Komninos, N. & Dimitriou, T. (2006). Adaptive authentication and key agreement mechanism for future cellular systems. Paper presented at the 15th IST Mobile & Wireless Communications Summit, 04 - 08 June 2006, Mykonos, Greece.

CITY UNIVERSITY LONDON

City Research Online

Adaptive Authentication & Key Agreement Mechanism for Future Cellular Systems

N. Komninos, *Member, IEEE* and T. Dimitriou, *Member, IEEE*

Abstract— **Since the radio medium can be accessed by anyone, authentication of users is a very important element of a mobile network. Nowadays, in GSM/GPRS a challenge response protocol is used to authenticate the user to the mobile network. Similarly, in third generation mobile systems [3] a challenge response protocol was chosen in such a way as to achieve maximum compatibility with the current GSM security architecture. Both authentication mechanisms use symmetric key cryptography because of the limited processing power of the mobile devices. However, recent research [6] has shown that asymmetric, or public, key cryptography can be enabled successfully in future mobile terminals. In this paper, we propose a new adaptive authentication and key agreement protocol (AAKA) for future mobile communication systems. The novelty of AAKA and its main advantage over other challenge response protocols is that can be adaptive to the mobile environment and use symmetric and/or public key cryptography for user and network authentication.**

***Index Terms*—Authentication, GSM, UMTS, Key Agreement**

I. Introduction

The GSM network authenticates the identity of the subscriber through the use of a challenge response protocol [5]. Authentication involves two functional entities, the subscriber identity module (SIM) card in the mobile station (MS), and the authentication centre (AUC) in the network. Each subscriber is given a secret key, one copy of which is stored in the SIM card and the other in the AUC. An overview of the challenge response protocol is shown in Fig. 1.

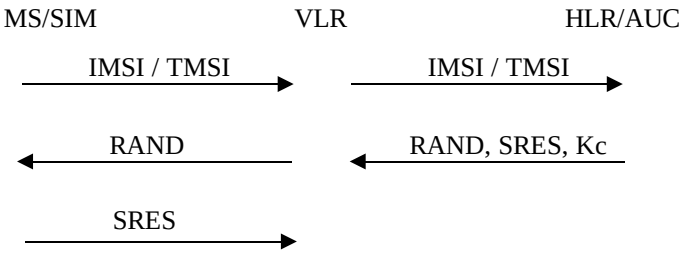

Fig. 1.Authentication and Key Agreement in GSM

N. Komninos is with the Athens Institute of Technology, 19002 Peania, Attiki, Greece (phone: 210-6682801; fax: 210-6682703; e-mail: nkom@ait.edu.gr).

T. Dimitriou is with the Athens Institute of Technology, 19002 Peania Attiki, Greece (e-mail: tdim@ait.edu.gr).

Upon receipt of an international mobile subscriber identity (IMSI) from the visitor location register (VLR), the AUC searches in the database for the corresponding subscribers authentication key (Ki). During authentication, the AUC generates a 128-bit random number (RAND) that it sends to the mobile. Both the mobile and the AUC then use the random number, in conjunction with the subscriber's secret key and the authentication algorithm (A3), to generate a 32-bit signed response (SRES) that is sent back to the AUC. Note that Ki is never transmitted over the radio channel. It is present in the subscriber's SIM, as well as the AUC, home location register (HLR), and VLR databases. If the number sent by the mobile is the same as the one calculated by the AUC, the subscriber is authenticated. Otherwise, if the number does not agree with the calculated one the connection is terminated and an authentication failure indicated to the MS.

Furthermore, the SIM contains the ciphering key generating mechanism algorithm (A8) which is used to produce 64 bit ciphering key (Kc). The ciphering key is computed by applying the same random number (RAND) used in the authentication process to the ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki). In addition, the Kc is used to encrypt and decrypt the data between the MS and VLR.

On the other hand, in the authentication and key agreement mechanism described in 3G security specifications [3], the subscriber and network authenticate each other, and also they agree on cipher and integrity key.

The authentication method was chosen by 3GPP in such a way as to achieve maximum compatibility with the current GSM security architecture and facilitate migration from GSM to UMTS. The method is composed of a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication derived from [4].

The subscriber and the network share a secret key K that is available only to the universal SIM (USIM) and the AUC in the user's home environment (HE). In addition the USIM and the HE keep track of sequence numbers (SQN_{ME}, SQN_{HE}) to support network authentication. The sequence number SQN_{HE} is an individual counter for each subscriber and the sequence number SQN_{ME} denotes the highest sequence

number the USIM has accepted.

An overview of the mechanism is shown in Fig. 2.

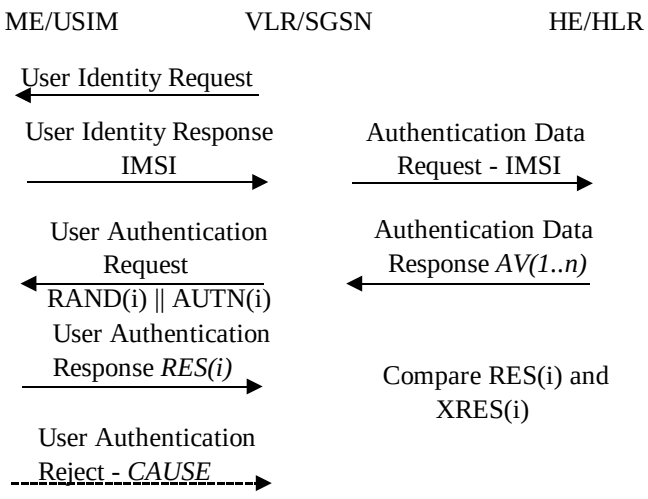

Fig. 2.Authentication and Key Agreement in UMTS

When a user registers for the first time in a serving network, or when the serving network cannot retrieve the IMSI from the temporary MSI (TMSI) by which the user identifies itself on the radio path, the VLR/serving GPRS support node (SGSN) requests the user to send its permanent identity. The user's response contains the IMSI in cleartext. Then, VLR/SGSN requests authentication data from the HE by sending the IMSI to the requesting node. Upon receipt of a request from the VLR/SGSN, the HE/HLR sends an ordered array of *n* authentication vectors (the equivalent of a GSM "triplet") to the VLR/SGSN. The authentication vectors are ordered based on sequence number. Each authentication vector consists of the following components: a 128-bit random number (RAND), an expected response (XRES), a 128-bit cipher key (CK), a 128-bit integrity key (IK) and an authentication token (AUTN). Different authentication vectors are used for each authentication and key agreement between the VLR/SGSN and the USIM.

When the VLR/SGSN initiates an authentication and key agreement, it selects the next authentication vector from the ordered array and sends the parameters RAND and AUTN to the user. Upon receipt of RAND and AUTN the USIM first computes the 48-bit anonymity key (AK) and retrieves the sequence number (SQN). Then it computes XMAC and compares with the MAC which is included in AUTN [3]. Next the USIM verifies that the received SQN is in the correct range. Finally, the USIM checks whether AUTN can be accepted and, if so, produces a variable in size, 4 to 16 bytes, response (RES) which is sent back to the VLR/SGSN. The USIM also computes 128-bit CK and IK [3].

The VLR/SGSN compares the received RES with XRES. If they match the VLR/SGSN considers the authentication and key agreement exchange to be successfully completed. The established keys CK and IK will then be transferred by the USIM and the VLR/SGSN to the entities which perform ciphering and integrity functions. Note that USIM and VLR/SGSN use f1, and f2 message authentication functions and f3, f4, f5 key generating functions.

II. Adaptive Authentication and Key Agreement Mechanism

The adaptive authentication and key agreement protocol (AAKA) is a challenge/response protocol that uses symmetric or public key cryptography to overcome security problems in 3G. These problems are related with IMSI, IMEI, and man-in-the-middle attacks. In 3G security specifications, for example, the IMSI is transmitted in cleartext when allocating TMSI to the user. Furthermore, the transmission of IMEI, which is not considered as a security parameter, is not protected. In addition, man-in-the-middle attacks are possible in 3G networks with disabled encryption.

In AAKA, users and network can be authenticated using public key encryption. Public key schemes can be enabled in future mobile terminals based on novel methods described in [6]. In particular, multiple crypto-processors can be used to perform public key complex computations [6]. The crypto-processor can be located either in a second cryptographic SIM card (CSIM) or in the mobile terminal itself. If we consider the network structure in Fig. 3, then authentication will involve three functional entities; the USIM, the CSIM and the AUC.

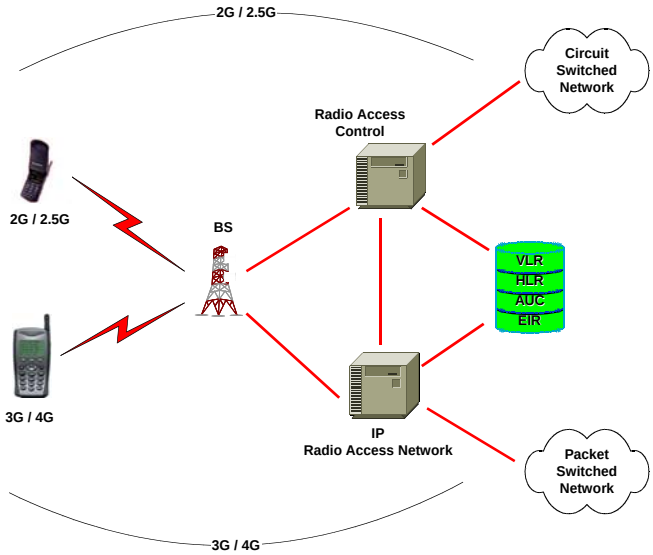

Fig. 3.Public Key Infrastructure in Future Mobile Networks

The subscriber and the network share a secret key K, and two public key pairs (P_{ME} and S_{ME}, P_{HE} and S_{HE}). The mobile equipment (ME), MS in 2G-2.5G, contains K, P_{HE} and S_{ME} stored either in the CSIM or USIM. Likewise, VLR/SGSN

and HLR/AUC contain K, P_{ME}, P_{HE} and S_{HE} in their databases. Similarly to 3G security specifications the CSIM/USIM and the HE keep track of sequence numbers to support network authentication. An overview of the AAKA mechanism is shown in Fig. 4.

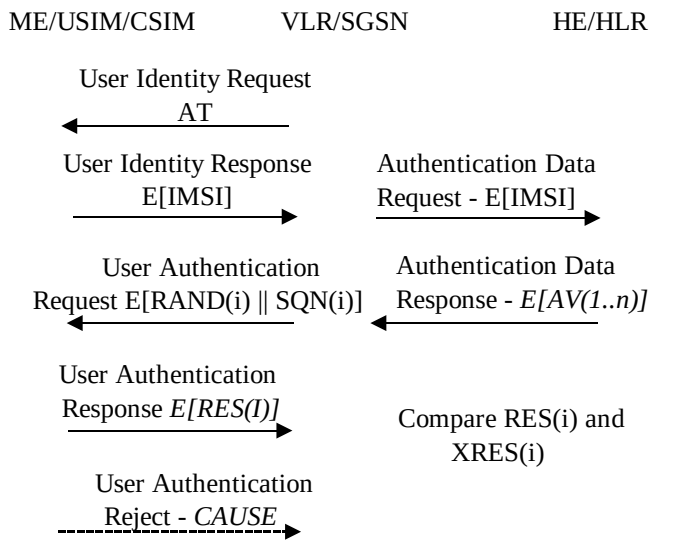

Fig. 4.Adaptive Authentication and Key Agreement Protocol Flow

When a user registers for the first time in a serving network, he/she will be assigned an authentication type (AT) number. The AT defines which encryption algorithm will be used and whether symmetric or public key encryption will be used in AAKA. Then AT will be sent to ME when the serving network requests user's permanent identity. Upon request of the IMSI, the user will respond with an encrypted, based on AT, IMSI. When public key encryption are applied the IMSI is first signed with ME's secret key and then encrypted with its public key, $P_{HE}[S_{ME}(H(IMSI)), IMSI]$, as shown in Fig. 5.

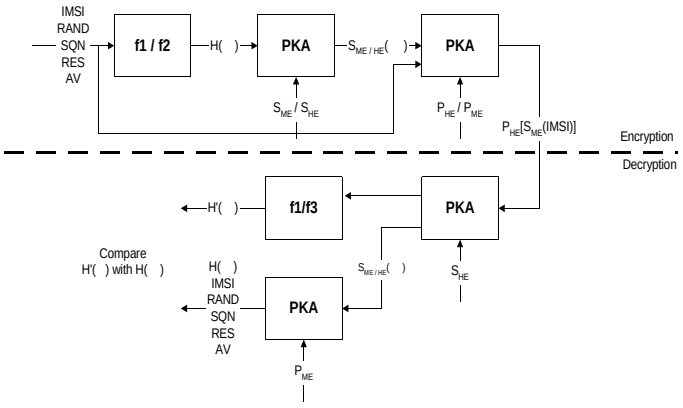

Fig. 5. Encryption/Decryption in AAKA using Public Key Cryptography and Digital Signatures

Upon receipt of the encrypted IMSI, VLR/SGSN forwards it to HE. Then HE/AUC first decrypts the signature and then retrieves the IMSI. Next, the HE/AuC sends an authentication response back to the VLR/SGSN that contains an encrypted and signed (Fig. 5) array of *n* authentication vectors AV(1..n). Each authentication vector consists of the following components: a 152-bit RAND, an XRES, a 128-bit CK, a 128-bit IK and a 48-bit SQN. Note that RAND contains 24 additional bits, which are used to identify AT in the specified IMSI/TIMSI. Similarly to UMTS each authentication vector is good for one authentication and key agreement between the VLR/SGSN and the USIM/CSIM.

When the VLR/SGSN initiates an authentication and key agreement, it selects the next authentication vector from the ordered array and sends the parameters RAND and SQN signed and encrypted to the user (Fig. 5). Upon receipt of RAND and SQN the USIM/CSIM first retrieves the SQN and RAND. Next the USIM/CSIM verifies that the received SQN is in the correct range and if so, the USIM produces a variable in size, 4 to 16 bytes, RES that is sent encrypted, with P_{HE}, back to the VLR/SGSN. VLR/SGSN decrypts and compares RES with XRES to authenticate ME. Upon authentication, the USIM/CSIM also computes 128-bit CK and IK to protect the air interface as presented in UMTS specifications [3].

The VLR/SGSN compares the received RES with XRES. If they match the VLR/SGSN considers the authentication and key agreement exchange to be successfully completed. The established keys CK and IK will then be used to perform ciphering and integrity functions. Similarly to UMTS, USIM/CSIM and VLR/SGSN use f1, and f2 message authentication functions and f3, f4, f5 key generating functions.

On the other hand when symmetric key encryption is used, the IMSI is encrypted using the f8 stream cipher and the authentication key (AK), which is computed from P_{HE} and K as shown in Fig. 6. As mentioned before, upon receipt of the IMSI, VLR/SGSN forwards it to HE/AUC which first computes the AK and then retrieves the IMSI. Next, the HE/AUC sends an encrypted authentication response back to the VLR/SGSN that contains a 152-bit RAND, an XRES, a 128-bit CK, a 128-bit IK and a 48-bit SQN.

When the VLR/SGSN initiates an authentication and key agreement, it selects the next authentication vector from the ordered array and sends the parameters RAND and SQN encrypted (Fig. 6) to the user. Next, the USIM/CSIM produces a variable in size, 4 to 16 bytes, RES which is sent encrypted back to the VLR/SGSN. Upon receipt of the encrypted RES, VLR/SGSN decrypts and compares the RES with XRES to authenticate the user. The air interface then is protected as presented in the UMTS specifications.

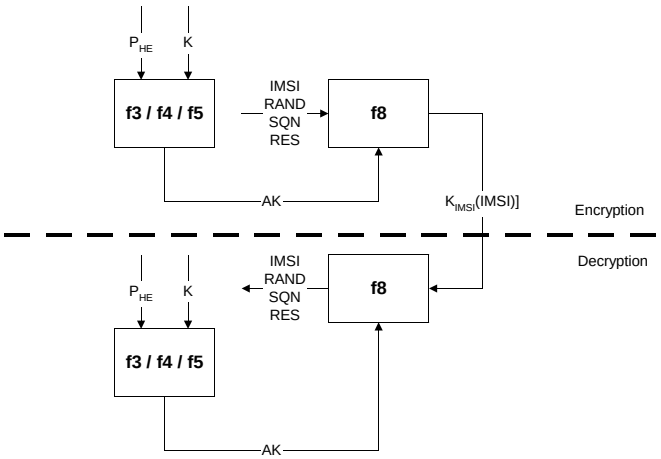

Fig. 6.Encryption/Decryption in AAKA using Symmetric Key Cryptography

III. Conclusion

In this paper an adaptive authentication and key distribution protocol (AAKA) was presented that can be applied in future mobile communication systems. AAKA is a challenge response protocol that uses symmetric and/or public key cryptography for user and network authentication. The novelty of AAKA and its main advantage over other challenge response protocols is that can be adaptive to the mobile environment. For example, when a customer registers for the first time in a serving network an authentication type (AT) can be assigned based on the level of security he/she requested. In AAKA we have defined two types of authentication; authentication using public key encryption and authentication using symmetric key encryption. Authentication using public key schemes requires several crypto-processors embedded to mobile devices for public key complex computations. However, when a subscriber has assigned authentication with public key encryption the VLR/SGSN still can use symmetric encryption if the network is overloaded at the time of AAKA. The additional information in RAND informs VLR/SGSN whether symmetric or public key encryption will be used in AAKA.

References

[1] 3GPP TS 21.133, "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements", 2004

[2] 3GPP TS 33.120, "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives", 2004

[3] 3GPP TS 33.102, "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Architecture", 2004

[4] ISO/IEC 9798-4, "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function", 2004

[5] ETSI GSM 03.20, "Digital cellular telecommunications systems (Phase 2+); Security related network functions", 2000

[6] N. Komninos and B. Honary, "Novel Methods for Enabling Public Key Schemes in Future Mobile Systems," *In 3rd International Conference on 3G Mobile Communication Technologies*, IEE Conference Publication 489, ISBN 0 85296 749 7, UK, 2002, pp. 455-458.

[7] H. Haverinen, N. Asokan, and T. Maattanen, "Authentication and key generation for mobile IP using GSM authentication and roaming," *IEEE International Conference on Communications*, 11-14 June 2001 Page(s):2453 - 2457 vol.8.

[8] T. Yuh-Ren and C. Cheng-Ju, "SIM-based subscriber authentication for wireless local area networks", *37th IEEE International Carnahan Conference on Security Technology*, 14-16 Oct. 2003 Page(s):468 – 473.

[9] L. Wei and W. Wenye, "A lightweight authentication protocol with local security association control in mobile networks" *IEEE Military Communications Conference*, 31 Oct.-3 Nov. 2004 Page(s):225 – 231, vol. 1.

[10] J. Jong Min, L. Goo Yeon, and L. Yong, "Mutual authentication protocols for the virtual home environment in 3G mobile network", IEEE Global Telecommunications Conference, 17-21 Nov. 2002 Page(s):1658 – 1662, vol.2.