Improved IP Multimedia Subsystem Authentication Mechanism for 3G-WLAN Networks

Madhu J. Sharma and Victor C.M. Leung
Department of Electrical and Computer Engineering
The University of British Columbia, Vancouver, Canada, V6T 1Z4
Email: {madhusj,vleung}@ece.ubc.ca

***Abstract*—The provision of IP Multimedia Subsystem (IMS) introduces important advantages for users of 3G WLAN networks. However, a multi pass authentication procedure needs to be performed before accessing the IMS, resulting in added overhead and quality of service (QoS) degradation, which deters service providers from adopting the IMS model. The problem is further compounded when the user moves from one Wireless Local Area Network (WLAN) domain into another, requiring that the authentication procedure be constantly 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 derive an analytical model of our proposed scheme, and conduct numerical analysis that reveal a user authentication delay decrease of more than 50 percent.**

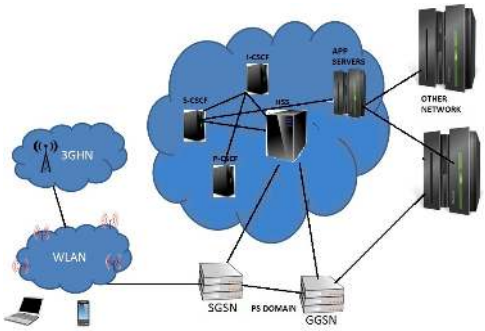

Fig. 1. IMS architecture over 3GPP-WLAN

I. Introduction

The IP Multimedia Subsystem is a standardised Next Generation Networks (NGN) architecture for providing Internet media services capability defined by the European Telecommunication Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP). 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. Thus, it is not difficult to envisage IP Multimedia Subsystem (IMS) deployed on top of a heterogeneous 3G-WLAN architecture, given that Wireless Local Area Network (WLAN) support higher data rates, limited coverage and low implementation and service costs compared to 3GPP. As a result, innovative applications that require better quality of service (QoS) such as video conferencing and real-time applications can be offered. With such coexistence capabilities, users can seamlessly handover from 3GPP to WLAN and vice-versa without serious service disruption. Although it offers plenty of options for network operators to offer innovative services, the complexity of the resulting architecture raises significant security concerns.

One of the requirements of this architecture stipulates that a mobile user should follow a multi-pass authentication process to access IMS services. This is because the inherent nature of IP-based networks exposes the User Equipment(UE) and service providers to security attacks. It can be shown that a UE authenticated by 3GPP-WLAN can impersonate another user to gain illegal access to IMS services. Multi pass authentication procedure involves an execution of Extended Authentication Protocol-Authentication and Key Agreement (EAP-AKA) with the access network and IP Multimedia Subsystem Authentication and Key Agreement (IMS- AKA). This results in discernible delays and battery power drain during UE authentication. Therefore, it becomes necessary to reduce the time required to re-authenticate the WLAN-UE link.

There is limited literature that deals with reducing authentication costs for mobile IMS users. Ntantogian et al [1] proposed a one-pass AKA on top of WLAN, which reduces the authentication costs using an International Mobile Subscriber Identity-IP Multimedia Private Identity ($impi - imsi$) pair [2]. Unfortunately, the user becomes vulnerable to potential spoofing attacks by rogue third party application vendors. A similar scheme was proposed by Lin et al [3], which involves a UMTS authentication procedure followed by $impi$ verification to secure IMS access. Huang et al [4] proposed an authentication scheme that requires several architectural changes to IMS, whereas Long et al [5] proposed a secure authentication model that does not require significant changes to the existing architecture. However, the policy of fetching authentication vectors induces serious delays especially, when the user tries to re-associate with IMS. In the next section we present a rapid access mechanism based on reusing authentication vectors, which greatly reduces delay with no compromise on security.

In contrast to the existing literature on the subject, we propose a robust one-pass IMS authentication mechanism on top of the modified EAP AKA protocol and Intra WLAN pre-Authentication protocol [6], that introduces improved efficiency and re-authentication delays. Our protocol reduces redundant exchange of authentication vectors and the associ-

978-1-4244-9920-5/11/$26.00 ©2011 IEEE

ated costs of using a multis-pass authentication protocol. The resulting network protocol is simple to implement and does not necessitate changes to the existing architecture.

The rest of the paper is organized as follows. In Section II, we discuss background on authentication mechanisms for heterogeneous 3GPP-WLAN. In Section III, we introduce the proposed solution. We present our performance evaluations in Section IV, security analysis in Section V, sand conclude the paper in Section VI.

II. BACKGROUND

A. IMS Architecture

The IMS core network, as shown in Fig 1, predominantly consists of the Call Session Control Function (CSCF) (see [7] [8]) and the Home Subscriber Server (HSS). The CSCF node facilitates Session Initiation Protocol (SIP) session setup and teardown [9], [10]. The 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. A Subscriber Location Function (SLF) is needed to map user addresses when multiple HSSs are used. The Call Session Control Function is divided into three logical verticals: Proxy CSCF (P-CSCF), Interrogating CSCF (I-CSCF), and Serving CSCF (S-CSCF).The P-CSCF is responsible for routing incoming SIP messages to the IMS registrar server and for facilitating policy control. The I-CSCF acts as an inbound SIP proxy server in the IMS. The 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 the S-CSCF using SIP.

B. 3G-WLAN Authentication

At the beginning of the process, the UE authenticates with the home access network [11] as illustrated in Fig 2. This process involves the following: User Equipment (UE), a WLAN Authentication Authorization and Accounting server (WAAA), a Home Authentication Authorization and Accounting server (HAAA), an Access Point (AP) and a Home Subscriber Server (HSS). We make use of an improved version of EAP-AKA, which distinctly minimizes re-authentication delays. In modified EAP-AKA protocol [12], the WAAA locally re-authenticates stationary users on behalf of HAAA and HSS. The strategy of localizing authentications within the WLAN domain reduces authentication delays and minimizes dependence on critical servers in the 3G Home Network (3GHN).

In the standard EAP-AKA protocol, the UE and the HAAA must generate a Master session key (MSK) and an Extended MSK($EMSK$) after a successful authentication. The MSK is transported to the AP to be used in generating a Transient Session Key (TSK). There, the $EMSK$ is generated but its usage is not yet specified. In this protocol, the key hierarchy in EAP-AKA protocol is extended by introducing WLAN domain-level and local-level keys derived from MSK and $EMSK$. $EMSK$ is used to derive additional keys, namely

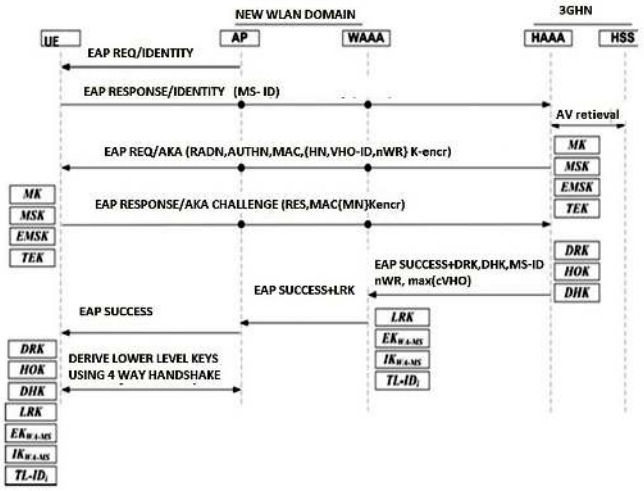

Fig. 2. Mod EAP-AKA Authentication

the Handover Root Key (HOK), the Domain-level Handover key (DHK) and the Local-level handover key (LHK), to achieve faster pre-authentication without compromising security. Domain-level keys are unique keys derived by the HAAA and the UE per WLAN domain. Local-level keys are unique keys derived by the WAAA and the UE per AP within the WLAN domain. The local-level keys are later used to derive TSK.

The procedure is as follows:

1) The HAAA generates the next local ID, $IDWLAN$, to be used by the UE in the next pre-authentication and a nonce value (HN). The HAAA indicates the permitted number of pre-authentications (nWR) the UE can perform before falling back to mod-EAP-AKA authentication. The WAAA and UE adjust the WLAN counter (WC), according to $npre$, where WC is the number of times pre-authentications has been performed. In addition, the UE generates a nonce, UN.
2) Five new keys are generated [12]. (a) A Root handover key, HOK is derived from $EMSK$ by the HAAA and the UE only. Both nodes use a special Pseudo-random Function (PRF) similar to the one used in generating MSK in the standard EAP-AKA protocol

$$HOK = PRF(EMSK, EAP - AKAsessionID| HAAAID|UEM, 256), \quad (1)$$

where "|" denotes concatenation and,

$$EAP - AKAsessionID = (EAP|RAND|AUTN) \quad (2)$$

UEM is the UE address in the medium access control layer, HAAA ID is the identity of the HAAA server and $AUTN$ is an authentication vector. (b) The domain-level handover key, DHK is derived from HOK by HAAA and UE only

$$DHK = PRF(HOK, HN|WAAAID|UEM, 256), \quad (3)$$

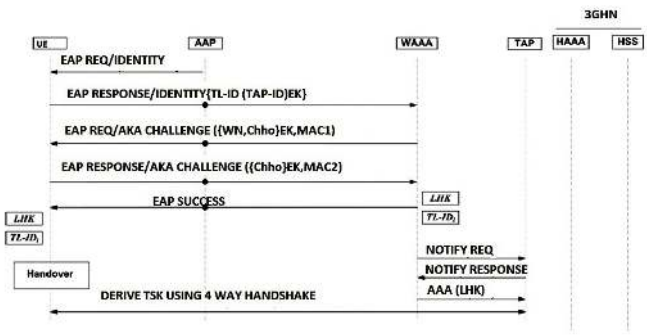

Fig. 3. Intra WLAN Re-Authentication Protocol

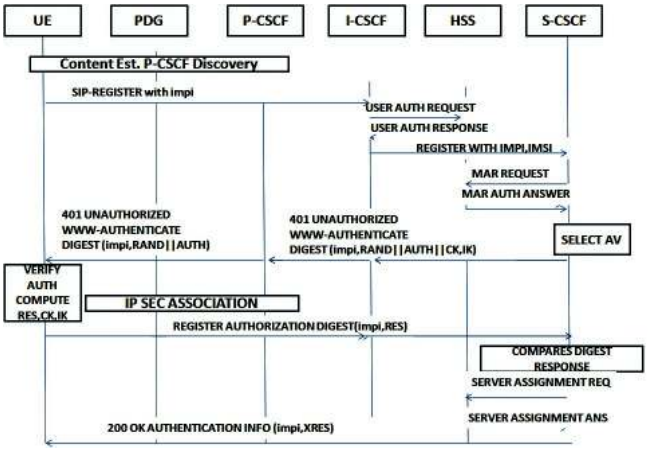

Fig. 4. Traditional IMS AKA Protocol

where WAAA ID is the identity of the WAAA server. (c) The domain-level and local-level reauthentication keys, DRK and LRK. (d) A $KWAAA-UE$ key, which is used to secure traffic between the UE and WAAA. This key is only derived by the UE and WAAA. The derivation is explained in [12].

3) The HAAA securely delivers DRK, DHK, $npre$ and $IDWLAN$ to the WAAA.
4) The WAAA securely delivers LRK to the AP.
5) Derivation of HOK, DHK, DRK, LRK, and $KWAAA-UE$ by the UE.

A UE roams to a neighbor AP when experiencing poor signal-strength from the currently associated AP in the same WLAN domain. Therefore, we make use of the Intra WLAN pre-Authentication protocol to secure access to Target Access Point (TAP) and minimize delay [6]. Here, the WAAA handles UE authentication instead of the HSS and HAAA. The protocol proceeds as follows:

1) When the UE recognizes the need for handover within the WLAN domain, it invokes the Intra-WLAN pre-authentication protocol and sends an EAP message to the currently associated AP, as shown in Fig.3. The AP replies with an identity request message.
2) The UE responds to the request with $IDWLAN$, $TWAAA$ ID and TAP ID
3) Receiving $TWAAA$ ID and TAP ID indicates a handover pre-authentication request. The WAAA classifies this request as Intra-WLAN, if the received $TWAAA$ ID matches its identity and the TAP ID matches the identity of one of the APs in the WLAN domain. The WAAA then consults WC and prepares a challenge message that includes a fresh nonce, WN, and the next $IDWLAN$, and WC and $MAC1Intra$ calculated using $KWAAA-UE$,

$$MAC1Intra = SHA-1(KWAAA-UE, WC| IDWLAN|WN) \quad (4)$$

, where $SHA-1$ is the Secure Hash Algorithm.
4) On the UE's side, the WC stored in the UE's database is matched with the WC recently received. Then a new $MAC1Intra$ is calculated and compared with the received $MAC1Intra$. If both checks are positive, then the UE stores $IDWLAN$ and replies with WC and $MAC2Intra$,

$$MAC2Intra = SHA-1(KWAAA-UE, WC|WN) \quad (5)$$

5) The WAAA then derives a local-level handover key, LHK, from DHK as follows:

$$LHK = PRF(DHK, WC|TAPID|UEM, 512) \quad (6)$$

The WAAA increments WC and sends EAP success message to the UE. Consequently, the UE derives LHK and increments WC. WAAA and TAP exchange Notify-Request and Accept RADIUS AAA message to confirm handover operation.

C. IMS Authentication

After the packet data protocol context activation, if the UE wants to use IMS multimedia services, the UE will activate the IMS registration procedure, which is depicted in Fig.4.

1) The UE sends a SIP Register message with $impi$ [13], which passes through the UMTS Packet-Switched (PS) domain and P-CSCF and then arrives at ICSCF.
2) When I-CSCF receives the register message, it sends a User Authorization Request (UAR) to the HSS to ask for the available S-CSCFs that can serve the UE. Then the HSS gives a User Authorization Answer (UAA) to I-CSCF to inform about the available S-SCSCFs that can serve the forthcoming UE.
3) After I-CSCF identifies the address of S-CSCF, it then forwards the Register message to the S-CSCF.
4) If S-CSCF does not have a valid authentication vector (AV) for UE, S-CSCF sends a Multimedia Authentication Request (MAR) over Cx reference to HSS for obtaining an AV array [14]. Otherwise, this Step and step 6 can be skipped. Note that an AV contains (i) a random number RAND, (ii) an expected response XRES, (iii) a cipher key CK, (iv) an integrity key IK, and (v) an

authentication token AUTH Otherwise these steps can be skipped.

5) S-CSCF stores the AV and selects one array AV(i) from the vector. Then it sends a "401 unauthorized message" notice to P-CSCF via I-CSCF.
6) P-CSCF keeps CK(i) and IK(i) and then sends the 401 message to UE with $impi$, RAND(i) and AUTH(i).
7) UE authenticates the server by checking AUTH(i), computes the RES(i), and then sends the Register message with $impi$ and RES(i) to S-CSCF.
8) S-CSCF checks the RES(i) with XRES(i) values; if they match, then the UE is a legitimate user. SCSCF sends Server Assignment Request (SAR) to HSS to inform which S-CSCF will serve the UE. HSS then sends a Server Assignment Answer (SAA) to S-CSCF.
9) S-CSCF sends a "200-OK" message to UE.

III. Proposed IMS Authentication

The previous section 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. In this section, we introduce the one - pass IMS authentication procedure as shown in Fig.5. The proposed protocol offers high degree of security to the user and the network amidst threats. Assume that the UE has completed modified the EAP-AKA procedure. From the aforementioned AKA procedures, it is clear that there is a repetition of authentication steps. Hence, we propose a novel IMS-authentication procedure, which supports key re-use. This protocol is based on the assumption that all UE would request IMS services from the cellular operator. Upon mod EAP-AKA authentication occurring, a RAND, XRES and encryption keys are securely transported from HAAA to S-CSCF via HSS. This greatly reduces the time required to derive authentication vectors, when S-CSCF validates the IMS user for the first time. Subsequent, authentications are solely based on $impi$ verification. Ideally, this IMS registration expires in 600,000 seconds. However, in real time applications, the UE or the network initiates IMS re-registration quite often, depending on the changes in the underlying network. The protocol develops as follows:

1) Initially, when UE tries to secure first time access to IMS, it sends a SIP Register message with the $impi$ parameter value to Packet Data Gateway (PDG), a sequence number (SN) and time stamp (TS), which notifies the network that it has completed EAP-AKA. This ensures IMS access to subscribers only.
2) PDG can identify $imsi$ of the UE from the $impi$. PDG forwards $imsi$ and $impi$ to P-CSCF.
3) I-CSCF identifies S-CSCF using the name address resolution mechanism and forwards the SIP register message to S-CSCF.
4) 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 [15]. Further, S-CSCF encapsulates XRES stored during mod EAP-AKA, in a 200 OK message and forwards it to the user.
5) The aforementioned step can be avoided during WLAN re-authentications. When UE moves from one AP to another in the same WLAN domain, Intra WLAN pre-authentication is invoked. If IMS re-authentication is required, then the S-CSCF compares the received $imsi$ with the stored $imsi, impi$ pair. If the $imsi$ values match, it then sends a OK signal to the UE.
6) UE receives 200 OK message. P-CSCF stores encryption keys.

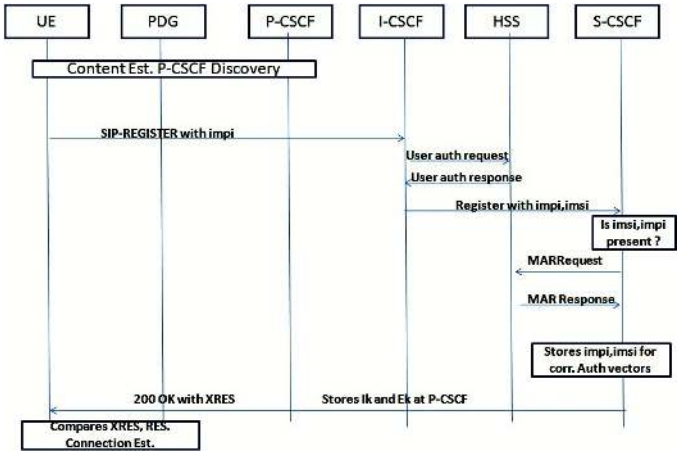

Fig. 5. Proposed IMS AKA Protocol

IV. Performance Evaluation and Analysis

Considering the delivery cost D_i as an evaluation metric, we compare our protocol with original IMS-AKA protocol. We assume that the delivery cost between UE and S-CSCF is one unit and the delivery cost of one signalling message in the IMS layer ie between any two of I-CSCF, S-CSCF and HSS is α units.

In existing IMS-AKA, if $impi, imsi$ values are not present in S-CSCF, it interacts with HSS to derive the vector pair. From Fig.4,

$$D_{I1} = 4 + 6\alpha \tag{7}$$

If they are present in S-CSCF, then it reduces the message-exchange between HSS and S-CSCF to,

$$D_{I2} = 4 + 4\alpha \tag{8}$$

, where α is a value between 0 and 1. The AV contains n arrays, where n$\geq$1; therefore one out of n IMS registrations executes Steps 4 and 5. Then the IMS registration cost is computed as follows

$$D_I = (D_{I1}/n) + ((n-1) * D_{I2}/n) = 4 + ((2n+1) * 2\alpha/n) \tag{9}$$

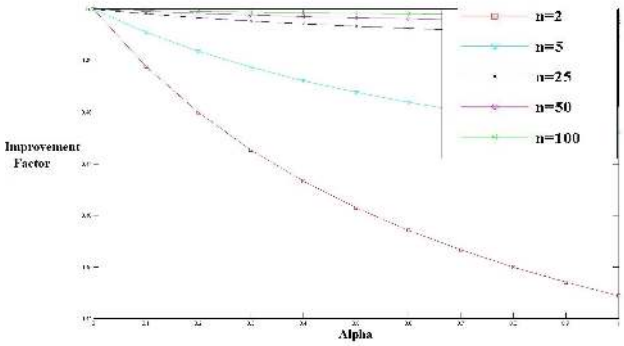

Fig. 6. α vs Improvement Factor over IMS-AKA

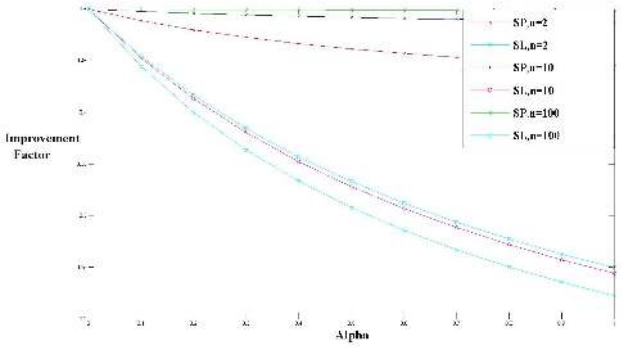

Fig. 7. Comparison of our protocol and Long et al's protocol

In our proposed protocol as in Fig.5, If $impi, imsi$ values are not present in S-CSCF, then:

$$D_{P1} = 2 + 4\alpha \tag{10}$$

If the vectors are present in S-CSCF, then

$$D_{P2} = 2 + 2\alpha \tag{11}$$

.
Hence, the IMS registration cost is

$$D_P = 2 + ((n+1) * 2\alpha/n) \tag{12}$$

The improvement factor S_P is the improvement in IMS registration cost over the original protocol. It is obtained as follows,

$$S_P = (D_I - D_P)/D_I = n(\alpha+1)/(2n + \alpha(1+2n)) \tag{13}$$

Plugging typical values for n and α shows an improvement of 50 percent over the traditional multi-pass IMS-AKA. Fig. 6 plots the improvement achieved by the proposed protocol over the original one for different values of n and α.

Our protocol is better than the previously proposed one-pass IMS Authentications. We consider the improvement factor derived in Long et al [5].

$$S_L = n/(2n + (2n+1)\alpha) \tag{14}$$

$$S_P/S_L = (1+\alpha) \tag{15}$$

Fig. 7 plots the improvement achieved by the proposed protocol over the one proposed by Long et al, for different values of n and α. Thus, it can be observed that the proposed protocol achieves better performance in terms of delay, without compromising any security considerations.

A. Total Delay Analysis

Most of the previous IMS authentication protocols are based on IMS-AKA on top of fast EAP-AKA. The following evaluation explains why mod-EAP AKA is a better protocol than the standard fast EAP-AKA for IMS access. We determine the total authentication delay D_{auth} for IMS access,

$$D_{auth} = D_{proc} + D_{trans} + D_{prop} \tag{16}$$

, where, D_{proc} is the processing delay at each node. D_{trans} and D_{prop} are transmission and propagation delays. D_{trans} is negligible. Propagation delay is due to message exchanges between UE and AP (D_{propUA}), AP and WAAA (D_{propAW}), WAAA and HAAA(D_{propWH}), UE and S-CSCF(D_{propUS}). During the re-authentication process with Target AP, the total delay for IMS authentication on fast EAP-AKA is

$$D_{auth} = D_{proc} + 5D_{propUA} + 4D_{propAW} + 4D_{propWH} + 2D_{propUS} \tag{17}$$

In our proposed protocol the total delay is

$$D_{auth} = D_{proc} + 5D_{propUA} + 4D_{propAW} + +2D_{propUS} \tag{18}$$

Thus, our protocol achieves significant improvement in performance by reducing the message exchange between HAAA and WAAA during re-authentications.
Our proposed IMS protocol is much faster than the existing schemes. Storing essential vectors and response message further reduces delay and promotes efficient key re-use. Mathematical analysis shows a 50 percent improvement over the multi pass AKA for IMS access.

The generation of additional keys during mod-EAP AKA procedure may require better processing capabilities at the end nodes. This is a compromise we need to make in order to reduce authentication delays. Faster authentication times translate to better quality of service. The proposed protocol also achieves better results during re-registrations.

The number of times the UE handles message processing is directly related to battery drain. Since, the number of message

passing between the UE and IMS is limited, it does not impose a drain in energy levels. We have tried to limit the number of times the UE is involved in message processing .

V. Security Analysis

In this section, we briefly analyze the security of our proposed protocol.

Fake IMS identity manifestations are eliminated as this method is based on $impi$ value of the UE. The $impi$ value is unique, and the $impi - imsi$ pair is securely derived from HSS by S-CSCF, when the UE tries to authenticate for the first time.

Replay attacks are avoided when S-CSCF evaluates TS and SN. If TS is acceptable, it checks whether SN is less than SN_{max}. SIP requests with greater SN values will be discarded. Further, PDG and S-CSCF would also know that UE has completed mod-EAP AKA, thereby preventing illegal access.

Better security for UE from malicious application providers as this method is based on authentication between S-CSCF and the UE. IMS services are not initiated before the user compares XRES and RES values.

This protocol guarantees confidentiality and integrity as no key is transmitted in the clear. Keys, nonces and counters are securely transmitted to protect against eavesdropping attacks. There is no key exchange between UE and AP when the UE authenticates with the access network.

All the keys generated in this protocol are fresh and discarded periodically. The concerns of using stale authentication keys during IMS-AKA are allayed, as the previously generated keys in mod-EAP-AKA are used only for the first time, and discarded upon IMS authentication.

Thus, our protocol introduces considerable improvement in performance, without compromising security.

VI. Conclusion

In this paper, we identified the security challenges of IMS implementation over 3G-WLAN heterogeneous networks. A re-authentication protocol based on key exchange procedure was discussed. We capitalized on the execution of mod-EAP-AKA to shorten the execution of IMS-AKA and eventually speed up re-authentications. The analysis shows an improvement in speed of 50 percent compared to traditional IMS-AKA and significant improvement over other proposed protocols, in terms of security and performance. Security issues identified in Lin et al were eliminated. Thus, we hope to address some of the key issues in IP Multimedia Subsystem, without introducing any changes to the existing architecture. As part of our future work, we would like to perform extensive security analysis and extend the research to accommodate Inter-WLAN re-authentications.

Acknowledgment

The authors acknowledge fruitful discussions with Dr. Ali Al Shidhani. This work has been supported in part by TELUS, the Natural Sciences and Engineering Council of Canada, and the Institute for Computing, Information and Cognitive Systems (ICICS) at UBC.

References

[1] C. Ntantogian and C. Xenakis, "One-pass eap-aka authentication in 3g-wlan integrated networks," *Wirel. Pers. Commun.*, vol. 48, pp. 569–584, March 2009. [Online]. Available: http://portal.acm.org/citation.cfm?id=1502537.1502563

[2] C. Ntantogian, C. Xenakis, and I. Stavrakakis, "Efficient authentication for users autonomy in next generation all-ip networks," 2007, pp. 295 –300.

[3] Y.-B. Lin, M.-F. Chang, M.-T. Hsu, and L.-Y. Wu, "One-pass gprs and ims authentication procedure for umts." *IEEE Journal on Selected Areas in Communications*.

[4] C.-M. Huang and J.-W. Li, "Efficient and provably secure ip multimedia subsystem authentication for umts," *Comput. J.*, vol. 50, pp. 739–757, November 2007. [Online]. Available: http://portal.acm.org/citation.cfm?id=1349545.1349547

[5] X. Long and J. Joshi, "Enhanced one-pass ip multimedia subsystem authentication protocol for umts," in *Communications (ICC), 2010 IEEE International Conference on*, May 2010, pp. 1 –6.

[6] A. "Al Shidhani and V. Leung, "Pre-authentication schemes for umts-wlan interworking," *Eurasip J. Wirel.Commun.Netw.*, pp. 5:1–5:16, February 2009. [Online]. Available: http://dx.doi.org/10.1155/2009/806563

[7] "3GPP", "3G Security;3G security;Access security for IP-based services," 3rd Generation Partnership Project (3GPP), TS 33,203, Dec. 2009. [Online]. Available: http://www.3gpp.org/ftp/specs/html-info/33203.htm

[8] 3GPP, "SR VCC Support for IMS Emergency Calls," 3rd Generation Partnership Project (3GPP), TR 23.870. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/23870.htm

[9] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261 (Proposed Standard), Internet Engineering Task Force, June 2002, updated by RFCs 3265, 3853, 4320, 4916, 5393, 5621. [Online]. Available: http://www.ietf.org/rfc/rfc3261.txt

[10] "3GPP", "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; Release 5," 3rd Generation Partnership Project (3GPP), TS 24,228, Dec. 2005. [Online]. Available: http://www.3gpp.org/ftp/specs/html-info/24228.htm

[11] 3GPP, "Technical Specification Group Services and System Aspects;3G Security;Release 9," 3rd Generation Partnership Project (3GPP), TS 33,102, Dec. 2009. [Online]. Available: http://www.3gpp.org/ftp/specs/html-info/33102.htm

[12] A. Al Shidhani and V. Leung, "Local fast re-authentication protocol for 3g-wlan interworking architecture," in *Wireless Telecommunications Symposium, 2007. WTS 2007*, april 2007, pp. 1 –8.

[13] "3GPP", "3G Security;Network Domain Security;Ip network layer security," 3rd Generation Partnership Project (3GPP), TS 33,210, Dec. 2009. [Online]. Available: http://www.3gpp.org/ftp/specs/html-info/33210.htm

[14] 3GPP, "Technical Specification Group Core Network and Terminals;Cx and Dx interfaces based on the Diameter protocol;Release 8," 3rd Generation Partnership Project (3GPP), TS 29,229, 2008. [Online]. Available: http://www.3gpp.org/ftp/specs/html-info/29229.htm

[15] "3GPP", "Technical Specification Group Core Network and Terminals; IP Multimedia (IM) Subsystem Cx and Dx interfaces;Release 8," 3rd Generation Partnership Project (3GPP), TS 29,228, Sep. 2009. [Online]. Available: http://www.3gpp.org/ftp/specs/html-info/29228.htm