通信情報保護學會論文誌
第7卷 第2號, 1997. 6

부호 분할 다중 접속 이동 통신망을 위한 인증 키 분배 프로토콜

전학성*, 김동규**

An authenticated key distribution protocol for the CDMA mobile communication network

Hak S. Jeon, Dong K. Kim

요 약

본 논문에서는 부호 분할 다중 접속(Code Division Multiple Access) 이동 통신망을 위한 안전하고 최소의 인증 및 키 분배 프로토콜을 제안한다. 가입자의 인증과 가입자 트래픽의 안전성을 유지하기 위해 CDMA 이동 통신망의 보안 프로토콜은 개발되었다. 기존 프로토콜은 이동 통신망의 무선 구간에 대한 통신 보안을 고려하였고, 유선 구간의 통신 보안은 고려하지 않는다. 본 논문에서는 무선 구간의 통신 뿐만 아니라 유선 구간의 통신 보안을 보장할 수 있는 인증 및 키 분배 프로토콜을 제안한다. 제안된 프로토콜은 사용자 식별 번호의 기밀성을 유지하면서, 기존 프로토콜과 비교하여 최소의 정보 흐름을 유지한다.

Abstract

In this paper, we introduce a secure and minimal protocol for authenticated key distribution over the CDMA mobile communication network. The CDMA mobile communication network has been developed the security protocol that provides a means for user authentication and subsequent protection of user traffic. However, this model has no security assumptions for the intermediate, fixed networks. To avoiding these drawbacks, we introduce a minimal authenticated key distribution protocol. This protocol provides the security of the intermediate and fixed network in mobile environment, and maintains the confidentiality of user identification and the minimum size of information flow compared with the existing protocols.

* 한국전자통신연구원 이동망서비스 연구실
** 아주대학교 컴퓨터공학과

I. Introduction

The CDMA mobile communication network, a commercial prototype digital cellular system based on a direct sequence spread spectrum technology, has been developed in the Korea. Several subsystems in the CDMA mobile communication networks are integrated and the mobile terminal is moving in places. In the CDMA mobile communication network, security threats such as illegal accesses and eavesdropping are exasperated. To provide the proper privacy and authentication, the CDMA mobile communication network needs some cryptosystem for providing security services such as user authentication, transmission confidentiality, and key distribution. Privacy and authentication in the CDMA mobile communication networks are generally linked together because the derivation of a session key for an encryption algorithm is often an integral part of the authentication process. The subsequent use of this session key achieves the encryption of user traffic. The access control and derivation of a session key are a single activity called authentication and key agreement.[1], [2], [3]

The CDMA mobile communication network has been developed the security model that are based upon the secret key method like the Interim Standard IS-95 of the Telecommunication Industries Association (TIA) for United States Digital Cellular. This model provides a means for user authentication and subsequent protection of user traffic. However, this model has no assumptions about the security of the intermediate, fixed networks. To avoiding these drawbacks, we propose the secure and minimal protocol for authenticated key distribution. In this protocol, we consider the following design criteria : no shared security information, user identity confidentiality, and minimal protocol overhead. First, the secret sensitive information such as the session key must not be propagated from the home area to a visiting area or between visiting areas. Second, to keep both the movement and the current whereabouts of mobile user's secret, all user identification information must be protected from disclosure. Third, the number of messages exchanged between the home network and the visited network for the purpose of authentication must be kept minimal.

This paper is organized as follows. In section II, we review the privacy and authentication needs in the CDMA mobile communication network. In section III, we review the existing approaches in the CDMA mobile communication network. In section IV, we propose the authenticated key distribution protocol for the CDMA mobile communication network and evaluate this protocol.

II. Privacy and Authentication Needs

Because the media in mobile communications is shared, privacy and authentication are lost unless some method is established to regain it. Cryptography provides the means to regain control over privacy and authentication.[2]

Today many people think that the CDMA modulation schemes are too difficult to decode, and thus are inherently secure. We know that what is difficult today is easy tomorrow. To provide privacy and authentication for a cellular phone, some cryptographic system will be necessary. We define requirements that a cryptographic system used for the CDMA mobile communication network would need to meet. We provide a template for examining cryptographic system to choose between cryptographic alternatives. In this section, we discuss levels of privacy and requirements of privacy.

1. Privacy definitions in mobile communications

When most people think of privacy, they think of either of four levels : none, wireline level, commercial level or military level privacy. We consider four levels of privacy as follows :

A. With no privacy enabled, anyone with a digital scanner could monitor a call. All cellular phones with no privacy would be awarded that their conversation could be monitored.

B. Most people think wireline communications are secure. In case of tapping a wireline, anyone knows that they are not. The types of conversations that would be protected with this level are the routine everyday conversations of most people. These types of communications would be discussion of a personal nature that most people would not want exposed to the general public.

C. The level of commercial security would be useful for conversations where proprietary information is discussed. We need a cryptographic system for maintaining this level, but it is not critical.

D. The military/government level privacy is considered when cryptography is discussed. The requirements for this level would be defined by the appropriate government agencies.

2. Privacy requirements in mobile communications

Users of mobile phones have come to expect some level of privacy in their communications. Although telephone taps are easy to do, they are most times easy to discovery. In mobile communications, we may give up our rights to privacy unless the mobile system design is done in a way to maintain privacy. A user of the CDMA mobile communication network needs privacy in the following areas :

A. During call setup, the cellular phone will communicate to the network information, such as calling number, called number, and type of services requested. All this information must be sent in a secure way.

B. All voice communications must be encrypted so that they are not capable of being intercepted by some listening on the air interface.

C. All user signal communications must be encoded so that they are not capable of being intercepted by someone monitoring on the air interface.

D. When cellular phones communicate with the land network, the communication must be encrypted so that the location of phones is not disclosed.

III. Existing Approaches in the CDMA mobile communication network

In this section, we briefly review how current CMS reconciles the terminal mobility with authentication.

1. Privacy and Authentication

For the access control and the protection of user information sent via the air interface, the CDMA cellular network considers the privacy and authentication process. We link together the authentication and privacy because the derivation of a session key for an encryption algorithm is often an integrated part of the authentication process. An integration of the derivation of a session key and the authentication is called by the authentication and key agreement.[3] In the CMS, the authentication mechanism uses shared secret key (SSD).

2. Shares Secret Data (SSD) System

In the shared secret key system used for the CDMA cellular network, a secret number, the A-key, is stored in the network and in the mobile station. The A-key is a 64-bit number assigned by the service provider to the user upon initialization of service. The user enters the A-key into the mobile station via the key pad. Upon provisioning a mobile station with a new A-key, the mobile station performs a registration attempt to establish the shared secret data (SSD). The A-key is not used directly for the authentication process. The SSD is derived from the A-key to authenticate the user in both "home" and "visited" networks. The SSD is a 128-bit pattern stored in the mobile station and in the network. It is partitioned into 64-bits SSD__A and SSD__B. The visitor location register (VLR) of the visited network obtains a copy of the SSD computed by the authentication center (AC) of the home network via intersystem communications. Security is maintained by all signaling communications between mobile station and the network via a challenge-response protocol. The challenge is global for all mobile stations within the same area.

Global challenge procedure

Fig. 1 shows the global challenge procedure, in which mobile stations' registrations, originations, or page responses proceed as follows :

- The base station periodically sends a random number, RAND, on the control channel. RAND is changed frequently.
- When the mobile station is registering, placing a call, or responding to a paging, it executes the CAVE algorithm and computes AUTHR, the response to the challenge. It then sends RAND, AUTHR, call history count (COUNT), and other data to the network as components of a service request.

- As the network, the value of AUTHR is computed internally and compared with the value of AUTHR received from the mobile station. If the comparison by the network is successful, call processing continues. If the comparison fails, the network may optionally not process the service request.

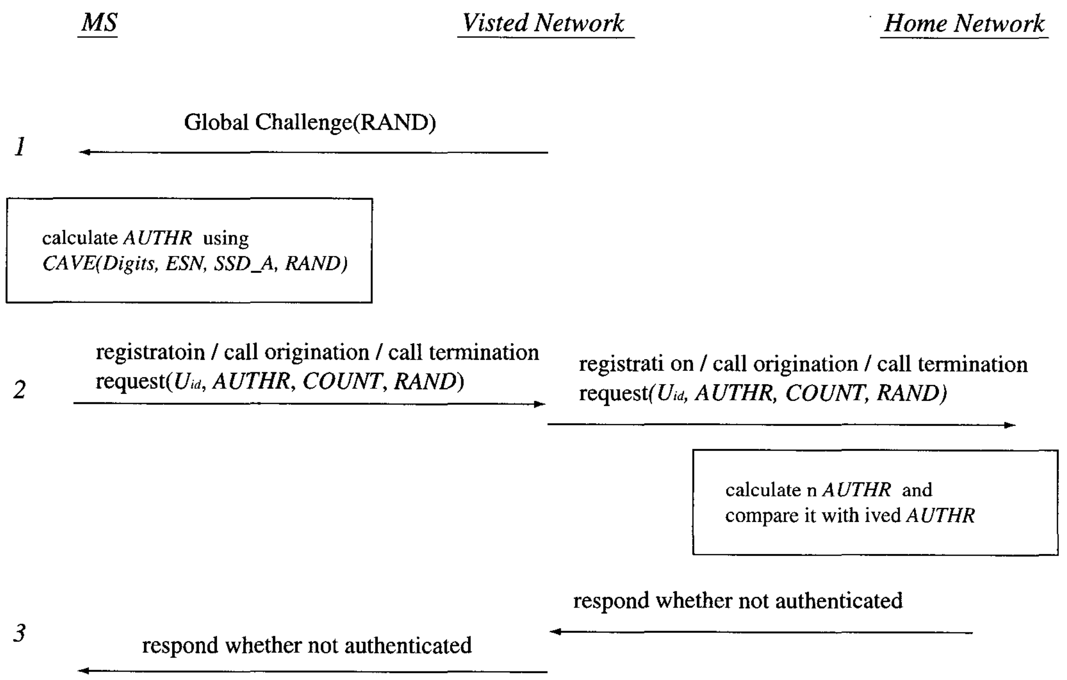

MS
Visted Network
Home Network
1
Global Challenge(RAND)
calculate AUTHR using
CAVE(Digits, ESN, SSD_A, RAND)
2
registratoin / call origination / call termination
request(U_id, AUTHR, COUNT, RAND)
registrati on / call origination / call termination
request(U_id, AUTHR, COUNT, RAND)
calculate n AUTHR and
compare it with ived AUTHR
3
respond whether not authenticated
respond whether not authenticated

Fig. 1. Global challenge procedure

Unique challenge procedure

Fig. 2 shows the unique challenge procedure. The unique challenge procedure is initiated by the home or visited network and can be performed on any signaling channel.

- At the network, a 24-bit random number RANDU is generated and sent to the mobile station via the unique challenge message. The CAVE process is initialized and executed to produce AUTHU. At the mobile station, the received RANDU and its internally stored values for remaining AUTHU is then sent to the network via a unique challenge confirm message.
- Upon receipt of the unique challenge confirm message from the mobile station, the network compares the received value of AUTHU to that generated and stored internally. If comparison fails, the network may deny further access attempts by the mobile station.

Evaluation of this approach

This protocol has the following advantages:

- for authentication between mobile terminals and visited network, the use of home

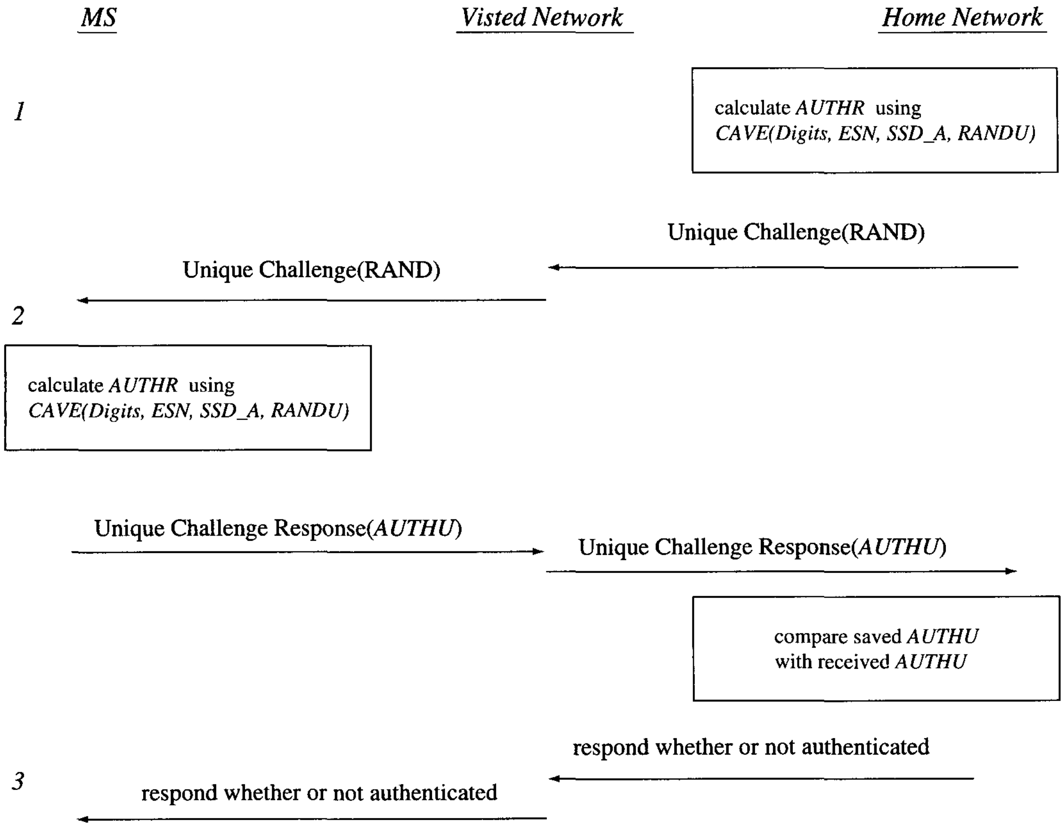

MS
Visted Network
Home Network
1
calculate AUTHR using CAVE(Digits, ESN, SSD_A, RANDU)
Unique Challenge(RAND)
Unique Challenge(RAND)
2
calculate AUTHR using CAVE(Digits, ESN, SSD_A, RANDU)
Unique Challenge Response(AUTHU)
Unique Challenge Response(AUTHU)
compare saved AUTHU with received AUTHU
respond whether or not authenticated
3
respond whether or not authenticated

Fig. 2. Unique challenge procedure

network specific algorithms may be possible ;

- can be easily adapted to calculate session keys ;
- relatively use simple and fast algorithms ;
- small amount of data required for authentication.

However, this protocol has the following disadvantages :

- secured databases have to be available in the network ;
- the network operator and the mobile terminal share a temporal key for authentication and privacy, and must use a standardized authentication algorithm ;
- it may be difficult to adapt the authentication mechanisms or between arbitrary entities, must distribute the shared secret keys.

IV. Minimal Authenticated Key Distribution Protocol

The authentication and key agreement technique in the CDMA mobile communication networks take into account some usability concern in order to minimize the burden on the user and provide a transparent user interface. However, it has no assumptions about the security of the intermediate and fixed networks. In this section, we design an authenticated key distribution protocol (AKDP) on top of three-party authentication and key distribution protocols.[4]

We assume the followings about a AKDP for privacy and authentication of mobile terminals in the CDMA mobile communication network. First, we assume that mobile terminals are authenticated with a traditional server-based authentication mechanism. Second, these are registered with authentication servers in home network. Third, we characterize the mobile environments as the speed at which mobile users move across visiting areas in the network.

1. Design criteria

In order to avoid the drawbacks of existing approach in the CDMA mobile communication network, the protocol must consider the following design criteria.

- Do not share secret information. The mobile system should not propagate secret information from home network to visited network.
- Keep user's identity secure. It is often desirable to keep both the movements and the current whereabouts of mobile user's secret. Thus, user's identification information must be protected from disclosure.
- Keep protocol's overhead minimal. It should keep minimal the message exchanged between the home network and the visited network.

2. Authenticated key distribution protocol

The protocol, which enables a user presently located in a visited network to request the transfer of location-dependent authentication information from the authentication center (AC) of his home network to its peer such as visitor location register (VLR) in the visited network. In this protocol, we define the used notation as follows :

- U_{id}, $\overline{U}_{id}$ - identification of the mobile station or user U in different protocol flows
- AS_h, AS_V - authentication server of home network or visited network
- k_A - master key shared between U and AS_h.
- k_{ssd} - location-dependent session key to be shared by the AS_V and the U.
- k_{net} - long-term key shared by the AS_V and the AS_h and installed out-of-band.
- R_u, R_v, R_h - random number issued by U, AS_V or AS_h
- $AUTHR_u$, $AUTHR_v$, $AUTHR_h$ - authentication result issued by U, AS_V or AS_h, and computed using CAVE that is a strong one-way hashing function such as MD5.

Fig. 3 shows the base protocol for authenticated key distribution. We describe thedetails of the protocol as follows.

1) The mobile station or user U begins by generating a random number R_u and computes $k_{ssd} = SSDGEN(R_u, U_{id}, k_A)$where SSDGEN is a one-way hashing function. Next, it computes AUTHR and sends it

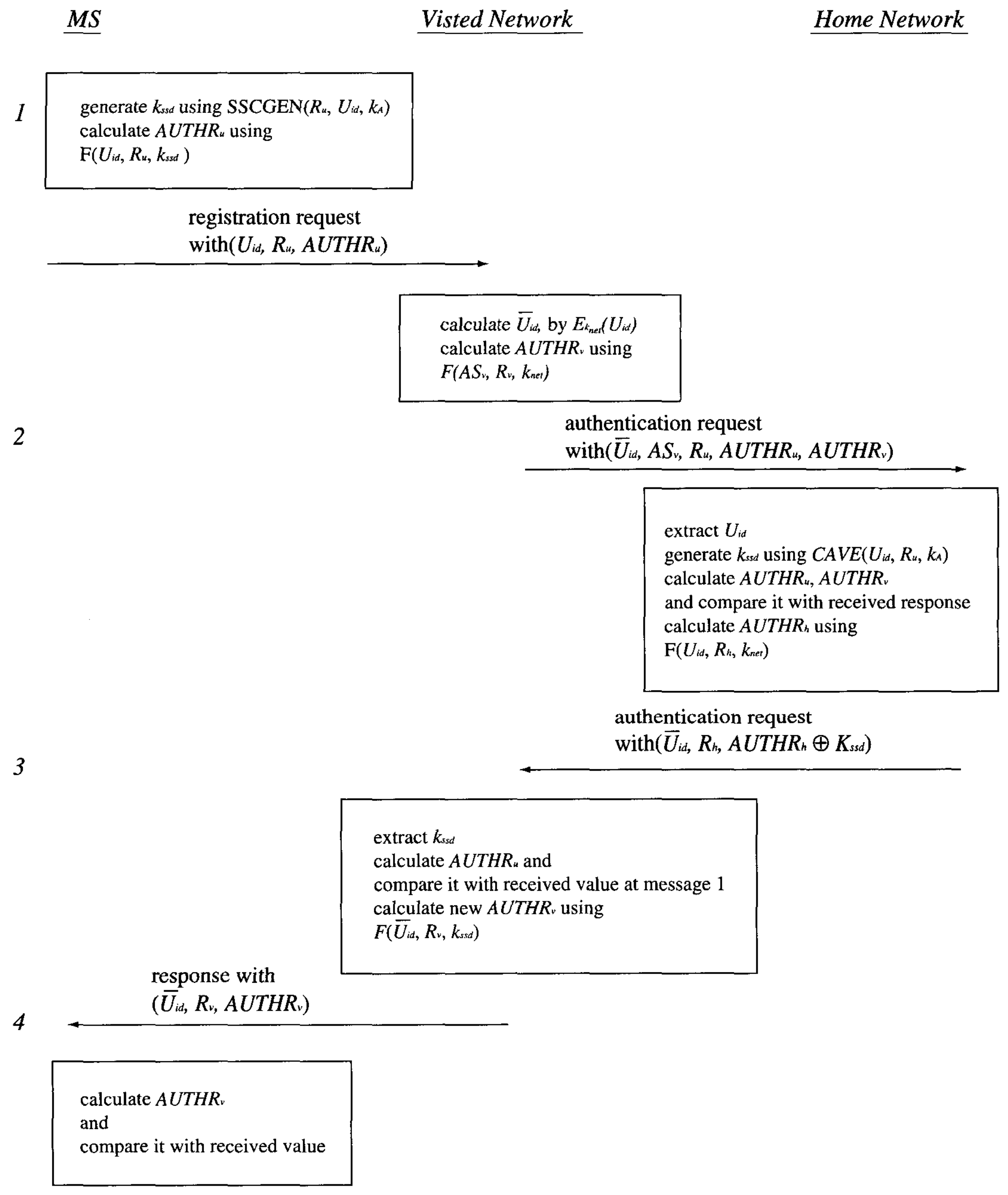

MS
Visted Network
Home Network
1
generate k_{ssd} using SSCGEN(R_u, U_{id}, k_A)
calculate $AUTHR_u$ using
F(U_{id}, R_u, k_{ssd})
registration request
with(U_{id}, R_u, $AUTHR_u$)
calculate $\overline{U}_{id}$, by $E_{k_{net}}(U_{id})$
calculate $AUTHR_v$ using
$F(AS_v, R_v, k_{net})$
2
authentication request
with($\overline{U}_{id}$, AS_v, R_u, $AUTHR_u$, $AUTHR_v$)
extract U_{id}
generate k_{ssd} using $CAVE$(U_{id}, R_u, k_A)
calculate $AUTHR_u$, $AUTHR_v$
and compare it with received response
calculate $AUTHR_h$ using
F(U_{id}, R_h, k_{net})
authentication request
with($\overline{U}_{id}$, R_h, $AUTHR_h \oplus K_{ssd}$)
3
extract k_{ssd}
calculate $AUTHR_u$ and
compare it with received value at message 1
calculate new $AUTHR_v$ using
$F(\overline{U}_{id}, R_v, k_{ssd})$
response with
($\overline{U}_{id}$, R_v, $AUTHR_v$)
4
calculate $AUTHR_v$
and
compare it with received value

Fig. 3. Authenticated Key Distributed Protocol

the local AS_V.

2) Upon receipt of the initial message, recognizes that the U is a roaming one, and that it have no means of authenticating this U. AS_V request a authentication of the user from its home network. The request also authenticates

AS_V to AS_h and U to AS_h. For the confidentiality of user identity, we modify U_{id} as $\overline{U}_{id} = E_{k_{net}}(U_{id})$.

Next, it generates R_V and computes the $AUTHR_V$ and sends it the AS_h.

3) When AS_h receives the message in flow 2, it proceeds as follows :

- Extracts the U_{id}.
- Calculate K_{ssd} using U_{id}, R_u and K_u.
- Calculate $AUTHR_V$ and $AUTHR_u$ compares these to the corresponding message in flow2.
- Generates R_h and computes $AUTHR_h$.
- Computes the key token as $AUTHR_h \oplus K_{ssd}$ and sends it to AS_V.

4) Upon receiving the message in flow 3, AS_V does the following :

- Calculate $AUTHR_h$ and extracts the session key, K_{ssd}.
- Calculate $AUTHR_u$ and compares it to the corresponding message received in flow 1 from U. This comparison checks the integrity of key, K_{ssd}.

5) For subsequent network access in the visited network, the mobile station or user can be authenticated via protocol flow 1 using K_{ssd} and $\overline{U}_{id}$.

3. Protocol evaluation

We evaluate the proposed protocol along the lines of the previously stated design criteria.

Do not share secret information.

The proposed protocol maintains the user's secret information such as K_A by allowing a visited network to obtain a temporary key for a visiting user. The key is valid only within this network it was issued for. Thus, the secret information is not propagated from the home network to the visited network.

Keep user's identity secure.

Until now we have tampered with the issue of protecting the user's identity. This issue is very important but can not be discussed thoroughly in this paper given that our main concern is with the authentication of mobile terminals. However, it is worth noting that many variables influence the way of protecting the user's identity.

Our discussion so far applies only to the first time a user roams in a visiting area. Moreover, it applies only to the flow 1 of the authentication protocol where U_{id} field denotes the user's identity. In the subsequent protocol flow, the obvious solution is to use the same U_{id} construction as in flow 1. However, since AS_v and AS_h are assumed to share a strong secret key, k_{ssd}, the protection of the U_{id} field can be strengthened further. (This is completely independent of the way U_{id} is computed in Flow 1.) One possibility is to set by $\overline{U}_{id} = E_{k_{net}}(U_{id})$ where $\overline{U}_{id}$ denotes the user identification field in flows 2 and 3.

Once AS_v authenticates the user (and AS_h) in flow 3 and establishes a temporary record in its VLR, it can also assign a temporary identity to the user. This is different from the traveling alias referred to before. A temporary identity is issued by the local AS_v based on its own policy. It serves to identify a particular visit of a given user in a visiting area and remains valid as long as the user's entry in the VLR does not expire.

Keep protocol's overhead minimal.

Given the initial requirement that the home network be contacted to affirm the mobile terminal's birthplace(and solvency), it is impossible to design a protocol with less than two flows traversing inter-network boundaries, i.e., $AS_v \rightarrow AS_h$ and $AS_v \leftarrow AS_h$. In addition, at least one flow is necessary for the user to make initial contact with the local AS. This makes a minimum flows which is the number of flows in our protocol.

A closely-related issue is the size of each protocol flow. Of particular interest are the sizes of flows 2 and 3 since both cross domain boundaries and potentially traverse significant distances.

V. Conclusion

To provide the proper privacy and authentication, the mobile system needs some

cryptosystem for providing security services such as user authentication, transmission confidentiality, and key distribution. Privacy and authentication in the mobile system are generally linked together because the derivation of a session key for an encryption algorithm is often an integral part of the authentication process. The existing mobile system has been developed the security model that are based upon the secret key method. This model provides a means for user authentication and subsequent protection of user traffic. However, this model has no security for the intermediate, fixed networks. To avoiding these drawbacks, we propose the secure and minimal protocol for authenticated key distribution. This protocol protects to propagate the secret information from the home network to the visited network. This protocol allows a transparent terminal interface either to the visited network or to the home network. This protocol protects the user identity from disclosure. This protocol used the timestamp based authentication keeps minimal the message exchanged between the home network and visited network.

References

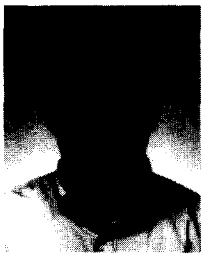
[1] Victor K. Li, and Xiaoxin Qiu, "Personal Communication System (PCS)," Proceeding of the IEEE, vol. 83, no. 9, September 1995, pp 1210~1243.

[2] Joseph E. Wilkes, "Privacy and Authentication Needs of PCS," IEEE Personal Communications, August 1995, pp 11~15.

[3] Dan Brown, "Techniques for Privacy and Authentication in Personal Communication System," IEEE Personal Communications, August 1995, pp 6~10.

[4] Refik Molva, Didier Samfat, and Gne Tsudik, "Authentication of Mobile Users," IEEE Network Magazine, April 1994, pp 26~36.

□ 著者紹介



전 학 성

중앙대학교 공과대학 전기전자계산학과(공학사)
중앙대학원 전자계산학과(이학석사)
정보처리 계산조직응용 기술사
현재 한국전자통신연구원 이동통신연구단 책임연구원
현재 아주대학교 컴퓨터 공학과 박사과정

※ 관심분야 : 이동통신 보안, 이동 컴퓨팅 보안, CORBA 기반 지능망, JAVA

김 동 규

서울대학교 공과대학 졸업(학사)
서울대학교 자연과학대학원 졸업(석사)
미국 Kanasas 주립대 대학원 졸업(Ph.D. 전산학 박사, 정보통신 전공)
미국 Kanasas 주립대 전산학과 교수
1979. 3 ~ 현재 아주대학교 컴퓨팅공학과 교수
저서 : 데이타 통신시스템, 희중당, 1986년
저서 : 컴퓨터 통신 네트워크, 상조사, 1988년
한국통신학회 상임이사, 한국통신정보보호학회 부회장

※ 주관심 분야 : 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링,
정보통신 Security, 분산처리 시스템