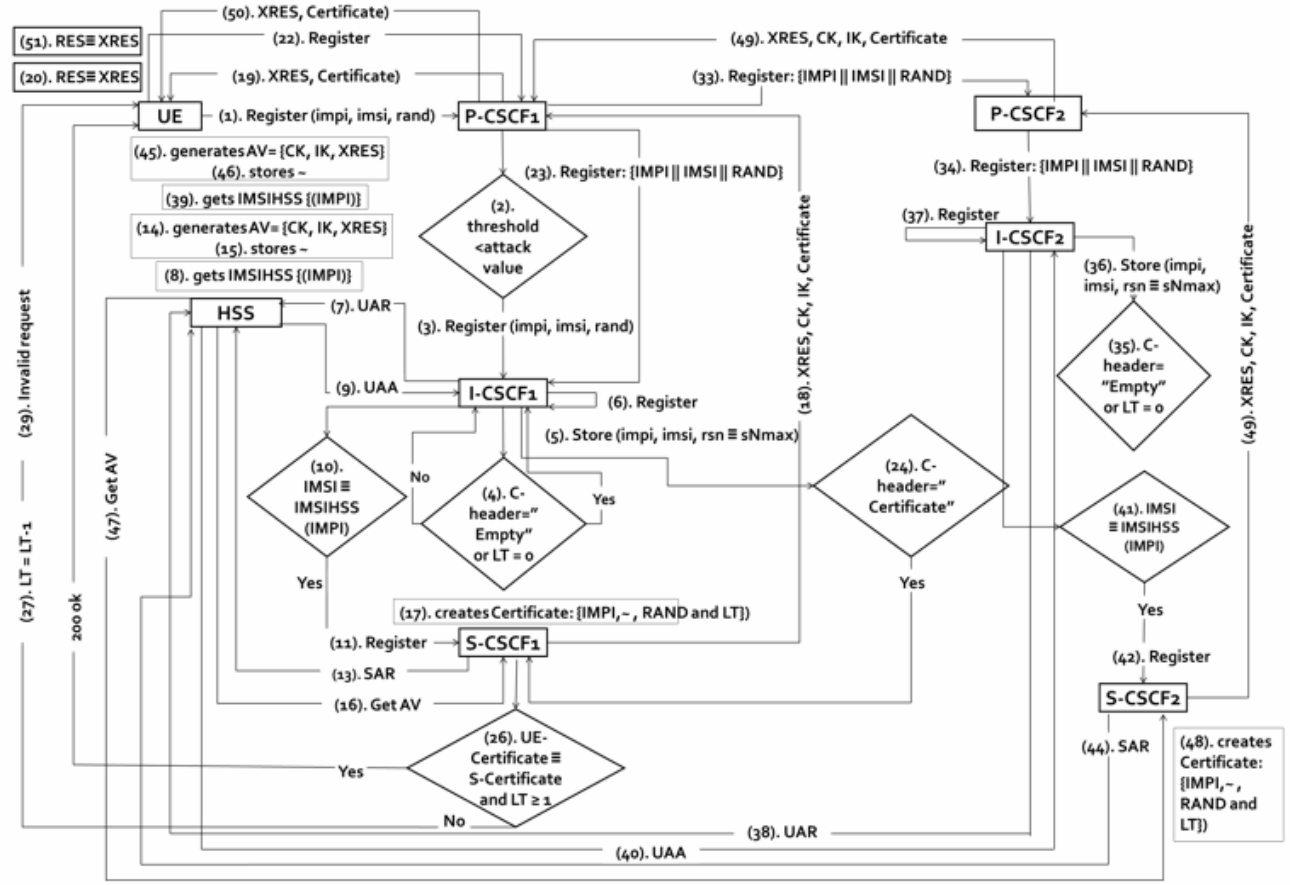



**Figure 7.** Registration flow using COAP

## 5 Results and Analysis

Testbed is developed for IMS entities including P-CSCF, S-CSCF and I-CSCF by installing client side and server side software using FOKUS. It contains SIP servers, HSS and cell phone as UE as illustrated in Figure 8. We have performed multiple registrations by exchanging all messages. Moreover, proposed scenarios are also implemented to evaluate the bandwidth consumption, signaling and load transaction cost, transmission cost and the congestion analysis for COAP. During these implementations, SIP headers are also modified to support certificate based scenario where certificate is allocated to the context header and other related security parameters are also updated. We have also analyzed the congestion scenario on SIP severs during peak hours. Moreover, a high bandwidth utilization is also analyzed at IMS servers by considering UMTS, LTE and IMS authentication scenarios. Table 2 explores the parameters and range of values used in testbed.

### 5.1 Bandwidth Consumption

In this section we have analyzed that how much bandwidth is consumed by exchanging messages during authentication in IMS-AKA, EAKI [15], O-TIM [18], E-OIA [14] and COAP scenario. During IMS AKA, the messages exchanged between UE and servers are observed in a testbed scenario and the sum of bits transmitted during all messages are calculated for IMS AKA, XA, HU and COAP scenario. During IMS AKA, UE transmits $IM_{PI}$ of 128 bits to P-CSCF that further forwards the $IM_{PI}$. S-CSCF transmits parameters $IM_{PI}$, $n(i)$, $AU_{TH}(i)$, $C_K(i)$ and $I_K(i)$ of size 640 bits to I-CSCF. P-CSCF replies with parameters $IM_{PI}$, $n(i)$ and $AU_{TH}(i)$ of size 384 bits to UE that transmits parameters $IM_{PI}$, $RES(i)$ of size 160 bits to S-CSCF.

The messages exchanged between HSS and IMS servers are observed where I-CSCF transmits 416 bits containing $IM_{PI}$ and $IM_{PU}$ along with 32 bits for authentication type. HSS replies with a 128 bits message containing SCSCF name, registration status and S-CSCF capabilities. S-CSCF also transmits 128 bits message to HSS that replies with $A_V$ of size 640 bits. S-CSCF transmits SAR of 416 bits to HSS that replies with SAA of 32 bits. Sum of messages is 5600 bits for IMS AKA as shown in Figure 9. During COAP, messages exchanged between UE and IMS servers are observed where UE transmits $IM_{PI}$, $IM_{SI}$ and $n$ of 384 bits to P-CSCF. I-CSCF transmits 128 bits to S-CSCF that transmits certificate of 504 bits to P-CSCF that further transmits 448 bits to UE. I-CSCF transmits parameters $IM_{PI}$, $IM_{SI}$ and $VN$ of 128 bits each and authentication type of 32 bits to HSS. ICSCF receives 128 bits SAR from HSS.

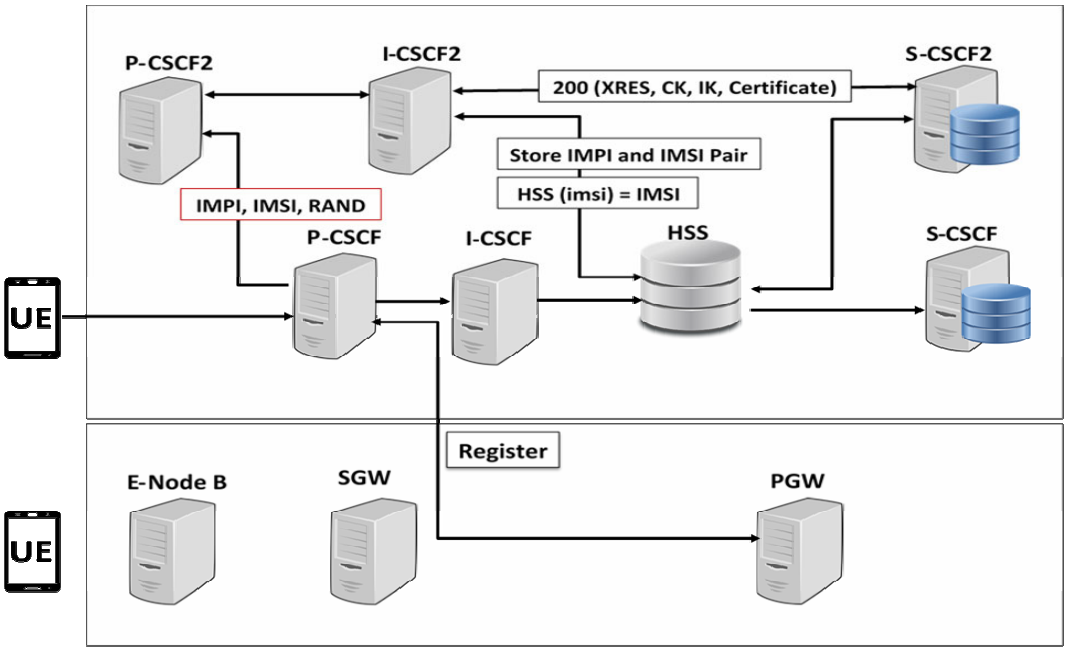



**Figure 8.** Testbed environment for COAP

**Table 2.** Testbed Parameters

| Testbed 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 |
| Number of Authentications | 1 – 12 |
| Transmission Cost | 0 – 200 |
| Response Time | 0 – 13 milliseconds |
| Total authentication P-CSCF | 0 – 10 requests |
| Total authentication S-CSCF | 0 – 1000 requests |

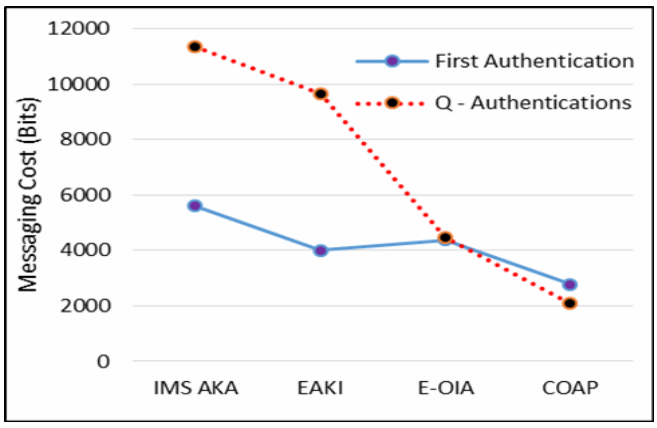



**Figure 9.** Message size for first and Q-authentication

S-CSCF transmits SAR of 416 bits to HSS that replies with an $A_V$ of 448 bits. EAKI [15] and E-OIA [14] require 4000 bits and 4374 bits respectively for first time authentication. COAP dominates by achieving, 2772 bits because of merging MAR and MAA in SAR and SAA. Secondly, results for Q=5 consecutive authentications are observed as 11360 bits, 9635 bits, 4470 bits and 2080 bits for IMS AKA, EAKI, E-OIA and COAP respectively.

Figure 10 elucidates that during re-authentications, the number of messages processed by S-CSCF are 03 for COAP and 05 for IMS AKA. P-CSCF processes 04 messages for IMS AKA including Register message, 401 message from $SCSCF_1$ to UE, Register and OK messages. For COAP, 02 messages including Notify and OK are processed. HSS processes 06 messages for IMS AKA and 04 messages for COAP.

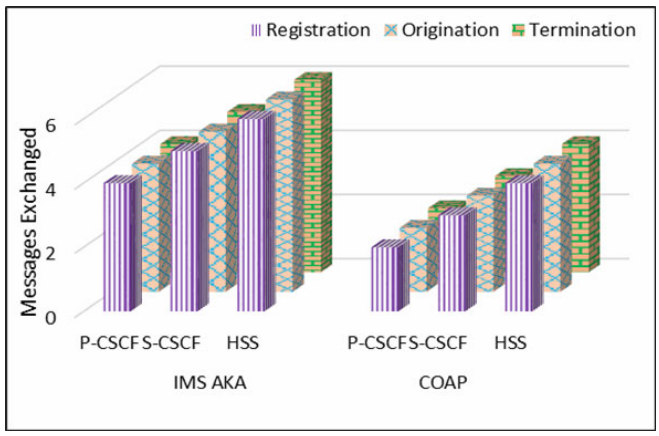
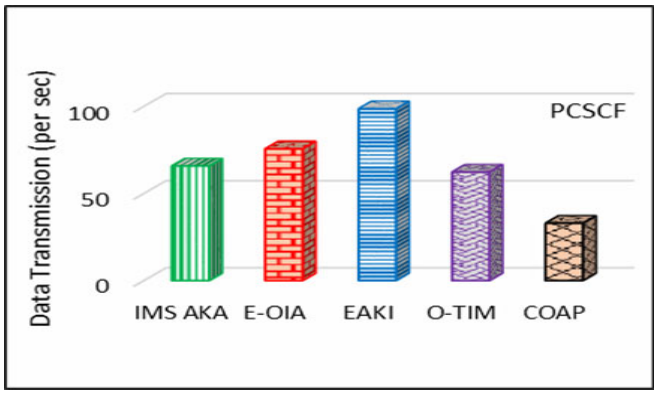


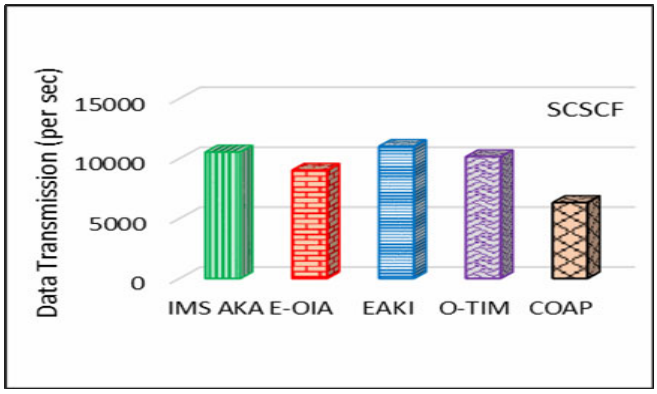

**Figure 10.** Messages exchanged for first authentication

Figure 11(a) elucidates total data transmission messaging cost at P-CSCF during peak hours. COAP dominates with 32.94 whereas IMS AKA, E-OIA [14], EAKI [15] and O-TIM [18] generates 65.78, 75.68, 98.66 and 62.35 cost respectively. Figure 11(b) elucidates the signaling and load transaction messages generated at S-CSCF that are 6325 messages for COAP. IMS authentication generates 10542 messages for signaling and load transaction messages whereas E-OIA [14] generates 9030 messages, EAKI [15]

generates 11020 and scheme [12] generates 10157 messages.




(a) P-and




(b) S-CSCF

**Figure 11.** Transaction cost for (a) P-and (b) S-CSCF

## 5.2 Response Time

Figure 12 elucidates the response time where it is observed that during first authentication the response time for EAKI [15] is 12.4 milliseconds, O-TIM [18] requires 10.4, IMS requires 9.8, E-OIA [14] consumes 8.2 whereas COAP consumes 10.3 milliseconds. During first authentication of each scheme including COAP, the response time is high due to download of the $A_V$'s required for future authentications.

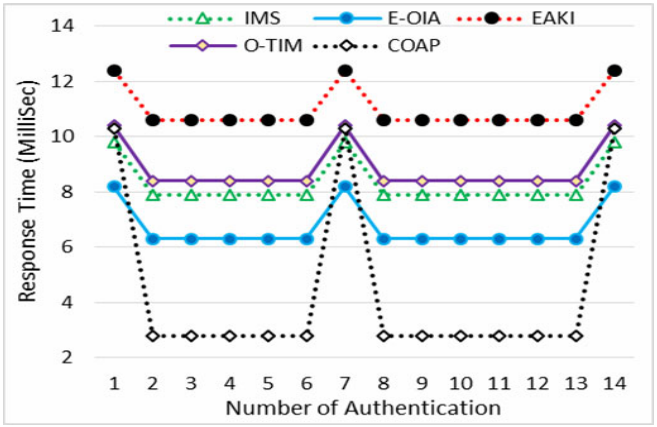



**Figure 12.** Response time for authentication

For first authentication, COAP generates certificate and its response time is slightly greater than preliminaries. For re-authentications, COAP outperforms preliminaries by consuming a lowest response time. During the 7th authentication, response time is higher for COAP and preliminaries as well due to re-authentication with complete steps and downloading the new AV's. After limit of 05, re-authentication is performed with full steps.

## 5.3 Transmission Cost

In this scenario, the cost from UE to S-CSCF and then back via CSCFs is one unit. Secondly, cost of messages between CSCFs and HSS or other CSCFs is alpha as one unit. We have also considered assumptions in E-OIA [14]. The delivery cost of IMS AKA without $A_V$ in the S-CSCF for the UE is $\sigma_{IMS} = 4 + 6\alpha$ where $\alpha$ represents units and its values is less than 1. Figure 13 illustrates that 4 messages are originated from UE and 6 messages are exchanged between CSCFs and HSS. For $A_V$ in S-CSCF to UE, transmission cost is $\sigma_{IMS_{Av}} = 4 + 4\alpha$. Total expected IMS registration transmission cost $\sigma_{IMS_{Toal}}$ is given in equation (1).

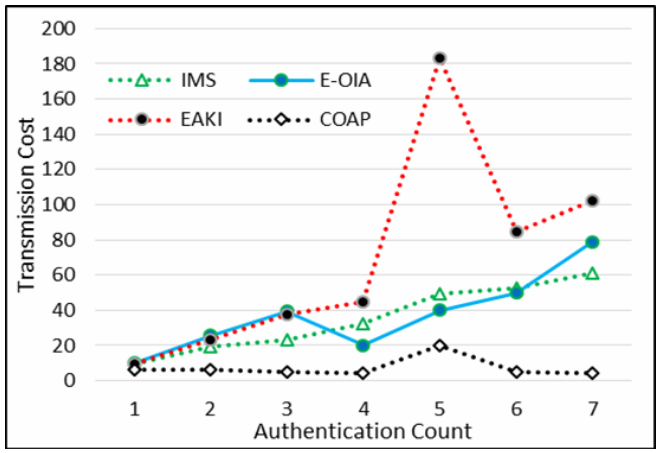



**Figure 13.** Transmission cost for authentication

$$\sigma_{IMS_{Toal}} = \left(\frac{1}{m} \times \sigma_{IMS}\right) + \frac{m-1}{m} \times \sigma_{IMS_{Av}} = \frac{1}{4} + 2m + 1/m \times 2\sigma \quad (1)$$

The registration cost in COAP is reduced and also involves an additional cost to generate a new certificate is $\sigma_{COAP} = 2 + 4\alpha$ without $A_V$. Certificate is used for 3 iterations and cost for COAP is $\sigma_{COAP_{Av}} = (4\alpha - 1)/m + 3$. Improvement over E-OIA is $Sp_{E-olA} = (m(2m-1) + 1 - 2\alpha) / 2m(1+m) + 2\alpha)$ and improvement over IMS AKA is in (2).

$$Sp_{IMS\ AKA} = \sigma_{IMS_{Total}} - \frac{\sigma_{COAP_{Av}}}{\sigma_{IMS_{Total}}} = [m + 2\alpha(2m-1)+1]/(4m+4\alpha m+2\alpha) \quad (2)$$

## 5.4 Traffic Load

We have used fluid mobility model to analyze cost for first and subsequent re-authentications using parameters of [25]; (i) UE's mobility with a velocity $v$ (ii) direction is distributed over [0, 2π] iii) density ρ within registration area and iv) length L of area as $A = \rho \times v \times (\frac{L}{\pi})$. In LTE\UMTS, requests are generated for UEs within registration area with a rate $R_{\frac{UMTS}{LTE}} = \frac{\rho \times v \times L}{\pi} = (384 \times 5.95 \times 32.45)/\pi) =$ 5.60/sec. If half of UMTS users in an area request for IMS services, then rate $R_{IMS} = 5.60/2 = 2.8/\text{sec}$ and de-registration area equals $DeR_{IMS} = 2.8/\text{sec}$.

Authentication request messages per second arriving at S-CSCF as $Reg_{IMS\_HSS} = R_{IMS} \times RegArea_{TOTAL} = 2.8 \times 128 = 358.4$. During call origination, $\phi = (\gamma \times \tau) = 3 \times 1.05 = 3.15 \times 10^6$ per hour and 875 per second. Number of calls originated at P-CSCF per registration area is observed as $RegArea_{TOTAL}/\phi = 875/128 = 6.835$ as explored in Figure 14.

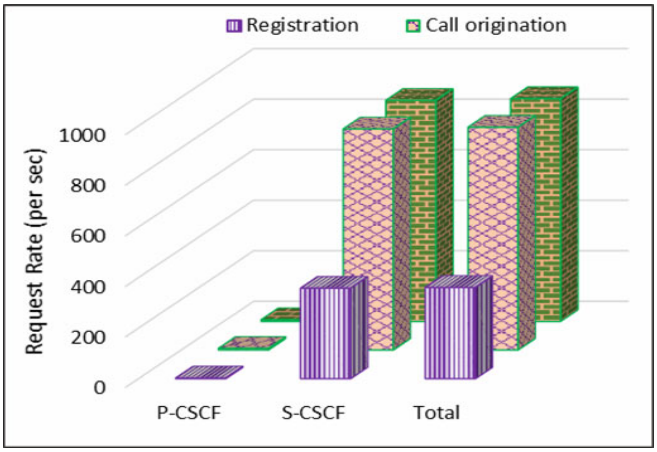
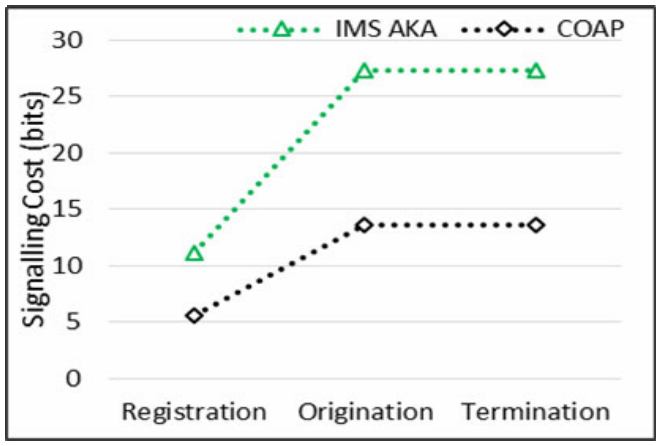


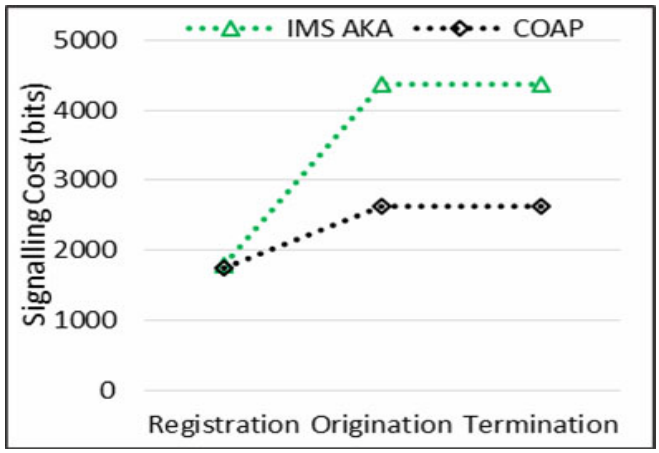

**Figure 14.** Total auth requests - P-CSCF and S-CSCF

Figure 15(a) elucidates traffic load in bits per second during first authentication at P-CSCF$_1$. The values for call origination and termination are same as per assumptions of fluid mobility model that new calls are originated when existing calls are terminated. The signaling cost for call origination at PCSCF$_1$ is 27.34 and 13.67 bits/s for IMS AKA and COAP respectively where COAP consumes less cost due to reduction in number of messages.

Figure 15(b) elaborates the bits per second for first time authentication request at SCSCF$_1$. It can be observed that number of bits exchanged through SCSCF$_1$ are much large as compared to PCSCF$_1$ because SCSCF$_1$ is involved in more activities and hence more messaging for exchanging data with UE and HSS. Initially the signaling cost at SCSCF$_1$ is 1792 bits/s for IMS AKA and 1752 bit/s for COAP during registration phase but it is much improved in origination and termination that is 2625 bits/s for COAP as compared to 4375 bits/s for IMS AKA at S-CSCF. It proves that our reduction in MAR and MAA messages results in less traffic load at servers.




(a) PCSCF




(b) S-CSCF

**Figure 15.** Traffic load during first authentication for (a) PCSCF and (b) S-CSCF

## 6 Conclusion

IMS authentication is necessary to avail multimedia calls initiated from UMTS, VoLTE or 5G. We have reduced the number of messages during first authentication. For re-authentications due to lossy channel or during peak hours, we have reduced these costs by introducing a certificate that allows to re-authenticate without complete steps until the expiry of certificate. Proposed COAP reduces bandwidth consumption, communication cost, response time and traffic load. Results for bandwidth consumption shows

a 65% messaging cost improvement than the original IMS authentication. COAP can obtain more than 50% bandwidth improvement and 50% improvement than IMS authentication and preliminaries. Traffic load shows a 66% improvement at P-CSCF and 10% improvement at S-CSCF over IMS AKA. It proves the dominance of COAP over preliminaries and reduces redundancy without lowering security strengths. In future, we shall analyze the impact of COAP to measure congestion resolution costs.

**Conflicts of Interest:** Authors declare no conflict of interest.

## References


[1] A. Passarella, A Survey on Content-centric Technologies for the Current Internet: CDN and P2P Solutions, *Computer Communications*, Vol. 35, No. 1, pp. 1-32, January, 2012.

[2] M. Conti, S. Chong, S. Fdida, W. Jia, H. Karl, Y.-D. Lin, P. Mähönen, M. Maier, R. Molva, S. Uhlig, M. Zukerman, Research Challenges towards the Future Internet, *Computer Communications*, Vol. 34, No. 18, pp. 2115-2134, December, 2011.

[3] D.-N. Le, DDOS Attack Defense in IP Multimedia Subsystem of NGNs Using Rulers in SNORT, *Global Journal of Computer Science and Information Technology*, Vol. 1, No. 1, pp. 88-99, September, 2014.

[4] G. Camarillo, T. Kauppinen, M. Kuparinen, I. M. Ivars, Towards an Innovation Oriented IP Multimedia Subsystem [IP Multimedia Systems (IMS) Infrastructure and Services], *IEEE Communications Magazine*, Vol. 45, No. 3, pp. 130-136, March, 2007.

[5] H. Yeganeh, A. H. Darvishan, M. Shakiba, NGN Functional Architecture for Resource Allocation and Admission Control, *International Conference on Telecommunication in Modern Satellite, Cable, and Broadcasting Services*, Nis, Serbia, 2009, pp. 533-539.

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

[7] A. S.-Esguevillas, B. Carro, G. Camarillo, Y.-B. Lin, M. A. García-Martín, L. Hanzo, IMS: The New Generation of Internet-Protocol-Based Multimedia Services, *Proceedings of the IEEE*, Vol. 101, No. 8, pp. 1860-1881, August, 2013.

[8] M. T. Beck, S. Feld, A. Fichtner, C. Linnhoff-Popien, T. Schimper, ME-VoLTE: Network Functions for Energy-Efficient Video Transcoding at the Mobile Edge, *International Conference on Intelligence in Next Generation Networks*, Paris, France, 2015, pp. 38-44.

[9] R. Libnik, A. Svigelj, Adaptive Probe Based Congestion Aware Handover Procedure Using SIP Protocol, *International Journal of Computers Communications & Control*, Vol. 10, No. 5, pp. 686-701, October, 2015.

[10] J. M. Been, W. S. Yang, J. H. Kim, J.-O. Lee, Management of IoT Traffic Using a Virtualized IMS Platform, *Asia Pacific Network Operations and Management Symposium*, Busan, South Korea, 2015, pp. 456-459.

[11] J. Fu, C. Wu, J. Chen, R. Fan, L. Ping, Lightweight Efficient and Feasible IP Multimedia Subsystem Authentication, *International Conference on Networking and Information Technology*, Manila, Philippines, 2010, pp. 139-144.

[12] C.-M. Huang, J.-W Li, Reducing Signaling Traffic for the Authentication and Key Agreement Procedure in an IP Multimedia Subsystem, *Wireless Personal Communications*, Vol. 51, No. 1, pp. 95-107, October, 2009.

[13] Y.-B. Lin, M.-F. Chang, M.-T. Hsu, L.-Y. Wu, One-pass GPRS and IMS Authentication Procedure for UMTS, *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 6, pp. 1233-1239, June, 2005.

[14] X. Long, J. Joshi, Enhanced One-pass IP Multimedia Subsystem Authentication Protocol for UMTS, *International Conference on Communications*, Cape Town, South Africa, 2010, pp. 1-6.

[15] H.-M. Sun, B.-Z He, S. Chang, C.-H Cho, Efficient Authentication and Key Agreement Procedure in IMS for UMTS, *International Journal of Innovative Computing, Information and Control*, Vol. 8, No. 2, pp. 1385-1396, February, 2012.

[16] L. Gu, M. A. Gregory, Improved One-pass IMS Authentication for UMTS, *The International Conference on Information Networking*, Barcelona, Spain, 2011, pp. 31-36.

[17] O. Ojesanmi, T. Oyebisi, E. Oyebode, O. Makinde, Performance Analysis of Congestion Control Scheme for Mobile Communication Network, *International Journal of Computer Science and Telecommunications*, Vol. 2, No. 8, pp. 33-36, November, 2011.

[18] N. Vrakas, D. Geneiatakis, C. Lambrinoudakis, Obscuring Users' Identity in VoIP/IMS Environments, *Journal of Computer & Security*, Vol. 43, pp. 145-158, June, 2014.

[19] R. Libnik, A. Svigelj, Adaptive Probe-based Congestion-aware Handover Procedure Using SIP Protocol, *International Journal of Computers Communications & Control*, Vol. 10, No. 5, pp. 686-701, July, 2015.

[20] B. D. Deebak, R. Muthaiah, K. Thenmozhi, P. I. Swaminathan, Analyzing Secure Key Authentication and Key Agreement Protocol for Promising Features of IP Multimedia Subsystem Using IP Multimedia Server-Client Systems, *Multimedia Tools and Applications*, Vol. 75, No. 4, pp. 2111-2143, February, 2016.

[21] D. Kutscher, F. Mir, R. Winter, S. Krishnan, Y. Zhang, C. Bernardos, *Mobile Communication Congestion Exposure Scenario*, RFC 7778, July, 2016.

[22] M. Ghorbanzadeh, A. Abdelhadi, C. Clancy, *Cellular Communications Systems in Congested Environments*, Springer, 2016.

[23] P. Nanda, J. Kumar, QOS Improvement in Mesh Network Using Traffic Offloading Through 2G/3G Networks, *International Journal of Engineering Studies*, Vol. 8, No. 2, pp. 117-128, December, 2016.

[24] N. H. Doust, M. N. Jahromi, Detecting Flooding Attacks on IMS Networks Using Kullback-Leibler Divergence and Triple EWMA, *Signal Processing and Renewable Energy*, Vol. 1, No. 4, pp. 31-43, December, 2017.

[25] J. AL-Saraireh, S. Yousef, Extension of Authentication and Key Agreement Protocol (AKA) for Universal Mobile Telecommunication System (UMTS), *International Journal of Theoretical and Applied Computer Sciences*, Vol. 1, No. 1, pp. 109-118, 2006.

## Biographies

**Humaira Ashraf** is Asst. Prof. 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.

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

**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 Prof. at Department of Computer Science and Engineering, Air University, Islamabad. Her areas of interest include NGN, Handover, security and IMS.

**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.