Ad Hoc Networks 71 (2018) 1–13

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

An enhanced authentication scheme in mobile RFID system

Shin-Yan Chiou[a,b,c,*], Shan-Yen Chang[a]

[a] Department of Electrical Engineering, College of Engineering, Chang Gung University, 259 Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan, Taiwan
[b] Department of Nuclear Medicine, Linkou Chang Gung Memorial Hospital, Tao-Yuan, Taiwan
[c] Center for Biomedical Engineering, Chang Gung University, Tao-Yuan, Taiwan

ARTICLE INFO

Article history:
Received 15 June 2017
Revised 19 October 2017
Accepted 15 December 2017
Available online 16 December 2017

Keywords:
Mobile RFID
Authentication
Privacy

ABSTRACT

The popularization of wireless networks and mobile applications has increased the importance of RFID technologies. However, since wireless networks does not guarantee transmission channel security, putting private user information at risk for unintentional disclosure. Previous research has introduced a security mechanism to provide privacy and authentication. This mechanism is based on quadratic residue, does not require a secure channel and fits EPC Class-1 Gen-2 specifications. However, this mechanism cannot resist replay attacks, and lacks an efficient means of its server is not able to find determining validating values, making it difficult to implement. This paper proposes an improvement scheme that uses virtual IDs and time parameters. It does not need a secure channel, fits EPC Class-1 Gen-2 specifications, is resistant to replay attacks, and can efficiently find validation information. The proposed scheme is applied to mobile devices as a proof of concept for use in wireless/mobile RFID systems.

1. Introduction

(Capability of RFID tags.) Radio Frequency Identification (RFID) systems [6,7,13] are a type of wireless communications technology. Such systems usually consist of a Reader, Tag and Server. The operating principle is that the sensor emits radio waves, sensing tags within the sensing range, causing the tag to operate through electromagnetic induction. Tags can be classed as active and passive. Active tags contain a battery, can autonomously send data, and feature stronger computing power. This study uses EPC Calss-1 Gen-2 standard passive tags, which rely on radio waves emitted by the Reader to drive electromagnetic induction. These tags have low computing power, and do not support computation-intensive algorithms, including symmetric encryption, asymmetric encryption, or hash functions. Currently, such passive tags are frequently found in stored value cards and library books.

(Security of mobile RFID readers.) Generally speaking, in RFID systems the reader is fixed in place, thus many studies combine the reader and server into a single unit. However, with the increased penetration of wireless/mobile networks, fixed equipment is gradually giving to wireless/mobile devices. However, this development has raised new problems. Compared to transmission channels for fixed devices, transmissions for wireless/mobile devices are more vulnerable to attack, thus raising serious safety and privacy concerns.

(RFID applications.) RFID systems have been used in a wider range of applications [14–16]. South Korea has installed RFID systems in taxis [10–12] to provide passengers with location information and thus protect their safety. Darianian et al. proposed a mobile RFID smart home system [4] which uses tags to identify various objects, allowing for automated response and control. In the future, mobile RFID equipment may be applied to electronic trading operations.

(Security of previous RFID systems.) Chen et al. [22] proposed an RFID authentication scheme by using hash functions and quadratic residues. However, their scheme is vulnerable to impersonation attacks. Chen–Deng [3] proposed a scheme which is based on CRC and PRNG and satisfies EPC Class-1 Gen-2 standards, but was highly vulnerable to impersonation attacks. In addition, to authenticate the Reader, the Tag had to perform $n+1$ CRC validations, thus making implementation difficult. Liu and Bailey [1] proposed a Privacy and Authentication Protocol in which the Tag and Reader use privacy status and a hash value to calculate a shared key to achieve privacy and authentication. However, this scheme is unable to ensure Tag anonymity or EPC Class-1 Gen-2 standards, and thus may be vulnerable to tracking and impersonation attacks. Yeh et al. [17] proposed a new RFID authentication scheme to improve Chen's scheme [22]. However, their scheme is unable to ensure EPC Class-1 Gen-2 standards and does not have reader-server insecurity assumption. Chen et al. [18] proposed a mutual authentication scheme for RFID conforming EPCglobal Class 1 Gen-

* Corresponding author at: Department of Electrical Engineering, College of Engineering, Chang Gung University, 259 Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan, Taiwan.
E-mail address: ansel@mail.cgu.edu.tw (S.-Y. Chiou).

https://doi.org/10.1016/j.adhoc.2017.12.004
1570-8705/

eration 2 standards. However, their scheme is vulnerable to tracking, impersonation and desynchronisation attacks. Cho et al. proposed a hash-based scheme [8] to provide transmission without the need for a secure channel. However, this scheme is vulnerable to desynchronisation attacks and impersonation attacks on the Tag and Reader, and the Tag uses hash calculations and thus does not meet the EPC Class-1 Gen-2 standard. Doss et al. proposed a method [5] that provides authentication for wireless/mobile RFID systems, and can ensure user privacy. However, in this scheme, the Server is unable to effectively find information for authentication and is vulnerable to replay attacks. Liao et al. proposed a method [11] which uses the ECC's new RFID scheme. Their scheme can be applied in RFID system, but it is vulnerable to impersonation or tracking attacks. Akgün et al. used physically unclonable functions (PUFs) to propose a mobile RFID authentication scheme [2], but this requires the tags to use a lot of hashes, and thus cannot meet the EPC C1G2 standard. Also, in this scheme the server does not participate in verification and is thus unable to ensure transmission security between the Reader and Server, making it inapplicable to mobile RFID systems.

(Proposed scheme.) This study proposes a secure and more efficient mutual authentication scheme for wireless/mobile RFID systems. The proposed scheme satisfies the EPC C1G2 standards, provides secure transmissions in wireless/mobile networks, and offers easier comparison and calculations for Server, Reader and Tag. It not only provides security properties such as tag anonymity, reader anonymity, and unforgeability, but also is resistant to tag-tracking attacks, reader-tracking attacks, replay attacks, and desynchronisation attacks. The security analysis is done based on the theorems and proofs with a formal proof method, random oracle model [26]. A proof of concept is executed on an Android smartphone, and the implementation time of the simulated results shows it is efficient.

(Paper content.) This paper is divided into eight sections. Section 2 describes the symbolic and security requirements, detailing the parameters and safety requirements for the proposed scheme. Section 3 reviews the relevant literature to explain and analyze the referenced schemes. Section 4 describes the security verification of the proposed method in detail. Section 5 analyzes the security of the proposed scheme, and investigates whether the proposed scheme can satisfy identity verification and privacy requirements, and whether it can provide secure transmission over wireless networks. Section 6 provides a comparison of system performance between the proposed method and others in terms of computation capacity, transmission frequency and transmission security. Section 7 describes an actual implementation on an Android smartphone. Section 8 presents conclusions.

2. Preliminary

2.1. Notations

Table 1 defines the symbols and parameters used in the proposed method. In the Table, p and q are two large prime numbers. In our scheme, only the *Server* and some Tags in the same group have the key k_{ST}. T_{th} is the defined time threshold such as two seconds.

2.2. Attacker model

In our scheme, any identity (i.e. *S, R*, or *T*) communicates with each other via an insecure public channel, offering adversaries opportunities to intercept. In the following, we present the assumptions of the attacker model [19–21].

(1) An adversary may eavesdrop on all communications between protocol actors over the public channel.

Table 1
Notations.

Notation	Description
p, q	Two large primes
k_{ST}	The shared key between Server and Tag
k_{ST_B}	The previous k_{ST}
k_{SR}	The shared key between Server and Reader
k_{SR_B}	The previous k_{SR}
t_X	The current time of X
T_{th_i}	The ith time threshold
ID_X	The ID of X
SID_X	The pseudo ID of X
$SID_X^{(S)}$	The pseudo ID of X in Server's database
$SIDB_X^{(S)}$	The previous pseudo ID of X in Server's database
$PRNG(\cdot)$	Pseudo random number generator

(2) An attacker can modify, delete, resend and reroute the eavesdropped message.
(3) An attacker cannot be a legitimate Server *S*.
(4) The attacker knows the protocol description, which means the protocol is public.

2.3. Security requirements

The proposed method's authentication scheme conducts mutual authentications and ensures the security of the transmitted data. Security requirements are described as Definition 1 below:

Definition 1 (Security requirements). The proposed scheme should meet the following conditions.

(1) Tag anonymity. Aside from the Server, the Tag's private data contents should not be disclosed to anyone (including the Reader or an Attacker).
(2) Resistance to Tag-tracking attacks. Aside from the Server, the Tag cannot be tracked by anyone.
(3) Reader anonymity. Aside from the Server, the Reader's private data contents should not be disclosed to anyone (including the Tag or an Attacker).
(4) Resistance to Reader-tracking attacks. Aside from the Server, the Reader cannot be tracked by anyone.
(5) Unforgeability. Aside from a legitimate Server, Reader and Tag, no one should be able to successfully pose as one of these actors for authentication.
(6) Resistance to replay attacks. An attacker is prevented from impersonating any legitimate Server, Reader or Tag from an eavesdropped date.
(7) Resistance to desynchronisation attacks. Attackers should not be able to block data transmissions, causing the Server, Reader or Tag to be unable to synchronously update, and thus undermining the following authentication iteration.

2.4. Scheme objectives

The objectives of the proposed secure authentication protocol are listed in Definition 2, and include the characteristics listed in Definition 3.

Definition 2 (Validity of the secure authentication protocol). Assume Server *S* produces Reader *R* which senses Tag *T*, thus initiating the security authentication protocol. If we can achieve the following points, then the secure authentication protocol is correct.

(1) *S, R* and *T* are mutually authenticating.
(2) Aside from *S*, others (including *R*) are unable to determine the internal data in *T*.
(3) Aside from *S*, others (including *T*) are unable to determine the internal data in *R*.