Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/081L13

An Improvement on the Self-Verification Authentication Mechanism for A Mobile Satellite Communication System

Chin-Ling Chen[1,*], *Kai-Wen Cheng*[1], *Young-Long Chen*[2], *Ing-Chau Chang*[3] *and Cheng-Chi Lee*[4]

[1] Department of Computer Science and Information Engineering, Chaoyang University, 168 Jifeng E. Road, Wufeng District, Taichung, 41349, Taiwan, R.O.C.
[2] Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, Taichung, 404, Taiwan, R.O.C.
[3] Department of Computer Science and Information Engineering, National Changhua University of Education, Changhua, 500, Taiwan, R.O.C.
[4] Department of Library and Information Science, Fu Jen Catholic University, New Taipei City, 24205, Taiwan, R.O.C.

Received: 19 Apr. 2013, Revised: 14 Aug. 2013, Accepted: 15 Aug. 2013
Published online: 1 Apr. 2014

Abstract: In 2009, Chen et al. proposed a satellite communication system for mobile devices to achieve wide communication. In this scheme, there are some security loopholes that need to be fixed since the mobile device was stolen. Since a malicious attacker intercepts the mobile user's information they can proceed with different attacks. Hence, we propose a novel scheme to improve the mobile user's communication protocol to enhance security. In this paper, the mobile satellite communication system achieves low computation and increases the system's security. The mobile user need not worry about sensitive information being revealed or stolen by malicious attacks, so that the mobile satellite communication system can be widely promoted in real life.

Keywords: Satellite Communication System, Mutual Authentication, Impersonation Attack, Mobile Device, Wireless Communication

1 Introduction

In recent years, information technology has developed very fast and network usage has become more popular. A satellite communication system is composed of a wireless network and satellite. A satellite communication system offers many conveniences such as permitting the user to communicate with others at any time. The traditional satellite communication system uses a Geosynchronous Equatorial Orbit (GEO) satellite that operates simultaneously with the Earth's equator. Since the GEO's transmission signal suffers from a delay problem, a Low-Earth Orbit (LEO) satellite gradually experiences problems. To reduce the signal reduction and transmission delay, using an LEO satellite to construct a communication system has become popular. In 1996, Cruickshank [1] proposed a satellite communication system based on the Public Key Cryptosystem (PKC), but in Cruickshank's scheme, the computation cost of the satellite communication system was too high. Therefore, Cruickshank's scheme is not suitable for mobile devices. In 2003, Hwang et al. [2] proposed a satellite communication system based on the Secret Key Cryptosystem (SKC) to solve Cruickshank's problems. Hwang et al.'s scheme reduces the computation cost of a satellite communication system so that the satellite communication system can integrate a mobile device to make it more convenient. Hwang et al.'s scheme improved the high computation cost but the scheme does not reduce the communication cost. To reduce computation and communication costs, Chen et al. [3] proposed a self-verification authentication mechanism for a mobile satellite communication system in 2009. Chen et al.'s scheme was based on session key agreement and reduced the communication cost and computation cost proposing a lightweight communication protocol.

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

However, Chen et al.'s scheme does not protect the mobile user's information. So, malicious attackers can successfully attack the satellite communication system or steal sensitive information about the mobile user. Hence, we improved Chen et al.'s scheme so that the proposed protocol would be more secure, and the attacker could not take advantage of any security loopholes to attack the satellite communication system or steal sensitive information regarding the mobile user. The improved scheme can enhance security and resist attacker attempts at impersonating the legal mobile user to communicate with other mobile users via the satellite communication system. In addition, when the mobile user receives the information from the network control center, the mobile user can perform mutual authentication to detect if the sender is legal or not. The network control center can also verify whether the mobile user is legal or not. The common architecture for a mobile satellite communication system is shown in figure 1.

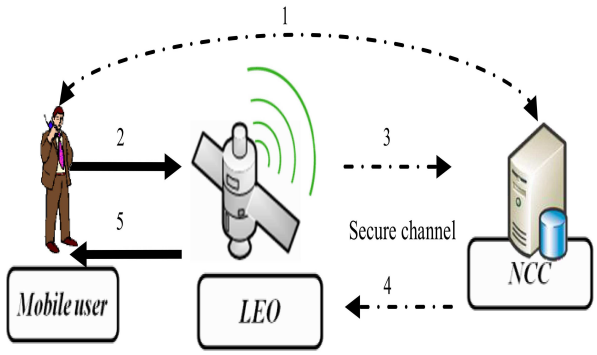

Figure 1: Common architecture of the mobile satellite communication system

In figure 1, the scenario of the satellite communication system is described as follows:
(1) Mobile user: The user can use the mobile device to communicate with others via the satellite communication system.
(2) Network control center (NCC): The network control center verifies if the user's identity is legal or not and stores the mobile user's information.
(3) LEO: The LEO transmits the communication information between the mobile user and the NCC.
Step 1: Mobile user to NCC: The mobile user sends the registration messages to the NCC. The NCC stores the registration information in its database and sends the temporary identity to the mobile user.
Step 2: Mobile user to LEO: The mobile user sends the authentication request information to the NCC via the LEO.
Step 3: LEO to NCC: After receiving the authentication request, the LEO forwards it to the NCC.
Step 4: NCC to LEO: When receiving the authentication request information, the NCC verifies it and sends back the response message to the mobile user via the LEO.
Step 5: LEO to mobile user: Upon receiving the response message, the LEO forwards it to the mobile user.
Reviewing Chen et al.'s scheme, the satellite communication system uses the LEO to construct a mobile communication system. In order to achieve more efficient and more secure communication for a satellite communication system, we list the following requirements to achieve what we want.
(1) Mutual authentication: In order to ensure security between the sender and receiver, mutual authentication is an important issue. Mutual authentication can prevent server spoofing attacks or impersonation user attacks [1, 4, 5, 6].
(2) Confidential communication: In the wireless network, information is vulnerable to eavesdropping attacks. Therefore, the satellite communication system must ensure communication security between the mobile user and the network control center [3].
(3) Mobile user's privacy: A secure satellite communication system needs to guarantee the mobile user's privacy. Therefore, how to protect the mobile user's identity and related information becomes an important issue [3, 7].
(4) Low computation: The communication system with a mobile device must have a low computation such that it is suitable for a mobile device [2, 3, 7, 8].
(5) Minimum trust: Because the network control center is vulnerable to becoming a target, the legal mobile user must reduce the amount of sensitive information stored at the network control center [3, 7].
(6) Session independence: The malicious attackers may intercept the session key to derive private information from the server or user. To guarantee the security of a satellite communication system, the session key must be for one-time use. Then, even if the attacker intercepts the session key it can't affect the system security [3, 5, 9, 10, 11]
The rest of this paper is organized as follows: In Section 2, we describe Chen et al.'s scheme and the weaknesses of the scheme. Our proposed scheme is described in Section 3. In Section 4, the property analysis and security analysis are presented. We discuss the performance and compare it with related works in Section 5. Our conclusions are presented in Section 6.

2 Review of Chen et al.'s Scheme

Chen et al. proposed a self-verification authentication mechanism for mobile satellite communication systems. The scheme is divided into three phases: the initial phase, the registration phase and the authentication phase. First, we introduce the notation used in the scheme as follows:

2.1 Notation

U_{ID} : the identity of the mobile user
T_{ID} : the temporary identity of a mobile user
LEO_{ID} : the identity of an LEO satellite
pw : the password of the mobile user
x : the private key of the network control center
$MAC_k()$: a one-way hash function with a key k
$E_k[m]$: using a secret-key to encrypt a message m
$D_k[m]$: using a secret-key to decrypt a message m
$h(.)$: a one-way hash function
$A? = B$:check if A is equal to B
$\oplus$:the XOR operation

2.2 Chen et al.'s Initial Phase

In the initial phase, the network control center selects a large prime number and a generator, g from multiplicative groupZ_p^* with order, q (q is a large prime factor of $p-1$) based on the discrete logarithm problem. Then the network control center selects a long-term use of the private key, x and the corresponding public key,y for the network control center as:

$$y = g^x mod\, p \tag{1}$$

2.3 Chen et al.'s Registration Phase

The mobile user registers to be a legitimate user at the network control center.
Step 1: The mobile user submits his identity U_{ID} to the network control center.
Step 2: The network control center decides on an initial temporary identity, T_{ID} for the mobile user. The temporary identity, T_{ID} is updated for the next transaction. The network control center selects a random number, k, the interval of random number k is $1 <= k < q$. The network control center computes the parameter, r and signature, s:

$$r = g^k mod\, p \tag{2}$$

$$s = h(U_{ID})x + kr^{-1} mod\, q \tag{3}$$

and then, the network control center generates the mobile user's master key,key :

$$key = h(U_{ID}, k) \tag{4}$$

Finally, the network control center stores the information(U_{ID}, T_{ID}, r, s) in the verification table and sends the message(U_{ID}, T_{ID}, key) to the mobile user.
Step 3:After receiving the message from the network control center, the mobile user stores the message(U_{ID}, T_{ID}, key) in the mobile device.

2.4 Chen et al.'s Authentication Phase

When the mobile user wants to communicate with the other mobile users, the mobile user needs to generate the session key to communicate with the network control center via the satellite communication system.
Step 1: The mobile user computes the session key,sk and the message authentication code,c:

$$sk = h(key, T_{ID}) \tag{5}$$

$$c = MAC_{key}(U_{ID}, T_{ID}, sk) \tag{6}$$

and then the mobile user sends the verification message (T_{ID}, c) to the LEO.
Step 2: After receiving the verification message (T_{ID}, c) from a mobile user, the LEO appends his identity LEO_{ID} to the verification message. Then, the LEO sends the verification message (LEO_{ID}, T_{ID}, c) to the network control center.
Step 3: Upon receiving the verification message, the network control center checks whether the identity of the LEO is legal or not. If the satellite's identity is legal, the network control center utilizes the verification message, (T_{ID}, c) to find the corresponding information (U_{ID}, r, s) of the mobile user from a verification table. When the network control center finds the mobile user's registration information, the network control center verifies the signature, s to ensure that the registration information was not tampered with by a malicious attacker:

$$g^s ? = y^{h(U_{ID})} r^{r^{-1}} mod\, p \tag{7}$$

If above equation holds, the network control center computes the mobile user's master key, key' and session key,sk' :

$$key' = h(U_{ID}, k) \tag{8}$$

$$sk' = h(key', T_{ID}) \tag{9}$$

After computing the parameters key' and sk' , the network control center computes the message authentication code, c' and checks whether the authentication message, c is the same as c' :

$$c' = MAC_{key'}(U_{ID}, T_{ID}, sk') \tag{10}$$

$$c' ? = c \tag{11}$$

If above equation holds, it means the verification message (T_{ID}, c) and session key,sk are valid. Finally, the network control center generates the new temporary identity, T_{IDnew} and updates the verification table. Then, the network control center utilizes the session key, sk to encrypt the temporary identity, T_{ID} and T_{IDnew}

$$C_1 = E_{sk'}(T_{ID}, T_{IDnew}) \tag{12}$$

The network control center sends back the message , $(LEO_{ID}, C_1)$to the mobile user via the LEO.
Step 4: Once the verification messages are received, the LEO forwards the message,C_1 to the mobile user. When the mobile user receives the message, the mobile user uses the session key, sk to decrypt the message and updates the temporary identity, T_{IDnew} for next verification:

$$(T_{ID}, T_{IDnew}) = D_{sk}(C_1) \tag{13}$$

2.5 Weaknesses of Chen et al.'s Scheme

Chen et al.'s scheme has some security loopholes that an attacker can utilize to attack the satellite communication system or steal sensitive information. We point out some security loopholes that need to be fixed as follows:
1. When a mobile user loses his or her mobile device, a malicious attacker can intercept the mobile user's information [12, 13] from the mobile device. The malicious attacker can use the existing information $(U_{ID}, T_{ID}, key)$to attack the satellite communication system or impersonate the legal mobile user to communicate with others.
2. Once a malicious attacker possesses the information (U_{ID}, T_{ID}, key), the malicious attacker can compute the session key, $sk = h(key, T_{ID})$ and the message authentication code $c = MAC_{key}(U_{ID}, T_{ID}, sk)$used between the mobile user and the network control center. Then, the malicious attacker can use the session key, sk and message authentication code, c to process an impersonation attack [10-13].
3. Malicious attackers can intercept the U_{ID}; the master key,key and T_{ID} from the mobile device. They can utilize the information(T_{ID}, key) to compute the session key, sk with $sk = h(key, T_{ID})$. Therefore, the attackers can process a server spoofing attack or impersonation attack with the session key,sk. Hence, Chen et al.'s scheme does not achieve mutual authentication between the network control center and mobile users.
Hence, we improve Chen et al.'s scheme to achieve a more secure communication. In our scheme, the mobile user applies the mutual authentication in the satellite communication system that ensures the security of communication between the mobile user and the network control center. In our scheme, the mobile device does not store any sensitive information from the mobile user to prevent the mobile user from losing his mobile device. Therefore, our scheme can protect the mobile user's privacy and increase the satellite communication system's security.

3 The Improved Scheme

3.1 Initial Phase

The network control center first generates a private key for long-term use and a corresponding public key, described as follows:
In the initial phase, the network control center selects a large prime number and a generator, g from multiplicative groupZ_p^* with order, q (q is a large prime factor of$p-1$) based on the discrete logarithm problem. Then the network control center selects a long-term use of the private key, x and the corresponding public key,y for the network control center as:

$$y = g^x mod\, p \tag{14}$$

3.2 Registration Phase

The mobile user registers with the network control center to be a legal user. In this phase, we assume no-one can know the identity and password of mobile user. Hence, the identity and password of mobile user is not public.
Step 1:The mobile user inputs his identity, U_{ID} and password, pw to a mobile device. Then the mobile device utilizes the information to compute w:

$$w = h(U_{ID}, pw) \tag{15}$$

The mobile user sends the information, w to network control center.
Step 2:The network control center decides on an initial temporary identity, T_{ID} for the mobile user. The temporary identity, T_{ID}, is refreshed for each successful authentication.
Step 3:The network control center selects a random number, k. Then the network control center computes signature (r,s):

$$r = g^k mod\, p \tag{16}$$

$$s = h(w)x + kr^{-1} mod q \tag{17}$$

Upon computing the signature, s, the network control center computes b:

$$b = h(s,x) \oplus w \tag{18}$$

Finally, the network control center stores the information (T_{ID}, r, s, b) in the verification table and sends the message (T_{ID}, r) to the mobile user.After receiving the message from the network control center, the mobile user stores the message (T_{ID}, r) in the mobile device.

3.3 Authentication Phase

When the mobile user wants to communicate with other mobile users, the mobile user needs to go through the verification procedures in this system. In this phase, the mobile user and network control center should process mutual authentication to resist known attacks.
Step 1:The mobile user inputs his identity, U_{ID} and password, pw. The mobile device computes parameter, w and master key, key:

$$w = h(U_{ID}, pw) \tag{19}$$

$$key = h(w, r) \tag{20}$$

Then the mobile user computes the session key, sk and message authentication code, c:

$$sk = h(key, T_{ID}) \tag{21}$$

$$c = MAC_{key}(w, T_{ID}, sk) \tag{22}$$

Then the mobile user sends the verification message (T_{ID}, c) to the LEO.
Step 2:Once the verification message (T_{ID}, c) is received, the LEO adds the satellite,$LEO_{ID}$to the verification message. Then the LEO sends the message (LEO_{ID}, T_{ID}, c) to the network control center.
Step 3:When the network control center receives the verification message (LEO_{ID}, T_{ID}, c) , it checks to see if the identity is legal or not. Then the network control center utilizes the verification message to find the corresponding information(r, s, b) for the mobile user from the verification table. When the network control center finds the mobile user's information, the network control center verifies the signature to ensure that the information was not tampered with by a malicious attacker:

$$g^s ? = y^{h(w)} r^{r^{-1}} mod\, p \tag{23}$$

Using the parameter, b and the signature, s private key, x compute w:

$$w = h(s, x) \oplus b \tag{24}$$

If the mobile user's information was not tampered with, then the network control center computes the master key', and session key, sk':

$$key' = h(w, r) \tag{25}$$

$$sk' = h(key', T_{ID}) \tag{26}$$

After generating the session key, the network control center computes the message authentication code, c' and checks to see if the authentication message from the mobile user is the same as that of the network control center:

$$c' = MAC_{key'}(w, T_{ID}, sk') \tag{27}$$

$$c' ? = c \tag{28}$$

If so, the verification message and session key are valid. Finally, the network control center generates a temporary identity,T_{IDnew} and updates the verification table. Then, the network control center utilizes the session key,sk' to encrypt the temporary identityT'_{ID} and ,T_{IDnew}:

$$C_2 = E_{sk'}(T'_{ID}, T_{IDnew}) \tag{29}$$

Then it sends back the message (LEO_{ID}, C_2) to the mobile user via an LEO.
Step 4:After receiving the authentication message(LEO_{ID}, C_2),the LEO forwards message $C_2$to the mobile user.When message C_2 is received, the mobile user decrypts the message and checks to see if the temporary identity, , T'_{ID} is the same as the original. If the same, the mobile user updates the temporary identity, T_{IDnew} for the next verification:

$$(T'_{ID}, T_{IDnew}) = D_{sk}(C_2) \tag{30}$$

$$T'_{ID} ? = T_{ID} \tag{31}$$

4 Analysis

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

4.1 Property Analysis

4.1.1 Mutual Authentication

(1) NCC authenticates mobile user: Moreover, he or she has to compute the message authentication code. The NCC will check to see whether the message is correct or not by $c' ? = c$. If message c is valid, the NCC can confirm that the mobile user is legitimate.
(2)Mobile user authenticates NCC: If the mobile user receives the response message from the NCC, he or she will check the message $T'_{ID} ? = T_{ID}$ to authenticate the NCC. If the encrypted message C_2 is valid, the mobile user can confirm that and communicate with the NCC.
According to the above two cases, our improved scheme provides mutual authentication between the mobile user and the NCC.

4.1.2 Confidential Communication

In a wireless network, communication security is the most important issue for every mobile user. In our scheme, the communication system protects the confidential message by a one-way hash function and uses the session key to encrypt the message. The satellite communication system uses the session key $sk = h(key, T_{ID})$ to ensure communication security between the mobile user and the network control center. Session key $sk = h(key, T_{ID})$ is composed of a user's master key,$key = h(w,r)$ (when $w = h(U_{ID}, pw)$ and $r = g^k mod p$) and a temporary identity, T_{ID}. Even if the malicious attacker intercepts the session key, sk, the attacker can't utilize the session key to discover the user's identity, U_{ID} and password, pw.

4.1.3 User's Privacy

For every communication and authentication, the mobile user uses the temporary identity, T_{ID} and message authentication code, $c = MAC_{key}(w, T_{ID}, sk)$ to communicate or authenticate with the network control center. However, our scheme also avoids a mobile device to store the mobile user's information. The mobile device only stores the mobile user's temporary identity, T_{ID} and parameter, r. The malicious attacker picks up a mobile device that does not contain any information about the mobile user. Since the message authentication code, c,where $c = MAC_{key}(w, T_{ID}, sk)$, is protected by the user's master key,$key = h(w,r)$even if the malicious attacker intercepts the message (T_{ID}, c) , the attacker can't identify the user's real identity, U_{ID} and password,pw by a message authentication code. The master key has two unknown parameters, w and r, so that the attacker can't discover the user's identity, U_{ID} and password, pw. So, the mobile satellite communication system rigorously controls the security of communication and authentication for the mobile user's privacy. When the mobile user communicates with other mobile users via the satellite communication system, the network control center doesn't reveal the mobile user's real identity, U_{ID}.

4.1.4 Low Computation

Since the mobile device is not suitable for heavy computation, the satellite communication system must have the characteristics of a lightweight operation. In our scheme, the network control center takes the burden of most of the computation and the mobile device reduces unnecessary burden. The mobile user only computes a one way hash function or symmetric encryption, so our scheme is suitable for a mobile device.

4.1.5 Minimum Trust

In the satellite communication system, the network control center is vulnerable to attackers. In Chen et al.'s scheme, the network control center stores the mobile user's identity, U_{ID} that the attacker can utilize to construct a master key, $key = h(w,r)$ and a session key, $sk = h(key, T_{ID})$to impersonate a legal user. In our scheme, the network control center doesn't store mobile users' sensitive information. The network control center only stores the parameter, r and the user's temporary identity, T_{ID}. So, our scheme avoids malicious attacks on satellite communication systems. Even if a malicious attacker attacks the satellite communication system, they can't obtain secret information or tamper with the important parameters. The network control center uses the signature,$s = h(w)x + kr^{-1} mod q$ to protect the important information. Only a malicious attacker who holds the server's private key,$x$can obtain sensitive information. In fact, it is impossible to reveal a mobile user's information. Our scheme can achieve the minimum trust.

4.1.6 Session Independence

In our scheme, the satellite communication system uses the session key, sk to guarantee communication security between the mobile user and the network control center. If a malicious attacker intercepts the session key, the communication system may create security loopholes. Then a malicious attacker can use these loopholes to steal or tamper with a mobile user's information. In our scheme, the session key has independent features. When the mobile user wants to communicate with the network control center, the user must have the session key, sk to communicate with others in the satellite communication system. Since the session key includes the temporary identity $T_{ID}$and master key,$key = h(w,r)$the temporary identity$T_{ID}$is changed by every authentication. So if a malicious attacker intercepts this session key,$sk = h(key, T_{ID})$,it can't be used for the next communication. The session key is a one-time use key.

4.1.7 Known Key Security

In our scheme, even if a malicious attacker intercepts the last communication message or session key, it can't be used to derive the next session key or communication message. The established session key,$sk = h(key, T_{ID})$includes the mobile user's master key,$key = h(w,r)$and temporary identity,T_{ID}After each authentication, the temporary identity is updated. Therefore, the satellite communication system has the feature of session key independence.

4.2 Attack Analysis

4.2.1 Resist Stolen Verification Table

If a malicious attacker invades the network control center to steal the verification table, the attackers can't use the information $(T_{ID}, r, s, b)$to impersonate the legal mobile user or network control center. Even if a malicious attacker obtains the information (T_{ID}, r, s, b),they can't utilize the signature, $s = h(w)x + kr^{-1}modq$to compute the random number, k.In our scheme, a malicious attacker doesn't know the network control center's private key, x because the signature involves unknown parameter, w.We improve the satellite communication system so that it does not store the mobile user's information at the network control center, and the mobile device does not store mobile users' sensitive information. In our scheme, we create the minimum trust for a network control center, which means that no sensitive information about a mobile user is stored at the network control center. The network control center stores w,$w = h(U_{ID}, pw)$ is calculated by a mobile device as the mobile user's information rather than using plain text to transfer the registration message. Our scheme can prevent the theft of the verification table.

4.2.2 Resist The Impersonation User Attack

Upon receiving the authentication message, the network control center finds the mobile user's information and uses the signature $s = h(w)x + kr^{-1}modq$ to authenticate whether the mobile user is valid or not. The attacker can't tamper with the real signature, $s = h(w)x + kr^{-1}modq$to obtain the mobile user's information at the network control center. Because a malicious attacker doesn't know the network control center's long-term private key, x, he can't impersonate the legal mobile user to attack the satellite communication system.

4.2.3 Resist The Server Spoofing Attack

In a satellite communication system, the LEO and network control center transfers messages via a secure channel so the attackers can't fool the satellite or network control center to steal sensitive information. In order to replicate the satellite, the malicious attacker would have to spend a lot of money to construct a satellite communication system. So, it is difficult for any malicious attacker to replicate the satellite or network control center. In addition, if a mobile user sends out the authentication message, $c = MAC_{key}(w, T_{ID}, sk)$,the counterfeit network control center doesn't have the necessary private key, x of the real network control center. Hence, a malicious attacker can't access the parameter,w with the mobile user's information $b = h(s, x) \oplus w$ In order for a malicious attacker to construct the session key,$key = h(w, r)$, he must possess parameter w and parameter r. If a malicious attacker wants to communicate with other mobile users he must construct a session key in advance, thus our scheme can resist a malicious attacker from fooling a server.

4.2.4 Resist ID-theft Attack

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

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} andand the message authentication code, c,so the mobile user doesn't know the network control center's sensitive information. Even if the mobile user invades the network control center to steal the verification table and obtain information (T_{ID}, r),the mobile user can't use information(T_{ID}, r) to reveal the network control center's private key, x. On the other hand, the signature,$s = h(w)x + kr^{-1}modq$,must use the network control center's private key, x to verify it. Even if a legal mobile user steals information(T_{ID}, r, s, b) it will not reveal the 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 internal attack.

4.2.6 Resist Replay Attack

Since the established session key,$sk = h(key, T_{ID})$includes the mobile user's temporary identity, T_{ID} and the T_{ID} will be updated for each transaction, the malicious attacker intercepts the authentication message(T_{ID}, c) that can't perform the replay attack. The old temporary identity, T_{ID}will be replaced by the new temporary identity,T_{IDnew}. So, the malicious attacker can't use the old message to achieve the replay attack during satellite communication.

4.2.7 Resist The Modification Table Attack

Even if a malicious attacker invades the network control center, the attacker can't tamper with information(T_{ID}, r, s, b)stored at the network control center. Because a malicious attacker doesn't know the network control center's private key, x, the attacker can't tamper with signature ,$s = h(w)x + kr^{-1} mod q$.In the authentication phase, the network control center first checks whether the information is correct via $g^s ? = y^{h(w)} r^{r^{-1}} mod p$Thus, our scheme can resist a modification table attack.

5 Discussions

In this section, we compare our scheme with other schemes using the seven properties and seven attacks for evaluating satellite communication systems, as shown in Table 1. It is easy to see that our scheme can achieve all security requirements. Therefore, our scheme is superior to other schemes. In addition, we compare the computation cost with other schemes in Table 2. Although our computation cost is higher than the others, our scheme can satisfy the most security requirements and enhance the system's security.

6 Conclusions

The proposed scheme achieves complete protection against known attacks, since the mobile user does not store sensitive information in a mobile device. Even if a mobile user loses his/her mobile device, he/she need not worry about the revelation of their confidential information. Our scheme does not suffer from mobile device loss due to attacks and uses the message authentication code to protect the security of mobile satellite communication.
In summary, our scheme has the following characteristics:
(1) Our scheme uses a mutual authentication mechanism to ensure communication security between the mobile user and network control center.
(2) The network control center and mobile user store a minimum of confidential information to achieve the most complete protection between the network control center and mobile user.
(3) Even if a mobile device is lost, it does not affect the security of the mobile satellite communication.
(4) Our scheme uses the network control center's private key and signature to protect the mobile user's information from being stolen or modified.
(5) Our scheme prevents a legal mobile user from stealing the network control center's private key and prevents the possibility of an insider attack occurring.

Table 1: Security comparison between our scheme and others

	Chen et al.'s scheme [3]	Chang et al.'s scheme [4]	Hwang et al.'s scheme [10]	Our scheme
Mutual authentication	No	Yes	No	Yes
Confidentiality	Yes	No	NA	Yes
User's privacy	No	No	No	Yes
Low computation cost	Yes	No	Yes	Yes
Minimum trust	Yes	Yes	Yes	Yes
Session independence	Yes	No	No	Yes
Known key security	Yes	NA	NA	Yes
Resist server spoofing attack	No	No	No	Yes
Resist impersonation user attack	No	No	No	Yes
Resist the stolen verification table	Yes	Yes	Yes	Yes
Resist the modification table attack	Yes	Yes	Yes	Yes
Resist replay attack	Yes	Yes	Yes	Yes
Resist ID-theft attack	No	No	No	Yes
Resist the legal user steals the server's private key	Yes	Yes	Yes	Yes

Table 2: Computation cost between our scheme and others

	Chen et al.[3]		Our scheme	
	User	Server	User	Server
Registration phase		$2T_h+$ $2\ _{mul}+T_{exp}$	T_h	$2T_h+$ $2\ T_{mul}+T_{exp}$
Authentication phase	$2T_h+$ T_{sym}	$5T_h+T_{sym}+$ $3T_{mul}+3T_{exp}$	$4T_h+$ T_{sym}	$6T_h+T_{sym}+$ $3T_{mul}+3T_{exp}$
Total cost	$9T_h+2T_{sym}+5$ $T_{mul}+4T_{exp}$		$13T_h+2T_{sym}+$ $5\ T_{mul}+4T_{exp}$	

T_h: one-way hash function operation
T_{sym}: symmetric decrypt/encrypt operation
T_{mul}: the multiplication operation

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] H. S. Cruickshank, A security system for satellite networks, IEEE Satellite System Mobile Communications and Navigation, 187-190 (1996).
[2] M. S. Hwang, C. C. Yang and C. Y. Shiu, An authentication scheme for mobile satellite communication systems, ACM Operating Systems Review, 145-148 (2003).
[3] T. H. Chen, W. B. Lee and H. B. Chen, A self-verification authentication mechanism for mobile satellite communication systems, Computers and Electrical Engineering, **35**, 41-48 (2009).
[4] Y. F. Chang, C. C. Chang, An efficient authentication protocol for mobile satellite communication system, ACM Operation Systems Review, **39**, 70-84 (2005).
[5] T. H. Chen, H. C. Hsiang and W. K. Shih, Security enhancement on an improvement on two remote user authentication schemes using smart cards, Proceedings of 11th International Conference on Parallel and Distributed System, 73-77 (2005).
[6] G. S. Wen, M. W. Jian, Efficient remote mutual authentication and key agreement, Computers and Security, **25**, 72-77 (2005).
[7] Y. Y. Wang, J. Y. Liu, F. X. Xiao and J. Dan, A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communications, **32**,583-585 (2009).
[8] A. Aziz, W. Diffie, Privacy and authentication for wireless local area networks, IEEE Personal Communications, 25-31 (1994).
[9] R. J. Hwang, F. F. Su, A new efficient authentication protocol for mobile networks, Computer Standards and Interface, **28**, 241-252 (2003).
[10] C. L. Hsu, A user friendly remote authentication scheme with smart cards against impersonation attack, Applied Mathematics and computation, **170**, 135-143 (2005).
[11] S. K. Kim, M. G. Chung, More secure remote authentication scheme, Computer Communications, **32**, 1018-1021 (2009).
[12] H. Y. Lin, Security and authentication in PCS, Computer and Electrical Engineering, 225-248 (1999).
[13] R. G. Song, Advanced smart card based password authentication protocol, Computer Standards and Interface, **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.

Young-Long Chen received the B.S. degree in automatic control engineering from Feng Chia University, Tai-Chung, Taiwan, in 1988, the M.S. degree in engineering science from National Cheng Kung University, Tainan, Taiwan, in 1995 and the Ph.D. degree in electrical engineering from National Chung Cheng University, Chia-Yi, Taiwan, in 2007. From 1995 to 1999, he worked for Formosa Petrochemical Corporation as a Design Engineer. From 1999 to 2007, he was a Lecturer with the Department of Electrical Engineering, Chienkuo Technology University, Taiwan. From 2007 to 2009, he was a Professor with the Department of Electrical Engineering, Chienkuo Technology University, Taiwan. Since 2009, he has been with the Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, Taiwan, where he is currently a Professor. His research interests include wireless communications, wireless sensor networks, information security, digital signal processing, fuzzy neural networks and embedded systems.

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. He is a member of the Institute of Electrical and Electronics Engineers (IEEE).

Cheng-Chi Lee received the B.S. and M.S. in Information Management from Chaoyang University of Technology, Taichung, Taiwan, in 1999 and in 2001. He received the Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. From 2007, he is an associate professor of Department of Library and Information Science, Fu Jen Catholic University. From 2009, he is an Editorial Board member of International Journal of Network Security and International Journal of Secure Digital Information Age. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 40 articles on the above research fields in international journals.