A NEW SIGNALLING PROTOCOL FOR SEAMLESS ROAMING IN HETEROGENEOUS WIRELESS SYSTEMS

Azita Laily Yusof, Mahamod Ismail, Norbahiah Misran
Dept of Electrical, Electronic & System Engineering,
Universiti Kebangsaan Malaysia,
43600 UKM Bangi, Selangor,
Malaysia.
Tel.: +60389216122, Fax : +60389216146
Email: laily012001@yahoo.com, {mahamod, bahiah}@eng.ukm.

ABSTRACT

The world is undergoing a major telecommunications revolution that will provide ubiquitous communication access to citizens, wherever they are. Seamless roaming across different wireless networks which has different types of services and quality of service guarantees has becomes a major topic for the past several years in the research area. With the integration of different technologies, the signaling protocol of mobility management must be designed to support seamless roaming for both intra and interdomain system. In this paper**,** we designed a simplified system architecture, called enhanced system architecture evolution (eSAE) to support mobility between multiple heterogeneous wireless system. eSAE contains fewer network nodes and is reduced to only the enhanced node B (eNB) and access gateway (aGW) that comprise Mobility Management Entity (MME) and User Plane Entity (UPE). We designed a signaling protocol for the location registration due for intersystem roaming in next generation wireless systems. Performance analysis has been carried out and based on this proposed architecture, it is shown that this enhancement can reduce the signaling cost and latency of location registration.

Keywords: Seamless roaming; Handoff latency; Intra and interdomain system; Heterogeneous wireless system

1 INTRODUCTION

In the next generation wireless systems, it is expected that the population of the mobile users will be increased with the development of various applications in the seamless global . Mobile users can have different services that suits their need and can move freely between different wireless systems. However, different wireless system will have different environments, interworking and integration. This scenario has becomes challenges for the researcher to support intra and intersystem mobility for providing continuous wireless services to mobile users in the next generation heterogeneous wireless networks.

There has been many proposals to integrate different wireless systems. In [1], the mobility gateway location register (GLR) has been developed to support the intersystem roaming. The GLR converts signaling and data formats from one network to another. This protocol needs to request location registration after it receives signals from the new system and this cause high overhead of signaling cost and processing time. It also causes the triangular call routing problem because the call for roaming mobile in the same network need to route to the previous network before delivered to the new network. Boundary location register (BLR) [2] was designed in order to solve this problem. In this protocol, the home location register (HLR) is not involved in location registration unless the mobile goes through into another system. So the incoming calls of intersystem roaming mobiles are delivered to them directly. However, this approach is not scalable in the sense that one BLR gateway is needed for each pair of adjacent networks when integrating multiple networks.

In [3], they proposed a distributed gateway foreign agent (GFA) where each foreign agent [FA] can function dynamically either as an FA or GFA.

There is no fixed regional network boundary and mobile decides to perform the home location update scheme increases the requirement of the processing capability on each mobility agent and mobile terminals. The hierarchical Intersystem Mobility Agent (HIMA) [4] was proposed where it acts as an anchor point to forward data as the user moves from one network to another. The HIMAs are placed at the gateway routers or anchor routers for mobile users with high roaming profiles. However, the scheme of address administrative issues and service level agreements across different wireless network and service providers is not analyzed in this paper.

In [5], the author introduced an architecture called ubiquitous Mobile Communications (AMC) to integrate multiple heterogeneous systems. AMC eliminates the need for direct SLA among service providers by using a third party, Network Interoperating Agent (NIA). In this paper, they use distributed and hybrid scheme as a network selection. However, because the decision making is implemented in the mobiles, so the system information has to be broadcasted to the mobiles periodically by the handoff management module, resulting in a great update cost of the system. Moreover, the existing protocol does not consider the determination of the NIA's number required for global integration. Low complexity, centralized network selection scheme [6] has been proposed to overcome the shortcomings of NIA. The proposed scheme eliminated the update cost whereby this scheme will only be invoked by changes in end users' service requirements, beginning of a new application, or ending of an existing application.

In this paper, we propose a simplified network architecture, eSAE to support the low latency system. The network is simplified and reduce to only the Base Station called enhanced Node B (eNB) and access gateway (aGW) that consists of Mobility Management Entity (MME) and User Plane Entity (UPE). The system uses all Internet Protocol (IP) network where all services are via packet switch domain only. In this proposed architecture, we design a signaling protocol for authentication and authorization.

The rest of this paper is organized as follows. First we describe the existing system architecture and the signaling protocol called AMC. Then we present our proposed simplified architecture followed by the authentication and authorization information flow in eSAE. We discuss the simulation results and finally the conclusion.

2 CURRENT AMC PROTOCOL

AMC integrates heterogeneous wireless systems using a third party, called Network Interoperating Agent (NIA) which eliminates the need for SLAs according to its changing mobility and packet arrival pattern. However, this among different network operators. The architecture shown in figure 1, where the NIA functions as a trusted third party for authentication dialogs between the foreign agent and home network. The working principle of this third party architecture is as follows. When a mobile user requests services from an foreign network (FN) and the FN determines that it has no SLA with the user's HN provider, it forwards the request to NIA to authenticate the user. Then, NIA talks to the user's HN provider and mediates between the FN and HN for authentication message exchanges. Once the user is authenticated, NIA also creates security associations/keys required between different network entities. At the end of the proposed security procedures, the HN and FN will be mutually authenticated, and will have session keys for secured data transfer. They integrate the authentication and Mobile IP registration processes as defined in [5].

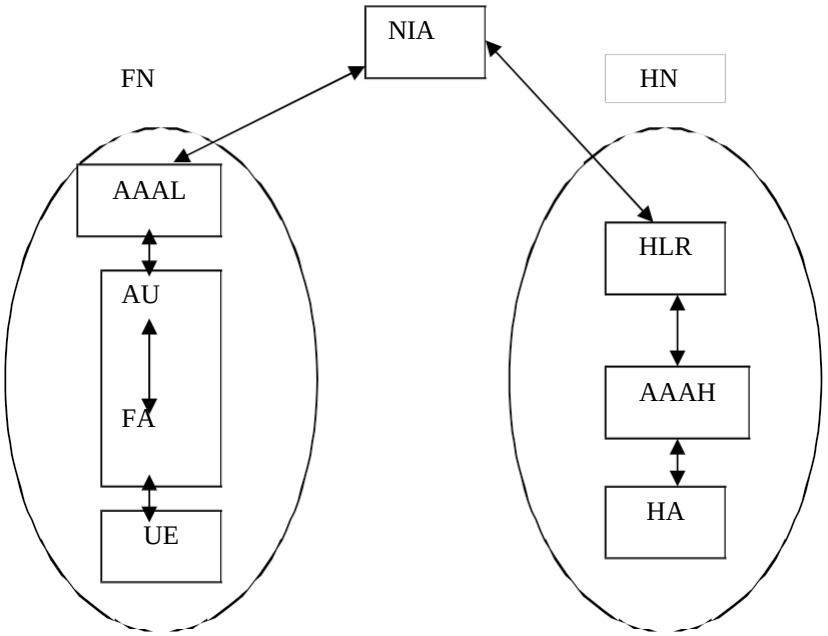

Figure 1 : The architecture for AMC

3 THE PROPOSED ARCHITECTURE

Figure 2 shows our proposed architecture for the next generation wireless systems. eSAE will have two types of network elements supporting the user and control planes.

- The first is the enhanced base station, so called enhanced node B (eNB). This enhanced base station provides air interface and performs radio resource management for the access system.
- The second is the access gateway (aGW). The aGW provides termination of the bearer. It also acts as a mobility anchor point for the user plane. It implements key logical functions including Mobility Management Entity (MME) to manage/store user equipment (UE) context, generate temporary identities, UE authentication and authorization and mobility management and User Plane entity (UPE) to manage/store UE context and packet routing/forwarding, initiation of paging.

Comparing the functional breakdown with existing architecture:

- Radio Network elements functions, such as Radio Network Controller (RNC), are distributed between the aGW and the eNB.
- Core Network elements functions, such as SGSN and GGSN or PDSN (Packet Data Serving Node) and routers are distributed mostly towards the aGW.

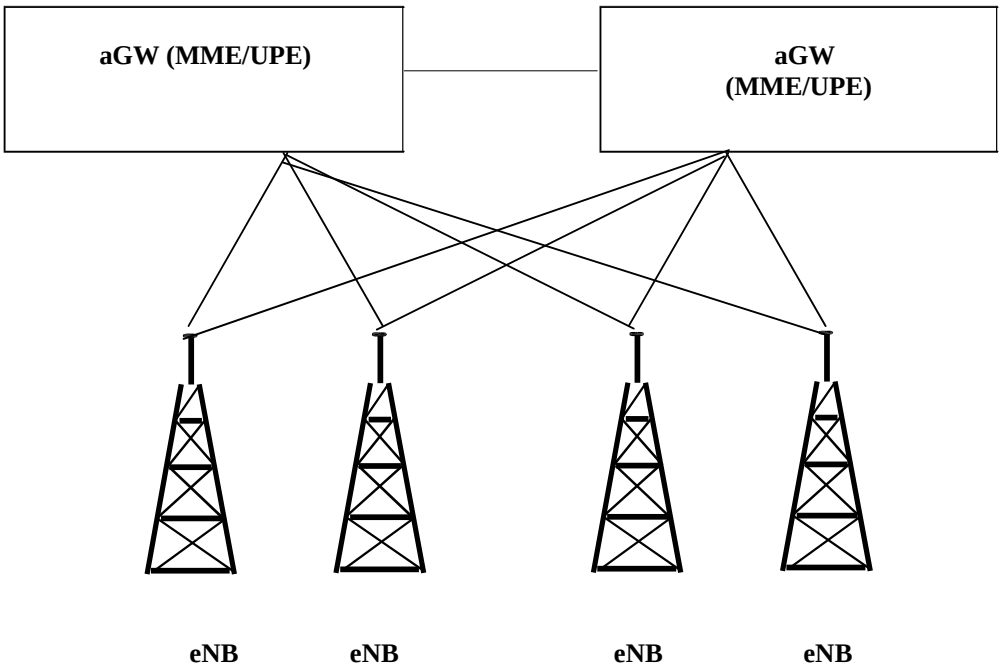

Figure 2 : The proposed mobility management architecture for next generation all-IP-based wireless systems

3.1 Authentication and Authorization

The working principle of this architecture is as follows. When a mobile user requests service from a FN and the FN determines that it has no SLA with user's home service subscriber (HSS), it forwards the request to aGW to authenticate the user. Then, aGW talks to user's HSS and mediates between FN and HSS for authentication message exchanges. Once the user is authenticated, aGW also creates security associations/keys required between different network entities. Finally the HSS and FN will be mutually authenticated, and will have session keys for secured data transfer.

The authentication and Mobile IP registration processes are integrated in the proposed architecture using the procedures defined in [7]. IEEE 802.1x port access control standard [8] is used for end-to-end mutual authentication between a UE and its HSS. IEEE 802.1x uses a special frame format known as Extensible Authentication Protocol (EAP) over LAN (EAPOL) for transportation of authentication messages between a UE and an access point (AP). EAP [9] over RADIUS [10] or Diameter [11] is used for the transportation of authentication messages between other entities. When the UE roams into a FN, the authentication and MIP registration are carried out as described below. Here, EAP-SIM [12] is used to illustrate the authentication process. Note that any other authentication schemes, e.g. EAP-AKA [13], EAP-SKE [14], EAP-TLS [15] etc. can also be used. Figure 3 shows the location registration procedure.

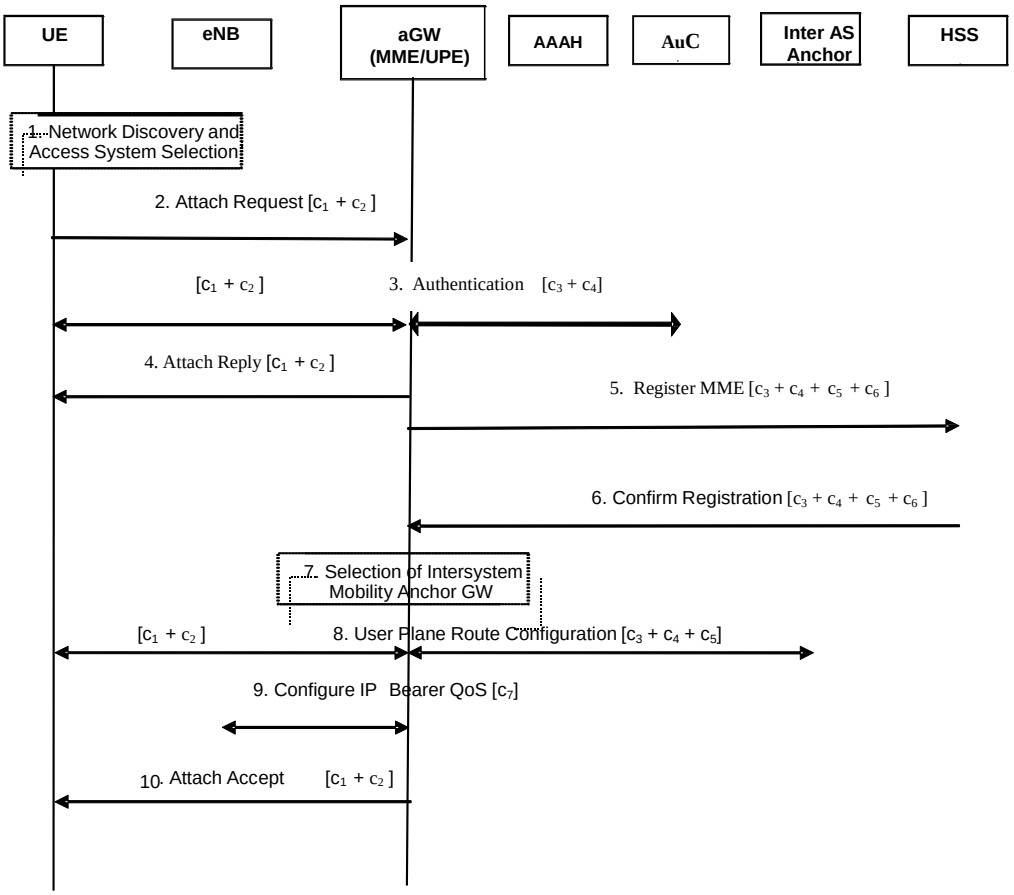

Figure 3 : The authentication and authorization signaling messages

1. The UE discovers new access system and performs access system and network selection.
2. The UE sends an attach request, MIP *Registration Request* including *Mobile-AAA Authentication* extension (as defined in [16]) to the aGW. The UE also includes a *SIM Key Request* extension [19] and a *Network Access Identifier* (NAI) [18], e.g. *UE@relam*, in its MIP *Registration Request*. The *SIM Key Request* extension contains a random number (NONCE_UE) picked up by the UE, which is used for new authentication key generation as discussed later in this section.
3. When the aGW receives the MIP *Registration Request* and finds the *Mobile-AAA Authentication* extension, it learns that the UE is a roaming user. Based on the NAI in the MIP *Registration Request*, the aGW recognizes that the operator does not have direct SLA with the UE's HN and forwards the MIP *Registration Request* to the Home AAAH server (AAAH). Once the AAAH receives the MIP *Registration Request* containing the *SIM Key Request* extension, first it verifies the *Mobile-AAA authentication* extension. If the authentication is successful, it contacts the home authentication center (AuC) of the UE and obtains *n* number of triplets (RAND, SRES, Kc), where RAND denotes a random number, SRES denotes the response and Kc is the key used for encryption. Then it forwards a copy of these triplets to aGW. When aGW receives n triplets it derives a UE_AAAH key (K_{UE_AAAH}) and calculates message authentication code (MAC) for the RANDs (MAC_RAND) using [19]

$$K_{UE\_AAAH} = h(n * Kc \,|\, NONCE\_UE) \text{ and}$$

$$MAC\_RAND = PRF(K_{UE\_AAAH}, \alpha) \quad (1)$$

where α is $n*RAND \mid$ key lifetime; and $h()$ and $PRF()$ denotes a one-way hash function and a keyed pseudo-random function, respectively.

Then, aGW sends the RANDs, MAC_RAND and *SIM Key Reply* extension to UE. The UE derives the corresponding SRES and Kc values using its SIM card and the received RANDs. It also calculates (K_{UE_AAAH}) and MAC_RAND using (20). It validates the authenticity of RANDs by comparing the calculated MAC_RAND with the received MAC_RAND. Thus, confirming that the RANDs are generated by its HN. If the MAC_RAND is valid, the UE calculates a MAC for its SRES values using [19]

$$MAC\_SRES = PRF(K_{UE\_AAAH}, n * SRES) \quad (2)$$

The MAC_SRES is used by aGW to know if the SRES values are fresh and authentic. The UE also generates security association keys; (K_{UE_eNB}) for the eNB and (K_{UE_HSS}) for the HSS using [19]

$$K_{UE\_eNB} = PRF(K_{UE\_AAAH}, Add_{eNB}) \text{ and}$$

$$K_{UE\_HSS} = PRF(K_{UE\_AAAH}, Add_{HSS}) \quad (3)$$

where Add_{eNB} and Add_{HSS} are the IP address of eNB and HSS, respectively. These keys are used to authenticate subsequent Mobile IP registrations until the key lifetime expires.

4. Now, the UE resends MIP *Registration Request* message to the eNB containing *SRES* extension [19] and *Mobile-AAA Authentication* extension. When eNB detects the presence of *Mobile-AAA Authentication* extension, it forwards the MIP *Registration Request* message to aGW. aGW calculates MAC_SRES and compares that with the received MAC_SRES. If valid, it forwards the MIP *Registration Request* message to the AAAH. After successful authentication AAAH forwards the MIP *Registration Request* containing K_{UE_HSS} (calculated using (4)) to the HSS.

$$K_{UE\_HSS} = PRF(K_{UE\_AAAH}, Add_{eNB,} Add_{HSS}) \quad (4)$$

5. The HSS confirms the registration of the new aGW. Subscription data authorising the Default IP Access Bearer are transferred. Information for policy and charging control of the Default IP Access Bearer is sent to the aGW.
6. An Inters AS Anchor is selected. The IP address configuration is determined by user preferences received from the UE, by subscription data, or by HPLMN or VPLMN policies.
7. The Inter AS Anchor configures the IP layer with the determined user IP address. The user plane is established and the default policy and charging rules are applied. The user plane establishment is initiated by the aGW.
8. The aGW provides the Evolved RAN with QoS configurations for the Default IP Access Bearer, e.g. the upper limits for transmission data rates.
9. The aGW accepts the UE's network attachment and allocates a temporary identity to the UE. Also the determined user IP address is transferred. aGW calculates UE-eNB security key, K_{UE_eNB}, and forwards the MIP *Registration Reply* (containing K_{UE_eNB} and the Kc keys) to eNB. eNB extracts K_{UE_eNB} and the Kc keys and send a MIP *Registration Reply* to the UE. The Kc keys are used for secure data transfer between the UE and eNB providing confidentiality and integrity to the data traffic.

4 PERFORMANCE ANALYSIS of eSAE

In this section, we analyze the performance of signaling cost and latency of location registration due to intersystem roaming. The costs for location registration are associated with the traffic of messages between the entities and the accessing cost of databases. To compare the total of signaling cost between the proposed and existing architecture, we assume the following parameters :

Table 1 : Simulation parameters

p	transmission cost of messages between the UE and the eNB
α	transmission cost of messages between the eNB and the aGW
β	transmission cost of messages between the aGW and the HSS
c_1	transmission cost of messages between the UE and the eNB
c_2	transmission cost of messages between the eNB and the aGW
c_3	transmission cost of messages between the aGW and the AAAH
c_4	transmission cost of messages between the AAAH and the AUC
c_5	transmission cost of messages between the AUC and the IASA
c_6	transmission cost of messages between the IASA and the HSS
c_7	transmission cost of messages between the eNB and the aGW

We assume that a mobile keeps the same mobility pattern when it moves into another system. Further, we assume that the updating, deletion and retrieval in the database have the same cost, *a*. We calculate the total signaling of location registration which is the sum of the transmission cost and the cost associated with database access. Then we calculate the latency of location registration where we assume the average processing time of each database access is $1/\mu$ and the average waiting time is *w*. So the latency for location registration is the total time including waiting time in queue and the processing time.

Figure 4 shows the comparison of total signaling cost as a function of intersystem roaming probability. As we can see from the graph, the total signaling cost increases as the intersystem roaming probability increases,. We can also observe that the total signaling cost of the eSAE protocol is much lower than the NIA protocol. It is seen that as compared to the NIA protocol, the eSAE protocol yields significantly improved because of the simplified architecture. The NIA protocol has to access more databases compared to the eSAE protocol. Similar to the case of total signaling cost, the latency of location registration increases with the increases of the intersystem roaming probability. Figure 5 shows the result obtained. Therefore, eSAE protocol reduces the total signaling cost and latency of location registration so that it is more suitable for an intersystem roaming environment.

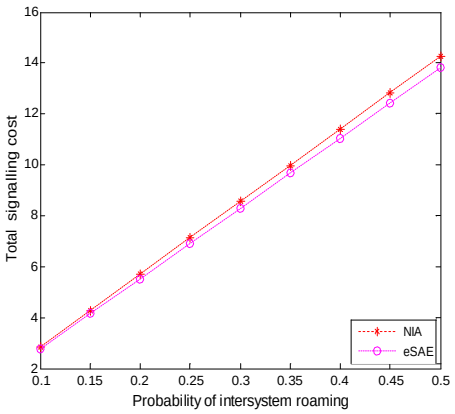

Figure 4 : Total cost of location registration

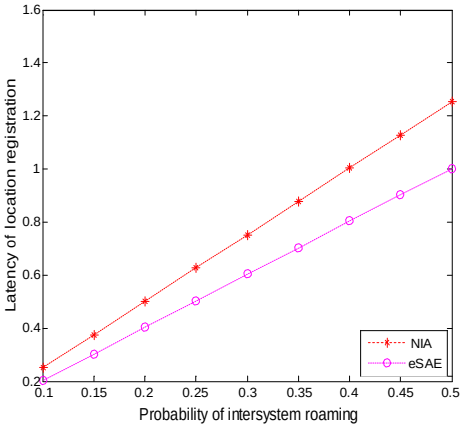

Figure 5: Latency of location registration

5 Conclusion

In this paper, we introduced a new signaling protocol for mobility management which is based on the enhancement of the SAE architecture. We proposed the detailed procedure of location registration for the eSAE protocol. This protocol is specifically developed to decrease the latency of the NIA protocol. To summarize the comparison of eSAE and NIA protocol, we measured the signaling cost of location registration. Moreover, we evaluated the latency of the location registration, which is composed of waiting time and processing time at a specific database. The results show that the eSAE protocol is able to reduce the signaling cost and latency of location registration for the mobile's moving across different networks.

4 REFERENCES

[1] ETSI TS 129 120 V3.0.0, "Universal mobile telecommunications systems (UMTS); mobile application part (MAP) specification for gateway location register (GLR)", 3GPP/ETSI 2000, 2000-2003.

[2] I.F. Akyildiz, W. Wang, "A new signaling protocol for intersystem roaming in next generation wireless systems", IEEE Journal on Selected Area in Communications, vol.19, no. 10, Oct. 2001, pp. 2040-2052.

[3] I.F. Akyildiz, W. Wang, "A novel distributed dynamic location management scheme for minimizing signaling costs in mobile IP", IEEE Transactions on Mobile Computing, vol. 1, No 3, July 2002, pp. 163-175.

[4] N. Shenoy, "A framework for seamless roaming across heterogeneous next generation wireless

networks", Journal on ACM Wireless Networks.

[5] I.F. Akyildiz, S. Mohanty, J. Xie, "A ubiquitous mobile communication architecture for next-generation heterogeneous wireless systems", IEEE Communications Magazine, vol. 43, no. 6, pp. 29-36, June 2005.

[6] H. Jia, Z. Zhang, P. Cheng, H. Chen, A. Li, " Study on network selection for next generation heterogeneous wireless networks", in Proc. IEEE International Symposium on Personal, Indoor and Mobile radio Communications", 2006.

[7] Glass, S., Hiller, T., Jacobs, S., and Perkins, C., "Mobile IP authentication, authorization, and accounting requirements," *RFC 2977, IETF*, 2000.

[8] "IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control." IEEE Std 802.1X-2001.

[9] Blunk, L. and Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)," *RFC 2284, IETF*, 1998.

[10]Rigney, C. and *et al*, "Remote Authentication Dial In User Service (RADIUS)," *RFC 2865, IETF*, 2000.

[11]Calhoun, P. R., "Diameter Mobile IPv4 application," *Internet Draft, draft-ietf-aaa-diameter-mobile ip 16.txt, work in progress*, 2004.

[12]Haverinen, H. and Salowey, J., "EAP SIM authentication," *Internet Draft, draft-haverinen-pppest-eap-sim-16.txt, work in progress*, 2004.

[13]Arkko, J. and Haverinen, H., "EAP AKA Authentication," *Internet Draft, draft-arkko-pppest-eap-aka-09. txt, work in progress*, 2003.

[14] Salgarelli, L., "EAP SKE authentication and key exchange protocol," *Internet Draft, draft-salgarelli-pppext-eap-ske-03.txt, work in progress*, May 2003.

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

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

[17]Haverinen, H., Asokan, N., and Maattanen, T., "Authentication and key generation for Mobile IP using GSM authentication and roaming," in *Proc. IEEE ICC (ICC'01)*, pp. 2453{2457.

[18]Calhoun, P. and Perkins, C., "Mobile IP network access identi¯er extension for IPv4," *RFC 2290, IETF*, 2000.

[19] Haverinen, H., Asokan, N., and Maattanen, T., "Authentication and key generation for Mobile IP using GSM authentication and roaming," in *Proc. IEEE ICC (ICC'01)*, pp. 2453{2457.

[20]"3GPP System to WLAN ¯ Interworking: Functional and Architectural De¯ni-tion." *Tech. rep. 3GPP TR 23.934 v0.3.0*. 3GPP.