Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2009, Article ID 806563, 16 pages
doi:10.1155/2009/806563

Research Article

Pre-Authentication Schemes for UMTS-WLAN Interworking

Ali Al Shidhani and Victor C. M. Leung

Department of Electrical and Computer Engineering, University of British Columbia, 2332 Main Mall, Vancouver, BC, Canada V6T 1Z4

Correspondence should be addressed to Ali Al Shidhani, alia@ece.ubc.ca

Received 31 January 2009; Accepted 30 April 2009

Recommended by Yang Xiao

Interworking Universal Mobile Telecommunication System (UMTS) and IEEE 802.11 Wireless Local Area Networks (WLANs) introduce new challenges including the design of secured and fast handover protocols. Handover operations within and between networks must not compromise the security of the networks involved. In addition, handovers must be instantaneous to sustain the quality of service (QoS) of the applications running on the User Equipment (UE). There is a need to design fast and secured handover protocols to operate in UMTS-WLAN interworking architectures. This paper proposes two secured pre-authentication protocols in the UMTS-WLAN interworking architectures. Performance analysis of the proposed protocols show superior results in comparison to existing protocols in terms of authentication signaling cost, authentication delay and load on critical nodes involved in the authentication procedure. Additionally, the security of the proposed protocols was verified by the Automated Validation of Internet Security Protocols and Applications (AVISPA) security analyzer.

1. Introduction

UMTS-WLAN interworking is being widely considered by cellular service providers because of its advantages for both end users and service providers. The 3rd Generation Partnership Project (3GPP) has recently published specifications detailing suggested UMTS-WLAN interworking architecture [1]. A simplified architecture following a nonroaming reference model [1] is shown in Figure 1. Interworking UMTS and WLAN introduces new handover and security challenges. Handovers in general are classified into horizontal and vertical handovers [2]. Horizontal Handovers (HH) occur when roaming within a network employing the same wireless technology while Vertical Handovers (VH) occur when roaming between networks employing different wireless technologies. Handovers are further subdivided into link-layer (L2) handovers and Internet Protocol (IP)-layer (L3) handovers [2].

Link-layer handover handles association and authentication of the WLAN User Equipment (UE) to a target attachment point. IP-layer handover is generally based on Mobile IP (MIP) functionalities and aims to register a new UE IP address in the visited network. This paper discusses the authentication operation during link-layer HH within WLANs when operating in a UMTS-WLAN interworking architecture. In such architecture, the UE must be initially authenticated by servers in the UMTS Home Network (UHN) such as the Home Location Register (HLR), Home Subscriber Server (HSS), and Home Authentication, Authorization, and Accounting (HAAA) server [3].

Several UMTS-WLAN authentication schemes have been proposed in the literature. Kambourakis et al. [4], Prasithsangaree and Krishnamurthy [5], and Chen et al. [6] proposed using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) [7, 8], EAP-Tunneled TLS (EAP-TTLS) [9], and Protected EAP (PEAP) [10], respectively, to authenticate a UE in the UMTS-WLAN interworking architecture. These authentication protocols are based on public key cryptography and require digital certificate management to operate properly.

3GPP recommends invoking EAP with Authentication and Key Agreement (EAP-AKA) to authenticate a UE in the UMTS-WLAN interworking architecture [3, 11]. EAP-AKA relies on pre-shared secrets held by the UE and HSS and does not require public key cryptography or digital certificate management. In EAP-AKA, the UE, and the

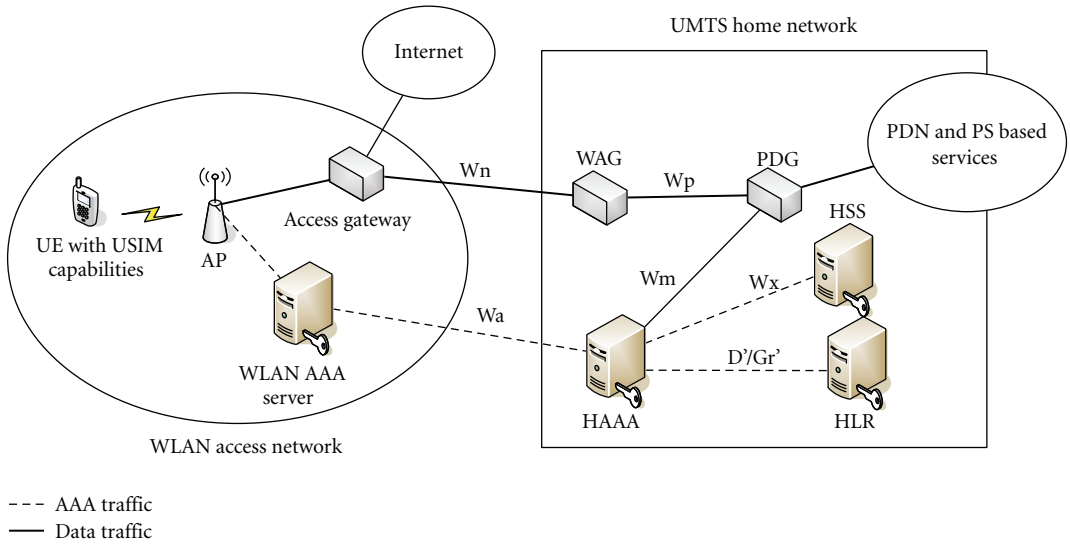


Figure 1: Simplified UMTS-WLAN interworking architecture.

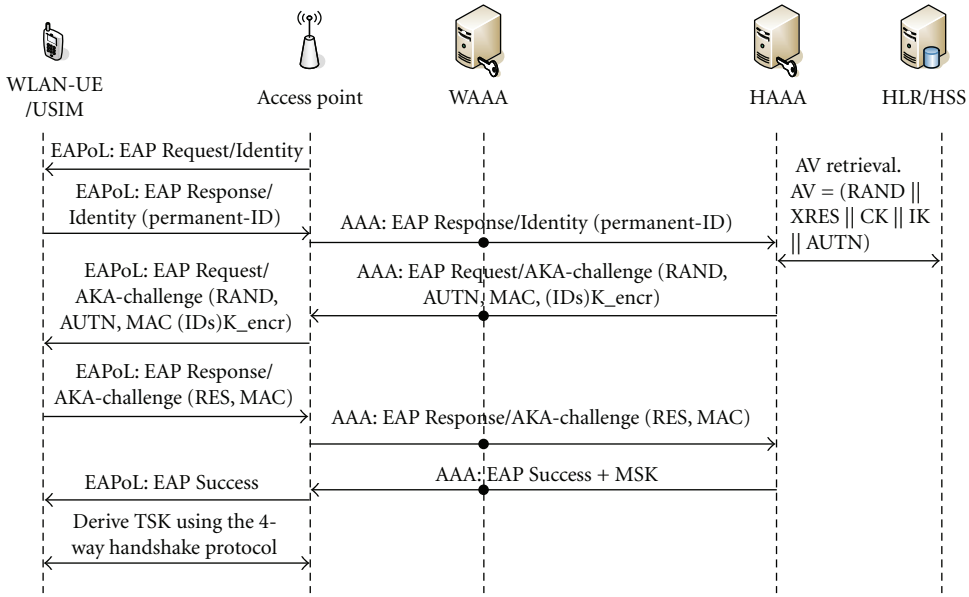


Figure 2: EAP-AKA authentication protocol.

HAAA exchange series of EAP messages to request/respond authentication information. HAAA communicates with the HSS to obtain Authentication Vectors (AVs) as shown in Figure 2. The UMTS Subscriber Identity Module (USIM) application on the UE and the HSS execute special message authentication and key generation functions known as "f1–f5" functions [12] to generate AVs. On successful mutual authentication, the UE and HAAA derive important security keys like the Master Session Key (MSK), Extended MSK (EMSK), and Transient EAP Key (TEK) [11]. The integrity and confidentiality of EAP messages are protected by K_auth and K_encr keys derived from TEK. The UE and its associated WLAN Access Point (AP) use MSK to derive a new session key, the Transient Session Key (TSK), which is later used to secure communications between them. TSK is derived from MSK using the 4-way handshake protocol introduced in IEEE 802.11i [13]. Due to the need to retrieve authentication information from authentication servers in the UHN, EAP-AKA authentication protocol is prone to high authentication delays and introduces redundant signaling traffic between the WLAN network and the UHN.

Generally, handover delay caused by roaming between and within WLANs is composed of delays like AP scanning delays [14], authentication delays, and MIP registration delays in the case of L3 handover. Several proposals reported in the literature focused on minimizing authentication delays during HH in autonomous WLAN networks [15–20]. However, the problem of reducing authentication

delays during HH when the UE operates in UMTS-WLAN interworking architecture remains mostly unexplored. In such architecture, authentication delay largely contributes to the overall handover delay because the UE needs to communicate with the UHN to successfully complete the authentication procedure. In practice, the UHN could be far away from the UE and separated by multiple networks and proxy AAA servers, resulting in high authentication and handover delays. Due to these reasons, invoking EAP-AKA protocol whenever WLAN HH takes place in UMTS-WLAN interworking architecture is unfavorable.

In our preliminary work, we have proposed two protocols to reduce authentication delays during WLAN HH in UMTS-WLAN interworking architecture. The proposed protocols were immature and initial and limited performance and security discussion were presented [21]. In this paper, we present improvements to the protocols and conduct extensive and thorough performance and security analysis on them. The comprehensive performance analysis considers important metrics like authentication signaling cost, authentication delay, and resource optimization of critical nodes involved in the authentication procedure. The thorough security analysis employs widely-accepted formal security verification tools to confirm that our protocols can withstand all forms of authentication and key secrecy attacks. In comparison with EAP-AKA protocol, our protocols achieve outstanding performance while preserving adequate security. The rest of this paper is organized as follows. In Section 2 we report some related works. In Section 3 we give detailed descriptions of our proposed protocols. In Section 4 we evaluate the performance of our protocols. In Section 5 we analyze the security of our proposed protocols. In Section 6 we present some conclusions.

2. Related Work

Research to reduce authentication delay during HH in WLANs in the context of UMTS-WLAN interworking architecture is in its initial stages. 3GPP did not specify protocols specific to UMTS-WLAN interworking to support WLAN HH. Thus, EAP-AKA protocol is invoked whenever HH takes place. On the other hand, many research studies are focusing on WLAN HH in autonomous WLANs architecture. In terms of network architecture, a major difference between authenticating a roaming UE in autonomous WLANs architecture in contrast to UMTS-WLAN interworking architecture is that authentication servers reside in the WLAN network in the former case and they reside in the UHN in the latter case. Another difference is that IEEE recommends invoking EAP-TLS protocols in autonomous WLANs, while 3GPP recommends invoking EAP-AKA authentication protocols in UMTS-WLAN interworking architecture. Therefore, existing HH authentication protocols designed specifically for autonomous WLANs architecture are not directly applicable over the UMTS-WLAN interworking architecture. Besides, several HH authentication protocols proposed for WLANs attain reduction in authentication delay at the cost of operational and security problems like introducing extra signaling overhead in the WLAN network [15–17] or demonstrating high dependency on UE mobility patterns [18, 19].

The rudimentary handover and security support in the base IEEE 802.11 protocol [22] has been enhanced in IEEE802.11i [13], IEEE802.11f [23], and IEEE802.11r [24]. Handover protocols in IEEE802.11i are optional and have seen limited implementation and deployment support [25]. Handover protocols in IEEE802.11f are not suitable for UMTS-WLAN interworking environments because strong trust agreements are required between WLAN administration domains for secure inter-Extended Service Set (inter-ESS) HH across these WLAN domains. On the other hand, IEEE802.11r supports only intra-ESS HH within specific WLAN domain but not inter-ESS HH.

Many papers in the literature proposed mechanisms to reduce intra- or inter-ESS HH delays in autonomous WLAN architecture. Some papers achieved this goal by preauthenticating the UE before handover, predistributing security keys, predicting UE's next move, introducing public key cryptography, or adopting hybrid techniques combining more than one method. Mishra et al. [15], Kassab et al. [16], and Hur et al. [17] proposed proactive key distribution using neighbor graphs to predict potential Target AP (TAP). These schemes utilize EAP-TLS and may result in unnecessary distribution of keys and increase signaling overhead in the WLAN as the number of UEs increases. Pack and Choi [18] and Mukherjee et al. [19] proposed mechanisms to predict UE mobility and hence preauthenticating the UE with the TAP before handover. The protocols share similar drawbacks as in [15–17] and their operations are restricted to intra-ESS HH. In the context of UMTS-WLAN interworking architecture, the UE roams between WLANs belonging to different administration and security domains, which imply that protocols designed to work in autonomous WLAN architectures like in [15–19] cannot be simply migrated to operate in the UMTS-WLAN interworking architecture.

Techniques to reduce delays in the event of WLAN HH in UMTS-WLAN interworking architecture have been proposed in [20, 26, 27]. Long et al. [20] proposed localized UE authentication for inter-ESS HH, in an architecture similar in concept to the UMTS-WLAN interworking architecture. The proposed mechanism requires that the UE should be authenticated by its home network while roaming. This protocol achieves fast inter-ESS HH by means of public key cryptography. Lee et al. [26] proposed a location-aware handover protocol. Location-aware service brokers are introduced in the interworking architecture to predict UE movement and perform fast authentication during handover. This scheme aims at offloading the 3G AAA servers from handling authentication whenever the UE moves, thus reducing authentication and handover delays. The drawback of this approach is that it requires major modifications to the existing 3G-WLAN interworking architecture. Lim et al. [27] proposed a protocol to reduce probing/scanning delays of the target AP. The downside to this solution is that APs must perform some of the functionalities of UMTS base station and share some control channels with it.

In comparison with protocols in [4–6, 15–20, 26, 27], our proposed protocols enjoy unique characteristics which make them first in their kind. Firstly, they are designed to operate in the 3GPP-specified UMTS-WLAN interworking architecture and adopt a variation of EAP-AKA protocols according to 3GPP recommendations unlike [4–6, 15–17]. Secondly, they are independent of UE movement pattern or TAP predictions contrasting protocols in [18, 19, 26]. Thirdly, they do not rely on public key cryptography like protocols in [4–6, 15–17, 20], which might require substantial processing resources that may not be available in mobile UEs. Fourthly, they do not require major modifications to APs or the introduction of new servers in the UMTS-WLAN interworking architecture as the case in [26, 27]. Finally they avoid unnecessary generation and pre-distribution of keys to TAPs and are therefore more efficient and secure.

3. Proposed Protocols

Novel pre-authentication protocols are proposed to improve intra- and inter-ESS WLAN HH when operating in a UMTS-WLAN interworking architecture. Intra- and Inter-WLAN ESS Fast Pre-authentication protocols (Intra/Inter-WLAN FP) preauthenticate the UE locally before handover takes place which results in reduction in the handover delay. To realize our proposed protocols, simple modifications are required to the standard EAP-AKA authentication protocol.

3.1. Assumptions. Firstly, some general assumptions are outlined which are similar in part to the assumptions made by 3GPP for authenticating a UE in UMTS-WLAN Interworking architecture [3].

(i) A WLAN AAA (WAAA) server exists in every WLAN. WAAA controls multiple APs forming a "WLAN domain." The WAAA and all APs in its domain must share a Long Term Security Association (LTSA).

(ii) WAAAs belonging to different WLAN domains must have LTSA and roaming agreements with the HAAA in the UHN.

(iii) WAAA and UE must maintain a WLAN counter (WC) which indicates the number of times pre-authentications has been performed. They are incremented by both corresponding nodes after every successful pre-authentication.

(iv) The HAAA or WAAA must supply a new UE local identity to the UE during authentication session to be used in future pre-authentications.

3.2. Modifications to EAP-AKA Protocol. In the standard EAP-AKA protocol, the UE and the HAAA must generate MSK and EMSK after a successful authentication [3, 11]. MSK is transported to the AP to be used in generating a TSK. EMSK is generated but its usage is not yet specified. We propose using EMSK to derive additional keys to achieve faster pre-authentication without compromising security. We extended the key hierarchy in EAP-AKA protocol by introducing WLAN domain-level and local-level keys derived from MSK and EMSK. 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 TSKs.

MSK is used to derive additional keys to speed UE's reauthentication operations only, that is, without handover. Usage of MSK to speed reauthentication operation in UMTS-WLAN interworking is described in [28]. We propose using EMSK as the root key for handover pre-authentications. The keys derived from EMSK are the Handover Root Key (HOK), the Domain-level Handover key (DHOK) and the Local-level handover key (LHOK). LHOK is ultimately used to derive TSK in Intra- and Inter-WLAN FP. To derive the required additional keys we suggest the following modifications to EAP-AKA authentication protocol as depicted in Figure 3.

(i) The HAAA generates the next local ID, $\mathrm{ID}_{\mathrm{WLAN}}$, to be used by the UE in the next pre-authentication and a nonce value (HN). The HAAA should indicates the permitted number of pre-authentications (n_{pre}) the UE can perform before falling back to standard EAP-AKA authentication. The WAAA and UE adjust the maximum value WC can reach according to n_{pre}. In addition, the UE generates a nonce, UN.

(ii) Five new keys are generated.

(a) Root handover key, HOK. This key is derived from EMSK by the HAAA and the UE only. Both nodes use a special Pseudorandom Function (PRF) similar to the one used in generating MSK in the standard EAP-AKA protocol [11]

$$\mathrm{HOK} = \mathrm{PRF}(\mathrm{EMSK}, \text{EAP-AKA session ID} \mid \text{HAAA ID} \mid \mathrm{UEM}, 256), \tag{1}$$

where "|" denotes concatenation and,

$$\text{EAP-AKA session ID} = (\text{EAP Type Code}|\mathrm{RAND}|\mathrm{AUTN}) \tag{2}$$

see, [29].
UEM is the UE address in the medium access control layer. HAAA ID is the identity of the HAAA server.

(b) The domain-level handover key, DHOK. It is derived from HOK by HAAA and UE only

$$\mathrm{DHOK} = \mathrm{PRF}(\mathrm{HOK}, \mathrm{HN} \mid \text{WAAA ID} \mid \mathrm{UEM}, 256), \tag{3}$$

where WAAA ID is the identity of the WAAA.

(c) The domain-level and local-level reauthentication keys, DRK and LRK. Their derivation and usage are detailed in [28].

(d) A key used to secure traffic between the UE and WAAA, $\mathrm{K}_{\mathrm{WAAA\text{-}UE}}$. This key is only derived by the UE and WAAA

$$\mathrm{K}_{\mathrm{WAAA\text{-}UE}} = \mathrm{PRF}(\mathrm{DHOK} \oplus \mathrm{DRK} \mid \text{WAAA ID} \mid \mathrm{UEM}, 256). \tag{4}$$

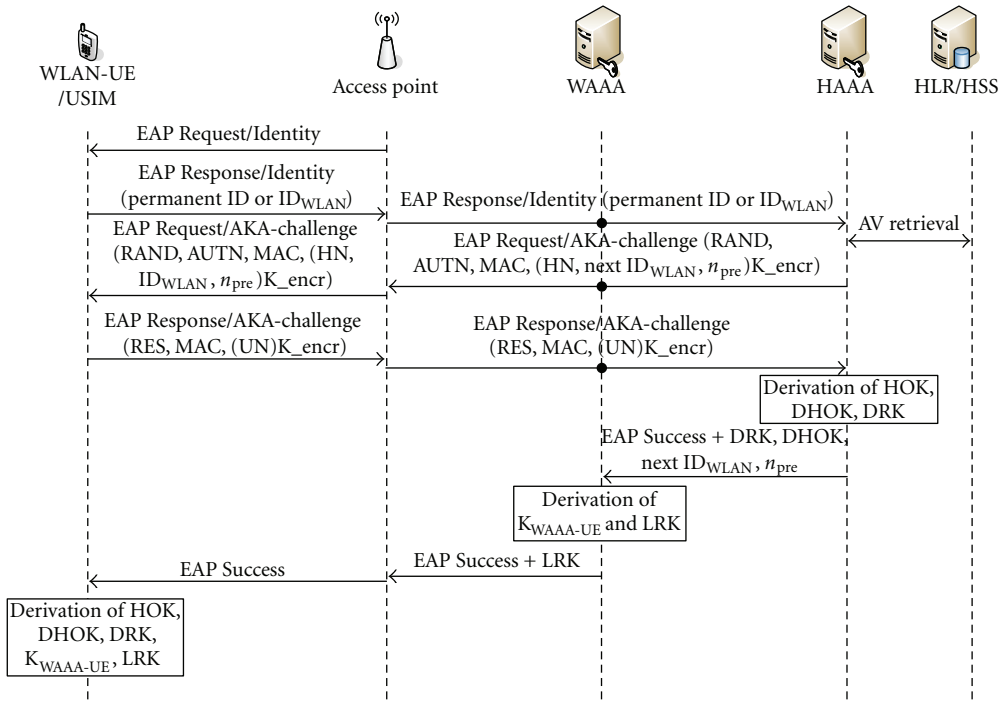


Figure 3: Modified EAP-AKA authentication protocol.

(iii) Secure delivery of DRK, DHOK, n_{pre} and ID_{WLAN} by the HAAA to the WAAA.

(iv) Secure delivery of LRK by the WAAA to the AP.

(v) Derivation of HOK, DHOK, DRK, LRK, and $K_{WAAA\text{-}UE}$ by the UE.

3.3. Intra/Inter-WLAN Fast Pre-authentication. A UE roams to a neighbor AP when experiencing poor signal-strength from the currently associated AP. The Target AP (TAP) might be in the same WLAN domain or belong to a different WLAN domain. Due to the lack of WLAN HH authentication protocol support by 3GPP in UMTS-WLAN interworking architecture and inadaptability of autonomous WLAN HH authentication protocols, we designed Intra- and Inter-WLAN Fast Pre-authentication protocols (Intra/Inter-WLAN FP) to minimize authentication delay and signaling overhead during intra- and inter-ESS HH. The proposed protocols utilize EAP-AKA messages and can efficiently operate in the UMTS-WLAN interworking architecture. Intra-WLAN FP is locally executed when the currently associated AP and the TAP reside in the same WLAN domain. Inter-WLAN FP is executed when the currently associated AP and the TAP reside in different WLAN domains. Intra/Inter-WLAN FP minimizes the dependency on HSS and HAAA to authenticate the UE which results in improved performance without compromising security.

The UE needs to supply target AP and target WAAA identities it requires to handover to, TAP ID and TWAAA ID. Therefore we propose adjusting IEEE 802.11 *Probe Response* management frames transmitted by the TAP to include its identity and the identity of WAAA it is associated with as Information Elements (IEs). Element IDs 7–15 and 32–255 are reserved for future use and can be used for this purpose [22]. Handover related decisions like handover triggers and best TAP selection is out of the scope of the paper. Figure 4 depicts Intra-WLAN FP operation.

In Intra-WLAN FP, the WAAA handles UE authentication instead of the HSS and HAAA. Intra-WLAN FP protocol proceeds as follows.

(1) When the UE recognizes the need for handover, it sends an *EAPoL-start* message to the currently associated AP, not shown in Figure 4. The AP replies with an identity request message.

(2) UE responds to the request with ID_{WLAN}, TWAAA ID and TAP ID.

(3) Receiving TWAAA ID and TAP ID indicates a handover pre-authentication request. The WAAA classifies this request as an 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 ID_{WLAN} as well as WC and $MAC1_{Intra}$ calculated using $K_{WAAA\text{-}UE}$,

$$MAC1_{Intra} = \text{SHA-1}(K_{WAAA\text{-}UE}, WC \mid ID_{WLAN} \mid WN), \quad (5)$$

where SHA-1 is the Secure Hash Algorithm.

(4) In the UE's side, WC stored in the UE's database is matched with WC recently received. Then a new $MAC1_{Intra}$ is calculated and compared with the received $MAC1_{Intra}$. If both checks are positive,

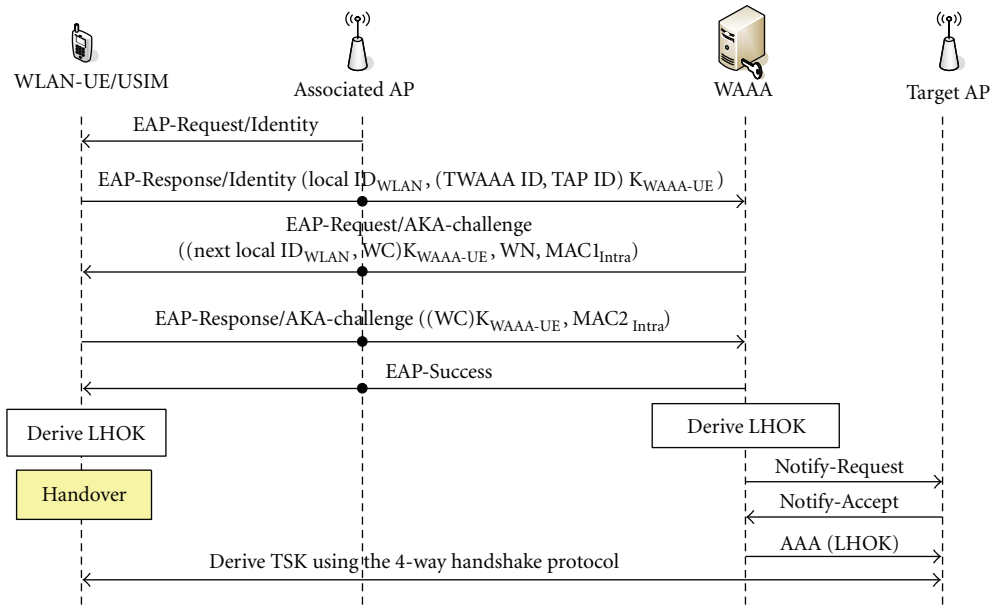


Figure 4: Intra-WLAN Fast Pre-authentication protocol.

the UE stores ID_{WLAN} and replies with WC and $MAC2_{Intra}$,

$$MAC2_{Intra} = \text{SHA-1}(K_{WAAA\text{-}UE}, WC \mid WN). \quad (6)$$

(5) The WAAA then derives a local-level handover key, LHOK, from DHOK as follows:

$$LHOK = PRF(DHOK, WC \mid TAP\ ID \mid UEM, 512). \quad (7)$$

The WAAA also increments WC and sends *EAP success* message to the UE. Consequently, the UE derives LHOK and increments WC. WAAA and TAP exchange *Notify-Request* and *Notify-Accept* RADIUS AAA message to confirm handover operation [30]. Finally LHOK is pushed to the TAP in *RADIUS Access-Accept* message with *MS-MPPE-Recv-Key* attribute [11].

In Inter-WLAN FP, authentication procedure is completed without the need to retrieve security keys from the HSS as shown in Figure 5. The protocol proceeds as follows:

(1) The UE replies to the identity request message with ID_{WLAN}, TWAAA ID, and TAP ID.

(2) The handover pre-authentication request is classified as Inter-WLAN by the WAAA if the TWAAA ID does not match its identity and TAP ID does not match any of the AP identities in the WLAN domain. The WAAA retrieves the UE permanent ID and forwards it along with the TAP ID and TWAAA ID to the HAAA.

(3) Upon receiving the IDs, the HAAA recognize that an Inter-WLAN FP is requested and prepares an authentication challenge. The challenge includes the next ID_{WLAN}, UN, newly generated HN and $MAC1_{Inter}$

$$MAC1_{Inter} = \text{SHA1}(K\_\text{auth}, UN \mid ID_{WLAN} \mid \text{new HN}). \quad (8)$$

UN was previously received by the HAAA in the modified EAP-AKA protocol.

(4) Upon receiving the authentication challenge, the UE checks UN, calculates a new $MAC1_{Inter}$ and compares it with the received $MAC1_{Inter}$. If all verification returns positive, ID_{WLAN} is stored and a reply message is prepared. The reply message includes the new HN, newly generated UN, WC, and $MAC2_{Inter}$,

$$MAC2_{Inter} = \text{SHA-1}(K\_\text{auth}, \text{new UN} \mid \text{new HN} \mid \text{last HN} \mid WC). \quad (9)$$

(5) Upon receiving the message, the HAAA consults WC to verify that pre-authentication limit is not exceeded and verifies $MAC2_{Inter}$. If all verifications are successful, the HAAA validates HOK lifetime, generates a new DHOK and DRK and *EAP Success* message is sent to the UE.

(6) Upon receiving *EAP success* message, the UE derives a new DHOK, DRK, $K_{TWAAA\text{-}UE}$, and LHOK. It also increments WC.

(7) AAA message that includes DHOK, DRK, WC, n_{pre}, UE permanent ID, ID_{WLAN}, and TAP ID is sent to the TWAAA by the HAAA. As a result, $K_{TWAAA\text{-}UE}$ and LHOK are generated and WC is incremented by TWAAA. Lastly, TWAAA confirms handover with TAP by exchanging RADIUS AAA *Notify-Request* and *Notify-Accept* message and forwards LHOK in *Access-Accept* message.

At the conclusion of a successful Intra- or Inter-WLAN FP, a fresh LHOK is held by the UE and the TAP. The LHOK is used to generate TSK, which is then used to

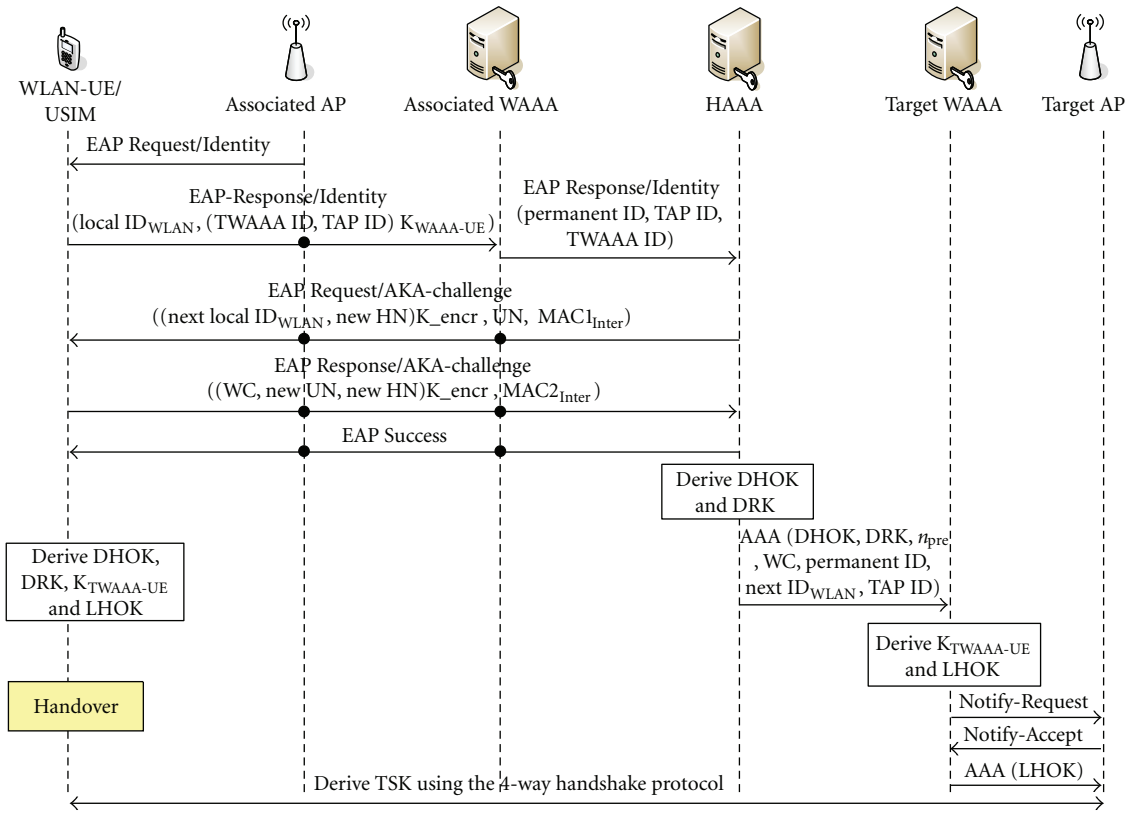


Figure 5: Inter-WLAN fast pre-authentication protocol.

derive additional keys that are needed to secure the link between the UE and the TAP. EAP-AKA highly depends on IEEE802.1X [31] protocol implemented in the AP to successfully control UE's network access. IEEE802.1X is a port-based access control protocol. When an EAP session completes successfully between the UE and the AP, normal communications is permitted by the latter to pass through an authorized port. Therefore, simultaneous exchange of normal communications and EAP session is disallowed. We propose two classes of Intra/Inter-WLAN FP execution depending on the implementation of IEEE802.1X protocol in the AP. The two classes differ on whether IEEE802.1X protocol in the AP permits single or multiport communications. Based on this, each class imposes different effect on the authentication delay. Single-port communication implies that normal communications between the UE and the AP is disallowed when EAP session is executed. Multiport communications implie that the AP can still handle normal communications while processing EAP messages. Multiport communications are achievable by simple modifications to the IEEE802.1X protocol in the AP. In studying the performance of our proposed protocols, both single-port and multiport communications are considered.

4. Performance Evaluation

In this section we evaluate the performance of our proposed pre-authentication protocols against EAP-AKA protocol. Performance evaluation against protocols in the literature like [15–19] is not reasonable because of the difference in the network architecture. We considered three performance metrics in our study, they are authentication signaling cost, authentication delay, and the load on critical nodes in the UMTS-WLAN interworking architecture.

4.1. UE Movement and Authentication Scenarios. Performance evaluations are studied based on a fixed path UE movement. This movement might not reflect realistic UE paths but it is considered here for performance evaluation purposes only. Initially, the UE is connected to AP1 in WLAN1 as depicted in Figure 6. The UE then performs two intra-ESS HH to APs 2 and 3 in WLAN1, respectively. Later, it performs an inter-ESS HH to AP1 in WLAN2 followed by two intra-ESS HH to AP2 and AP3 in WLAN2, respectively.

Three authentication scenarios are considered in the performance study.

Scenario 1 (Sc1). This scenario adopts authentication protocols specified by 3GPP [3]. The UE performs EAP-AKA authentication whenever it starts communicating with an AP regardless whether HH was performed or not.

Scenario 2 (Sc2). This scenario executes our proposed modifications to EAP-AKA protocols and Intra/Inter-WLAN FP protocols. The IEEE802.1X protocol in the APs in this scenario supports single-port communications.

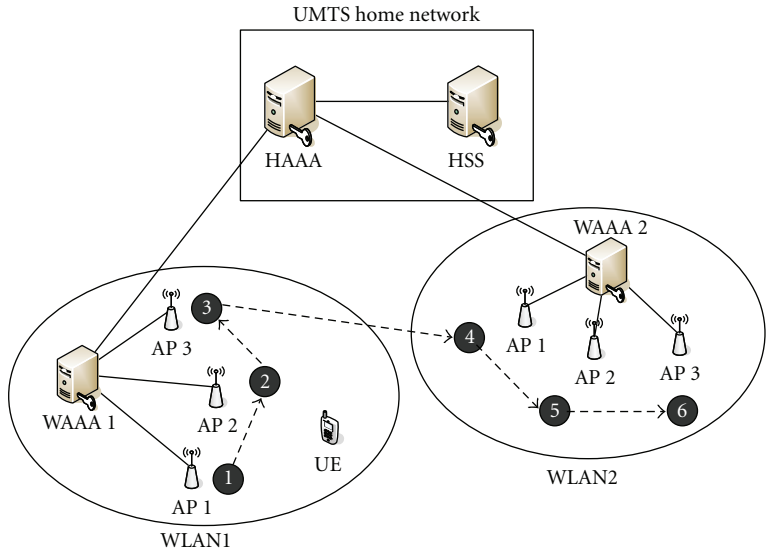


Figure 6: UE movement.

Scenario 3 (Sc3). This scenario is identical to Sc2 in terms of message signaling, however, IEEE802.1X protocol in the APs supports multiport communications. Therefore, the UE and APs are capable of handling normal communications while processing EAP messages for pre-authentication purposes.

Our proposed pre-authentication protocols represented by Sc2 and Sc3 are expected to show similar results in terms of authentication, signaling cost, and the load on critical nodes, however, authentication delay experienced by these scenarios should distinctly differ. Authentication protocols invoked in Sc2 and Sc3 depend on the number of permitted pre-authentications (n_{pre}). For example, setting n_{pre} to 1, 3, and 5 mean that our modified EAP-AKA protocol is going to be invoked thrice, twice, and once, respectively. The value of n_{pre} should be carefully chosen by the service provider; very high value might negatively affect security because of frequent reuse of HOK and DHOK while very low values might negatively affect performance due to contacting UHN repeatedly for authentication. Figure 7 depicts the authentication protocols in Sc1 and Sc2 when $n_{\text{pre}} = 5$.

4.2. Authentication Signaling Cost. Studying the signaling cost produced by an authentication protocol is an important metric in evaluating its performance. Authentication signaling cost is the accumulative traffic load introduced in the network by exchanging authentication signaling during a communication session [32]. For simplicity, all nodes are a single hop (H) apart except between WAAA and HAAA. The authentication signaling cost (C) for the authentication scenarios when $n_{\text{pre}} = 5$ are calculated as follows:

$$\begin{aligned} C_{\text{Sc1}} &= \left(6\ M_{\text{EAP-AKA(stnd)}}\right) \times S \times Nm, \\ C_{\text{Sc2}} &= C_{\text{Sc3}} = \left(M_{\text{EAP-AKA(}\ \text{mod}\ \text{)}} + 4\ M_{\text{Intra}} + M_{\text{Inter}}\right) \times S \times Nm, \end{aligned} \tag{10}$$

where (M) is the number of messages exchanged in each authentication protocol, S is the average message size, it is set to 100 bytes. Nm is the average number of UE movements during a session, $Nm = Ts/Tr$. Ts is the average session time, it is set to 1000 seconds. Tr is the average WLAN resident time, it varies from 10 to 40 seconds. Figure 8 shows the authentication signaling cost against UE resident time when $H_{\text{WAAA-HAAA}} = 3$ for different n_{pre} values.

Generally the higher the UE resident time the less authentication signaling is generated. It is clear from the figure that the authentication signaling cost of Sc2 is less than Sc1. Our proposal reduces signaling cost by 13% when compared to Sc1 when $n_{\text{pre}} = 1$. Improved performance results are achieved when increasing n_{pre} value. Reduction in signaling cost experienced in Sc2 reaches up to 21% and 29% in comparison to Sc1 when setting n_{pre} values to 3 and 5, respectively. As discussed earlier, Sc1 experience the same signaling cost in spite of n_{pre} value. Increasing n_{pre} value means reducing the frequency of invoking the modified EAP-AKA protocol and permitting additional local pre-authentications without the need to contact UHN hence achieving drastic reduction in authentication signaling cost.

4.3. Authentication Delay. Authentication delay plays an important factor in the overall handover delay. In this paper we assume that delays that constitute handover delay, other than authentication delay, like AP scanning delay and MIP registration delay have an equal effect on all authentication scenarios. Authentication delay is calculated starting from sending *EAP Request/Identity* message and ends by invoking the 4-way handshake protocol. Generally, the delay between two nodes, A and B is defined as follows:

$$\begin{aligned} T_{\text{A-B}} = {} & M_{\text{A-B(wl)}}\left(D_{\text{trans(wl)}} + 2D_{\text{proc}}\right) \\ & + M_{\text{A-B(wi)}} H_{\text{A-B}}\left(D_{\text{trans(wi)}} + 2D_{\text{proc}}\right), \end{aligned} \tag{11}$$

where $M_{\text{A-B(wl/wi)}}$ signifies the number of messages exchanged between nodes A and B in the wireless network and

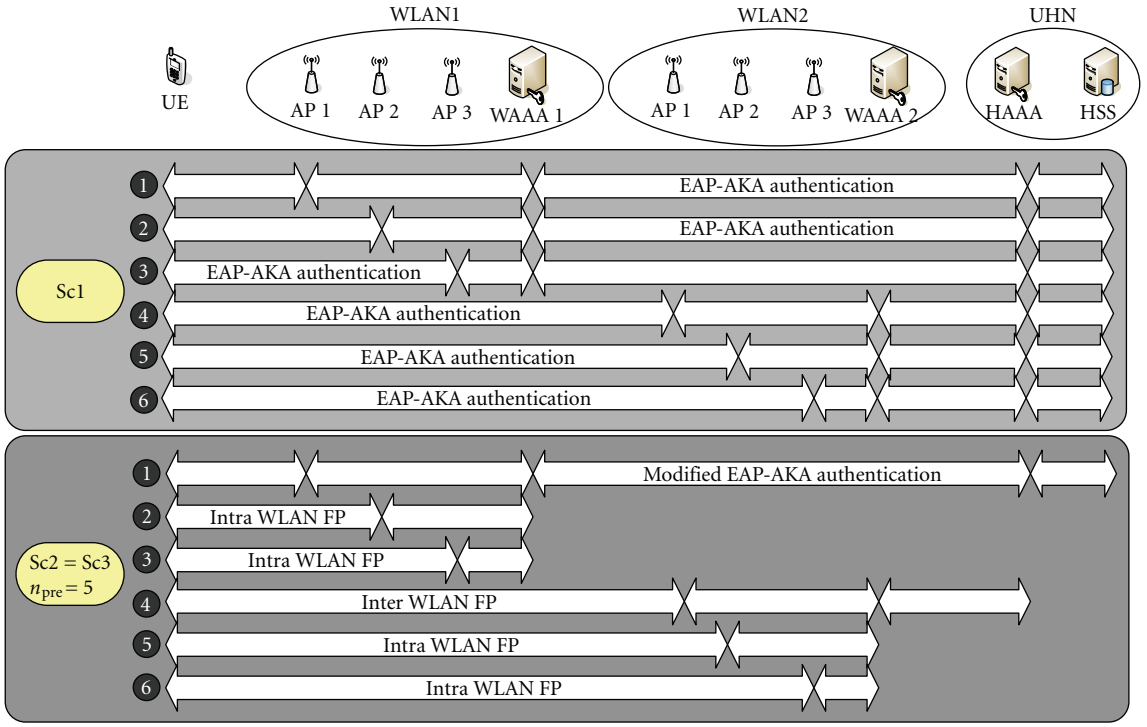


FIGURE 7: Authentication scenarios when $n_{pre} = 5$.

wired network, respectively, $H_{A\text{-}B}$ are the number of hops separating A and B in the wired network, $D_{trans(wl/wi)}$ are the transmission delay that includes propagation and routing delay in the wireless and wired networks, respectively. $D_{trans(wl)}$ is set to 2 milliseconds while $D_{trans(wi)}$ is set to 0.5 milliseconds. D_{proc} is the nodal processing delay which includes queuing delay, it is set to 0.001 milliseconds. All parameter values used in the study are taken from [32]. From (11), authentication delay (T) of each authentication protocol is calculated. The authentication delay in the standard and modified EAP-AKA when $n_{pre} = 5$ is given by

$$\begin{aligned} T_{\text{EAP-AKA(stnd)}} &= T_{\text{EAP-AKA(mod)}} \\ &= \left(5D_{\text{trans-wl}} + 10D_{\text{proc}}\right) + \left(4D_{\text{trans-wi}} + 8D_{\text{proc}}\right) \\ &\quad + \left(12D_{\text{trans-wi}} + 24D_{\text{proc}}\right) + \left(2D_{\text{trans-wi}} + 4D_{\text{proc}}\right) \\ &\quad + 2D_{\text{AV}} + D_4. \end{aligned} \tag{12}$$

The authentication delay for Intra/Inter-WLAN FP in Sc2 and Sc3, is given by

$$\begin{aligned} T_{\text{Intra-Sc2}} &= \left(5D_{\text{trans-wl}} + 10D_{\text{proc}}\right) \\ &\quad + \left(7D_{\text{trans-wi}} + 14D_{\text{proc}}\right) + D_4, \end{aligned}$$

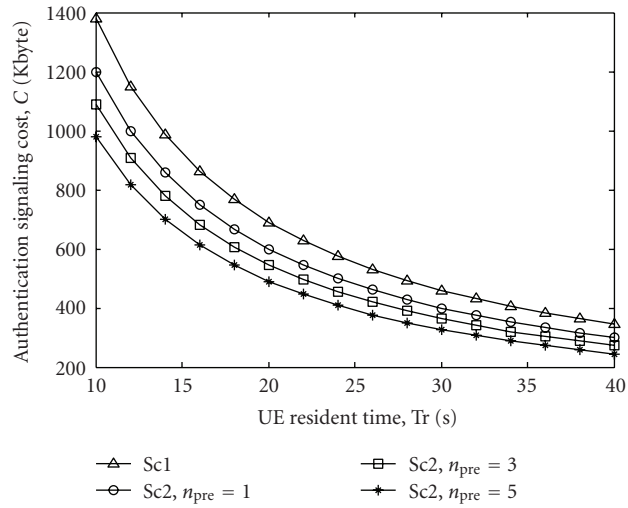


FIGURE 8: Authentication signaling cost for Sc1 and Sc2 for different n_{pre} values.

$$\begin{aligned} T_{\text{Inter-Sc2}} &= \left(5D_{\text{trans-wl}} + 10D_{\text{proc}}\right) + \left(7D_{\text{trans-wi}} + 14D_{\text{proc}}\right) \\ &\quad + \left(15D_{\text{trans-wi}} + 30D_{\text{proc}}\right) + D_4, \\ T_{\text{Intra-Sc3}} &= 3D_{\text{trans-wi}} + 6D_{\text{proc}} + D_4, \\ T_{\text{Inter-Sc3}} &= 6D_{\text{trans-wi}} + 12D_{\text{proc}} + D_4. \end{aligned} \tag{13}$$

D_4 denotes the delay incurred by executing the 4-way handshake protocol, it is set to 20 milliseconds. Note that

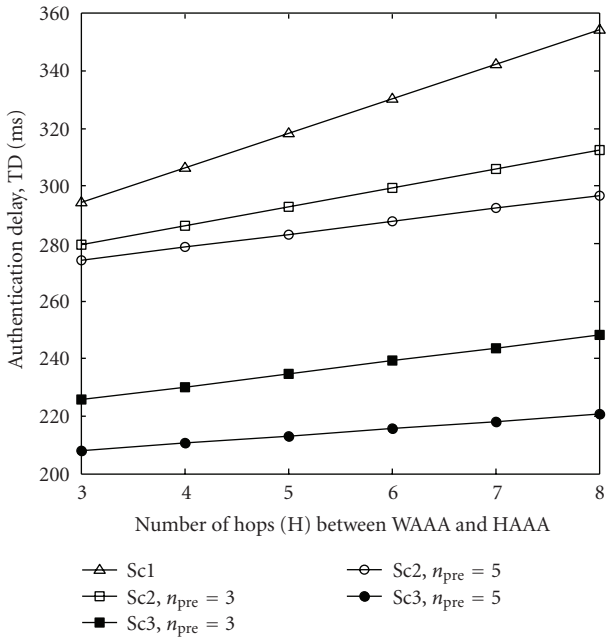


Figure 9: Authentication delay in Sc1, Sc2, and Sc3 when varying $H_{\text{WAAA-HAAA}}$.

Table 1: Number of keys generated in the three authentication scenarios.

	Sc1	Sc2 = Sc3		
n_{pre}	—	1	3	5
UE	36	39	29	19
WAAA1	0	5	4	4
WAAA2	0	5	5	4
HAAA	24	23	16	9
HSS	12	6	4	2
Total: all nodes	72	78	58	38
Total: critical nodes	72	68	49	30
Total key size in UE (byte)	1272	1500	1160	820

D_{AV} is the processing delay of generating AVs using "f1–f5" functions in the HSS and USIM, it is set to 0.001 milliseconds. The processing delays incurred by generating new keys in our proposed protocols by WAAA are expressed as a normal processing delay (D_{proc}). This is because WAAAs are usually equipped with high processing capabilities and control far less number of UEs compared to HSS and HAAA. Although our proposed protocols in Sc2 and Sc3 undergo similar authentication signaling cost, they differ distinctly in the authentication delay. The total authentication delay (TD) for each scenario when $n_{\text{pre}} = 5$ is calculated as follows:

$$\begin{aligned} \text{TD}_{\text{Sc1}} &= 6T_{\text{EAP-AKA(stnd)}}, \\ \text{TD}_{\text{Sc2}} &= T_{\text{EAP-AKA(mod)}} + 4\,T_{\text{Intra-Sc2}} + T_{\text{Inter-Sc2}}, \\ \text{TD}_{\text{Sc3}} &= T_{\text{EAP-AKA(mod)}} + 4\,T_{\text{Intra-Sc3}} + T_{\text{Inter-Sc3}}. \end{aligned} \quad (14)$$

By varying $H_{\text{WAAA-HAAA}}$ and n_{pre} values, we can compare the authentication delays of the three scenarios. Figure 9 shows the authentication delay of each scenario for different n_{pre} values. Our protocols represented by Sc2 and Sc3 outperform standard authentication protocol. When $n_{\text{pre}} = 1$, authentication delay in Sc2 is slightly less than Sc1 due to multiple execution of the modified EAP-AKA authentication which is a delay intensive operation. However, since Sc3 takes advantage of the multiport communications in the AP, it experiences much less delay reduction comparing to Sc1. Our proposed protocols demonstrate exceptional results when increasing n_{pre} value as shown in Figure 9. When $n_{\text{pre}} = 3$ and $H_{\text{WAAA-HAAA}} = 8$, delay reduction in Sc2 and Sc3 reaches up to 12% and 30%, respectively, compared to Sc1.

When $n_{\text{pre}} = 5$, our protocols capitalize on the single execution of the modified EAP-AKA protocol to perform several pre-authentications without the need to involve HSS and HAAA in the authentication procedure which ultimately reduces authentication signaling cost and authentication delay. In such settings, authentication delay reduction in Sc2 and Sc3 reaches up to 16% and 38% comparing to Sc1. Increasing n_{pre} value reflects in more reductions in the authentication delay in our proposed protocols comparing to the standard protocol. This feature illustrates the superiority and suitability of our proposed protocols to sustain quality of service of delay-sensitive applications running on the UE.

4.4. Load on Critical Nodes. In UMTS-WLAN interworking architecture, critical nodes involved in the authentication procedure are HSS, HAAA, and the UE. HSS and HAAA are considered critical because they handle the authentication of hundreds of thousands of UEs. The UE is considered critical as well because of the limitation in its processing capabilities. In EAP-AKA, key generation and distribution schemes are included in the authentication procedure. In our proposed protocols, HSS and HAAA delegate the authentication responsibility to trusted WAAA. Therefore, the processing overhead on these critical nodes is reduced. Since our modifications to EAP-AKA introduced additional keys generated by UE, HAAA, and WAAA, a study on the effect of the additional keys was important. In our study we considered the number and memory sizes of keys introduced in each authentication protocol starting from CK and IK down the hierarchy to the key used in the 4-way handshake protocol, that is, MSK in Sc1 and LHOK/LRK in Sc2. Figure 10 illustrates the keys generated by each node during UE movement when $n_{\text{pre}} = 5$. Table 1 indicates the total number of keys generated by all nodes for different n_{pre} values.

As indicated by Table 1, the total number of keys generated by all nodes in Sc2 decreases as n_{pre} value increase. When $n_{\text{pre}} = 1$, Sc2 generates 6 more keys in total comparing to Sc1 due to frequent execution of the modified EAP-AKA protocol. As n_{pre} value increase, the frequency of executing the modified EAP-AKA protocol decreases and hence fewer keys are generated. When increasing n_{pre} to 5, the total number of keys generated by all nodes in Sc2 is almost half of that generated in Sc1. Critical nodes in Sc2 generate 4 keys less than Sc1 when n_{pre} is set to 1, Sc2 generates less than half the number of keys generated in Sc1 when n_{pre}

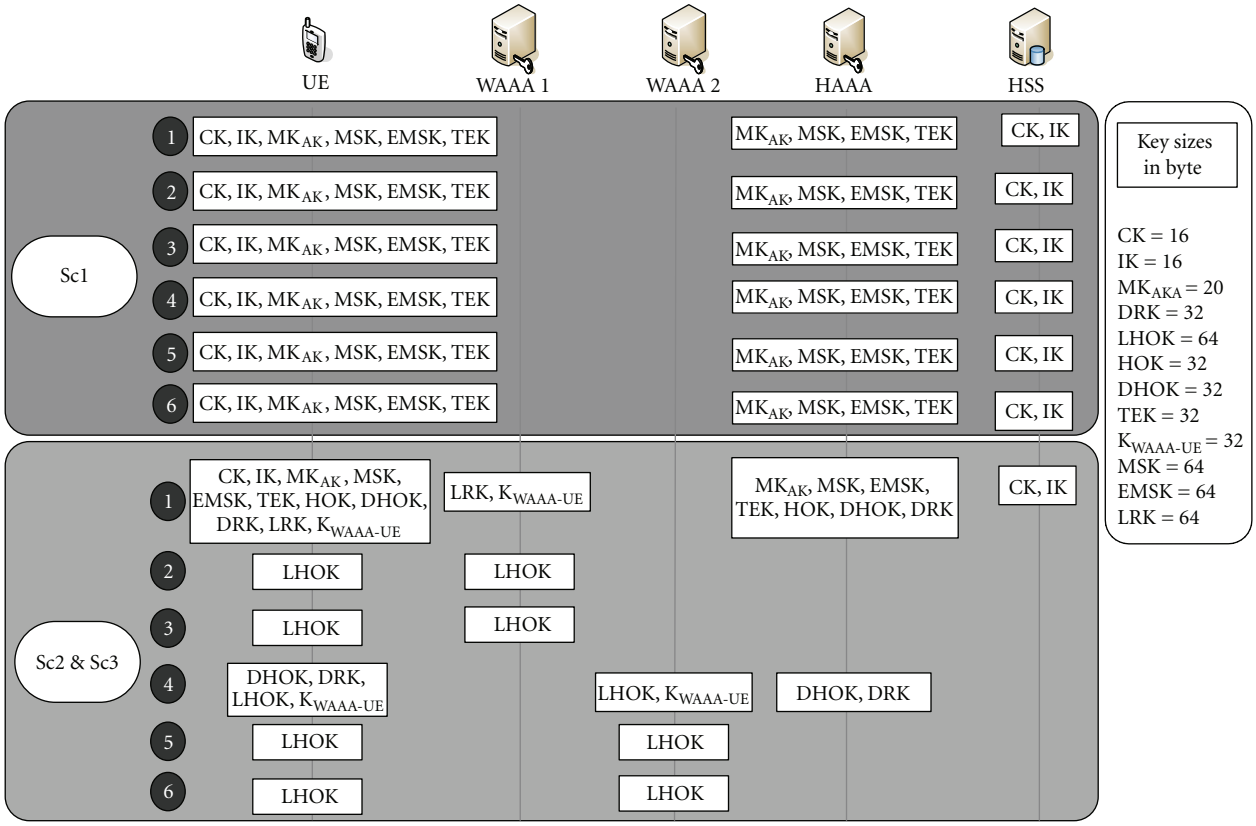


Figure 10: Keys generated by each node when $n_{pre} = 5$.

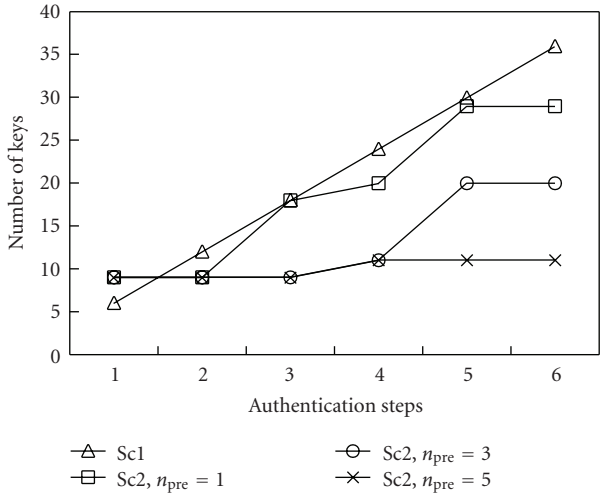


Figure 11: Number of keys generated by HSS and HAAA.

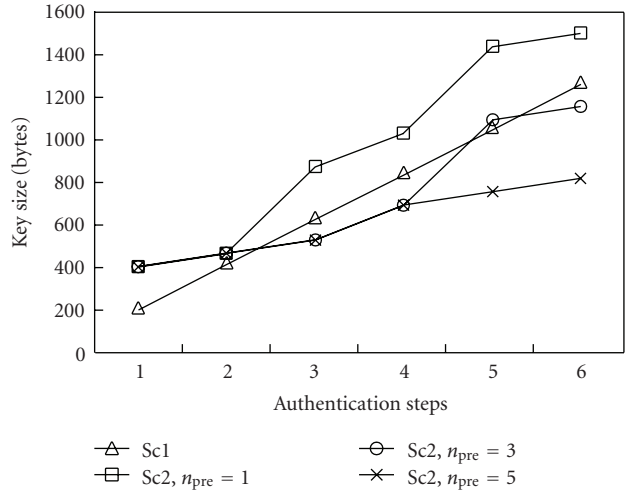


Figure 12: Memory storage space required by the UE to store security keys.

is set to 5. Critical nodes in Sc2 generate and maintain far less number of keys compared to their counterparts in Sc1 because the WAAA handle some of the key generation activity. The number of keys generated by critical nodes in addition to WAAA1 and WAAA2 in Sc2 is 58 and 38 when $n_{pre} = 3$ and $n_{pre} = 5$, respectively, which is clearly less than the number of keys generated by all nodes in Sc1.

From Table 1, the number of keys generated by HSS and HAAA in Sc1 is always greater than the number of keys generated by HSS and HAAA in Sc2. This is also illustrated in Figure 11. Number of keys generated by HSS and HAAA are 29, 20, and 11 when n_{pre} is set to 1, 3, and 5, respectively, compared to 36 keys generated in Sc1. This advantage is highly valued when more UEs roam to the network. For

```
role waaaserver
  (
    P, WAAA, AP1, AP2    : agent, % UE, WAAA server, Access Point 1 and 2
    F1, HMAC             : hash_func,   % MAC generation and key generation functions
    KPW, KAP1W, KAP2W, DHOK: symmetric_key,
    WCN, AP2_ID          : text,   % WLAN counter and AP2 ID
    SND_AP1W, RCV_AP1W, SND_AP2W, RCV_AP2W : channel (dy))
played_by WAAA def=
local
   WN, INTRA_ID        : text,   % WAAA nonce and UE ID
   WCNE                : {text}_symmetric_key,
   MAC1_INTRA, LHOK : hash (symmetric_key.text.text.text),
   MAC2_INTRA          : hash (symmetric_key.text.text),
   State               : nat
const
    request_id, respond_id, success : text,
    lhok3, wn1, wn2          : protocol_id
init State := 2
transition
1. State = 2 /\ RCV_AP1W (respond_id.INTRA_ID') = | >
    State' := 5 /\ WN' := new()     /\ WCNE' := WCN_KPW
                /\ MAC1_INTRA' := HMAC (KPW.INTRA_ID'.WN'.WCN)
                /\ SND_AP1W (WN'.MAC1_INTRA'.WCNE')
                /\ witness (WAAA, P, wn1, WN')   % for UE to authenticate WAAA
2. State = 5 /\ RCV_AP1W (WCNE'.MAC2_INTRA')
               /\ MAC2_INTRA' = HMAC (KPW.WN.WCN) = | >
    State' := 8 /\ LHOK' := F1 (DHOK.WCN.INTRA_ID.AP2_ID)
                /\ request (WAAA, P, wn2, WN) % for WAAA to authenticate UE
                /\ SND_AP1W (success) /\ SND_AP2W (success.{LHOK'}_KAP2W)
                /\ secret (LHOK', lhok3, {P, WAAA, AP2})
end role
```

Figure 13: HLPSL code describing WAAA's role in Intra-WLAN FP.

example, when 5 UEs exist in the network and followed the same movement indicated by Figure 6, HSS and HAAA end up generating 180 keys in Sc1 while only 55 keys are necessary in Sc2 when $n_{\text{pre}} = 5$. This shows that our proposed protocols are capable of managing large number of UEs in the interworking architecture efficiently comparing to standard EAP-AKA protocol.

Since the UE has limited processing capabilities and storage capacity, we evaluated the number of keys generated by it as well as the memory size required to store security keys. Continuing a similar trend, the UE generates less number of keys as the value of n_{pre} increases. Generally the number of keys generated by the UE in Sc2 is less than Sc1 when $n_{\text{pre}} > 2$. Furthermore, while the UE requires 1.272 Kbytes of storage space in Sc1, it needs 1.160 Kbytes and 820 bytes of storage space in Sc2 when n_{pre} is set to 3 and 5, respectively. Figure 12 illustrates the amount of storage space required by the UE. Since the modified EAP-AKA protocol is invoked thrice when $n_{\text{pre}} = 1$ in Sc2, more storage space to store the keys in the UE is anticipated.

5. Security Analysis

Performance improvements to authentication protocols should not compromise its security. In this section we analyze the security of the proposed protocols in terms of supporting secured key management scheme, mutual authentication service, protection of the integrity of exchanged messages, and protection of transmitted identities.

5.1. Secured Key Management. Keys must be held by the minimum number of nodes possible. Unnecessary distribution of keys must be avoided and keys must be unique to key holders. Additionally, keys must never be shared between nodes from the same hierarchal level and keys used directly in protecting communication messages must not be reused. These measures are collectively known as the principle of least privilege, which prevents the "domino effect" problem [33] in key management protocols. Our protocols are designed to abide by the principles of least privilege. For example, DHOK is only generated by the UE and HAAA because no other node has access to HOK and HN values used in the generation process. This key is only used by the UE and WAAA and never shared between different WAAA servers residing in different WLAN networks. Similarly, LHOK is only generated by the UE and WAAA because no other node has access to DHOK and WC values used in the generation process. LHOK is used by the UE and TAP only and is never shared between different TAPs and never reused in future pre-authentications. To emphasize the principle of least privilege, the HAAA must delete DHOK from its database after delivering it to the WAAA. Likewise, the WAAA must delete LHOK from its database after delivering it to the TAP.

Keys, nonces, and counters are securely transmitted to protect against eavesdropping attacks. No keys are transmitted in the WLAN link between the UE and AP. Sensitive security information traveling between the HAAA

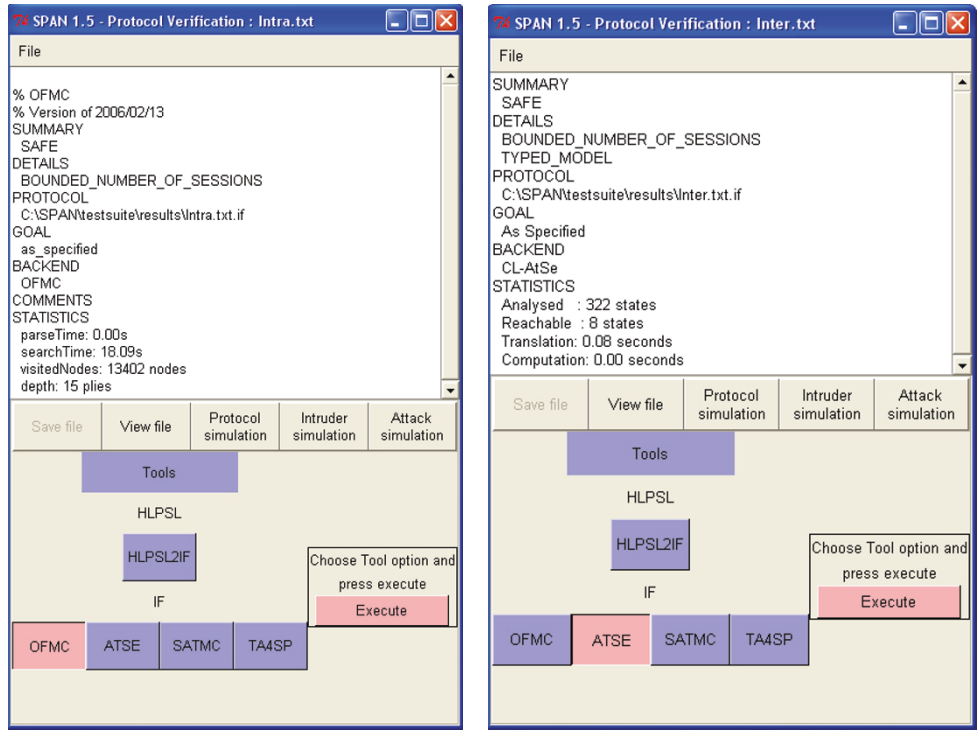
```
role peer (
  P, WAAA1, WAAA2, AP1, AP2, HAAA      : agent,  %UE, WAAA servers, APs and HAAA
    F1,HMAC                : hash_func,   %MAC generation and key generation functions
    KPH                    : symmetric_key,   % shared key between UE and HAAA
    HOK, MSK                 : symmetric_key,
    HN, UN                   : text,   % HAAA nonce and UE nonce
    WAAA2_ID, AP2_ID       : text,   % WAAA2 AND AP2 identities
    SND_AP1P, RCV_AP1P : channel (dy))
played_by P def=
local
    NUN, NHN, WCN, INTER_ID    : text,  % New UN, New HN, WLAN Counter, UE Identity
    WCNE                                : {text}_symmetric_key,
    MAC1_INTER, DHOK, LHOK              : hash (symmetric_key.text.text.text),
    MAC2_INTER                          : hash (symmetric_key.text.text.text.text),
    State                               : nat
const
    request_id, respond_id, success  : text,
    lhok1, nhn1, nhn2          : protocol_id
init State  := 1
transition
1. State = 1 /\ RCV_AP1P (request_id) = | >
    State′ := 5 /\ INTER_ID′ := new()  /\ SND_AP1P (respond_id.INTER_ID′)
2. State = 5 /\ RCV_AP1P ({NHN′}_KPH.UN′.MAC1_INTER′)
              /\ MAC1_INTER′ =HMAC (KPH.UN.INTER_ID.NHN′) = | >
    State′ := 9 /\ NUN′ := new()
              /\ MAC2_INTER′ := HMAC (KPH.NUN′.NHN′.HN.WCN)
              /\ WCNE′ := {WCN}_KPH
              /\ SND_AP1P (WCNE′.{NUN′}_KPH.{NHN′}_KPH.MAC2_INTER′)
              /\ request (P, HAAA, nhn1, NHN′)
              /\ witness (P, HAAA, nhn2, NHN′)
3. State = 9 /\ RCV_AP1P (success) = | >
    State′ := 13 /\ DHOK′ := F1 (HOK.NHN.WAAA2_ID.INTER_ID)
              /\ LHOK′ := F1 (DHOK.WCN.AP2_ID.INTER_ID)
              /\ secret (LHOK′, lhok1,{P, WAAA2, AP2}) % to assure secrecy of
                                                       % LHOK between UE, TWAAA and
                                                       % TAP
end role
```

Figure 14: HLPSL code describing UE's role in Inter-WLAN FP.

and WAAA and between WAAA and TAP are protected by the LTSA previously established between them. Nonces and counters are encrypted with $K_{\text{WAAA-UE}}$ in Intra-WLAN FP and with K_encr in Inter-WLAN FP when traveling in the WLAN link between the UE and AP. Furthermore, all keys are freshly generated to defend against replay attacks. EMSK and HOK are fresh because a new RAND and AUTN values are used to generate them. DHOK is fresh because a new HN is used to generate it. Since DHOK is fresh, $K_{\text{WAAA-UE}}$ is believed to be fresh as well. Finally, LHOK is fresh because WC is used to generate it which is continuously incremented after every successful pre-authentication.

5.2. Mutual Authentication and Keys Secrecy. Our proposed protocols provide mutual authentication service to protect against Man-In-the-Middle attacks (MITM), impersonation attacks, and rogue AP attacks. To verify this, we tested our protocols using formal security verification tool known as the "Automated Validation of Internet Security Protocols and Applications" (AVISPA) [34]. AVISPA package is a state-of-the-art tool for the automatic verification and analysis of Internet security protocols. AVISPA integrates automatic security analysis and verification back-end servers like "On-the-Fly Model-Checker" (OFMC), "Constraint-Logic-based Attack Searcher" (Cl-AtSe), and SAT-based Model-Checker (SATMC). Protocols under examination by AVISPA must be coded in the "High Level Protocol Specifications Language" (HLPSL) to be tested by the back-end servers.

HLPSL is an expressive, role-based formal language used to describe the details of the protocols in question. Typically, HLPSL code includes the roles played by all the principals in the security protocol, like UE, WAAA, and HAAA, as well as the role of the environment and the security goals that has to be achieved. Figure 13 illustrates WAAA's role in Intra-WLAN FP expressed in HLPSL. To permit testing the support of secured mutual authentication between the UE and WAAA, request and witness terms are used. The statement (request(WAAA,P,wn2,WN)) in Figure 13 indicates the requirement that the WAAA authenticates the UE while the statement (witness(WAAA, P, wn1, WN′)) indicates the requirement that the WAAA should be authenticated by the UE. Figure 14 illustrates UE's role in Inter-WLAN FP expressed in HLPSL. To permit testing the confidentiality of LHOK, the term secret is used. The statement (secret (LHOK′, lhok1, {P, WAAA2, AP2}) in Figure 14 indicates the



(a) (b)

Figure 15: (a) Message returned by SPAN as a result of testing Intra-WLAN FP with OFMC. (b) Message returned by SPAN as a result of testing Inter-WLAN FP with Cl-AtSe.

Figure 16: Message returned by AVISPA web interface after testing Intra-WLAN FP with SATMC.

requirement to keep LHOK confidential to the UE, TWAAA, and the TAP.

The support of secured mutual authentication in addition to the secrecy of keys in Intra/Inter-WLAN FP was tested using OFMC, Cl-AtSe, and four SAT solvers in SATMC. All tests returned positive results and confirmed the security of mutual authentication service and no authentication attacks were found. Results also confirmed the secrecy of LHOK and no vulnerabilities were discovered. A stand-alone graphical version of the AVISPA package was used in testing our protocols named Security Protocol ANimator for AVISPA (SPAN). Figure 15(a) demonstrate the messages returned by SPAN as a result of testing Intra-WLAN FP with OFMC and Figure 15(b) shows the message returned by SPAN as a result of testing Inter-WLAN FP protocol by Cl-AtSe. Figure 16 shows results of testing Intra-WLAN FP with zchaff SAT solver in SATMC. AVISPA Web Interface was used in SATMC testing because of problems running SATMC in the stand-alone version. Output text was rearranged to fit in a single screen.

5.3. Protection of Message Integrity. The integrity of authentication challenges and responses are protected by appending a Message Authentication Code (MAC) that covers important information carried in EAP messages. MAC preserves the integrity of EAP message, protects against MITM attacks, and validates the authenticity of the sender. In Intra-WLAN FP, MAC_{Intra} is calculated using $K_{WAAA\text{-}UE}$ while MAC_{Inter} is calculated using K_auth in Inter-WLAN FP. $MAC2_{Inter}$ plays an important role to assure the authenticity of the UE to the HAAA by including the last HN value.

5.4. Protection of Identities. It is always desirable to conceal the identity of the UE, TAP ID, and TWAAA ID to protect against eavesdropping and tracking of UE movement. In our proposed protocols, the UE is supplied a local ID, ID_{WLAN}, to be used in future pre-authentications instead of its permanent ID. Local IDs are one-timer identifiers valid for a single pre-authentication session. Therefore, a UE must obtain a new local ID for the subsequent pre-authentication procedure. New local IDs sent by the WAAA and received by the UE are encrypted with $K_{WAAA\text{-}UE}$ and K_encr in Intra-WLAN FP and Inter-WLAN FP, respectively. Current local IDs supplied by the UE and received by the WAAA cannot be encrypted because the identity of the UE must be known to extract the proper decryption key. This is the only case the local ID travels in clear text. This clear text transmission does not form a threat since this local ID is not reused in the future. TWAAA ID and TAP ID are also encrypted with $K_{WAAA\text{-}UE}$ when transmitted by the UE to the WAAA to defend against rogue AP attacks as well as to prevent tracking UE's movement.

6. Conclusions

It is common for UEs to perform horizontal handovers within and between WLANs in UMTS-WLAN interworking architecture due to the limited coverage area of WLAN networks. Handover delays affect the Quality of Service of applications running on the UE. It is always desirable to minimize handover delays. One of the major factors of delay during handover is the delay of mutual authentication between the UE and authentication servers. We designed pre-authentication protocols to reduce authentication delays that occur during intra- and inter-ESS horizontal handovers in UMTS-WLAN interworking environments. The proposed intra- and inter-WLAN pre-authentication protocols proved to surpass existing authentication protocols in terms of authentication signaling cost, authentication delay, and the load the authentication protocol places on critical nodes. The proposed protocols also achieve important security goals like the support of secured key management scheme and the support of mutual authentication service. The security of our protocols was verified by the "Automated Validation of Internet Security Protocols and Applications" (AVISPA) package. Examination of our protocols by AVISPA demonstrated its resistance to authentication attacks and confirmed key's confidentiality.

Acknowledgments

This work was supported in part by the Sultan Qaboos University under Contract number 1907/2005, Bell Canada, and the Natural Sciences and Engineering Research Council of Canada under Grant CRDPJ 328202-05. Part of this work was presented at the *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, *Qshine 2007*, Vancouver, Canada, August 2007.

References

[1] 3rd Generation Partnership Project, "3GPP system to wireless local area network interworking, system description (Release 7)," Technical Specification Group Services and System Aspects TS 23.234 v.7.2.0, 3GPP, Valbonne, France, June 2006.

[2] M. Shi, X. Shen, and J. W. Mark, "IEEE802.11 roaming and authentication in wireless LAN/cellular mobile networks," *IEEE Wireless Communications*, vol. 11, no. 4, pp. 66–75, 2004.

[3] 3rd Generation Partnership Project, "3G security; WLAN interworking security (Release 7)," 3GPP Technical Specifications TS 33.234 v7.0.0, 3GPP, Valbonne, France, March 2006.

[4] G. Kambourakis, A. Rouskas, G. Kormentzas, and S. Gritzalis, "Advanced SSL/TLS-based authentication for secure WLAN-3G interworking," *IEE Proceedings: Communications*, vol. 151, no. 5, pp. 501–506, 2004.

[5] P. Prasithsangaree and P. Krishnamurthy, "A new authentication mechanism for loosely coupled 3G-WLAN integrated networks," in *Proceedings of the 59th IEEE Vehicular Technology Conference (VTC '04)*, vol. 5, pp. 2998–3003, Milan, Italy, May 2004.

[6] H. Chen, M. Zivkovic, and D.-J. Plas, "Transparent end-user authentication across heterogeneous wireless networks," in *Proceedings of the 58th IEEE Vehicular Technology Conference (VTC '03)*, vol. 3, pp. 2088–2092, Orlando, Fla, USA, October 2003.

[7] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," IETF RFC 3748, June 2004.

[8] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol," IETF RFC 2716, October 1999.

[9] P. Funk and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)," IETF Internet Draft, draft-ietf-pppext-eap-ttls-05.txt., July 2004.

[10] A. Palekar, D. Simon, J. Salowey, G. Zorn, H. Zhou, and S. Josefsson, "Protected EAP Protocol (PEAP) Version 2," IETF Internet Draft, draft-josefsson-pppext-eap-tls-eap-09.txt, October 2004.

[11] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," IETF RFC 4187, January 2006.

[12] 3rd Generation Partnership Project, "Security architecture (Release 7)," 3GPP Technical Specifications, 3G Security TS 33.102 v7.0.0, 3GPP, Valbonne, France, December 2005.

[13] IEEE Standard for local and metropolitan area networks, "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications, MAC Security Enhancements," IEEE Std 802.11i, 2004 Edition.

[14] A. Mishra, M. Shin, and W. Arbaugh, "An emprical analysis of the IEEE 802.11 MAC layer handoff process," *ACM SIGCOMM Computer Communications Review*, vol. 33, 2003.

[15] A. Mishra, M. Shin, N. L. Petroni Jr., T. C. Clancy, and W. A. Arbaugh, "Proactive key distribution using neighbor graphs," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 26–36, 2004.

[16] M. Kassab, A. Belghith, J.-M. Bonnin, and S. Sassi, "Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks," in *Proceedings of the 1st ACM International Workshop on Wireless Multimedia Networking and Performance Modeling (WMuNeP '05)*, pp. 46–53, Montreal, Canada, October 2005.

[17] J. Hur, C. Park, and H. Yoon, "An efficient pre-authentication scheme for IEEE 802.11-based vehicular networks," in *Advances in Information and Computer Security*, vol. 4752 of *Lecture Notes in Computer Science*, pp. 121–136, Springer, Nara, Japan, October 2007.

[18] S. Pack and Y. Choi, "Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1x model," in *Proceedings of IFIP TC6 Personal Wireless Communications*, vol. 234, pp. 175–182, October 2002.

[19] A. Mukherjee, T. Joshi, and D. P. Agrawal, "Minimizing re-authentication overheads in infrastructure IEEE 802.11 WLAN networks," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC '05)*, vol. 4, pp. 2344–2349, New Orleans, La, USA, March 2005.

[20] M. Long, C.-H. Wu, and J. D. Irwin, "Localised authentication for inter-network roaming across wireless LANs," *IEE Proceedings: Communications*, vol. 151, no. 5, pp. 496–500, 2004.

[21] A. Al Shidhani and V. Leung, *Secured Fast Handover Protocols for 3G-WLAN Interworking Architecture*, Qshine, Vancouver, Canada, 2007.

[22] IEEE Standard for local and metropolitan area networks, "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications," ANSI/IEEE Std 802.11, 1999 Edition (R2003).

[23] IEEE Standard for local and metropolitan area networks, "IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," IEEE Std 802.11f-2003.

[24] IEEE Standard for local and metropolitan area networks, "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications, Fast BSS transition," IEEE Std 802.11r (Draft 3), 2005.

[25] S. Bangoale, C. Bell, and E. Qi, "Performance study of fast BSS transition using IEEE802.11r," in *Proceeding of the International Conference on Wireless Communications and Mobile Computing (IWCMC '06)*, pp. 737–742, Canada, 2006.

[26] M. Lee, G. Kim, and S. Park, "Seamless and secure mobility management with Location-Aware Service (LAS) broker for future mobile interworking networks," *Journal of Communications and Networks*, vol. 7, no. 2, pp. 207–221, 2005.

[27] C. Lim, D.-Y. Kim, O. Song, and C.-H. Choi, "SHARE: seamless handover architecture for 3G-WLAN roaming environment," *Journal of Wireless Networks*, vol. 15, no. 3, pp. 353–363, 2009.

[28] A. Al Shidhani and V. C. M. Leung, "Local fast re-authentication protocol for 3G-WLAN interworking," *Security and Communication Networks*, 2008.

[29] B. Aboba, "Extensible Authentication Protocol (EAP) Key Management Framework," IETF Internet Draft (draft-ietf-eap-keying-14), June 2006.

[30] W. Arbaugh, "Handoff Extension to RADIUS," IETF Internet Draft (draft-irtf-aaaarch-handoff-04), October 2003.

[31] IEEE Standard for local and metropolitan area networks, "Port-based Network Access Control," IEEE Std 802.1x, 2001 Edition (R2004).

[32] H.-H. Choi, O. Song, and D.-H. Cho, "Seamless handoff scheme based on pre-registration and pre-authentication for UMTS-WLAN interworking," *Wireless Personal Communications*, vol. 41, no. 3, pp. 345–364, 2007.

[33] R. Housley and B. Aboba, "Guidance for AAA Key Management," IETF Internet Draft (draft-housley-aaa-key-mgmt-06), November 2006.

[34] AVISPA—Automated Validation of Internet Security Protocols, http://www.avispa-project.org.