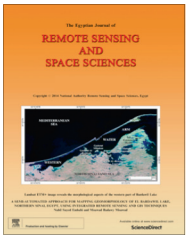
The Egyptian Journal of Remote Sensing and Space Sciences (2014) 17, 171–177

HOSTED BY

National Authority for Remote Sensing and Space Sciences

The Egyptian Journal of Remote Sensing and Space Sciences

www.elsevier.com/locate/ejrs
www.sciencedirect.com



RESEARCH PAPER

Verification of authentication protocols for mobile satellite communication systems

Reham Abdellatif Abouhogail

Electrical Quantities Metrology Dept., National Institute of Standards, Cairo, Egypt

Received 30 May 2013; revised 14 April 2014; accepted 7 July 2014
Available online 17 August 2014

KEYWORDS

Security;
Satellite communication systems;
Verification of protocols

Abstract In recent times, many protocols have been proposed to provide security for mobile satellite communication systems. Such protocols must be tested for their functional correctness before they are used in practice. Many security protocols for the mobile satellite communication system have been presented. This paper analyzes three of the most famous authentication protocols for mobile satellite communication system from the security viewpoint of data desynchronization attack. Based on strand spaces testing model, data desynchronization attacks on these protocols were tested and analyzed. Furthermore, improvements to overcome the security vulnerabilities of two protocols are mentioned.

1. Introduction

Nowadays, Mobile satellite communication systems have become one of the most important technologies. Security is a very important requirement in any system, especially in wireless communication systems. For a satellite user to communicate with other users, he must be authenticated first by the remote server. This paper is concerned with the authentication between mobile users and the remote server. Many mobile satellite communication systems have been proposed in recent years (Chang and Chang, 2005; Chen et al., 2009; Lasc et al., 2011; Eun-Jun et al., 2011; Lee et al., 2012; Cruickshank, 1996; Hwang et al., 2003). In the past, for more than 10 years the traditional satellite communication system that was used was the geostationary satellite. The geostationary satellite is located in geosynchronous equatorial orbit (GEO). Such a satellite returns to the same position in the sky after each sidereal day (Larson and Wertz, 1999). 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, low-earth-orbit (LEO) satellite communication systems are used for establishing personal communication systems as shown in Fig. 1. This is due to their large broadcasting range and communication area, small attenuation of the signals and a shorter transmission delay (Chen et al., 2009). There have been many researches on the authentication protocols for the mobile satellite communication system. Some protocols are based on public key cryptosystems like Cruickshank (1996) which involves heavy computation costs. In 2003, Hwang et al. (2003) proposed an authentication protocol using symmetric encryption to reduce the complexity of computations. But both Cruichshank's protocol and Hwang et al.'s protocol

E-mail addresses: rehlatif@yahoo.co, rehlatif@gmail.com
Peer review under responsibility of National Authority for Remote Sensing and Space Sciences.

1110-9823 © 2014 Production and hosting by Elsevier B.V. on behalf of National Authority for Remote Sensing and Space Sciences.
http://dx.doi.org/10.1016/j.ejrs.2014.07.002

were not good for forward secrecy and efficiency. In 2005, Chang and Chang (2005) proposed a new protocol to solve the weakness found in previous protocols. They used the Diffie–Hellman key exchange (Diffie and Hellman, 1976). But from our analysis in Section 3 we found that Change et al.'s protocol (Chang and Chang, 2005) is susceptible to data desynchronization attack. In 2009, Chen et al. (2009) proposed a protocol based on discrete logarithm problem. It overcomes the complexity of public key infrastructure, reduces the hard computation from the mobile user and does not require sensitive verification table for the NCC. But this protocol is susceptible to data desynchronization attack as will be declared in Section 4.

In 2012, Lee et al. (2012) pointed out that Change et al.'s protocol (Chang and Chang, 2005) lacked user anonymity and impersonation attack. Lee et al. proposed a new protocol that has low computation cost. He claimed that his protocol avoids previous security flaws. But this protocol is also susceptible to data desynchronization attack as will be declared in Section 5.

In our paper we presented an analysis for the three most famous authentication protocols for mobile satellite communication systems (Chang and Chang, 2005; Chen et al., 2009; Lee et al., 2012). We are concerned with the data desynchronization attack in our analysis for these protocols. We chose this type of attack for our analysis because this attack depends on jamming which is considered the most dangerous enemy in space communication. The notations in Table 1 are used throughout this paper.

2. Definition of strand spaces model

A strand is a sequence of actions executed by a single principal in a single local session of a protocol (Guttman, 2011). We enrich strands to allow them to synchronize with the projection of the joint state that is local to the principal P executing the strand. The actions on a strand are defined into: message transmissions, message receptions, and state synchronization events. Strands are used for the protocol and communication behavior (Guttman, 2011). A strand is a (linearly ordered) sequence of nodes $n_1 \Rightarrow \ldots \Rightarrow n_j$, each of which represents either:

Transmission of some message $\mathrm{msg}(n_i) = t_i$, graphically $\bullet \xrightarrow{t_i}$;
Reception of some message $\mathrm{msg}(n_i) = t_i$, graphically $\xrightarrow{t_i} \bullet$;

A strand is a sequence of transmission and reception events local to a particular run of a principal. If this principal is honest, it is a regular strand. If it is dishonest, it is a penetrator strand (Guttman and Javier Thayer Fabrega, 2001). A bundle C is a causally well-founded collection of nodes and arrows of both kinds. In a bundle, when a strand receives a message m, there is a unique node transmitting m from which the message was immediately received. By contrast, when a strand transmits a message m, many strands (or none) may immediately receive m. The height of a strand in a bundle is the number of nodes on the strand that are in the bundle (Guttman and Javier Thayer Fabrega, 2001). In the following sections an analysis of the most three famous schemes for mobile satellite authentication protocols is presented. Suggestions are presented to improve these schemes. We assume in the three presented protocols that the LEO satellite is always a trust node. During the paper, transmission of messages from the *NCC* to the user U means transmission from the *NCC* to the LEO, then transmission from the LEO to U. Also the opposite is correct. Transmission of messages from the user U to the *NCC* means transmission from U to the LEO, then transmission from the LEO to the *NCC*.

Table 1 Notations.

Notation	Interpretation
U	The mobile user
LEO	Low earth orbit satellite
NCC	Network Control Centre
P_n	The penetrator
U_{ID}, LEO_{ID}	User/LEO permanent identity
T_{IDu}	User temporary identity
sk	Session key
$\mathrm{MAC}_k(.)$	Keyed one-way hash function using the key k
$(m)_k$	Symmetric key encryption function for a message m using the key k
$H(.)$	One-way hash function
K_s	User's long term secret key
$\oplus$	XOR function
$\|\|$	Concatenation operator
P	Authentication token
x	Long term private key
y	Long term public key
L	Large Prime number

3. Data desynchronization attack on the CC protocol

3.1. The CC protocol

Chang and Chang proposed a mutual authentication mechanism (Chang and Chang, 2005) hereafter referred to as the CC protocol. In the CC protocol, the authentication between the mobile user and the network control center (*NCC*) is within a LEO satellite communication system. Mobile users are interconnected directly through LEO satellite links, while communication between satellites and the *NCC* is managed by Gateways. The CC protocol is composed of three phases: registration, authentication and mobile update.

3.1.1. The registration phase

In this phase, U has to register at the system. U is assigned a permanent identity U_{ID}, the secret key K shared between U and *NCC*, a temporary identity T_{IDu} by the gateway, and the number of times (N) that the mobile user can access the service before an update phase is required.

3.1.2. The authentication phase

The authentication phase is performed by U and *NCC* before any communication. Note that *NCC* stores (U_{ID}, T_{IDu}, LEO_{ID}, $H^{N+1-(j-1)}(K||U_{ID}||T_{IDu})$, $(N-(j-1))$) for U, and U keeps (U_{ID}, T_{IDu}, K, $(N-(j-1))$) at this stage. The details are described as follows:

Step 1: the LEO sends the authentication request to U.