A New Service for Digital Mobile Communications

Min-Shiang Hwang †‡ Email: m24@twnmoctl.bitnet
Jyh-Kong Wey †‡ Email: wey@twnmoctl.bitnet
Wei-Pang Yang † Email: wpyang@twncu01.bitnet

Department of Computer and Information Science †
National Chiao Tung University
Hsinchu, Taiwan 300, R.O.C.

Directorate General of Telecommunication Laboratories ‡
Ministry of Transportation and Communications
Chung-Li, Taiwan 320, R.O.C.

Abstract
In this paper, we propose a new service for digital mobile communication systems. The service can provide for two or more users to hold a secure conference. Two requirements must be considered: privacy and authentication. Privacy is to ensure that an eavesdropper cannot intercept conversations of a conference. Authentication issue is to ensure that service is not obtained fraudulently in order to avoid charge for usage. We present a new conference key distribution scheme for digital mobile communication systems. In the scheme, a group of users can generate a common secret key over the public channel to hold a secure conference. 

Key words: Cryptography; Mobile communication; Security

1 Introduction
Mobile satellite communications have been carried out in many systems not only for maritime systems but also for aeronautical and land mobile satellite communication systems. A main characteristic of the mobile satellite communication systems is that they provide wireless access to the traditional wireline networks for a large number of access services such as telephone calls. But wireless transmission are vulnerable to relatively easy interceptions [6], such as fraudulent call attempts and intrusion or listening-in by third parties. Thus, we must take actions to prevent various kinds of intrusion. For example, sensitive data must be protected against disclosure to an unauthorized person. Fraudulent modification of messages, repeating old messages or one user masquerading as another must also be prevented. Data are more vulnerable in network than anywhere else, especially in the mobile communication networks. For this reason, we really need to consider a feasible solution for implementation of secure mobile communication systems.

A simple but effective method for secure digital communications is the use of encryption methods. Two of the encryption methods: private-key cryptosystems such as DES [13, 18] and FEAL-32 [12], and public-key cryptosystems such as RSA [16] are available. Public-key cryptosystems re-
quire high computational complexity for increasing security. As a result, public-key cryptosystems cannot be used in low-cost and low-power mobile (portable) communication systems because no protocols have provided acceptable call-setup time performance [5]. Private-key cryptosystems is simple and faster than the public-key cryptosystem as far as computational complexity is concerned. But private-key cryptosystems require a tremendous effort on key management and distributions [3]. Private-key cryptosystems require that users (portable) to the conversation share knowledge of a secret key, and that other unauthorized users do not have access to this key. Key agreement is the process by which these users agree upon the proper key.

In this paper, we propose a new service for digital mobile communication systems. Three or more users can hold a secure electronic conference provided by this service. Two requirements must be considered: privacy and authentication. Privacy is to ensure that eavesdropper cannot intercept conversation content of a conference and information about conferences’ locations. The authentication issue is to ensure that service is not obtained fraudulently in order to avoid charges for usage. We thus have the following four security goals for the mobile communication system:

1. Privacy of conversation contents during the conference.
2. Privacy of information about conferences’ locations in the conference.
3. Control of fraud which ensures that the portable unit is authentic to deter fraudulent access.
4. Prevention of replaying attack which ensures that intruders are not able to obtain sensitive data by replaying a previously intercepted message.

Since the portable unit must operate over long periods of time on small low-power batteries, low complexity implementation of the encryption function is critical. Private-key cryptosystems meet such criteria [2]. As mentioned above, the private-key cryptosystems require an agreed-upon session key by the conferences in the conference.

In this paper, we present a new conference key distribution scheme for digital mobile communication systems. In the scheme, a group of conferences can generate a common secret key over the public channel to hold a secure conference.

This paper is organized as follows. In the next section, we review previous key distribution schemes and their problems when they are applied to mobile communication systems. In Section 3, we present a new scheme for mobile communication systems. In Section 4, we analyze the security of our schemes. Finally, Section 5 presents our conclusion.

2 Related Key Distribution Schemes

A key distribution protocol for mobile communication systems was first proposed in [10]. The mobile communication systems may be regarded as star-type networks. For convenience, let “portable” denotes a user terminal. Each user terminal in the network communicates with another user via a network center. In order to remove the key management at a network center and to avoid hardware limitation user terminals to obtain a common secret key in a reasonable time, Tatebayashi et al. [19] employed a public key cryptosystem such as RSA cryptosystem for uplink channels (from a user terminal to a network center), and a secret key cryptosystem such as Vernam cipher for downlink channels (from a network center to user terminals). Unfortunately, this method has been attacked by Park et al. [14]. Recently, Hwang proposed another scheme based on symmetric key cryptography [7]. This method requires a key management at the network center. Beller, Chang, and Yacobi of Bellcore proposed three elegant public-key/private-key hybrid key agreement and authentication protocols [1, 2]. Their methods are based on the modular square root technique [13] and the Diffie-Hellman technique [7].

The above key distribution schemes, however, can be used only by two user terminals. If three or more user terminals want to communicate in order to hold an electronic conference, they have to derive one communication key for each link in the digital mobile communication systems. Doing so, it requires \((m - 1)\) times more computations than that needed for two users, where \(m\) is the number of users terminal.

The concept of conference key distribution was first proposed by Ingemarsson et al. [8]. A number of studies have been carried out for conference key distribution systems [9, 10, 11]. Since these schemes require a high computational complexity (modular exponentiation) as the fundamental arithmetic, these schemes are not suitable to use in low-cost and low-power mobile communication systems. In this article, a new conference key distribution scheme is proposed for low-complexity digital mobile communication systems. In our scheme, a group of conferences can generate a common secret key over the public channel to hold a secure conference.
3 A New Efficient Scheme

In this section we present a conference key distribution protocol for digital mobile communications. The protocol is based on the public-key cryptography. In this scheme, the network center need not keep the secret keys of all conference.

Without loss of generality, let user terminal $T_i$ be the terminal logged in by the chairperson $U_1$ who initiates the secure electronic conference with $m$ conferees, $U_1, U_2, \ldots, U_m$. Moreover, let $NC$ be the network center; $T_i$ be the terminal logged in by $U_i$; $ID_i$ be the unique identity of $U_i$; $CK_1$ and $CK_2$ be the random numbers generated by $T_i$; and $t_i$ be a current date and time in which message is sent. The symbol $||$ denotes a concatenation of two numbers. $NC$ generates each user $U_i$ secret $s_i$ from $ID_i$ and $s_i = f(ID_i)$, where $f$ is a secret one-way function which only the network center knows.

This protocol for the conference key distribution is based on the asymmetric key cryptography. We use the RSA cryptographic method as the asymmetric cryptosystem. In the following protocol, the modulus $n$ is a product of $p$ and $q$, where $p$ and $q$ are large prime numbers. The encryption exponent $e$ is chosen to be 3. The decryption exponent $d$ is a number satisfying $ed \mod \phi(n) = 1$ where $\phi(n)$ denotes the Euler’s totient function of $n$. This key distribution protocol, as illustrated shown in Figure 1, can be summarized as follows:

Confereen Key Distribution Protocol (CKDP):

Step 1: Initial terminal $T_1$ chooses random numbers $CK_1$ and $CK_2$, and the key $CK = CK_1 + CK_2$ as a common secret session key.

Step 2: $T_1$ sends $(t_1||s_1||CK_1||CK_2||ID_1, i = 1, \ldots, m)^3 \mod n$ to the network center (NC).

Step 3: $NC$ decrypts the encrypted data signal and gets $(t_1||s_1||CK_1||CK_2||ID_1, i = 1, \ldots, m)$. $NC$ extracts $t_1$, $s_1$, $CK_1$, $CK_2$, and $ID_1, i = 1, \ldots, m$ from the decrypted data. $NC$ checks the validity of the timestamp $t_1$. $NC$ verifies $T_1$ and computes $CK = CK_1 + CK_2$.

Step 4: $NC$ calls the other terminals of conference. $NC$ randomly chooses a coefficient $a$ which is securely known only by $NC$ and then constructs a polynomial of one degree $y = CK + ax \mod n$. $NC$ also randomly chooses $x_0$ and obtains $y_0$ from $y = CK + ax \mod n$.

Step 5: Each terminal, $T_i, i = 2, \ldots, m$, chooses random numbers $x_{i1}$ and $x_{i2}$ as a key-encryption key.

Step 6: Each $T_i, i = 2, \ldots, m$ sends $(t_i||s_i||x_{i1}||x_{i2}||ID_i)^3 \mod n$ to $NC$.

Step 7: $NC$ decrypts the encrypted data signal and gets $(t_i||s_i||x_{i1}||x_{i2}||ID_i)$. $NC$ extracts $t_i$, $s_i$, $x_{i1}$, $x_{i2}$, and $ID_i$ from the decrypted data. $NC$ checks the validity of the timestamp $t_i$. $NC$ verifies $T_i$ and computes $z_i = x_{i1} + x_{i2}$.

Step 8: $NC$ obtains $y_i, i = 2, \ldots, m$ by substituting $z_i$ into equation $y_i = CK + az_i \mod n$.

Step 9: $NC$ broadcasts $(x_0, y_0, y_2, y_3, \ldots, y_m)$ to $T_i, i = 2, \ldots, m$.

Step 10: $T_i$ computes the common secret session key with $T_1$, $CK = y_i - (2^{x_{i2}} - x_{i1}) x_i \mod n$.

4 Security Analysis

In this section, we shall show that both user authentication as well as session key distribution are addressed in our scheme simultaneously.

The network center will authenticate the chairperson’s identification $ID_1$ by checking the correctness of $ID_1$ at step 3 of the proposed protocol. Similarly, the network center can authenticate other users’ identification $ID_i$ for those who participate in this conference invited by the chairperson by checking the correctness of $ID_i$ at step 7 of the proposed protocol. Therefore, the protocol ensures that a portable unit does not access the network using a false identity in order to avoid charges for usage.

Since the common secret session key $CK$ is sent to network center by encryption function, an intruder cannot decipher $CK$ except when one knows the secret key of the network center in Protocol CKDP. Therefore, the conference have a secure conversation.

Similarly, the location of conferees is protected by the above mentioned encryption function. It is difficult for an intruder to obtain the location of $ID_i$ from the equation $(t_i||s_i||CK_1||CK_2||ID_i, i = 1, \ldots, m)^3 \mod n$ of step 2 in protocol CKDP.

Basically, the step 8, step 9, and step 10 in the proposed protocol is implementations of (2, m) Shamir’s threshold scheme [17]. Therefore, revealing the secret conference key of our scheme is equivalent to nullifying the Shamir’s threshold scheme.

In order to pass the verification of step 3 and step 7 in our protocol, an intruder must change $t_i$ into a new time $t_i^*$ such that $(T" - T^*) \leq \Delta T$, where $T^*$ is the time when the system receives the illegal login message, and $\Delta T$ is the expected legal time interval for transmission delay. Once $t_i$ is changed, an intruder will fail the verification of step 3 and step 7 in the proposed protocol. Therefore, the pro-
posed scheme is secure against replaying attacks.

5 Conclusions
We have proposed a scheme for holding secure electronics conferences in digital mobile communication systems. The protocol enable hardware-limited user terminals to obtain a common secret conference key in a reasonable time. Both user authentication as well as key distribution are examined in the proposed scheme simultaneously. The other feature of our scheme is that the chairperson can freely choose a common key $CK$ shared among all legitimately intended principals and himself.

Acknowledgments
We wish to thank many anonymous referees for their suggestions to improve this paper. This research was funded by grant NSC83-0108-E-009-039 from the National Science Council, Taiwan, Republic Of China.

References


Figure 1: Conference Key Distribution Protocol (CKDP).