An Authentication Technique Based on Distributed Security Management for the Global Mobility Network

Shigefusa Suzuki, *Member, IEEE*, and Kazuhiko Nakada

***Abstract*— This paper proposes an authentication technique for use in the global mobility network (GLOMONET), which provides a personal communication user with global roaming service. This technique is based on new distributed security management, where authentication management in roaming-service provision is conducted only by the roamed network (the visited network). The original security manager (OSM) administrates the original authentication key (OAK) acquired when a user makes contracts with the home network, while the temporary security manager (TSM) is generated for a roamer in the visited network in order to provide roaming services. The TSM generates and administrates the temporary authentication key (TAK) for a roamer, which key is confidential to the OSM, releases the TAK administration when a roamer moves to other networks, and then disappears. The proposed authentication technique consists of two phases. In the roaming-service-setup phase, triggered by the user's location registration request, authentication control to set up the roaming-service environment is negotiated by the TSM in the visited network, the OSM, and the roamer. In the roaming-service-provision phase, triggered by the user's service request, authentication control to provide the roaming service is negotiated (using the TAK acquired by the roamer in the first phase) only by the visited network and the roamer. This authentication control using the TAK provides a unified authentication procedure with a single logic to both subscribers and roamers. In addition, the security management of the whole GLOMONET is reinforced and the security responsibility is made clear by allocating the subscriber's/roamer's security administration to only the TSM.**

***Index Terms*—Authentication, mobilty, roaming.**

I. Introduction

THE demand for personal communication systems, including cellular phones [1]–[3] and CAS (cordless access services) [4]–[7], has recently been growing rapidly, not only in Japan, but also throughout the world. To support global mobility, roaming service must be provided both in the home network (contracted network) and in the roamed network (visited network).

Mobility is a function that enables a user ("user" here is a general term for a human being, an IC card, a terminal, and so on) to move inside and around networks, and the network providing this function is called the mobility network. The mobility network includes the GSM [1], USDC [2], and PDC [3] systems, and the GSM system is used in more than 70 countries around the world and helps to promote globalization. While the existing mobility network expands, the network architecture technology for the personal communication systems capable of users' global mobility is also advancing dramatically. The UPT (universal personal telecommunication) [8] and the FPLMTS (future public land mobile telecommunication systems) [9], [10], based on IN (intelligent network) technology, are being studied energetically in order to provide personal communication service flexibly and effectively. This paper calls the mobility network capable of global mobility based on the IN the global mobility network (GLOMONET).

The global mobility in the GLOMONET will expand the possibility of a malicious attacker fraudulently gaining access to a user's personal assets. Security management techniques capable of strong authentication and the responsibility management among plural networks must therefore be established without losing its global user mobility capability.

At the moment, the secret key cryptosystems implemented in digital cellular systems, such as GSM and IS-41 [11], and the public key cryptosystems are being studied for UPT and FPLMTS in ITU-T and ITU-R. Since the public key cryptosystems are strong in the security aspect but are inferior to the secret key cryptosystems with respect to processing time, this paper focuses on the secret key cryptosystems.

Existing digital cellular systems adopt the VLR (visitor location register) [3] network architecture. When the roaming service in these systems is set up, the authentication data travel among the home network, the visited network, and the user's terminal, whereas once the roaming service is provided, the authentication data travel only between the visited network and the user's terminal. It is important to consider the secure system architecture or the secure procedure suitable for this kind of environment.

In the GSM [12] authentication technique, the user authentication key is concealed from the visited network by sending only several RAND (challenge)/SRES (response) pairs to the visited network. Since several RAND/SRES pairs are transmitted, the number of network signals increases, and additional pairs need to be supplied when the pairs are short. This authentication technique, therefore, is suitable to the environment where the users do not move around the networks so frequently and stay in the home network for long periods.

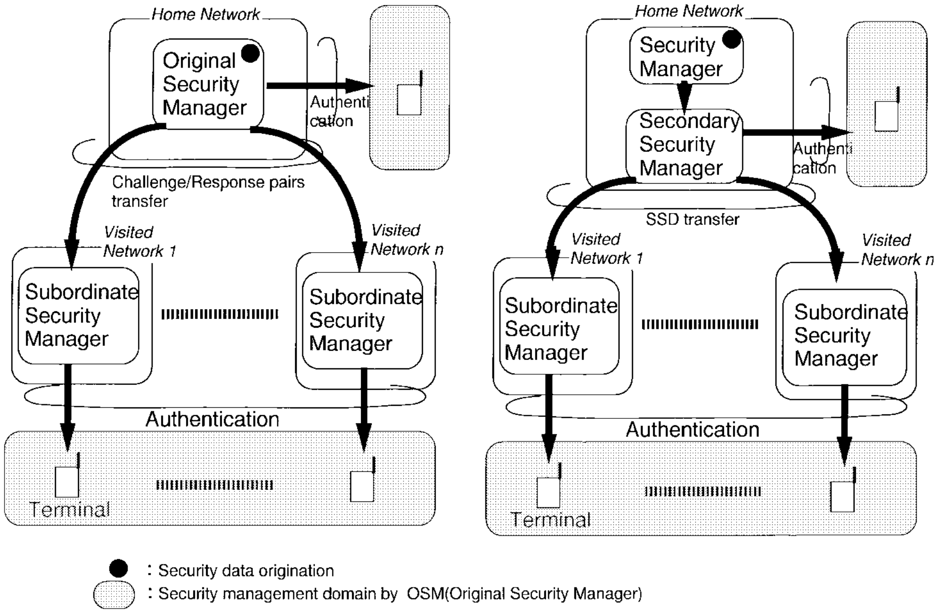
In the IS-41 authentication technique [11], the original authentication key is concealed from the visited network by

Manuscript received September 30, 1996; revised April 25, 1997.

The authors are with the NTT Network Service Systems Laboratories, 9-11, Midori-Cho 3-Chome Masashino-shi, Tokyo, 180 Japan (e-mail: suzuki.shigefusa@nslab.ntt.co.jp)

Publisher Item Identifier S 0733-8716(97)06083-6.

0733–8716/97$10.00 © 1997 IEEE


Home Network
Original Security Manager
Authentication
Challenge/Response pairs transfer
Visited Network 1
Visited Network n
Subordinate Security Manager
Subordinate Security Manager
Authentication
Terminal
Home Network
Security Manager
Secondary Security Manager
Authentication
SSD transfer
Visited Network 1
Visited Network n
Subordinate Security Manager
Subordinate Security Manager
Authentication
Terminal
● : Security data origination
: Security management domain by OSM(Original Security Manager)

(a) (b)

Fig. 1. Existing centralized security managment examples. (a) GSM security management concept and (b) IS-41 security management concept.

creating temporary authentication data (SSD: shared secret data) for user authentication. Since the SSD is transmitted to the visited network without being ciphered, it is possible for the SSD to be tapped by an eavesdropper or to be leaked in the home network. To overcome this problem, the synchronized call counter is managed by the user and the network. This call counter is updated and notified to the network call by call, and is used to detect the illegal clone terminal whose counter is not synchronized. From the viewpoint of security administration, however, it is desirable to prevent the authentication key from being leaked at most first, and then consider the security against clone terminals which have obtained the leaked key.

In addition, in the GSM or IS-41 authentication technique, because the authentication key or data are generated in the home network and are used in the visited network without being modified, the security responsibility allocation between the visited network and the home network is unclear when the illegal event is discovered in the visited network. Therefore, even when the security administration in the visited network is inappropriate, it is probable that the home network takes all of the responsibilities for security because it is the home network that determines whether or not to provide a service to a roamer without knowing the service providing conditions in the visited network.

This paper clarifies the security network architecture in the roaming environment and the requirements for security threats to each functional element. To satisfy these requirements in the GLOMONET, we propose an authentication management architecture based on distributed security management and a concrete authentication technique (procedure and algorithm). We also show a protocol example using Intelligent Network Application Protocol (INAP) [13], [14] based on our security technique.

In this paper, Section II clarifies the security network architecture in the roaming environment and the requirements for security threats to each functional element. To satisfy these requirements in the GLOMONET, we propose an authentication management architecture based on distributed security management in Section III. Within a frame of this architecture, we propose a concrete authentication procedure in Section IV. We also show a protocol example using the INAP [13], [14] based on our security technique in Section V.

II. Security Requirements

A. Security Network Functional Model and Threats

To study security in roaming-service provision, it is required to extract the network functional entity and establish a network functional model to clarify security functional allocation [15], [16].

Our security network functional model consists of a user, a terminal, a visited network, a visited network operator, a home network, and a home network operator based on the VLR architecture. Fig. 1 shows our security network functional model based on the VLR architecture.

The threats in each functional entity to be studied are as follows.

1) Threats on interworking between user and terminal:
   - service availability by an illegal user;
   - user data modification by an illegal user.
2) Threats on interworking between terminal and visited network:
   - service availability by a clone terminal;
   - user data modification by a clone terminal;
   - signal eavesdropping between a terminal and a network;
   - signal modification between a terminal and a network.

Consideration of the threats mentioned above is especially needed when a terminal interworks with a visited network on wireless interface.

3) Threats on interworking within a network:
- signal modification within a network;
- signal eavesdropping within a network.

Security within a visited network or a home network is dependent on the network operator's security administration policy.

4) Threats on interworking between networks:
- service availability by a fraudulent network;
- user data modification by a fraudulent network;
- signal modification between networks;
- signal eavesdropping between networks.

These threats increase as the number of roaming networks increases.

5) Threats on interworking between operator and database:
- illegal user data modification by a fraudulent operator;
- disclosure of user data to a fraudulent operator.

We do not discuss 1) in this paper since it is not a network subject, and it requires that local security measures between a user and a terminal be taken. Points 3) and 5) should be considered in relation to the network functional allocation and security administration rather than in relation to authentication procedures. This is discussed in Section III-A. Points 2) and 4) should be considered in relation to authentication procedures, and are discussed in Section IV.

B. Security Requirements for Threats

From the point of authentication key management in roaming-service provision, security threats can be categorized as follows:

- illegal access by a fraudulent functional entity;
- eavesdropping on the signals between entities; and
- leak of an authentication key shared by functional entities.

Anonymous interference with the signals (such as jamming) is difficult to prevent by authentication procedures, and is therefore outside the scope of this paper. Requirements for each threat are studied below.

1) Illegal Access by a Fraudulent Entity: Illegal access by a fraudulent entity can be prevented by authentication. Authentication measures can be classified as follows.

a) Challenge/response interactive authentication using secret key cryptosystems [15]: In this measure, an authenticating entity authenticates an authenticated entity by sending a random number (challenge) to the authenticated entity and receiving a response. The authenticating entity compares the response with the calculated result using the secret key shared between the authenticating entity and the authenticated entity.

This measure requires an appropriate algorithm for strong confidentiality to be chosen, because the authentication key may be disclosed by a chosen plaintext attached to the authenticated entity.

b) One-way authentication using a password [15]: In this measure, an authenticating entity authenticates an authenticated entity by receiving an ID (identification number) and a password from the authenticated entity and confirming their validity.

This measure requires a random and long password to be chosen because the password may be disclosed by a good guess.

c) One-way authentication using synchronized data such as time stamps or counters [15]: In this measure, an authenticating entity authenticates an authenticated entity by comparing the synchronized data such as time stamps or counters from the authenticated entity.

In the case of a time stamp for synchronized data, too much time precision makes it difficult to synchronize the timing between the authenticating entity and the authenticated entity, while too little time precision increases the possibility of false authentication and illegal access by an attacker.

In the case of a counter or a sequential number for synchronized data, on resetting, the initial authentication data sent to the authenticating entity are always the same, and the subsequent authentication data are the same as well. This may enable easy illegal access by an attacker who eavesdrops to obtain the authentication data signals after resetting.

To overcome these problems, a method that uses the time as an initial value and uses the previous authentication data stored in the network as synchronized data has been proposed [17].

d) One-way authentication using public key cryptosystems [18]: In this measure, an authenticating entity authenticates an authenticated entity by receiving an ID or a text encrypted by a secret key and retrieving the ID or the text by decrypting the message by using the public key.

A problem with this measure is that the algorithm is complex, and authentication therefore takes a relatively long time [19].

This paper focuses on point a) (challenge/response interactive authentication) which is secure and efficient. The requirements to be considered are as follows:

r1) user authentication by the visited network;
r2) visited network authentication by the user;
r3) home network authentication by the visited network;
r4) visited network authentication by the home network.

2) Eavesdropping of the Signals Between Entities: Eavesdropping of the signals between entities can be protected by ciphering the signals.

The objects to be ciphered are as follows:

- the original authentication key Kh shared between the user and the home network;
- the authentication key Kn used for mutual authentication of the network entities;
- the authentication key Kv used for user authentication by the visited network.

In the case of challenge/response interactive authentication, consideration is required not just for passive eavesdropping, but also for active eavesdropping such as a chosen plaintext attack in order to keep confidentiality. This kind of eavesdropping can be prevented by selecting an appropriately secure algorithm such as FEAL [20], [21].

The requirements to be considered to prevent eavesdropping of the signals are as follows:

r5) confidentiality of the signals between the visited network and the terminal;
r6) confidentiality of the signals between the visited network and the home network.

3) Leak of an Authentication Key Shared by Entities: Although we have discussed the threats of eavesdropping by a stranger, it is possible that the entities concerned take illegal action in roaming-service provision. Therefore, it is desirable not to leak the authentication keys needed for their authentication to the other networks. From the viewpoint of authentication key administration, the requirements to be considered for the threats of leak to the other networks concerned are as follows:

r7) confidentiality of the original authentication key shared by the user and the home network to the visited network;
r8) confidentiality of the user authentication key in the key generating network to the other networks.

III. Security Network Functional Architecture

A. Concept

1) Distributed Security Management: In the GSM or IS-41 system, the authentication data generated by the home network security manager are transparently transferred to the visited network security manager, and the visited network authenticates a roamer on the basis of that information. Thus, the visited network security manager is subordinate to the home network security manager. That is, these systems can be considered as centralized security management systems, where the home network security manager administrates the whole global network security in a concentrated way.

In the GSM system, for example, the home network security manager manages the user authentication key, and the challenge/response pairs generated by the home network security manager are transferred to the subordinate security manager in the visited network in order to authenticate the roamer [Fig. 1(a)]. In the IS-41 system, on the other hand, the home network security manager generates the secondary authentication key (SSD), and sends it to the subordinate security manager in the visited network to authenticate a roamer [Fig. 1(b)].

The main reasons that the centralized security management by the home network is chosen are as follows.

- Because most users lead their lives almost only in the home network and the roaming frequency is relatively low, the home network centralized system will probably cause no serious problems with signaling traffic and administration.
- Because the service provision in the home network is essential and the roaming service can be considered as a limited supplementary service, the security should be controlled in a concentrated way by the home network.
- It is technically difficult to implement different authentication data or procedures for each network in the terminal. If the security is not managed in a concentrated way, the software change in the terminal may be needed whenever a terminal makes a contract with a new roamed network.

But since the user acts globally, the concept mentioned above should be reconsidered. That is, as a user roams around the world more and more and stays for longer and longer periods, the possibility that a roamer will suffer damage in the visited network will become higher. Therefore, If the centralized security management concept is applied, the home network may have to take all of the responsibility for the damage which may be ascribed to the deficient security of the visited network. And it seems almost impossible for the home network to administrate the security of all of the visited networks in the world. This means that in the GLOMONET environment, the centralized security management concept has its limitations, and it suggests that the connection between the home network security manager and the visited network security manager should be as loose as possible.

The home network and the visited network should therefore independently own each security manager and independently administrate the security of a subscriber/roamer, as is shown in Fig. 2.

However, since it is ineffective to permanently place different security managers for each respective network, we introduce the concept of a temporary security manager (TSM), which temporarily administrates security while a roamer stays in the network as in the VLR concept. Each TSM controls the authentication of a subscriber/roamer by the security information administrated only by itself.

Introduction of this concept unifies the security control in the home network and in the visited network. The proposed concept is a distributed security management such that each TSM controls the authentication of the subscriber/roamer based on the security information generated and administrated only by itself.

2) Security Manager's Function in Each Call-Control Phase: In order to provide roaming service, the following two call-control phases are generally required.

Phase 1—Service Setup Phase: In this phase, initiated by a user's roaming to another network, the procedure to allow a roaming-service request by a roamer, and the procedure to set up a roaming-service environment in the visited network and in the terminal take place. This phase is closely related to the subscriber profile transfer from the home network to the visited network which is needed in the VLR architecture.

Phase 2—Service-Provision Phase: In this phase, after Phase 1 is completed, roaming service is provided in the visited network.

In Phase 1, when a user roams to the visited network for the first time, the subscriber data of a roamer generally exist only in the home network. Therefore, the final responsible security manager to allow the roaming-service request by a roamer

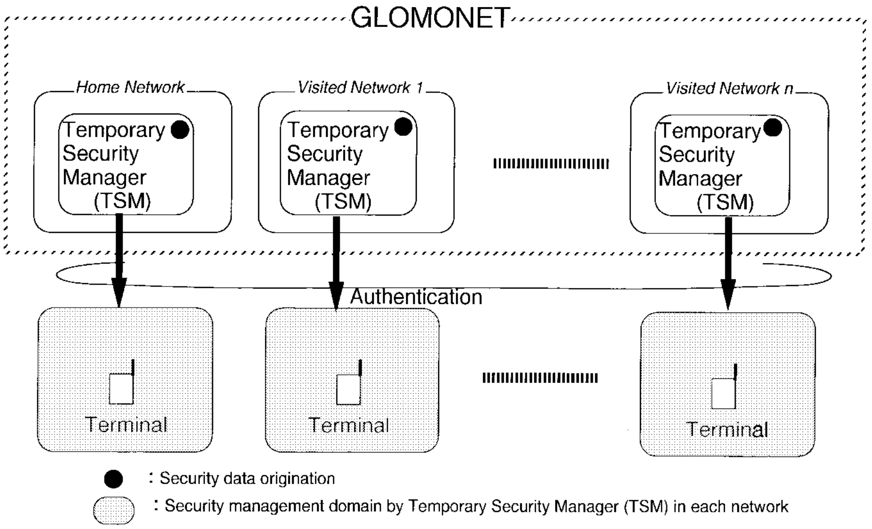

GLOMONET
Home Network
Visited Network 1
Visited Network n
Temporary ● Security Manager (TSM)
Temporary ● Security Manager (TSM)
Temporary ● Security Manager (TSM)
Authentication
Terminal
Terminal
Terminal
● : Security data origination
: Security management domain by Temporary Security Manager (TSM) in each network

Fig. 2. Proposed distributed security management concept.

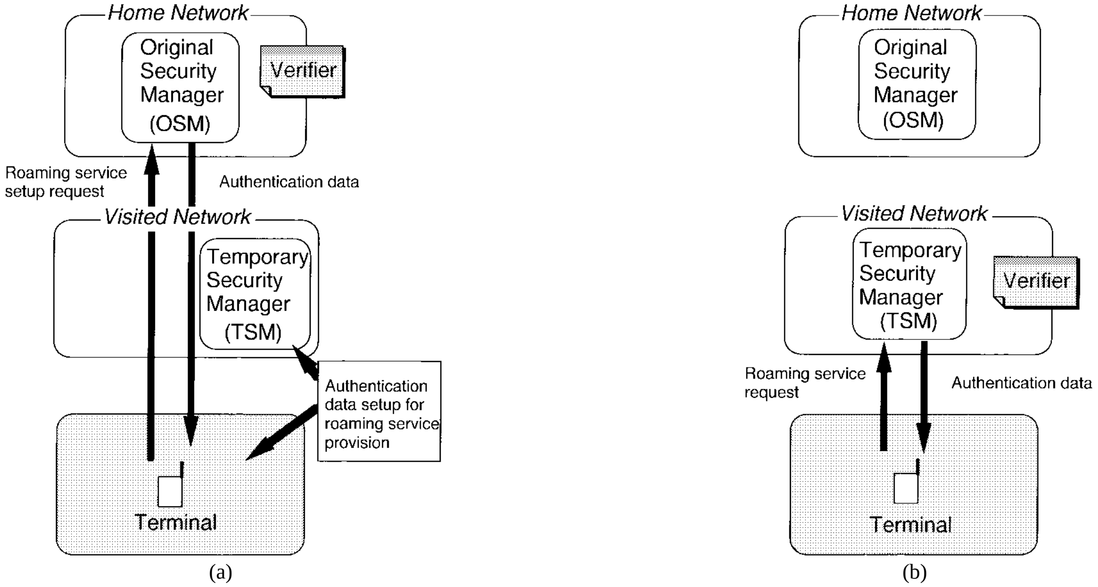

Home Network
Original Security Manager (OSM)
Verifier
Roaming service setup request
Authentication data
Visited Network
Temporary Security Manager (TSM)
Authentication data setup for roaming service provision
Terminal
(a)
Home Network
Original Security Manager (OSM)
Visited Network
Temporary Security Manager (TSM)
Verifier
Roaming service request
Authentication data
Terminal
(b)

Fig. 3. Verifier in roaming call processing. (a) Roaming-service-setup-phase and (b) roaming-service-provision phase.

and to assure environment setup is, as in the existing systems, the original security manager (OSM) in the home network. To set up the environment for roaming-service provision, the original authentication key shared between the OSM and the roamer is used. The OSM is independent of the TSM in the home network, and sets up environments for roaming-service provision in cooperation with the TSM in the visited network only during this phase [Fig. 3(a)].

In Phase 2, since the roaming-service-provision environment is prepared beforehand both in the roamer and in the TSM, the TSM is now ready to control authentication in a unified manner on the basis of the security information administrated by the TSM. As we have discussed in the distributed security management concept, it is the TSM in each network that authenticates the user/roamer in each access to the home/visited network after Phase 1 [Fig. 3(b)].

3) Measures to Prevent the Threats Within a Network: In Section II-A, we mentioned that: 3) threats on interworking within a network, and 5) threats on interworking between operator and database should be discussed in relation to the security network functional allocation and the administration policy. These threats are both subjects within a network, and can be reinforced with the points as follows.

- A roamer's authentication information should be generated temporarily in order to prevent illegal action resulting from information leakage.
- The visited network should take all of the responsibility when illegal action was discovered in itself in order to promote incentives to the security management reinforcement in each network.

We therefore introduce a concept in which the visited network generates the authentication key for the roamer [based

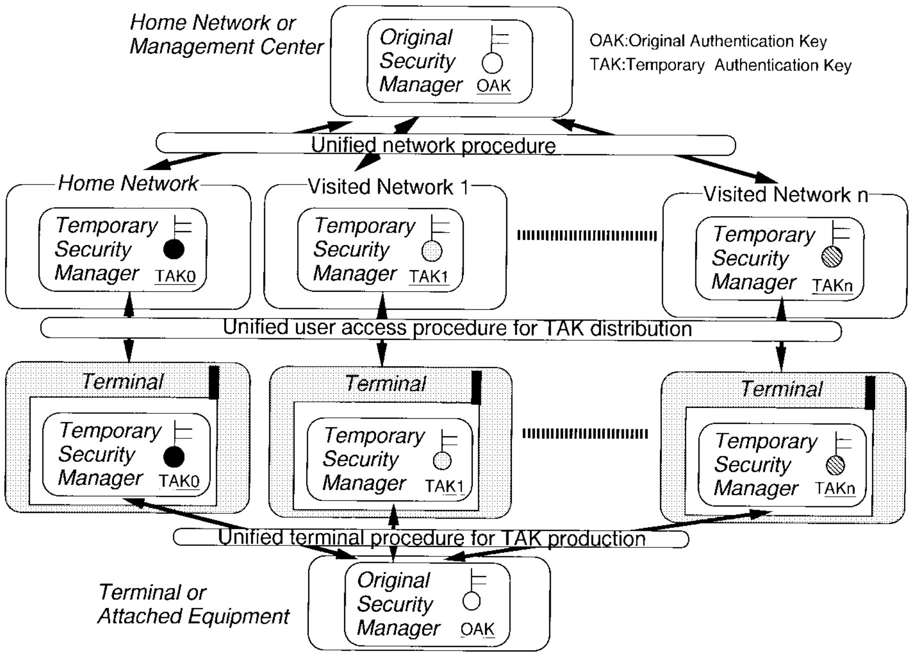

Home Network or
Management Center
Original Security Manager OAK
OAK:Original Authentication Key
TAK:Temporary Authentication Key
Unified network procedure
Home Network
Visited Network 1
Visited Network n
Temporary Security Manager TAK0
Temporary Security Manager TAK1
Temporary Security Manager TAKn
Unified user access procedure for TAK distribution
Terminal
Terminal
Terminal
Temporary Security Manager TAK0
Temporary Security Manager TAK1
Temporary Security Manager TAKn
Unified terminal procedure for TAK production
Terminal or
Attached Equipment
Original Security Manager OAK

Fig. 4. Authentication management functional architecture in the GLOMONET.

on point 1) Distributed security management], and the temporary authentication key (TAK) valid only while the roamer stays in the visited network should be used. This concept is similar to the SSD in IS-41, but is considerably different in the administration aspect in that this proposed concept is based on the distributed security management architecture, the TAK is generated by the visited network, and the TAK is only recognized by the visited network. In addition, the use of a temporary authentication key reinforces the overall GLOMONET security since the roamer's original authentication key (OAK) is not revealed during service provision.

B. Proposed Authentication Management Functional Architecture

Fig. 4 shows the proposed authentication management functional architecture in the GLOMONET.

In this architecture, the OSM in the network manages the OAK, which is only used to assure the TAK to be distributed to the authorized user in the roaming-service-setup phase. The home network and the visited network have the same TSM function to manage the TAK while a user stays in each network. The OSM can unify the procedure with the TSM in the home network and the procedure with the TSM in the visited network. Although the OSM is implemented in the home network in the existing systems, it can be implemented outside the home network using the same procedure. For simplicity, however, we limit our discussion to the case where the OSM exists in the home network.

The TAK distribution from the visited network (including the home network) to the roamer (the subscriber) is also performed in the unified user access procedure, both in the visited network and in the home network.

The security management function in the user's terminal is provided by a single terminal in the GLOMONET. The TSM in the terminal receives the TAK generated in the visited network on each roaming in order to use it in the roaming-service-provision phase. The OAK, on the other hand, is managed in the OSM in the user's terminal, and is only used in the roaming-service-setup phase to acquire the authentication data authorize the TAK which is used in the roaming-service-provision phase.

The OSM implementation in the IC card attached to the terminal is also possible. The OSM does not have to recognize where it is located and apply different algorithms for the visited network and for the home network since the unified procedure is introduced in all networks, both in the home network and in the visited network.

To summarize, distinctive characteristics of the proposed authentication management functional architecture are that the security management allocation and the procedures between the user and the home network are the same as those between the roamer and the visited network, and that the OSM and the TSM are independently realized, and the procedures between them are unified for every TSM so as to reinforce the security of the entire GLOMONET and to enable the various authentication techniques to be extended to different personal communication systems in the future.

IV. Proposed Authentication Technique Procedure

A. Authentication Procedure

Fig. 5(a) shows the proposed authentication procedure in the roaming-setup phase. This procedure assumes that the authentication key Kh is shared between the user and the home network, and that the authentication key Kn is shared between the visited network and the home network by a highly secure procedure such as off-line communication (to share Kh,

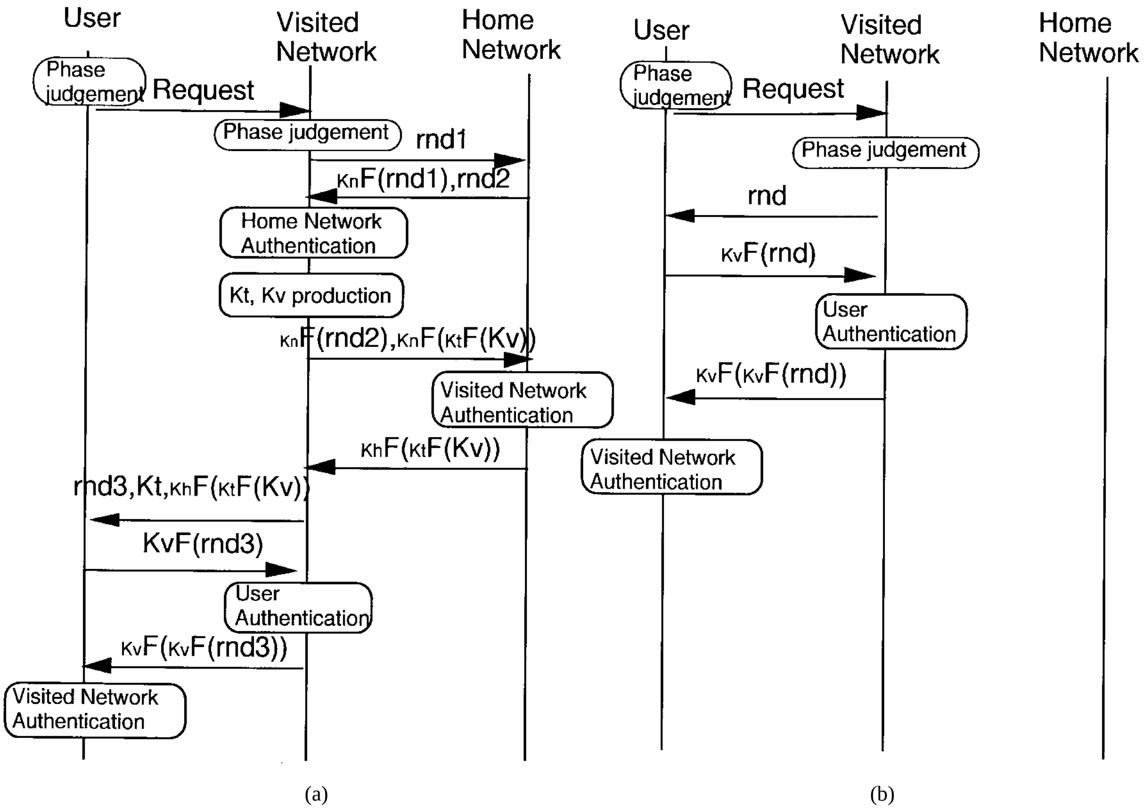


Fig. 5. Proposed authentication protocol. (a) Proposed authentication protocol in roaming-service-setup phase and (b) proposed authentication protocol in roaming-service-provision phase.

for example, a credit-card-like terminal-attached device, such as SIM [1], is transported to the user). The Kn should be provided for each roamed network. To reduce the number of authentication keys required, it may be possible to make the use of the public key cryptosystems.

The proposed authentication procedure is described below, where the notation KeyF(rnd) means the random number rnd encrypted by the authentication key Key.

- The user receives the area identifying information notified from the roamed network, when it moves to a service zone of a roamed network, and judges the roaming-service phase by comparing the information with the memorized information in the terminal
- The visited network receives the service request from the terminal.
- The visited network judges the roaming-service phase by checking the existence of the VLR function triggered by the user's service request.
- The visited network sends the random number rnd1 to authenticate the home network.
- The home network responds with the calculated result KnF(rnd1) and the random number rnd2 to authenticate the visited network.
- The visited network authenticates the home network by KnF(rnd1). This authentication is to satisfy requirement r3) discussed in Section II-B.
- The visited network generates the user authentication key Kv and the temporary cipher key Kt to cipher the Kv. The user authentication key Kv is ciphered by the Kt to satisfy requirement r8) which is not fulfilled in the IS-41 system. Requirement r7) is also met because the original authentication key Kh is not used to authenticate the user.
- The visited network sends the Kv, which is ciphered by the Kt and is further ciphered by the authentication key Kn shared between the visited network and the home network, and it also sends the authentication response KnF(rnd2). KtF(Kv) is ciphered by Kn in order to prevent a fraudulent user without Kn from generating Kv. Requirement r6) (the confidentiality of the signals between the visited network and the home network) is satisfied by ciphering the signals by Kn.
- The home network authenticates the visited network by the signal KnF(rnd2). This authentication satisfies requirement r4).
- The home network deciphers the signal received from the visited network, ciphers it by the Kh, and sends the ciphered signal KhF[KtF(Kv)] to the visited network.

Ciphering by the Kh satisfies requirement r6) (the confidentiality of the signals between the visited network and the home network).

- The visited network sends the Kt and the random number rnd3 to authenticate the user with the signal KhF[KtF(Kv)] received from the home network.

Ciphering by Kh satisfies requirement r5) (the confidentiality of the signals between the user and the visited network).

- The user deciphers the signal by the stored authentication key Kh and the obtained cipher key Kt to acquire the Kv, and returns the rnd3 encrypted by the Kv to the visited network.

- The visited network authenticates the user by KvF(rnd3), regards this signals as the authentication challenge, and returns the response ciphered by Kv to the user. This authentication satisfies requirement r1).
- The user authenticates the visited network by the authentication response signal KvF[KvF(rnd3)] using the Kv acquired from the visited network. This authentication satisfies requirement r2).

In this phase, the mutual authentication of the visited network and the home network should be optional since it depends on the agreements between the network operators. The authentication of the visited network by the user can be also optional according to the visited network's security policy because the security management for a roamer is controlled by the visited network.

Fig. 5(b) shows the proposed authentication procedure in the roaming-service-provision phase. The mutual authentication by the authentication key Kv acquired in the roaming-service-setup phase satisfies requirements r1) and r2). In this phase, too, the user authentication by the visited network can be optional according to the visited network's security policy. The roaming-service phase difference is reflected only in the method of acquiring the TAK. In the roaming-service-provision phase, the TAK which has been managed by the TSM is used, while in the roaming-service-setup phase, the TSM accesses the OSM to make the TAK authorized by the OSM. The authentication procedure from then on is the same, regardless of the phase. It is also possible for the network to use the same procedure as the roaming-service-setup phase, even in the roaming-service-provision phase in order to change the TAK regularly to reinforce security or to change the TAK by sensing the clone terminal.

In this authentication procedure, TAK production also takes place in the home network. The only difference between the case in the home network and that in the visited network is whether the OSM is in the same network or in different networks, and it is possible to produce the TAK with the same authentication control procedure without being aware of whether the TSM is in the visited network or in the home network. To discover an intentional attack and to prevent it from being successful, functions such as monitoring of the successive authentication failure events of the same user, monitoring of the short period access by the same user from a different network, and monitoring of the authentication request from the communicating user which should not require authentication may be needed.

V. Signaling Protocol Example

This section describes an authentication signaling protocol example based on the IN function, which is inevitable for the realization of the GLOMONET.

A. Assumptions

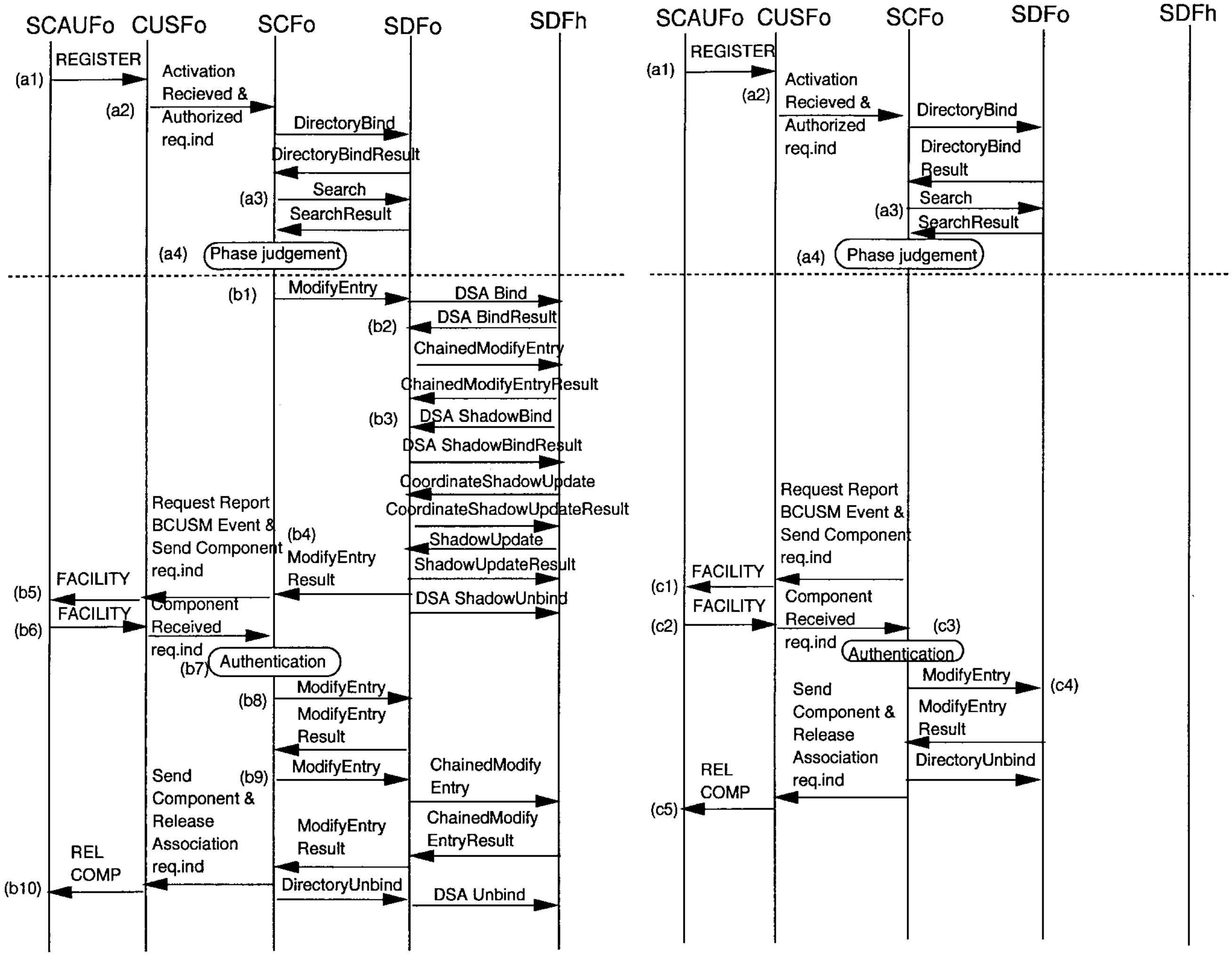
- With IN CS2 [13], [14] capabilities in the networks, the INAP is used as an internetwork signaling protocol.
- The UPT network functional architecture in the ISDN environment based on the VLR system is used [22].
- Location registration signals go through the SCAUF–CUSF interaction, and the REGISTER and RELCOMP messages in the DSS 1 protocol [22] are used.
- The SDF–SDF relationship is used for user profile transfer.

B. Signaling Protocol

Fig. 6 shows a signaling protocol example for location registration based on the proposed authentication protocol. The notations "o," "h," and "p" "o" and "h" for each functional entity in the figure, respectively, mean the originating network (which corresponds to the visited network), and the home network, and the previously visited network.

a) Phase judgment
  a1) The SCUAFo sends a location registration request toward the CUSFo by using a REGISTER message.
  a2) Receiving the request from the SCUAFo, the CUSFo triggers the SCFo.
  a3) The SCFo tries to obtain the Kn and the Kv by the Search Operation.
  a4) The SCFo judges the phase; if the Kv is not obtained, it is the roaming-service-setup phase, and if the Kv is obtained, it is the roaming-service-provision phase.

b) Roaming-service-setup phase [Fig. 6(a)]
  b1) The SCFo requests the authentication data transfer and the user's service profile transfer to the SDFo by ModifyEntry Operation.
  b2) The authentication is performed between the SDFo and the SDFh by the Bind operation. The authentication of the entity based on the challenge/response interactive authentication is studied in IN CS-2, but the authentication procedure is dependent on the agreements between network operators. Here, we show an example based on the existing X.509 [23].
  b3) The service profile is copied from the SDFh to the SDFo by the ShadowUpdate operation.
  b4) The service profile and the authentication data KhF[KtF(Kv)] are transferred by the ModifyEntry result.
  b5) The SCFo generates the challenge (rnd), and sends it with the cipher key Kt and the authentication data KhF[KtF(Kv)] to the SCAUFo through the CUSFo by using a FACILITY message.
  b6) The SCAUFo returns the authentication response KvF(rnd) calculated in the terminal to the SCFo through the CUSFo by using a FACILITY message.
  b7) The SCFo performs the authentication and the service profile check.
  b8) The SCFo performs location registration and stores the Kv in the SDFo by ModifyEntry Operation.
  b9) The SCFo performs location registration in the SDFh through the SDFo by the ModifyEntry operation.



(a)

(b)

Fig. 6. Signaling protocol example for location registration based on the proposed authentication protocol. (a) Roaming-service-setup phase. (b) Roaming-service-provision phase.

b10) The success of location registration and the authentication response KvF[KvF(rnd)] are notified by the SCFo, through the CUSFo, to the SCAUFo by using a RELCOMP message.

c) Roaming-service-provision phase [Fig. 6(b)]

c1) The SCFo generates the challenge (rnd), and sends it to the SCAUFo through the CUSFo by using a FACILITY message.

c2) The SCAUFo returns the authentication response KvF(rnd) calculated in the terminal to the SCFo through the CUSFo by using a FACILITY message.

c3) The SCFo performs the authentication and the service profile check.

c4) The SCFo performs the location registration in the SDFo by the ModifyEntry Operation.

c5) The success of location registration and the authentication response KvF[KvF(rnd)] are notified to the SCAUFo, through the CUSFo and by the SCFo, by using a RELCOMP message.

VI. Conclusion

In the authentication technique proposed in this paper, each TSM controls and administrates the authentication of the home subscriber and the roamer in the same manner in service provision in order to unify the procedures in the GLOMONET. The authentication control of the subscriber/roamer by the TAK generated by the TSM enables the security of the whole GLOMONET to be reinforced because the TAK is renewed in each roaming to prevent fraudulent action to plural roamed networks, and the TAK administration by the TSM clarifies the administration responsibility when an illegal access takes place. Although this paper suggested that the TAK be generated at each roaming, the TAK generation may be performed at each location registration within a network in order to enhance security. In such a case, special consideration for the balanced system design would be needed because the number of signals would increase.

Our proposed authentication technique is generally suitable for the distributed security management of global communication, and its use in other fields, such as the internet, will be studied.

REFERENCES

[1] ETSI GSM Specifications, Series 01–12.

[2] TIA/EIA IS-54, *Cellular System Dual-Mode Mobile Station-Base Station Compatibility Standard*, Telecommun. Ind. Assoc., Apr. 1992.

[3] TTC JJ-70.10, *Personal Digital Cellular Digital Mobile Communication Networks Inter-Node Interface—Mobile Application Part—*, Telecommun. Technol. Committee, 1995.

[4] R. Steedman, "The common air interface MPT 1375," in *Cordless Telecommunications in Europe*, W. K. W. Tuttlebee, Ed. Berlin: Springer-Verlag, 1990.

[5] RCR STD-28, *Personal Handy Phone System ARIB standard*, ver. 2.0, Res. Develop. Cen. for Radio Syst., Dec. 1995.

[6] ETSI, *Digital European Cordless Telecommunications Common Interface*, Radio Equipment and Syst., Valbonne, France.

[7] JTC J-STD-014, *Personal Access Communications System Air Interface Standard*," Joint Tech. Committee, June 1995.

[8] ITU-T, Recommendation Q.76, *Service Procedures for Universal Personal Telecommunication, Functional Modeling, and Information Flow*, 1995.

[9] ITU-T Draft Recommendation Q.FNA, *Network Functional Model for FPLMTS*, ver. 6.0.0, Jan. 1997.

[10] ITU-T, Draft Recommendation Q.FIF, *Information Flows for FPLMTS*, ver. 6.0, Jan. 1997.

[11] TIA/EIA IS-41, *Cellular Radio Telecommunications Intersystem Operations*," Telecommun. Ind. Assoc., Dec. 1991.

[12] D. Brown, "Techniques for privacy and authentication personal communication systems," *IEEE Personal Commun.*, Aug. 1995.

[13] ITU-T, Draft Recommendation Q.1224, *Distributed Functional Plane for Intelligent Network CS-2*," Jan. 1997.

[14] ITU-T, Draft Recommendation Q.1228, *Interface Recommendations for Intelligent Network CS-2*, Jan. 1997.

[15] ITU-T, Draft Recommendation Q.ASEC, *Security Mechanisms and Protocols for Protecting the Access to Network Services*," Jan. 1997.

[16] ITU-T, Draft Recommendation Q.NSEC, *Network Security*, Jan. 1997.

[17] S. Suzuki, T. Nohara, and T. Nakanishi, "A proposal for one-way authentication in UPT," presented at the 1996 Spring Soc. Conf. IEICE.

[18] W. Diffie and M. W. Hellman, "New direction in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, Nov. 1976.

[19] M. Matsui, "Cryptography and authentication technology," *J. Inst. Electron., Inform. Commun. Eng.*, vol. 79, pp. 107–114, 1996.

[20] S. Miyaguchi, "The FEAL cipher family," in *Advances in Cryptology—CRYPTO'90*, LNCS 537. Berlin: Springer-Verlag, 1991, pp. 627–638.

[21] S. Miyaguchi, S. Kurihara, K. Ohta, and H. Morita, "Expansion of FEAL cipher," *NTT Rev.*, pp. 117–127, Nov. 1990.

[22] ITU-T, temporary document, *Baseline Document on Requirement for UPT (SS1/CS2)*, Jan. 1997.

[23] ITU-T, Recommendation X.508, *The Directory-Authentication Framework*, Feb. 1993.

Shigefusa Suzuki (M'86), for a photograph and biography, see this issue, p. 1607.

Kazuhiko Nakada received the B.S. and M.S. degrees from Waseda University, Tokyo, Japan, in 1992 and 1994, respectively.

In 1994, he joined NTT, Japan, and since 1996, he has been responsible for developing the personal handy-phone system (PHS). He is currently with the NTT Network Service Systems Laboratories.

Mr. Nakada is a member of the IEICE of Japan.