國立交通大學

資訊科學與工程研究所

碩士論文

以群組認證金鑰支援跨網域漫遊的認證與金鑰分配機制

Group Authentication Key-based Authentication and Key Agreement for Inter-network Roaming

研究生：陳鈺玟
指導教授：曾建超　教授

中華民國　九十六　年七月

以群組認證金鑰支援跨網域漫遊的認證與金鑰分配機制

Group Authentication Key-based Authentication and Key Agreement for Inter-network Roaming

研 究 生：陳鈺玟　　Student：Yu-Wen Chen

指導教授：曾建超　　Advisor：Chien-Chao Tseng

國 立 交 通 大 學

資 訊 科 學 與 工 程 研 究 所

碩 士 論 文

A Thesis

Submitted to Institute of Computer Science and Engineering

College of Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer Science

July 2007

Hsinchu, Taiwan, Republic of China

中華民國九十六年七月

以群組認證金鑰支援跨網域漫遊的認證與金鑰分配機制

研究生： 陳鈺玟　　指導教授： 曾建超 教授

國立交通大學資訊學院資訊科學與工程研究所

摘　要

本論文提出一個群組認證與金鑰分配機制，這個機制可以減少行動台(mobile station; MS)的服務網路(Serving Network; SN)與家網路(Home Network; HN)之間的認證訊息流量。在傳統的無線網路認證與會議金鑰產生機制中，SN 對於每一個來訪的 MS 都會發出認證需求，要求 MS 的 HN 進行 MS 的認證並回傳 MS 的認證資料，因此當有多個 MSs 漫遊至同一 SN 時，這些 MS 的認證需求會產生 SN 與 HN 之間的訊息流量以及網路延遲，影響即時通訊系統的服務品質。因此本篇論文以群組認證的概念，利用群組成員經常一起漫遊或漫遊於相同路線的特性，讓第一個執行認證程序的 MS 在認證同時，順便幫同群組的其他 MS 取得可共享的群組認證資料。若群組成員想在同一個 SN 上認證，則 SN 上的認證者(Authenticator)可直接利用先前取得的群組認證金鑰來與 MS 進行近端認證(Local Authentication)，不用再向 MS 的 HN 發送認證的訊息。因此可以減少 SN 與 HN 之間的訊息流量與認證延遲，大幅改善 MS 於無線網路漫遊時的認證速度與效能，更提昇了即時通訊的服務品質。

關鍵詞：群組，認證，認證與金鑰分配機制，群組金鑰，漫遊，網路。

Group Authentication Key-based Authentication and Key Agreement for Inter-network Roaming

Student： Yu-Wen Chen　　Advisor： Dr. Chien-Chao Tseng

Institute of Computer Science and Engineering
College of Computer Science
National Chiao Tung University

ABSTRACT

This thesis presents a Group Key-based Authentication and Key Agreement (GK-AKA) mechanism to reduce the number of authentication messages exchanged between a serving network (SN) and the home network (HN) of a mobile station (MS). Current Authentication and Key Agreement (AKA) protocols are designed for an SN to authenticate each individual MS in wireless environments. Therefore, when multiple MSs from the same network visit an SN, the SN needs to ask the HN of the MSs to authenticate each MS and return the MS's authentication data individually. Each of these authentications will cause a number of authentication messages exchanged between the SN and HN of the MSs, and lengthen the handover latency, which may degrade the quality of real-time services.

In this thesis, we propose a GK-AKA mechanism that adopts the concept of group authentication to eliminate the number authentications between the SN and HN of the MSs. In many circumstances, a group of MSs may roam together or along the same path, or visit the same SN. In GK-AKA, when the first MS of an MS group visits an SN, the SN will perform a "full" authentication with the MS's HN, and obtain the authentication

data not only for the first MS but also for the rest of the MSs of the same group. Later on, when an MS of the same group visit the SN, the SN can authenticate the MS locally, without sending authentication request to the MS's HN. Performance analysis shows that GK-AKA can reduce the authentication signal overhead between SN and HN significantly.

Index Terms—security, group key, AKA (Authentication and Key Agreement), roaming, wireless network.

誌　謝

首先，我要感謝我的指導教授-曾建超老師兩年來的悉心指導。兩年前剛考上交大資工所，去敲老師的門、表達加入意願時，老師還希望我能多考慮其他領域的教授。最後是我三顧茅廬，厚著臉皮硬『盧』很久，老師才願意將我收入門下。拜在曾老師門下的這兩年來，我除了學習到許多專業知識外，也深刻體認到做學問的第一步就是要積極奮發、主動出擊。

同時要感謝曹孝櫟教授、紀光輝教授與蘇坤良教授於百忙之中撥冗審閱我的碩士論文並擔任口試委員，老師們所提供的寶貴建議本篇論文更為完善，也感謝老師們的指導於鼓勵，讓我在學術的路上能獲得更多經驗。另外也要特別感謝曹孝櫟教授提供我聯發科技的工讀機會，以及指導我如何進行工研院的專利攻防口試。

本篇論文的原始構想源自王瑞堂(以下簡稱 RT)學長。當老師在國外參訪時，因為有了 RT 的指導與從旁協助，讓我能早早立定研究方向，多方蒐集資料。而與 RT 討論時，也學習到從不同的角度衡量問題解法的可能性。與 RT 合作最大的樂趣就是互相攻擊對方的安全機制是否真的安全，在腦力激盪的同時，往往可以順道改進自身方法的缺點。感謝 RT 給予我的一切協助，祝 RT 能早日畢業，順利拿到博士學位。

此外，我要感謝前瞻資料庫實驗室(Advanced Database System Lab)的博士班洪智傑學長，他在資料分析方面給予我相當大的協助，除了教導我如何將繪圖軟體與文書處理軟體運用得淋漓盡致之外，同時也在我求學的路上不斷地鼓勵我。沒有他的陪伴，我無法平安順利地渡過兩年的研究所生涯。祝智傑學長也能早日畢業，拿到博士學位。

朋友們，感謝你們在我生活中所給予的幫助與精神上的鼓勵，讓我沉重的壓力能得到舒緩。而交大的學長、同學、學弟們，感謝你們豐富我的校園生活。

感謝外婆時常燉雞湯幫我補身子，感謝九十高齡的奶奶頂著大太陽來參加我的畢業典禮。最後，要感謝我的家人們全力支持我追尋自己的夢想，對於我任性辭去工作的決定，毫無怨言。

僅以此論文，獻給我最親愛的家人、與關心我的師長朋友們。

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

With the tremendous growth of mobile services and applications, wireless network brings up a whole new experience to people's daily life. The wireless networks can be simply divided into two major categories: Data Networks and Cellular Networks. Different infrastructures provide distinct uses. One of the most prevalent data networks is WLAN [17] which is operated by IEEE 802.11 standard. WLAN can be easily built up and is popular with the low cost and high bandwidth. Cellular networks including GSM [16], GPRS [16], TETRA [20], and UMTS [15], provide wider communication range than general data networks. The cost to construct the whole network system is extremely high and the bandwidth of communication is relatively low. With the amazing rangy distance, cellular networks still reverse the way how people communicate.

Data in wireless networks are transmitted over the air that makes the wireless communications vulnerable. In order to secure wireless communications, many researches have proposed numerous schemes to provide different security level. Extensible Authentication Protocol (EAP) [1] provides multiple authentication methods. EAP-Authentication and Key Agreement (EAP-AKA) [3] developed by 3rd Generation Partnership Project (3GPP) based on both challenge-response mechanisms and symmetric secret keys is now commonly used in wireless networks and provides compatibility to WLAN, GSM network, and UMTS network. The conventional AKA protocols for wireless network consist of 3 main components: the roaming MS group who send out authentication requests, the SN who provide access to internet for roaming MSs and stands for the au-

thenticator, the HN who manages the MS profile and plays as the authentication server (AS). Majority of the AKA protocols are designed for individual mobile station (MS) while the group communication become one of the most desired real-time applications.

Group communications over wireless network such as video conference, chatting programs, and games, have some special properties: 1. MSs often communicating to each other usually belong to the same Home Network (HN), 2. MSs in the same group tend to migrate to the same Serving Network (SN). For example, some employees in the same company on their way to a meeting place hold a conference call; a public transport company whose buses are all equipped with mobile routers (MR) so that the passengers can access internet via the MR on bus, and buses on the same route are requested to be authenticated by the same SN around the route; firemen with TETRA handsets on the move to the places on fire. Those group communications rely on real-time services and are sensitive to the latency caused by handoff. However, the security protocols which aim to provide secure communications increase the handoff delay. Moreover, the conventional AKA mechanisms designed for individual MS may produce multiple Authentication Data Request messages for each roaming MS sent from the same SN to the same HN since the MSs in the same group usually belong to the same HN. Hence, when the roaming MS group send authentication request to the SN may cause the signaling overhead between SN and HN as shown in Figure 1-1.

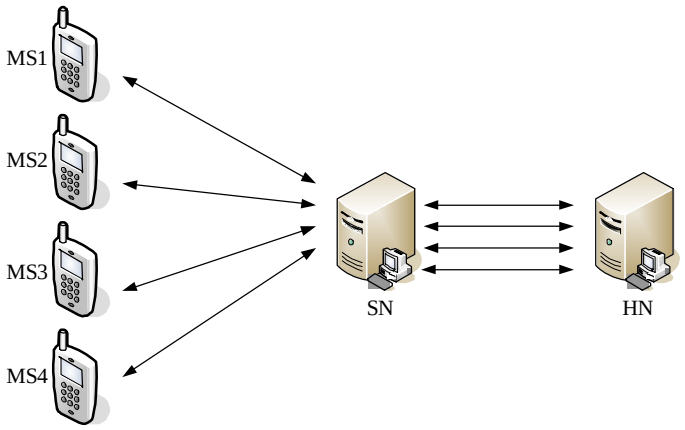


Figure 1-1 Signaling overhead between SN and HN while Authentication

For example, when some Taiwanese with CHT mobile phones tour round Hong Kong, the CHT company will be charged the registration commission from the telecomm operator in Hong Kong on handling roaming CHT mobile phones.

1.2 Objective

Since the mobile stations belonging to the same HN are apt to handoff together to the same SN, the MSs group could share a group secret and reversely take the advantage of sharing group secret as a trick to reduce the original repeating traffic between SN and HN.

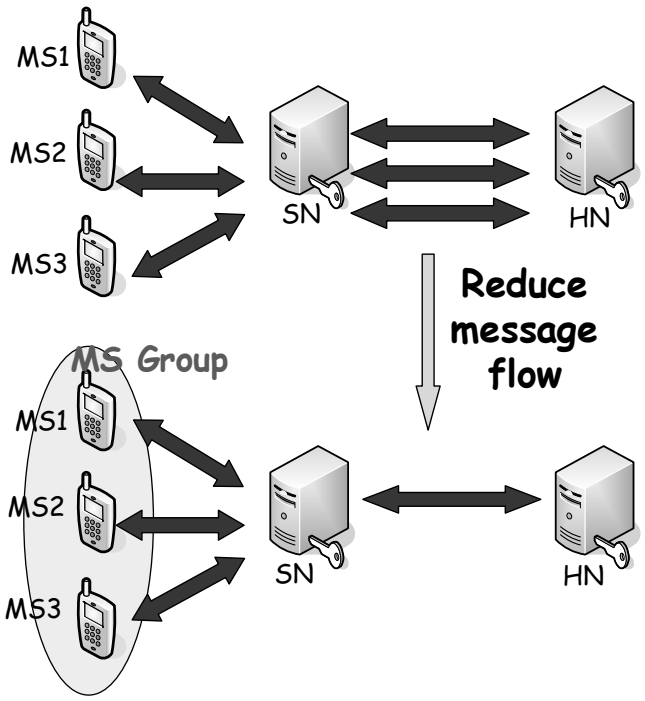


Figure 1-2 Reduce the signaling overhead between SN and HN

Let the MSs in the same group share a group secret for group authentication that every member in group can use the group secret to authenticate itself while roaming to a foreign network. The first member initiates the authentication procedure sends an authentication request message to SN with his individual identity (MS ID), group identity (GID) and other necessary information. Based on the GID, SN can obtain authentication data for group from HN instead of for individual MS. As show in Figure 1-2, the group

authentication data stored in SN can be re-used for the rest member in group without extra messages exchanged between SN and HN. Thus the signaling overhead can be reduced. Furthermore, with the existing group authentication data in SN, full authentication backward to the HN is not required and local authentication takes place instead.

The objective of this research is to reduce the signaling overhead between SN and HN. This is achieved by providing group authentication data for SN when the first member in roaming MS group request for authentication so that authentication data are pre-distributed for the rest members in group. The proposed AKA mechanism should be able to fulfill following requirements:

1. Perform on the premise that the network has property of group.
2. Reduce the signaling overhead between SN and HN.
3. Provide an end-to-end security channel between the MS and SN.

1.3 Synopsis

The remainder of this thesis is organized as follows. Chapter 2 briefly introduces background technologies and related work. Chapter 3 presents the proposed mechanism, including the system architecture and message flows. We analyze the security and signaling overhead of the proposed mechanism in chapter 4. In the end, we conclude the thesis and introduce our future works in chapter 5.

Chapter 2

Background and Related Work

This chapter presents some popular AKA mechanisms for the fabulous 3G networks. After a brief introduction to the basic system architecture, both the pro and con are analyzed and discussed as the related work.

2.1 UMTS AKA

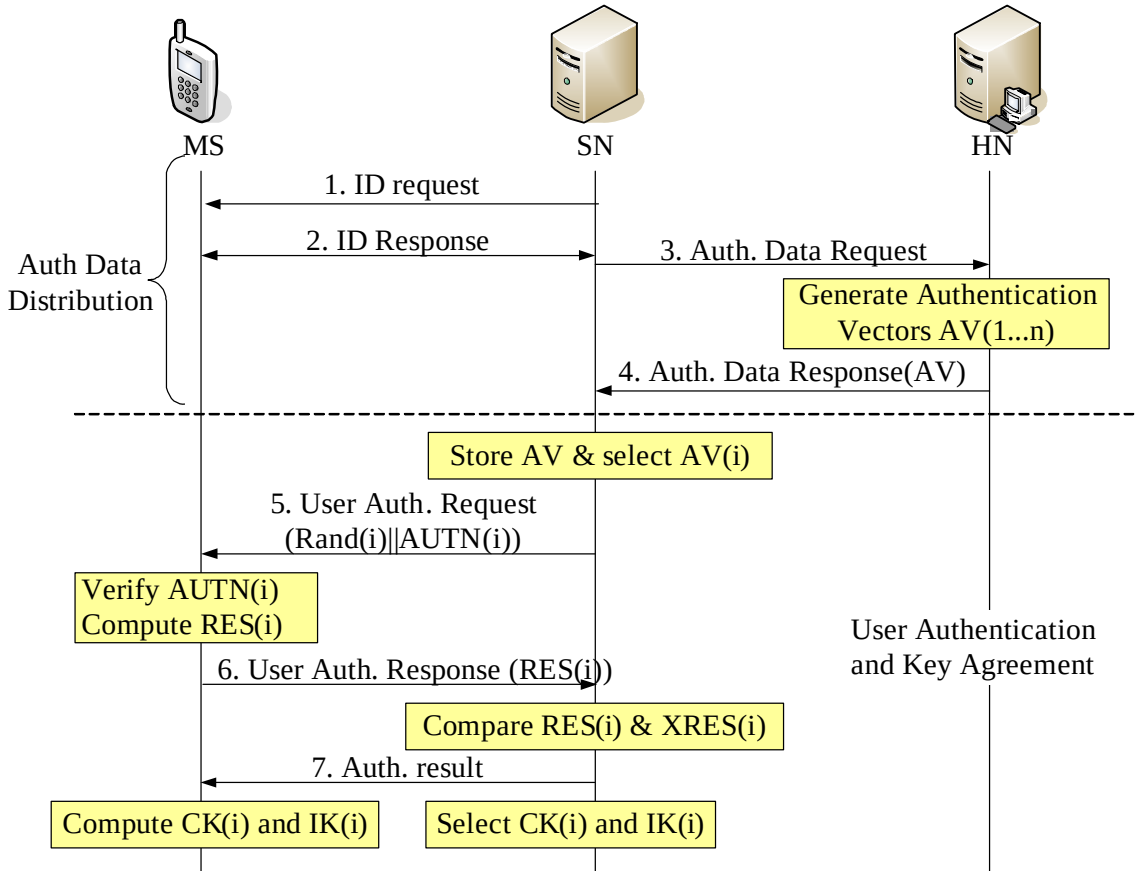


Figure 2-1 An overview of UMTS AKA mechanism

The AKA procedure are extensively applied into widely divergent formats in multifarious networks for its facility and brief principle. Take UMTS AKA [14] for example. The

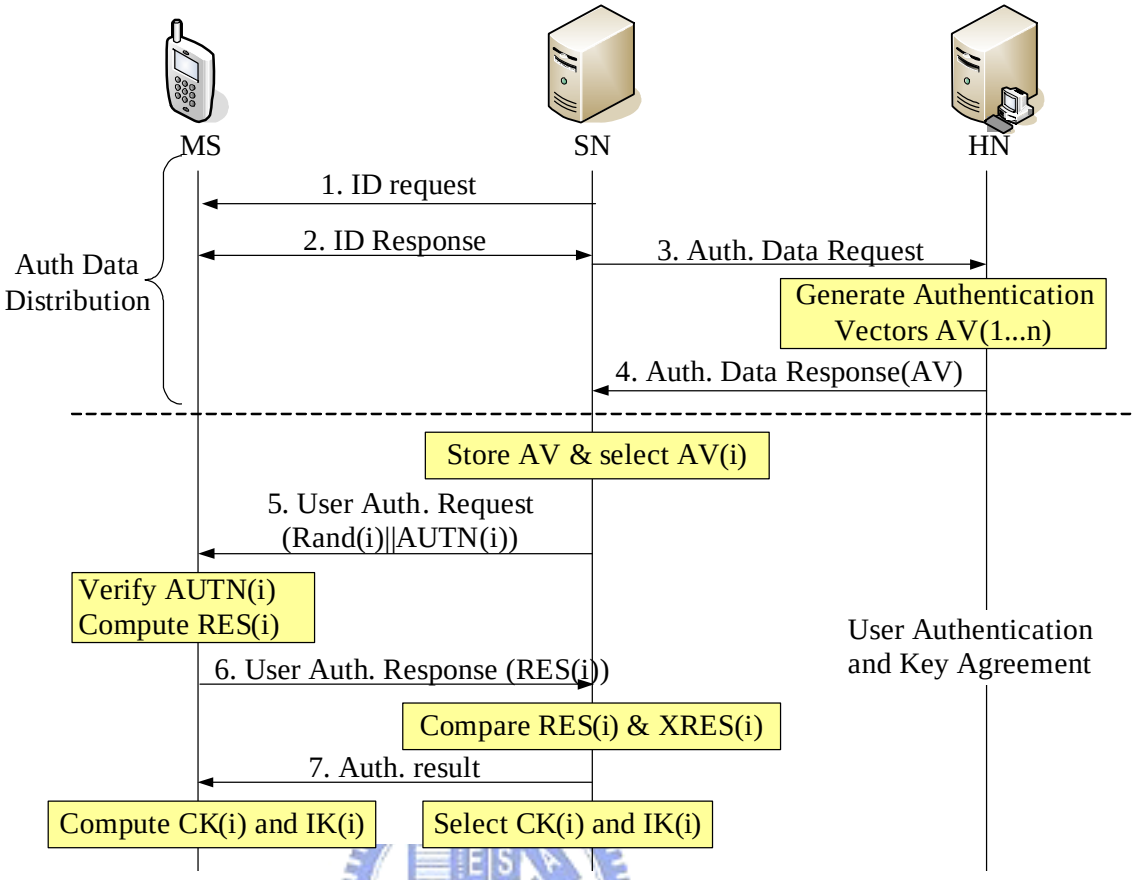
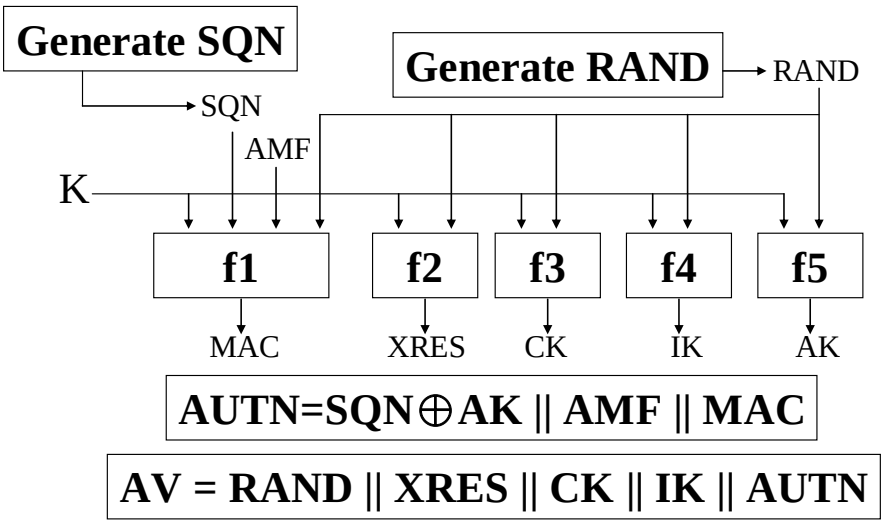


Figure 2-1 shows the overview of UMTS AKA protocol. The entire UMTS AKA mechanism can be divided into two procedures: I. Authentication Data Distribution and II. User Authentication and Key Agreement. The first procedure is for HN to distribute the request authentication data for proper SN which provides access to Internet for the roaming MS. The second procedure is to establish a new pair of reliable session key between MS and SN. This process is illustrated in 7 major steps below:

1: ID Request: Upon MS proposing an access request, Serving Network (SN) initiates the authentication procedure by sending requests to MS and asking for MS's identity.

2: ID Response: The International Mobile Subscriber Identity (IMSI) of MS is sent from MS to SN so that SN can identify MS and transfer the authentication request backward to the HN of MS.



AMF: Authentication Management Field
AUTN: Authentication Token
CK: Cipher Key
IK: Integrity Key

Figure 2-2 Operation in HN in UMTS AKA

3: Authentication Data Request: The purpose of this step is for SN to request Authentication Vectors (AV(i…n)) from the Home Network (HN). The ordered list on "n" authentication vectors based on sequence number (SQN) may be computed or pre-computed on demand and sent from HN to SN. The operation of generating each attributes in AV is shown in Figure 2-2. A cipher key K for MS, a random number RAND are the common parameters used as input in addition to Authentication Management Field (AMF) and Sequence Number (SQN) to generate AV(i) comprising MAC (Message Authentication Code), XRES (eXpected Response), CK, IK, AK (Anonymity Key) and AUTN (Network Authentication Token).

4: Authentication Data Response: After generating the AV for specific MS, HN sends it to SN so that SN is authorized to authenticate MS with the temporary authentication data.

5: User Auth. Request: After generating the AV for specific MS, HN sends it to SN so that SN is authorized to authenticate MS with the temporary authentication data. Up receiving the message from HN, SN selects the next unused Authentication Vector from

the ordered array and then sends both the RAND(i) and AUTN(i) of the ith selected vector to MS so that MS can verify the correctness of SQN and computes the proportional response RES(i).

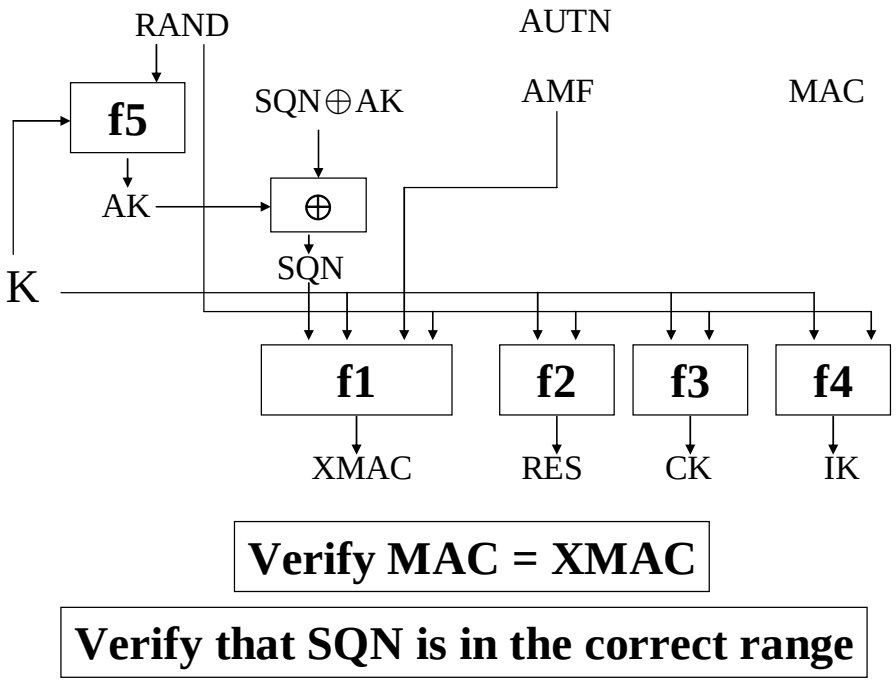


Figure 2-3 Operation in MS in UMTS AKA mechanism

6: User Auth. Response: MS verifies the correctness of SQN first by computing a XMAC and comparing it with the MAC in AUTN(i). If the SQN is correct, MS then computes the proportional response RES(i) and sent it back to SN in the response message. The operation in MS is illustrated in Figure 2-3.

7: Auth. Result: Once the RES(i) is sent to SN and verified correct, the SN chooses the corresponding CK/IK as the session key for the following connection. While waiting for the authentication result, MS computes the CK/IK in advance for usage until new authentication procedure is requested or Disconnection.

2.2 UMTS X-AKA

To reduce the traffic between SN and HN, Chung-Ming Huang and Jian-Wei Li pro-

posed another AKA protocol called UMTS X-AKA [4]. The Figure 1-1 illustrates the detail steps of X-AKA. The concept of UMTS X-AKA is to realize local authentication by means of a transient key TK generated by HN and stored in SN. The UMTS X-AKA can be decomposed into two major procedures: (1) Registration & Distribution of Authentication Vectors, (2) Authentication & Key Agreement (for the j-th round)

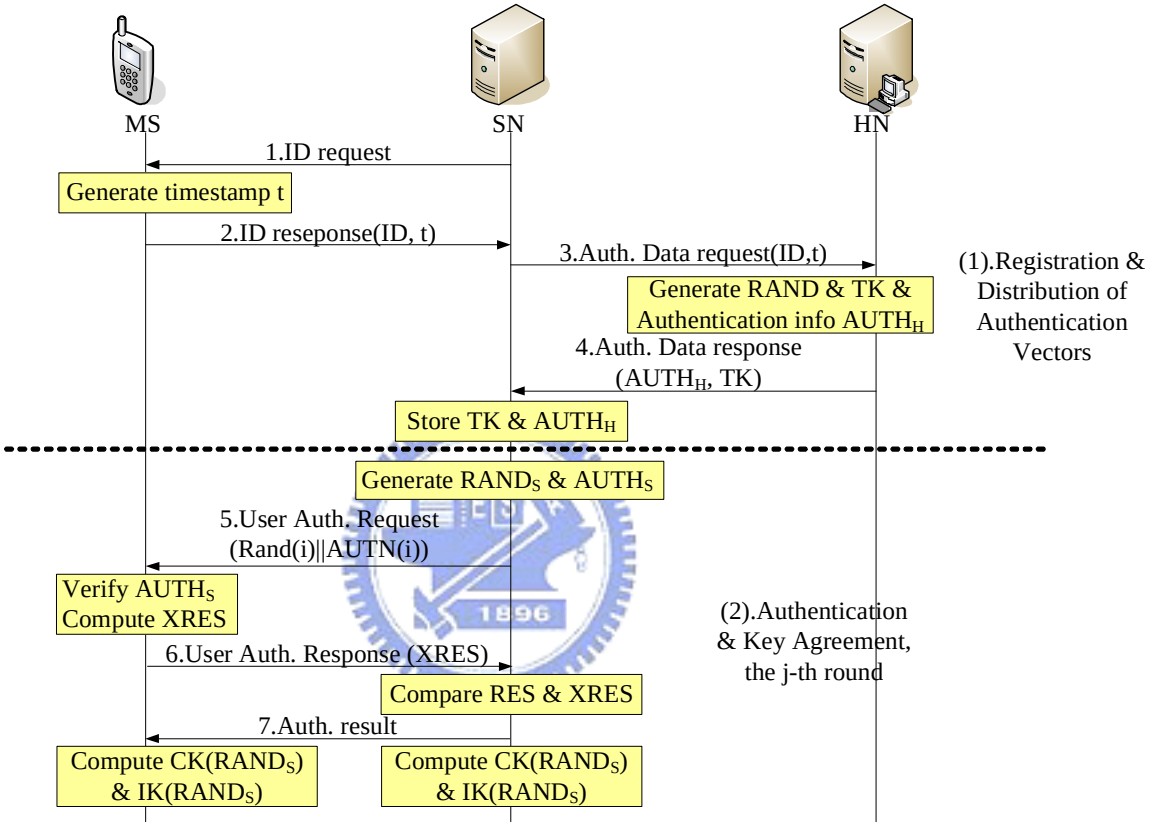


Figure 2-4 An overview of UMTS X-AKA mechanism

The UMTS AKA provides mutual authentication and the freshness assurance of the agreed session key. Compared with GSM AKA, the UMTS AKA is proven to be relatively secure [12] not only in reply attack caused by limited authentication data but also in false base station attack caused by unidirectional authentication. However, the UMTS AKA has three known flaws in (1) bandwidth consumption between HN and SN, (2) storage space of SN for spare authentication vector, and (3) sequence number synchronization. (1) and (2) are solve in UMTS X-AKA. However, the synchronization still cost for extra messages in UMTS X-AKA

However, most of the conventional AKA mechanisms are for single Mobile Station. When multiple MSs communicate and move as a group in Wireless Network, the current AKA mechanisms are suffered from the same issue: SN has to transfer multiple messages with Authentication Data Request for different MSs to the same HN and receive response messages with Authentication Data since the MSs in the same group belong to the same HN. Based on the group concept, we propose a sharing group authentication key-based Authentication and Key Agreement mechanism to reduce the signaling overhead between SN and HN. With this group authentication procedure, not only the bandwidth between SN and HN is saved but also the key pre-distributed is achieved for group members.

the next chapter.

Chapter 3

Group Authentication Key-based AKA

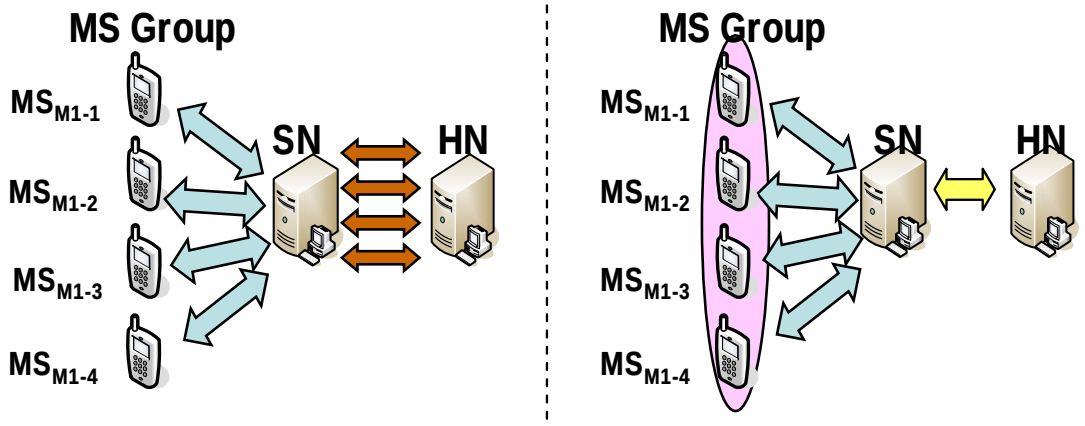
The aforementioned authentication and key agreement protocols are widely implemented, however, the complexity and costs are relatively high when bursts of authentication messages pump for group communications. In this paper, we propose an adaptive authentication protocol based on group authentication key to lessen the complexity and latency caused by group authentication. The idea of grouping mobile stations is based on clustering; people living in the same community, working in the same company, studying in the same campus, or even casually being on the same bus, tend to move from one place to another together. When a group of mobile users migrates simultaneously, the first member who hands off may provide not only a personal identity but also sometimes a group identity to serving network. In our approach, however, mobile station provides only individual identity. The serving network may first check if this MS belongs to any active group which any members has already finished his authentication procedure and made the group authentication data available in database of serving network for the rest members in the same group. Assume that MS1 is the first member who performs authentication procedure when handoff, SN may obtain some authentication data for both MS and his group from their home network. Instead of generating and distributing individual authentication data for each mobile station respectively, our scheme produce authentication data for groups of users so that mobile stations in the same group share the same batch of authentication data including group transient authentication key and information in group list. By reducing the redundant messages, such as *Authentication Data Request* sent out by different MS in the same group to the same home network, the system may avoid suffering from significant latency and bottleneck

between serving network and home network.

The proposed protocol can be divided into three main procedures: 1.Setup procedure, 2. Authentication Data Distribution, 3. Mutual Authentication and Key Agreement. We will describe the details of each step from section 3.2.

3.1 Architecture

The basic architecture is shown in Figure 3-1 where Figure 3-1(a) shows how the traditional AKA protocols work with roaming MS group and Fig.(b) the proposed GK-AKA. The HN represents the Authentication Server (AS) or the Authentication Center (AuC) which controls and manages all the authentication data for MS. The SN represents the authenticator in various wireless networks, such as Access Point in 802.11 network, or Serving Network in cellular network. Without loss of generality, the roaming group is called G1 with group identity ID_{M1}. The roaming MSs are numbered in sequence as MS_{M1-1} the first member who performs authentication procedure, and the following members sending authentication request are MS_{M1-2}, MS_{M1-3}, and MS_{M1-4}.



(a). The traditional AKA (b). The proposed GK-AKA

Figure 3-1 System Architecture for roaming MS group

3.2 Setup Procedure

Unlike conventional AKA protocols generating difference authentication data for indi-

vidual MS, our proposed mechanism provides group authentication data for a set of mobile stations. Thus before the AKA mechanism starts, the HN generates the group authentication data and distributes the necessary part to mobile stations in the same group. Group authentication data includes 1). *Group Information* and 2). *Message Authentication Code (MAC) Algorithms*. The Group Information consists of the Group Authentication Key (GAK) shared by HN and group members and the Index Table stored in only HN shown in Table. 1. After this step, HN holds the GAK and the Index Table while each MS holds the GAK, Group ID, its individual member ID and Initial Value, and is unaware of other MSs' personal information.

3.2.1 Group Authentication Key (GAK)

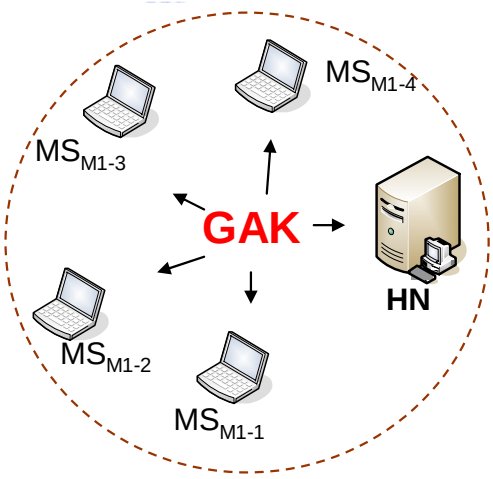


Figure 3-2 Group Authentication Key

For the most part of networks, Group Key is introduced for encryption. Each member in the trust-group owns an individual key for end-to-end communication and shares a common group key for group communications. Here we define an entirely difference group key called Group Authentication Key (GAK) which is still shared by all members in the same group as shown in Figure 3-2 and used in not encryption but authentication. One MS can belong to more than one group and hold multiple GAKs as shown in

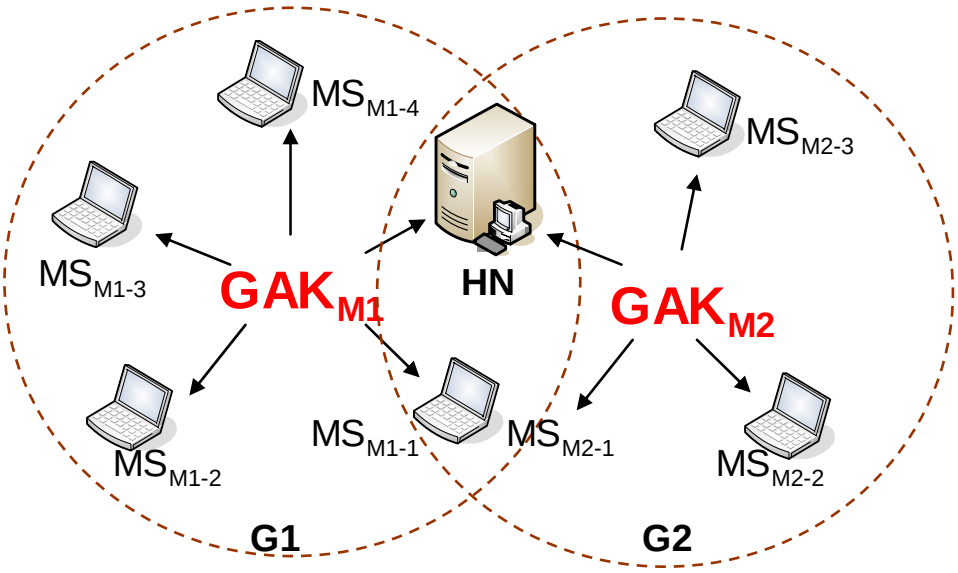


Figure 3-3.

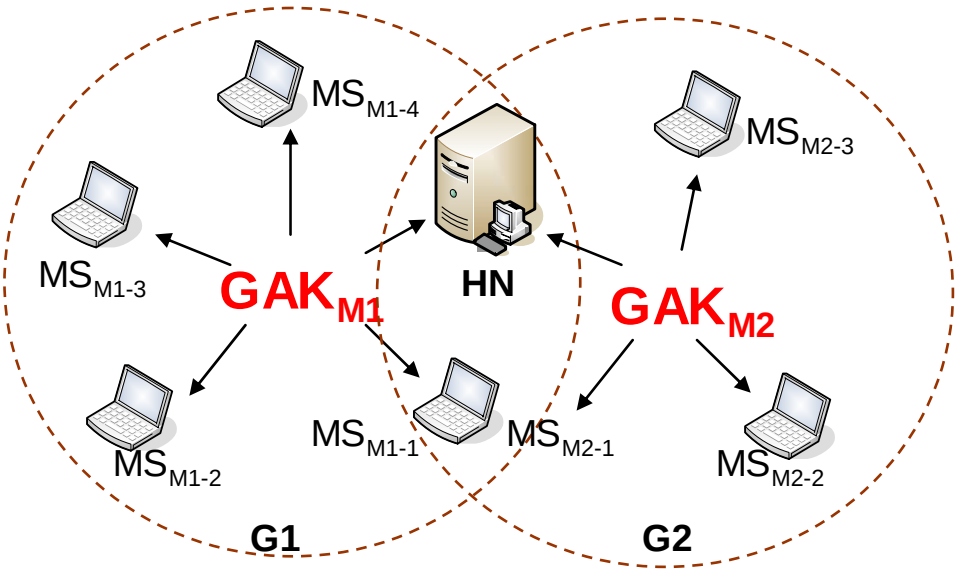


Figure 3-3 One MS belongs to multiple MS groups

The GAK, as well as the individual authentication key for each MS, may be pre-defined or computed on demand. The generation and distribution of GAK with the members joining or leaving are managed by the Authentication Center (AuC) in users' home network, and the details will not be discussed in this paper and can be referred to [10].

3.2.2 Index Table

Table I. Index Table

Group	Group ID	Member ID	Initial Value	Other Info
G1	ID_{M1}	ID_{M1-1}	IV_{M1-1}	…
		ID_{M1-2}	IV_{M1-2}	…
		ID_{M1-3}	IV_{M1-3}	…
		ID_{M1-4}	IV_{M1-4}	…

The major attributes comprise Group Identity (GID), Group Authentication Key (GAK), Member Identities (MS ID), Initial Value (IV_i) for each member, and other information. In this proposed protocol, the digits of initial value IV_i are so large that each value is unique and distinct from one another and no members can spy on others' initial values. With the peculiarity of practically unlimited, the initial value of members can also be different and unique from group to group. Besides the facility for distinguishing from members, the initial value IV_i also behaves as the sequence number in UMTS AKA where SQN is responsible for the synchronization between MS and SN in User Authentication Procedure in UMTS AKA.

3.2.3 Message Authentication Code (MAC) Algorithms

The cryptographic MAC algorithms are short pieces of information used to authenticate a message. The inputs for MAC algorithms consist of a secret key and some information and outputs generated by MAC algorithms are usually not reversible. The MAC algorithms used in the proposed approach are:

f0: generating MAC for HN to authenticate MS.

f1: generating MAC for MS to authenticate SN.

f2: generating MAC for SN to authenticate MS.

f3: key generation.

3.3 Authentication Data Distribution Procedure

The idea of the proposed protocol relies on the premise that members in the same group tend to migrate continuously and the latency arises from handoff procedure is proportional to the number of drifters. For n mobile stations, conventionally, SN has to send n *Authentication Data Request* message separately. However we now reduce the redundant messages to the same destination arisen from different members in the same trust group by providing the group authentication data-Group Transient Key (GTK)-substituting for the original GAK so that the primitive authentication key will not be revealed and the computed transient key can be periodically updated based on the random number provided by SN and MS to ensure the freshness of authentication material.

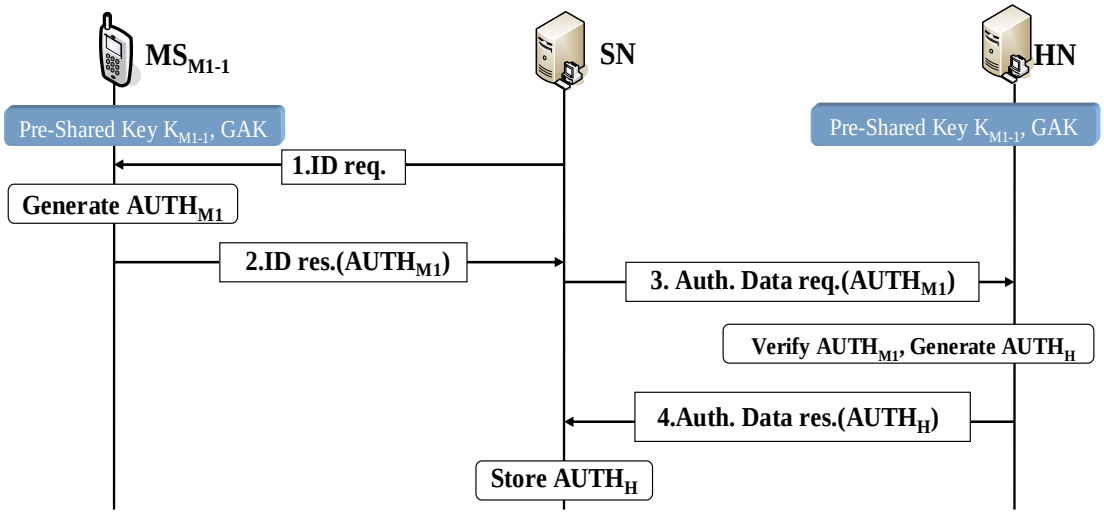


Figure 3-4 Distribution of Authentication Data in the proposed AKA mechanism

Let the first member who performs authentication procedure be MS_{M1-1}. Figure 3-4 illustrates the operation of GAK. The detail steps are as follows:

1. ID Req.: SN tries to get MS_{M1-1}'s identity.

2. ID Res.($AUTH_{M1}$): Upon receiving the *ID Req.* message, MS_{M1-1} generates

$$AUTH_{M1} = (ID_{M1}||ID_{M1-1}||RN_{M1-1}||MAC_{M1-1})$$

where ID_{M1} the GID, ID_{M1-1} the MID, a random number RN_{M1-1}, and MAC_{M1-1} =

$f0(K_{M1-1}, RN_{M1-1})$ for HN to authenticate MS before distributing group authentication data to SN. The detail operation is presented in Figure 3-5.

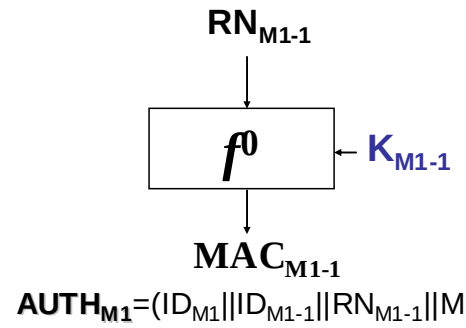


Figure 3-5 Generation of MAC_{M1-1} in MS in the proposed GAK-AKA mechanism

3. Auth. Data Req.($AUTH_{M1}$): Since MS_{M1-1} is the first MS in group, SN has no data to authenticate MS_{M1-1}. SN then transfers the message to HN and requests for data to authenticate the roaming group G1 which MS_{M1-1} belongs to.

4. Auth. Data Res.($AUTH_H$): HN first verifies the MAC_{M1-1} in $AUTH_{M1}$ with K_{M1-1} the pre-share key of MS_{M1-1}. If MS_{M1-1} is confirmed legit, HN retrieves the corresponding GAK of MS group G1 to generate a Group Transient Key (GTK)

$$GTK_{M1} = f3(RN_{M1-1}||RN_H||AMF||GAK)$$

. The group authentication data sent to SN is $AUTH_H = (RN_H||AMF||RN_{M1-1}||GTK_{M1})$ where RN_H is the random number generated by HN, AMF the Authentication Management Field, RN_{M1-1} the random number used as one of the input of GTK_{M1}, and the GTK_{M1} of course. The Index Table for G1 is also sent to SN in this step. Figure 3-6 illustrates the operation in HN while HN receives the authentication request of MS_{M1-1} from SN.

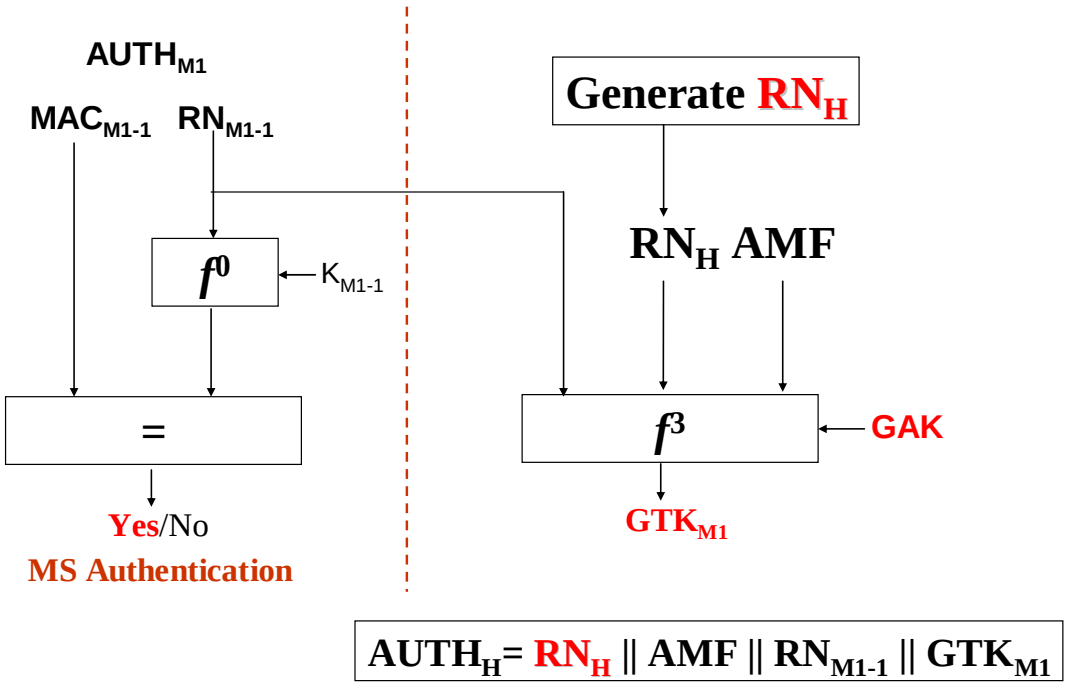


Figure 3-6 The Operation in HN when SN sends the authenticate request of MS_{M1-1}

3.4 Mutual Authentication and Key Agreement Procedure

This procedure focuses on the mutual authentication between MS and SN, and is designed to generate the session key between MS and SN so that a secure channel is established between MS and SN. Figure 3-7 presents the message flows.

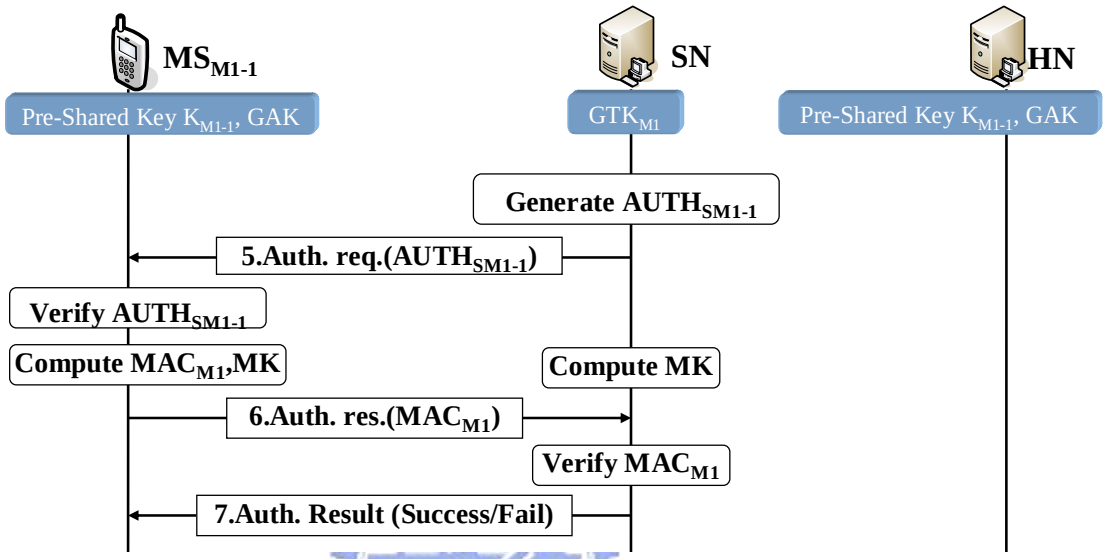


Figure 3-7 Mutual Authentication and Key Agreement in the proposed mechanism

5. Auth. Req.(AUTH$_{SM1-1}$): After obtaining the group authentication data AUTH$_H$ for MS group G1, SN initiates the *i*-th run of mutual authentication procedure between SN and MS$_{M1-1}$ by generating AUTH$_{SM1-1}$ = (AMF||RN$_H$||RN$_{M1-1}$||MAC$_S$||RN$_{SM1-1}$) where the first three parameters are necessary for mobile station to generate GTK$_{M1}$, MAC$_S$ = *f1*(GTK$_{M1}$||RN$_{M1-1}$||IV$_{M1-1}$+*i*), and a random number RN$_{SM1-1}$ generated by SN and used to challenge MS$_{M1-1}$ later. While waiting for the response from MS$_{M1-1}$, SN can compute the Master Key MK = *f3*(GTK$_{M1}$||RN$_{M1-1}$||RN$_{SM1-1}$) for the subsequent sessions between MS$_{M1-1}$ and SN in advance. The detail operations are shown in Figure 3-8.

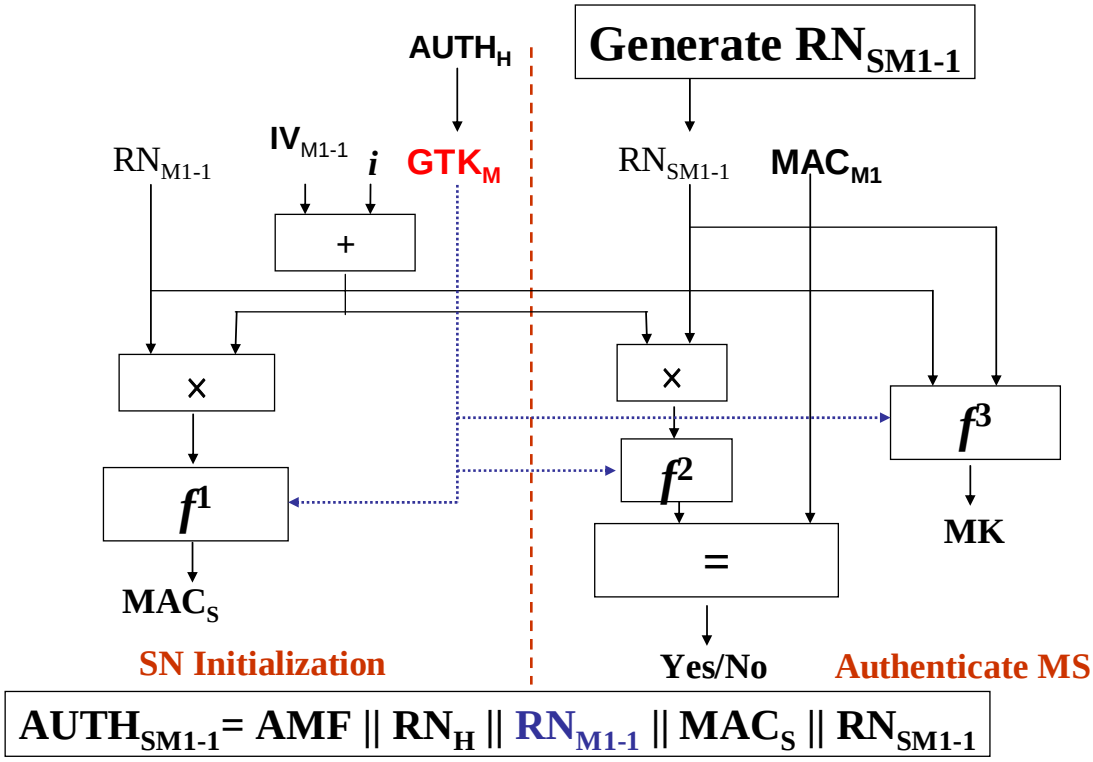


Figure 3-8 The operation in SN while authenticating MS_{M1-1}

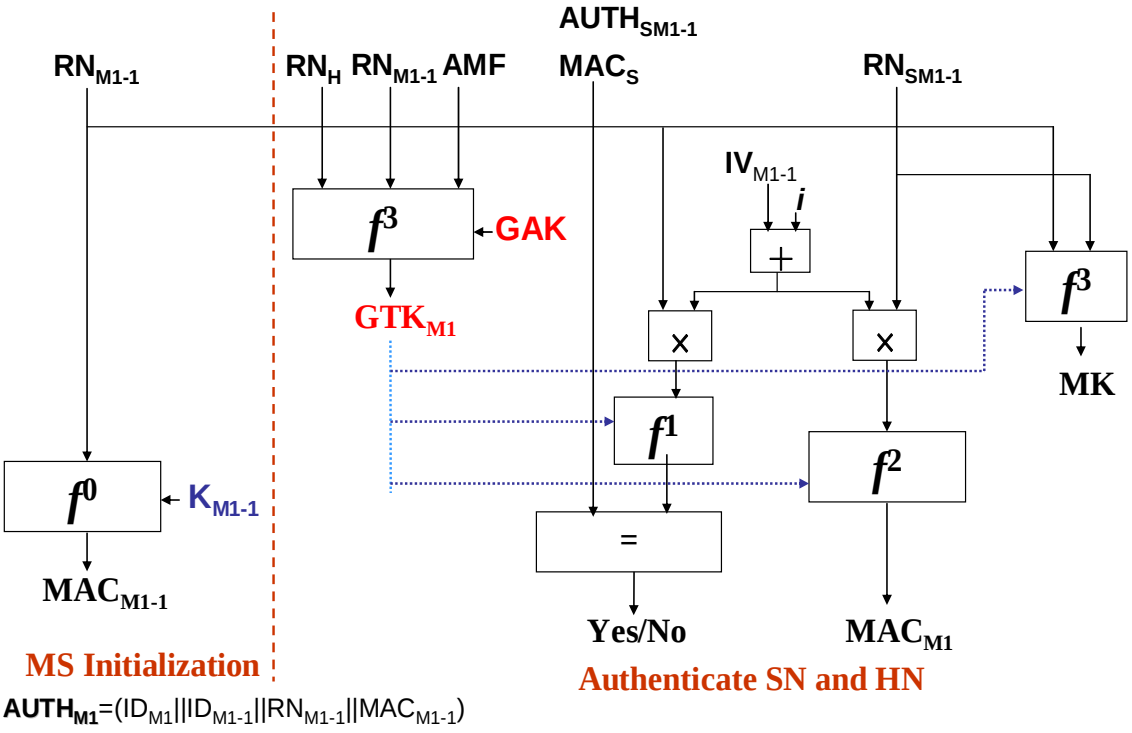


Figure 3-9 The operation in MS_{M1-1} in Mutual Authentication and Key Agreement procedure

6. Auth. Res.(MAC_{M1}): First of all, MS_{M1-1} computes the GTK_{M1} with the first three arguments in $AUTH_{SM1-1}$ and the GAK stored in each mobile station in the same group. MS_{M1-1} then authenticates SN by computing and comparing a corresponding result of MAC_S. After successfully authenticating SN, besides generating the Master Key MK between SN and MS_{M1-1}, MS_{M1-1} also generates the response message MAC_{M1} = $f2(GTK_{M1}||RN_{SM1-1}||IV_{M1-1}+i)$. Figure 3-9 shows the detail computation in MS_{M1-1}.

7. Auth. Result (Success/Fail): SN authenticates MS_{M1-1} by verifying whether MS_{M1-1} generates the correct response or not in Figure 3-8. The message sent to MS_{M1-1} indicates the result of mutual authentication procedure.

After the full authentication process, the MK generated separately after step 5 in both MS_{M1-1} and SN can be used as the material for various keys.

When the second member MS_{M1-2} in roaming MS group requests for authentication, SN initiates the mutual authentication procedure with the existing GTK_{M1} so that the original step 3 and 4 are skipped and the signals between SN and HN are eliminated. The procedure of authenticating MS_{M1-2} is shown in Figure 3-10.However, the random numbers used to compute the challenge messages, such as RN_{M1-2} for MAC_S and RN_{SM1-2} for MAC_{M1}, are entirely different from those used in authentication of MS_{M1-1}. Figure 3-11 illustrates the operation of MAC algorithms in SN when authenticating MS_{M1-2} and Figure 3-12 presents the operation in MS_{M1-2}.

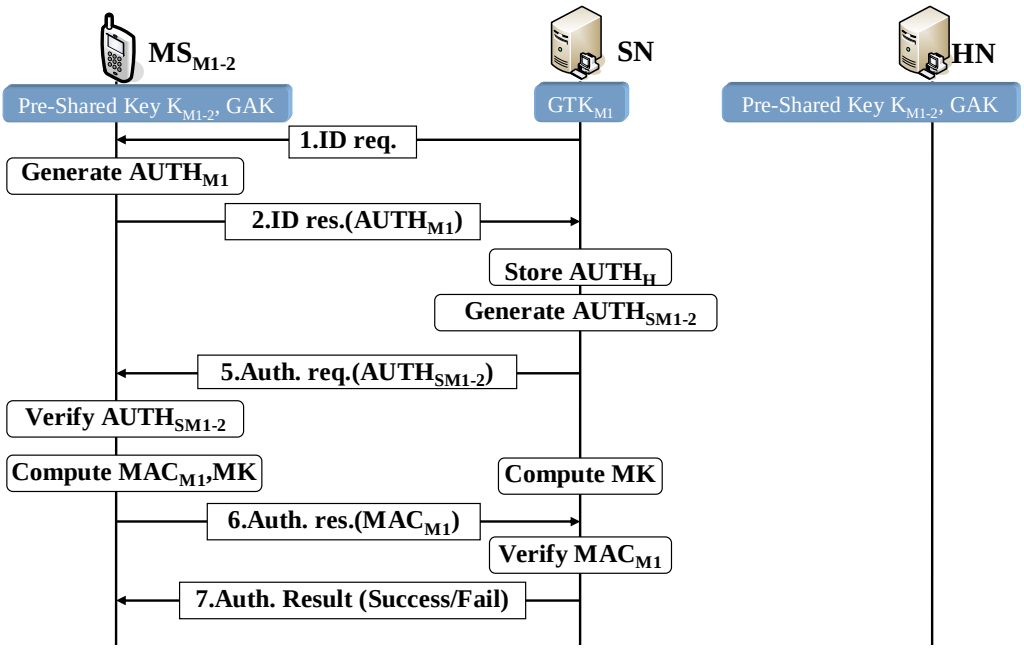


Figure 3-10 Authentication and Key Agreement for MS_{M1-2}

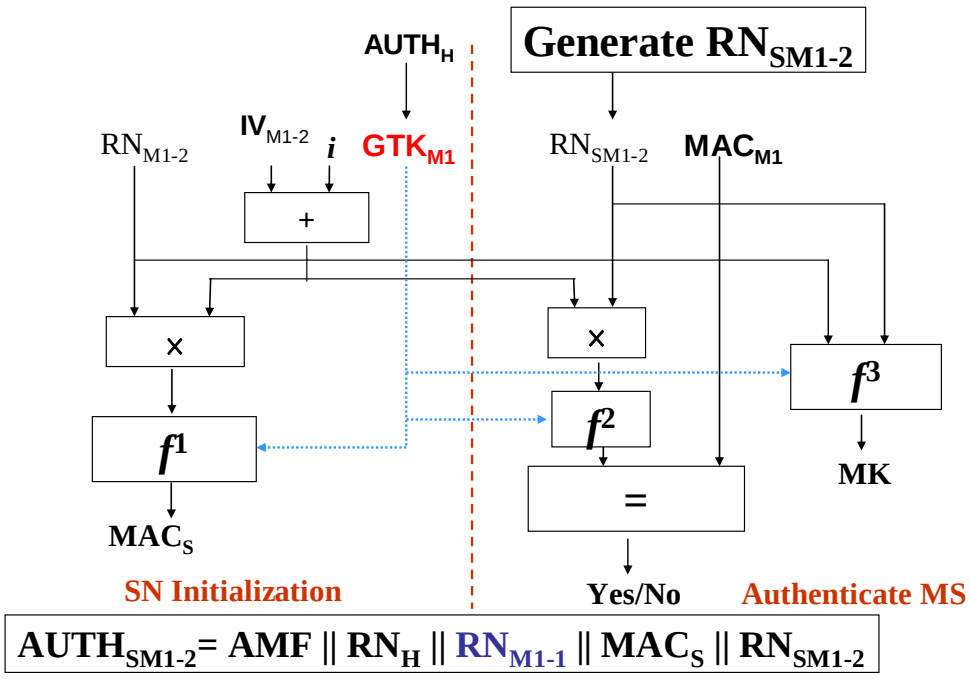


Figure 3-11 The operation in SN while SN authenticating MS_{M1-2}

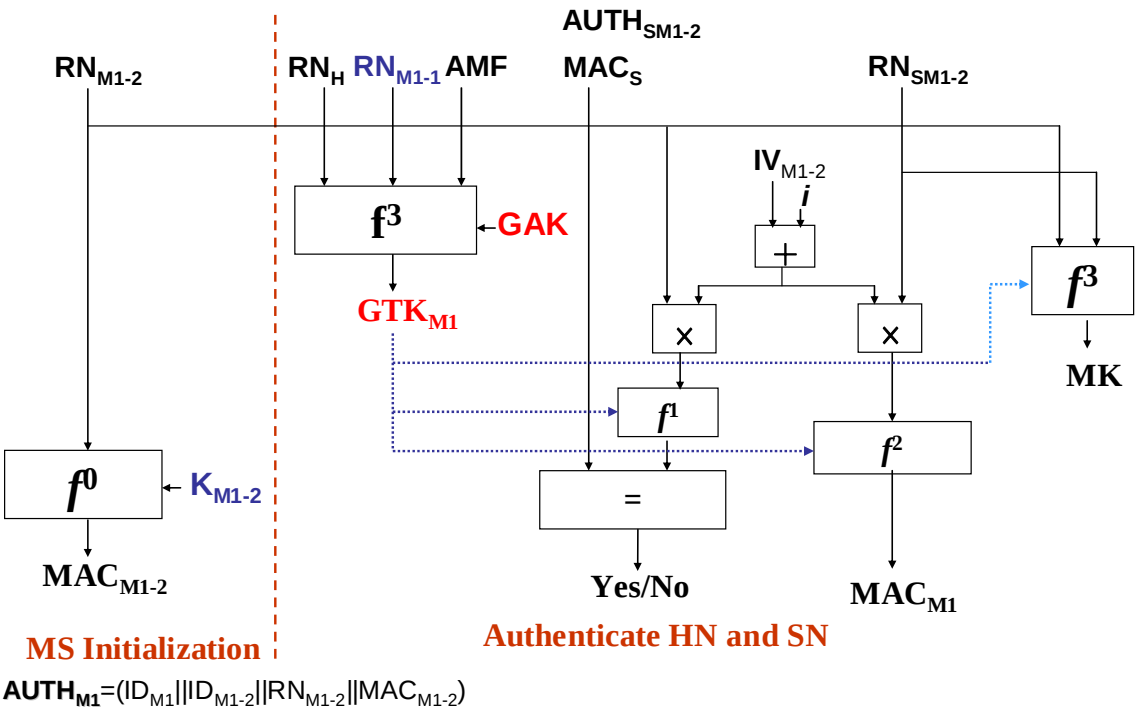


Figure 3-12 The operation in MS while SN authenticating MS_{M1-2}


E
S
A
1896

Chapter 4

Security Considerations

In this section, we discuss some performance analysis and efficiency evaluations of the aforementioned protocols in related work and our proposed GAK protocol based on the shared group authentication key. Here we consider 1.the storages cost in SN, 2.the signals transferred between SN, and HN

4.1 Security Analysis

First of all, our proposed protocol satisfies the following concepts of secure wireless network user authentication:

1. **Mutual Authentication**: In this GAK protocol, mutual authentication of MS and HN is done by producing the same GTK, and mutual authentication of MS and SN is done by generating and comparing the challenge messages RES_S and RES_M. In particular, even though all members share the same GTK, when one adversarial member, MS1 for example, tries to personate another member, MS2 for example, by eavesdropping and collecting the traffic between MS2 and SN, MS1 fails to generate the correct RES_M which must be calculated by GTK, RN_{S2}, and most important of all the initial value j_2 of MS2. In other words, the SN can easily distinguish one member from another even though all members have the same GTK and in case some of them may intercept other members' challenge messages.
2. **Reply Attack Resistance**: When an attacker attempts to intercept an authentication packet and later transmit it to the expected destination, the receipt of duplicated packet may cause some undesired consequence. In our proposed

scheme, whenever a user authentication is requested, new random numbers RN_{Mi} and RN_S from MS and SN respectively are both produced to provide temporally use of generating challenge messages. Besides, the initial value j_i in both MS and Group List stored in SN brings about the synchronization between MS and SN since they are requested to keep the same value so that SN can identify MS successfully. Therefore, the proposed protocol is able to provide reply attack resistance.

3. **Secure Key Derivation**: The session key shared between MS and SN is generated respectively by each side without any extra messages exchange in this proposed protocol. Therefore we can keep the session key from being attacked or intercepted by adversaries.
4. **Scalability**: Since the proposed protocol is based on the concept of group authentication, the number of messages is less than most of the prevalent AKA protocols when multiple users request for authentication simultaneously. The conventional AKA protocols generate different authentication data for individual mobile station while our GAK protocol uses the same GTK and Group List to authentication a party of users. Because parts of the redundant messages are reduced by using the GTK directly, our proposed method is able to process multiple authentication requests if the scale of users grows.

4.2 Performance Analysis

Our proposed mechanism takes the GTK as a substitute for the original GAK so that the primary GAK can be protected whereas the SN can be fully authorized to authenticate the roaming MS group with exactly one key instead of several distinct authentication data for individual MSs. For HN, the signaling overhead between SN is reduced. For SN, not only the communication bandwidth between HN is saved but also the storage

cost for user database is diminished. As for MS, except the first member in group, authentication key is pre-distributed without extra message exchange. Furthermore, one MS can belong to more than one group and hold multiple GAKs. Thus the MS is able to decide different group identity for group authentication when roaming to different SNs.

One of the most important performance evaluations of AKA protocols are the secure level. In our proposed mechanism, HN authenticates the legitimacy of MS before providing the group authentication data to SN so that SN cannot obtain MS's authentication data without a request message from MS. The freshness of messages for mutual authentication between SN and MS can be assured by the random number generated by both side. If a malicious MS tries to impersonate other members in the same group with the identical GAK, SN is able to identify the vicious member by comparing the IV in Index Table provided by HN. With the unique MKs for different pairs of MS and SN, the secure channel between MS and SN is established.

4.3 Efficiency Evaluation

We evaluate the storage cost by the authentication data in database of SN and approximately measure the quantities of the signals transferred between MS, SN and HN in mathematical way. The cost of storage and signals compared with UMTS AKA[15] and UMTS X-AKA[4] is tabulated in Table II ,where n is the number of mobile stations, g is the number of roaming groups, and m represents the times of authentication requests from each MS if every mobile station is assumed to send more than just one authentication request. By observing the effect caused by argument m, we can scrutinize the difference in number of signals between our proposed method and the aforementioned AKA protocols.

Table II QUALITATIVE ANALYSIS OF THREE KINDS OF AKA PROTOCOLS

mechanism	STORAGE IN SN	Signals between HN and SN	
		One MS	n MSs
UMTS AKA	n*AV(s)	2	2n
UMTS X-AKA	n*(TK+AUTH)	2	2n
GAK AKA	g*(GTK+Index Table)	2	2g

The proposed AKA mechanism only needs *g* authentication data in an SN whereas the other approaches require *n* different authentication data. Since only the very first member of each group perform full authentication, the signaling overhead in our proposed scheme is obviously *n*/*g* times less than that in [15] and [4]. Generally speaking, the number of groups *g* and is much smaller than the number of MSs *n*. Figure 4-1 shows the number of signals between SN and HN in the three AKA mechanisms, in which each MS transfers three authentication requests. Notice that the number of signals in GK-AKA is related to the number of groups, *g*, whereas factors in UMTS AKA are the number of MSs *n*, and the number of authentication requests transferred by each MS and that in UMTS X-AKA is *n* as well.

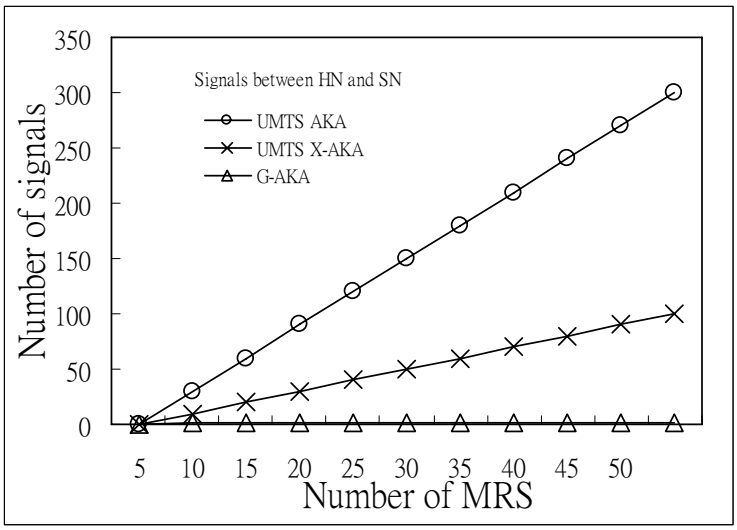


Figure 4-1 The signaling overhead between HN and SN with *g* = 1 and m = 3.


E
S
A
1896

Chapter 5

Conclusion and Future Work

We proposed an authentication and key agreement scheme based on Group Key that allows mobile stations to share a group secret including group key and identity for authentication. With the shared group authentication data, not only the signaling overhead between HN and SN is considerably reduced, but also the storage cost in SN is appreciably diminished. Thus our proposed mechanism is able to fasten the handoff procedure and provide better services for real-time applications. The proposed scheme fits all networks with group character, such as TETRA network [20], 802.16 WiMAX networks [18][19], and also the security system in company. We can extend the group concept to the serving network side when one SN cooperates with another one. By sharing the group secret, SN may be able to pre-authenticate the coming MS if the MS hands over from a member SN.


E
S
A
1896

Reference

[1] B. Aboba, et al., “Extensible Authentication Protocol (EAP)”, RFC 3748, June 2004.

[2] B. Aboba, et al., “PPP EAPTLS Authentication Protocol”, RFC 2716 IETF, October 1999.

[3] J. Arkko, et al., “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”, RFC 4187, January 2006.

[4] C.-M Huang, et al., “Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption”, Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference, 28-30 March 2005, pp.392 - 397 vol.1.

[5] H. Haverinen, et al., “Extensible Authentication Protocol Method for Global System for Mobile Communication (GSM) Subscriber Identity Modules (EAP-SIM) ”, RFC 4186 IETF, January 2006.

[6] R. Housley, et al., “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC 3280 IETF, April 2002.

[7] V. C. Joseph, et al., “Verifiable AKA for Beyond 3G Wireless Packet Services”, Wireless and Optical Communications Networks, 2006 IFIP International Conference, 11-13 April 2006.

[8] W. Liang, et al., “A Local Authentication Control Scheme Based on AAA Architecture in Wireless Networks”, Vehicular Technology Conference, 2004, VTC2004-Fall, IEEE 60th. Vol. 7, 26-29 September 2004, pp5276-5280.

[9] W. Simpson, et al., “PPP Challenge Handshake Authentication Protocol (CHAP)”, RFC 1994 IETF, August 1996.

[10] D. Wallner, et al., “Key Management for Multicast: Issues and Architectures ”, RFC 2627 IETF, June 1999.

[11] C.-K Wong, Mohamed Gouda, and Simon S. Lam, “Secure Group Communications Using Key Graph”, IEEE/ACM Trans. Netw, Vol. 8, No. 1, February 2000, pp.78-85

[12] M. Zhang, et al., “Security analysis and enhancements of 3GPP authentication and key agreement protocol”, Wireless Communications, IEEE Transactions on Volume 4, Issue 2, March 2005 pp.734 - 742.

[13] 3rd Generation Partnership Project (3GPP) [Online] Available: http://www.3gpp.org/

[14] 3rd Generation Partnership Project; Technical Specification Group SA; 3G Security, “Security Threats and Requirements”, 3GPP, TR 21.133, 1999.

[15] 3rd Generation Partnership Project; Technical Specification Group SA; 3G Security, “Report on the evaluation of 3GPP standard confidentiality and integrity algorithms, version 1.0.0, 2000-12”, 3GPP, TR 33.908, 1999.

[16] European Telecommunications Standards Institute (EISI), GSM 02.09 Security Aspects, June 1993.

[17] IEEE Std IEEE 802.11TM-

[18] IEEE Std IEEE 802.16™-2004, “IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems”, Oct. 2004.

[19] IEEE Std IEEE 802.16e™-2005, “IEEE Standard for Local and Metropolitan Aarea Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems”, Dec. 2005http://shop.ieee.org/ieeestore/Product.aspx?product_no=SS95394.

[20] TETRA MoU Association [Online] Available: http://www.tetramou.com/