A New Authentication Scheme with Anonymity for Wireless Environments

Jianming Zhu and Jianfeng Ma, Member, IEEE

Abstract —*Wireless network is susceptible to security attacks because its openness of transmission media. Wireless network security is somewhat more concentrated and complex than that of wired network. Authentication is the most essential procedure to ensure that the service is properly used. But its limited resource, such as weak power supplies and limited bandwidth, must be taken into account in the design of security schemes. In this paper, we present a new and efficient wireless authentication protocol providing user anonymity. Our scheme is based on the hash function and smart cards, and mobile users only do symmetric encryption and decryption. In our protocol, it takes only one round of message exchange between the mobile user and the visited network, and one round of message exchange between the visited network and the corresponding home network. The most significant feature is one-time use of key between mobile user and visited network. Finally, the performance of our scheme is analyzed*[1].

Index Terms — Anonymity, authentication, security, wireless network.

I. INTRODUCTION

The network security is always an important issue. Because wireless is broadcast in nature, anyone within range of a wireless device can intercept the packets being sent out without interrupting the flow of data between wireless device and base station. It is because of this that wireless network security is somewhat more concentrated than that of wired networks. Wireless communication suffers from threats inherited from wired networks and those that are specific in the wireless environment. But because of its limited resource and a higher channel error rate than wired networks, those security schemes in wired network couldn't be used directly in wireless environment. So, the security protocols in wireless network should be designed to minimize the message sizes and the number of messages exchanged.

The security features for mobile communication system include: confidentiality on the air interface, anonymity of the user and, most importantly, authentication of the user to the network in order to prevent fraudulent use of the system [1]. For the lack of a physical association between the mobile nodes (MNs) and the wired network and easy access to the radio, proper authentication is necessary to protect the communication against illegal usage and to ensure that users are connected to the network that he trusts. To provide universal wireless access to services, such authentication must deal with users' roaming among areas administered by different network operators (NOs), and be implemented by users' devices with limited computing resources. During the authentication process, some secret information must be mutually agreed upon so the following communication can proceed efficiently in protected mode to achieve desired confidentiality.

In this paper, we present a simple authentication protocol providing user anonymity for wireless environments. The remainder of the paper is organized as follows: in Section 2, we review previous authentication protocols for wireless environments. A simple and efficient wireless authentication protocol is presented in Section 3. In section 4, we analyze the performances of our protocol and compare our protocol with others. Finally, a concluding remark is given in Section 5.

II. REVIEW OF PREVIOUS WORKS

In recent years, many authentication protocols for the wireless network have been proposed [1]-[7]. When a mobile user roaming in wireless environment, it is desirable to protect the relevant information about him. Assuring the anonymity of a mobile user prevents unintended parties from associating him with the messages to/from him or with the sessions in which he participates. The disclosure of a mobile user's identity allows unauthorized entities to track his moving history and current location. The illegal access to any information related to users location without his notice can be a serious violation of his privacy. So, anonymity is one of importance property of these protocols.

A basic solution for the provision of user anonymity is to use the temporary identity (TID) of a mobile user instead of his real one. Several security-related protocols with anonymity for wireless mobile communication systems have been proposed based on the symmetric key cryptography or the public key cryptography [1]-[7]. However, in a mobile communication system, there are a few things to consider when security protocols are being designed. First, the low computational power of mobile devices should be considered, which means a security protocol requiring heavy computation on the mobile nodes is not adequate. Secondly, wireless mobile communication networks have a lower bandwidth and a higher channel error rate than wired networks. So, the security protocols should be designed to minimize the message sizes and the number of messages exchanged. Our proposed authentication scheme is based on the public key cryptosystems, but mobile users only do symmetric encryption and decryption. In our protocol, it takes only one round of message exchange between the mobile user and the visited

[1] This work was supported by the National High Technology Research and Development Program (863 Project) under Grant No. 2002AA143021.

ZHU Jianming and MA Jianfeng are with the School of Computer Xidian University, Xi'an 710071, P.R.China. (e-mail: tyzjm65@ 163.com).

Contributed Paper
Original manuscript received September 24, 2003
Revised manuscript received November 20, 2003

network, and one round of message exchange between the visited network and the corresponding home network. The most significant feature is one-time use of key between mobile user and visited network.

III. PROPOSED AUTHENTICATION PROTOCOL

In this section, we propose a simple and efficient authentication protocol with anonymity for wireless environment.

A. The Model

In wireless environments, MN indicates mobile user, HA indicates home agent of a mobile user MN, and FA indicates foreign agent of the network that a mobile user MN wants to visit. A simplified model is shown in Fig. 1, in which f indicates a fixed node, HA and FA indicate a mobile agent, respectively. R indicates a router. In our protocol, MN wants to directly communicate with FA. FA is responsible for authenticating MN by HA.

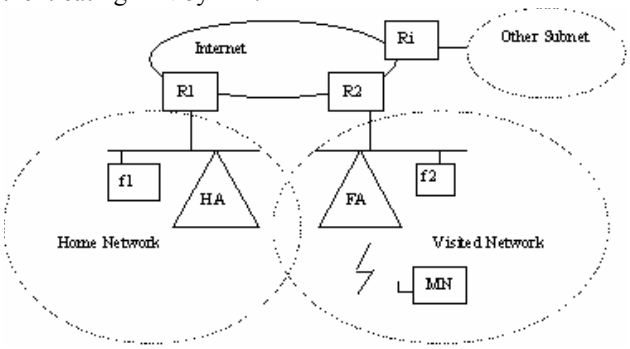

Fig. 1. The model of wireless environments

B. Protocol goals

We will consider the security goals that may be achieved after the successful run of the wireless authentication protocol. They include the following:

- mutual authentication of mobile user and visited network
- mutual agreement of shared secret key
- mutual implicit key authentication
- assurance of session key freshness
- non-repudiation of origin for relevant user data
- confidentiality of relevant data
- user anonymity as a data origin and destination

As well as these requirements, another factor in design of authentication protocol for the wireless environment is the limited resource of the mobile devices.

C. Notations

We use the following notations:

T_A	Timestamp generated by an entity A
$Cert_A$	Certificate of an entity A
$(X)_K$	Encryption of a message X using a symmetric key K
$E_K(X)$	Encryption of a message X using an asymmetric key K
h(X)	a one-way hash function
p	a large prime
q	a large prime such that $q \mid p$ -1
$g \in Z_p^*$	an element of Z_p^* of order q

D. Initial Assumptions

We assume a protocol environments of wireless mobile system in which the proposed authentication protocol is executed. In this paper, we assume that we have a network in which centralized PKI or KDC (Key Distribution Center) is available. In our network, both HA and FA possess X.509 public key certificates issued by hierarchies of certification authorities (CAs).

A certificate defined in X.509 contains the user's public key and other information and a signature of this information by CA. For example, the equations below are certificates.

$$Cert_A = \{ID_A, KU_A, Date_A, LF_A, E_{KR_{CA}}(ID_A, KU_A, Date_A, LF_A)\}$$

Where $Cert_A$ represents the certificate of entity A, in which ID_A means the identity of entity A, KU_A is the public key of entity A, KR_{CA} is the private key of entity CA, $Date_A$ is the issue date of the certificate to A, and LF_A is the lifetime. These data are signed by CA using its private key KR_{CA}.

On the other hand, the HA picks up an m -bits random number N and keeps it secretly. Note that in order to prevent the exhaustive search attack, m should be sufficiently large, e.g. m 100. When a new user MN wants to register at his HA, he submits his identity ID_{MN} to the HA. The HA computes a password PW_{MN} for this user as follows:

$$PW_{MN} = h(N \,||\, ID_{MN}).$$

The HA delivers PW_{MN} to this user through a secure channel.

The HA issues a smart card for the user, which contains r, ID_{HA} and a hash function h, where ID_{HA} is the HA's identity, h is a strong one-way function, r is as follows:

$$r = h(N \,||\, ID_{HA}) \oplus h(N \,||\, ID_{MN}) \oplus ID_{HA} \oplus ID_{MN} \quad (1)$$

where " $\oplus$ " indicates the bit-wise XOR operation, "||" is concatenation.

E. Design of Authentication Protocol

In this section, we propose a simple and efficient wireless authentication scheme with user anonymity. The protocol has two phases: in the first phase, FA authenticates to MN and establishes a session key; in the second phase, MN visits FA and FA serves for MN. We now describe our scheme.

1) The first phase

In this phase, FA authenticates MN each other through HA. If MN is a legal user of HA, FA will issue a temporary certificate $TCert_{MN}$ to MN, which will be used in second phase when MN communicates with FA. Fig. 2 shows the authentication process.

Step1 MN → VA

When a mobile user MN enters a new foreign network FA, he sends a request by the radio channel and begins a registration process with FA to identify himself to be a legal subscriber of his home network HA. MN keys password PW_{MN} to the device, then the device generates a secret random number x_0 automatic and save it secretly, where $x_0 \in [1,...,q-1]$. MN Computes $n = r \oplus PW_{MN}$ and generates its timestamp T_{MN} and his temporary key $L = h(T_{MN} \oplus PW_{MN})$, and then encrypts x_0 with the key L using a symmetric encrypt algorithm. Finally, MN sends n, $(x_0)_L$, T_{MN} and his home network identity ID_{HA} to FA .

Step 2 FA → HA

After receiving the message from user MN, FA decides if the timestamp T_{MN} is within some allowable range compared with its current time. If the decision is positive, FA generates a secret random number b , and then computes its signature using his private key KR_{FA} , i.e. $E_{KR_{FA}}(h(b,n,(x_0)_L,T_{MN},Cert_{FA}))$. FA generates its timestamp T_{FA} and sends b , n , $(x_0)_L$, T_{MN} , signature, T_{FA} and $Cert_{FA}$ to HA.

Step3 HA→FA

Receiving the message from FA, HA decides if the certificate $Cert_V$ is valid and the timestamp T_{FA} is within some allowable range compared with its current time. If it is not valid, HA terminates the execution. Otherwise, HA computes as follows and gets the MN's real identity

$$h(N \| ID_{HA}) \oplus n \oplus ID_{HA} = ID_{MN}. \qquad (2)$$

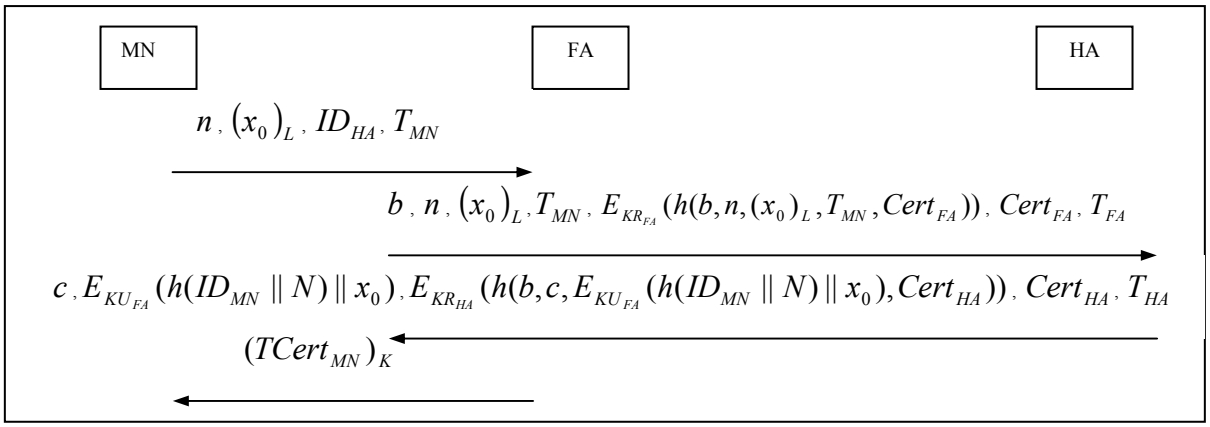

Fig. 2. The protocol of the first phase

Then, HA verifies if the MN is a legal user. If verification is not true, HA sends the message "This user is a illegal user." Otherwise, HA identifies MN to be a legal user and then do as follows:

- HA computes $L = h(T_{MN} \oplus h(N \| ID_{MN}))$ and decrypts the message $(x_0)_L$ to get x_0 .
- HA generates a secret random number c .
- HA encrypts $h(ID_{MN})$ and x_0 with the public key of FA and computes its signature using his private key KR_{HA}, i.e. $E_{KR_{HA}}(h(b,c,E_{KU_{FA}}(h(ID_{MN}) \| x_0),Cert_{HA}))$.
- HA generates its timestamp T_{HA} .

Finally, HA sends c , $E_{KU_{FA}}(h(ID_{MN}) \| x_0)$, signature, T_{HA} and $Cert_{HA}$ to FA .

Step4 FA → MN

After receiving the message from HA, FA decides if the certificate $Cert_H$ is valid and the timestamp T_{HA} is within some allowable range compared with its current time. If it is not valid, FA terminates the execution. Otherwise, FA has known that MN is a legal user. FA issues to MN the temporary certificate $TCert_{MN}$, which includes lifetime and other information. Then, FA computes $k = h(ID_{MN}) \oplus x_0$ and symmetrically encrypts the $TCert_{MN}$ with the secret key k . Finally, FA saves $h(ID_{MN})$ and x_0 , then sends $(TCert_{MN})_K$ to MN. So far, FA has finished the process of authentication to MN and established session keys.

After receiving the message from FA, MN computes $k = h(ID_M) \oplus x_0$ and decrypts $(TCert_{MN})_K$ to get $TCert_{MN}$.

2) The second phase

When MN visits FA at ith session, M sends the follows message to FA:

MN → FA:

$$TCert_{MN}, (x_i \| TCert_{MN} \| OtherInfomation)_{k_i}$$

Where $k_i = h(ID_M) \oplus x_{i-1}$, $i = 1, \cdots, n$. Firstly, FA checks if the certificate $TCert_{MN}$ is valid. If it is not valid, FA terminates the execution. Otherwise, FA computes k_i and decrypts $(x_i \,||\, TCert_{MN} \,||\, OtherInfomation)_{k_i}$ with k_i to get $x_i \,||\, TCert_{MN} \,||\, OtherInfomation$. FA can compare the two $TCert_{MN}$ and verifies the integrity of the information. FA saves x_i in order to compute next session key and provides service for MN. Because x_i can be computed only by the MN who generated it, k_i plays a role of one-time key to access the visited network.

IV. Performance Analysis

We evaluate our proposal with respect to protocol goals considered in the beginning of the protocol design. Concerning the protocol goals required in wireless authentication protocol, our scheme satisfies the goals as has been presented.

A. Security

In the first phase of our protocol, its security is based on the hash function and smart cards. When HA authenticates FA each other, we use the public key encryption algorithm, whose security is based on the difficult problem of disperse logarithm.

In step 1, MN computes temporary key L using hash function and smart cards. The security of hash and the privacy of the big number N assure the unforgability of r, n and L. The temporary key L contains timestamp, which ensures its freshness.

In step 2, for verifying whether MN is legal user, FA forwards the information containing the request information of MN and the certificate of FA. The signature over the hashed value of message provides the implicit entity authentication. The hash operation assures the integrity of information and random number b can prevent from replay attack.

In step 3, HA assures the freshness of information using random number and prevent from replay attack using the timestamp.

In step 4, FA trusts MN because FA trusts HA. On the other hand, MN trusts FA because MN trusts HA. The trust relation between MN and FA is established through HA.

In the second phase, the MN can prove himself by presenting $TCert_{MN}$ to FA. Because x_i can be computed only by the MN who generated it, k_i plays a role of one-time ticket to access the visited network.

B. Anonymity and Untraceability

In our protocol, the anonymity of MN is obtained by hash function and smart cards. MN hides his real identity in (1). Only HA can get the real identity of MN using (2) because HA knows the secret number N.

If user certificate is used several times in the protocol, the user may be traced. So, we use one-time key and a temporary certificate when MN communicates with FA in our protocol to get the untraceability.

C. Implementation Requirements

Because of the considerations about hardware complexity, battery power, and computation delay, some mobile units, e.g., pocket cellular telephones, cannot perform complicated operations that require expensive hardware or are time-consuming. So, we consider a computational load on user part of the proposed scheme. Our scheme is based on the public key cryptosystems, but mobile users only do symmetric encryption and decryption. In our protocol, it takes only one round of message exchange between the mobile user and the visited network, and one round of message exchange between the visited network and the corresponding home network. The most significant computation required on the user part is the operation of symmetric encryption. By avoiding employing public key cryptography on the user part, we keep the computation cost down on user part.

We compare our scheme with the previous protocols [1], [3]. Table 1 shows our protocol is much more practical and efficient in terms of communication and computation cost, because both of the XOR operations and concatenation can be done very efficiently compared to multiplication with the same length of operands.

TABLE 1 COMPARISON BETWEEN PROTOCOLS AT USER

	ASPeCT[1]	GoKim[3]	Proposed Protocol
The number of exponential operation	2	2	0
The number of hash operation	1	4	2
The number of symmetric encryption/decryption	2	4	2
The number of asymmetric encryption/decryption	0	0	0
The number of exchange information at user	2	3	1

V. Conclusion

In wireless mobile communication system, user anonymity and user authentication have been addressed. The advantage of our proposed authenticating mobile users protocol is simple and efficient. The security of the proposed scheme relies on the two assumptions: tamper-proof devices and the security of the one-way scheme. Our scheme is based on the public key cryptosystems, but mobile users only do symmetric encryption and decryption. In our protocol, it takes only one round of message exchange between the mobile user and the visited network, and one round of message exchange between the visited network and the corresponding home network. The most significant feature is one-time use of key between mobile user and visited network.

REFERENCES

[1] Horn G., Preneel B., "Authentication and Payment in Future Mobile Systems." ComputerSecurity - ESORICS'98, Lecture Notes in Computer Science, 1485, 1998, pp. 277-293.

[2] M.G.Rahman, H.Imai. "Security in wireless communication." Wireless Personal Communications. Vol.22, No.2, August 2002, pp.213-228

[3] Jaeseung Go, Kwangjo Kim. "Wireless Authentication Protocol Preserving User Anonymity." SCIS 2001, Japan, January 23-26, 2001

[4] Z.J.TZENG, W.G.TZENG. "Authentication of Mobile Users in Third Generation Mobile System." Wireless Personal Communicatons, pp35-50, Vol 16,2001

[5] D. Alevras, M. Grotschel, P. Jonas, U. Paul, and R.Wessaly, "Survivable Mobile Phone Network Architectures: Models and Solution Methods," IEEE Comm. Mag., pp.88-93, March, 1998.

[6] M.-F. Chang, Y.-B. Lin, and S.-C. Su, "Improving the Fault Tolerance of GSM Networks," IEEE Network, pp. 58-63, Jan./Feb., 1998.

[7] P. Krishnamurthy and J. Kabara, "Security architecture for wireless residential networks", Proc. VTC'2000, Boston, MA, September 2000.

ZHU Jianming received the B. S. in Mathematics from Huaibei Coal & Normal College , Huaibei, Anhui, China in 1985, and obtained his M. E. degree in computer and its application from Taiyuan University of Technology, Taiyuan, Shanxi, China in 1998. Since 1989 he has been with Shanxi Finance & Taxes College (Taiyuan) as a lecturer, associate professor. Currently, he is pursuing his Ph.D. degree in Computers with Their Applications at Xidian University, Xi'an, Shaanxi, China. His research interests include Information security, Cryptography and E-commerce.

MA Jianfeng received his B. S. degree in mathematics from Shaaxi Normal University (Xi'an) in 1985, and obtained his M. E. and Ph. D. degrees in computer software and communications engineering from Xidian University (Xi'an) in 1988 and 1995 respectively. Since 1995 he has been with Xidian University as a lecturer, associate professor and professor. He is also a supervisor of Ph. D students in "Cryptography" and "Computers with Their Applications" at the university. From 1999 to 2001, he was with Nanyang Technological University of Singapore as a research fellow. He is an IEEE member and a senior member of Chinese Institute of Electronics (CIE). His research interests include information security, coding theory and network management.