EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

An efficient and secure anonymous authentication scheme for mobile satellite communication systems

Eun-Jun Yoon[1*], Kee-Young Yoo[2], Jeong-Woo Hong[3], Sang-Yoon Yoon[3], Dong-In Park[3] and Myung-Jin Choi[4*]

Abstract

This paper proposes a new efficient and secure anonymous authentication scheme for mobile satellite communication systems. Compared with the related schemes, the proposed scheme achieves the following three main advantages: (1) It is just based on a secure one-way hash function for avoiding complex computations for both mobile users and network control center (NCC), (2) it does not require sensitive verification table which may cause NCC to become an attractive target for numerous attacks (e.g., insertion attacks and stolen-verifier attacks), and (3) it provides higher security level (e.g., secure mutual authentication and key establishment, confidential communication, user's privacy, simple key management, and session key independence). As a result, the proposed scheme is very suitable for lightweight-device environments because of very low computation overload on the part of both mobile user and NCC.

Keywords: mobile satellite communication system, user authentication, key establishment, public-key management, anonymity

1 Introduction

Recently, mobile satellite communication systems have captured much attention because these systems provide the opportunity to make personal communication as broad as possible [1-11]. Within mobile satellite communication systems, the problem arises how to mutually authenticate each other and whether confidentiality of communication is guaranteed. In 1996, Cruickshank [12] first proposed a security system for satellite networks. In the Cruickshank's scheme, public-key cryptosystem (PKC) is used to provide authentication between a mobile user and the satellite network [13]. However, the scheme has the following three disadvantages: (1) It requires the complex computation overhead, (2) it requires the complexity of the public-key management in a PKI, and (3) user's privacy is not kept confidential. In 2003, Hwang et al. [14] proposed another authentication scheme for mobile satellite communication system based on secret-key cryptosystems (SKC). The scheme reduced the complex computation overhead for mobile users by adopting only SKC instead of PKC. However, Hwang et al.'s scheme also has the following three disadvantages: (1) It is insecure to the known key attack, (2) it is insecure to the stolen-verifier attack, and (3) the session key needs to be updated on the server side whenever the mobile user is authenticated.

In 2005, to overcome the weaknesses of Hwang et al.'s scheme, Chang et al. [15] proposed a hash-chain-based authentication scheme to improve efficiency and security. Due to the inverse direction when hashing the input value, a leaked hashed value of the chain is useful only for directly generating the valid value of the preceding, but not of the following session. This can preserve the authentication token used in the following session from leakage. However, Chang et al.'s scheme still has the following three disadvantages: (1) An adversary can impersonate as either the mobile user or the network control center (NCC) using the compromised hash values from NCC, (2) user's privacy is not kept confidential, and (3) it requires a great amount of communication bandwidth and computation resources.

* Correspondence: ejyoon@knu.ac.kr; prime@kari.re.kr
[1]School of Computer Engineering, Kyungil University, 33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea
[4]Satellite Information Research Institute, Korea Aerospace Research Institute, 45 Eoeun-Dong, Yuseong-Gu, Daejeon 305-333, Republic of Korea
Full list of author information is available at the end of the article

Quite recently, Chen et al. [16] proposed a self-verification authentication scheme for mobile satellite communication systems. Chen et al.'s scheme is based on PKC and SKC and achieves the following three advantages: (1) It does not require the public-key infrastructure (PKI), (2) it reduces the complex computation for mobile users, and (3) it does not require sensitive verification table. Nevertheless, we found that Chen et al.'s scheme still requires high computations for both mobile users and NCC. For instance, it requires one pair of secret-key encryption/decryption computations during the authentication phase. In addition, for repelling an insertion attack in which an intruder inserts a verification item into the verification table, NCC always must verify if $g^s = y^{h(U_{ID})} \cdot r^{r^{-1}} \bmod p$ holds during the authentication phase. We can see that the verification equation requires three exponential computations. Chen et al. claimed that these operations could be performed either off-line or by another authentication server in order to reduce complex computations. However, these solutions may cause increased communication delay.

Based on Chen at al.'s scheme, this paper proposes a new efficient and secure anonymous authentication scheme for mobile satellite communication systems. Compared with the above-related schemes, the proposed scheme achieves the following three main advantages: (1) It is just based on a secure one-way hash function for avoiding complex computations for both mobile users and NCC, (2) it does not require sensitive verification table which may cause NCC to become an attractive target for numerous attacks (e.g., insertion attacks and stolen-verifier attacks), and (3) it provides higher security level (e.g., secure mutual authentication and key establishment, confidential communication, user's privacy, simple key management, and session key independence) [16,17]. As a result, the proposed scheme is very suitable for lightweight-device environments because of very low computation overload on the part of both the mobile user and NCC.

The paper is organized as follows. Section 2 describes background concepts of mobile satellite communication systems and the required essential properties to efficiently establish a secure mobile satellite communication link. Section 3 presents the proposed authentication scheme. Discussion and security analysis are described in Section 4. Finally, conclusions will be given in Section 5.

2 Preliminaries

This section introduces the basic concepts of mobile satellite communication systems and the required security properties to efficiently establish a secure mobile satellite communication link [1,12-16].

2.1 Mobile satellite communication systems

The traditional satellite communication system employed a geostationary satellite, located in geosynchronous equatorial orbit (GEO), circling the planet in full 24 h. However, the quite far distance, exactly 22,300 miles, between the geostationary satellite and the earth resulted in a signal delay problem. Over the past 10 years, considerable attention has been paid to low-earth-orbit (LEO) satellite communication systems for establishing personal communication systems due to their large broadcasting range and communication area, small attenuation of the signals, and a shorter transmission delay [1].

The LEO satellite communication system, as illustrated in Figure 1, consists of the mobile users, the LEO satellites, the gateways, and a network control center (NCC) [2]. The responsibility of the LEO satellite is to forward communications among mobile users, other LEO satellites and the gateways in the system. A gateway with a wired channel to NCC (the solid line in Figure 1) presides over communications between NCC and LEO satellites. In general, many different telecommunication systems are connected together via the satellite communication model to provide diversified communication services, thus forming the so-called mobile satellite communication system (MSCS for short). For example, if a mobile user wants to communicate with a terrestrial mobile user such as a GSM user, the mobile user must contact and perform mutual authentication with NCC which will subsequently contact the GSM network. A communication link is then established between the mobile user and the other GSM user [16].

2.2 Required essential properties

As Figure 1 shows, communications among mobile users, LEOs, and gateways are open on the air (thunderbolt line), while NCC is assumed to communicate with the gateway via a secure channel (solid line). Based on this assumption, the following several essential properties [16,18-22] must be considered to efficiently establish a secure mobile satellite communication link and prevent various cryptographical attacks. We can find out that many researchers [16,18-22] claimed the following properties are absolutely required for efficient and secure mobile satellite communication environments.

(1) *Mutual authentication*: Mutual authentication between mobile users and NCC is an essential requirement, while many authentication schemes in the literature only provide unilateral authentication, i.e., GSM. Without proper authentication for NCC, the mobile user might be fooled during the user

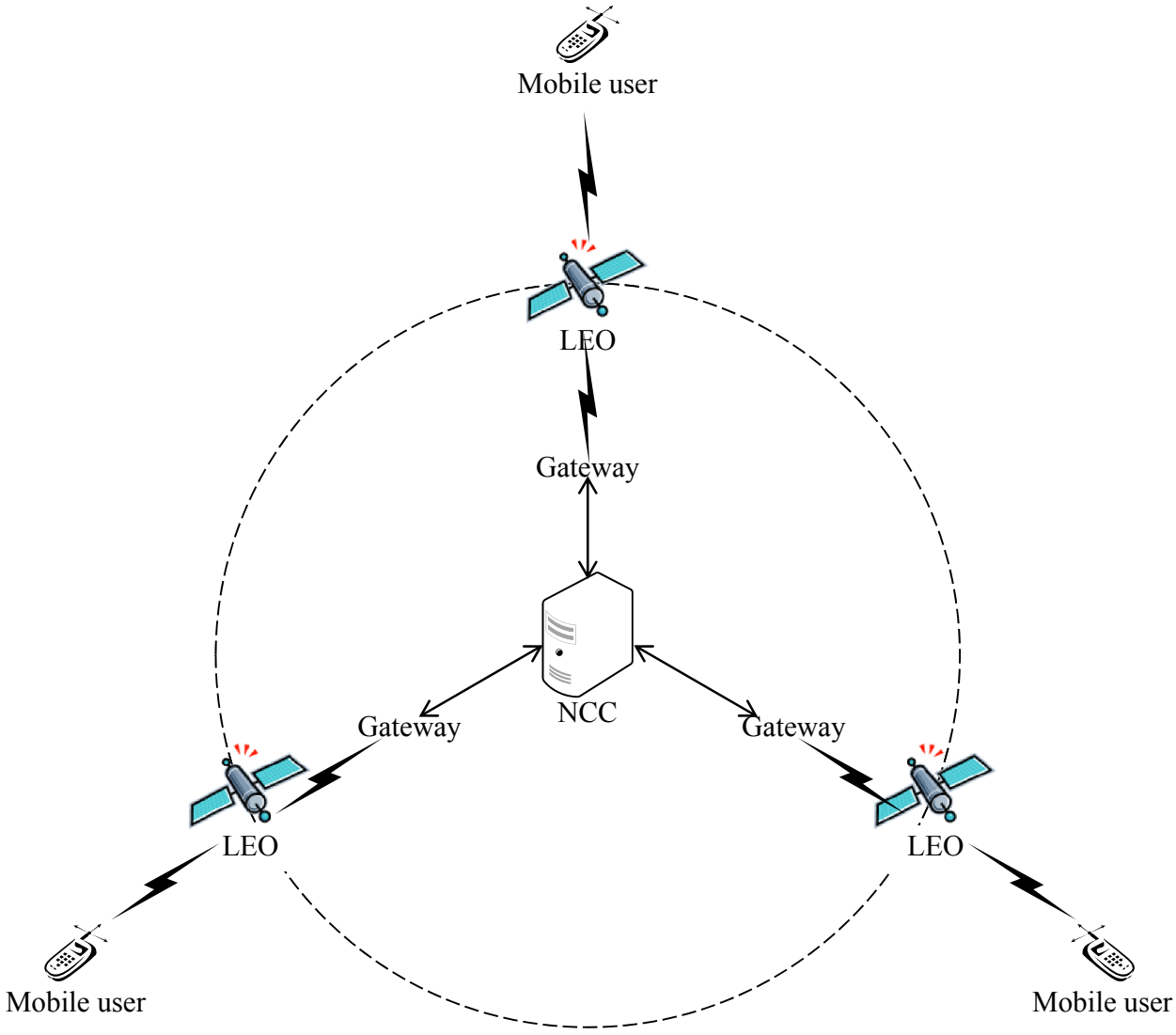

Figure 1 Overview of a simple mobile satellite communication network: wired secure network (solid lined) and wireless network (thunderbolt lined).

authentication phase to send his/her sensitive information to an unidentified target or be fooled into establishing a connection to retrieve services which are not recognized by legitimate NCC.

(2) *Confidential communication*: Communication over wireless paths is susceptible to eavesdropping. Security protocols guarantee the confidentiality of communications between mobile users and NCC by encrypting them using the shared session key.

(3) *User's privacy*: There are two major privacy issues of concern for mobile networks: user's identity and location. Since sometimes the user's real identity is sensitive to adversaries [6] or the linkable identity of a user is useful in mining his/her behavior, the user's identity and associated information must be kept secret from outsiders as well as the mobile user's current location.

(4) *Low computation and update cost*: A security protocol should result in low computation cost. Due to limited resources, on one hand, complex computations will fail in the hand-held device of a mobile user and, on the other hand, frequent computations and updates might cause NCC to become a bottleneck. This property is not only of concern for lightweight hand-held devices in PCS and MSCS, but also for NCC.

(5) *Simple key management*: As protecting the secret key from being compromised is a very critical issue in any environment concerning security, key management should be simple as well as safeguard

against possible risks. In order to ease the problem of key management, first, the security-sensitive table (generally for storing the secret keys shared with legal users) should be removed from the server side and, secondly, the heavy burden of maintaining a public-key infrastructure should be avoided in practical applications such as GSM and UMTS.

(6) *Minimum trust*: It is well-accepted that NCC is trustworthy, since legal mobile users register their private information to obtain services at NCC, but the trust level of the other third parties involved should be as little as possible.

(7) *Session independence*: It is always possible that a session key can be compromised for some reasons. An adversary may derive the secret key from the last session as well as the next session (so-called known key attacks) if these keys have correlation with the compromised session key. To avoid that the revealed key may influence the security, the session key must be derived from a one-time-use parameter. This measure can prevent impersonation or replay attacks.

3 The proposed authentication scheme

This section presents the proposed anonymous authentication scheme for a mobile satellite communication system, which enables NCC and users to simultaneously negotiate the shared session key.

Initially, a cryptosystem based on secure one-way hash function, such as SHA-2 or SHA-256 [23,24], is established. Following the registration of a mobile user at NCC, the NCC generates an authentication token for this mobile user with its long-term private key and deduces the user's master key. This master key can only be computed from the NCC's long-term private key by NCC.

Before communicating with NCC, the mobile user computes a message authentication code (MAC) and sends it to NCC. Upon receiving the MAC code, NCC recovers the user master key to verify the received MAC. If it holds, NCC deduces the session key shared with the user from the user master key and the corresponding temporary identity. Then NCC generates a new temporary identity used in the next authentication phase by the user. The new temporary identity of the user is encrypted with the old one using the deduced session key. This encrypted message is sent to the user with its MAC as a response. Once the user has checked the validity of received MAC, the scheme ends. Clearly, the proposed scheme does not involve a PKC, a SKC, a PKI and certificate stored in the mobile user's computer. The proposed scheme consists of two phases: registration and authentication. Notations used in this paper are defined as follows:

- U, NCC: two communicating parties, a user and the network control center;
- U_{ID}, T_{ID}, and LEO_{ID}: the identity of a mobile user, the temporary identity of a mobile user, and the identity of a LEO satellite, respectively;
- x: a long-term private key of NCC;
- $X \rightarrow Y : M$: a party X delivers a message M to another party Y;
- $h(\cdot)$: a secure one-way hash function, such as SHA-2 or SHA-256 [23,24];
- $MAC_k(\cdot)$: a message authentication code (MAC) involving a key k;
- $\oplus$: a bit-wise exclusive-or operation;

3.1 Registration phase

Figure 2 illustrates the proposed registration phase. Assume that NCC owns its long-term private key x. During the registration phase, a mobile user U requests to be a legal user from the system and NCC does the following operations:

R1. $U \rightarrow NCC$: U_{ID} A mobile user U selects its identity U_{ID} freely and then submits it to NCC via a secure channel.

R2. $NCC \rightarrow U$: Smart card(T_{ID}, key)

For each mobile user U with an identity U_{ID} in the system, NCC decides an initialized temporary identity T_{ID}, which is refreshed for the next authentication after each successful authentication. Afterward, NCC generates the user master key key = $h(U_{ID}, x)$. NCC stores $\{T_{ID}$, key$\}$ onto the user's smart card and then releases it to the mobile user U via a secure channel. Finally, NCC computes $V = U_{ID} \oplus h(T_{ID}, x)$ and then stores $\{V, T_{ID}\}$ in the verification table. This operation is used to repel against an insertion attack in which an intruder inserts a verification item into the verification table.

3.2 Authentication phase

Figure 3 illustrates the proposed authentication phase. During the authentication phase, a mobile user U must be authenticated before communicating with another mobile user or accessing the resources in the system. In addition, he/she has to ascertain the identity of the network with whom he/she communicates. In the proposed authentication phase, we assume that *LEO* and *NCC* already established secure communication channel based on ordinal cryptographic techniques such as SSL protocol and TLS protocol [25]. The authentication phase goes as follows:

A1. $U \rightarrow LEO$: T_{ID}, mac_U If U wants to negotiate a session key sk with *LEO*, he/she does the following operations with mobile device:

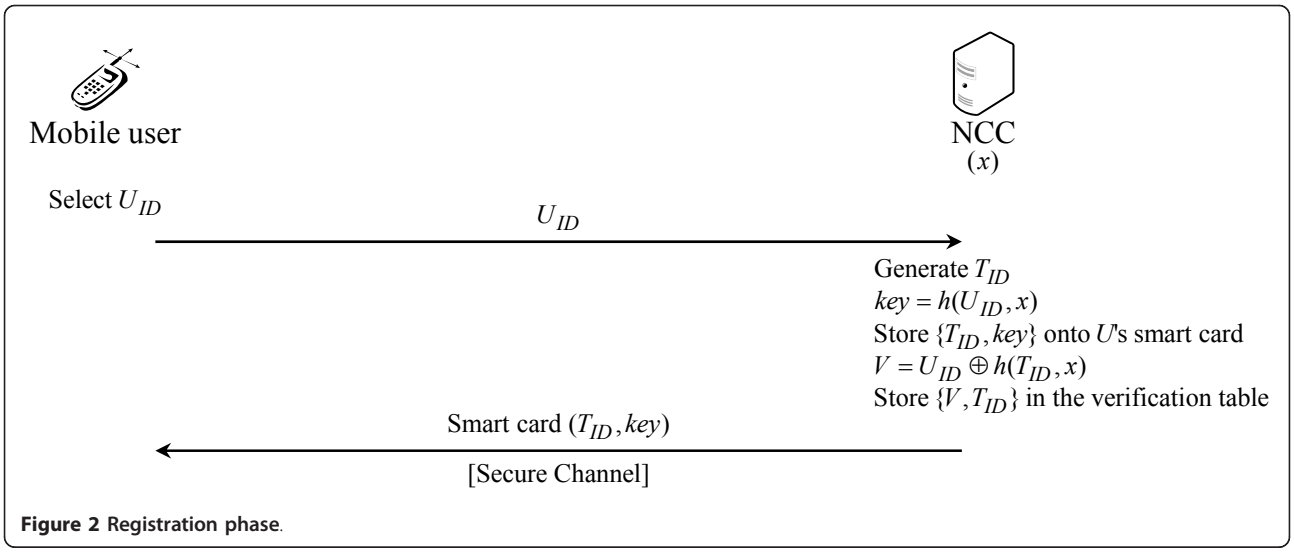

Figure 2 Registration phase.

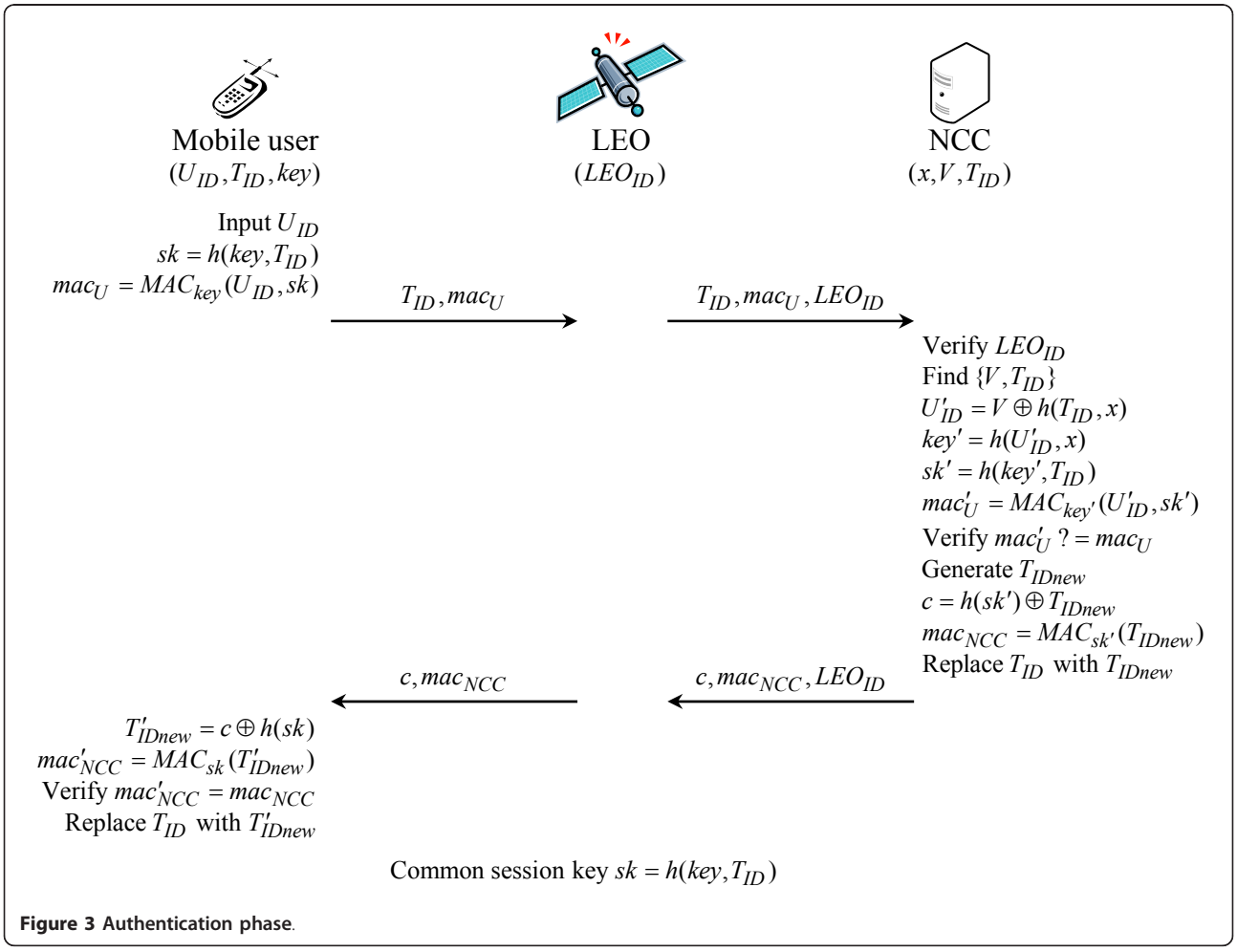

Figure 3 Authentication phase.

(a) Open the login application software using itself smart card into his/her mobile device and then input his/her identity U_{ID}.
(b) Compute the session key $sk = h(\text{key}, T_{ID})$, where T_{ID} is refreshed after one successful login.
(c) Compute a message authentication code $mac_U = MAC_{\text{key}}(U_{ID}, sk)$ and send it with T_{ID} to the *LEO*.

A2. $LEO \rightarrow NCC$: T_{ID}, mac_U, LEO_{ID} Upon receiving the authentication message from U, the *LEO* forwards it to the NCC by appending its identity LEO_{ID}.

A3. $NCC \rightarrow LEO$: c, mac_{NCC}, LEO_{ID} Upon receiving the message from *LEO*, the NCC checks the legitimacy of the *LEO* and does the following operations:

(a) Find the corresponding information $\{V, T_{ID}\}$ associated with T_{ID} by looking up the verification table, where $V = U_{ID} \oplus h(T_{ID}, x)$.
(b) Compute $h(T_{ID}, x)$ using its long-term secret key x and the received T_{ID}
(c) Extract U's identity U'_{ID} by computing $V \oplus h(T_{ID}, x)$ as follows:

$$\oplus h(T_{ID}, x) = U_{ID} \oplus h(T_{ID}, x) \oplus h(T_{ID}, x) = U'_{ID}V$$

(d) Compute the possible user master key $\text{key}' = h(U'_{ID}, x)$ using the extracted U'_{ID} and the possible session key $sk' = h(\text{key}', T_{ID})$.
(e) Compute $mac'_U = MAC_{\text{key}'}(U'_{ID}, sk')$ and check if mac'_U to the received mac_U. If this holds, the mobile user U is authenticated and the session key is confirmed; otherwise, this authentication request is rejected.
(f) Generate a new temporary identity TID_{new} and update the old T_{ID} with $T_{ID_{\text{new}}}$ in the verification table for next time to authentication.
(g) Computes $c = h(sk') \oplus T_{ID_{\text{new}}}$ and a message authentication code $mac_{NCC} = MAC_{sk'}(T_{ID_{\text{new}}})$. Then return $\{c, mac_{NCC}, LEO_{ID}\}$ to the *LEO*.

A4. $LEO \rightarrow U$: c, mac_{NCC} The *LEO* just forwards c and mac_{NCC} to U.

A5. Once U receives c and mac_{NCC}, he/she extracts the new temporary identity $T'_{ID_{\text{new}}}$ using c and sk by computing $c \oplus sk$ as follows:

$$c \oplus sk = h(sk') \oplus T_{ID_{\text{new}}} \oplus sk = T'_{ID_{\text{new}}}$$

U then computes $mac'_{NCC} = MAC_{sk}(T'_{ID_{\text{new}}})$ and checks if mac'_{NCC} is equal to the received mac_{NCC}. If this holds, the mobile user ascertains the identity of NCC and replaces T_{ID} with $T'_{ID_{\text{new}}}$ for the next authentication. At the same time, the session key sk is mutually confirmed.

U and NCC uses the one-time session key $sk = h(\text{key}, T_{ID})$ to protect (e.g., encrypt) further information exchanged in the session.

4 Discussion and security analysis

This section discusses whether the above-required essential properties in a mobile satellite communication network can all be satisfied in the proposed authentication scheme. In addition, we analyze the security of the proposed scheme against diverse attacks.

4.1 Discussion of the required essential properties

(1) *Mutual authentication*: Mutual authentication between U and NCC is achieved, because both are able to deduce U's master key $\text{key} = h(U_{ID}, x)$ and the identical session key $sk = h(\text{key}, T_{ID})$. In step A1 of the proposed scheme, U sends a MAC message $mac_U = MAC_{\text{key}}(U_{ID}, sk)$ as a authentication request to NCC, and then, NCC authenticates U by verifying if U knows/possesses master secret key *key*. If U is legal, it can generate sk to encrypt the new temporary identity $T_{ID_{\text{new}}}$ and another MAC message $mac_{NCC} = MAC_{sk'}(T_{ID_{\text{new}}})$ as a response to U. Accordingly, U can authenticate NCC by verifying the MAC mac_{NCC}. Therefore, the proposed scheme provides secure mutual authentication.
(2) *Confidential communication*: In the proposed scheme, communication between U and NCC is kept confidential by encrypting the messages (e.g., NCC's response message $c = h(sk') \oplus T_{ID_{\text{new}}}$ with the shared session key $sk = h(\text{key}, T_{ID})$. Furthermore, the shared session key sk is simultaneously confirmed by both participants before performing their subsequent communication. Therefore, the proposed scheme provides confidential communication.
(3) *User's privacy*: In the proposed scheme, U's identity U_{ID} is never transmitted over the public network for authentication purposes. In addition, a different temporary identity T_{ID} is used in each session to keep the privacy of U. Since T_{ID} is unlinkable, *LEO* and gateway does not have any idea who is communicating with NCC. Therefore, the proposed scheme provides user's privacy.
(4) *Low computation and update cost*: Since there is no exponential computation and symmetric computation required on both sides during the authentication phase in the proposed scheme, but only a few hashing operations, the proposed scheme is efficient and easy to implement on mobile devices. Therefore,

the proposed scheme provides low computation and update cost.

(5) *Simple key management*: In the proposed scheme, the key management is very simple since only the long-term private key x of NCC is maintained in the system. As the key is used only by NCC itself, there is no PKI required. Furthermore, no sensitive information is stored in NCC. This implies that even from a compromised NCC, no secret keys can be obtained. Therefore, the proposed scheme provides simple key management.

(6) *Minimum trust*: In the proposed scheme, no other trust parties are required except NCC. It is reasonable to assume that NCC is trustworthy since U must register at NCC with their private information to obtain services. Therefore, the proposed scheme provides minimum trust.

(7) *Session independence*: The fresh session key sk is not deduced from the last session key, and there is no relationship among the session keys. Once the past session key is compromised for some reasons, an adversary trying to mount a known key attack can derive the newer session keys only in case that he/she knows the master key key = $h(U_{ID}, x)$. Therefore, the proposed scheme provides session independence.

The required essential properties of the proposed scheme is compared with the schemes in [12,14,15], and [16] in Table 1. It can be seen that only the proposed scheme can fulfill the seven criteria for designing an authentication scheme for mobile satellite communication systems.

4.2 Security analysis

(1) *Insertion attacks*: Assume that an attacker is able to intrude NCC and then inserts a fake ($V = U_{ID} \oplus h(T_{ID}, x)$, T_{ID}) into the verification table. If he/she wants to impersonate a legal user U, he/she must be able to deduce the same master key key = $h(U_{ID}, x)$ which would be deduced by NCC from the fake (V, T_{ID}). However, he/she has no idea about the long-term private key x to solve U_{ID} from $V = U_{ID} \oplus h(T_{ID}, x)$ like NCC does. He/she fails to impersonate a legal user without knowing U's identity U_{ID}. Therefore, the proposed scheme is secure to insertion attacks.

(2) *Stolen-verifier attacks*: In the proposed scheme, the verification table does not contain any sensitive information. If an attacker steals the verification table, he/she has no efficient way to solve U's identity U_{ID} or the long-term private key x from $V = U_{ID} \oplus h(T_{ID}, x)$ and T_{ID} without knowing x or U_{ID}. Therefore, the proposed scheme is secure to stolen-verifier attacks.

(3) *Secret key guessing attacks*: The only secret on the user side is the user master key key = $h(U_{ID}, x)$. The key is a strong secret key with long enough bits and protected in a tamper-resistant mechanism such as a smart card. There is no efficient way to obtain it, but brute-force guessing. Therefore, the proposed scheme is secure to secret key guessing attacks.

(4) *Replay attacks*: NCC generates a new temporary identity $T_{ID_{\text{new}}}$ after a successful authentication. Since the temporary identity T_{ID} is used only once, the derived session key $sk = h(\text{key}, T_{ID})$ is changed in each session. Therefore, the authentication message $mac_U = MAC_{\text{key}}(U_{ID})$ and NCC's response messages $(c, mac_{NCC} = MAC_{sk'}(T_{ID_{\text{new}}}))$ are renewed each time. Therefore, the proposed scheme is secure to replay attacks.

(5) *Impersonation attacks*: An attacker may impersonate a legal user by forging an authentication request $\{T_{ID}, mac_U = MAC_{\text{key}}(U_{ID}, sk)\}$. As NCC should check the validity of the MAC message by computing the user master key key = $h(U_{ID}, x)$ and the session key $sk = h(\text{key}, T_{ID})$ to generate the same MAC, the attacker must know how to compute key and sk; otherwise, he/she cannot pass the authentication. However, he/she has no feasible way to know these

Table 1 Comparisons of essential properties for mobile satellite communication systems

	Cruickshank	Hwang et al.	Chang et al.	Chen et al.	Proposed
Mutual authentication	Yes	Yes	Yes	Yes	Yes
Confidentiality	Yes	NA	NA	Yes	Yes
User's privacy	No	Yes	No[b]	Yes	Yes
Low computation cost	No	No	No[c]	No	Yes
Simple key management	No	No	Yes	Yes	Yes
Minimum trust	No[a]	Yes	Yes	Yes	Yes
Session independence	Yes	No	Yes	Yes	Yes

NA: not addressed

[a] CAs are required

[b] Partial privacy

[c] Depending on the access times that the NCC provides

two keys. Therefore, the proposed scheme is secure to impersonation attacks.

4.3 Performance analysis

This subsection provides the performance analysis in terms of communication costs. Since there is no exponential computation required on both sides during the authentication phase in the proposed scheme, but only a few hashing operations, the proposed scheme is efficient and easy to implement on mobile devices. A comparison of the computation complexity among related works is shown in Table 2. On the side of the mobile user U, there are one hash function operations and two MAC operations. On the other hand, there are four hash function operations and two MAC operations employed on the side of NCC. Clearly, the proposed scheme is more computationally efficient compared to Cruickshank's scheme [12] involving four asymmetric cryptographic operations, Hwang et al.'s scheme [14] involving four symmetric cryptographic operations, Chang et al.'s scheme [15] involving (N-(j-1))+3 times of hash function operations in the jth authentication, where the system parameter N is the number of times of contact with NCC, and NCC has 3 hash function operations, and Chen et al.'s scheme [16] involving two symmetric cryptographic operations. In Chen et al.'s scheme, for repelling an insertion attack in which an intruder inserts a verification item into the verification table, NCC always must verify if $g^s = y^{h(U_{ID})} \cdot r^{r^{-1}} \bmod p$ holds during the authentication phase. We can see that the equation requires three exponential computations. Chen et al. claimed that these operations could be performed either off-line or by another authentication server in order to reduce complex computations. However, these solutions may cause increased communication delay. Moreover, Chen et al. did not explained the computation costs in their performance analysis to solve k from $s = h(U_{ID})x + kr^{-1} \bmod q$ by NCC. We can see that it requires much time to find a random number x which satisfies the equation $s = h(U_{ID})x + kr^{-1} \bmod q$ because of the random number k, $1 \le k < q$, where q is a large prime factor of p - 1. On the other hand, the proposed scheme does not require any symmetric and asymmetric operations. Therefore, the proposed scheme is more efficient compared with previous related schemes [12,14-16].

4.4 Formal proofs

This subsection proves the security of the proposed authentication scheme based on random oracle model [26-28].

4.4.1 Security model

Communication Communication between NCC and U is provided via a wireless network, upon which third parties can easily eavesdrop and which is easily cut or disturbed. Therefore, we describe the communications in an RFID system using two players–client and server.

Client In the proposed scheme, we suppose small mobile devices as clients. The clients only have poor electronic power provided by servers and can only perform light calculations.

Server In the proposed scheme, we imagine NCC and LEO as servers. Generally, a mobile user communicates with LEOs through wireless channels, and then the LEOs communicate with NCC servers through secure channels. We assume that the communication between NCC and LEO is secure using ordinal cryptographic techniques such as SSL and TLS. Therefore, we describe the communications in a mobile satellite communication system using two players–client (Mobile user) and server (NCC).

Functions Let functions (FR(), SR(), $CheckC$(), $CheckS$()) be indexes of the client U_{ID} and secret key key. Intuitively, each function means the following. FR() is responses from server to client (i.e., mobile user). SR() is the returning responses from client (i.e., mobile user) to server. $CheckC$() means the verification check of the client's output by the server. $CheckS$() is the result of verification check of the server's output by the client. SK() is the key updating processes.

Oracles Security notions for robust mutual authentication protocols are defined by the success probability of the adversary, which is allowed to access the oracles.

Table 2 Comparisons of computation complexity in the authentication phase

	Cruickshank	Hwang et al.	Chang et al.	Chen et al.	Proposed
Hash operations	-	-	*N-(j-1)+3/3	1/3	1/4
MAC operations	-	-	-	1/1	2/2
Symmetric operations	1/1	2/2	-	1/1	-
Asymmetric operations	1/1	-	-	(0/3)	-
Equation solving operations	-	-	-	k	-

*jth authentication request

k means computation time to solve k from $s = h(U_{ID})x + kr^{-1} \bmod q$

() means off-line or another authentication server's operations

We first show oracles that the adversary can access. S^O and C^O are oracles as server' output and client' output. FR^O, SR^O, and SK^O are oracles as functions used in server or client.

4.4.2 Security proofs

The goal of our authentication scheme is to achieve mutual authentication that preserves privacy. We prove that the proposed scheme satisfies the above security notions using a game style proof technique. The security proof based on Ohkubo et al.'s model [28] is adopted to proof the mutual authentication and security of the session key in the proposed scheme. The construction of the proofs is as followings. The proofs are constructed following game-based techniques. We make four steps as games as follows.

(1) *Game 0:* Simulator *SIM* executes simulations following protocols.
(2) *Game 1:* Simulator *SIM* executes simulations setting the outputs of oracles random values, instead of the results of functions.
(3) *Game 2:* Excluding the case in which adversary accesses to oracles with the information of the secret key directly from the adversary's win.
(4) *Game 3:* Replying changed from challenge oracle *CO* to adversary and set the replying random values set regardless of coin-flipping results.

Through these games, we show that the adversary in the protocol (i.e., Game 0) is in the same situations in that it is given no information related to the secret key, and there are no means other than random guessing.

Definition 1 *Secure two-party authentication protocol: A two-party authentication (TPA) protocol is secure in our model if the following requirements are satisfied:*

Validity: When the protocol is run among two oracles (a client and a server) in the absence of an active adversary, the oracles accept the same key.

Indistinguishability: For all probabilistic, polynomial-time adversaries AD, $Adv_{TPA}^{AD}(k)$ *is negligible.*

As a result, the following theorems are shown.

Theorem 1 *The proposed authentication scheme TPA is secure, if hash functions* $h(\cdot)$ *and* $MAC(\cdot)$ *are random oracles.*

Proof Adversary A_{TPA} is allowed to access the oracles, S^O, C^O, FR^O, SR^O, SK^O. Let the maximum number of queries be q times and the size of secret key *key* be n bits. In addition, the adversary A_{TPA} can use the simulator *SIM* to perform the Games 0, 1, 2, 3. From Games 0, 1, 2, and 3, we can conclude the following A_{TPA}^{AD}'s advantages.

$$\begin{aligned} Pr[A_{TPA}^{AD} \text{ in Game 0}] &= Pr[A_{TPA}^{AD} \text{ in Game 1}] \\ &\le Pr[A_{TPA}^{AD} \text{ in Game 2}] + \frac{q}{2^n} \\ &= Pr[A_{TPA}^{AD} \text{ in Game 3}] + \frac{q}{2^n} \\ &= \frac{1}{2^n} + \frac{q}{2^n} \\ &= \frac{q+1}{2^n} \end{aligned} \quad (1)$$

From the Equation (1), we can obtain the following A_{TPA}^{AD}'s advantages.

$$Pr[A_{TPA}^{AD} \text{ in Game 0}] = \frac{1}{2} + \varepsilon_{TPA} \le \frac{1}{2^n} + \frac{q}{2^n} \quad (2)$$

From the Equation (2), we can say that

$$\varepsilon_{TPA} \le \frac{q}{2^n} \quad (3)$$

As a result, it can be shown that the proposed *TPA* scheme is secure two-party authentication protocol, if $q \ll 2n$ and $h(\cdot)$, $MAC(\cdot)$ are random oracles. Due to space limitations, we omit the detailed proof, as it is almost similar to the Ohkubo et al.'s proof method (see Proofs 1 ~ 4 of Appendix) [28]. Readers are referred to [28] for more complete references.

5 Conclusion

Based on Chen et al.'s scheme, this paper proposed a new efficient and secure anonymous authentication scheme for mobile satellite communication systems. Compared with the related schemes, the proposed scheme achieves the following three main advantages: (1) It is just based on a secure one-way hash function for avoiding complex computations for both mobile users and network control center (NCC), (2) it does not require sensitive verification table which may cause NCC to become an attractive target for numerous attacks, and (3) it provides higher security level (secure mutual authentication and key establishment, confidential communication, user's privacy, simple key management, and session key independence). In addition, the proposed scheme not only is secure against well-known cryptographical attacks such as insertion attacks guessing attacks, stolen-verifier attacks, secret key guessing attacks, replay attacks, and impersonation attacks but also provides secure mutual authentication and session key establishment. As a result, we believes that the proposed scheme is very suitable for lightweight-device environments since it provides security, reliability, and efficiency.

Acknowledgements
We would like to thank the anonymous reviewers for their helpful comments. This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(no. 2010-0010106) and partially supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency(NIPA-2011-(C1090-1121-0002)). The authors declare that they have no competing interests.

Author details
[1]School of Computer Engineering, Kyungil University, 33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea [2]School of Computer Science and Engineering, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, Republic of Korea [3]Korea Institute of Science and Technology Information, 335 Gwahangno, Yuseong-Gu, Daejeon 305-806, Republic of Korea [4]Satellite Information Research Institute, Korea Aerospace Research Institute, 45 Eoeun-Dong, Yuseong-Gu, Daejeon 305-333, Republic of Korea

Competing interests
The authors declare that they have no competing interests.

Received: 6 January 2011 Accepted: 1 September 2011
Published: 1 September 2011

References

1. G Comparetto, R Ramirez, Trends in mobile satellite technology. IEEE Comput. **30**(2), 44–52 (1999)
2. SS Jeng, HP Lin, Smart antenna system and its application in low-earth-orbit satellite communication systems, in Proceedings of the Microwaves. Antennas and Propagation **146**(2), 125–130 (1999)
3. KY Lam, SL Chung, M Gu, JG Sun, Lightweight security for mobile commerce transactions. Comput Commun. **26**(18), 2052–2060 (2003). doi:10.1016/S0140-3664(03)00188-9
4. HY Lin, Security and authentication in PCS. Comput Electr Eng. **25**(4), 225–248 (1999). doi:10.1016/S0045-7906(99)00010-5
5. HY Lin, L Harn, Authentication protocols for personal communication systems. ACM SIGCOMM Comput Commun Rev. **25**(4), 256–261 (1995). doi:10.1145/217391.217456
6. M Spreitzer, M Theimer, Secure mobile computing with location information. Commun ACM. **36**(7), 27 (1993). doi:10.1145/159544.159558
7. WAP forum, wireless application protocol, wireless transport layer security specification; version (12-Feb-1999) http://www.wapforum.org
8. RC Ayan, SB John, Energy-efficient source authentication for secure group communication with low-powered smart devices in hybrid wireless/satellite networks. EURASIP J Wirel Commun Netw, 1–18 (2011). Article ID **392529**
9. B Francesco, B Cecilia, AC Enzo, C Stefano, EC Giovanni, N Massimo, P Claudio, P Marco, R Stefano, VC Alessandro, LTE adaptation for mobile broadband satellite networks. EURASIP J Wirel Commun Netw, 1–13 (2009). Article ID **989062**
10. ES Ray, D Anton, VC Alessandro, Satellite communications. EURASIP J Wirel Commun Netw, 1–2 (2007). Article ID **058964**
11. G Thierry, B Pascal, A QoS architecture for DVB-RCS next generation satellite networks. EURASIP J Wirel Commun Netw, 1–9 (2007). Article ID **58484**
12. HS Cruickshank, A security system for satellite networks. in *Proceedings of the IEEE Satellite Systems for Mobile Communications and Navigation*, 187–190 (1996)
13. C Ellison, B Schneier, Ten risks of PKI: what you're not being told about public-key infrastructure. Comput Secur J. **16**(1), 1–7 (2000)
14. MS Hwang, CC Yang, CY Shiu, An authentication scheme for mobile satellite communication systems. ACM SIGOPS Oper Syst Rev. **145**(2-3), 42–47 (2003)
15. YF Chang, CC Chang, An efficient authentication protocol for mobile satellite communication systems. ACM SIGOPS Oper Syst Rev. **39**(1), 70–84 (2005). doi:10.1145/1044552.1044560
16. TH Chen, WB Lee, HB Chen, A self-verification authentication mechanism for mobile satellite communication systems. Comput Electr Eng. **35**(1), 41–48 (2009). doi:10.1016/j.compeleceng.2008.05.003
17. A Aziz, W Diffe, Privacy and authentication for wireless local area networks. IEEE Pers Commun First Quart. **1**(1), 25–31 (1994)
18. GA Safdar, MP O'Neill, Performance analysis of novel randomly shifted certification authority authentication protocol for MANETs. EURASIP J Wirel Commun Netw, 1–11 (2009). Article ID **243956**
19. R Jian, L Yun, L Tongtong, SPM: source privacy for mobile ad hoc networks. EURASIP J Wirel Commun Netw, 1–10 (2010). Article ID **534712**
20. V Vijay, O Diethelm, S Jaleel, JH Antoni, J Sanjay, Broadcast secrecy via key-chain-based encryption in single-hop wireless sensor networks. EURASIP J Wirel Commun Netw, 1–12 (2011). Article ID **695171**
21. JM Li, YH Park, X Li, A USIM-based uniform access authentication framework in mobile communication. EURASIP J Wirel Commun Netw, 1–12 (2011). Article ID **867315**
22. JY Huang, IE Liao, HW Tang, A forward authentication key management scheme for heterogeneous sensor networks. EURASIP J Wirel Commun Netw, 1–10 (2011). Article ID **296704**
23. B Schneier, *Applied Cryptography*, 2nd edn. (Wiley, New York, 1996)
24. N Sklavos, O Koufopavlou, Implementation of the SHA-2 hash family standard using FPGAs. J Supercomput. **31**(3), 227–248 (2005). doi:10.1007/s11227-005-0086-5
25. R Oppliger, R Hauser, D Basin, SSL/TLS session-aware user authentication. IEEE Comput. **41**(3), 59–65 (March 2008)
26. M Bellare, P Rogaway, Provably secure session key distribution: The three party case, in *Proceedings of 27th ACM Symposium on the Theory of Computing*, 57–66 (1995)
27. M Bellare, D Pointcheval, P Rogaway, Authenticated key exchange secure against dictionary attacks, in *Proceedings of Eurocrypt 2000, LNCS*. **1807**, 139–155 (2000)
28. M Ohkubo, S Matsuo, Y Hanatani, K Sakiyama, K Ohta, Robust RFID authentication protocol with formal proof and its feasibility, Cryptology ePrint Archive Report 2010/393, 1–23

doi:10.1186/1687-1499-2011-86
Cite this article as: Yoon *et al.*: An efficient and secure anonymous authentication scheme for mobile satellite communication systems. *EURASIP Journal on Wireless Communications and Networking* 2011 **2011**:86.