International Journal of Mobile Computing and Multimedia Communications
Volume 12 • Issue 1 • January-March 2021

# Super Lightweight Mobile RFID Authentication Protocol for Bit Replacement Operation

Yubao Hou, Hunan International Economics University, China
Hua Liang, Hunan International Economics University, China
Juan Liu, Hunan Software Vocational Institute, China

## ABSTRACT

In the traditional RFID system, the secure wired channel communication is used between the reader and the server, and the new mobile RFID system is different from the traditional RFID system. The reader and the server communicate based on the wireless channel. This makes authentication protocols applicable to traditional RFID systems not applicable to mobile RFID systems. To solve this defect, a two-way authentication protocol MSB is proposed for ultra-lightweight mobile radio frequency identification system based on bit replacement operation. MSB (most significant bit) encrypts information based on bitwise operations, and the amount of computation of the communication entity is reduced. Tags, readers, and servers first authenticate and then communicate. MSB can be resistant to common attacks. The security analysis of the protocol shows that the protocol has high security attributes, and the performance analysis of the protocol shows that the protocol has the characteristics of low calculation volume. The formal analysis of the protocol is given based on GNY logic.

## KEYWORDS

Bit Replacement Operation (BRO), Mobile System, Mutual Authentication, Radio Frequency Identification (RFID), Ultra-Lightweight

## INTRODUCTION

With the development of information technology, RFID technology and communication network technology are bound to be deeply integrated. Optimistically in the long run, RFID technology has a broad prospect and is in the ascendant. However, due to cost, security risks, etc., the application of RFID is still subject to some restrictions and full of challenges.

Radio frequency identification technology appeared in the 1930s and 1940s, it was widely spread in the 1990s. Due to the limited technology at the time and the low demand from people, RFID technology was used in the RFID system application to exchange information between the reader and the server based on a wired connection. This exchange method is generally considered as safe and reliable. This system is called the traditional RFID system *(Liu D W, et al.,2016;Wang W C,et al.,2018)*.

In the 21st century, with the rapid development of science and technology and the growth of human needs, traditional RFID systems have been unable to meet people's needs, it leads to the emergence of mobile RFID systems *(Zhao T F, et al.,2019)*. The biggest difference between a mobile RFID system and a traditional RFID system is that the communication between the reader and the

DOI: 10.4018/IJMCMC.2021010104

server in the mobile RFID system is not based on a wired connection link, but a wireless connection line is used for information transmission. Due to its inherent properties, wireless links have certain security risks *(Xie R, et al.,2018;Bai Z & He Y G,2019)*. The mutual authentication protocol applicable to the traditional RFID system is no longer applicable to the mobile RFID system, so it is necessary to design a new mutual authentication protocol for the mobile RFID system.

The wireless communication network has three characteristics:

(1) Compared with wired network, wireless communication network has great openness;
(2) The wireless communication network is mobile;
(3) The transmission channel of the wireless communication network is unstable and will change.

It is precisely because of these three characteristics that the security problem of wireless communication networks is more serious than that of wired communication networks. The specific manifestations are as follows:

(1) The wireless communication network is vulnerable to monitoring attacks, and the signal will be intercepted;
(2) The wireless communication network is subject to insertion attacks, which leads to control of the wireless communication network system;
(3) Users can use wireless communication networks without authorization;
(4) The wireless communication network has obvious robustness;
(5) The mobile IP security problem of the wireless communication network is relatively serious;
(6) The wireless communication network will be subject to wireless interference.

Based on the security problem of wireless communication networks, an ultra-lightweight mutual authentication protocol for mobile RFID systems is presented based on bit replacement operations. In order to achieve the goal of reducing the computational load of communication entities, bit operations are used to encrypt the information in the designed protocol. At the same time, GNY logical formal analysis and security analysis of the protocol are carried out. GNY logic was proposed by Gong, Needham and Yahalom in 1990 *(Gong L, et al.,1990)*. It is a logic for analyzing authentication protocols. A completely different state search tool is used in GNY Logic, which includes a set of beliefs that are maintained by each topic and a set of inference rules to obtain new beliefs from old beliefs. BAN logic has a very simple and intuitive rule set, so it is easy to use. GNY logic can be used to find serious errors in the protocol, which has attracted widespread attention from security researchers. The application of GNY logic has epoch-making significance. It has greatly promoted the development of formal verification of security protocols and inspired many methods of formal verification of security protocols.

## 2. RELATED WORK

In the one-way authentication mobile authentication protocol, it is found that the protocol cannot resist man-in-the-middle attacks and replay attacks *(Sandhya M & Rangaswamy T R,2011)*. An elliptic curve mobile authentication protocol was proposed *(Zhou J, et al.,2012)*, but this solution could not ensure the privacy of the reader side. At the same time, the computational load on the label side is also large.

A lightweight mobile mutual authentication protocol was given *(Sun Z W & Li S,2019)*. The protocol's encryption of information was mainly based on the PUF (Physical Unclonable Function). Asynchronous attacks cannot be resisted in the protocol. The attacker can obtain the complete communication message by listening. When the communication entity's session is blocked, the attacker can replay the information which is obtained by listening multiple times, the encryption key