An Authentication Scheme for Mobile Satellite Communication Systems

Min-Shiang Hwang† Chao-Chen Yang‡ Cheng-Yeh Shiu†

Department of Information Management,†
Department of Information and Communication Engineering,‡
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.
Email: mshwang@mail.cyut.edu.tw

Abstract

This paper discusses the security aspects of a registration protocol in a mobile satellite communication system. We propose a new mobile user authentication and data encryption scheme for mobile satellite communication systems. The scheme can remedy a replay attack.
Keywords: Authentication, cryptography, mobile satellite communication system, security.

I Introduction

Wireless communications have continuously advanced through recent times. Wireless communication systems are closely related to our daily life. The innovative wireless techniques are developed through continuous invention. The Mobile Satellite Communication System (MSCS) is the present culmination of this continuous research and development.

Numerous satellite communication systems have been developed. These mobile communication systems have some common characteristics: large broadcasting range and communication area. Because of these characteristics, satellite communications do not have geographic or environmental limitations (dead space). Satellite systems can communication around the globe. Therefore, the best communications system for out of the way terrain or tall mountain ranges is a mobile satellite communication system.

To ensure stability, a central satellite-processing unit is used in the stability model. The computation ability of this processing unit is not powerful, so the satellite cannot perform complex computations. Moreover, the available communication bandwidth is not always sufficient for satellite communication systems. Other research has been aimed at this same problem [2].

The traditional satellite communication system is placed in Geostationary Earth Orbit (GEO). Because the GEO distance is far from the earth there is a signal communication delay problem. GEO is therefore not fit for use in a personal Communication System (PC-S). Low Earth Orbit (LEO) satellite communication systems have recently been developed. In general, the LEO satellite communication system constitutes exact global MSCS using sixty-six LEO satellites [5]. The LEO satellite orbits closer to the earth than the GEO satellite. There are three main advantages in LEO satellite systems: the signal communication attenuation is small, the signal communication delay time is short, and the data communication channels are wide but narrower than GEO. Therefore, the LEO satellites are fit for use in PCS [3].

Communication security has always been an important issue [7, 8]. A satellite communications system communicates with wireless messages. Because the data is transmitted over the air, transmitted data is easy to steal or falsify. Security for wireless communications is thus an important research topic [10].

There are two security requirements for communication systems. One is that an eavesdropper cannot intercept messages during the communication. Two is that the service is not obtained fraudulently in order to avoid usage charge; that is prevention of fraud by ensuring that the user's portable units are authentic. Since the main purpose of LEO satellite is only to forward messages to the receiver, the LEO satellite are not provided powerful computation. It is important research topic that how to authenticate a legal user for mobile satellite communication systems with low computations.

In 1996, Cruickshank proposed an authentication protocol for satellite networks [4]. His protocol uses a public-key cryptosystem for mutual authentication between the mobile user and satellite network and uses a secret key to encrypt confidential data. The authentication protocol encryption/decryption uses complex computations. The mobile user must have a large and powerful computation unit to comply with this protocol. Although this protocol can satisfy the above two security requirements, it is high computation for LEO satellite systems. In this paper, we propose an efficient authentication protocol for LEO satellite systems.

Communications security is important in a LEO satellite communication system. In this paper, we propose a secure scheme for mobile user authentication and secure communications. In the next section, the LEO mobile satellite communication system is introduced. We introduce our scheme in Section 3. Section 4 gives a security analysis of our scheme. Finally, Section 5 gives some concluding remarks.

II LEO Satellite Communication System

The LEO satellite communication system is comprised of LEO satellites, a gateway, mobile users and a Network Control Center (NCC) [9]. Many LEO communication systems have been developed [5]. The LEO satellite manages communications between the mobile user and the gateway, a mobile user and other mobile users, a gateway and other gateways, a gateway and the NCC, or LEO satellite with other LEO satellites in the system (shown in Figure 1). The gateway presides over communications with NCC and LEO satellites. Moreover, it is connected with local telecommunications systems to produce a diversified communications system [6].

The LEO satellite orbit is near the earth. The communication signal delay time is short, and the signal weakness is slight. The satellite provides a broad communication bandwidth [1]. The LEO communication range is smaller by virtue of its nearness to the earth. The LEO orbit time is short. The orbit is always between two and four hours. This orbit time prevents communication breaks. When the LEO leaves its communication station, the signal is handed over to the next LEO. The mobile users and satellites have a hand-over problem in the LEO satellite communication system.

III Our Scheme

There are two phases in our scheme: mobile user registration and the mobile user authentication phase. We use a session key to encrypt confidential data. We introduce these phases in the next sub-sections.

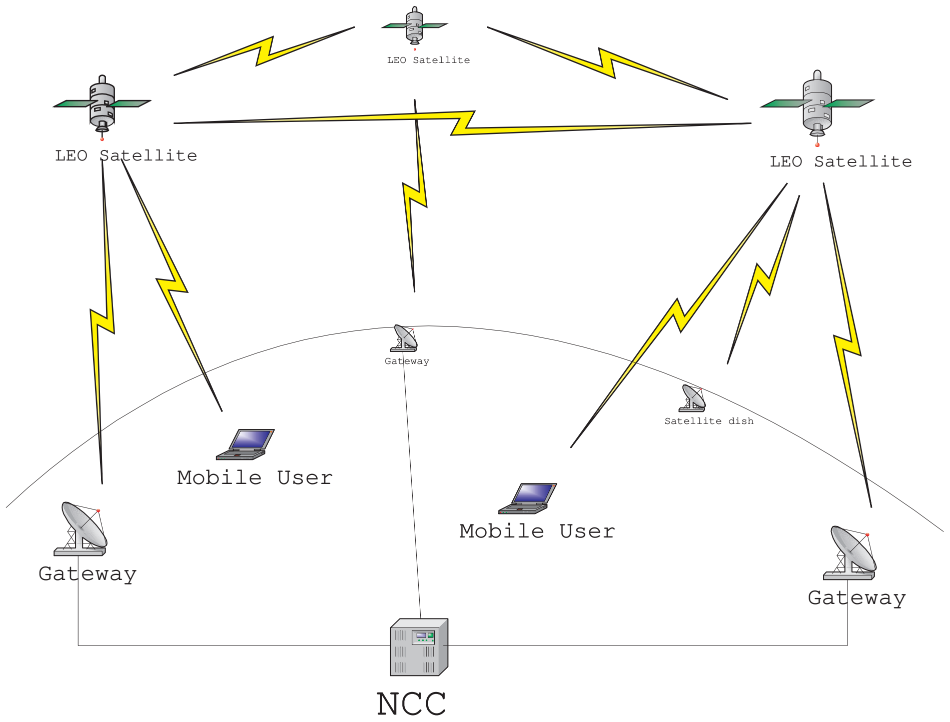

Figure 1: A simple LEO satellite communication system

3.1 Mobile User Registration Phase

Before accessing a LEO satellite communications system service, the mobile user must register as a legal user in the system. The gateway allocates the new mobile user a permanent identity (U_{ID}), secret key (K_{md}), and a temporary identity (T_{ID}). The gateway sends the mobile user's identity to NCC over a secret channel. After the user registration phase, the mobile user stores a message (U_{ID}, T_{ID}, K_{md}) in private. The NCC stores these messages (U_{ID}, T_{ID}, K_{md}) and LEO_{ID} for each mobile user. Here, K_{md} denotes a secret key shared by the mobile user and the NCC. LEO_{ID} denotes the identity ID of LEO.

3.2 Mobile User Authentication Phase

When a mobile user wants to communicate with other mobile users, that mobile user must be authenticated. A mobile user authentication protocol is shown in Figure 2. Some notations in our proposed method are denoted as follows:

- AUTH Request: LEO sends a request for mobile user authentication.
- U_{ID}: A mobile user identity in the system.
- T_{ID}: A mobile user temporary identity in the system.
- K_{md}: A session key between the mobile user and NCC.
- $K_{md}(\cdot)$: A symmetric cryptosystem (i.e. DES-like) with secret key K_{md}.

The procedures of our scheme are shown as follows. The arrow indicates the direction of message transmission and the data after the colon is the transmitted message. For example,

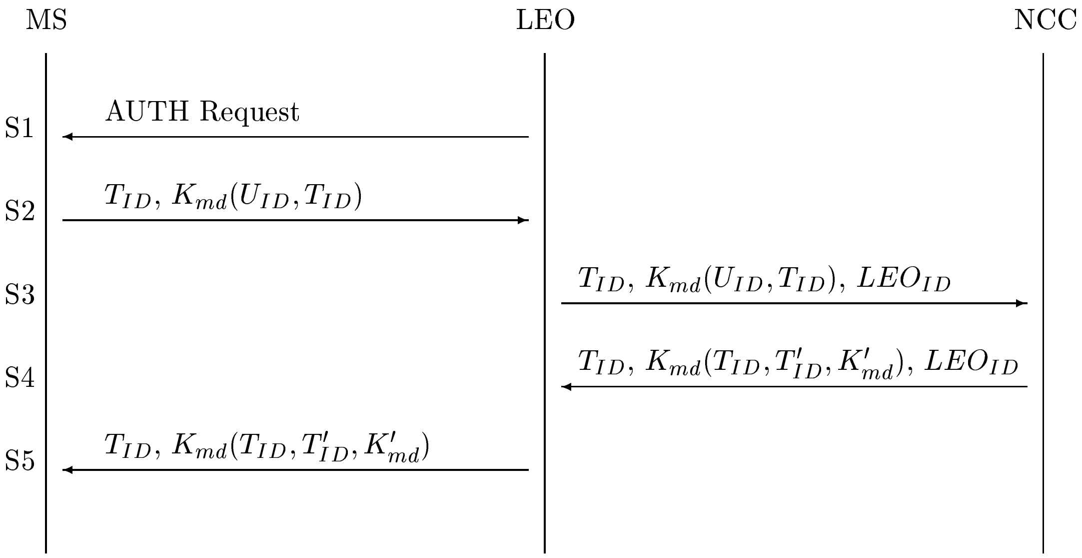

Figure 2: A mobile user authentication protocol

the statement, (LEO $\rightarrow$ MS: AUTH Request), means that the message (AUTH Request) is transmitted from LEO to MS.

- Step 1: LEO $\rightarrow$ MS: AUTH Request.
  LEO sends an authentication request to the mobile user.

- Step 2: MS $\rightarrow$ LEO: T_{ID}, $K_{md}(U_{ID}, T_{ID})$.
  When the mobile user receives the authentication request, the mobile user encrypts his/her identity U_{ID} and T_{ID} with the session key K_{md}. Then, the MS sends the encrypted message and T_{ID} to LEO.

- Step 3: LEO $\rightarrow$ NCC: T_{ID}, $K_{md}(U_{ID}, T_{ID}), LEO_{ID}$.
  When LEO receives the messages from the MS, it appends his/her identity ($LEO_I D$) to the message and sends the messages to the NCC.

- Step 4: NCC $\rightarrow$ LEO: T_{ID}, $K_{md}(T_{ID}, T'_{ID}, K'_{md}), LEO_{ID}$.

  1. NCC receives these messages from LEO. The NCC authenticates whether LEO_{ID} from the LEO is lawful. If the LEO is legal, NCC uses T_{ID} to obtain the session key between the MS and NCC using the lookup table. Next, the NCC obtains the mobile user's ID and T_{ID} by deciphering $K_{md}(U_{ID}, T_{ID})$. The NCC checks if the decrypted T_{ID} is equal to the antecedent T_{ID}. The NCC also checks U_{ID}.
  2. If the mobile user's ID is legal, the NCC randomly generates a new T'_{ID} and a new session key (K'_{md}) for the user and updates the new data in the database. The NCC encrypts the old T_{ID}, new T'_{ID}, and new K'_{md} with the old session key K_{md}. Next, the NCC sends the encrypted messages, the old T_{ID}, and LEO_{ID} to LEO.

- Step 5: LEO $\rightarrow$ MS: T_{ID}, $K_{md}(T_{ID}, T'_{ID}, K'_{md})$.
  When LEO receives the message, it confirms the LEO_{ID}, and forwards the messages to the mobile user.

- Step 6: MS.
  When the mobile user receives the message, the MS uses the old session key to decrypt the message (T_{ID}, T'_{ID}, K'_{md}) and verifies the old T_{ID}. The MS stores the new T'_{ID} and new session key K'_{md}. In the next communication, the mobile user uses the new T'_{ID} and session key for authentication.

IV Security Analysis

The mobile user identity U_{ID} is encrypted between MS and NCC. Therefore, the mobile user's location is protected.

The NCC generates a new T_{ID} for each mobile user in each session. The T_{ID} is used only one-time. An attacker cannot use the old T_{ID} to impersonate the mobile user.

Our scheme uses a session key to encrypt the messages. In order to avoid the replay attack, the NCC and the mobile user change their session keys in each session. It is difficult to use the guessing and replay attacks against our scheme. In addition, LEO does not know the session key. Therefore, it cannot decrypt and obtain the transmitted messages.

V Conclusion

We have proposed a simple authentication scheme for MSCS. The scheme not only reduces the computation but also enhances the security. In this study, we used a symmetric cryptosystem to attain this objective.

ACKNOWLEDGEMENTS

Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC91-2213-E-324-003.

References

[1] Prakash Chitre and Ferit Yegenoglu. Next-generation satellite networks: Architectures and implementations. *IEEE Communications Magazine*, pages 30–36, Mar. 1999.

[2] Jean-Noel Colcy, Geoff Hall, and Rafael Steinhauser. Euteltracs:the european mobile satellite service. *IEEE Communication Engineering*, pages 81–88, Apr. 1995.

[3] Gary Comparetto and Rafols Ramirez. Trends in mobile satellite technology. *IEEE Computer*, pages 44–52, Feb. 1997.

[4] H.S. Cruickshank. A security system for satellite networks. *IEEE Satellite System for Mobile Communication and Navigation*, pages 187–190, May 1996.

[5] Carl E. Fossa, Richard A. Raines, Gregg H. Gunsch, and Michael A. Temple. An overview of the IRIDIUM low earth orbit (LEO) satellite system. In *Proceedings of the IEEE 1998 National Aerospace and Electronics Conference, NAECON'1998*, pages 152–159, 1998.

[6] B. Gavish. Low earth orbit satellite based communication systems - research opportunities. *European Journal Of Operational Research*, 99(1):166–179, 1999.

[7] Min-Shiang Hwang. Dynamic participation in a secure conference scheme for mobile communications. *IEEE Transactions on Vehicular Technology 48(5)*, pages 1469–1474, Sep. 1999.

[8] Min-Shiang Hwang and Wei-Pang Yang. Conference key distribution protocols for digital mobile communication systems. *IEEE Journal on Selected Areas in Communications*, 13(2):416–420, Feb. 1995.

[9] S.S. Jeng and H.P. Lin. Smart antenna system and its application in low-earth-orbit satellite communication systems. *IEE Proceedings Microwaves, Antennas and Propagation*, 146(2):125–130, Apr. 1999.

[10] Hung-Yu Lin. Security and authentication in PCS. *Computers and Electrical Engineering*, pages 225–148, Dec. 1999.