Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/081L14

Enhancing An AAA Scheme using ID-based Tickets with Anonymity in Future Mobile Communication

Chin-Ling Chen[1,*], *Kai-Wen Cheng*[1], *Chih-Cheng Chen*[2] *and Ing-Chau Chang*[3]

[1] IDepartment of Computer Science and Information Engineering, Chaoyang University, 168 Jifeng E. Road, Wufeng District, Taichung, 41349, Taiwan, R.O.C.
[2] Department of Mechatronics Engineering National Changhua University of Education, Changhua 50007, Taiwan, R.O.C.
[3] Department of Computer Science and Information Engineering, National Changhua University of Education, Changhua 50007, Taiwan, R.O.C.

Received: 20 Apr. 2013, Revised: 15 Aug. 2013, Accepted: 16 Aug. 2013
Published online: 1 Apr. 2014

Abstract: In 2011, Moon and Lee proposed an AAA scheme using ID-based tickets with anonymity in future mobile communication in order to provide a ubiquitous communication environment. However, there are some security loopholes that need to be addressed. When malicious attackers steal a mobile device, they can utilize the mobile's information to access resources or request services. We therefore propose a novel scheme to improve mobile communication protocol to ensure communication security. The proposed scheme achieves low computation, and resists known attacks. The mobile user need not worry about his or her sensitive information being revealed or stolen by malicious attackers.

Keywords: AAA, mutual authentication, lost mobile device attack, networks

1 Introduction

With the rapid growth of mobile communication technology, mobile users can access Internet services via an open network environment. Therefore, a means of ensuring communication security has become an important issue in such a distributed environment. Mutual authentication and key agreement become important methods for communication. Password authentication is a widely used mechanism for authenticating a legitimate user. If a mobile user wants to access the service from a service provider or server, they must pass the authentication process. In traditional password authentication mechanisms [1,2,3,4,5,6,7,8,9,10], the server side always maintains a verification table, which contains the mobile user's identity and password. If the verification table is stolen or modified by malicious attackers, the communication system will be compromised.

Recently, several researches [11,12,13,14,15,16,17,18,19] have proposed approaches for accessing resources in multi-server environments. These protocols can be divided into two types, hash based authentication, and public key based authentication. In 2001, Tsaur et al. [12] proposed a remote user authentication scheme based on RSA cryptosystem and Lagrange interpolating polynomial, for multi-server environments. Lin et al. [13] then proposed a new efficient remote user authentication scheme based on the simple Euclidean geometric properties. In 2011, Moon and Lee [20] proposed an AAA (Authentication, Authorization, Accounting) scheme using ID-based tickets with anonymity, for future mobile communication. Moon and Lee used a pre-shared key and digital signature to propose a communication protocol. However, Moon and Lee's scheme does not protect the mobile user's information, so malicious attackers can successfully attack the communication system, or steal sensitive information. We, therefore, improve Moon and Lee's scheme such that the proposed protocol is more secure, and the attacker cannot take advantage of any security loopholes to attack the communication system, or steal sensitive information belonging to the mobile user.

Our scheme enhances communication security, and precludes the impersonation of the legal mobile user by malicious attackers. In addition, when the mobile user receives a message from the home Authentication,

* Corresponding author e-mail: clc@mail.cyut.edu.tw

Authorization, Accounting server (AAAH) or service provider, the mobile user can perform mutual authentication to detect if the sender is legal. On the other hand, the AAAH or service provider can also verify whether the mobile user is legal. The common architecture for the communication system is shown in Figure 1.

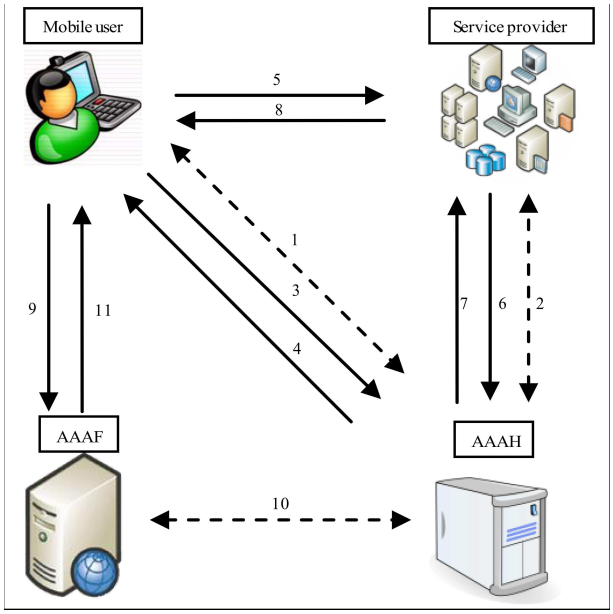

Figure 1: The scenario of the future mobile environment

The scenario of the mobile communication environment is described as follows:
(1) Mobile user: The mobile user can use the mobile device to access services in a roaming environment.
(2) AAAH: The AAAH server verifies the user's identity, and issues the certificate for the legal user as an authorization certificate.
(3) Service provider: The service provider offers a variety of services for legal mobile users.
(4) AAAF: When the mobile user is roaming in foreign network, the foreign Authentication, Authorization, Accounting server (AAAF) will verify the user's identity, and communicate with the AAAH.
Step 1: Mobile user to AAAH: The mobile user sends the registration messages to the AAAH server. The AAAH computes the registration information and stores it in its database. Finally, the AAAH server sends the registration information to the mobile user.
Step 2: Service provider to AAAH: The service provider submits the registration messages to the AAAH server. The AAAH then issues the secret key for the service provider.
Step 3: Mobile user to AAAH: The mobile user sends the authentication message to the AAAH.
Step 4: AAAH to Mobile user: After receiving the authentication message, the AAAH verifies it, and then issues the authorization certificate to the mobile user.
Step 5: Mobile user to Service provider: When the mobile user wants to request a service, she transmits the request service message and authorization certificate to the service provider.
Step 6: Service provider to AAAH: When the request service message is received, the service provider sends the authentication message to the AAAH.
Step 7: AAAH to Service provider: After verifying the service provider's legality, the AAAH transmits the mobile user's information to service provider.
Step 8: Service provider to Mobile user: When the authentication process is passed, the service provider offers the service to the mobile user.
Step 9: Mobile user to AAAF: When the mobile user wants to renew the authorization certificate in a foreign network, she submits the request message to the AAAF.
Step 10: AAAF to AAAH: Once the mobile user passes the authentication process, the AAAF delivers the user information to AAAH via a secure channel. The AAAH generates a new certificate, and sends it back to the AAAF.
Step 11: AAAF to Mobile user: Finally, the AAAF forwards the certificate to the mobile user.

Reviewing Moon and Lee's scheme, the communication system consists of the mobile device, the AAA server, and the service provider, which together make up a mobile communication environment. In order to achieve more efficient and more secure communication for the communication environment, we list the following requirements:
(1) Mutual authentication: In order to ensure security between the sender and receiver, mutual authentication is crucial. Mutual authentication can prevent known attacks [9,16].
(2) Confidential communication: In the open network, the transmitted data is vulnerable to eavesdropping attacks. Therefore, the communication system must ensure communication security between the sender and receiver [5,6,20].
(3) Anonymity: The mobile communication must guarantee the mobile user's privacy. Thus, the means of protecting the mobile user's real identity and related information becomes an important issue [3,4,6,9,20].
(4) Low computation: The mobile communication environment is constructed by mobile device and other participates. Thus, the protocol must have a low computation, such that it is suitable for a mobile device [2,9].
(5) Integrity: The communication message may be deleted, modified, or forged by malicious attackers in an insecure network. Therefore, the communication system must ensure that the authorization certificate cannot be modified or forged [2,5,20].
(6) Session independence: Malicious attackers may

intercept the session key in order to obtain private information from the server or user. To guarantee the security of the communication system, the session key must have a one-time use only. In this way, even if the attacker intercepts the session key, the system security remains unaffected [9,16].
The rest of this paper is organized as follows: In Section 2, we points out Moon and Lee's weaknesses. Our proposed scheme is described in Section 3. In Section 4, the property analysis, and security analysis are presented. We then discuss the performance, and compare with related works in Section 5. Our conclusions are presented in Section 6.

2 The Weaknesses of Moon and Lee's scheme

Moon and Lee's scheme has some security loopholes which can be exploited in order to attack the communication system or impersonate legal users to access the service. Three such loopholes are:
1. When a mobile user loses his or her mobile device, a malicious attacker can use the mobile device to attack the communication system, or impersonate the legal mobile user to access the service. This is because the session key $SK = PW_i \oplus AT \oplus X_i \oplus Y_i$ and ticket $Ticket = (ID_{AAAH}, Sign_{AAAH}[ID_{U_{Anony}}, Lifetime, h(X_i||Y_i)])$are stored in the mobile device. Malicious attackers can use the mobile device to send the request service message to the service provider. The service provider only verifies the secret value, $h(X_i||Y_i)$. In this way, malicious attackers can impersonate legal users to access services [21,22].
2. In Moon and Lee's scheme, the mobile device needs to compute a lot of exponent operations and asymmetric key encryption. This is not suitable for mobile devices [2,9].
3. In Moon and Lee's scheme, the symmetric key KS_{U-AAAF}does not update in each transaction between mobile users and the AAAF. If the malicious attackers hold the key, they can use symmetric key $KS_{U-AAAF}$to decrypt the transmitted message $E_{KS_{U-AAAF}}[ID_i, OTP, AT, Ticket]$, and in this way obtain sensitive information $(ID_i, OTP, AT, Ticket)$belonging to the mobile user. Malicious attackers can use $(ID_i, OTP, AT, Ticket)$ to impersonate a legal user. Thus, Moon and Lee's scheme doesn't achieve known key security [23,24].

In this paper, we improve on Moon and Lee's scheme to achieve more secure and less resource intensive communication. In our scheme, the mobile user applies mutual authentication in the communication system, which ensures secure communication. The mobile device does not store any sensitive information, precluding attacks from lost mobile devices. Our scheme can therefore protect the mobile user's privacy, and reduce demands placed on the communication system.

3 Our scheme

3.1 Notation

MU :the mobile user
$AAAH$:the home AAA server
$AAAF$:the foreign AAA server
SP :the service provider
ID_i :the identity of the ith mobile user
PW_i :the password of the ith mobile user
$ID_{U_{Anony}}$:the anonymous identity of the mobile user
$S_i, H_i, X_i, Y_i, A_i, F_i, G_i$:the authenticate parameter (i=1, 2,n)
OTP, OTP_{new}:the old and new one-time password, respectively
AT, AT_{new}:the old and new authentication time, respectively
M_{req} :the request message of renew certificate
$Sign_*$: the signature of *
KU_*, KR_*:the public and private keys of *, respectively
$Lifetime$: the lifetime of ticket or certificate
$Cert$: tthe authorization certificate
$nonce_x$: the nonce generated by x
KS_{U-*} : the shared symmetric key between mobile user and *
SK_{U-*} : the shared session key between mobile user and *
$E_*[]$: the encryption with key of *
$h(.)$: a one-way hash function
$A? = B$:check if A is equal to B
$\oplus$:the XOR operation

3.2 Registration phase

In this phase, we discuss the registration scenario in two parts. In Class 1, the mobile user registers with the AAAH to be a legal user. In Class 2, the service provider registers with the AAAH to be a legal provider.
Class 1 The mobile user registers to AAAH
Step 1:The mobile user selects the identity ID_i and password PW_i , then the mobile device computes:

$$A_i = h(ID_i||PW_i) \quad (1)$$

$$X_i = h(A_i||PW_i) \quad (2)$$

After this, the mobile device sends the registration information A_i to the AAAH via secure channel.
Step 2:Upon receiving the registration information, the AAAH uses secret value Y_i and private key x to compute parameters F_i and G_i :

$$F_i = A_i \oplus h(Y_i) \quad (3)$$

$$G_i = h(Y_i||x) \oplus F_i \quad (4)$$

and then the AAAH generates a nonce $nonce_i$ to compute temporary identity T_{ID} for the mobile user:

$$T_{ID} = h(A_i||x||nonce_i) \quad (5)$$

Finally, the AAAH sends the parameter F_i and temporary identity T_{ID} to the mobile user.
Class 2 The service provider registers to AAAH
Step 1:The service provider sends the identity ID_{SP} to the AAAH via secure channel.
Step 2:On receiving the message, the AAAH computes parameter P_i using private key x and secret value Y_i :

$$P_i = h(ID_{SP}||Y_i) \oplus h(x) \tag{6}$$

The AAAH then sends the parameter P_i to the service provider.

3.3 Authentication and certificate issues phase

When the mobile user wants to access the service, she needs to go through the verification procedures. In this phase, the mobile user and the AAAH should process mutual authentication to identify their identities. After completing the authentication procedure, the AAAH issues the certificate to the mobile user.
Step 1:The mobile user enters her identity ID_i and password PW_i to the mobile device. The mobile device then computes:

$$A_i = h(ID_i||PW_i) \tag{7}$$

$$X_i' = h(A_i||PW_i) \tag{8}$$

After completing the above step, the mobile device checks whether the parameter X_i' is the same as X_i :

$$X_i'? = X_i \tag{9}$$

If the above equation holds, the mobile device computes the following parameters:

$$h(Y_i) = F_i \oplus A_i \tag{10}$$

$$C_1 = h(A_i \oplus T_{ID}) \tag{11}$$

$$KEY = h(C_1||h(Y_i)) \tag{12}$$

$$C_2 = h(KEY||T_{ID}) \tag{13}$$

The mobile device then sends the verification message (T_{ID}, C_2) to the AAAH.
Step 2:On receiving the verification message form mobile user, the AAAH utilizes the temporary identity T_{ID} to find the corresponding information of the mobile user, and computes:

$$F_i' = h(Y_i||x) \oplus G_i \tag{14}$$

$$A_i' = F_i' \oplus h(Y_i) \tag{15}$$

$$C_1' = h(A_i' \oplus T_{ID}) \tag{16}$$

$$KEY' = h(C_1'||h(Y_i)) \tag{17}$$

After computing the parameters C_1' and KEY',the AAAH computes the ciphertext C_2' , and checks whether the ciphertext is the same as C_2 :

$$C_2' = h(KEY'||T_{ID}) \tag{18}$$

$$C_2'? = C_2 \tag{19}$$

If the above equation holds, then the verification message and mobile users are valid; otherwise the AAAH terminates this section.
When the mobile user passes the authentication process, the AAAH generates a new nonce , $nonce_i$ and updates the new temporary identity T_{IDnew} of the mobile user for the next verification:

$$T_{IDnew} = h(A_i||x||nonce_i) \tag{20}$$

$$C_3 = h(KEY'||T_{IDnew}) \tag{21}$$

The AAAH then issues a certificate to mobile user. The certificate includes the signature of the AAAH, the certificate's lifetime ,$Lifetime$ and ciphertext C_3:

$$Sig_1 = Sign_{AAAH}[T_{IDnew}, Lifetime, C_3] \tag{22}$$

$$Cert = (ID_{AAAH}, Sig_1) \tag{23}$$

The AAAH also computes the session key SK_{U-AAAH} as follows:

$$SK_{U-AAAH} = h(T_{ID}||ID_{AAAH}||C_1'||C_2') \tag{24}$$

Finally, the AAAH utilizes the session key to encrypt a new temporary identity ,T_{IDnew} and the certificate $Cert$.

$$C_4 = E_{SK_{U-AAAH}}[T_{IDnew}, Cert] \tag{25}$$

The AAAH then sends ciphertext C_4 to the mobile user.
Step 3:Once the verification messages are received, the mobile device computes the session key, and decrypts the messages:

$$SK_{U-AAAH}' = h(T_{ID}||ID_{AAAH}||C_1||C_2) \tag{26}$$

$$(T_{IDnew}, Cert) = D_{SK_{U-AAAH}}[C_4] \tag{27}$$

The mobile device then computes parameter C_3' to authenticate the AAAH:

$$C_3' = h(KEY'||T_{IDnew}) \tag{28}$$

$$C_3'? = C_3 \tag{29}$$

If the above equation holds, then the AAAH is valid; otherwise the mobile device terminates this transaction.
Finally, the mobile user updates the temporary identity T_{IDnew} for the next authentication.

3.4 Service request phase

When the mobile user wants to request a service, he must pass the authentication phase. The mobile user submits his information and certificate to the service provider. If the mobile user is legal, the service provider only offers the related service to the mobile user.
Step 1:The mobile user enters her identity ID_i and password PW_i to the mobile device. The mobile device then computes:

$$A_i = h(ID_i||PW_i) \tag{30}$$

$$X_i' = h(A_i||PW_i) \tag{31}$$

After completing the above step, the mobile device checks whether the parameter X_i' is the same as X_i :

$$X_i'? = X_i \tag{32}$$

If the above holds, the mobile device computes the request service message:

$$h(Y_i) = F_i \oplus A_i \tag{33}$$

$$C_5 = h(A_i \oplus T_{IDnew}) \tag{34}$$

$$KEY_{U-SP} = h(T_{IDnew}||ID_{SP}||C_5) \tag{35}$$

$$C_6 = h(A_i||KEY_{U-SP}) \tag{36}$$

and then sends the message (T_{IDnew}, C_6) to the service provider.
Step 2:Upon receiving message, the service provider generates nonce , $nonce_i$and computes parameter K :

$$K = h(ID_{SP}||P_i||nonce_{SP}) \tag{37}$$

The service provider sends the ID_{SP}, the mobile user's temporary identity ,T_{IDnew} nonce ,$nonce_{SP}$ and parameter K to the AAAH.
Step 3:After receiving the information from service provider, the AAAH checks whether the service provider is valid or not:

$$P_i' = h(ID_{SP}||Y_i) \oplus h(x) \tag{38}$$

$$K = h(ID_{SP}||P_i'||nonce_{SP}) \tag{39}$$

$$K'? = K \tag{40}$$

If holds, the AAAH uses the temporary identity ,T_{IDnew} to find the mobile user's information in the database.

$$F_i' = h(Y_i||x) \oplus G_i \tag{41}$$

$$A_i' = F_i' \oplus h(Y_i) \tag{42}$$

After this, the AAAH generates nonce , $nonce_{AAAH}$and computes authentication information Q_i for the service provider.

$$Q_i = h(P_i'||nonce_{AAAH}) \tag{43}$$

The AAAH generates a new temporary identity T_{IDnew}' for the mobile user for the next verification:

$$T_{IDnew}' = h(A_i'||x||nonce_i) \tag{44}$$

Finally, the AAAH uses a secret value to encrypt the message $(h(Y_i), A_i', Cert, Q_i, nonce_{AAAH}, T_{IDnew}')$

$$w = E_{P_i'}[h(Y_i), A_i', Cert, Q_i, nonce_{AAAH}, T_{IDnew}'] \tag{45}$$

and sends w to the service provider.
Step 4:Once the messages are received, the service provider decrypts the messages to obtain the mobile user's information.

$$(h(Y_i), A_i', Cert, Q_i, nonce_{AAAH}, T_{IDnew}') = D_{P_i'}[w] \tag{46}$$

$$Q_i' = h(P_i||nonce_{AAAH}) \tag{47}$$

$$Q_i? = Q_i \tag{48}$$

If the above equation holds, then the AAAH is valid. The service provider then computes the following information to verify the mobile user:

$$C_5' = h(A_i' \oplus T_{IDnew}) \tag{49}$$

$$KEY_{U-SP}' = h(T_{IDnew}||ID_{SP}||C_5') \tag{50}$$

$$C_6' = h(A_i||KEY_{U-SP}') \tag{51}$$

$$C_6'? = C_6 \tag{52}$$

If the above equation holds, the service provider constructs the session key SK_{U-SP} between the mobile user and the service provider, and then uses key KEY_{U-SP}' to encrypt the session key SK_{U-SP} .

$$SK_{U-SP} = h(T_{IDnew}||ID_{SP}||KEY_{U-SP}'||C_6) \tag{53}$$

$$C_7 = E_{KEY_{U-SP'}}[SK_{U-SP}] \tag{54}$$

Finally, the service provider sends C_7 to the mobile user.
Step 5:Upon receiving the messages from service

provider, the mobile device decrypts the messages, and checks whether or not the messages are valid.

$$(SK_{U-SP}) = D_{KEY_{U-SP}}[C_7] \tag{55}$$

$$SK'_{U-SP} = h(T_{IDnew}||ID_{SP}||KEY_{U-SP}||C_6) \tag{56}$$

$$SK'_{U-SP}? = SK_{U-SP} \tag{57}$$

If the above equation holds, the mobile user uses the session key SK'_{U-SP} to encrypt the certificate and service type $Service-type$.

$$C_8 = E_{SK'_{U-SP}}[Cert, Service-type] \tag{58}$$

The mobile user then sends the message C_8 to the service provider.

Step 6:After receiving the message, the service provider decrypts the message, and checks if the certificate is valid.

$$(Cert, Service-type) = D_{SK_{U-SP}}[C_8] \tag{59}$$

The service provider then checks if the certificate's lifetime is valid or not. The service provider offers the service $offer-service-type$ to the mobile user, then utilizes the session key to encrypt the service and new temporary identity T'_{IDnew}

$$C_9 = E_{SK_{U-SP}}[offer-service-type, T'_{IDnew}] \tag{60}$$

Finally, the service provider sends the ciphertext C_9 to the mobile user.

3.5 Certificate renewal from foreign network phase

When the mobile user roams in a foreign area, and the certificate has expired, or she wants to renew the certificate, she must pass the authentication phase. If the mobile user obtains the new certificate, she can then request a service in a foreign network.

Step 1:The mobile user enters her identity ID_i and password PW_i to the mobile device. The mobile device then computes:

$$A_i = h(ID_i||PW_i) \tag{61}$$

$$X'_i = h(A_i||PW_i) \tag{62}$$

After completing the above step, the mobile device checks whether the parameter X'_i is the same as X_i :

$$X'_i? = X_i \tag{63}$$

Then the mobile user is valid. The mobile device generates a certificate renewal message M_{req} and computes:

$$h(Y_i) = F_i \oplus A_i \tag{64}$$

$$C_{10} = h(A_i \oplus T'_{IDnew}) \tag{65}$$

$$KEY = h(C_{10}||h(Y_i)) \tag{66}$$

$$C_{11} = h(KEY||T'_{IDnew}) \tag{67}$$

and then sends the message $(T'_{IDnew}, C_{11}, M_{req})$ to the AAAF.

Step 2:Upon receiving the message, the AAAF verifies whether the mobile user is valid:

$$F'_i = h(Y_i||x) \oplus G_i \tag{68}$$

$$A'_i = F'_i \oplus h(Y_i) \tag{69}$$

$$C'_{10} = h(A'_i \oplus T'_{IDnew}) \tag{70}$$

$$KEY' = h(C'_{10}||h(Y_i)) \tag{71}$$

$$C'_{11} = h(KEY'||T'_{IDnew}) \tag{72}$$

After computing the parameter C'_{11} , the AAAH checks whether the parameter is the same as the authentication message C_{11}; otherwise the AAAF terminates this section.

$$C'_{11}? = C_{11} \tag{73}$$

If the above equation holds, the AAAF sends the message $(T'_{IDnew}, A'_i, C'_{10}, C'_{11}, M_{req})$to the AAAH via secure channel.

Step 3:The AAAH generates a new temporary identity (T''_{IDnew} , new lifetime ,$Lifetime_{new}$ and new certificate$Cert_{new}$ for the mobile user:

$$T''_{IDnew} = h(A'_i||x||nonce_i) \tag{74}$$

$$Sig_2 = Sign_{AAAH}[T''_{IDnew}, Lifetime_{new}] \tag{75}$$

$$Cert_{new} = (ID_{AAAH}, Sig_2) \tag{76}$$

The AAAH then sends the new certificate $Cert_{new}$ and new temporary identity T''_{IDnew} to the AAAF via secure channel.

Step 4:The AAAF computes the parameterC_{12} , and uses the mobile user's master key KEY' to encrypt the new temporary identity , T''_{IDnew} the new certificate , $Cert_{new}$and parameter C_{13}.

$$C_{12} = h(A'_i||ID_{AAAF}||KEY') \tag{77}$$

$$C_{13} = E_{KEY'}[T''_{IDnew}, Cert_{new}, C_{12}] \tag{78}$$

Finally, the AAAF sends the message C_{13} back to the mobile user.

Step 5:Upon receiving the message, the mobile user

utilizes the master key KEY to decrypt the message, and authenticates the AAAF:

$$(T''_{IDnew}, Cert_{new}, C_{12}) = D_{KEY}[C_{13}] \quad (79)$$

$$C'_{12} = h(A_i||ID_{AAAF}||KEY) \quad (80)$$

$$C'_{12}? = C_{12} \quad (81)$$

If the above equation holds, the mobile user ensures the AAAF is valid. The mobile user then updates the new temporary identity T''_{IDnew} and new certificate $Cert_{new}$ for the next authentication.

4 Analysis

Our scheme can withstand different types of attacks, and enhances the communication system's security. Even if the mobile device is lost, the security of the mobile user's information is not affected. In this section, we analyze the security of our scheme, and discuss other possible attacks.

4.1 Property Analysis

4.1.1 Confidential communication

In wireless or wire networks, communication security is the most important issue for any user. In our scheme, the communication system protects confidential messages by a one-way hash function, and uses the symmetric key. In the authentication and certificate issue phase, the AAAH and mobile user use the session key $SK_{U-AAAH} = h(T_{ID}||ID_{AAAH}||C'_1||C'_2)$to ensure communication security. The session key SK_{U-AAAH} is composed of the AAAH's identity ID_{AAAH}, two secret parameters C'_1 and C'_2, (where $C'_1 = h(A'_i \oplus T_{ID})$ and $C'_2 = h(KEY'||T_{ID})$) and a temporary identity T_{ID}. Even if an attacker intercepts the session key , the attacker cannot use the session key to discover the mobile user's identity ID_i , or password PW_i . No one can construct the same session key to impersonate the mobile user.

4.1.2 User's Privacy

For every service request and authentication, the mobile user uses the temporary identity T_{ID} and ciphertext C_2 to request a service or authenticate with the AAAH or service provider. However, our scheme also precludes a mobile device from storing the mobile user's information. The mobile device only stores the mobile user's temporary identity T_{ID}, and parameter F_i . The malicious attacker picks up a mobile device that does not contain any of the mobile user's sensitive information.Since the ciphertext C_2 , where ($C_2 = h(KEY||T_{ID})$), is protected by the user's master key KEY, $KEY = h(C_1||h(Y_i))$,$C_1 = h(A_i \oplus T_{ID})$, $A_i = h(ID_i||PW_i)$ even if the malicious attacker intercepts the message (T_{ID}, C_2) the attacker cannot identify the user's real identity ID_i or password PW_i by ciphertext C_2 . The master key has two unknown parameters, C_1 and $h(Y_i)$, such that the attacker cannot discover the user's identity ID_i or password PW_i . So, the system rigorously controls the security of communication and authentication for the mobile user's privacy. When the mobile user requests a service, the service provider cannot reveal the mobile user's real identity ID_i .

4.1.3 Low Computation

Since mobile devices are not suitable for heavy computation, the system must have the characteristics of a lightweight operation. In our scheme, the mobile device only performs a one-way hash function, or symmetric encryption, so our scheme is suitable for a mobile device.

4.2 Attack Analysis

4.2.1 Resist Stolen Verification Table

If a malicious attacker invades the AAAH to steal the verification table, the attackers cannot use the information (F_i, G_i, T_{ID}) If a malicious attacker invades the AAAH to steal the verification table, the attackers cannot use the information attacker obtains the information (F_i, G_i, T_{ID}) , they cannot utilize above parameters to compute secret value Y_i and $x(h(Y_i||x) = F_i \oplus G_i)$. In our scheme, a malicious attacker does not know the AAAH's private key, x because the secret value $h(Y_i||x)$ involves two unknown parameters Y_i and x.Our scheme does not store the mobile user's information at the AAAH or service provider, and the mobile device does not store mobile users' sensitive information. On the other hand, no sensitive information belonging to a mobile user is stored at the AAAH. Our scheme can prevent the theft of the verification table.

4.2.2 Resist stolen mobile device attack

In our improved scheme, if a malicious attacker obtains the mobile user's information, the attacker cannot easily obtain any parameter without passing self-authentication. Even if the malicious attacker extracts the parameters (F_i, A_i, T_{ID}) , since the identity ID_i and password PW_i are protected by hash function, the attacker still cannot obtain

any sensitive information (such as ID_i, PW_i or AAAH's secret key x)from those parameters. Notably, the malicious attacker doesn't know the mobile user's identity ID_i and password , PW_i and the parameter is always protected by two unknown factors. Therefore, no-one can use a stolen mobile device to pass the authentication without the mobile user's password and identity.

4.2.3 Resist impersonation attack

Upon receiving the authentication message, the AAAH utilizes the temporary identity to find the corresponding information about the mobile user, and computes (F_i', A_i', C_1', C_2') to authenticate whether the mobile user is valid or not. A malicious attacker cannot impersonate a legal user to transmit an authentication message (T_{ID}, C_2).The parameter $C_2(C_2 = h(KEY||T_{ID})$,$KEY = h(C_1||h(Y_i))$,$C_1 = h(A_i \oplus T_{ID}))$ includes two unknown parameters A_i and secret value $h(Y_i)$ thus, the malicious attacker cannot impersonate a legal mobile user to request a service, or to attack our system.

4.2.4 Resist ID-theft attack

In our scheme, the mobile user's real identity ID_i is not known by other mobile users, the service provider, or the AAA server. The proposed scheme provides a temporary identity T_{ID} as the mobile user's identity to communicate with the service provider or the AAAH. In the registration phase, the mobile user uses the parameter A_i to register to be a legal mobile user. The AAAH uses the parameter A_i as the mobile user's registration information. So, the network control center does not know the mobile user's real identity ID_i. Thus, our scheme can resist an ID-theft attack, even if the attacker intrudes upon the service provider or AAAH.

4.2.5 Resist legal user stealing the server's private key

In our scheme, the mobile user only owns the temporary identity T_{ID} and the parameter F_i, so the mobile user doesn't know the AAAH's sensitive information. Even if the mobile user invades the AAAH to steal the verification table and obtain information (F_i, G_i, T_{ID}), the mobile user cannot use information (F_i, G_i, T_{ID}) to reveal the AAAH's private key, x. The mobile user can utilize F_i to compute $h(Y_i||x) = F_i \oplus G_i$. However, there are two unknown values, F_i and x, in $h(Y_i||x) = F_i \oplus G_i$. On the other hand, if a legal mobile user steals information (F_i, G_i, T_{ID}), it will not reveal the AAAH's private key, x. So, our scheme not only resists legal mobile users from stealing the server's private key, but also prevents the possibility of an internal attack.

4.2.6 Resist Replay Attack

Since the established session key $SK_{U-AAAH} = h(T_{ID}||ID_{AAAH}||C_1'||C_2')$ includes the mobile user's temporary identity T_{ID} , and the T_{ID} is updated for each transaction, a malicious attacker intercepts the authentication message (T_{ID}, C_2) that can't perform the replay attack. The old temporary identity T_{ID} will be replaced by the new temporary identity T_{IDnew}. Thus, the malicious attacker cannot use the old message to achieve the replay attack.

5 Discussions

In this section, we compare our scheme with others using the six properties and six attacks for evaluating communication systems, as shown in Table 1. It is easy to see that our scheme can achieve the listed security requirements of section 1, and resist known attacks. Therefore, our scheme is superior to other schemes. In Table 2, we compare the computing cost with Moon and Lee's scheme, since the computing cost of the exponential and asymmetric encryption is heavier than that of hash function. Therefore, our computation cost is lower than their scheme.

Table 2: Computation cost comparison between Moon and Lee's scheme and our scheme

	Moon and Lee [20]	Our scheme
Registration phase	NA	7 T_h
Authentication &certificate issues phase	2 T_h +2 T_{sym} + 2 T_{mul} +10 T_{exp} + 1 T_{sig}	15 T_h +1 T_{sym} + 1 T_{sig}
Service request phase	1 T_h +1 T_{sym} + 1 T_{asy} +1 T_{mul}	13 T_h +4 T_{sym}
Certificate renewal from foreign network phase	2 T_h +3 T_{sym} + 2 T_{asy} +2 T_{mul} + 9 T_{exp} +2 T_{sig}	13 T_h +1 T_{sym} + 1 T_{sig}
Total cost	5 T_h +6 T_{sym} + 2 T_{asy} +5 T_{mul} + 19 T_{exp} +3 T_{sig}	48 T_h +6 T_{sym} + 2 T_{sig}

T_h: the time of one-way hash function operation
T_{sym}: the time of symmetric decryption/encryption operation
T_{asy}: the time of asymmetric decryption/encryption operation
T_{mul}: the time of multiplication operation
T_{exp}: the time of exponential operation
T_{sig}: the time of signing a signature

Table 1: Security comparison between our scheme and others

	Hsu's scheme [21]	Kim et al.'s scheme [22]	Moon and Lee's scheme [20]	Our scheme
Mutual authentication	No	No	No	Yes
Confidentiality	No	Yes	No	Yes
User's privacy	No	No	Yes	Yes
Low computation	No	No	No	Yes
Session independence	NA	NA	Yes	Yes
Integrity	No	No	Yes	Yes
Resist stolen verification table	NA	No	No	Yes
Resist stolen mobile device attack	NA	No	No	Yes
Resist impersonation attack	Yes	No	No	Yes
Resist the ID-theft attack	No	No	Yes	Yes
Resist legal user stealing the server's private key	NA	Yes	NA	Yes
Resist replay attack	Yes	Yes	Yes	Yes

6 Conclusions

We have improved the security of Moon and Lee's scheme. Although Moon and Lee claim their scheme can resist various known attacks, we have shown that the scheme is indeed vulnerable to mobile device attack. In Moon and Lee's scheme, malicious attackers can impersonate any legal user in order to log into the AAAH, or service provider, without, at any time, knowing the mobile user's password.

In summary, our scheme has the following characteristics:

(1) Our scheme can achieve mutual authentication to ensure communication security between the mobile user, service provider, and AAAH.

(2) Even if malicious attackers steal the mobile user's mobile device, they cannot reveal the mobile user's sensitive information via mobile device.

(3) Our scheme uses the digital signature mechanism to protect the mobile user's information from being stolen or modified.

Our scheme prevents a legal mobile user from stealing the AAAH's private key, and precludes the possibility of an insider attack.

Acknowledgement

This research was supported by the National Science Council, Taiwan, R.O.C., under contract number NSC 101-2221-E-324-005-MY2.

References

[1] T. Hwang, W. C. Ku, Reparable key distribution protocols for Internet environments, IEEE Transactions on Communications, **43**, 1947-1949 (1995).

[2] H. M. Sun, An efcient remote user authentication scheme using smart cards, IEEE Transactions on Communications, **46**, 958-961 (2000).

[3] H. M. Sun, An efcient remote user authentication scheme using smart cards, IEEE Transactions on Communications, **49**, 414-416 (2003).

[4] Amit K. Awashti, SunderLal , An enhanced remote user authentication scheme using smart cards, IEEE Transactions on Communications, **50**, 583-586 (2004).

[5] C. Chang, K. F. Hwang, Some forgery attacks on a remote user authentication scheme using smart cards, Computer and Information, **14**, 289-294 (2003).

[6] M. L. Das, A. Saxena, V. P. Gulati, A dynamic ID-based remote user authentication scheme, IEEE Transactions on Communications, **50**, 629-631 (2004).

[7] W. C. Ku, S. T. Chang, Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards, IEICE Transactions on Communications, **88**, 2165-2167 (2005).

[8] M. S. Hwang, C. C. Lee, Y. L. Tang, A simple remote user authentication scheme, Mathematical and Computer Modeling, **36**, 103-107 (2002)

[9] W. C. Ku, S. M. Chen, Weaknesses and improvements of an efcient password based remote user authentication scheme using smart cards, IEEE Transactions on Communications, **50**, 204-207 (2004).

[10] C. Lee, M. S. Hwang, W. P. Yang, A exible remote user authentication scheme using smart cards, ACM Operating Systems, **36**, 46-52 (2002).

[11] W. B. Lee, C. C. Chang, User identication and key distribution maintaining anonymity for distributed computer network, Computer and Systems, 211-214 (2000).

[12] W. J. Tsuar, C. C. Wu, W. B. Lee, A exible user authentication for multi-server internet services, Computer Science, **2093**, 174-183 (2001).

[13] L. Li, I. Lin, M. Hwang, A remote password authentication scheme for multi-server architecture using neural networks, IEEE Transactions on Neural Network, **12**, 1498-1504 (2001).

[14] C. Lin, M. S. Hwang, L. H. Li, A new remote user authentication scheme for multi-server architecture, Future Generation Computer Systems, **1**, 13-22 (2003).
[15] W. J. Tsuar, An enhanced user authentication scheme for multi-server internet services, Applied Mathematics and Computation, **170**, 258-266 (2005).
[16] T. S. Wu, C. L. Hsu, Efcient user identication scheme with key distribution preserving anonymity for distributed computer networks, Computer Security, **23**, 120-125 (2004).
[17] Y. Yang, S. Wang, F. Bao, J. Wang, R. Deng, New efcient user identication and key distribution scheme providing enhanced security, Computer Security, **23**, 697-704 (2004).
[18] W. S. Juang, Efcient multi-server password authenticated key agreement using smart cards, IEEE Transactions on Consumer Electronic, **50**, 251-255 (2004).
[19] C. Chang, J. S. Lee, An efcient and secure multi-server password authentication scheme using smart cards, IEEE. Proceeding of the International Conference on Cyberworlds, 417-422 (2004).
[20] J. S. Moon, I. Y. Lee, An AAA scheme using ID-based ticket with anonymity in future mobile communication, Computer Communications, **34**, 295-304 (2011).
[21] C. L. Hsu, A user friendly remote authentication scheme with smart cards against impersonation attack, Applied Mathematics and computation, **170**, 135-143 (2005).
[22] S. K. Kim, M. G. Chung, More secure remote authentication scheme, Computer Communications, **32**, 1018-1021 (2009).
[23] H-Y.Lin, Security and authentication in PCS, Computer and Electrical Engineering, 225-248 (1999).
[24] R-G Song, Advanced smart card based password authentication protocol, Computer Standards and Interface's, **32**, 321-325 (2010).

Chin-Ling Chen was born in Taiwan in 1961. He received the B.S. degree in Computer Science and Engineering from the Feng Chia University in 1991; the M.S. degree and Ph.D. in Applied Mathematics at National Chung Hsing University, Taichung, Taiwan, in 1999 and 2005 respectively. He is a member of the Chinese Association for Information Security. From 1979 to 2005, he was a senior engineer at the Chunghwa Telecom Co., Ltd. He is currently a professor of the Department of Computer Science and Information Engineering at Chaoyang University of Technology, Taiwan. His research interests include cryptography, network security and electronic commerce.

Kai-Wen Cheng was born in 1988. He received the B.S degree in Department of Computer Science and Information Engineering from Feng Chia University, Taichung Taiwan in 2010. He is studying the Master degree in Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung, Taiwan, in 2010. His research interests include information security and cryptology.

Chih-Cheng Chen is an assistant professor in Department of Industrial Engineering and Management in National Chin-Yi Institute of Technology. From 1996 to 2004, he was a senior engineer of Syntegra Tech. Company, which is an integration application software provider for the enterprise. He earned a Master and Ph.D. Degrees in Department of Mechatronics Engineering from National Changhua University of Education in 2005 and 2011 respectively. His research interests include mobile technology and RFID applications.

Ing-Chau Chang received his B.S. degree in Department of Computer and Information Science from National Chiao Tung University, Hsinchu, Taiwan, R.O.C., in 1990. and the M.S. and Ph.D. degrees in Institute of Computer Science and Information Engineering from National Taiwan University, Taipei, Taiwan, R.O.C., in 1992 and 1997, respectively. He is currently an associate professor in the Department of Computer Science and Information Engineering, National Changhua University of Education, Changhua, Taiwan, R.O.C. His current research topics include wireless networks, multimedia network protocols, and multimedia systems.