2003 International Symposium on Advanced Intelligent Systems
September 25-28, 2003, Jeju, Korea

Authentication and Key Agreement Protocol for Secure End - to - End Communications on Mobile Networks

Jeong-Hyun Park, Jin-Suk Kim, Hae-Kyu Kim, Jeong-Mo Yang*, Seung-Jae Yoo*

Information Technology Management Research Group,
Electronics and Telecommunications Research Institute (ETRI)
161 Kajong-Dong, Yusong-Gu, Taejon, 305-350, Korea

Email) jh-park {kimjs, hkkim}@etri.re.kr

*Information Engineering Department, Joongbu University
San2-25, Majon-Ri, Chuboo-Myun, Kumsan-Gun, ChungNam, 312-702, Korea

Email)jmoyang{sjyoo}@joongbu.ac.kr

ABSTRACT: This paper presents mutual authentication scheme between user and network on mobile communications using public key scheme based on counter, and simultaneously shows key agreement between user and user using random number for secure communications. This is also a range of possible solutions to authentication and key agreement problem - authentication and key agreement protocol based on nonce and count, and secure end-to-end protocol based on the function $Y = f(.)^{1/C_i}$, C_i is count of user I, and f(.) is one way function.

Key Words: Authentication Protocol, Key Agreement, Mobile Communications

I. INTRODUCTION

Once a shared Digital mobile communication systems transmit user data, and signaling data between digital cellular communications and array of ports via radio, making them more susceptible to eavesdropping than are conversations carried via wires. There is no physical link between the user and the mobile exchange, which could serve to identify the user for routing and charging purposes. The location of a particular user may be considered to be valuable information which, like conversion content, may need to be protected. Furthermore, the lack of association between a user and a particular physically secure location can make the digital mobile communications more vulnerable to attempts at fraudulent acquisition of service. It is important that digital mobile communication systems provide privacy at least comparable to that of the wireline network.

In digital mobile communications, authentication via secret key and/or public key techniques can be applied to the transmitted bits by the mobile station and network in order to ensure that an eavesdropper on the radio interface cannot intercept conversions. Secret key techniques require that both parties (mobile station and network) to conversion share knowledge of a secret key, and that other parties do not have access to this key. Public key techniques hold the promise of simplifying the provision of privacy authentication, thus reducing the cost to provide digital mobile communications. Various security protocols for the wireless mobile communication system have been proposed such as challenge/response scheme based on private key techniques which use in GSM and IS-41 area. The security protocols of most standard system are based on the secret key scheme since the computation required for the algorithm is negligible compared to the public key computation. The existing or emerging standards for such protocols in digital mobile communications industry, specifically GSM [1] (Group Special Mobile of the European Telecommunications Standards Institute - ETSI), DECT (Digital European Cordless Telephone, also of ETSI), and IS-95 [2] of the Telecommunications Industries Association (TIA) for U.S. Digital Cellular, all currently employ private key technology (symmetric key scheme) only. Both private key methods provide a means for user authentication and subsequent protection of user traffic. While public key

schemes were considered with only slight attention, they were rejected primarily because there were, at the time, no protocols which provided acceptable call-setup time performance. Tatebayshi et al. [3] and Beller et al. [4] showed a protocol by which an entity A and a network center share a session key. However, they didn't show a method by which two entities A and B can share a session key. Actually, the early version of Tatebayshi et al. was broken by Simmons' replay attack. The station-to-station (STS) protocol is a three pass variation on Diffie-Hellman that allows the establishment of a shared secret key between parties with mutual entity authentication and mutual explicit key authentication. The common secret key established by the STS protocol is given by $K = g^{rirj}$. In fact the STS protocol is a directly strengthened version of the basic Diffie-Hellman protocol, with the main additions being the encrypted and signed commitments in the second and third messages to the temporary public keys used to compute K. There are a number of other protocols proposed for authentication in mobile environments such as Park's protocol [8], Lin and Harn scheme [9], and Zhou and Lam scheme [10]. This paper presents a possible solution for authentication and key agreement using the combined scheme of secret and public technologies for security between user and network on wireless networks.

II. AUTHENTICATION AND KEY AGREEMENT PROTOCOL FOR SECURE END TO END COMMUNICATIONS ON MOBILE NETWORKS

In this section, we show security protocols which will be provided mutual authentication between user and network, key agreement and enciphering function between users for secure wireless mobile communications.

A. *Authentication Protocol based on count and nonce*

The following is the procedure of mutual authentication, key agreement, and enciphering function. There is three phases for security protocol such as initial phase, authentication and key agreement phase, and enciphering and communications phase. We assume that the authentication center and user have a reliable data of user such as user identity (ID), personal identification number (PIN), and basic parameters.

1) **Initial Phase:** The authentication center (AC) selects one way functions f1, f2, f3, large prime numbers p, q, n (= p x q), and primitive elements g of GF (p) and GF(q). The AC then determines integers e (encryption key) and d (decryption key), satisfying e (P, public key) x d (S, secret key) = 1 {mod ((p - 1) x (q - 1))}, with both e and d less than n.

Step 1: Each user of the communication facility needs to visit the authentication center for registration before he can communicate with other users secretly. User I will present his identity ID_i, PIN_i, and other personal data to the AC. Then AC computes SID_i for user I as SID_i (I=1,2,..) = $f1(PIN_i//ID_i//\text{Card No.}//\text{Registration Date})_i^{-d}$ (mod n), where SID_i^e x $(PIN_i//ID_i//\text{Card No.}//\text{Registration Date})_i$ (mod n) = 1, and prepares Pc (Public Key of authentication center).

Step 2: Then, the authentication center stores the set of parameters (f1, f2, f3, e(P), d(S), n, g, Pc, and random number generation algorithm, authentication algorithm, ciphering algorithm, C_i (initial counter), and others) in the subscriber smart card for user I and give him it. This is the same for user J and all users.

2) **Mutual Authentication and Key Agreement Phase between User I, Network and User J**

We use I -> AC: m to denote that I sends message (m) to AC (authentication center, network operator, or service provider). Let {m}k denote m encrypted with key k, and (m1/m2) denote concatenation. R1 and R2 are random numbers generated by user I and user J, respectively. R is random number generated by authentication center. Ps is secret key of authentication center (a pair with Pc for authentication center).

Step 1: User I -> AC: f3 $[\{(SID_i//R//\text{Time Stamp}//R)^{Si}\}^{Pc}//(R1^{Pj})]^{1/Ci}$//user J's phone digits.

Step 2: AC verifies user I using SID_i, R, and C_i, then AC -> User J: f3 $(R1^{Pj})$//paging.

Step 3: User J -> AC: f3 $[\{(SID_j//R//\text{time Stamp})^{Sj}\}^{Pc}//\{(R1//R2)^{Pi}\}]^{1/Cj}$, and AC verifies user J as SID_j, R, and C_j.

Step 4: AC -> User I/User J: $f2\{(R1//R2)^{Pi}//\text{Time Stamp}\}^{Ps}$) for user I, and $f2\{(R1//R2)^{PiPj}//\text{Time Stamp}\}^{Ps}$) for user J, respectively.

Step 5: User I and user J verifies AC using R1 and R2, respectively.

3) **Secure Communication Phase of User to Network for Relevant Data Confidentiality on Air Interface**

Step 1: User I and network make common session key using R1 (XOR) R.

Step 2: User I and network generate key stream using private key algorithm with common session key, and make bit wise exclusive OR-logic

(XOR) with key stream for ciphering of plain data bit.

Step 3: User I secretly communicate with network each other, and if there is some error and sync problem, then they start secure communications with first common session key for only the session. Next time, they will make other different session key for their secure communications using other R_i (XOR) R.

4) Secure Communication Phase of User I to User J

Step 1: User I and User J make common session key using R1 (XOR) R2.

Step 2: User I and User J generate key stream using private key algorithm with common session key, and make bit wise exclusive OR-logic (XOR) with key stream for ciphering of plain data bit.

Step 3: User I secretly communicate with User J each other, and if there is some error and sync problem, then they start secure communications with first common session key for only the session. Next time, they will make other different session key for their secure communications using other R_i (XOR) R_j.

The scheme is based on public key technique using counter for authentication and key agreement of users. Authentication of user I is based on $1/C_i$ and SID_i as SID_i (i =1,2,..) = f1 $(PIN_i//ID_i//\text{Registration Date})_i^{-d}$ (mod n), where SID_i^e x $(PIN_i//ID_i//\text{Card No.}//\text{Registration Date})_i$ (mod n) = 1. The network can also checks the right user by the random number (R) with gcd (R, n-1) = 1, R ∈ [1, n-1] which is generated by the authentication center. The common session key for secure communication between users on the mobile environments is based on combination of R1 and R2 which is generated by User I and User J. The security of the scheme is based on to solve the primes p and q from n as the computational difficulty of factoring large composite number n and to solve the decryption key (d) from SID_i = f1 $(PIN_i//ID_i//\text{Card No.}//\text{Registration Date})_i^{-d}$ mod n as discrete logarithm problem in GF(p) and GF(q). The authentication center has only p and q for all users and it is different from RSA (Rivest, Shamir, Adleman) scheme. The scheme also uses private key algorithm with session key R1 (XOR) R2 for ciphering between users. The use of time stamp and counter is for authentication and prevention from replay attack. The counter will be reset periodically for quarterly or yearly if needed from network.

B. Authentication Protocol based on $Y=f(.)^{1/ci}$

We also show secure end to end protocol based on public key scheme using the function $Y= f(.)^{1/ci}$, C_i is counter which is generated by the network, and f(.) is one way function. The following is the procedure of security protocol based on function $Y= f(.)^{1/ci}$ for authentication, key agreement, and enciphering function. There is three phases for security protocol such as initial phase, authentication and key agreement phase, and enciphering and communications phase. We also assume that all the clocks in the network are synchronized, the authentication center and user have a reliable data of user such as user identity (ID), personal identification number (PIN), and basic parameters. The initial phase, key agreement and authentication phase, and ciphering and communications phase are basically same except use the function $Y = f(.)^{1/ci}$ as follow.

1) **Initial Phase:** The authentication center (AC) selects one way functions f1, f2, f3, large prime numbers p, q, n (= p x q), and primitive elements g of GF (p) and GF(q). The AC then determines integers e (encryption key, Public Key (P)) and d (decryption key, Secret Key (S)), satisfying e x d = 1 {mod ((p - 1) x (q - 1))}, with both e and d less than n.

Step 1: Each user of the communication facility needs to visit the authentication center for registration before he can communicate with other users secretly. User I will present his identity ID_i and other personal data to the AC. Then AC computes SID_i for user I as SID_i (I=1,2,..) = f1(Card $No_i//ID_i//\text{Registration Date})_i^{-d}$ (mod n), where SID_i^e x (Card $No_i//ID_i//\text{Registration Date})_i$ (mod n) = 1, and generates R, where R is a random number R ∈ [1, n-1], with gcd (R, n-1) = 1.

Step 2: Then, the authentication center stores the set of parameters (f1, f2, f3, d, n, g, random number generation algorithm, counter, and others) in the subscriber smart card for user I and give him it. This is the same for user J and all users.

2) **Authentication and Key Agreement Phase:** We use I -> J: m to denote that I sends message (m) to J. Let {m}k denote m encrypted with key k, and (m1/m2) denote concatenation. R1 and R2 are random number generated by user I and user J, respectively.

Step 1: User I -> AC: f3 $\{(SID_i//Ci//\text{Time Stamp})^d//(R1^{Pj})\}^{1/Ci}$//user J's phone digits.

Step 2: AC verifies user I using SID_i, R, and C_i, then AC -> User J: f3 $(R1^{\text{Time Stamp}})$ //paging.

Step 3: User J -> AC: $\{f3\ (SID_j//R//\text{time Stamp})^d//(R1//R2)^{\text{Time Stamp}}\}^{1/cj}$, and AC verifies user J as SID_j, R, and C_j.

Step 4: AC -> User I: $f3(R1//R2)^{\text{Time Stamp}(Ci+1)}$, and AC -> User J: $f3(R2^{\text{Time Stamp }(Cj+1)})$.

Step 5: User I and user J verifies AC using R1 and R2, respectively.

3) **Enciphering and Secure Communications Phase**

Step 1: User I and User J make common session key using R1 (XOR) R2.

Step 2: User I and User J generate key stream using private key algorithm with common session key, and make bit wise exclusive OR-logic (XOR) with key stream for ciphering of plain data bit.

Step 3: User I secretly communicate with User J each other, and if there is some error and sync problem, then they start secure communications with first common session key for only the session. Next time, they will make other different session key for their secure communications using other R_i (XOR) R_j.

The scheme above using the function $Y = f(.)^{1/ci}$ is based on that user and the network already know counter value each other. The initial phase, authentication and key agreement phase, and enciphering and secure end to end communications between users are basically same. Our schemes have authentication function of user and the network, key agreement and enciphering functions between users for secure end to end communications.

III. CONCLUDING REMARKS

The communications between two mobile stations should be protected from both the outsiders (who can only accretion what can be intercepted via radio waves) and the insider (who obtain information by theft, conspiracy, or computer intrusion, or any method outside of scanning the radio link) of the mobile network, which means that a session key exchanged between them should not be exposed even to their home networks. We have considered security protocol for authentication required for users and the network, and key agreement required for users for secure end to end communications. The scheme is based on the public key technique using count, reverse value of count, and nonce for authentication and key agreement, and the private key algorithm for secure communications on two distinct mobile stations. This is also a range of possible solutions to authentication and key agreement problem in mobile network.

REFERENCES

[1] ETSI-GSM, "Technical Specification 03.20: Security Related Network Functions", Version 3.3.2, 1992.

[2] TIA/EIA/IS-95-A, "Mobile Station-Base Station Compatibility for Dual-Mode Wideband Spread Spectrum Cellular System", July 1993.

[3] M. Tatebayshi, N. Matsuzaki, and D. B. Newman, "Key Distribution Protocol for Digital Mobile Communication Systems", Proc. Of Crypto'89, August 1989.

[4] M.J. Beller, L.F. Chang, and Y. Yacobi, "Privacy and Authentication on a Portable Communication System", IEEE Journal on selected areas in Communications, pp.821-829, 1993.

[5] Klaus Vedder, "Security Aspects of mobile Communications", In computer Security and Industrial Cryptography - State of the art and Evolution, Springer-Verlag, pp193-210, May 1991.

[6] ITU-T Draft Recommendation Q.FIF, "Information Flows for IMT-2000 Ver.7.1", March 1997.

[7] P. L. Montgomery, "Modular Multiplication Algorithm using Lookahead Determination", IEICE Trans., Vol.7, No.1, pp.70-77, January 1993.

[8] C-S. Park, "On Certificate-based security protocols for wireless mobile communication systems", IEEE Network, September/October, pp.50-55, 1997.

[9] H.Y. Lin and L. Harn, "Authentication Protocols for Personal communication systems", Proc. Of ACM SIGCOMM'95, pp.256-261, August 1995.

[10] J. Zhou and K.Y. Lam, "Undeniable Billing in Mobile Communication, Preprint, 1998.