Journal of Zhejiang University-SCIENCE C (Computers & Electronics)
ISSN 1869-1951 (Print); ISSN 1869-196X (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

A three-level authenticated conference key establishment protocol for UMTS networks*

Chung-Fu LU[1,2], Tzong-Chen WU[1], Chien-Lung HSU[†‡3]

([1]*Department of Information Management, National Taiwan University of Science and Technology, Taiwan 106, Taipei*)

([2]*Department of Computer and Communication Engineering, Taipei College of Maritime Technology, Taiwan 111, Taipei*)

([3]*Department of Information Management, Chang Gung University, Taiwan 333, Taoyuan*)

[†]E-mail: clhsu@mail.cgu.edu.tw

Received June 13, 2010; Revision accepted Nov. 5, 2010; Crosschecked Mar. 31, 2011

Abstract: A conference key establishment protocol allows a group of conferees to agree on a secret key shared among them for secure group communication. This paper proposes a three-level conference key establishment protocol based on the Universal Mobile Telecommunications System (UMTS) framework to establish a group-level key, home location register (HLR) level keys, and visitor location register (VLR) level keys simultaneously for a group of conferees. The group-level key is used to secure the communications for all conferees, the HLR-level key is for those within the same HLR domain, and the VLR-level key is for those within the same VLR domain. The group-level key can be used for securing inter-domain group-oriented applications such as commercial remote conferencing systems. The HLR- and VLR-level keys can be used for securing intra-domain subgroup applications (e.g., location-based or context-aware services) and dynamic key updating. Since our proposed protocol exploits existing UMTS security functions and the exclusive-or operation, it is compatible with UMTS architecture. This means that it is fast and easy to implement on the existing UMTS architecture. Furthermore, the proposed protocol has low computational complexities and can provide cost effectiveness, load-amortization, scalability, user authentication, key establishment, key confirmation, key updating, and lawful interception.

Key words: Universal Mobile Telecommunications System (UMTS), Three-level, Conference key establishment, Secure group communication, Authentication

doi:10.1631/jzus.C1000194 **Document code:** A **CLC number:** TP309

1 Introduction

With the rapid growth of mobile wireless networks, many mobile applications like computers, audio, video, and telecommunications are merging. Above all, mobile telecommunication systems play an ever increasing role in new business opportunities. To pave the way for this promising future, a smooth evolution from second generation (2G) telecommunication systems to third generation (3G) systems has to be ensured. Compared with 2G systems, 3G systems have higher data rates and security. 3G mobile systems provide data rates of up to 2 Mb/s to offer mobile services such as wireless voice, data, and multimedia. They also provide the mechanism to mutually authenticate the mobile device and the serving network using 3G authentication and key agreement (AKA) (3GPP, 2001; 2009a; 2009b).

The Universal Mobile Telecommunications System (UMTS) is a popular 3G system. In such a system, encryption of traffic at the air interface is optional, and the decision to employ air interface encryption (AIE) depends on the network operator. Mobile users are usually unaware of whether AIE is being employed. Network operators usually disable AIE, and hence transmitted messages can be easily eavesdropped. In addition, AIE provides a secure

‡ Corresponding author

* Project supported by Chang Gung University (No. UARPD390111), the Chang Gung Memorial Hospital (No. CMRPD390031), and the National Science Council (No. 98-2410-H-182-007-MY2)

channel only between a mobile user and the UMTS core network. If any two mobile users want to securely communicate with each other, UMTS can act as a trusted third party and separately establish a secure channel for each user by using AIE. However, this is inefficient in terms of computational and communication costs. Costs would increase markedly if UMTS were used for securing group communications.

A secure group communication is the basis for many recent group-oriented applications such as a teleconferencing. To make sure that the data is available only to authorized users in the group, a secret group key should be established for them at any point in time. A number of solutions for establishing secure group communications have been proposed. They can be divided into two categories: symmetric and asymmetric cryptography solutions. Symmetric solutions (Um and Delp, 2006a; 2006b; Dong *et al*., 2009) can establish a secure key with predefined secret keys shared between any two users. The predefined secret keys are unnecessary in asymmetric solutions (Nam *et al*., 2005; Tseng, 2007; Lee *et al*., 2009), but such solutions are inefficient and impractical in UMTS networks. Symmetric solutions are better suited for establishing secure group communications in UMTS networks.

A trivial solution is to set up a secure end-to-end connection between any two users for establishing a secret group communication between them based on symmetric cryptography. However, this solution is prohibitively inefficient in computational, storage, and communication costs. The coordinator (which may be the UMTS core network) or the chairperson will become a potential bottleneck for secure group communications. Also, such a solution might protect the communication between users from being eavesdropped by UMTS. This violates the lawful interception requirement of the UMTS standard (3GPP, 2009c; 2009d; 2009e).

Another efficient solution to secure group communication is called a group key establishment protocol. It allows a number of users to cooperatively establish a secret group key for securing their group communication. There have been many studies on this topic (Ng and Mitchell, 2004; Nam *et al*., 2005; Um and Delp, 2006a; 2006b; Tseng, 2007; Dong *et al*., 2009; Lee *et al*., 2009; Sun and Yu, 2009; Manulis and Sadeghi, 2010). However, these proposed group key establishment protocols are inefficient and not fully applicable to existing UMTS, since they may change the existing UMTS architecture or require extra security modules.

Elaborating on UMTS architecture and group-oriented applications, this paper proposes a three-level conference key establishment protocol based on UMTS framework. A group of participants can be divided into subgroups according to UMTS architecture. The proposed protocol establishes a group-level key, home location register (HLR) level keys, and visitor location register (VLR) level keys simultaneously for a group of conferees. The group-level key can secure the communications for all conferees, the HLR-level key is for those within the same HLR domain, and the VLR-level key is for those within the same VLR domain. The purpose of the group-level key is the same as that of the secret group key established by the traditional conference key protocols. The other keys are used for subgroup applications and UMTS. For subgroup applications, the HLR- and VLR-level keys can be used to protect some sensitive services. These two keys can also be used for improving key updating in dynamic group membership management. The group-level key can be used for securing inter-domain group-oriented applications such as commercial remote conferencing systems. In addition, UMTS networks generally provide basic communication services. They can use our proposed protocol to provide some value-added services, such as secure group communications and location-based or context-aware services.

Consider an example of UMTS-based telematics systems in which vehicular services and applications are based on a UMTS network. In such a system, location-based information and services are sensitive to user privacy and security. Vehicles with telematics systems can use our proposed protocol to establish a group-level key for securing communications among some vehicles. These vehicles use the group-level key to share and secure their current position. In addition, a telematics system should consider the dynamic problems that may occur when some trusted vehicles join or leave the group of vehicles. Under such scenarios, the HLR- and VLR-level keys can be used to update the group-level key efficiently. Moreover, the service providers of telematics systems can use HLR- or VLR-level keys to provide securely value-added services such as location-based e-coupons, up-to-date

traffic reports, or seating availability at nearby restaurants, and to push proactively user-sensitive advertisements, etc.

The proposed protocol is compatible with UMTS architecture since it exploits only the existing UMTS security functions and the exclusive-or (XOR) operation. It has low computational complexities and can provide cost effectiveness, load-amortization, scalability, user authentication, key establishment, key confirmation, key updating, and lawful interception.

2 UMTS architecture

The high-level system architecture of the UMTS (Fig. 1) consists of the following elements: user equipment (UE), UMTS terrestrial radio access network (UTRAN), and core network (CN). UE is a combination of mobile equipment (ME) and subscriber identity module/UMTS subscriber identity module (SIM/USIM). It provides the mobile operating functions as an integral part of UMTS. UTRAN consists of one or more radio network subsystems (RNS). RNS provides all the transmission and control functions that are necessary for radio coverage of the service area. It includes one or more base transceiver stations (B nodes) and the radio network controller (RNC). B node is a logical node responsible for the radio transmission to UE and for the radio reception from the UE. Each B node serves one radio cell. RNC

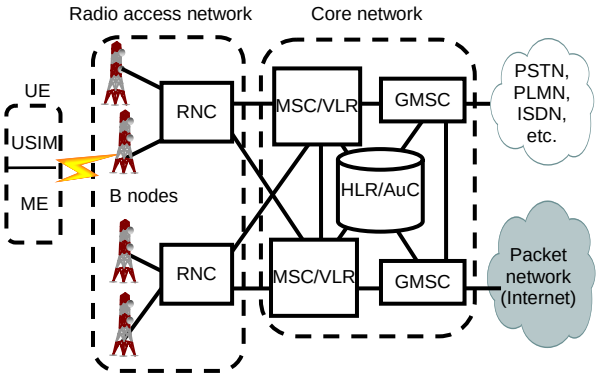

Fig. 1 Universal Mobile Telecommunications System (UMTS) architecture

UE: user equipment; USIM: UMTS subscriber identity module; ME: mobile equipment; RNC: radio network controller; MSC/VLR: mobile switching center/visitor location register; GMSC: gateway mobile switching center; PSTN: public switched telephone network; PLMN: public land mobile network; ISDN: integrated services digital network; HLR/AuC: home location register/authentication center

is the network element responsible for mobility management, call processing, link maintenance, and handover mechanisms. RNC collects the packet switched (PS) and circuit switched (CS) traffics from all connected B nodes. Up to three RNCs are linked to a 3G mobile switching center/visitor location register (MSC/VLR) or 3G serving GPRS support node (SGSN). CN consists of the following main elements (3GPP, 2009a; 2009b):

HLR/AuC (home location register/authentication center): a database located in the user's home network that stores the master copy of the user's service profile. HLR/AuC also stores the UE location at the level of MSC/VLR and/or the serving system.

MSC/VLR: the switch (MSC) and the database (VLR) that serves UE in its current location for circuit switched (CS) services. The MSC is used to switch the CS transactions, and the VLR's function is to hold a copy of the visiting user's service profile, as well as more precise information, on the UE location within the serving system. This part of the network, accessed via MSC/VLR, is often referred to as the CS domain.

GMSC (gateway mobile switching center): the switch at the point where the UMTS public land mobile network (PLMN) is connected to external CS networks. All incoming and outgoing CS connections go through GMSC.

3 The proposed three-level conference key establishment protocol for UMTS

First, MSC/VLR must have exclusive-or (XOR), f_1, f_2, and f_3 functions used in the existing UMTS networks. The channel between MSC/VLR and HLR/AuC is secure. Without loss of generality, the notations are as defined in Table 1.

The proposed protocol consists of three phases: user registration, mutual authentication, and conference key establishment.

3.1 User registration phase

This phase is identical to that of UMTS (3GPP, 2001; 2009a; 2009b). When a mobile conferee wants to use the UMTS service, he/she has to register beforehand with a mobile network operator. When subscribing to the service, the user will receive a USIM smart card storing a subscriber key shared between USIM and AuC.

Table 1 Notations used in this paper

Notation	Description
N	The number of conferees who want to agree on a common secret key shared among them
η	The number of HLR/AuCs to which these N conferees belong
$\mathrm{HLR/AuC}_i$	The ith HLR/AuC
$\mathrm{MSC/VLR}_{i,j}$	The jth MSC/VLR with the domain $\mathrm{HLR/AuC}_i$
$U_{i,j,k}$	The kth conferee belonging to MSC/VLR j in $\mathrm{HLR/AuC}_i$, $1\le k\le\omega_{i,j}$
v_i	The number of MSC/VLRs belonging to $\mathrm{HLR/AuC}_i$, i=1, 2, …, η
$G_{i,j}$	The conferee subgroup belonging to $\mathrm{MSC/VLR}_{i,j}$
$\omega_{i,j}$	The number of conferees belonging to MSC/VLR j in HLR/AuC i, $\omega_{i,j}=\lvert G_{i,j}\rvert$
G_C	The set of all conferees. $G_\mathrm{C}=\cup G_{i,j}$ ($\forall i$=1, 2, …, η and j=1, 2, …, v_i) and $\lvert G_\mathrm{C}\rvert=N$
$\mathrm{CK}_{i,j,k}$	The cipher key shared between the conferee $U_{i,j,k}$ and the serving network
$\mathrm{IK}_{i,j,k}$	The integrity key shared between the conferee $U_{i,j,k}$ and the serving network
K_C	The established group-level key for all participating conferees
$\mathrm{K2}_i$	The established HLR-level key for the participating conferees within HLR/AuC i
$\mathrm{K1}_{i,j}$	The established VLR-level key for the participating conferees within VLR j in HLR/AuC i
$A\rightarrow B$: M	The sender A sends a message M to the receiver B
$f_1(\cdot)$	The network authentication function of existing UMTS networks
$f_2(\cdot)$	The user authentication function of existing UMTS networks
$f_3(\cdot)$	The cipher key derivation function of existing UMTS networks

3.2 Mutual authentication phase

This phase is identical to that of UMTS (3GPP, 2001; 2009a; 2009b). That is, each legal mobile conferee must perform UMTS AKA to authenticate the legitimacy of the conferee and the serving network, and agree on the cipher and the integrity keys (i.e., CK and IK) for accessing the network services. In the proposed protocol, each conferee $U_{i,j,k}$ will obtain the $\mathrm{CK}_{i,j,k}$ and $\mathrm{IK}_{i,j,k}$ after performing this phase.

3.3 Conference key establishment phase

Suppose a group G_C of N conferees wants to establish three secret keys: a VLR-level key, an HLR-level key, and a group-level key. The VLR-level key is used to establish a secure channel for the conferees belonging to the same MSC/VLR domain. The HLR-level key is used to establish a secure channel for the conferees belonging to the same HLR/AuC domain. The group-level key is a common secret key shared among all conferees in the group G_C. The group-level key can secure the communications for all conferees. The VLR- and HLR-level keys can be applied to some subgroup applications and can be used for group-level key updating when conferees leave or join the group.

The logical architecture for our conference key establishment phase and the three-level key derivation tree are shown in Figs. 2 and 3, respectively. For simplicity, we assume that the first conferee $U_{1,1,1}$ in the $G_{1,1}$ is the chairperson whose main responsibility is to originate this phase and then cooperate with other conferees $U_{i,j,k}\in G_\mathrm{C}\backslash U_{1,1,1}$ to agree on the above three keys (group-level key K_C, HLR-level key $\mathrm{K2}_i$, and VLR-level key $\mathrm{K1}_{i,j}$). $U_{i,j,k}$ is the kth conferee belonging to $\mathrm{MSC/VLR}_{i,j}$ in $\mathrm{HLR/AuC}_i$, where $1\le k\le\omega_{i,j}$. Detailed descriptions of this phase are given below.

1. $U_{1,1,1}\rightarrow\mathrm{MSC/VLR}_{1,1}$: $r_{1,1,1}$, InviteMsg$\{U_{i,j,k}\in G_\mathrm{C}\backslash U_{1,1,1}\}$.

The chairperson $U_{1,1,1}$ uses his/her cipher key $\mathrm{CK}_{1,1,1}$ to compute $\mathrm{SKR}_{1,1,1}=f_2(\mathrm{CK}_{1,1,1}, r_{1,1,1})$, where $r_{1,1,1}\in_R Z_q$. Finally, $U_{1,1,1}$ sends $r_{1,1,1}$ together with the invitation message InviteMsg$\{U_{i,j,k}\in G_\mathrm{C}\backslash U_{1,1,1}\}$ to his/her serving network $\mathrm{MSC/VLR}_{1,1}$. The message InviteMsg$\{U_{i,j,k}\in G_\mathrm{C}\backslash U_{1,1,1}\}$ means that the chairperson wants to invite the users in $U_{i,j,k}\in G_\mathrm{C}\backslash U_{1,1,1}$ to cooperate with him/her for performing the conference key establishment phase.

2. $\mathrm{MSC/VLR}_{1,1}\rightarrow U_{i,j,k}$: InviteMsg$\{U_{i,j,k}\in G_{i,j}\backslash U_{1,1,1}\}$.

On receiving InviteMsg$\{U_{i,j,k}\in G_\mathrm{C}\backslash U_{1,1,1}\}$ sent from $U_{1,1,1}$, the serving network $\mathrm{MSC/VLR}_{1,1}$ invites each conferee $U_{i,j,k}\in G_{i,j}\backslash U_{1,1,1}$ to perform the subsequent steps.

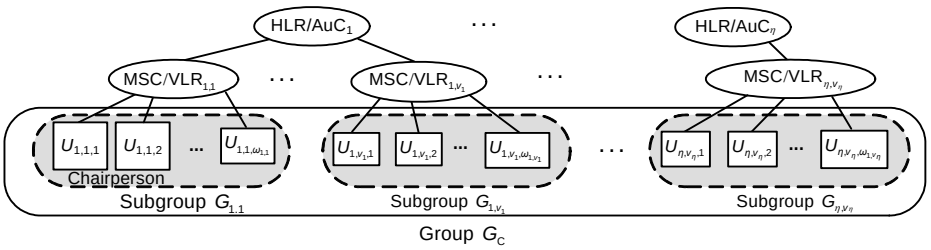

Fig. 2 Logical architecture for the proposed conference key establishment

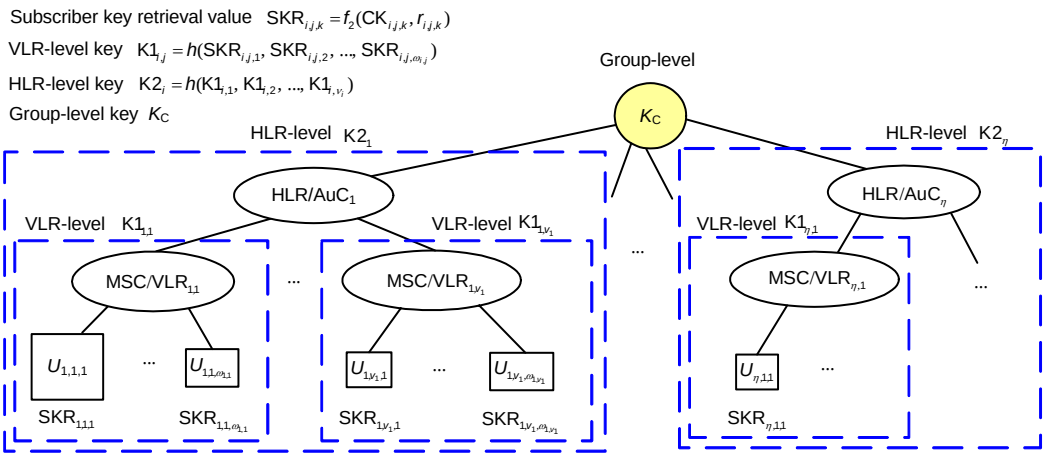

Fig. 3 Three-level key derivation tree

3. $U_{i,j,\omega_{i,j}} \rightarrow \mathrm{MSC/VLR}_{i,j}$: $r_{i,j,k}$.

Each conferee $U_{i,j,k} \in G_{i,j} \backslash U_{1,1,1}$ accepts the invitation from $\mathrm{MSC/VLR}_{1,1}$ and then selects $r_{i,j,k} \in_R Z_q$ and computes $\mathrm{SKR}_{i,j,k}=f_2(\mathrm{CK}_{i,j,k}, r_{i,j,k})$. Finally, $U_{i,j,k}$ sends $r_{i,j,k}$ to his/her serving network $\mathrm{MSC/VLR}_{i,j}$.

4. $\mathrm{MSC/VLR}_{i,j} \rightarrow \mathrm{HLR/AuC}_i$: $\mathrm{K1}_{i,j}$.

Each $\mathrm{MSC/VLR}_{i,j}$ (i=1, 2, …, η; j=1, 2, …, v_i) computes all $\mathrm{SKR}_{i,j,k}$'s and computes VLR-level key $\mathrm{K1}_{i,j}=h(\mathrm{SKR}_{i,j,1}, \mathrm{SKR}_{i,j,2}, ..., \mathrm{SKR}_{i,j,\omega_{i,j}})$ for the subgroup $G_{i,j}$, where h is regarded as an iterative function for $f_3(\cdot)$. For example, $h(\mathrm{SKR}_{i,j,1}, \mathrm{SKR}_{i,j,2}, \mathrm{SKR}_{i,j,3}, \mathrm{SKR}_{i,j,4})$ can be defined as $f_3(f_3(f_3(\mathrm{SKR}_{i,j,1}, \mathrm{SKR}_{i,j,2}), \mathrm{SKR}_{i,j,3}), \mathrm{SKR}_{i,j,4})$, or $f_3(\mathrm{SKR}_{i,j,1}\|\mathrm{SKR}_{i,j,2}\|\mathrm{SKR}_{i,j,3}\|\mathrm{SKR}_{i,j,4})$. Finally, $\mathrm{MSC/VLR}_{i,j}$ sends $\mathrm{K1}_{i,j}$ to his/her $\mathrm{HLR/AuC}_i$.

5. $\mathrm{HLR/AuC}_1 \rightarrow \mathrm{HLR/AuC}_i$: K_C ($i \neq 1$).

The chairperson $U_{1,1,1}$'s $\mathrm{HLR/AuC}_1$ generates the group-level key K_C for the group G_C and sends K_C to $\mathrm{HLR/AuC}_i$ (i=2, 3, …, η).

6. $\mathrm{HLR/AuC}_i \rightarrow \mathrm{MSC/VLR}_{i,j}$: $\mathrm{K2}_i$, K_C.

On receiving the K_C from $\mathrm{HLR/AuC}_1$ and $K1_{i,j}$'s from $\mathrm{MSC/VLR}_{i,j}$ (j=1, 2, …, v_i), each $\mathrm{HLR/AuC}_i$ (i=1, 2, …, η) computes the HLR-level key $\mathrm{K2}_i = h(\mathrm{K1}_{i,1}, \mathrm{K1}_{i,2}, ..., \mathrm{K1}_{i,v_i})$ and sends ($\mathrm{K2}_i$, K_C) back to $\mathrm{MSC/VLR}_{i,j}$ via a secure channel.

7. $\mathrm{MSC/VLR}_{i,j} \rightarrow U_{i,j,k} \in G_{i,j}$: $\mathrm{KMAC1}_{i,j,k}$, $\mathrm{C1}_{i,j,k}$, $\mathrm{KMAC}_{i,j}$, $C_{i,j}$.

Each $\mathrm{MSC/VLR}_{i,j}$ (i=1, 2, …, η; j=1, 2, …, v_i) computes $\mathrm{KMAC1}_{i,j,k}=f_1(\mathrm{CK}_{i,j,k}, r_{i,j,k}, \mathrm{K1}_{i,j})$, $\mathrm{C1}_{i,j,k}=\mathrm{SKR}_{i,j,k} \oplus \mathrm{K1}_{i,j}$, $\mathrm{KMAC}_{i,j}=f_1(\mathrm{K1}_{i,j}, K_\mathrm{C}, \mathrm{K2}_i)$, and $C_{i,j}=f_3(\mathrm{K1}_{i,j}, \mathrm{KMAC}_{i,j}) \oplus (K_\mathrm{C}\|\mathrm{K2}_i)$, where '⊕' denotes an exclusive-or (XOR) operation. Finally, $\mathrm{MSC/VLR}_{i,j}$ sends $\{\mathrm{KMAC1}_{i,j,k}, \mathrm{C1}_{i,j,k}, \mathrm{KMAC}_{i,j}, C_{i,j}\}$ back to the conferee $U_{i,j,k}$.

8. $U_{i,j,k} \in G_\mathrm{C}$: retrieve $\mathrm{K1}_{i,j}$, $\mathrm{K2}_i$, K_C.

Each $U_{i,j,k}$ computes $\mathrm{K1}'_{i,j}=\mathrm{SKR}_{i,j,k} \oplus \mathrm{C1}_{i,j,k}$ and verifies it by checking if $f_1(\mathrm{CK}_{i,j,k}, r_{i,j,k}, \mathrm{K1}'_{i,j})$ is equal to the received $\mathrm{KMAC1}_{i,j,k}$. If it holds, $\mathrm{K1}'_{i,j}$ is a valid VLR-level key. With the knowledge of the valid $\mathrm{K1}'_{i,j}$, $U_{i,j,k}$ further computes $K'_\mathrm{C}\|\mathrm{K2}'_i=f_3(\mathrm{K1}'_{i,j}, \mathrm{KMAC}_{i,j}) \oplus C_{i,j}$ and checks if $f_1(\mathrm{K1}'_{i,j}, K'_\mathrm{C}, \mathrm{K2}'_i)$ is identical to the received $\mathrm{KMAC}_{i,j}$. If it holds, the group-level key K'_C and the HLR-level key $\mathrm{K2}'_i$ are verified.

We give a simple example to demonstrate our conference key establishment phase as follows. Suppose there are four conferees $U_{1,1,1}$, $U_{1,1,2}$, $U_{1,2,1}$, and $U_{2,1,1}$ belonging to two HLR/AuC domains (Fig. 4), where G_C={$U_{1,1,1}$, $U_{1,1,2}$, $U_{1,2,1}$, $U_{2,1,1}$}, $G_{1,1}$={$U_{1,1,1}$, $U_{1,1,2}$}, $G_{1,2}$={$U_{1,2,1}$}, and $G_{2,1}$={$U_{2,1,1}$}. That means N=4 and η=2. There are two MSC/VLRs in HLR/AuC$_1$ and one MSC/VLR in HLR/AuC$_2$, which means ν_1=2 and ν_2=1. In HLR/AuC$_1$, $U_{1,1,1}$ and $U_{1,1,2}$ belong to MSC/VLR$_{1,1}$ and $U_{1,2,1}$ belongs to MSC/VLR$_{1,2}$, which means $\omega_{1,1}$=2 and $\omega_{1,2}$=1. In HLR/AuC$_2$, $U_{2,1,1}$ belongs to MSC/VLR$_{2,1}$, which means $\omega_{2,1}$=1. Without loss of generality, the conferee $U_{1,1,1}$ in $G_{1,1}$ is the chairperson, whose main responsibility is to originate the conference key establishment phase and then cooperate with other conferees $U_{1,1,2}$, $U_{1,2,1}$, and $U_{2,1,1}$ to agree on the above three keys. After performing this phase, each conferee can be given a group-level key K_C, an HLR-level key K2$_i$, and a VLR-level key K1$_{i,j}$. For example, the conferee $U_{1,1,1}$ is given a group-level key K_C shared with G_C={$U_{1,1,1}$, $U_{1,1,2}$, $U_{1,2,1}$, $U_{2,1,1}$}, an HLR-level key K2$_1$ shared with $G_{1,1}\cup G_{1,2}$={$U_{1,1,1}$, $U_{1,1,2}$, $U_{1,2,1}$}, and a VLR-level key K1$_{1,1}$ shared with $G_{1,1}$={$U_{1,1,1}$, $U_{1,1,2}$}.

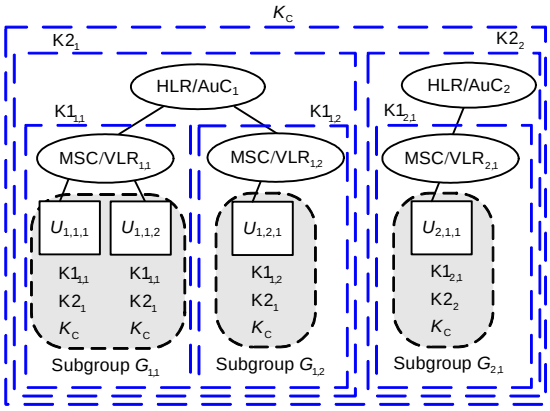

Fig. 4 Example of the proposed conference key establishment phase

3.4 Key updating

Without loss of generality, when a user $U_{i,j,k+1}$ within HLR i and VLR j joins the group G, the UMTS will perform a UMTS AKA protocol to authenticate the user and establish a secret key CK$_{i,j,k+1}$ shared between him/her and the UMTS. The UMTS can use CK$_{i,j,k+1}$ to securely transmit (K1$_{i,j}$, K2$_i$, K_C) to the user.

When a user $U_{i,j,k}$ wants to leave the group G, the UMTS will perform the following steps:

1. Determine a new group-level key K_C^*, a new HLR-level key K2$_i^*$ of HLR i, and a new VLR-level key K1$_{i,j}^*$ of VLR j within HLR i.

2. Use K2$_\alpha$ to securely transmit K_C^* to the conferees within every HLR α ($\alpha\neq i$).

3. Use K1$_{\alpha,\beta}$ to securely transmit (K_C^*, K2$_i^*$) to the conferees within VLR β ($\beta\neq j$).

4. Use CK$_{i,j,\varepsilon}$ ($\varepsilon\neq k$) to securely transmit (K_C^*, K2$_i^*$, K1$_{i,j}^*$) to all conferees within VLR j and HLR i.

4 Analysis and discussion

A secure and practical conference key establishment protocol for mobile communications should be executed efficiently on portable devices, and implemented without modifying the existing UMTS. Security analysis, efficiency analysis, and implementation discussions of the proposed protocol are given below based on the UMTS and its secure algorithms.

4.1 Security analysis

We will show that the proposed protocol achieves the security requirements of Diffie *et al*. (1992).

1. Integration of entity authentication and key establishment: The proposed protocol achieves entity authentication and key establishment using the existing UMTS AKA protocol. The derivation and verification of all secret keys for the conference are primarily achieved by the shared cipher key CK$_{i,j,k}$ established by the UMTS AKA.

2. Prevention of reflection attacks: The structures of authentication and exchanged messages are asymmetric, which implies that they can withstand potential reflection attacks (Ng and Mitchell, 2004). That is, the proposed protocol can prevent an adversary from masquerading as some entity to communicate with an honest user.

3. Prevention of replay attacks: All transmitted messages are linked with the random number $r_{i,j,k}$ and the cipher key CK$_{i,j,k}$. A replay attack is excluded in our protocol. The proposed protocol can achieve key independence, which implies that forward and backward secrecy are satisfied.

4. Prevention of compromising attacks: The

random number $r_{i,j,k}$ controlled by each conferee and the cipher key $CK_{i,j,k}$ are logically linked with the established secret keys (i.e., $K1_{i,j}$, $K2_i$, and K_C). Without knowledge of these, an adversary cannot compromise all secret keys from the eavesdropping messages.

5. Prevention of forgery attacks: The message authentication code (MAC) function f_1 can be regarded as a symmetric signature function that provides the integrity of the transmitted messages. All MAC values (i.e., $KMAC1_{i,j,k}$ and $KMAC_{i,j}$) are logically linked with the cipher key $CK_{i,j,k}$. Hence, an adversary cannot forge a valid MAC without knowledge of $CK_{i,j,k}$ generated by the UMTS AKA protocol.

4.2 Performance analysis

In this subsection, we evaluate the performance of our proposed conference key establishment protocol in terms of computational complexities and communication overheads. No research has focused on the group key agreement protocol for UMTS. Hence, we discuss the performance analysis of our proposed protocol only in terms of computational complexities and communication overheads. For convenience, we first define some notations (Table 2).

Table 2 Notations for performance analysis

Notation	Description
T_{f1}	The time for computing a network authentication function f_1 of existing UMTS networks
T_{f2}	The time for computing a user authentication function f_2 of existing UMTS networks
T_{f3}	The time for computing a cipher key derivation function f_3 of existing UMTS networks
T_{XOR}	The time for computing an XOR operation of existing UMTS networks
$\|a\|$	The bit-length of a variable a

The computational complexities and communication overheads of the proposed conference key establishment protocol are listed in Table 3. The security functions and operations (i.e., f_1, f_2, f_3, and XOR operation) of the existing UMTS have low computational complexities. Since our proposed protocol exploits the existing UMTS functions and operations, it has low computational complexities. In addition, our proposed protocol is practical and efficient due to $O(N)$ rounds of the message transmission, $O(1)$ completion time, $O(1)$ waiting time, and $O(N)$ communication overheads.

Table 3 Performance of the proposed conference key establishment protocol

Protocol	Computational complexity	Communication overhead
HLR/AuC	T_{f3}	$\|K_C\|+\|f_1(\cdot)\|$
MSC/VLR	$(\omega_{i,j}+1)T_{f1}+\omega_{i,j}T_{f2}$ $+2T_{f3}+(\omega_{i,j}+1)T_{XOR}$	|InviteMsg{}| $+(\omega_{i,j}+1)\|f_1(\cdot)\|$ $+(\omega_{i,j}+2)\|f_3(\cdot)\|$
Mobile conferee	$2T_{f1}+T_{f2}+T_{f3}+2T_{XOR}$	|InviteMsg{}|+|q|

T_{f1}, T_{f2}, T_{f3}, and T_{XOR}: time for computing a network authentication function f_1, a user authentication function f_2, a cipher key derivation function f_3, and an XOR operation of existing UMTS networks, respectively. $\omega_{i,j}$: number of conferees belonging to MSC/VLR j in HLR/AuC i; K_C: established group-level key for all participating conferees; q: order of prime field Z_q; $|\cdot|$: bit-length

Previously proposed group key establishment protocols are inefficient and not fully applicable to existing UMTS, since they may change the existing UMTS architecture or require extra security modules. Under existing UMTS architecture and exploiting only the existing UMTS security modules, an alternative solution is to set up a secure end-to-end connection between every two users for establishing a secret group communication between them based on symmetric cryptography. This alternative solution is prohibitively inefficient in rounds, computational time, waiting time, key storage, and communication overheads (Table 4). The coordinator (possibly the UMTS core network) or the chairperson will become a potential bottleneck for secure group communications.

Table 4 Comparisons between our proposal and common end-to-end encryption for group communications

Parameter	Time complexity	
	Common end-to-end encryption for group communications	The proposed protocol
Rounds of the message transmission	$O(N^2)$	$O(N)$
Completion time	$O(N^2)$	$O(1)$
Waiting time	$O(N)$	$O(1)$
Communication overhead	$O(N^2)$	$O(N)$
Key storage of each mobile conferee	$O(N)$	$O(1)$

N: the number of conferees who want to agree on a common secret key shared among them

4.3 Implementation considerations

Our proposed protocol has the following practical characteristics in terms of implementation considerations:

1. Ease of use and implementation on UMTS: Most security modules and architectures used in our protocol are inherent in the UMTS. Only one random number generator should be implemented in the mobile terminals. One possible alternative solution is that the random numbers could be generated by the conferee's keying chars or numbers. Hence, it is very simple and easy to implement our proposed protocol on the UMTS.

2. Scalability: The number of message transmissions between HLR/AuC and MSC/VLR are independent of the number of mobile terminals in our protocol. Scalability of the proposed protocol depends on that of the existing UMTS, since the number of conferees depends on the number of the mobile terminals controlled by each MSC/VLR.

3. Load-amortization: The protocol can be performed by the conferees in parallel. The effort (e.g., computational complexity or rounds of message transmission) required for each conferee is the same. Our protocol can hence achieve load-amortization.

4. Lawful interception (3GPP, 2009c; 2009d; 2009e): Lawful interception (LI) is the interception of telecommunications by a law enforcement agency (LEA). It allows the authorized LEA to eavesdrop suspected malicious mobile user(s) lawfully for combating criminal activities and performing security investigations. The LEA may be police, intelligence agencies, independent commissions against corruption, etc. LI of public telecommunications systems in each country is based on national legislation. A telecommunication company is generally required to set up an adequate LI system before it is granted an operating license. The existing UMTS systems adopted the LI requirement and recommendations defined in the 3rd Generation Partnership Project (3GPP) Technical Specification TS 33.106 (3GPP, 2009c). The proposed protocol allows UMTS to derive all secret keys for LI since the VLR-level keys, the HLR-level keys, and the group-level key are computed using the system. It provides LI as required in UMTS.

5 Conclusions

This paper has proposed a three-level conference key establishment protocol to establish three types of secret keys shared by conferees within the same MSC/VLR domain, the same HLR/AuC domain, and all conferees, respectively. The proposed protocol is compatible with UMTS architecture since it exploits only the existing UMTS security functions and exclusive-or (XOR) operation. This means that it is fast and easy to implement on the existing UMTS architecture. The proposed protocol has low computational complexity and is cost effective. Furthermore, it can achieve load-amortization, scalability, user authentication, key establishment, key confirmation, key updating, and lawful interception.

References

3GPP, 2001. 3G Security: Integration Guidelines. 3GPP TS 33.103 V4.2.0.

3GPP, 2009a. 3G Security: Security Architecture. 3GPP TS 33.102 V9.1.0.

3GPP, 2009b. 3G Security: Cryptographic Algorithm Requirements. 3GPP TS 33.105 V9.0.0.

3GPP, 2009c. 3G Security: Lawful Interception Requirements. 3GPP TS 33.106 V9.0.0.

3GPP, 2009d. 3G Security: Lawful Interception Architecture and Functions. 3GPP TS 33.107 V9.0.0.

3GPP, 2009e. 3G Security: Handover Interface for Lawful Interception (LI). 3GPP TS 33.108 V9.1.0.

Diffie, W., van Oorschot, P.C., Wiener, M.J., 1992. Authentication and authenticated key exchange. *Des. Codes Cryptogr.*, **2**(2):107-125. [doi:10.1007/BF00124891]

Dong, J., Ackermanna, K., Nita-Rotarua, C., 2009. Secure group communication in wireless mesh networks. *Ad Hoc Networks*, **7**(8):1563-1576. [doi:10.1016/j.adhoc.2009.03.004]

Lee, C.C., Lin, T.H., Tsai, C.S., 2009. A new authenticated group key agreement in a mobile environment. *Ann. Telecommun.*, **64**(11-12):735-744. [doi:10.1007/s12243-009-0096-z]

Manulis, M., Sadeghi, A.R., 2010. Key agreement for heterogeneous mobile ad-hoc groups. *Int. J. Wirel. Mob. Comput.*, **4**(1):17-30. [doi:10.1504/IJWMC.2010.030972]

Nam, J., Lee, J., Kim, S., Won, D., 2005. DDH-based group key agreement in a mobile environment. *J. Syst. Software*, **78**(1):73-83. [doi:10.1016/j.jss.2004.10.024]

Ng, S.L., Mitchell, C., 2004. Comments on mutual authentication and key exchange protocols for low power wireless communications. *IEEE Commun. Lett.*, **8**(4):262-263. [doi:10.1109/LCOMM.2004.825724]

Sun, B., Yu, B., 2009. The Three-Layered Group Key Management Architecture for MANET. Proc. 11th Int. Conf. on Advanced Communication Technology, p.1378-1381.

Tseng, Y.M., 2007. A secure authenticated group key agreement protocol for resource-limited mobile devices. *Comput. J.*, **50**(1):41-52. [doi:10.1093/comjnl/bxl043]

Um, H., Delp, E.J., 2006a. A Secure Group Key Management Scheme for Wireless Cellular Networks. Proc. Third Int. Conf. on Information Technology: New Generations, p.414-419. [doi:10.1109/ITNG.2006.17]

Um, H., Delp, E.J., 2006b. A New Secure Group Key Management Scheme for Multicast over Wireless Cellular Networks. Proc. 25th IEEE Int. Performance Computing and Communications Conf., p.23-30. [doi:10.1109/.2006.1629386]