Authenticated Key-Exchange in a Mobile Radio Network

Min-Shiang Hwang [†]
Email: mshwang@dec8.cyit.edu.tw

Chii-Hwa Lee [‡]
Email: gis81817@cis.nctu.edu.tw

Department of Information Management [†]
ChaoYang Institute of Technology
Wufeng, Taiwan, R.O.C.

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

May 21, 2007

Abstract

A new method is proposed in this study for implementation of secure digital mobile communication systems. Two requirements for the systems must be considered, i.e., privacy and authentication. Privacy ensures that an eavesdropper cannot intercept conversations between two parties. Authentication ensures that service is not obtained fraudulently in order to avoid charge for usage. Additionally, a new key distribution scheme is designed for practical implementation in a low-cost and low-power digital mobile communication system.

1 INTRODUCTION

One of the main features of mobile communication systems is that it provides wireless access to the traditional wireline networks for a large number of access services, e.g., telephone calls. However, wireless transmissions are vulnerable to relatively easy interceptions [1], e.g., fraudulent call attempts and intrusion or listening-in by third parties. Thus, actions must be taken to prevent various kinds of intrusion [2]. For example, sensitive data must be protected against disclosure to an unauthorized individual. Furthermore, fraudulent modification of messages, repeating old messages or one user masquerading as another must also be prevented. A feasible solution must be found for eavesdropping in, and illegal access to, mobile communications systems.

A simple but feasible method for secure digital communications is the use of encryption methods. Two of the encryption methods, i.e., secret-key cryptosystems (such as DES [3, 4] and FEAL-32 [5]) and public-key cryptosystems (such as RSA

†

‡

†

‡

[6]), have already been proposed. For increasing security, computations of public-key cryptosystems become more complex correspondingly. As a result, public-key cryptosystems cannot be used in a low-cost and low-power mobile (portable) communication system because no protocol has yet provided acceptable call-setup time performance [7]. Computations for secret-key cryptosystems are faster and less complex than that of public-key cryptosystems. However, secret-key cryptosystems demand a serious effort towards key management and distributions [8]. Secret-key cryptosystems require that the mobile users share a common secret-key, and that other users do not have access to this key. Key agreement is the process by which these users agree upon the proper key.

In this study, a new method is proposed for implementation of secure digital mobile communication systems. The privacy and authentication requirements can be satisfied by addressing the following four security criteria [9]:

1. Privacy of conversation content between two parties. An unauthorized user cannot decipher the conversation content of two parties.

2. Privacy of information regarding mobile users location. An unauthorized user cannot find out the location of another mobile users.

3. Control of fraud which ensures that the portable unit is capable to deter fraudulent access. An unauthorized party cannot fabricate a legal portable unit in order to avoid charges for usage. An illegal portable unit cannot access the network using a false identity in order to avoid charges for illegitimate usage.

4. Prevention of replaying attack which ensures that intruders are not capable of obtaining sensitive data by replaying a previously intercepted message.

Since the portables must operate over long periods of time on small low-power batteries, low complexity implementation is critical[10]. As mentioned above, computations for secret-key cryptosystems are faster and less complex than that of public-key cryptosystems. However, secret-key cryptosystems demand a serious effort towards an agreed-upon session key before service calls.

A key distribution protocol for mobile communication systems was proposed in [11]. The mobile communication systems is geographically regarded as a star-type network in [11]. Each portable unit communicates with another user via a network center. In order to remove the key management at the network center and to enable hardware-limited portable units (user terminals) to obtain a common secret key in a reasonable amount of time, Tatebayashi et al. [11] employed a public key cryptosystem such as the RSA cryptosystem for uplink channels (from a portable unit to a network center), and a secret key cryptosystem such as the Vernam cipher for downlink channels (from a network center to portable unit). Unfortunately, this method has been attacked by Park et al. [12]. Recently, Ballard et al. and Hwang proposed another scheme based on secret-key cryptosystems [13, 14]. These methods require a key management at the network center. We refer interested readers to these papers [12, 13, 14].

Beller, Chang, and Yacobi of Bellcore proposed three elegant public-key/secret-key hybrid key agreement and authentication protocols [15, 10]. Their methods are based on the modular square root technique [16] and the Diffie-Hellman technique [17] in which their scheme requires a number of computations. Beller and Yacobi developed a new public-key protocol for agreement and authentication [18]. Their methods are based on the Rabin scheme and ElGamal scheme. This protocol provides security which is comparable to the well known RSA public-key protocol; however, two orders of magnitude less on-line computation are required on all portable units of the protocol. The protocol requires precomputation on the order of 200 modular multiplications in the portable unit for each execution.

In this study, a new key distribution scheme is designed for practical implementation in a low-cost and low-power digital mobile communication system. Related cryptography is reviewed in Section 2. Our proposed scheme for secure mobile communication systems is presented in Section 3. In Section 4, the security of our scheme is analyzed. In Section 5, we discuss and evaluate the complexity of the proposed scheme. Concluding Remarks are finally made in Section 6.

2 RELATED CRYPTOGRAPHY

The protocol for the key distribution is based on two public-key cryptographies, i.e., the RSA cryptographic scheme and ElGamal's signature scheme.

In 1978, Rivest, Shamir, and Adleman of MIT [6] proposed a well-known public-key (RSA) cryptosystem based on the difficulty of factoring. In this scheme, the enciphering keys are pairs (e, n) which consists of an exponent e and a modulus n that is the product of two large distinct odd primes p and q. This pair satisfies the equation $\gcd(e, \phi(n)) = 1$, where $\phi(n)$ denotes the Euler's totient function of n. To encipher a plaintext block M, we form a ciphertext block C by

$$C = M^e \bmod n. \tag{1}$$

The deciphering procedure requires knowledge of the secret key d which satisfies $ed \bmod \phi(n) = 1$. To decipher the ciphertext block C, we compute

$$M = C^d \bmod n. \tag{2}$$

In 1985, ElGamal [19] proposed a public key cryptosystem and a digital signature scheme based on discrete logarithms. In this scheme, two public values P and g are in the system. P is a large prime number and $(P-1)$ has a large prime factor. g is the primitive element in the Galois field $GF(P)$. Each user U_i has a secret key

x_i, $x_i \in [1, P-2]$, and a public key y_i, where $y_i = g^{x_i} \bmod P$. Thus, recovering the secret information from the public information requires the computation of a discrete logarithm modulo P. If user A wants to sign a message block M, an integer between 0 and $(P-1)$, and send the signed message to user B, user A does the following:

1. Randomly chooses a secure integer k, $1 < k < (P-1)$, such that $\gcd(k_i, P-1) = 1$.
2. Compute $h = g^k \bmod P$.
3. Evaluate s such that $M = xh + ks \bmod (P-1)$, where x is a secret key maintained by user A.

Once these calculations have been performed, user A's signature on M is the pair (h, s). Since $M = xh + ks \bmod (P-1)$, $g^M = g^{xh+ks} = g^{xh}g^{ks} = y^h h^s \bmod P$, the recipient B can verify that $(M, h, s) = S_x(M)$ by checking that $g^M = y^h h^s \bmod P$ is satisfied.

3 OUR SCHEME

In our scheme, we make M in ElGamal's scheme as ID (the user identity) and $S_x(M)$, the signed version of M associated with system's secret key x, as the authentication certificates of the user. A legal user, when desiring to call a service, inserts his service card into a portable unit. The service card contains identity (ID_i) and certificate (C_i) of the legal user. The certificate C_i satisfies $ID_i = xh + kC_i$. The network center then uses the public key to verify that $g^{ID_i} = y^h h^{C_i} \bmod P$.

In order to withstand replaying attacks, a time stamp [8] and a random number are introduced in the authentication certificate.

In our new protocols, let NC be the network center; P_i be the portable unit of

U_i; ID_i be the unique identity of U_i; r_i be the random number generated by P_i; T be a current date and time when message is sent, and $||$ denotes a concatenation.

The new key distribution scheme can be divided into four phases, i.e., the system's initialization phase, the registration phase, the service call request phase, and the authentication phase.

System's initialization phase: Before registering to the network center, the mobile communication system must generate some parameters for registration center in this phase.

1. Choose the system-wide parameters, namely the prime P, the primitive element g, the system secret ket x_s with the corresponding public key y_s, the RSA modulus n, and the RSA decryption-key d. These parameters are stated in Section 2.

2. Distribute these parameters (P, g, y_s, n, d) via an authentic and confidential channel to the network center.

Before accessing service calls in a mobile communication system, a new user must register his identity at the system registration center via the registration phase. The center provides the new user with a service card through a secure channel. A legal user, when desiring to call a service, inserts his service card into a portable unit.

Registration phase: Suppose that a new user U_i submits his ID_i to the system. The system does the following to compute the certificate C_i for user U_i:

1. Randomly chooses a secure integer k_i, $1 < k_i < (P-1)$, such that $\gcd(k_i, P-1) = 1$.

2. Compute $h_i = g^{k_i} \bmod P$.

3. Evaluate C_i such that $ID_i = x_s h_i + k_i C_i \bmod (P-1)$, where x_s is a secret key maintained by the system and $y_s = g^{x_s} \bmod P$ is a public key of the system.

The registration center issues a service card through a secure channel to the new user. This service card records the values of ID_i, h_i, C_i, P, and the RSA modulus n.

Service call request phase: Upon a service call request, U_i inserts his service card into a portable unit. The portable unit will perform the following operations:

1. Choose a random number SK_i as a common secret session key.

2. Generate a random number r such that $\gcd(r, C_i) = 1$.

3. Generate S_1 by the server-aided computation protocol [20].

   (a) Randomly generate an integer vector $R = [r_1, r_2, \cdots, r_m]$ and a binary vector $B = [b_1, b_2, \cdots, b_m]$ such that $r = \sum_{j=1}^{m} b_j r_j \bmod (P-1)$, $1 \leq r_j < P$, and $Weight(B)$, the Hamming weight, equals to $\sum_{j=1}^{m} b_j$, where m and l are some integers and $Weight(B) \leq l$.

   (b) Compute $h'_i = h_i^3 \bmod n$.

   (c) Send P, R, and h'_i to NC.

   (d) NC computes and sends back to the portable unit $Y = [y_1, y_2, \cdots, y_m]$ such that $y_j = h_i^{r_j} \bmod P$.

   (e) Compute $S_1 = \prod_{b_j} y_j \bmod P$ for which $b_j = 1$.

4. Compute $t = f(S_1, T) \bmod (P-1)$, where f is a one-way function and T is the current date and time.

5. Compute $S_2 = C_i + rt \bmod (P-1)$.

6. Send $C = (ID_i||h_i||S_1||S_2||T||SK_i)^3 \bmod n$ to NC.

Authentication phase: After NC receives the message C sent from user U_i at time T', then NC performs the following tasks:

1. Decrypt and extracts the encrypted data signal with the RSA cryptosystem and gets ID_i, h_i, S_1, S_2, T, SK_i.

2. Test the validity of ID_i. If the format of ID_i is incorrect, then the system rejects the service request.

3. Test the time interval between T and T'. If $(T'-T) \geq \Delta T$, where ΔT denotes the expected legal time interval for transmission delay, then the system rejects the service request.

4. If $h_i^{S_2} = g^{ID_i} y_s^{-h_i} S_1^{f(S_1,T)} \bmod P$, then NC accepts the service request. Otherwise, it rejects the request.

If the user is a legal one, the service request is validated. We now show that the equation $h_i^{S_2} = g^{ID_i} y_s^{-h_i} S_1^{f(S_1,T)} \bmod P$ holds as follows:

$$\begin{aligned} h_i^{S_2} &= h_i^{C_i+rt} \bmod P, \\ &= h_i^{C_i} h_i^{rt} \bmod P, \\ &= h_i^{C_i} S_1^{f(S_1,T)} \bmod P. \end{aligned} \tag{3}$$

And,

$$\begin{aligned} g^{ID_i} &= g^{x_s h_i + k_i C_i} \bmod P, \\ &= g^{x_s h_i} g^{k_i C_i} \bmod P, \\ &= y_s^{h_i} h_i^{C_i} \bmod P. \end{aligned} \tag{4}$$

From equation (3) and (4), the equation $h_i^{S_2} = g^{ID_i} y_s^{-h_i} S_1^{f(S_1,T)} \bmod P$ holds.

4 SECURITY ANALYSIS

Both user authentication as well as session key distribution are shown in this section to be capable of being simultaneously examined in our schemes.

Because our scheme is based on the ElGamal digital signature scheme, it is relatively difficult for the user U_i to compute the secret key of the system from the equation $y_s = g^{x_s} \bmod P$. It is also difficult for an intruder to obtain the system-generated random number k_i directly from the equation $h_i = g^{k_i} \bmod P$ of step 2 in the registration phase. This provides the intruder with little information to obtain the authentication certificates of legals user from the equation $ID_i = x_s h_i + k_i C_i \bmod (P-1)$ of step 3 in the registration phase and the equation $S_2 = C_i + rt \bmod (P-1)$ of step 5 in the service call request phase. This difficulty results from the complexity of computing discrete logarithms over finite fields [19].

The network center will authenticate the user identity ID_i by verifying the validity of ID_i at step 2 of the authentication phase. Intruders, although capable of forging a valid identity, do not pass the test of step 4 in the authentication phase without a valid corresponding secret parameters. Therefore, our scheme ensures that a portable unit does not access the network using a false identity in order to avoid charges for usage.

In order to pass the test of step 3 in the authentication phase, the intruder must change T into a new time T^* such that $(T'' - T^*) \leq \Delta T$, where T'' is the time when the network center receives the illegal service request. Once T is changed, the intruder will fail the test of step 4 in the authentication phase unless either t or S_2 has been changed accordingly. Therefore, the proposed scheme is secure against replaying attacks.

Since the common secret session key SK is sent to the network center by an encryption function, an intruder cannot deciphers SK except for when the secret key of the network center is known. Therefore, the portable unit which require that services share knowledge of a secret key with the network center. Other parties do not have access to this key.

Similarly, the location of users is protected by the above mentioned encryption function. It is difficult for an intruder to obtain the location of ID_i from the equation $h_i^3 \bmod n$ of step 3(b) and the equation $(ID_i||h_i||S_1||S_2||T||SK_i)^3 \bmod n$ of step 6 in the service call request phase.

Basically, step 3 of the service call request phase is an implementation of the server-aided computation protocol [20]. In this implementation, a small device such as a smart card can efficiently execute secret computations using computing power of auxiliary devices (the network center in this case). Since r is a random number and is used only once for each service requested, our scheme is secret against Pfitzmann and Waidner's passive attacks [21].

Since important information (such as SK_i, h_i, etc.) is encrypted before transferring to NC or the destination, the security requirements of our scheme are satisfied four security criteria which are stated in Section 1. The mobile network in our scheme can be composed of intermediate networks managed by different administrative authorities.

The protection against replay attacks relies on the synchronization of clocks. The scheme tests $T' - T \geq \Delta T$ to detect replays of calling messages. However, this test may be susceptible in the following two cases. One is that as a result of possibly induced communication delays and loose clock synchronization if ΔT is small, legitimate authentication requests are denied. The other is that replaying attacks if ΔT

is large. Many schemes involving the technology of synchronizing clocks in computer communications have been proposed for solving the above problem [22, 23].

5 COMPUTATIONAL ANALYSIS AND COMPARISON

The computational complexity of our scheme in the portable is dominated by the multiplication of step 3 in the service call request phase. This computation only needs $2(l-1)$ multiplications and $2(m+1)$ communications. If we choose $m = 40$ and $l = 20$, the secret r in the service call request phase could be revealed by searching a true vector B via the exhaustion of $\sum_{j=1}^{l} \binom{m}{j} > \binom{m}{l} > 10^{26}$ possibilities only [20]. In this case, the portable unit only requires 19 modular multiples. The amount of communication is 82 integers of size at most $\log P$ bits. For high security, we let P is an integer of length 256 bits. If we use a 9600 bps as a transmission device. The portable unit takes about 2 seconds in transmission.

There are also one modular multiplications for step 4 and 5, and three for step 6, leading to a total of 24 modular multiples for the whole scheme. The size of the message $(ID_i||h_i||S_1||S_2||T||SK_i)$ of step 6 in the service call request phase is 768 bits long. However, we can reduce the size by the modulus n. Therefore, there are three modular multiplications for step 6 in the service call request phase. If we use an i8086/5MHz ($30msec/256-bit$ modular multiplication) as a service card with a bit rate of around 200-300 kbit/s for a narrowband TDMA system for GSM [20, 24], the portable unit only takes 0.8 second in average. This is achievable in real time by a portable unit. On the contrary, the third scheme (MSR+DH scheme) of [10] requires 212 modular multiples (6.36 second on an i8086/5MHz microprocessor). Thus, our proposed scheme is practical for implementation in low-cost and low-power secure mobile communication systems.

6 CONCLUSIONS

Mobile communication systems consist of mobile switching centers, base stations, and portable units. Since the mobile switching centers and base stations generally reside at a fixed location, the switching centers and base stations can be installed using high-power, high-cost mechanisms. However, the portables are movable and are carried by persons or on vehicles. Since the portables must operate over long periods of time on small low-power batteries, low complexity implementation is critical.

One mobile switching center can service many base stations, and one base station can service many portables. The role of the network center in our scheme can be taken over by the base station or the mobile switching center, both of which can perform complex computations in a reasonable time. In comparison, the portables are required to perform only relatively simple computations.

A scheme has been proposed in this study for private and authenticate communication in digital mobile systems. This scheme enables hardware-limited portable unit to obtain a common secret session key in a reasonable amount of time. Both user authentication as well as key distribution are simultaneously examined in the proposed scheme.

ACKNOWLEDGEMENTS

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC86-2621-E-324-001-T.

References

[1] S. R. Hall and D. P. Maher: *Closing in on wireless privacy.* "AT& T Technology", Vol. 8, No. 3, 1993, p.22–25.

[2] C. Déchaux and R. Scheller: *What are GSM and DCS.* "Electrical Communication", 2nd Quarter 1993, p.118–127.

[3] National Bureau of Standard: *Data Encryption Standard.* FIPS, NBS, 1977.

[4] M. E. Smid and D. K. Branstad: *The data encryption standard: past and future.* "Proc. of the IEEE", Vol. 76, No. 5, 1988, p.550–559.

[5] S. Miyaguchi: *The FEAL cipher family.* Proc. of CRYPTO'90, August 1990, p.727–638.

[6] R. L. Rivest, A. Shamir, and L. Adleman: *A method for obtaining digital signatures and public key cryptosystems.* "Communications of the ACM", Vol. 21, No. 2, 1978, p.120–126.

[7] ETSI: *Digital European cordless telecommunications common interface part 7: Security features.* Technical Report Version 5.03, European Telecommunications Standards Institute, ETSI, May 1991.

[8] Dorothy E. R. Denning: *Cryptography and Data Security.* Addison-Wesley, Massachusetts, 1982.

[9] Min-Shiang Hwang and Wei-Pang Yang: *Conference key distribution protocols for digital mobile communication systems.* "IEEE Journal on Selected Areas in Communications", Vol. 13, No. 2, 1995, p.416–420.

[10] M. J. Beller, L. F. Chang, and Y. Yacobi: *Privacy and authentication on a portable communications system.* "IEEE Journal on Selected Areas in Communications", Vol. 11, No. 6, 1993, p.821–829.

[11] M. Tatebayashi, N. Matsuzaki, and Jr. D. B. Newman: *Key distribution protocol for digital mobile communication systems.* Proceedings of Crypto'89, 1989, p. 324–334.

[12] C. Park, K. Kurosawa, T. Okamoto, and S. Tsujii: *On key distribution and authentication in mobile radio networks.* Proceedings of Eurocrypt'93, 1993 p.461–465.

[13] M. Ballard, E. Issenmann, and M. Moya Sanchez: *Cellular mobile radio as an intelligent network application.* "Electrical Communication", Vol. 63, No. 4, 1989, p.389–399.

[14] T. Hwang: *Scheme for secure digital mobile communications based on symmetric key cryptography.* "Information Processing Letters", Vol. 48, 1993, p.35–37.

[15] M. J. Beller, L. F. Chang, and Y. Yacobi: *Privacy and authentication on a portable communications system.* IEEE Globecom'91, Phoenix, December 1991, p.1922–1927.

[16] M. O. Rabin: *Digitalized signatures and public-key functions as intractable as factorization.* Technical Report MIT/LCS/TR-212, Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, Mass., Jan. 1979.

[17] W. Diffie and M. E. Hellman: *New Directions in Cryptography.* "IEEE Transactions on Information Theory", Vol. 22, 1976, p.644–654.

[18] M. J. Beller and Y. Yacobi: *Fully-fledged two-way public key authentication and key agreement for low-cost terminals.* "IEE Electronics Letters", Vol. 29, No. 11, 1993, p.999–1001.

[19] T. ElGamal: *A public-key cryptosystem and a signature scheme based on discrete logarithms.* "IEEE Transactions on Information Theory", Vol. 31, No. 4, 1985, p.469–472.

[20] T. Matsumoto, K. Kato, and H. Imai: *Speeding up secret computations with insecure auxiliary devices.* Proceedings of CRYPTO'88, 1988, p.497–506.

[21] B. Pfitzmann and M. Waidner: *Attacks on protocols for server-aider RSA computation.* Proceedings of EUROCRYPT'92, 1992, p.153–162.

[22] D. L. Mills: *Internet time synchronization: The network time protocol.* "IEEE Transactions on Communications", Vol. 39, No. 10, 1991, p.1482–1493.

[23] D. L. Mills: *Precision synchronization of computer network clocks.* "ACM Computer Communication Review", Vol. 24, 1994, p.28–43.

[24] A. R. Potter: *Second generation cellular radio: UK industrial R&D.* Proceedings of the Cellular and Mobile Communications Conference, London, December 1987, p.19–28.