Interworking Security in Heterogeneous Wireless IP Networks

Wenhui Zhang
University of Stuttgart, Institute of Communication Networks and Computer Engineering
IKR, Pfaffenwaldring 47, D-70569 Stuttgart, Germany
E-mail: zhang@ikr.uni-stuttgart.de

***Abstract*– With the exponential growth of the Internet and the wide deployment of cellular networks, there is a trend to integrate the Wireless LAN (WLAN) and cellular networks. As the network evolves, it is believed that in the future, there will be all-IP based wireless networks, and the interworking will be based on an IPv6 platform. For the interworking of UMTS and the WLAN, and providing Mobile IP service across administrative domains, a generic AAA architecture and mechanism are needed. In this paper, the security requirements for Mobile IPv6 and its deployment across administrative domains are presented. The proprietary authentication and key derivation mechanisms for UMTS, the WLAN and the Internet are introduced. It is proposed that authentication for the interworking be performed on the IP layer, and both IP layer and link layer key materials be derived after authentication. In addition, it is revealed that Context Transfer protocol has its limitations for handover in heterogeneous networks, and accordingly re-authorization and new link layer key derivation procedures have been proposed.**

Key words: AAA, Security, Heterogeneous networks, Handover

I. INTRODUCTION

The second generation (2G) wireless systems have been a great success in the last decade. A mobile user, having a single contract with a service provider, can have network access either from his home service provider or other service providers, which is supported by the roaming agreement between service providers. Paying a single bill and having services at any-time, any-where provide users great convenience and partly account for the success of cellular systems.

With the exponential growth of the Internet and the wide deployment of cellular networks, wireless Internet is becoming a reality. Owing to the limited bandwidth and expensive service price of cellular networks, there is a trend to integrate the Wireless LAN (WLAN) and cellular networks, which will provide users with any-time, any-where connections as well as high speed and low cost data services within limited coverage areas.

As the network evolves, it is believed that in the future, there will be all-IP based wireless networks, and the convergence of different technologies will be based on a common IP platform [1]. There is active research work on IPv6 based wireless networks, an all-IP wireless network architecture based on IPv6 is currently being developed and implemented by the IST project Moby Dick [2].

In the future, having a service contract with the home network, a mobile user with a multi-technology terminal can have Internet access using various access technologies both in the home and foreign networks, independent on user location. This requires a mobility management protocol, that can route user data independent on user location. This problem has been well solved by Mobile IP [5], which has been developed to enable a mobile node to roam freely between IP networks. To extend Mobile IP for business operation across administrative domains, Authentication, Authorisation and Accounting (AAA) are considered necessary [12]; that is, in order to use local resources from a foreign network, a mobile user has to be authenticated and authorized locally. There is currently active research work in this area in IETF. A generic AAA architecture [10] has been proposed, and Diameter Base Protocol [14] has been specified as an AAA framework for applications.

For mobile Internet access, certain security associations are considered necessary. For example, Mobile IPv6 mandates the use of IPsec [9] to protect the integrity and authenticity of Binding Updates and Acknowledgements [5]; Mobile IP AAA Requirements [11] require security associations between a mobile terminal and the local and AAA home server. Usually, it is difficult to pre-establish all these security associations, and they have to be dynamically established.

To enable the convergence of different wireless technologies in an IP network, link layer security for wireless access is also indispensable. UMTS and the WLAN each has its own mechanisms for authentication and link layer security [3][25]. The author argues that link layer security is imperative for wireless network access no matter how well higher layer security mechanisms work.

The problem arises how to efficiently carry out mobility and AAA procedure, considering both IP and link layer security for wireless network access across administrative domains; and how to make the influence of security mechanisms on handover minimal. This is the focus of this paper, and it is organised as follows. Section II gives an overview of Mobile IPv6 and its AAA security requirements. Section III reviews the state-of-the-art authentication and key management of UMTS, WLAN 802.11 and the Internet. Section IV

proposes the authentication and security key derivation mechanism for interworking. Section V presents new handover signalling for interworking. Section VI concludes this paper.

II. Mobile IP and AAA security requirements

A. Mobile IP

Mobile IPv6 has been developed to enable a Mobile Node (MN) to maintain its connectivity to the Internet when moving from one Access Router (AR) to another. In Mobile IPv6, a MN is expected to be addressable at its home address, which is an IP address with the prefix from its home network. While a MN is attached to a foreign network away from home, it configures a Care-of Address (CoA), an IP address that has a subnet prefix from the local network, and sends a Binding Update message to register its CoA with a router called Home Agent (HA) in its home network. The HA replies to the MN by returning a Binding Acknowledgement message. Thus, when packets are sent to the home address of the MN, they can be redirected by the HA to the CoA of the MN, and a MN can maintain its connectivity when away from home. But there is a period during handover while a MN is unable to send or receive packets due to link layer switching and protocol operations. In order to provide seamless mobility, Fast handovers [6] and Hierarchical Mobile IP [7] have been proposed as extensions to Mobile IPv6 in order to reduce the handover latency and packet loss.

B. AAA infrastructure and protocols

To extend Mobile IP for business operation across administrative domains, AAA are considered necessary [12]. When a mobile user needs to access resources provided by an administrative domain other than his home domain, he has to be authenticated locally in order to make sure he is the right user, authorised to use resources he is entitled to, and accordingly be charged for the service.

Although in cellular networks, e.g. GSM and UMTS, the mobility and AAA problem are well solved and the algorithms are widely used, they are still at its inception phase in the Internet. There is currently active research work on AAA. IRTF AAAarch Research Group has proposed a generic AAA architecture [10] in order to support a wide variety of applications, which require AAA functionality and operate in a multi-domain environment. In such an architecture, generic AAA servers are deployed in different domains, which are capable of authenticating users, handling authorization requests, and collecting accounting data.

Mobile IP AAA Requirements [11] describe an infrastructure enabling AAA servers to authenticate and authorise network access requests from MNs. A MN belonging to its home domain requires resources in a foreign domain by providing some credential to a local attendant. The attendant consults the local AAA authority (AAAL) for proof of the credentials using a secure channel. The AAAL may not have enough

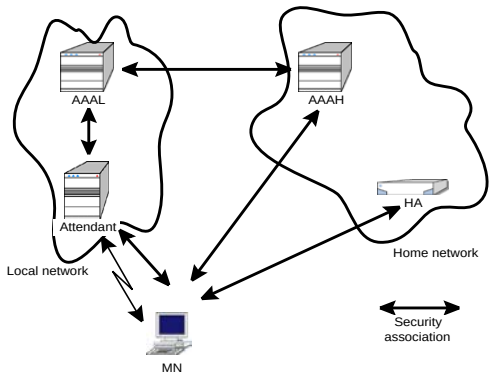

Fig. 1. Mobile IP AAA model and security associations

information to verify the credentials, it will contact an external authority, the MN's home AAA server (AAAH), to obtain necessary information. The current widely deployed AAA protocol is RADIUS [13], which was initially designed to provide dial-up Point-to-Point Protocol (PPP) and terminal server access. But it has certain limitations to be used as an AAA protocol [15]. A new AAA protocol Diameter [14] is designed to provide an AAA framework for applications such as network access or IP mobility, which is considered acceptable as an AAA protocol [15]. Its extension for Mobile IPv6 [16] has also been proposed.

C. Security association requirements

For the deployment of Mobile IP in a commercial environment, security can never be overemphasized. IPsec [9] provides the capability to secure communication across the Internet. A key concept for the authentication and confidentiality mechanism in IPSec is security association, which is a one-way relationship between a sender and a receiver, and offers security services to IP traffic. In order to have IPSec, secret keys have to be generated and distributed to communication partners manually or using protocols, such as IKE [17].

Mobile IPv6 specifies a security model and mandates the use of IPsec to protect the integrity and authenticity of Binding Updates and Acknowledgements [5] between a MN and its HA. In addition, Mobile IP AAA Requirements [11] also require security associations as depicted in Fig. 1. The data communicated between the AAAL and local attendant can be assumed via a secure channel, because they are in the same domain. It can also be assumed that there exists a long-term secret key shared by the MN and the AAAH owing to the service contract. The communication between the AAAL and the AAAH can be protected by a pre-established secure channel thanks to the roaming agreement between the two domains. For the security association between the MN and the HA, Mobile IPv6 requires manual and also allows automatic key management with IKE. However, manual configuration is not scalable, and IKE for Mobile IP requires many message exchanges between the MN and HA [8]. Moreover, it is also difficult to pre-establish the security association

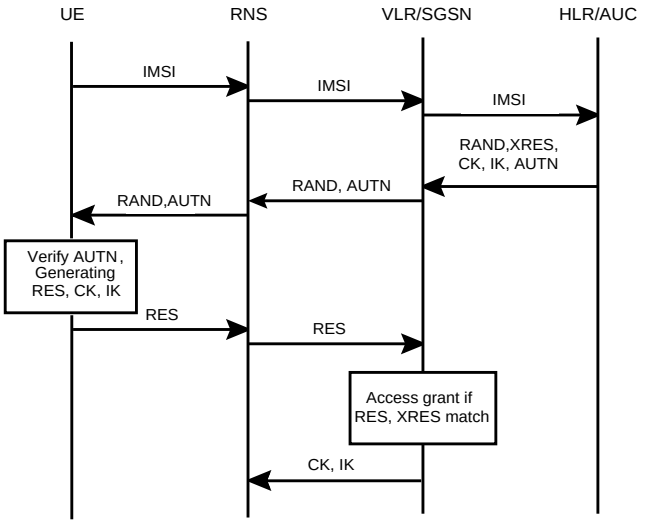

Fig. 2. UMTS authentication and key agreement

between the MN and the local attendant, therefore, it has to be dynamically established upon request.

III. STATE-OF-THE-ART

After discussing the Mobile IP and AAA security requirements. In this section, the state-of-the-art authentication and key management methods of UMTS, the WLAN and the Internet are presented.

A. UMTS

UMTS achieves mutual authentication of a user and the network based on a challenge-response and a sequence number-based protocol [3]. It uses a long-term secret key K, which is shared between and available only to the User Services Identity Module (USIM) in the User Equipment (UE) and the Authentication Centre (AuC) in the user's Home Environment (HE). Initially, the International Mobile Subscriber Identity (IMSI) is sent from the UE unprotected to Visitor Location Register (VLR)/Serving GPRS Support Node (SGSN) via the Radio Network System (RNS), and further forwarded to the Home Location Registor (HLR) of the UE. In the HE, authentication vectors are generated, each vector consists of a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. The authentication vectors are sent to the VLR/SGSN, and the RAND and AUTN from one vector are forwarded to the UE. The UE will authenticate the network using the AUTN. If authentication is successful, it will compute a response RES, a cipher key CK, and an integrity key IK using the secret key K and RAND. Authentication of the user is successful if the XRES and the RES from the user are the same. CK and IK will then be forwarded to the RNS to be used as the cipher and integrity key. The authentication procedure is depicted in Fig. 2.

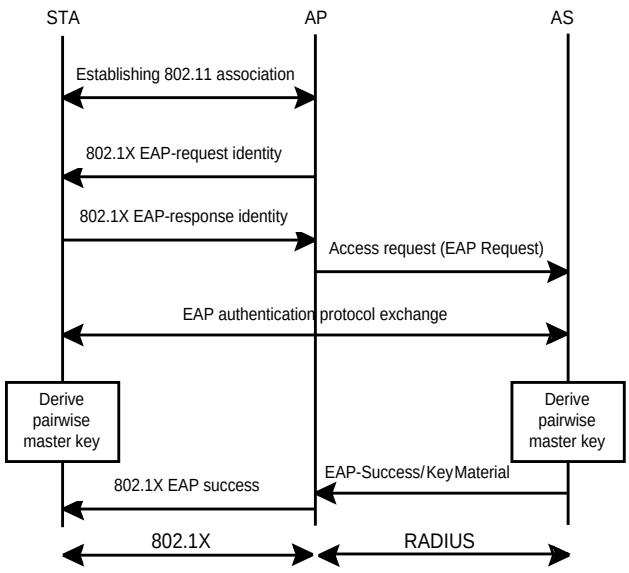

Fig. 3. 802.11i authentication

UMTS security keys CK and IK are derived during authentication by both the UE and the network. They belong to the conventional cryptography type [18], that is, both the sender and the receiver share the same secret key. Most control signalling information elements sent between the MS and the RNS are considered sensitive and are thus integrity protected using the integrity key IK. User data and some signalling information elements considered sensitive are confidentiality protected using the secret key CK. After handover, the security keys remain unchanged.

B. 802.11 WLAN

The initial WLAN 802.11 security mechanism has design flaws [24]. The new IEEE WLAN standard 802.11i is currently being standardized to improve the security [25]. Authentication of 802.11i involves three entities: the wireless station (STA), the Access Point (AP), and the Authentication server (AS). The authentication procedure is composed of two operational phases: establishing the 802.11 association, and 802.1X EAP [26] authentication, as illustrated in Fig. 3. During the first phase, a STA is associated with an AP, and the security capabilities of the AP are discovered. The authentication phase uses Extensible Authentication Protocol (EAP) [19] as the carrier for its authentication method, and the STA and AS are mutually authenticated. EAP is an authentication framework which supports different authentication methods. It supports key derivation using a key hierarchy in order to provide key materials for the subsequent key derivation.

The hierarchical key architecture also applies to 802.11i. In the authentication phase, both the AS and STA generate a Master key (MK) as a positive indication of the authentication, and further derive a Pairwise Master Key (PMK) to be used by the STA and its AP. After authentication, a four-way

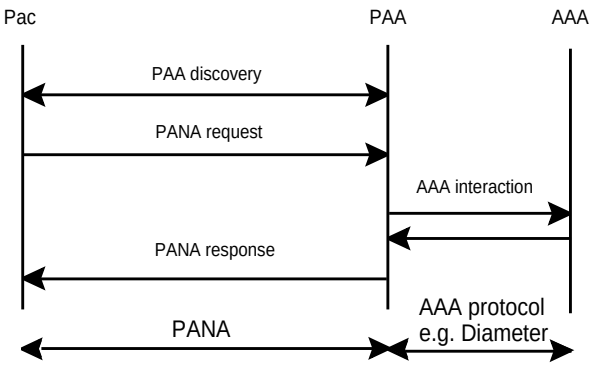

Fig. 4. Protocol for Carrying Authentication for Network Access

handshake is performed between the STA and its AP and a Pairwise Transit Key (PTK) is further derived from the PMK, and used by the STA and the AP to protect group key distribution as well as data transfer. 802.11i also provides several methods for data confidentiality, origin authenticity and replay protection.

Because the PMK is bound to the STA and AP, when handover happens, a new PMK has to be derived and distributed to the STA and the new AP. In order to expedite the handover process, 802.11i also proposes a link layer pre-authentication mechanism, i.e. a STA can get authenticated with multiple APs before handover happens. After handover, the STA and the new AP use a four-way handshake to derive a new PTK.

C. Internet

Mobile IP and AAA protocols enable mobile users to obtain services across different domains. Diameter is an AAA protocol between AAA servers and clients, it does not specify any particular mechanism for the network access authentication between a MN and an AAA client. IETF Protocol for Carrying Authentication for Network Access (PANA) working group aims to design a network layer access authentication protocol [20]. In PANA, the entity wishing to obtain network access is called PANA client (PaC), and the entity to authenticate the PaC and grant network access is called PANA Authentication Agent (PAA). PANA identifies EAP as its payload for carrying various authentication methods, however, does not specify and authentication method. Though EAP typically runs directly over data link layer, PANA enables EAP to run above IP. Fig. 4 shows a simplified PANA message exchange. At the beginning, the IP address of a PAA is discovered and a PANA session is established between a PaC and the PAA. Authentication is performed by transferring EAP messages in PANA messages between the PaC and the PAA. The PAA may interact with a other AAA server to authenticate the PaC by using AAA protocols, such as Diameter.

PANA relies on EAP methods to establish a PANA security association between the PaC and PAA to protect itself. By enabling fast re-authentication, PANA enable a PaC to re-establish the session without going through the whole authentication procedure.

D. Summary

UMTS and WLAN 802.11 each has its own technology specific method for authentication and link layer key derivation. For wireless access, link layer security is indispensable. The reason is that wireless access is especially vulnerable to attacks, thus both link layer signalling and sensitive user data have to be protected. For example, without link layer security, it is easy to launch denial-of-service attack on the link layer, no matter how well the upper layer security mechanisms work. If there is no link layer security in WLAN, an attacker can easily send disassociation packet to a STA or an AP and break the connection between them. Moreover, link layer encryption can also be used to protect IP packets and also hide the IP address of a user.

While UMTS authentication process is in fact a combination of authentication, key derivation and mobility management, these processes are still separate in the Internet. Network layer AAA protocol can be independent on the underlying link layer technology, thus provide a generic AAA method for the interworking of various systems. If network layer AAA protocols are used for wireless access, in addition to the required IPsec, link layer security is also necessary. In principle, IP layer and link layer security keys can be derived in separate processes, and mobility management and AAA procedures can also be decoupled from each other. But the signalling for these procedures will require many round trips to the MN's home domain, which uses a lot of bandwidth, and can lead to a long signalling latency. An optimal solution is to combine mobility management with AAA procedure, and meanwhile derive both IP and link layer security key materials.

IV. Interworking Authentication and Key Derivation

A. A general model

When preforming AAA functionality, the entities involved in UMTS, the WLAN and the Internet show some similarities. Thus AAA for wireless Internet access in an all-IP architecture can be described by a general model. Suppose a supplicant has a service contract with his home network, when he wishes to have network access from a foreign network, he has to be authenticated by the network. The credentials will be sent to a local authenticator, and the authenticator will contact the AAAL for authentication decision. The AAAL may not have enough information to authenticate the supplicant and will again contact the AAAH in the supplicant's home domain. The entities in the general model, e.g. supplicant, authenticator, AAAL and AAAH each has its corresponding realization in different technologies, as outlined in Table I. There is no AAAH for PANA and the WLAN,

because PANA only considers authentication between the user and the access network, and the WLAN does not deal with the home network.

	Supplicant	Authenticator	AAAL	AAAH
Mobile IP	MN	Attendant	AAAL	AAAH
PANA	PaC	PAA	AAA server	
UMTS	UE	RNS	VLR/SGSN	HLR/AuC
802.11	STA	AP	AS	

Table 1: AAA Entities

From the discussion in Section II, the IPsec between the MN and the authenticator, between the MN and the HA have to be dynamically established. In addition, link layer security between the MN and the authenticator is necessary. If link layer security between the MN and authenticator exists, the IPsec between the MN and attendant may not be necessary.

B. Authentication

In future all-IP based interworking scenario, wireless access points will also be IP routers, for example, the architecture developed by Moby Dick [2]. The advantage of IP layer authentication method is that it is a generic method, which can be used for various link layer technologies, and independent on any link layer technology [20]. Therefore, it is suitable for future all-IP based interworking scenario. Considering the state-of-the-art technology, a concatenation of PANA and Diameter can provide IP layer authentication; PANA is used for access authentication between a supplicant and an authenticator, and Diameter is used for the communication between AAA servers and clients.

As shown in Fig. 5, the authentication process for a MN is a concatenation of PANA at the wireless link and Diameter in the network, both carry EAP messages for authentication. When a MN attaches to a network, it discovers the AAA attendant by sending PANA discovery message. Cookies are exchanged in the following messages, which are used to prevent resource consumption attacks. EAP messages are communicated between the MN and its AAA servers during authentication; EAP allows different authentication methods to be used, and it is supported by both PANA and Diameter. The detailed messages depend on the selected authentication method decided by the network. For example, using UMTS Authentication and Key Agreement (AKA) algorithm in EAP messages [23], the MN and the access network are mutually authenticated requiring only one round trip signalling back to the home network. It is a similar procedure as UMTS authentication illustrated in Fig. 2. But the authentication messages exchanged are EAP messages carried in IP packets. Messages are exchanged in the wireless link using PANA, and in the

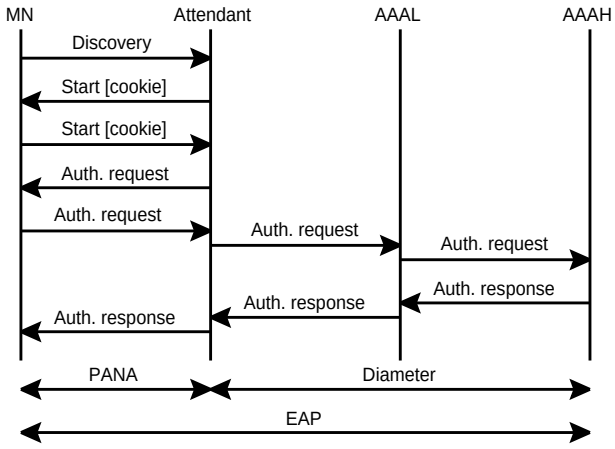

Fig. 5. Authentication signalling

network using Diameter with the help of the AAA infrastructure.

The attendant can be an AR providing Mobile IP service, and also acts as a PaC to communicate PANA messages with the MN, meanwhile, functions as an AAA attendant to communicate with the AAAL. Depending on the wireless technology used, it can preform networking and radio functions either as the RNS in case of UMTS or AP in case of WLAN. If the attendant has a wireless interface with the MN, it also requires link layer security keys to protect the wireless communication.

The authentication scenario mentioned here is a generic network layer approach, independent on any link layer technology. Different authentication methods can be supported thanks to the use of EAP. It requires only AAA infrastructures without extra security authority, thus is flexible and scalable. The AAA infrastructure can also be used to optimise mobility management. For example. Diameter Mobile IPv6 extension [16] uses the AAA infrastructure to support mobility management and to distribute security keys. This in addition requires an interface between the AAAH and AH.

C. Key derivation

Key materials for IPsec required by Mobile IP can be derived using IKE, but it requires several round trips to the home network. Instead, AAA entities can play a major role in key derivation and distribution. Using Diameter to assist key distribution, key materials can be derived using random numbers or Diffie-Hellman mechanism [16]. In order to have secure link layer connection, link layer security keys have to be derived. This can be achieved by combining it with IPsec key derivation.

Both PANA and Diameter use EAP to carry authentication messages, and EAP uses a hierarchical key architecture. The hierarchical key architecture will be beneficial for link layer key derivation, as well as inter-technology handover, which will be discussed in the next section. For example, key deri-

vation based on random numbers is as follows. After receiving the authentication request for a MN from an AAAL in a different domain, the AAAH generates two random numbers, one for the IPsec between MN and HA, and the other for the link layer security key between the MN and the attendant. The AAAH then derives IPsec and link layer key materials using the two random numbers, and the long-term secret and key derivation algorithm shared with the MN. The IPsec key material will be sent to the HA in a secure channel in the MN's home network, and the HA will use the key material to derive inbound and outbound IPsec keys shared with the MN. In the authentication response message, the AAAH sends the AAAL the link layer key material and two random numbers using Diameter messages. And the AAAL will use the link layer key material as an EAP Master Session Key (MSK) to derive a Transient Session Key (TSK) and send the TSK to the attendant for specific link layer cipher. The two random numbers generated by the AAAH will be also be forwarded the in the authentication response message and further sent to the MN. The MN will use these two random numbers and the long-term shared key to derive key material for IPsec with the HA, and also the MSK and TSK.

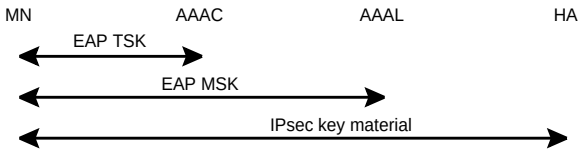

Fig. 6. Derived key material

The proposed scenario is a combination of authentication and key material derivation for both IPsec and link layer. The derived keys are shown in Fig. 6. The MSK is shared between the AAAL and MN as an indication of positive authentication. The TSK is shared between the MN and the attendant, and security keys can be derived from TSK for various link layer technologies. Thus the authentication and key derivation algorithm are independent on the underlying link layer technology, therefore, is suitable for the interworking of heterogeneous wireless networks. This algorithm does not exclude any other key materials derivation, and they can be derived and distributed in the same way when needed. The specific algorithms to derive key material and security keys are out of the scope of this paper.

V. Interworking Handover

A. Requirement

Mobile IPv6 [5] does not deal with how AAA sessions can be re-established in a new network after handover. In order to quickly re-establish the service context after handover, Context Transfer protocol [21] has been proposed by IETF. Service context, such as QoS and AAA context can be transferred from the old Access Router (oAR) to the new Access Router

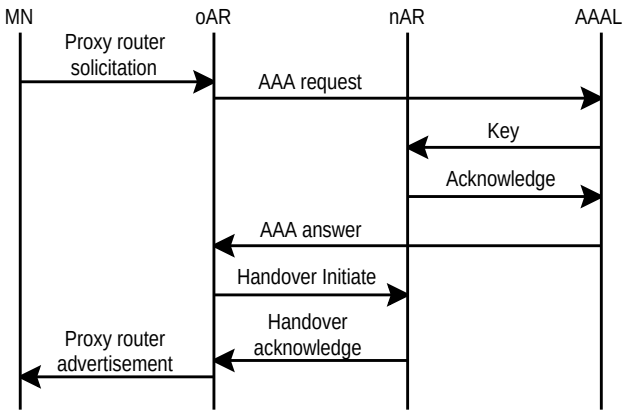

Fig. 7. Inter-technology Fast Handovers signalling

(nAR), and thus the service context can be re-established quickly without requiring the MN to establish it from scratch. For a MN with a CoA in a foreign network, his home address will be used to match the IPsec security policy [5]. Therefore, after handover, the IPsec between the MN and the HA can remain unchanged. In this case, Context Transfer is useful.

But Context Transfer, especially when used for interworking of UMTS and WLAN, has its limitations, because some context information can not simply be transferred, but should be rather renewed after handover. For example, in case of inter-technology handover, due to the different capabilities of the wireless access link, the authorisation in the old access link may not be valid in the new access link, that is, a service allowed using one access technology may not be allowed using another technology. In this case, before handover, the AAA server has to be contacted and new authorization has to be issued for the new access network. In addition, handover, especially inter-technology handover, new security keys for the new link layer technology have to be derived, because the new link layer may use different cryptography algorithm from the old one. It is also necessary that the new keys are independent from the old link layer keys, because by doing so, a compromise in security within one access link will not lead to the compromise in another.

B. Inter-technology Fast Handovers

Since Context Transfer alone will not work for inter-technology handover, extra signalling is required for the re-establishment of AAA context in the new subnet. In order to reduce the handover latency induced by the security procedure, new authorization and link layer keys can be obtained prior to handover. And this procedure can be combined with Fast Handovers proposed by IETF [22], so that seamless handover is possible, as shown in Fig. 7.

Before handover, a MN sends a Fast Handovers Router Solicitation message to the oAR indicating the identity of the nAR to request Fast Handovers support. Before continuing the Fast Handovers procedure, the oAR will first send an

AAA request to the AAAL on behalf of the MN. The AAAL will make new authorization and derive a new TSK using a challenge and the MSK shared with the MN. The AAAL then sends the TSK to the nAR. When an acknowledge is received from the nAR, an AAA acknowledge with the challenge will be sent to the oAR. The oAR then continues the Fast handover procedure by sending a Handover Initiate message to the nAR, and other context information can be embedded in this message. After receiving a Handover Acknowledge message from the nAR, the oAR can send a Fast Handovers Proxy Router Advertisement with the challenge to the MN. The MN can then derive a new TSK using the MSK and the challenge, and continue to execute link layer handover.

It can be seen that By combining the re-authorization and new key derivation with the help of Fast Handovers signalling prior to handover execution, the latency induced in the handover process is kept small, thus seamless handover is possible. In addition, by using EAP hierarchical key architecture, the new link layer key can be derived independent of the old one, and the signalling required is only within the same domain.

VI. Conclusions and future work

To support the interworking of UMTS and the WLAN in all-IP based wireless networks, a generic AAA architecture and AAA mechanism are required. The interworking will be built on a generic AAA architecture proposed by IRTF AAAarch Research Group. Authentication will be performed on the IP layer by concatenating Diameter and PANA and using EAP as the carrier for authentication methods. In addition, by integrating key derivation with the authentication procedure, both IP layer and link layer key materials can be derived. For inter-technology handover, Context Transfer alone is not enough, because new authorization and new link layer security keys have to be obtained for the new network. These procedures can be combined with Fast Handovers signalling, thus the latency induced is kept small.

Currently, a Diameter AAA architecture for Mobile IP users has been implemented in an IPv6 test bed in the University of Stuttgart based on Open Diameter API [27]. Future work will extend this implementation to combine authentication and Mobile IP Binding Update, and also to enable key material derivation for both IPsec and link layer during the authentication process.

Acknowledge

This work is partly funded by the EU project IST-2000-25394 Moby Dick. The author would like to thank Matthias Kabatnik and Christian Hauser for comments on this paper.

References

[1] De Vriendt, J., Laine, P., Lerouge, C., Xiaofeng Xu, “Mobile Network Evolution: A Revolution on the Move,” IEEE Communications Magazine, Apr. 2002, pp. 104 -111

[2] Moby Dick: Mobility and Differentiated Services in a Future IP Network, http://www.ist-mobydick.org, Jan. 2003

[3] 3GPP TS 33.102, V5.1.0 “3G Security: Security Architecture,“Dec. 2003

[4] Draft 3GPP TS 23.234 V1.10.0, “3GPP system to Wireless Local Area Network (WLAN) Interworking; System description,” May 2003

[5] D. Jingoism, C. Parkins, J. Argue, “Mobility Support in IPv6,” IETF draft-ITV-mobiles-ipv6-19.txt, work in progress, Oct. 2002.

[6] Rajeev Koodli, “Fast Handovers for Mobile IPv6,” IETF draft-ietf-mobileip-fast-mipv6-05.txt, work in progress, Sep. 2002.

[7] Hesham Soliman, Claude Castelluccia, Karim El-Malki, Ludovic Bellier, “Hierarchical Mobile IPv6 mobility management (HMIPv6),” draft-ietf-mobileip-hmipv6-08.txt, work in progress, Jun. 2003

[8] J. Arkko, V. Devarapalli, and F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents,“, IETF draft-ietf-mobileip-mipv6-ha-ipsec-06.txt, work in progress, Jun. 2003

[9] S. Kent, and R. Tension, “Security Architecture for the Internet Protocol,“ IETF RFC 2401, Nov. 1998

[10] C. de Last, et al., “Generic AAA Architecture,” IETF RFC 2903, Aug. 2000.

[11] S. Glass, et al. “Mobile IP Authentication, Authorization, and Accounting Requirements,” IETF RFC 2977 Oct. 2000

[12] Charles E. Perkins, “Mobile IP Joins Forces with AAA, “ IEEE Personal Communications, Aug. 2000, pp. 59 -61

[13] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2865, Jun. 2000

[14] P. Calhoun, J. Loughney, E. Guttman, G. Zorn and J. Arkko, “Diameter Base Protocol,“ IETF RFC 3588, Sep. 2003

[15] D. Mitton, M. St.Johns, S. Barkley, D. Nelson, B. Patil, M. Stevens and B. Wolff, “Authentication, Authorization, and Accounting: Protocol Evaluation,” IETF RFC 3127, Jun. 2001

[16] Stefano M. Faccin et al., “Diameter Mobile IPV6 application,“ IETF Internet draft, draft-le-aaa-diameter-mobileipv6-03, Apr. 2003

[17] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," IETF RFC 2409, Nov. 1998

[18] William Stalling, “Network Security Essentials,” Prentice Hall, 2000

[19] L. Blunk, et al., “PPP extensible Authentication Protocol (EAP),“ IETF Internet draft, draft-ietf-eap-rfc2284bis-04.txt, Jun. 2003

[20] D. Forsberg et al., “Protocol for Carrying Authentication for Network Access,“ IETF Internet draft, draft-ietf-pana-pana-01.txt, Jun. 2003

[21] J. Loughney, et al., “Context Transfer Protocol,“ IETF Internet draft, draft-ietf-seamoby-ctp-03.txt, Jun. 2003

[22] Rajeev Koodli, “Fast Handovers for Mobile IPv6,“ IETF Internet draft, draft-ietf-mobileip-fast-mipv6-06.txt, Mar. 2003

[23] J. Arkko and H. Haverinen, “EAP AKA Authentication,“ IETF Internet draft, draft-arkko-pppext-eap-aka-11.txt, Oct. 2003

[24] Arbaugh, W.A., Shankar, N., Wan, Y.C.J., Zhang, K., “Your 802.11 Wireless Network Has no Clothes,“IEEE Wireless Communications, Dec. 2002, pp. 44 - 51

[25] IEEE Std 802.11i/D4.1, “Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements,” Jul. 2003

[26] IEEE Draft P802.1X/D11, “Standards for Local and Metropolitan Area Networks: Standard for Port based Network Access Control,” Mar. 2001

[27] Open Diameter C++ API, http://www.opendiameter.org/diameter-api-html/