Providing Security in 4G Systems: Unveiling the Challenges

Mahdi Aiash, Glenford Mapp and Aboubaker Lasebae
School of Engineering and Information Science
Middlesex University
London, UK
{M.Aiash, G.Mapp, A.Lasebae}@mdx.ac.uk

Raphael Phan
Electronic and Electrical Engineering
Loughborough University
Loughborough, UK
R.Phan@lboro.ac.uk

***Abstract*— Several research groups are working on designing new security architectures for 4G networks such as Hokey and Y-Comm. Since designing an efficient security module requires a clear identification of potential threats, this paper attempts to outline the security challenges in 4G networks. A good way to achieve this is by investigating the possibility of extending current security mechanisms to 4G networks. Therefore, this paper uses the X.805 standard to investigate the possibility of implementing the 3G's Authentication and Key Agreement (AKA) protocol in a 4G communication framework such as Y-Comm. The results show that due to the fact that 4G is an open, heterogeneous and IP-based environment, it will suffer from new security threats as well as inherent ones. In order to address these threats without affecting 4G dynamics, Y-Comm proposes an integrated security module to protect data and security models to target security on different entities and hence protecting not only the data but, also resources, servers and users.**

Keywords- 4G systems, IEEE X.805, AKA protocol, Integrated Secuiry Layers, Targeted Security Models

I. INTRODUCTION

Due to some security weaknesses in 2/2.5G networks and the need to support voice and data transmission, third generation (3G) networks have been recently deployed.

Aside from supporting multimedia communication [3], 3G-based technologies, e.g., Universal Mobile Telecommunications System (UMTS) [4], [1] provide new services such as location dependent services, which along with the support of voice and high quality video traffic are the major innovations, compared to 2G technologies [3]. Furthermore, 2G's main security weaknesses have been tackled in 3G systems; a more generic Authentication and Key Agreement (AKA) method has been developed. In addition, integrity and stronger encryption mechanisms have been introduced.

However, due to the increasing demand–for ubiquitous connectivity and service provision, there is growing momentum to move towards Beyond 3G or 4G communication systems.

4G networks represent an open environment where different wireless technologies and service providers share an IP-based core network to provide uninterrupted services to their subscribers with almost the same quality of service (QoS). In 4G systems, mobile devices are expected to switch between networks of different operators and technologies; this is referred to as vertical handover and it is required to maintain the Service Level Agreements (SLAs) needed by their applications.

A proposal of a 4G architecture is the Y-Comm framework [7][8], which is been developed by a number of institutions. Y-Comm details the functionalities and mechanisms required to support heterogeneous networking.

It is no longer the case that security for communication frameworks is considered as an add-on rather than a fundamental issue. Future communication systems consider security from the initial stages of the design process. This is reflected in the design of 4G architectures such as Y-Comm where security is considered as an integral part of the design. However, in order to develop an efficient security module, it is necessary to identify the threats and risks faced by communication systems. But since analyzing security requirements of communication systems is quite complex, the ITU introduced a systematic analysis tool called X.805 [9] as a holistic approach to network security by discussing systems security requirements at different levels and pinpointing potential network vulnerabilities [9].

In this paper, we examine whether it is possible to use 3G security mechanisms such as AKA for 4G systems such as Y-Comm. The X.805 framework will be used to validate the AKA mechanisms on Y-Comm, hence revealing what additional security measures are needed to secure 4G systems. The rest of the paper is structured as follows: Section 2 describes the architecture of the X.805 standard. Section 3 explains the AKA protocol of 3G networks. Section 4 introduces the Y-Comm framework as an example of 4G networks while Section 5 proposes deploying the AKA protocol with Y-Comm; this proposal is analyzed using the X.805 standard in Section 6. The results of the analysis are summarized in Section 7. Section 8 introduces related work to enhance security in 4G systems, and then the paper concludes in the final section.

II. INTRODUCTION TO THE X.805 STANDARD

As described in [9], the X.805 standard proposes three security layers (applications, services and infrastructure), three security planes (end user, control and management) which are identified based on the activities performed over

the network, and eight security dimensions to address general system vulnerabilities (access control, authentication, non-reputation, data confidentiality, communication security, data integrity, availability, and privacy).

Figure 1 shows the complete architecture of the X.805 standard including Security Layers, Planes and dimensions.

The security layers of X.805 standard have already been applied to different communication systems such as WiFi, ATM and IP-based networks [11] [9] respectively.

III. The Use of the Authentication and Key Agreement (AKA) Protocol in 3G Networks

This section describes in some detail the AKA protocol [1] used in 3G networks. The AKA protocol follows the steps shown in the table.

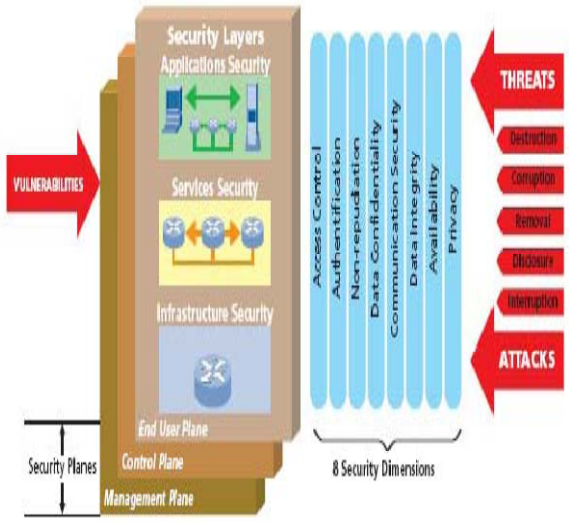

Figure 1. The X.805 standard architecture [10]

Table I. AKA Steps in 3G networks

Steps	Actions	Description
1	MS Sign-on ↓ BSc1/ SRNC1	Initial stage, the message includes Mobile Station's (MS) security preferences is sent to the Base Station Controller/ Serving Radio Network Controller (BSC/SRNC)
2	BSc1/ SRNC1 ↓ SGSN 1/VLR1	BSc1 consults the Serving GPRS Support Node/ Visitor Location Register (SGSN/VLR) whether to allow MS to join or not
3	SGSN 1/VLR1 ↓ HLR	VLR1 asks the Home Location Register (HLR) to send a set of security parameters attached to MS
4	HLR K_i AuC SV generating using the F1-F5 functions	HLR gets the key K_i from the Authentication Server (AuC) and uses it along with other parameters [1] to generate a Security Vector (SV) using F1- F2 functions
5	HLR SV ↓ VLR1/SGSN1	HLR sends SV to the VLR1
6	VLR1/SGSN1 RAND & AuTN ↓ MS	VLR1/SGSN1 sends a random value (RAND) and authentication token (AuTN) [1] to MS as a challenge
7	Mutual authentication between the network and MS	MS compares the re-generated SV's parameters to achieve mutual authentication
8	BSc1/ SRNC1 ↓ MS	BSC/SRNC sends back an integrity protected list of MS's security preferences

Although weaknesses have been shown on the basic AKA protocol improvements such as X-AKA and EAKAP [12][5], these weaknesses were not related to the basic architecture of the AKA protocol, but rather to the underlying functions used to achieve some security aspects. Therefore, many projects such as the Third Generation Partnership Project 3GPP project [13] use this protocol for network-level security.

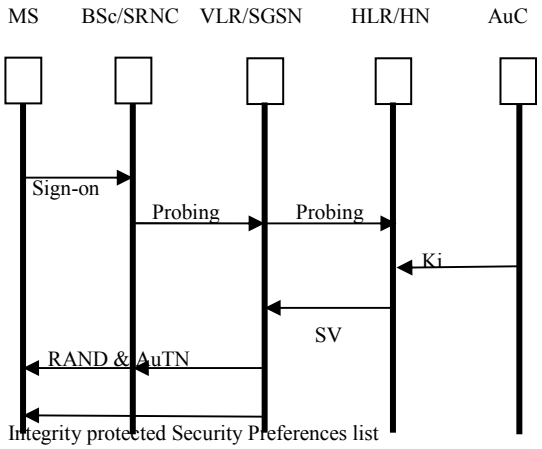

Figure 2. AKA architecture for 3G network

IV. Introduction to Y-Comm

As previously mentioned, Y-Comm is an example of a 4G system. The complete structure of Y-Comm is shown in Figure 3.

A very detailed explanation of the Y-Comm design is given in [7] and [8]. For Y-Comm to support mobile-initiated vertical handover, four layers are mainly concerned: in the peripheral framework we have the **Policy Management Layer (PML)** which helps the mobile device to decide when and why to handover as well as the **Vertical Handover Layer (VHL)** which is responsible for initiating, executing and terminating handover procedures. While in the Core framework we have the **Network Management Layer (NML)** that maintains all neighbouring networks characteristics and the **Reconfiguration Layer (REL)** which manages and controls network entities and resources to accommodate the handover.

The Y-Comm architecture in the core network is distributed and hence we can map into 3G/ UMTS infrastructure as shown in Figure 4.

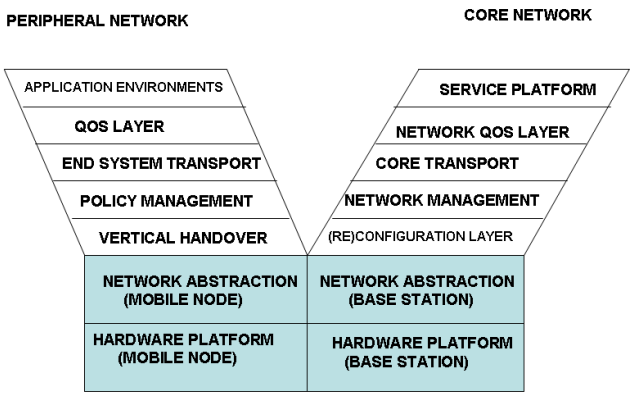

Figure 3. Y-Comm architecture [8]

However, it should be emphasized that Y-Comm is a 4G system and hence it supports several different wireless systems simultaneously. Hence Y-Comm supports different types of MSCs / SGSNs in addition to using media-independent handover mechanisms such as IEEE 802.21 [17] to support vertical handover.

It has been shown that the aforementioned AKA protocol is adequate for 3G based networks, this is due to a set of issues related to the architecture of the network. However, due to 4G networks' new features (all IP-Based connections, heterogeneous environment controlled by different operators), new mechanisms are proposed to support functions such as Vertical Handover. In fact, there is a need to cope with the complexity, openness and dynamics of 4G networks. Therefore, deploying current security mechanisms with future 4G networks is still an open question.

V. AKA PROTOCOL WITH Y-COMM

This section proposes an AKA protocol based on [1] to be deployed with Y-Comm in order to protect the network resources while performing a vertical handover [7]. In this example, MSC1/SGSN1 and SRNC1 represent the first network, while MSC2/SGSN2 and SRNC2 represent the second. By building on the mobile–initiated mobility model proposed in [14], AKA might be implemented as follows (see Figure 5).

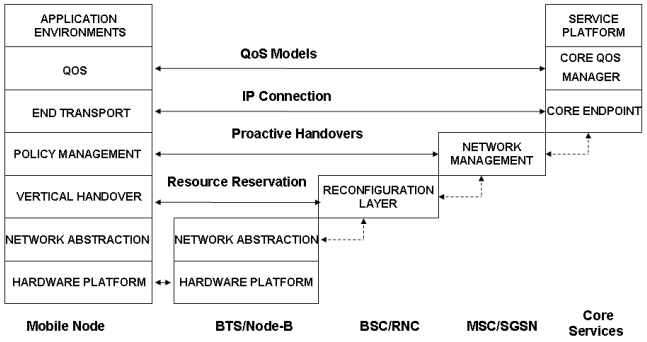

Figure 4. Mapping Y-Comm onto Mobile Infrastructure [14]

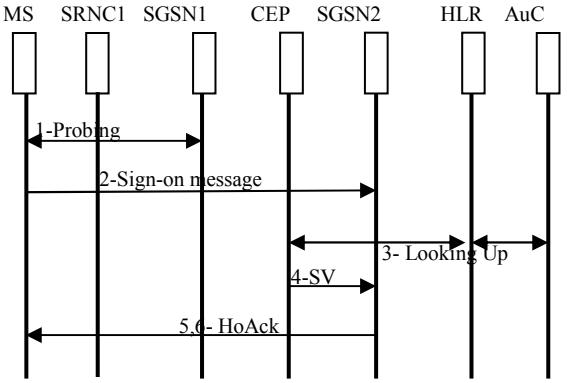

Figure 5. 3G-AKA in the Y-Comm

1. It is assumed that the MS has already joined a network and has been authenticated and has agreed with the network on the set of keys. The MS probes the network management layer (NML) in the core network to know about available networks [14].
2. Based on the characteristics of neighboring networks, the Policy Management Layer (PML) of the MS decides the target network [14].
3. The MS sends a sign-on message to the Core-endpoint specifying the target network; this message contains the MS' unique identifier and Key Set Identifier (KSI) which identifies the set of keys (CK, IK, AK) already established and used with the current VLR (VLR1).
4. When SGSN2/VLR2 receives the sign-on message, it checks with HLR to authenticate the MS and gets the corresponding security vector (SV). If the Lease Time field (LT) of the MS' security vector (SV) is about to expire (beyond a threshold, e.g., 80% of the time elapsed), HLR and AuC generate a new Security Vector for the MS to be used in the new network (SGSN2). HLR sends (SV) to SGSN2/MSC2/VLR2 thus the MS is authenticated and authorized to use the network. In

the case where LT is above the threshold, there is no need to re-generate a new set of keys.

5. MSC2/SGSN2 informs BSc2/SRNC2 of the handover and asks it to reserve a channel for the Mobile device. Once a channel is allocated, SRNC2 acknowledges that back to MSC2/SGSN2 which passes it to Core End- Point (CEP).
6. CEP sends Hand Over Acknowledgment (HOAck) message to the MS.
7. The MS needs to authenticate the new network (MSC2/VLR2). Therefore, once the MS joins the network, SGSN2 sends a challenge message containing the new AuTN and RAND (AuTN2, RAND2). MS follows the same procedure to verify the network Sequence number and MAC, and authenticate the network.

VI. Analysis of AKA on Y-Comm using the X.805 standard

In this section we apply the X.805 standard to analyze the performance of the AKA protocol, proposed in a previous section.

Since AKA protocols aim to provide network-level security, the functionality of this set of protocols is only related to the Infrastructure Layer of the X805 standard which is concerned with the security of network links and elements.

As previously mentioned, each layer is decomposed into three planes and for each plane the following eight vulnerabilities corresponding to the security dimensions of X.805 are examined as shown in Figure 6.

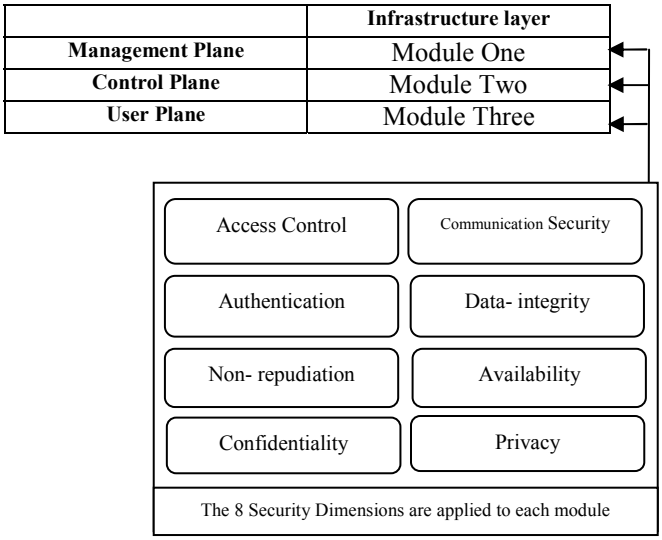

Figure 6. X.805 standard for the AKA protocol

The Management plane is represented as Module 1, the Control plane is represented as Module 2 and the User plane is represented as Module 3. In the table below, each vulnerability is analyzed relative to Module 1, 2 and 3.

The remainder of this section discusses the security dimensions for each of the three modules

Table II. Security vulnerabilities for each module

Vulnerabilities	Modules Involved
Access Control	Modules 1&2 : no access control mechanisms such as Access Lists (ACLs) or Firewalls are applied to restrict the access to network resources Module3: Users' access allowance is based on the authentication process.
Authentication	Modules 1, 2 & 3: AKA protocol provides mutual authentication between the mobile device (but not the user) and the network.
Non-Repudiation	Modules 1,2 & 3: since AKA protocol uses symmetric key-based mechanisms, non-repudiation is not provided
Data Confidentiality	Modules 1, 2 & 3: data confidentiality for the connection between the mobile device and the MSc/SGSN is achieved using Cipher Key (CK) and F6 function as an encryption algorithm [1]. However, no encryption is done beyond MSc/ SGSN.
Communication Security	Modules 1 & 2: no specific security mechanisms are proposed to protect the data transmitted in the core network as it is considered physically secure. Module 3: from a user perspective, once authentication and key agreement processes are done, the security of the wireless part of the connection is guaranteed.
Data Integrity	Modules 1, 2 & 3: AKA provides Data Integrity by implementing Integrity Key (IK) and Hashing algorithm (F7) for the MS- MSc/SGSN connection
Availability	Module 1, 2 & 3: no specific mechanisms such as intrusion detections/protections are implemented to ensure network elements and services are available [9] and to make sure that network resources are immune against denial of service attacks.
Privacy	Module 1, 2 & 3: although confidentiality is achieved by using encryption, there is no guarantee that subscribers' credentials are only revealed to authorized parties.

VII. SUMMARY OF RESULTS

The key vulnerabilities indicated by this work include access control, communication security, data confidentiality, availability and privacy. These vulnerabilities are not seen in 3G networks because the network infrastructure is wholly owned by the network operators and access is denied to other network entities. However, such assumptions are no longer valid in 4G systems and therefore must be addressed in the proposed security architecture.

Moreover, since 4G is an IP-Based environment, it will suffer from most of the IP-specific security vulnerabilities found in the Internet. Our experience of the Internet as the best example of a successful open architecture has taught us that it is not sufficient to only protect data but it is also necessary to protect entities from each other (DoS, Spam) and also to protect the network infrastructure. Hence 4G systems must also address these concerns.

VIII. OUR APPROACH

To address the security threats of 4G networks without affecting its openness, a multi-prong approach is required. In this section, we examine a new approach based on the concepts of an Integrated Security Module (ISM) to protect data and Targeted Security Models (TSMs) which are needed to protect entities, such as users and servers that are using the open infrastructure.

A. Integrated Security Module (ISM)

The different vulnerabilities outlined in the previous section point to the need to tackle these issues in an integrated fashion instead of using multiple uncoordinated actions. In addition, a framework such as Y-Comm allows us to integrate different security features with the variuos layers of the architecture. Furthermore, because Y-Comm consists of two frameworks, we must consider how the security of a given layer is mapped onto both frameworks at the same time, as shown in Figure 7. Our security module comprises the following layers:

1) Service And Application Security (SAS):

a) On the peripheral networks: Provides AAAC functions and authenticates the user to use the mobile node.

b) In the core network: SAS decides which services should be installed on a specific peripheral network and authenticates the users that can use this service.

2) QoS Based Security: Looks at QoS issues, e.g., Service Level of Agreements (SLA), network overloading and Denial of Service Attacks (DoS) in both the core and peripheral networks.

3) Network Transport Security (NTS):

a) In Peripheral networks: NTS is concerned with the access and visibility of end devices to the Internet.

b) In Core network: NTS is involved in setting up secure tunnels between core network endpoints.

4) Network Architecture Security (NAS): It defines the security issues and threats resulting from moving to a particular network type.

B. Targeted Security Models (TSMs)

In addition to the ISM, we need targeted security models to protect entities in the system. As mentioned in the previous section, it is not sufficent to only protect data but it is also necessary to protect the entities that use the open architecture from attacking each other and/or network infrastructure. TSMs are security models based around protecting a specific entity from being abused or attacked by other entities such as users in an open architecture. This is a new concept which we believe is necessary to provide a completely secure environment.

We have identified three security models that need to be developed, the first is called the connection security model which controls the connection between users and thus prevents a user from arbitrarily sending an unsolicited message to another user, e.g., Spam.

The second security model is concerned with restricting access to servers by introducing the concept of a scope. This is an enhancement of the "Off By Default" [20] proposal. So users can only access the server when they are in the same scope of the server.

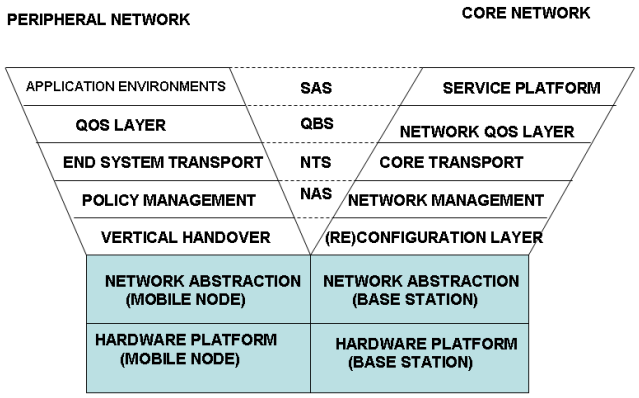

Figure 7. Y-Comm complete architecture [7]

Examples of scopes are Local: only a process on the same machine can access this server, LAN: only machines on the same LAN can access the server, Domain: only machines on the same domain can access the server, and finally Global where the service is globally accessible. We believe that this mechanism will greatly reduce Denial of Service attacks on offered services without limiting access to key parts of the infrastructure.

The final security model is for facilitating secure vertical handover and attempts to prevent network resources from being abused and overloaded. This is done by monitoring resource requests and ensuring access to vulnerable components does not exceed the available QoS. This model therefore makes use of the mechanisms in the QBM layer of the ISM. We are working on these models.

IX. RELATED WORK:

The IETF handover keying working group (HOKEY WG) [18] is currently working on a new mechanism to support inter-technology handover which deploys the Extensible Authentication Protocol (EAP) [19] to support handover key distribution. We are exploring how we might use this mechanism in our secure vertical handover model.

X. CONCLUSION:

In this paper we have demonstrated that the security requirements for 4G systems are much greater than those of 3G. A lot of this is due to the fact that in 4G systems we require a more open architecture with its inherent security vulnerabilities compared to the closed network of 3G systems. These requirements clearly indicate that we need an integrated security module to protect data across different networks and in addition, we need targeted security models to protect various entities: users, servers and network infrastructure.

REFERENCES

[1] P, Chandra, "Bulletproof wireless security : GSM, UMTS, 802.11 and ad hoc security," Newnes. Oxford, pp. 129-158, 2005.

[2] J. F. Kurose and K. W. Ross., "Computer networking: a top-down approach", 4th ed. Boston: Addison-Wesley/Pearson, pp. 551-553. 2007.

[3] L. Dell Uomo and E. Scarrone. "An all-IP solution for QoS mobility management and AAA in the 4G mobile networks ". In. Wireless Personal Multimedia Communications. The 5th International Symposium on. Italy, vol. 2, pp. 591- 595. 16-Dec 2002.

[4] J.H. Schiller." Mobile communications", 2nd ed. London : Addison-Wesley , pp. 136-154, 2003.

[5] F. Farhat, S. Salimi, and A. Salahi. "An Extended Authentication and Key Agreement Protocol of UMTS". In . Lecture Notes in Computer Science Proceedings of the 5th International Conference on Information Security Practice and Experience, Xi'an, China, pp. 230-244, 2009.

[6] G.Kambourakis, A. Rouskas, and S. Gritzalis. "Experminetal Analysis of an SSL-Based AKA Mechanism in 3G-and-Beyond Wireless Networks". Wireless Personal; Communication, 29(3/4), pp. 303-319, 2004.

[7] G. Mapp, D.N. Cottingham, F. Shaikh, P. Vidales, L. Patanapongpibul, J. Balioisian, and J. Crowcroft, "An Architectural Framework for Heterogeneous Networking". International Conference on Wireless Information Networks and Systems (WINSYS), pp. 5-10. August 2006

[8] G.E. Mapp, F. Shaikh, D. Cottingham, J. Crowcroft, and J. Beliosian. "Y-Comm: A Global Architecture for Heterogeneous Networking" . (Invited Paper). 3rd Annual International Wireless Internet Conference (WICON 2007), October 2007

[9] Z. Zeltsan. "ITU-T RecommendationX.805 and its application to NGN". www.itu.int/ITU-T/worksem/ngn/200505/.../s5-zelstan.pdf. [Accessed 16. Feb 2010].

[10] Y. Park and T. Park. "A Survey of Security Threats on 4G Networks" in. Commun. & Networking Lab., Samsung Adv. Inst. of Technol. Globecom Workshops, IEEE. Washington, DC, pp. 1-6. 22-01-2008.

[11] Bell Labs, "The Bell Labs Security Framework: Making the Case for End-to-End Wi-Fi Security," http://www.forsitegroup.com/pdf/wplucent_wifi_security.pdf. [Accessed 16.Feb. 2010].

[12] C.M. Huang and J.W. Li, "Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption". In: Proceedings of the 19th International Conference on Advanced Information Networking and Applications, Washington, DC, USA, vol. 1, pp. 392-397 ,2005.

[13] M. Garcia-Martin. "Input 3rd-Generation Partnership Project (3GPP) Release 5 Requirements on the Session Initiation Protocol (SIP)". RFC 4083, May 2005. http://www.packetizer.com/rfc/rfc4083/. [Accessed 16 Feb. 2010]

[14] G. Mapp, F. Shaikh, M. Aiash, R. Porto Vanni, M. Augusto, and E. Moreira," Exploring Efficient Imperative Handover Mechanisms for HeterogeneousWireless Networks",International Symposium on Emerging Ubiquitous and Pervasive Systems (EUPS-09) August 2009.

[15] ITU-R M.1645, "Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000," 2003. http://electronics.ihs.com/document/abstract/BNCFEBAAAAAAAAA. [Accessed 16. Feb. 2010].

[16] UMTS World. 2002. Overview of The Universal Mobile Telecommunication System. [Online] (Updated July, 15, 2002). Available at: http://www.umtsworld.com/technology/overview.htm. [Accessed 20 Nov 2009].

[17] Institute of Electrical and Electronics Engineers. IEEE 802.21/D8.0, Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services, December 2007.

[18] Handover keying working group (hokey wg). Internet Engineering Task Force. http://www.ietf.org/html.charters/hokey-charter.html [Accessed 16. Feb. 2010].

[19] B. Aboba, L. Blunk, J. Vollbrecht, and J. Carlson. RFC 3748, "Extensible Authentication Protocol (EAP)". Internet Engineering Task Force, June 2004. http://www.ietf.org/rfc/rfc3748.txt. [Accessed 16 Feb 2010].

[20] H. Ballani, Y. Chawathe, S. Rat. nasamy, T. Roscoe, and S. Shenker, "Off By Default!", in Proceedings of the Fourth Workshop on Hot Topics in Networking (HotNets-II), College Park, MD, USA, pp. 1-6. November 2005.