Human-centric Computing and Information Sciences
a SpringerOpen Journal

RESEARCH Open Access

# IP Multimedia subsystem authentication protocol in LTE-heterogeneous networks

Madhu J Sharma* and Victor CM Leung

*Correspondence:
madhusj@ece.ubc.ca
Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC, V6T1Z4 Canada

**Abstract**

IP Multimedia Subsystem (IMS) introduces important advantages for users of LTE-femtocell heterogeneous access networks. In order to access services hosted in the IMS layer, the user has to undergo authentication procedure with the access network, followed by an authentication procedure with the IMS layer. This multi-pass authentication procedure is essential for securing IMS from malicious users, resulting in added overhead and possible quality of service degradations. The problem is further compounded when the user moves from one femtocell domain into another, which requires the authentication procedure to be repeated. To mitigate this problem, we present a lightweight, robust, and architecture-compatible IMS authentication protocol that implements a one-pass IMS procedure by promoting efficient key re-use for a mobile user. We make use of Home Node B femtocells to perform the role of IMS proxy. To verify the feasibility of using our protocol in mobile networks, an abstract model of our protocol is derived. The abstract model is emulated using Asterisk server and virtualization techniques. We also analyze the authentication delay of our proposed scheme. Numerical results reveal a reduction in user authentication delay of more than 50 percent compared to the existing authentication procedure.

## Introduction

The goal of this paper is to extend the improved IP Multimedia Subsystem-Authentication and Key Agreement (IMS-AKA) protocol proposed in [1] to Long Term Evolution (LTE) domain, and perform a feasibility study using emulation techniques. LTE is commonly referred to as a type of Fourth Generation (4G) wireless service. LTE offers superior mobile broadband service using femtocells and picocells, in co-ordination with the core network. A deployment that supports macros, picos, femtos and relays in the same spectrum is called a heterogeneous network. In our paper, we present LTE-femtocell heterogeneous network for IMS access. The choice of the access network is prerogative of the mobile operator, because IMS services are independent of the underlying access network. However, to support rich applications offered by IMS, it is better to chose an access network that would support high bandwidths and low jitter. The speeds offered by todays LTE network clearly do not support bandwidth intensive applications like video conferencing and cloud gaming. Hence, we consider a heterogeneous LTE-femtocell network.

In the new LTE Evolved Packet Core (EPC) architecture, there is no circuit-switched domain to handle voice calls in the traditional 2G/3G way. A solution for voice over LTE will, therefore, be needed as LTE access becomes more widespread. In order to support voice calls, numerous approaches were considered, including IMS. IMS is an access independent subsystem, and offers much more than voice. As a result, it becomes much more easier to migrate services and solutions from one access network to another.

The IMS is a standardized Next Generation Network (NGN) architecture defined by the European Telecommunication Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP) to provide Internet media services capability [2]. As with the Internet, NGN is built around the Internet Protocol (IP) and its goal is to create a unified system that offers services like video, voice and data by encapsulating them into packets [3]. The NGN architecture can incorporate a variety of wireless and wireline technological alternatives for users to access the global telecommunication network.

### Related Work

There is limited literature that deals with reducing authentication costs for mobile IMS users. Just like any other IP based protocol, IMS is vulnerable to threats and security considerations [4]. The original 3GPP specifications for safeguarding IMS is a convoluted multiway procedure, and it does not suggest measures to thwart Denial of Service or malicious unregistrations.

The security issues related to IMS are briefly illustrated in [5]. IMS is based on Session Initiation Protocol (SIP) and IP protocols thats why it has inherent vulnerabilities related to them. Some of the highlighted concerned to the IMS security are Denial of Service (DoS), gateway attacks and illegal impersonation attacks.

User Datagram Protocol (UDP) Flood Attack is one of the attacks causing host based Denial of Service [6]. UDP is a connectionless protocol and it does not require any connection setup procedure to transfer data. A UDP Flood Attack is possible when an attacker sends a UDP packet from a random port on the victim system. In a spoofing attack, the intruder sends messages to a computer indicating that the message has come from a legitimate system. To be successful, the intruder must first determine the IP address of a trusted system, and then modify the packet headers.

N. Crespi et al. proposed a new functional entity, called WLAN SIP proxy, in the WLAN that enables the latter to perform localized IMS services [7]. This approach proves to be quite useful in LTE-Heterogeneous networks. Introduction of a SIP feature in Home Node B module would result in its participation during IMS registration sessions.

A one-pass AKA working on top of WLAN is proposed in [8], which reduces the authentication costs using an International Mobile Subscriber Identity-IP Multimedia Private Identity ($impi - imsi$) pair. Unfortunately, the user becomes vulnerable to potential spoofing attacks by rogue third party application vendors [9]. A similar scheme was proposed in [10], which involves a Universal Mobile Telecommunications System (UMTS) authentication procedure followed by *impi* verification to secure IMS access. The authentication scheme proposed in [11] requires several architectural changes to IMS, whereas the secure authentication model in does not require significant changes to the existing architecture [12]. However, the policy of fetching authentication vectors induces serious delays especially when the user tries to re-associate with IMS, e.g., after moving from one access network to a different one.

### Contribution

In contrast to the existing literature on the subject, we propose a robust one-pass IMS authentication mechanism which necessitates no change to the existing standardized IMS architecture [1]. We use of modified EAP-AKA protocol [13] for authentication with the access network. Some of the keys generated during this authentication process is reused in IMS authentication protocol, which introduces improvements in security and authentication delays. The resulting network protocol is simple to implement and does not necessitate changes to the existing architecture. The security properties of the proposed IMS-AKA are validated and examined using Automated Validation of Internet Security Protocols and Applications (AVISPA) security analyzer. AVISPA is a package used to test and validate the security of large- scale Internet security protocols [14,15]. The message exchange is coded using a programming language understandable by AVISPA. We perform detailed analysis of authentication delay to show a 50 percent improvement over the existing multi-pass authentication scheme proposed in the original 3GPP specification.

The contributions of this paper are as follows.

1. We made use of the Improved IMS-AKA protocol presented in [1], for IMS authentication in LTE-femtocell heterogeneous networks.
2. In order to test the usability of our protocol in mobile networks, we emulate our protocol using Asterisk open source SIP server. A comparative study of results of experimental analysis and theoretical analysis is performed. An exact model of IMS architecture is replicated using open source software tools and proprietary network components. The goal of this implementation is to test the usability of our protocol.
3. We perform detailed numerical analysis to show a 50 percent improvement over the existing multi-pass authentication schemes.

The rest of the paper is organized as follows. In Section “IMS Architecture”, we present some background on IMS and LTE-Heterogenous networks and analyze the problems in existing authentication mechanisms. In Section “Proposed Authentication Procedure”, we present our proposed IMS authentication protocol, emulation of our security protocol in Section “Protocol Emulation and Analysis”. In Section “Overhead in Security Policy”, we discuss the additional overhead involved in our protocol, conclude the paper in Section “Conclusion”.

## IMS Architecture

IMS is a standard that defines a generic architecture for offering Voice over IP (VoIP) and multimedia services [16]. This way, operators can take advantage of a powerful multi-vendor service creation industry, avoiding sticking to a single operator to obtain new services. IMS provides integrated services to its customers, and a platform for application providers to host their content on its servers.

The IMS does not mandate any particular business model. Instead, it lets operators charge as they think more appropriate. The IMS provides information about the service being invoked by the user, and with this information the operator decides whether to use differentiated rate for the service, apply traditional time-based charging, apply QoS-based, or perform any new type of charging [17].

The IMS core network, predominantly consists of the Call Session Control Function (CSCF) and the Home Subscriber Server (HSS). The CSCF node facilitates session setup and teardown using SIP. HSS plays the role of a location server in IMS and also serves as a single point of service for IMS subscribers and their services [18]. The Subscriber Location Function (SLF) is needed to map user addresses when multiple HSSs are used. CSCF is divided into three logical entities: Proxy CSCF (P-CSCF), Interrogating CSCF (I-CSCF), and Serving CSCF (S-CSCF). P-CSCF is responsible for routing incoming SIP messages to the IMS registrar server and for facilitating policy control. I-CSCF acts as an inbound SIP proxy server in the IMS. S-CSCF is the heart of the IMS core network. It facilitates the routing path for mobile originated or terminated session requests and is the most processing intensive node of the IMS core network. Finally, the Application Server (AS) is a standardized element in the IMS model, which hosts and executes services, and interfaces with S-CSCF using SIP.

The fact that IMS is an access network independent technology results in additional security concerns. There needs to be additional security measures that guarantee precise functioning of IMS regardless of what the access network offers. Hence, the architecture stipulates that a mobile user should follow a multi-pass authentication process to access IMS services. This is because the inherently open nature of IP-based networks exposes the User Equipment (UE) and service providers to security attacks. It has been shown that a UE authenticated by the LTE core network can impersonate another user to gain illegal access to IMS services [4,5]. The multi-pass authentication procedure authenticates the IMS subscriber in both the domains of the access network and the IMS, and involves an execution of Long Term Evolution- Authentication and Key Agreement ( LTE-AKA ) followed by IMS-AKA with IMS layer. The traditional IMS-AKA is shown in Figure 1. However, the operations in IMS-AKA are almost the same as that in LTE-AKA. It is inefficient that almost all involved steps in the multi-pass authentication are duplicated. This results in discernible delays and battery power drain during UE authentication, especially

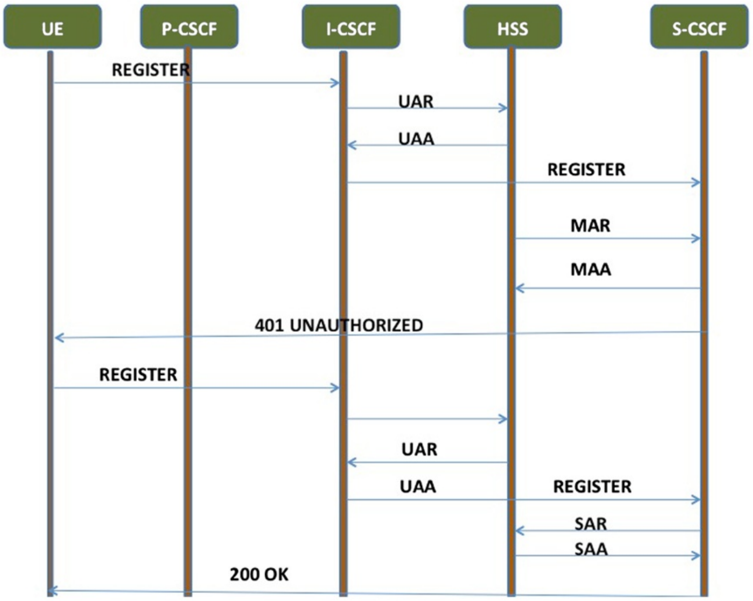

**Figure 1 Traditional IMS AKA Protocol.**

when UE needs to be re-authenticated multiple times due to mobility or a long-lived connection. Therefore, it is desirable to develop a procedure that reduces the time required to re-authenticate the IMS subscriber without compromising the level of security provided by the existing authentication procedure.

### LTE Heterogeneous Network

In this section, we present Long Term Evolution network for 4G access as shown in Figure 2, and unification of IMS services with the LTE core network. A true 4G technology needs to achieve stationary speeds of 1Gbit/s and mobile speeds of 100Mbit/s. There are more technical specifications, but these two are enough to distinguish 4G from non-4G technologies. In order to support the burgeoning needs of customers, LTE core network alone may not be sufficient. In such cases, the operators could make user of a set of one or more femtocells and a set of core network elements to manage and support the use of those femtocells in accessing network services, as in Figure 2. A femtocell is a radio access network element that supports LTE services, operates in a limited geographic area in licensed spectrum, may operate over the public internet, and supports a limited number of simultaneous users in generally small environments such as a home. The functionality of a femtocell is similar to a WLAN router. The Femtocell Access Point (FAP) helps to tunnel voice and multimedia content between UE and LTE core network. It is connected to the core network via broadband or air interface, with a capacity to hold few users in a residential area or business environment.

LTE is implemented on EPC. The transition to LTE/System Architecture Evolution (SAE) involves a fundamental shift to a "flat" all-IP system architecture that impacts every part of the network, with the Evolved Packet Core (EPC) at its centre. SAE specifies an all-IP network architecture designed to support end-to-end packet services. It comprises two tightly integrated components: the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) - a.k.a. LTE RAN - and EPC.

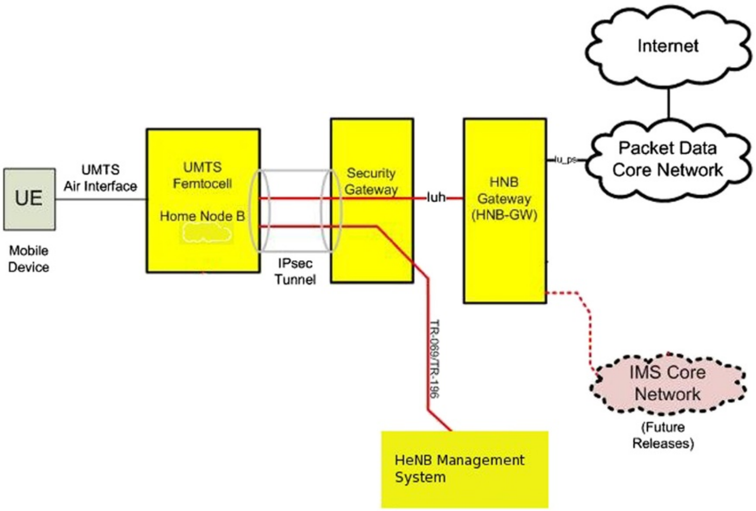

**Figure 2 LTE-femtocell Heterogeneous Network.**

### Components of LTE

The basic entities of Enhanced packed Core are shown in Figure 2. The only node in the Evolved Universal Terrestrial Radio Access (eUTRAN) is the eUTRAN Node-B (eNodeB). It is a radio base station that is in control of all radio related functions in the fixed part of the system. Typically, the eNodeBs are distributed throughout the networks coverage area, each residing near the actual radio antennas. The HSS is the master database for a given user. It is the entity containing the subscription-related information to support the network entities actually handling calls/sessions. Mobility Management Entity (MME) is the control plane entity within EPC. MME supports Non-Access-Stratum NAS signalling and security. It is responsible for authentication of users, bearer establishment, roaming and lawful interception of traffic. The Packet Data Network Gateway (PDN GW) is responsible for handling packet transport within the LTE. In order to support LTE-Heterogeneous networks, we need to include the following:

Home Node B (HeNB) is a base station located on the user premises and operates in the same radio interface as that of the operator [19]. The HeNB system can be deployed either in Closed Subscriber Group (CSG) mode or Open mode. In CSG mode, only certain subscribers can access the HeNB, whereas in Open mode any subscriber in the vicinity has access to HeNB. Secure Gateway (SeGW) is the door to the core network. All HeNBs must be authenticated by the SeGW before it could commence services. A SeGW may or may not use an Authentication Authorization and Accounting (AAA) server to complete authentication procedure. Femtocell Management System (FMS) is responsible for management of all the HeNBs. Depending on its location, either radio interface or broadband access is used for communication with HeNB. HeMS is responsible for running periodic updates and monitoring the health of a HeNB.

#### LTE Heterogeneous Network Authentication Procedure

The LTE-IMS authentication is a multi step process, during which both the user and HeNB are authenticated with the core network.

- **HeNB Authentication with LTE Secure Gateway**
  Upon gateway discovery, HeNB initiates an Internet Key Exchange (IKE) v2 based authentication by sending an IKE INIT Request to the secure gateway as shown in Figure 3. The request message consists of SA$_i$, which is the list of algorithms that support IKE. KE$_i$ denotes the HeNB's Diffie-Hellman value.

  $$IKE_{(INIT-REQ)} = PRF(SA_i, KE_i, Nonce) \tag{1}$$

  SeGW sends an INIT Response message, requesting a certificate from HeNB, certreq. It chooses the choice of the certificate vendor in SAr$_i$, completes Diffie-Hellman exchange with KE$_r$.

  $$IKE_{(INIT-RES)} = PRF(SA_r, KE_r, Nonce_r, certreq) \tag{2}$$

  HeNB sends an IKE auth request message AUTH, which consists of its unique ID, ID$_i$ , the requested client certificate, authentication payload and traffic selectors TS$_i$, TS$_r$. It also requests the server certificate from SeGW. The entire payload is

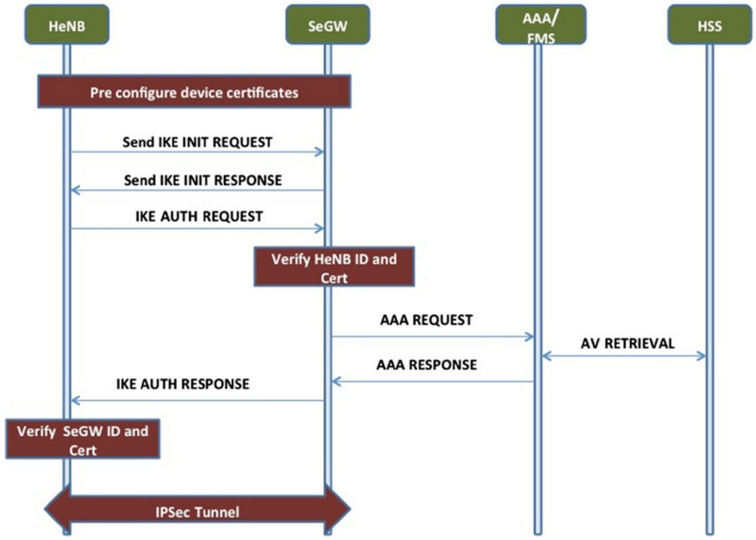

**Figure 3 HeNB Authentication in LTE-Heterogeneous Network.**

encapsulated for integrity protection.

$$IKE_{(AUTH-REQ)} = PRF(SA_i, AUTH, ID_i, TS_i, TS_r Nonce_i, cert, certreq) \tag{3}$$

SeGW first verifies that the certificate in the cert payload has not been tampered and the $\mathrm{ID}_i$ corresponds to the identity in the certificate. If the verification is successful, using the public key of the certificate, the SeGW generates the expected AUTH payload and compares it with the received AUTH payload. If they match, then the authentication of the HeNB is successful. Otherwise, the SeGW sends an IKEv2 Notification message indicating authentication failure. If the network policy requires femtocell subscription authorization, the SeGW contacts the AAA to verify that the HeNB identified by its ID is authorized to provide service. AAA contacts HSS to derive authentication vectors and responds with the authorization result.

$$IKE_{(AUTH-RESP)} = PRF(SA_r, AUTH, ID_r, TS_i, TS_r Nonce_i, cert) \tag{4}$$

HeNB verifies that the SeGW certificate in the CERT payload has not been modified and the identity IDr corresponds to identity in the server certificate. If the verification is successful, using the public key of the server certificate, the HeNB generates the expected AUTH payload and compares it with the received AUTH payload. If they match, then the SeGW (server) authentication is successful.
An IPsec SA pair is established between the FAP and the SeGW. Additional IPSec tunnels may be created, if required.

- **UE Authentication with LTE Core Network**
  If HeNB operates in CSG mode, HSS stores a record of list of all valid UEs in a particular CSG. The data can be retrieved by MME in order to verify CSG subscriptions and expiry time.
  - The UE initiates the LTE NAS procedure by sending an attach message to the HeNB. The attach message is usually in the form of a NAS Request message,

which consists of UE's International Mobile Subscriber Identity (IMSI). The process is shown in Figure 4.

- Upon receiving the NAS request, HeNB attaches the CSG-ID and forwards the request to HeNB gateway. If the UE identity has not been established before, the HeNB GW performs a registration procedure, before forwarding the NAS Request to the core network.
- The MME verifies whether it holds subscription data for the UE. If there is no subscription data in MME then it sends an Update Request message to the HSS.
- If the CSG ID is not valid, the MME shall send the corresponding NAS reject message to the UE.
- For valid UEs, the MME would continue with the generic LTE-AKA, to complete the authentication procedure as shown in Figure 5.

- **Registration of UE with IMS** HeNB assumes the role of a P-CSCF and SIP server for the UE [20].
  - The IMS HeNB performs the HeNB registration procedure to the HeNB-GW.
  - When the UE attempts to access the HeNB via an initial NAS message and there is no context in the HeNB allocated for that UE, the HeNB performs the UE Registration to the HeNB-GW.
  - The IMS HeNB requests IMS Access Authorization by providing necessary identifying information for the IMS HeNB and UE, e.g., HeNB Identity, IMSI, etc. to a RADIUS server associated with HSS.
  - The HSS grants the IMS access authorization to the UE after verifying one or more of the following criteria, as established by operator policy. Hence, all IMS authentications are localized to HeNB node.
  - In case the UE was already IMS registered via another IMS HeNB, IMS will de-register the UE from the previous IMS HeNB.
    event.

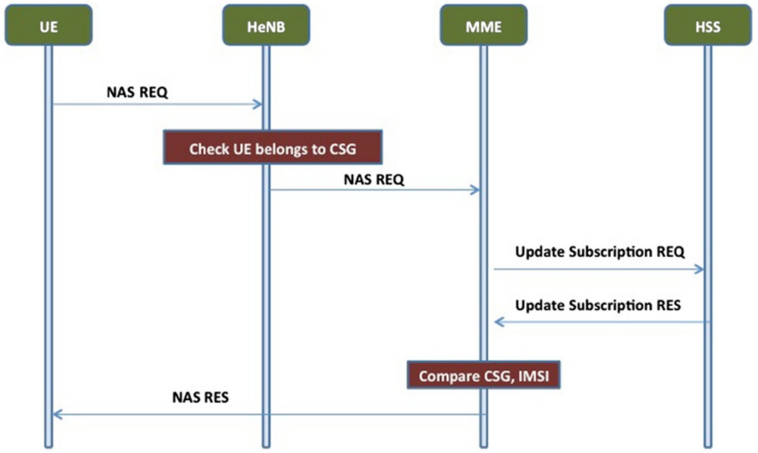

**Figure 4 UE Authentication with LTE Network.**

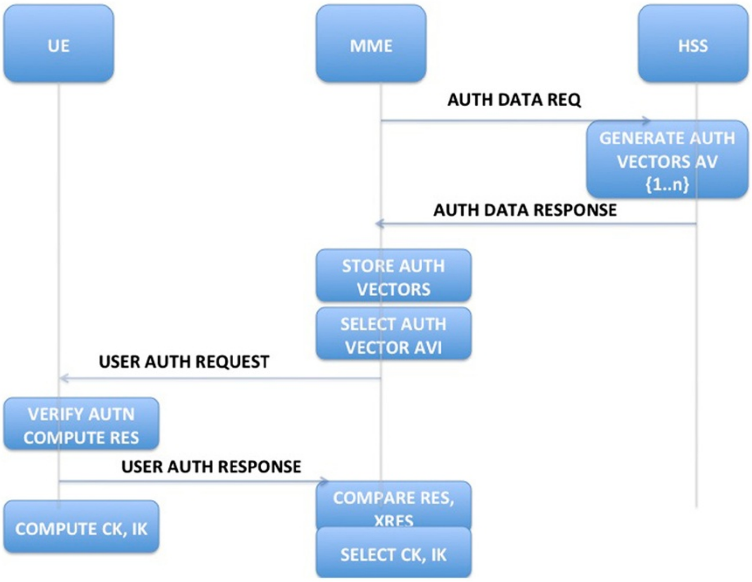

**Figure 5 LTE-AKA.**

### Problems in Existing Authentication Mechanisms

The traditional IMS-AKA given in Figure 1, clearly demonstrates the intricate authentication procedure followed between the UE and the system servers. These transactions produce significant overhead, as mentioned before, thus supporting our claim for the need to create a simplified and secure authentication procedure that reduces authentication delay without compromising security.

All security protocols for IMS layer, defined thus far would broadly fall under two categories.

- Network Attachment Sub-System (NASS) Bundled IMS authentication
- Password based Digest Authentication

#### *NASS Bundled IMS Authentication*

NASS based models do not implement any authentication mechanism at all, to reduce authentication delay. The IMS users are authenticated by underlying access network authentication and their identity and their IP address are sent to IMS network as the proof of authentication. Both solutions assume anti-spoofing mechanisms in access networks while forging of IP address would lead to forged identity in IMS network. The security level of IMS network corresponds to the security level of underlying access network.

Similarly, in the LTE-Heterogeneous domain, there is over reliance on HeNb, as it plays the role of proxy in LTE and IMS layers. If the security of HeNB is compromised, an intruder could hack into LTE and IMS layers. Further, HeNB is not authenticated with the IMS layer. This authentication procedure is a throw back to the initial days of IMS, where security is compromised for faster access to IMS layer. IMS architecture is mainly based on SIP, and SIP runs primarily on UDP. Integrity and confidentiality of messages exchanged between nodes could be compromised. Hence, it is essential to safeguard communication between HeNB and UE.

The existing one-pass authentication method is vulnerable to fake attack on IMS subscribers and temporary cheat attacks. It results in a situation where the UE and the P-CSCF do not have a cipher key (CK) and an integrity key (IK) to achieve conentiality and integrity protection support between the UE and the P-CSCF. This may lead to serious breach of security.

For instance, the LTE-IMS AKA protocol described in the existing protocols, the radius server is designed to accept the IP address of the latest REGISTER request as the client's IP address. Because the authentication is vulnerable to replay attack, and query floods, until the next REGISTER request is due, an adversary is able to re-register using the same challenge response with different IP address to redirect all the features to any other preferred destination. This effectively creates a denial of service and identify theft risk to the legitimate user. Also with the lack of two-way authentication, an adversary can hijack the session using man-in-the-middle attacks.

#### *Password based Digest Authentication*

Digest access authentication is password based identification method that allows secure user identification using passwords. However, Digest authentication does not protect IMS signaling. Digest authentication uses Message-Digest algorithm 5 (MD5) cryptographic hashing algorithm together with nonce values to prevent cryptanalysis. It should be difficult to determine original secret input key value by knowing only algorithm output value. However attacker may try to test large set of inputs (dictionary or some other suitable list) with brute force attacks in order to find a matching output. If user password is too simple then attacker has a good chance to find it. Digest authentication does not rely on use of smart cards for tamper-proof storage of user password. It is up to user to remember the password and so if users are given a chance to set password they tend to produce simple ones that will be easy to remember. This gives brute-force attacks a higher chance for success. In order to prevent attacker to discover different parameters required for brute-force attack IMS signaling traffic must be protected. Digest authentication should be coupled with Transport Layer Security (TLS) / IPSec to provide security for IMS signaling traffic.

## Proposed Authentication Procedure

In contrast to the existing model, we introduce 2 key changes.

### HeNB Authentication with IMS Layer

HeNB should be authenticated with the LTE core network as described in Section "LTE Heterogeneous Network Authentication Procedure" [21]. Then, the HeNB should be authenticated with S-CSCF in IMS layer using, one of the following security mechanisms [22].

- Trusted Node Authentication (TNA)
- SIP Digest

In our model, we make use of TNA to authenticate HeNB with S-CSCF. In TNA, access to IMS is granted based on a successful access level authentication performed by a trusted node in the network [23]. As HeNB already has secured access to the core network, further authentications are not necessary. Hence the HeNB acts as a trusted node to the IMS domain and takes on the role of both the SIP User Agent and proxy from an IMS UE perspective.

### UE Authentication with IMS Layer

First, the UE should be authenticated with the LTE core network as described in Section "LTE Heterogeneous Network Authentication Procedure ". In order to overcome some of the security deficiencies in the existing protocols, we introduce a security policy which necessitates the establishment of IPSec tunnel in addition to IMS-AKA.

- As shown in Figure 6, HeNB takes the role of P-CSCF. When UE is authenticated by the MME, the integrity and confidentiality keys are securely transported to HeNB.
- To initiate IMS-AKA, an IPSec tunnel is established between HeNB and UE.
- Initially, when UE tries to secure first time access to IMS, it sends a SIP Register message with the *impi* parameter value to HeNB, upon completion of LTE-AKA [24,25].
- HeNB identifies the appropriate I-CSCF and forwards the IMS initiation request.
- I-CSCF identifies S-CSCF using the name address resolution mechanism and forwards the SIP register message to S-CSCF.
- It is obvious that the (*imsi*, *impi*) pair would not present in S-CSCF. So it probes HSS with a Multimedia Auth Request, and receives the key value pair via Cx interface. Further, S-CSCF encapsulates XRES stored during LTE-AKA, in a 200 OK message and forwards it to the user.
- UE receives 200 OK message. HeNB stores encryption keys for subsequent re-authentications.

## Protocol Emulation and Analysis

The goal of this implementation is to test the usability of our protocol with the existing infrastructure. This section provides a brief description of the technologies used to implement the emulator and UEs. Abstraction of key IMS components including P-CSCF,

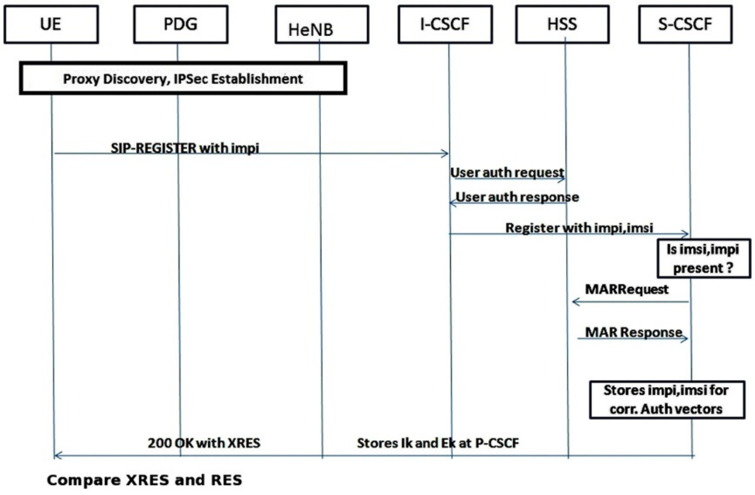

**Figure 6 UE Authentication with IMS Layer.**

S-CSCF and I-CSCF using linux network tools was essential to validate our protoco. The whole platform is deployed using three virtual machines which are built on top of Windows 2008 R2 server using VMWare virtualization tool. The server runs on Intel Core i7 processor at 3.05 Ghz and has 8GB of RAM. It consists of multiple Network Interface Cards (NIC) to support multiple local area networks (LAN). The network topology, designed for IPv4 protocol, is given in Figure 7.

- The entire network topology operates in two Virtual LANs (VLAN), namely VLAN 20 and VLAN 30. In order to provide suitable isolation between the two VLANs, we make use of a Cisco Catalyst 2950 24 switch. One to one correspondence exists between VLANs and the subnets. VLANs are configured to map directly to an IP subnet, which gives the appearance of involving Layer 3 (the network layer) in the context of VLANs. VLAN 20 operates in 10.1.100.0/24 subnet, while VLAN 30 operates in 172.16.200.0/24.
- A Windows Vista virtual machine takes the role of a UE in our model. Our network model is designed to support any popular SIP based softphone application. In this case, we have chosen Ekiga (formerly known as GNOMEMeeting). It is interoperable with many other standard compliant softwares, hardwares and service providers as it uses both the major telephony standards (SIP and H.323). It also runs a variation of a Virtual Private Network (VPN) client software[26]. The windows user primarily operates in VLAN 20 network.
- The gateway is a virtual machine which runs on CentOS 5.0 operating system. It is analogous to P-CSCF in an IMS architecture. It acts as the link between the user and the service layer. The gateway is designed to operate in two VLANs, namely VLAN 20 and VLAN 30. It can support Internet Security Association and Key Management Protocol (ISAKMP) protocol to support IPSec. For the user to initiate IMS-AKA, it is

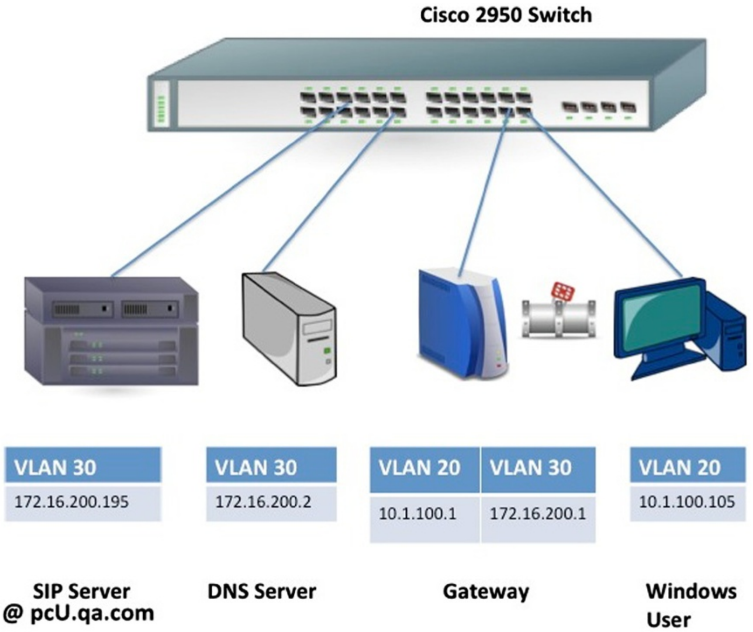

**Figure 7 Network Topology for Protocol Implementation.**

necessary to establish a secure tunnel between user and the gateway. It also supports secure transport of SIP messages to the service layer. The gateway configuration can be tweaked to limit the influx of SIP register requests from the user. This acts as a defence mechanism against DoS attacks. The gateway operates in both VLAN 20 and VLAN 30 networks.

- DNS Server assumes the role of an I-CSCF. Upon receiving the query from the gateway, DNS server would it query its database to identify the location of the server. The DNS server is implemented using a CentOS 5.0 linux virtual machine. The DNS server primarily operates in VLAN 30 network.
- The server is a Ubuntu-Linux virtual machine, that runs Asterisk. It is analogous to S-CSCF in an IMS architecture. Asterisk is an open source software which can be used to develop communication services [27]. Asterisk is considered for this emulation, because it is simple to implement. Numerous features can be provided by altering its configuration file suitably. Open source means that the developer can change source codes so the applications can be added easily by the user. Asterisk can be considered as a complete Private Branch Exchange (PBX ) or Software complete PBX and provide all PBX features. The advantage of Asterisk is that it can run on multiple operating systems and Asterisk is compatible with Simple Network Management Protocol (SNMP) for monitoring the alerts. For the server to support our protocol, it is necessary to alter configuration files to include user details. The protocol operates on User Datagram Protocol (UDP) port 5060. In order to debug connections, we make use of SIP Python script. The Asterisk server primarily operates in VLAN 30 network, and it is assigned a domain name of pcU.qa.com.
- All the nodes in the topology run a version of Wireshark for packet capture and analysis.

#### *IPSec Tunnel between Gateway and User*

IPSec VPN tunnelling is typically performed at Layer 3, or lower, of the OSI network model. To enable access, we establish encrypted network connectivity between a user and the internal network. VPNs use encryption and other security mechanisms to ensure that only authorized users can access the network. VPNs also ensure that data transmitted between computers cannot be intercepted by unauthorized users. In general, the data is encoded so that it cannot be understood, and the data has to be decrypted before it can be used.

The gateway has to be configured to set-up VPN tunnels with the user. There are plenty of open source VPN servers that run on Linux.We have used Open Swan for this implementation. As the first step, we need to define the Phase-1 negotiation parameters. In our model, we choose Digital Encryption Standard (DES), a 64-bit block algorithm that uses a 56-bit key and 3DES, in which plain text is encrypted three times by three keys for packet encryption. The encrypted data is then encapsulated using SHA-1 algorithm to check the authenticity of messages during phase 1 negotiations. We chose Diffie-Hellman 5 group configuration for generating the session keys. For authentication purposes, we used Pre-shared key (PSK) for simplicity. The IKE Phase -1 operates in main mode, which has three sets of 2-way message exchanges between the user and gateway.

Upon successful completion of IKE Phase 1, IKE phase 2 begins. IKE phase 2 operates in quick mode. It negotiates a shared IPSec policy, derives shared secret keying material used for the IPSec security algorithms, and establishes IPSec Security Associations (SA). Quick mode exchanges nonces that provide replay protection. The nonces are used to generate new shared secret key material and prevent replay attacks from generating phony SAs. The tunnel association and key exchange procedure has been captured and validated using Wireshark. A graph plotting the data transfer in bytes/tick against time is given in Figure 8. Bytes/tick will measure the total number of bytes in all packets matching the display filter for the graph in each measurement interval.The detailed key exchange is provided in the Appendix section.

### *SIP Registration*

After IKE phase two is complete and quick mode has established IPSec SAs, information is exchanged by an IPSec tunnel. Packets are encrypted and decrypted using the security policy specified in the IPSec SA. IPSec VPN association is indispensable in IMS-AKA because most of the SIP servers do not support TCP. VPN is the only solution to provide required level of security.

On successful IKE association, the gateway assigns a dynamic IP address in VLAN 30 for the windows user. The IP address is valid as long as the association is valid.

### *Authentication Procedure*

This subsection describes in detail how SIP messages are passed over the IMS network when establishing, participating in, and leaving an IMS network.

- All SIP requests are routed through the gateway. SIP runs primarily on UDP-5060, hence it is securely transported through IPSec tunnel.
- The gateway checks the destination of the SIP registrar. In this case, it is pcU.qa.com.
- The gateway queries the DNS-server, which runs on a CentOS 5.0 linux server, to get the address of the SIP registrar.
- The DNS Server returns the query with a valid IP address, or sends recursive queries to other DNS servers to get the IP address. In this case, the DNS server returns the IP address of 172.16.200.195 to the gateway.
- The gateway forwards the SIP register request to the Asterisk server.
- The server compares the user-identification, password, and subscription details. The user receives an OK message upon successful registration.
- The entire authentication process is monitored using Wireshark packet analyzer.

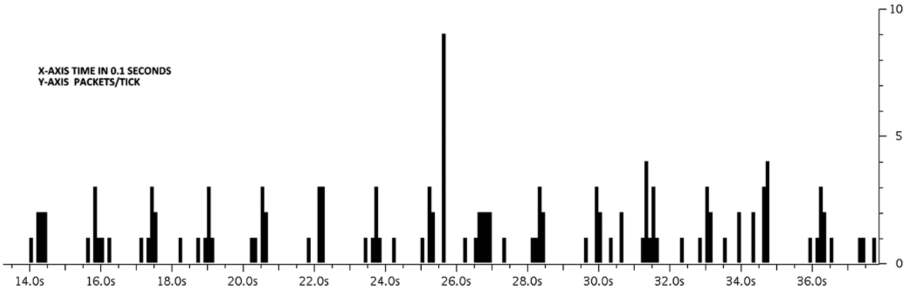

**Figure 8 A plot of packet transferred against time during ISAKMP.**

The implementation is studied for three scenarios, 1) SIP registration with invalid account details 2) SIP registration with a valid user account and 3) SIP unregister.

### *SIP Registration with Invalid Account*

Whenever a user tries to access IMS layer without a valid account, the registration requests are rejected by the authenticating server. In our implementation, the user generates a SIP request message encapsulated in MD5 digest message and forwards it to the gateway. The Asterisk server duly responds by sending a 404 Not found message.

### *SIP Registration with valid Account*

In this scenario, Ekiga client generates a SIP digest message with the following details. The Asterisk server validates the user details and responds with a 200 OK message. In this case, user is not authorized to use any of the subscription services. Any subscription requests or option updates would be duly responded with a 401 Not subscribed message. The graph representing message exchange during SIP registration is shown in Figure 9.

```
Method: REGISTER Request-URI:
sip:pcU.qa.com
CSeq: 4 REGISTER
Via: SIP/2.0/UDP/10.1.100.105:5060
User-Agest:Ekiga/3.2.7
From: <SIP:5005@pcU.qa.com>
Call-ID:d530d861-b4ea-1810
To: <SIP:5005@pcU.qa.com>
Contact: <SIP:5005@10.1.100.105>
Allow: INVITE, ACK, OPTIONS, BYE, CANCEL,
        SUBSCRIBE, REFER, PING
Expires: 3600
```

### *SIP Unregistration*

The unregister SIP requests are responded with a 200 OK message. The process follows similar procedure compared to SIP registration, in order to prevent malicious users from sending Unregister messages. The graph representing message exchange during SIP unegistration is shown in Figure 10.

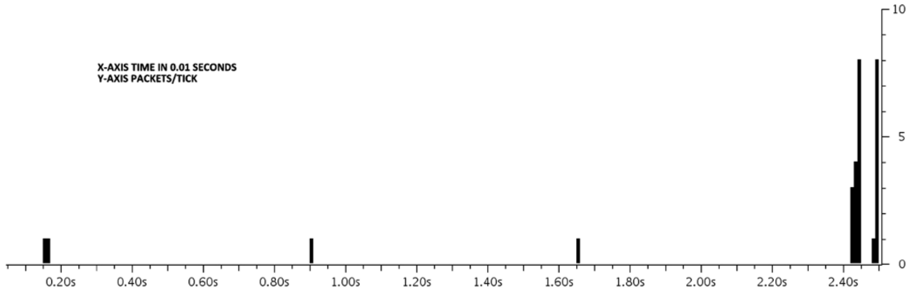

**Figure 9 A Plot of Message Exchange during SIP Registration.**

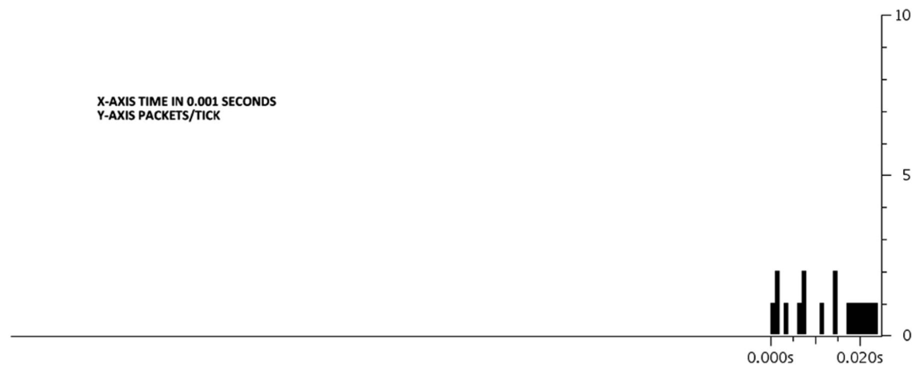

**Figure 10 A Plot of Message Exchange during SIP Unregistration.**

### *Comparison with two-pass IMS-AKA*

3GPP specified IMS-AKA process was explained in detail in Section "LTE Heterogeneous Network Authentication Procedure". Upon receiving the Register message, S-CSCF sends a 401 notification to the UE, requesting additional information. The additional information is usually sent in the form of an authentication challenge, along with a sequence number. IMS user computes the challenge response, generates a new Register message and forwards it to the S-CSCF. We have modelled this process using our network topology. In our proposed protocol, we have eliminated all redundant exchange of information between the user and authentication server.

The request methods is the typical number of packets generated during a call registration. The call setup and tear down times can be calculated based on the packets captured using Wireshark. For our protocol, the call setup merely requires 8.2005 Seconds. This is the time taken to establish IPSec tunnel and SIP Registration. IPSec tunnel establishment requires 5.786 Seconds, and SIP registration takes 2.4145 Seconds. In contrast to our protocol, the two-pass IMS-AKA requires 4.528 Seconds, after IPSec tunnel establishment. Despite propagation delays and processing delays, the user would enjoy remarkable reduction in authentication delay, if deployed in mobile networks. Detailed performance evaluation and analysis is presented in Section "Overhead in Security Policy".

## Overhead in Security Policy

This section is to analyze the additional delay in authentication procedure when IPSec is introduced to our protocol. Let $P_0$ denote the case where there is no IPSec configured between UE and P-CSCF, and $P_\phi$ denote the case where there is some security policy configured between the two nodes, in addition to the IMS-AKA. The packet overhead may occur due to adding extra headers by security policy, encryption of packet and so on.Let $T^s(k, P_\phi)$ is the time required by the sender to process $k^{th}$ packet with IPSec policy $P_\phi$ , $T^r(k, P_\phi)$ is the time required by the receiver to process $k^{th}$ packet, $T^t(k, P_\phi)$ is the time taken by the packets to traverse through the network between UE and P-CSCF. The total processing time of the $k^{th}$ packet is

$$T(k, P_\phi) = T^s(k, P_\phi) + T^r(k, P_\phi) + T^t(k, P_\phi) \tag{5}$$

Assuming that there are N packets required to establish a security association,

$$\sum_{k=0}^{N} T(k, P_{\phi}) = \sum_{k=0}^{N} [\, T^{s}(k, P_{\phi}) + T^{r}(k, P_{\phi}) + T^{t}(k, P_{\phi})] \tag{6}$$

Assume that the size of $k^{th}$ packet is $l_k$ bits, and then the total number of bits in N packets, denoted by Bn,

$$B_n = \sum_{k=0}^{N} l_k \tag{7}$$

We analyze the authentication delay in terms of the bit rate (bits/sec). *BR($P_{\phi}$)* denotes the bit rate that is achieved during IPsec security association,

$$BR(P_{\phi}) = \frac{B_n}{\sum_{k=0}^{N} [\, T^{s}(k, P_{\phi}) + T^{r}(k, P_{\phi}) + T^{t}(k, P_{\phi})]} \tag{8}$$

*BR($P_0$)* denotes the bit rate that is achieved without an IPSec association,

$$BR(P_0) = \frac{B_n}{\sum_{k=0}^{N} [\, T^{s}(k, P_0) + T^{r}(k, P_0) + T^{t}(k, P_0)]} \tag{9}$$

The overhead *O($P_{\phi}$)* associated with the IPSec associations can be expressed in terms of the bit rate,

$$O(P_{\phi}) = \frac{B_n}{\sum\limits_{k=0}^{N} \left[T^{s}(k, P_{\phi}) + T^{r}(k, P_{\phi}) + T^{t}(k, P_{\phi})\right]} - \frac{B_n}{\sum\limits_{k=0}^{N} \left[T^{s}(k, P_0) + T^{r}(k, P_0) + T^{t}(k, P_0)\right]} \tag{10}$$

$O(P_{\phi})$ refers to the overhead associated in encrypting and decrypting data.

Assume that security policy $P_{\phi}$ is configured in the authentication model. Through experiments we find the time involved in processing $k^{th}$ packet by $P_{\phi}$ during its authentication phase, $t_k(P_{\phi})$. Assume N packets are exchanged during authentication phase. Let total time in processing N packets be represented by $TN(P_{\phi})$, which can be calculated by

$$TN(P_{\phi}) = \sum_{k=1}^{N} t_k(P_{\phi}) \tag{11}$$

From the above equation, we can determine time $t_f(P_{\phi})$, when the st data packet is sent from a sender to a receiver with security policy $P_{\phi}$, time $t_l(P_{\phi})$ when last data packet is delivered to a receiver j from a sender i with security policy $P_{\phi}$. Hence, the total delay is

$$tt = t_l(P_{\phi}) - t_f(P_{\phi}) \tag{12}$$

## Conclusion

We have identified the security challenges of IMS implementation over Heterogeneous networks. An improved version of IMS-AKA protocol was discussed, which is efficient and better than existing protocols, in terms of security and performance. The problems associated with call set up and tear down due to the lack of circuit switched core network was discussed. We presented a readily available solution in the form of IMS and ways to improve IMS authentication process. We introduced a network topology using a collection of open source linux software, proprietary network components and virtualization tools to emulate our security protocol. The topology clearly emulates the real world IMS architecture and their roles in IMS-AKA. The numerical results obtained during the emulation process, shows an improvement over the existing scheme, in terms of security and authentication delay. Thus, we addressed some of the key issues in IMS, without introducing any serious changes to the existing architecture.

## Future Work

The proliferation of smart-phones and tablets are on the rise. Wearable networking, internet-of-Things, and smart home appliances, would mean more wireless devices per user. Eventually, all these devices would utilize LTE to access an information repository. It would be mundane to have a separate authentication mechanism for each device. In the future, researchers could extend this protocol to provide a unified authentication mechanism for multiple devices.

### Competing interests

We declare that there are no competing interests.

### Authors' contributions

MS was responsible for devising and emulating the protocol. MS and VL drafted the manuscript. Both authors read and approved the final manuscript.

Received: 1 March 2012 Accepted: 21 September 2012
Published: 15 October 2012

### References

1. Sharma M, Leung VCM (2011) Improved IP Multimedia Subsystem authentication mechanism for 3G-WLAN networks. International Journal of Security and Networks 6(2/3): 90–100
2. UMTS Forum (2001) Ranking of top 3G services. UMTS Forum Tech. Rep.
3. 3GPP.TS.22.934 (2002) Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network interworking
4. Bellman B (2007) Exploring IMS security mechanisms. Business Communications Review
5. Hunter MT, Clark RJ, Park FS (2007) "Security issues with the IP Multimedia Subsystem (IMS). ACM Workshop on Middleware for next-generation converged networks and applications. Article 7
6. Velasco V (2000) Introduction to IP Spoofing. http://www.sans.org
7. Crespi N, Lavaud S (2004) WLAN Access to 3G Multimedia Services. Information and Communication Technologies (ICT), Bangkok
8. Ntantogian C, Xenakis C, Stavrakakis (2007) Efficient authentication for users autonomy in Next Generation All-IP networks. Bio-Inspired Models of Network, Information and Computing Systems, Bionetics 2007. 2nd, 295–300
9. Lin Y, Chang M, Hsu M, Wu L (2005) One-pass GPRS and IMS authentication procedure for UMTS. IEEE Journal on Selected Areas in Communications 23(6): 1233–1239
10. Long X, Joshi J (2010) Enhanced One-Pass IP Multimedia Subsystem Authentication Protocol for UMTS, Proceedings of IEEE International Conference on Communications, ICC 2010, pp 1–6
11. Ntantogian C, Xenakis C (2009) One-Pass EAP-AKA Authentication in 3G-WLAN Integrated Networks. Wireless Personal Communications 48(4): 569–584
12. Huang C, Li J (2007) Efficient and Provably Secure IP Multimedia Subsystem Authentication for UMTS. The Computer Journal 50: 739–757
13. Al Shidhani A, Leung VCM (2009) Pre-authentication schemes for UMTS-WLAN interworking. EURASIP Journal on Wireless Communications and Networking 2009
14. Armando A, Compagna L (2004) An Optimized, Intruder Model for SAT-based Model-Checking of Security Protocols. Workshop on Automated Reasoning for Security Protocol Analysis, ARSPA, Electronic Notes in Theoretical Computer Science 125: 91–108
15. AVISPA-Automated Validation of Internet Security Protocols. http://www.avispa-project.org, 2002
16. 3GPP.TS.33.203 (2009) 3G Security; Access security for IP-based services
17. 3GPP.TR.23.870 (2009) SR VCC Support for IMS Emergency Calls
18. 3GPP.TS.33.102 (2009) Technical Specification Group Services and System Aspects; 3G Security;Release 9
19. 3GPP.TS.25.467 (2010) UTRAN architecture for 3G Home Node B
20. 3GPP.TR.23.832 (2010) IP Multimedia Subsystem (IMS) aspects of architecture for Home Node B (HNB)
21. Forsberg D (2010) LTE Key Management Analysis with Session Keys Context. Computer Communications 33(16): 1907–1915
22. Oredope A, Pham V, et al (2011) Deploying IP Multimedia Subsystem (IMS) Services in Future Mobile Networks. Communications (NCC), National Conference, January 2011

23. 3GPP.TS.24.228 (2005) Technical Specification Group Core Network and Terminals;Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3
24. 3GPP.TS.29.229 (2008) Technical Specification Group Core Network and Terminals; Cx and Dx interfaces based on the Diameter protocol; Release 8
25. 3GPP.TS.33.210 (2009) 3G Security;Network Domain Security;Ip network layer security
26. http://www.openswan.org/
27. http://www.asterisk.org/

doi:10.1186/2192-1962-2-16
**Cite this article as:** Sharma and Leung: **IP Multimedia subsystem authentication protocol in LTE-heterogeneous networks.** *Human-centric Computing and Information Sciences* 2012 **2**:16.

,