Security and Authentication Concepts for UMTS/WLAN Convergence

F. Fitzek M. Munari V. Pastesini S. Rossi L. Badia
Dipartimento di Ingegneria, Università di Ferrara,
via Saragat 1, 44100 Ferrara, Italy
frank@fitzek.net, {mmunari,vpastesini,srossi,lbadia}@ing.unife.it

***Abstract*— For a fast return of investment, network providers have to offer new services for the upcoming 3G mobile communication systems. Unfortunately 3G systems suffer by high installation costs and low quality of services in terms of high delays and low bandwidth. These drawbacks exclude many promising services such as real–time video conferences and multi–player gaming. Furthermore, high network installation costs inhibit quick growth and in turn slow down the recruiting of new customers. Therefore the convergence of 3G technologies with the beneficial wireless local area networks gained a lot of interest lately. Different architectures were introduced to combine these two technologies. The architectures differ in their security concepts. In this paper we give an overview of the discussed architectures and extend them by multi–hop capability in the WLAN network. Multi–hop will decrease the network installation costs furthermore and ease the installation of network components.**

I. Introduction

THE goal of this paper is to highlight the potentials of UMTS/WLAN convergence from the network provider's view. For a fast return of investment, network providers have to offer new services for the upcoming 3G mobile communication systems to convince the customer to upgrade their 2G terminals. To achieve a high acceptability of this technology these service has to be accessible in many places. This would lead to further costs for the network provider. Furthermore 3G networks suffer by high installation costs and low QoS in terms of high delays and low bandwidth. These drawbacks exclude many promising services such as real–time video conferences (because of the bandwidth requirements [1]) and multi–player gaming (because of the delay requirements [2]). These services can be offered with WLAN systems, which offer high data rates in an unlicensed frequency band. Further improvements for WLAN systems are on their way to support even quality of service (QoS) [3]. Therefore the convergence of 3G technologies with WLAN gained a lot of interest lately. Different architectures were introduced to combine these two technologies. The architectures of combined use of these technologies differ in terms of security concept and network provider structure.

For ease of installation and to reduce the network costs, we advocate the use of multi–hop capability in the WLAN network. There are several scenarios for which a coupled WLAN/UMTS architecture might be useful in order to simplify both installation and maintenance, as long as it improves the placement of the backbone structures. In [4] several kind of ad-hoc scenarios are identified and discussed, and their business aspects are emphasized. They include, but are not limited to, airports, trains, service areas, eHomes, policy and firefighters. The general scenario can be described as in Figure 1 Here, some access points will be connected via wire to the Internet. Other access points are acting as wireless router. These wireless routers (or even virtual access points) can be installed at any place where a power supply is available (e.g. lamps, illuminated advertising, electronic signs). By means of the wireless routers coverage extension is achieved. It is also possible to use customers' terminals to forward packets. The wireless routers are needed to overcome the critical density needed to achieve full connectivity.

This work is organized as follows: in Section II we describe in a detailed manner the possible approach to integrate UMTS and WLAN technologies. In Section III we present the issue of security. Section IV discusses, as a practical example, the EAP-AKA authentication procedure and finally Section V presents the conclusions.

II. Architecture

In the following we presented the possible approaches for the architecture as they are described in [5]. Each one presents its own pros and cons, which are summarized in Table II. In the following, we introduce a detailed description of each approach. The approaches can be mapped directly to the six scenarios given in [6].

Scenario	1	2	3	4	5	6
common billing and care	yes	yes	yes	yes	yes	yes
3GPP access control/charging	no	yes	yes	yes	yes	yes
PS services	no	no	yes	yes	yes	yes
service continuity	no	no	no	yes	yes	yes
seamless service continuity	no	no	no	no	yes	yes
PS services	no	no	no	no	no	yes

TABLE I
WLAN SCENARIOS

A. No or open coupling approach

This scenario (referred to Scenario 1 in [6]) involves two independent networks that may belong to different operators, which obviously must have a previous agreement on the issue. This networks share only the billing and charging system, each operator maintains its own access network interfaces,

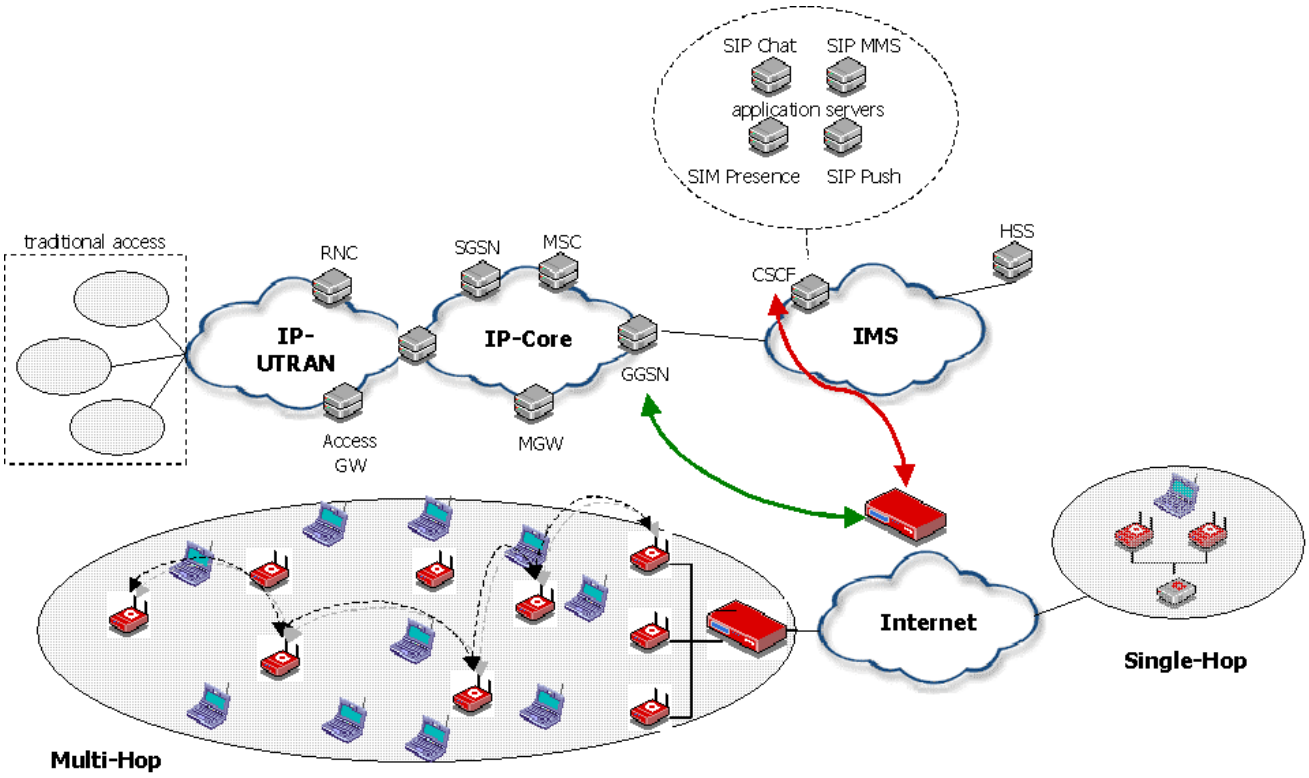

Fig. 1. Multi–Hop WLAN Network with UMTS connection.

independent authorization and authentication procedures, and IP address allocation. The billing system (CCBS) is the only link between two independent access networks (WLAN and RAN). We can talk about integrate customers care that means, for users, only one bill for the usage of 3G and WLAN services. Customers can access only to the Internet services through the WLAN but not to the 3G services, so there are no new requirements on UMTS specifications.

B. Loose coupling approach

In this architecture (referred to Scenario 2 in [6]), the operator of both networks could still not be the same. However, in contrast to the open coupling, also some features like the AAA-HLR (authentication, authorization and accounting) databases and policies are shared, and maintained during the handover process. Access technologies remain differently managed, e.g., with Mobile IP. The AAA-HLR link requires standardization (Radius/Diameter). The access to the WLAN can be obtained with a minimum effort, both for the subscriber and the operator, as the access control principles are 3G. Users can have WLAN and UMTS services using separate session, though with the same hardware (3G user profile include WLAN access). WLAN offers still the same set of services including Internet access, but it is more secure thanks to the authentication through 3G account (not only user name and password).

C. Tight coupling approach

This approach (referred to Scenario 3-5 in [6]) can be used only when both WLAN and UMTS networks belong to the same operator. Here, IP addresses at the mobile node can be maintained as well as AAA policies, QoS guarantees and so on. It is also possible that a micro-mobility protocol is used to manage a handover just as a change in the point of attachment to the network. WLAN and UMTS have two different kind of RAN, so WLAN is connected through border router to SGSN. Seamless handover between UMTS and WLANs as well as, WLAN access similar to UTRAN (3GPP radio protocols). As an effect, this approach requires additional standardization versus loose coupling. UMTS connection is only used for voice service but it can also be used for packet switched signaling (establish and manage packet switched connection). The existing GPRS signaling protocol can be used for establishing bearer data path through WLAN network. This kind of integration needs changes in GPRS procedure implemented at SGSN to distinguish if PS bearer paths are set-up through UMTS RNS or WLAN. WLAN is another radio access technology offered by the same mobile operator.

We can recognize three different steps of integration in this approach. In the first degree, 3G system PS based services are simply extended to the WLAN. This scenario allows access to all services, even though only a subset of the services is actually provided. Service continuity between the 3G system part and the WLAN part is not required. In the second case, service continuity is granted. This means that all the services supported survive a change of access between WLAN and 3G

TABLE II
COMPARISON OF DIFFERENT ARCHITECTURES

Approach	Advantages	Disadvantages
No Coupling (Common Billing and Customer Care)	Suitable for all WLAN technologies Rapid introduction No impact on GGSN nodes	Poor handover performance between UMTS and WLAN No common subscriber database
Loose Coupling (3G system based Access Control and Charging)	Common databases simplifies security and billing customers management No impact on GGSN nodes Suitable for all WLAN technologies	Poor handover performance between UMTS and WLAN
Tight Coupling (Access to 3G system PS based services)	Improved handover performance WLAN load does not affects UMTS UTRAN nodes	WLAN needs support the complete UMTS interface Only feasible if single operator is running both network SGSN and GGSN need to be updated to be able to handle the higher bit rates supported in the WLAN network Reimplementation of RNC functionality
Very tight Coupling	Reuse of RANAP	RNC must handle WLAN load

systems. We can have service continuity, no need to reestablish the service, but not for all service and not with the same QoS, because of the mobility between networks with different capabilities and characteristics of radio access technologies. Finally, we can integrate WLAN and UMTS so that seamless services continuity is ensured. This means that the integration is optimized, by reducing data loss and break time during changes of access technologies. It is now possible to maintain multimedia sessions, without changes in QoS, when customer leaves WLAN coverage areas.

D. Very tight coupling approach

This architecture (referred to Scenario 6 in [6])is similar to the former *Tight coupling approach*, but here WLAN APs are connected to the RNC of UMTS UTRAN. The WLAN is managed at the RNC level like other UMTS cells. Clearly this approach requires complex revision of radio procedures implemented at RNC, due to different UMTS and WLAN radio interfaces. Customers do not perceive from the usage of its equipment the difference between approach based on SGSN or RNC. Yet, a practical implementation of this kind of connection would be probably very slow. In fact, handover to UMTS SGSN need to recreate mobility state, acquire session PDP and RAB context. Even though GGSN still remains the gateway to the Internet, it on the other hand does not have this kind of information, that has to be required. For our purpose of security investigation, this approach does not present nothing more than the previous one, thus it can be seen in the same way as the *Tight coupling approach*.

III. SECURITY

The different architectures are analyzed from the security's point of view. The security concept is rather wide but the following objectives are identified as main in relation to user security features:

- user and network authentication (mutual authentication)
- key management
- services authorization
- integrity protection

The WLAN and the 3G network have different databases and authentication procedures. The authentication, authorization and accounting (AAA) register contains WLAN subscriber's profiles, whereas Home Location Register (HLR) contains all subscriber service authentication information.

The *No Coupling* scenario keeps the registers of the WLAN and the 3G network separated, such that each network manages its own security. Many omnipresent WLAN systems are not very secure and need to support a stronger security scheme. Therefore further improvements, such IEEE802.1x [7] at this level has to be done as shown in [8].

For the *Loose Coupling* approach it is possible to provide a higher level of security by combining the AAA databases. The elements of both networks are still the same, the changes are minimized, but the user should have the same security level for WLAN access as for 3G network access. This is an attractive aim for the subscribers and also for the operators. This integration level has tried to the customer may be capable of WLAN access only, or both WLAN and UMTS system access. If both networks are managed by different providers a pre-established agreement between those providers is necessary to guarantee an easy access, connectivity, and billing. To transport the authentication signaling between the two networks the extensible authentication protocol (EAP) can be used. EAP is a generic protocol that allows different authentication mechanisms (called EAP methods) to be transported.

Between the Access Point (AP) and the access server (AS) EAP messages are typically encapsulated in an AAA protocol, e.g. in RADIUS or Diameter. RADIUS [9], which is the standard IETF protocol, and Diameter Base Protocol [10], which is foreseen to replace RADIUS, can be used by a WLAN AAA procedure, and also be reused to accommodate legacy WLAN access networks. EAP packets can be transported over different protocols by Diameter EAP Application [11], and transported also over the interface between WLAN and 3GPP AAA server. After EAP packets are encapsulated., all informations and data to execute the authentication are retrieved from HLR. This procedure, through exchanges of challenge-response (EAP Request and EAP Response messages), reuses the algorithms of authentication, authorization and encryption of UMTS. In case a customer is a WLAN subscriber and also a UMTS subscriber at the same time, authentication procedure shall

rely on USIM based authentication mechanism. An example of USIM-based authentication procedure is EAP-AKA [5] whose detailed description is given in Section IV.

Finally, in the *Tight Coupling* and *Very Tight Coupling* approaches, the fact that the WLAN and UMTS operators are the same subject implies an advantage in the security issue management. In particular, each subscriber can gain access to the two technologies equivalently. The identification procedures can be decided from the operator with the desired degree of protection. However, it is desirable that the security is addressed similarly, which complicates the access from the WLAN terminals.

IV. USIM SOLUTIONS AND UMTS AKA

In *Loose coupling* architecture, the two AAA databases are connected and so they can exchange information concerning the customer. This inter–working between two registers arise in order to grant a greater level of security to the procedure of authentication within WLAN, traditionally less secure. The scenario is rather critic, because WLAN network is subject to many types of attack, that may have implication on the 3G assets. To assure the same level of security to both networks is an attractive project for the subscribers and also for the operators.

We assume to have the following scenario. An IEEE802.11 enabled access point is present, with fixed connection to the Internet. This access point is under the control of the network operator and can be seen as the access to the home network. A subset of the wireless and mobile terminals can transmit directly to the access point. The remaining terminals might use the multi hop capability of terminals or Virtual Access Points (VAP) [4] which are already connected to the home network. For the following example, we assume that we have one access point with a wired connection and an already established and secure multi hop network as given in Figure 2. Note that the wireless terminals in the multi hop network can either be virtual access points or other customers that are connected to the multi hop network.

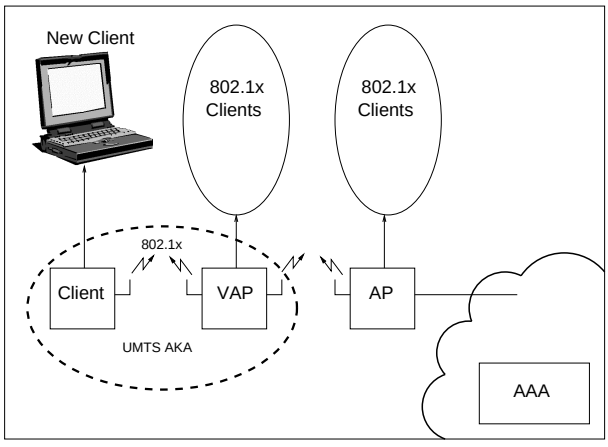

Fig. 2. Multi–Hop WLAN Network with VAP and UMTS–AKA.

Let us assume that EAP authentication is transported to a UMTS server by Diameter Extensible Protocol Application. EAP packets are encapsulated within Diameter messages as specified in Diameter EAP application. This procedure,through a exchange of messages (EAP Request, EAP Response messages), reuse the algorithms of authentication and encryption of UMTS, based on USIM. So it is necessary that a USIM card. However, requiring USIM based authentication does not mean that the USIM needs to be included in the WLAN card, for example the WLAN device can be linked with a UE supporting a USIM via, for example Bluetooth, Irda, USB or serial cable.

Different solutions are proposed to a USIM approach:

- By WLAN device communicating with UICC (e.g. via Bluetooth or IrDA port)
- External UICC card reader
- Dedicated UICC card reader within the WLAN card
- Storing UICC Data securely in software on the device (implementing a ”Virtual SIM”).

Using a USIM for access credential storage and authentication of a subscriber in a WLAN interworking with 3GPP system has a lot of advantages due to its being independents of the hardware and related to a very large distributed subscriber base, allowing continuity of services and roaming. An attractive approach is the definition of a WLAN independent application in the UICC (UMTS integrated circuit card). It is possible to build a WLAN specific UICC application, called WSIM, independent of other applications residing on UICC. A reference can be found in a 3GPP document [12], which already talks about the definition of WSIM. The WSIM can be combined with USIM and ISIM for a complete subscription to a 3G services or it can be stand-alone application, in case a WLAN subscriber is not access allowed on UTRAN. A WLAN specific application on UICC is important for a lot of reasons, which in particular include:

1) Independency of access credentials
   Access credentials can be shared between USIM and WLAN but also the operator can choose to differentiate the access rights.
2) Specificity of WLAN authentication algorithms
   It is necessary a specific authentication function implemented on the UICC to execute the whole EAP based authentication. If UICC only execute the standard USIM commands the security of the system can be compromised; UICC can use, e.g., UMTS AKA internally, but a specific algorithm can also be used.
3) Protection of USIM data
   When a specific WLAN application is used for interworking scenario and not USIM,it is possible to protect USIM data from the outside world because only the data needed in the WLAN situation can be filtered through this independent application, USIM itself remaining offline.

By this solution each subscriber has a NAI (Network Access Identifier), that can be derived from the IMSI, in which case this data element is shared with the USIM, but it can also be defined for a WLAN access, so it is stored independently in WSIM. Then WSIM can hide the real NAI, easily spied when

the client is connected to the Internet, by using a temporary NAI. It is possible also a backward compatibility with GSM, when a GSM subscriber hasn't a UICC card with a USIM applications (EAP/SIM procedure).

WLAN connection is established with a wireless LAN technology specific procedure. Then the user equipment sends an identifier, the so called Network Access Identifier (NAI), that contains either a temporary identifier allocated to UE in previous authentication or, in the case of first authentication, the International Mobile Subscriber Identity (IMSI). When the user has been authenticated, through the information retrieved from HLR, a new pseudonym are chosen, encrypted and saved by the UE to the next authentication. This procedure is very attractive because it is possible to use and adapt the UMTS Authentication and Key Agreement (UMTS-AKA). In [8] we introduced security and authentication approaches for WLAN using the UMTS–AKA protocol.

UMTS Authentication and Key Agreement (UMTS–AKA) specified in [13] protects the integrity of connection and realizes a key distribution mechanism. It is mainly based on a challenge–response mechanism, and in contrast to GSM–AKA it enables mutual authentication. In Figure 2 it is also highlighted where to apply UMTS–AKA in the scenario previously introduced. UMTS–AKA works in the following manner. The mobile terminal and the home environment agree on a secret key identifying the terminal. Whenever a Visitor Location Register (VLR) or Serving GPRS Support Node (SGSN) wants to authenticate the terminal, they convey a request of authentication data to the HLR. The HLR computes a set of authentication vectors and sent it back to the VLR/SGSN. After this exchange, the VLR/SGSN sends an authentication request to the terminal, including the Random Challenge (RAND) and the Authentication Token (AUTN). With this information and its private key (only now to this terminal and the home network), the terminal knows that this message was produced by the home network and retransmits the authentication response. By means of this information exchange the terminal is able to compute confidentiality key (CK) and integrity key (IK), while the VLR selects a CK and an IK.

A WLAN specific application on UICC is important for a lot of reasons. The first one is the independency of access credentials, which can be shared between USIM and WLAN. However, also the operator can choose to differentiate the access rights. Moreover, for the WLAN, a specific authentication function implemented on the UICC is necessary to execute the whole EAP based authentication. If UICC only execute the standard USIM commands the security of the system can be compromised; UICC can use UMTS AKA internally, but a specific algorithm can also be used. Finally, the USIM data must be protected. When a specific WLAN application is used for interworking scenario and not for USIM, it is possible to protect USIM data from the outside world, because only the data needed in the WLAN situation can be filtered through this independent application, USIM itself remaining off-line.

Applying this solution each subscriber has its own NAI, that can be derived from the IMSI. In this case the data element is shared with the USIM, but it can also be defined for a WLAN access, so it is stored independently in WSIM. The WSIM hides the real NAI, easily spied when the client is connected to the Internet, by using a temporary NAI. Backward compatibility with GSM is possible, when a GSM subscriber has not an UICC card with an USIM applications.

V. Conclusions

In this work we present an overview of the security issue for the UMTS/WLAN convergence. We have shown that such an integration is feasible, with the advantage of highly simplifying the installation and deployment procedure by means of multi-hop capability. On the other hand, several design choices have to be made, by involving at the same time to cut different points of trade-off. In particular, the non trivial task of guaranteeing an appropriate security degree has to be correctly addressed. As an example, the implementation of the UMTS-AKA has been discussed in detail as a promising way to manage security in loose coupled UMTS and WLAN networks.

References

[1] F. Fitzek and M. Reisslein, "MPEG–4 and H.263 Video Traces for Network Performance Evaluation," *IEEE Network*, Volume 15, No. 6, pages 40–54, 2001.

[2] F. Fitzek, A. Köpsel, A. Wolisz, M. Reisslein, M. A. Krishnam, "Providing Application–Level QoS in 3G/4G Wireless Systems: A Comprehensive Framework Based on Multi–Rate CDMA," *Proceedings of IEEE International Conference on Third Generation Wireless Communications*, pages 344–349, 2001.

[3] IEEE 802.11 WG, "Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS)," *Technical Report*, IEEE 802.11e/D3.0, 2002.

[4] F. Fitzek, P. Seeling, M. Reisslein, "Reference Models and Related Business Cases for Ad-Hoc Networks," *Proceedings of Wireless World Research Forum 6 (WWRF6)* Section WG4, 2002.

[5] 3GPP TS 23.234, "WLAN Subsystem", *Technical Report*, 3rd Generation Partnership Project, 2002.

[6] 3GPP TR 22.934, "WLAN Subsystem", *Technical Report*, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Feasibilty study on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 6) 2002-12.

[7] IEEE802, "Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control", *IEEE 802.1X-2001*, 2001.

[8] F. Fitzek, A. Köpsel, P. Seeling, "Authentication and Security in IP based Multi–Hop Networks," *Proceedings of Wireless World Research Forum 7 (WWRF7)*, Volume 1, Section WG3, 2002.

[9] 10 C. Rigney *et al.*, "Remote Authentication Dial In User Service (RADIUS)", *Technical Report*, IETF, RFC 2138, 1997.

[10] IETF, "Diameter base protocol," draft-ietf-aaa-diameter-17.txt.

[11] IETF, "Diameter Extensible Authentication Protocol (EAP) Application," draft-ietf-eap-01.txt.

[12] 3GPP TSG SA WG3 Security, "Use of smart cards in WLAN interworking," *Technical Report*, 3rd Generation Partnership Project, 2002.

[13] 3rd Generation Partnership Project, "Security Architecture", 3GPP TS 33.102 V5.0.0, Release 5, 2002.
`ftp://ftp.3gpp.org/specs/latest/Rel-5/33_series`