American Journal of Biochemistry and Biotechnology

Original Research Paper

A Classified Protection Protocol for RFID-based Medical Systems

[1]Xueping Ren and [2]Ming Jiang

[1]*Information Engineering School, HangZhou Dianzi University, Hangzhou 310018, China*
[2]*Institute of Software and Intelligent Technology, HangZhou Dianzi University, Hangzhou 310018, China*

Article history
Received: 28-06-2020
Revised: 20-07-2020
Accepted: 04-08-2020

Corresponding Author:
Xueping Ren
Information Engineering School, HangZhou Dianzi University, Hangzhou 310018, China
Email: renxp@hdu.edu.cn

Abstract: RFID technology has been used in many medical systems. The data transmitted in these medical systems is very important and sensitive. The security of these private data has a wide range of risks. Most existing protocols lack the idea of classified security protection for RFID-based medical systems. These protocols are difficult to apply directly. To address this problem, a reliable RFID based medical system classification protection protocol is proposed in this study without assuming that the channels between readers and server are safe. The protocol allows different participants to access the authorized tag data. The proposed protocol adopts timestamp, one-way hash function and mutual authentication procedure to provide security protection and good performance. Based on a formal analysis, GNY logic is used to verify the design correctness of the protocol. According to the analysis of attack model, the protocol can resist various attacks: Internal attack, replay attack, tracking attack, spoofing attack and DOS attack. Performance analysis indicates that the protocol has less communication overload, similar storage requirements and acceptable computation load compared with other related protocol.

Keywords: RFID, Classified Protection Protocol, RFID-Based Medical Systems

Introduction

Radio Frequency Identification (RFID) is an automatic identification technology. Prominent RFID applications include medical system (Zhao *et al*., 2018; Youssef *et al*., 2019), Supply Chain Management (SCM) (Sun and Wei, 2019) and Internet of Things (IoT) (Álvarez López *et al*., 2018). The tag communicates with a reader via wireless channels, where neither visual nor physical contact is needed. Some readers are fixed and some are mobile. The wireless communication is more vulnerable to malicious adversaries, which causes user privacy disclosure and security threats (Cha and Yeh, 2018; Alotaibi, 2019). Many schemes have been proposed to address these problems, some for IoT (Rasheed *et al*., 2019; Alotaibi, 2019), some for SCM (Ahamed *et al*., 2020; Ren *et al*., 2016) and some for medical system (Youssef *et al*., 2019; Mehra *et al*., 2018; Sanchez *et al*., 2019; Safkhani and Vasilakos, 2019).

In the medical system, RFID tags can be attached to the surface of the object, or implanted into it to collect its information (Fan *et al*., 2018). In addition, RFID has also been found to be of great help in improving the tracking of patients, medicines and medical assets in hospitals and the digitalization of these operations improves their efficiency and safety (Álvarez López *et al*., 2018). For patients, the tag can collect physical health data as well as communicate and interact with the server (Fan *et al*., 2018). It makes remote real-time monitoring and telemedicine become a reality for Wireless Body Area Networks (WBAN) (He *et al*., 2013) and mobile health networks (Zhang *et al*., 2015). Patients authorize doctors to monitor users' physical health data through RFID system (Zhang *et al*., 2016). For medical assets and medication, RFID systems can track and manage. There are a lot of medication errors in the medical system every year. By improving the automation of low-and medium-complexity tasks, RFID system can minimize medical errors (Fan *et al*., 2018).

Along with the advantages of medical RFID system, its security problems are increasingly prominent (Chen *et al*., 2016). It is known that personal physical health information is closely related to individual privacy and business interests. The information collected from tags is valuable for some agencies (e.g., insurers and cosmetic surgery hospitals). There are various participants (e.g., doctors, nurses, asset manager) in a medical system. Each participant has its authorized readers, who are permitted to access the authorized tag data, while any irrelevant sensitive data of other groups will not be disclosed publicly (Ning *et al*., 2011). The attackers may steal or fake the patients' medical privacy data, destroy the normal work process of the system and lead to the serious consequences of medical privacy data disclosure. Therefore, security has become one of the key issues to be solved in the application of RFID in medical system safety (Fan *et al*., 2018).

The RFID-based medical systems face two threats: External attack and internal attack. Both attacks may lead to security threats and privacy disclosure. External attack refers to illegal entities (such as insurers or business competitors), who may carry out replay attack, denial server attack and spoofing attack. Internal attack refers to legal entities, who may impersonate other legal entities to carry out authority-exceeding violation. For example, a reader of assert manager personates a nurse's reader to access a tag for achieving the privacy of patient.

Most existing protocols lack the idea of classified security protection for RFID-based medical systems. Another protocols assume the channels between readers and servers are secure. In fact, the channel between reader and server is not secure due to wireless communication.

Therefore, a reliable classified protection protocol for RFID-based medical system is proposed. The doctors, nurses and managers have been allowed to access the specified field areas of a Tag Identifier (TID). Readers can change roles successfully without tag intervention.

The proposed protocol adopts timestamp, one-way hash function, pseudorandom identifiers and mutual authentication procedure to provide security protection and good performance.

The organization of the paper is as follows. The requirement of the RFID-Based medical system and some related protocols are analyzed in section II. The proposed protocol is described in section III. Formal analysis of the protocol with GNY logic is provided in section IV. In the next section, the attack model is used to analyze the security against external and internal attacks. Performance analysis is carried out in section VI. Finally, section VII summarizes the scheme and discusses the future work (Rhee *et al*., 2005).

Related Works

Requirement of the RFID-Based Medical Systems

There are two typical architectures for the RFID system. One is that the connection between the server and the reader is wired and the reader is fixed. The other is that the connection between the server and the reader is wireless and the reader is portable (Fan *et al*., 2018).

In the first architecture mode, the channel between the reader and server is considered secure, while the channel of the second one is considered insecure. Both structures exist in the RFID-based medical system and it is necessary to ensure reliable and secure access to medical information of patients as well as sensitive information management (Fan *et al*., 2018).

The tags in medical systems usually contain some sensitive or personal data. These data are valuable for external entities. Divulging all or part of the data may damage the people's privacy and seriously affect their physical and mental health. For example, the medication provided by patients to insurance the insurers or business competitors are related to commercial interests and maintain the personal privacy of managers. Thus, only doctors or nurses can obtain the information. The nurse is allowed to read the medication of the patient, but not the previous medical history. Therefore, it is necessary to classify and protect the tag data. Legal readers are authorized to read part fields of the tags. Therefore, the medical system needs classified security protection.

This means that RFID tags should provide a mechanism to prevent tag information from being revealed by any malicious reader. When a TID is transmitted over a public channel, only the authenticated reader can read it. The exchanged data are protected to fight against forgery and data modification by either illegal readers or unauthorized legal readers. The protocol should provide entity authentications between valid readers, valid tags and authorized server.

The RFID-Based medical system needs resist the following attacks: Internal forgery attack, spoofing attack, replay attack, tracking attack and DOS attack.

Related Protocols

Many schemes have been proposed to address the potential security and privacy problems in RFID systems. Here the related schemes for the medical system or the hierarchic security protection are discussed.

Zhao (2014; Zhang and Qi, 2014) proposed two efficient ECC-based RFID authentication schemes that can be applied to the healthcare environment. Experimental results show that these ECC-based RFID authentication schemes are suitable for automated patient medication systems (Fan *et al*., 2018). However, the former cannot resist some attacks, such as replay attack, spoofing attack, DOS attack and location tracking attack. The latter claimed the scheme can resist all the attacks. Both of them are not suitable for the lightweight RFID system due to ECC. Fan *et al*. (2018) proposed a lightweight RFID protocol for medical privacy protection in IoT, which can withdraw various attacks. However, the above-mentioned protocols lack the classified security protection idea for overall management.

Fore-mentioned schemes allow all the authorized readers to access the entire identifiers of all legal tags. Based on the previous analysis, it is essential for authenticated entities to access the specified field areas of the Tag Identifier (TID) (Ning *et al.*, 2011). Ning *et al.* (2011) proposed a distributed Key Array Authentication Protocol (KAAP) for RFID systems. However, one reader is hard to change its role in KAAP. This feature limits the protocol scalability (Ren *et al.*, 2016). Ren *et al.* proposed a scalable authentication protocol with classified protection in RFID-based systems. Both of them can withdraw various attacks for lightweight RFID systems and assume that the communication between the server and the reader is safe. However, the connection between the server and the reader is wireless in medical RFID systems. The wireless communication is facing more serious challenges. Thus, this assumption does not hold in medical RFID system.

In view of patient privacy and overall management, there is not a suitable protocol that can be directly applied in medical RFID systems.

Proposed Protocol

The proposed protocol is shown in Fig. 1. The details of the protocol are as follows.

It describes the protocol in detail according to the sequence of message exchanges.

Challenge Messages

One reader generates a random number R_r, then computes $H_1 = h(PID_R||R_r)$ and $H_2 = h(PID_R||T_0)$ and sends them to the tag as an initial query.

Response Messages

Upon receiving the query, the tag verifies the reader by searching $H_1 = h(PID_R||R_r)$ in the access list L_R. If there is no PID_R to meet H_1, the protocol will terminate with an error code. Otherwise, the reader obtains PID_R. After generating a random number R_t, T computes $H_3 = h(PID_R||R_r||H_2) \oplus h(PID_t||R_r)$ and then sends H_3 and R_t to the reader.

Forward Messages

When the reader receives the response, it computes $h(PID_R||R_r||H_2)$ and records the timestamp T_0 and then extracts $h(PID_t||R_r)$ from H_3 and computes $H_4 = h(PID_t||R_t) \oplus h(PID_R||R_r||T_0)$. It forwards H_1, H_2, H_4, R_r, R_t, T_0 to the database DB for the further authentication.

Authenticate the Reader and the Tag

When receiving the authentication request from the reader, the server first detects whether $T - T_0 \prec \Delta t$, where T is the current timestamp of the server and Δt is the transmission delay threshold. If it is true, the server continues to verify the legitimacy of the reader and tag. Otherwise, the protocol will be terminated. The server verify the reader through $H_0 = h(PID_R||R_r)$ and $H_1 = h(PID_R||T_0)$. If the above step holds, the server would compute $h(PID_R||R_r||T_0)$ and verify the tag through $h(PID_t||R_r) = H_5 \oplus h(PID_R||R_r||T_0)$. If the formula holds, the tag is legal.

The server gets T_1 from the current timestamp of the server, computes $H_5 = h(PID_R||R_r||T_1)$, $H_6 = h(PID_t||PID_R||R_t||k_{ij})$ and $H_7 = h(PID_t||R_r) \oplus k_{ij}$ and sends them to the reader.

The Reader Authenticate the Server

After receiving the server's message, the reader first detects whether $T_2 - T_1 \prec \Delta t$, where T_2 is the current timestamp of the reader. If it is true, the reader checks $H_5 = h(PID_R||R_r||T_1)$ to verify the server. Then it gets k_{ij} from H_7 and computes $H_8 = h(PID_R||R_t||k_{ij})$. Finally, the reader resend H_6, H_7, H_8 to the tag.

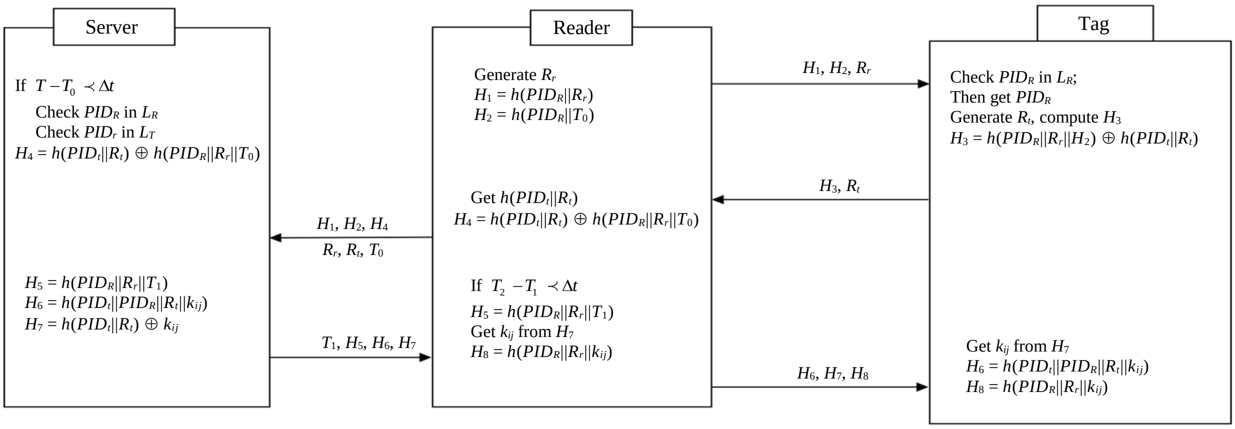
Server
If $T - T_0 \prec \Delta t$
Check PID_R in L_R
Check PID_r in L_T
$H_4 = h(PID_t||R_t) \oplus h(PID_R||R_r||T_0)$
$H_5 = h(PID_R||R_r||T_1)$
$H_6 = h(PID_t||PID_R||R_t||k_{ij})$
$H_7 = h(PID_t||R_t) \oplus k_{ij}$
H_1, H_2, H_4
R_r, R_t, T_0
T_1, H_5, H_6, H_7
Reader
Generate R_r
$H_1 = h(PID_R||R_r)$
$H_2 = h(PID_R||T_0)$
Get $h(PID_t||R_t)$
$H_4 = h(PID_t||R_t) \oplus h(PID_R||R_r||T_0)$
If $T_2 - T_1 \prec \Delta t$
$H_5 = h(PID_R||R_r||T_1)$
Get k_{ij} from H_7
$H_8 = h(PID_R||R_r||k_{ij})$
H_1, H_2, R_r
H_3, R_t
H_6, H_7, H_8
Tag
Check PID_R in L_R;
Then get PID_R
Generate R_t, compute H_3
$H_3 = h(PID_R||R_r||H_2) \oplus h(PID_t||R_t)$
Get k_{ij} from H_7
$H_6 = h(PID_t||PID_R||R_t||k_{ij})$
$H_8 = h(PID_R||R_r||k_{ij})$

Fig. 1: Proposed protocol

The Tag Authenticate the Server

After receiving the reader's response, the tag extracts k_{ij} from H_7, checks $H_6 = h(PID_t||PID_R||R_t||k_{ij})$ and $H_8 = h(PID_R||R_r||k_{ij})$ to verify the reader, the server and the k_{ij} value.

Formal Analysis of the Protocol with GNY Logic

GNY logic (Gong *et al*., 1990) was proposed, which is optimized and derived from BAN logic (Burrows *et al*., 1989). Based on the knowledge/belief, GNY Logic uses postulates and definitions to analyze whether the protocol goals can be derived from the initial assumptions and message exchanges in the reasoning progress. GNY logic is chosen to prove the secure correctness of the protocol.

The GNY formal logic analysis involves four steps: (1) Formalization of the protocol messages; (2) declaration of initial assumptions; (3) definition of anticipant goals; and 4) verification by logical rules and formulae.

Formalization of Messages

Each exchanged message is expressed with a logical formula and a formal message in the language of GNY Logic. For the sake of clarity, the same statements are used as (Gong *et al*., 1990; Ren *et al*., 2013).

According to the authentication phase, the formalized messages are as follows:

- M1 ($R \to T$): $h(PID_R||R_r)$, $h(PID_R||T_0)$, R_r
- M2 ($T \to R$): $h(PID_R||R_r||h(PID_R||T_0) \oplus h(PID_t||R_t)$, R_t
- M3 ($R \to S$): $h(PID_R||R_r)$, $h(PID_R||T_0)$, $h(PID_t||R_t) \oplus h(PID_R||R_r||T_0)$, R_r, R_t, T_0
- M4 ($S \to R$): $h(PID_R||R_r||T_1)$, $h(PID_t||PID_R||R_t||k_{ij})$, $h(PID_t||R_t) \oplus k_{ij}$
- M5 ($R \to T$): $h(PID_t||PID_R||R_t||k_{ij})$, $h(PID_t||R_t) \oplus k_{ij}$, $h(PID_R||R_r||k_{ij})$

Initial Assumptions

In order to specify the initial possessions and abilities of each participant, the following statements are assumed:

- (A1) $T \ni R_t$
- (A2) $T \mid\equiv \# k_{ij}$
- (A3) $T \ni PID_t$, $T \mid\equiv T \xleftrightarrow{PID_t} S$
- (A4) $T \mid\equiv \# PID_R$, $T \mid\equiv T \xleftrightarrow{PID_R} R$
- (A5) $R \ni R_r$
- (A6) $R \ni PID_R$, $R \mid\equiv R \xleftrightarrow{PID_R} T$
- (A7) $R \mid\equiv R \xleftrightarrow{PID_R} S$
- (A8) $R \mid\equiv \# k_{ij}$
- (A9) $S \ni k_{ij}$, $S \mid\equiv \# k_{ij}$
- (A10) $S \ni PID_t$, $S \mid\equiv \# PID_t$, $S \mid\equiv S \xleftrightarrow{PID_t} T$
- (A11) $S \ni PID_R$, $S \mid\equiv \# PID_R$, $S \mid\equiv S \xleftrightarrow{PID_R} R$

These statements show that each participator possesses its random number and the pseudorandom identifier. Each tag believes or is entitled to believe k_{ij} and PID_R are fresh. The server possesses k_{ij}, PID_R and PID_t and it believes that they are fresh.

Protocol Messages and Security Correctness Goals

The purpose of the protocol is to assure freshness of data and mutual authentication among *R*, *S* and *T*. The anticipant goal can be obtained as follows:

- (G1) $T \mid\equiv R \mid\sim R_r$
- (G2) $T \mid\equiv R \mid\sim PID_R$
- (G3) $R \mid\equiv T \mid\sim R_t$
- (G4) $S \mid\equiv R \mid\sim R_r$
- (G5) $S \mid\equiv R \mid\sim PID_R$
- (G6) $S \mid\equiv T \mid\sim R_t$
- (G7) $S \mid\equiv T \mid\sim PID_t$
- (G8) $T \mid\equiv \# h(PID_R||R_r)$
- (G9) $S \mid\equiv \# h(PID_t||R_t)$
- (G10) $S \mid\equiv \# h(PID_R||R_r)$
- (G11) $S \mid\equiv \# h(PID_R||T_0)$
- (G12) $R \mid\equiv S \mid\sim k_{ij}$
- (G13) $R \mid\equiv \# h(k_{ij})$
- (G14) $T \mid\equiv S \mid\sim k_{ij}$
- (G15) $T \mid\equiv \# h(k_{ij})$

The first to the seventh goals show belief requirements. The server and *T* believes *R* conveys R_r and PID_R. *R* believes *T* conveys R_t. The server believes *T* conveys PID_t and R_t. The next four goals show that the messages are not used in the previous sessions and indicate fresh requirements. The twelfth and thirteenth goals indicate *R* and *T* believe the server conveys k_{ij}. The last two goals show they believe that $h(k_{ij})$ is fresh.

Logic Verification

Logic verification is based on the formalized messages, the related GNY Rules and the assumptions.

Verifications for the first to the seventh goals are similar to (Rahman and Ahamed, 2014) and it will not be repeated here. This subsection will focus on verification of other goals.

For G8: From message M1 gets:

$$T \triangleleft *\left(PID_R \oplus R_r\right) \quad T \triangleleft *R_r \qquad (1)$$

Applying the Being-Told Rule T1: ($P \triangleleft (*X)$)/($P \triangleleft X$) deduces:

$$T \lhd \left(PID_R \oplus R_r\right) T \lhd R_r \qquad (2)$$

T can retrieve PID_R from L_R and applying the Being-Told Rule T2: $(P \lhd (X, Y))/(P \lhd X)$ deduces:

$$T \lhd PID_R \qquad (3)$$

Applying the Possession Rule P1: $(P \lhd X)/(P \ni X)$:

$$T \ni PID_R \;\; T \ni R_r \qquad (4)$$

Applying the Possession Rule P2: $(P \ni X, P \ni Y)/(P \ni (X, \mathrm{Y})$ deduces:

$$T \ni \left(PID_R, R_r\right) \qquad (5)$$

From the assumption A4, it gets:

$$T \mid\equiv \# PID_R \qquad (6)$$

Applying the Freshness Rules F1: $(P \mid\equiv \# (X))/(P \mid\equiv \# (X, Y), P \mid\equiv \# \mathrm{F}(X))$ deduces:

$$T \mid\equiv \#\left(PID_R, R_r\right) \qquad (7)$$

Applying the Freshness Rules F10: $(P \mid\equiv \# (X), P \ni X)/(P \mid\equiv \# H(X))$ deduces:

$$T \mid\equiv \# h\left(PID_R, R_r\right) \qquad (8)$$

Thus, T is entitled to believe that $h(PID_R \| R_r)$ is fresh.

Hereinafter, for simplicity, the applied logical rules and formula behind the formula are marked:

For G9: $S \mid\equiv \# h(PID_t \| R_t)$
$S \ni PID_t$ (1)//A10;
$R \lhd R_r$ (2)//M2, T1
$S \lhd R_t$ (3)//M3,T1
$S \ni PID_t \; S \ni R_t$ (4)//P1
$S \ni (PID_t, R_t)$ (5)//P2
$S \mid\equiv \# PID_t$ (6)//A10
$S \mid\equiv \# (PID_t, R_t)$ (7)//F1
$S \mid\equiv \# h(PID_t \| R_t)$ (8)//F10

Goal G9 is achieved.

Verifications for the tenth and eleventh goals are similar to the ninth goal, it is not repeated here:

For G12: $R \lhd h(PID_t \| R_t) \oplus k_{ij}$ (1)//M4
$R \lhd h(PID_t \| R_t) \oplus k_{ij}$ (2)//T1
$R \ni h(PID_t \| R_t) \oplus k_{ij}$ (3)//P1
$R \lhd {}^{*}h(PID_t \| R_t) \oplus h(PID_R \| R_r \| h(PID_R \| T_0))$ (4)//M2
$R \lhd h(PID_t \| R_t) \oplus h(PID_R \| R_r \| h(PID_R \| T_0))$ (5)//T1
$R \ni h(PID_t \| R_t) \oplus h(PID_R \| R_r \| h(PID_R \| T_0))$ (6)//P1
$R \ni R_r, R \ni PID_R$ (7)//A5, A6
$R \ni T_0$
$R \ni h(PID_R \| R_r), R \ni h(PID_R \| T_0)$ (8)//P2
$R \ni h(PID_R \| R_r \| h(PID_R \| T_0))$ (9)//(8)
$R \ni h(PID_t \| R_t)$ (10)//(6)(9)
$R \ni k_{ij}$ (11)//(3)(10)
$R \ni PID_R, R \mid\equiv R \xleftrightarrow{PID_R} S$ (12)//A6 A7
$R \ni (PID_R, k_{ij})$ (13)//P2;
$R \mid\equiv \# k_{ij}$ (14)//A8;
$R \mid\equiv \# (k_{ij}, PID_R)$ (15)//F1;
$R \mid\equiv S \mid \sim (k_{ij}, PID_R)$ (16)//I3
$R \mid\equiv S \mid \sim (k_{ij})$ (17)//I7;

AS a consequence, R is entitled to believe the server once conveyed k_{ij}:

For G13: From aforementioned formula (11) gets
$R \ni k_{ij}$ (1);
$R \mid\equiv \# k_{ij}$ (2)//A8;
$R \mid\equiv \# h(k_{ij})$ (3)//F10.

As a result, T is entitled to believe that $h(k_{ij})$ is fresh:

For G14: $T \lhd {}^{*}h(PID_t \| R_t) \oplus k_{ij}$ (1)//M5
$T \lhd h(PID_t \| R_t) \oplus k_{ij}$ (2)//T1
$T \ni h(PID_t \| R_t) \oplus k_{ij}$ (3)//P1
$T \ni R_t \; T \ni PID_t$ (4)//A1, A3
$T \ni k_{ij}$ (5)//(3)(4)
$T \ni PID_t, T \mid\equiv T \xleftrightarrow{PID_t} S$ (6)//A3;
$T \ni (PID_t, k_{ij})$ (7)//P2;
$T \mid\equiv \# k_{ij}$ (8)//A2;
$T \mid\equiv \# (k_{ij}, PID_t)$ (9)//F1;
$T \mid\equiv S \mid \sim (k_{ij}, PID_T)$ (10)//I3
$T \mid\equiv S \mid \sim (k_{ij})$ (11)//I7;

T is entitled to believe the server conveyed k_{ij} once:

For G15: From aforementioned formula (5), it gets
$T \ni k_{ij}$ (1);
$T \mid\equiv \# k_{ij}$ (2)//A2;
$T \mid\equiv \# h(k_{ij})$ (3)//F10.

Then, T is entitled to believe that $h(k_{ij})$ is fresh.

Security Analysis

Unlike most similar protocols, communication between the server and the reader is regarded as insecure because the connection between them is wireless in RFID-based medical systems. The wireless communication is facing more serious challenges.

Attack Model

In this section, security analysis of the scheme by using attack model is given. There are some different common possible attacks in the attack model: Replaying, forgery, tracking, spoofing and DOS. The protocol will not generate mismatching among the three participants (the reader, the tag and the server) when it performs incompletely. Thus, the desynchronization attack is not discussed here. It is assumed the attack cannot replicate a tag or a reader.

Security analysis is performed with three steps like (Ning *et al*., 2011): ① To suppose the action of the attacker; ② to simulate the process of the attacking step by step; and ③ to deduce the security.

Replay Attack

Replay attack is an active attack. The attacker obtains the message of the current session and then modifies, deletes or replays the message in the next session. The goal of the attack is to attain the sensitive data.

Under the replay attack, the attacker A performs the following actions:

In One Session

A has learnt: {$h(PID_R\|R_r)$, $h(PID_R\|T_0)$, R_r, $h(PID_R\|R_r\|h(PID_R\|T_0)) \oplus h(PID_t\|R_t)$, R_t}

In the Next Session

A disguises as a tag T_a:

$$R \to A(T_a) \nrightarrow T : h\left(PID_R\|R_r'\right), h\left(PID_R\|T_0'\right), R_r',$$
$$A(T_a) \to R : h\left(PID_{\mathrm{R}} \| R_r \| h\left(PID_R\|T_0\right)\right) \oplus h\left(PID_t\|R_t\right), R_t$$

R obtains $h'(PID_t\|R_t)$ from the message with PID_R, R_r' and T_0', then it sends $h'\left(PID_t\|R_t\right) \oplus_0 \; h\left(PID_R\|R_t \| T_0'\right)$, R_r', R_t, T' to the server for verification. The server will find there is no matching value for $h'(PID_t\|R_t)$ with R_t. The authentication will terminate.

In Bad Conditions

If A modifies the value of $h(PID_R\|R_r\|h(PID_R\|T_0)) \oplus h(PID_t\|R_t)$ and R_t and forwards to *R*, *R* obtains $h''(PID_t\|R_t)$ from them with PID_R, R_r' and T_0':

$$R \to S : h\left(PID_R\|R_r'\right), h\left(PID_R\|T_0'\right),$$
$$h''\left(PID_t\|R_t\right) \oplus h\left(PID_R\|R_r'\|T_0'\right), R_r', R_t'', T_0';$$
$$S \nRightarrow A(T_a);$$

The server verifies that PID_R is valid and it will find there is no PID_t to match with values $h''(PID_t\|R_t)$ and R_t'' and D. The authentication will fail.

In the Worse Conditions

If DB obtains PID_t'' based on $h''(PID_t\|R_t)$, then it responds to $h\left(PID_t''\|R_t''\right) \oplus k_{ij}$ and $h\left(PID_t''\|PID_R\|R_t''\|k_{ij}\right)$ to *R* by mistake. *R* forwards and A intercepts them:

$$\mathrm{S} \to R : h\left(PID_R\|R_t'\|T_1\right),$$
$$h\left(PID_t''\|PID_R\|R_t''\|k_{ij}\right) h\left(PID_t''\|R_t''\right) \oplus k_{ij};$$
$$R \to A(T_a) \to T : h\left(PID_t''\|PID_R\|R_t''\|k_{ij}\right) h\left(PID_t''\|R_t''\right)$$
$$\oplus k_{ij}, h\left(PID_R\|R_t'\|k_{ij}\right);$$
$$T : h\left(PID_t''\|PID_R\|R_t''\|k_{ij}\right) \neq h\left(PID_t \| PID_R \| R_t' \| k_{ij}''\right);$$

A cannot obtain k_{ij} and PID_t from these messages, then it disguises as a reader R_a and forwards these messages to *T* like spoofing attack.

After *T* receives those messages, it gets k_{ij}'' from $h\left(PID_t''\| R_t''\right) \oplus k_{ij}$ using PID_t and the latest random number R_t' . k_{ij}'' is not equal to k_{ij} since the probability that R_t' equals R_t'' is negligible. It will find that $h\left(PID_t''\|PID_R\|R_t''\|k_{ij}\right)$ differs from $h\left(PID_t \| PID_R \| R_t' \| k_{ij}''\right)$ and the authentication will be end with failure.

Hence, the protocol can resist the replay attack.

Internal Forgery Attack

The forgery attack can be categorized into an internal and external forgery attack. From the analysis of the replay attack, the scheme can resist the external forgery attack. Thus, the internal forgery attack is analyzed here. In the attack, the legal reader in one group oversteps its access of authority to achieve others' private information by forging another legal reader in another group (Ren *et al*., 2016).

During the internal reader forgery attack:

In One Session:

$$\tilde{r}_i(r_i) \to t_j) : h\left(PID_{\tilde{R}_i} \| \tilde{R}_{r_i}\right), h\left(PID_{\tilde{R}_i} \| T_0\right), \tilde{R}_{r_i}$$

The internal reader $\tilde{R}_i$ cannot disguise as another legal reader R_i, since PID_{R_i} is not equal to $PID_{\tilde{R}_i}$ and $\tilde{R}_i$ cannot obtain the *PID* of R_i. The tag identifies the reader as $\tilde{R}_i$. The tag and server will communicate with the reader as $\tilde{R}_i$. The internal attack will be failed.

In summary, the protocol can resist the internal attacks.

Spoofing Attack

In this attack, the attack can forge a legal reader to obtain the information of the legal tag and damage the normal communication. The attack also can forge a legal tag to obtain valid response (Ren *et al*., 2016).

During the spoofing attack, an attacker A performs the following actions:

In One Session

A disguises as a reader R_a and sends a query to T:

$$A(R_a)\rightarrow T: h\left(PID_{R_a} \| R_{r_a}\right), h\left(PID_{R_a} \| T_{a0}\right), R_{r_a}.$$

T cannot find a match to verify $A(R_a)$ by searching in the access list L_R. The authentication will be ended.

In Bad Conditions

$$T\rightarrow A(R_a): h\left(PID_{R_a} \| R_{r_a} \| h\left(PID_{R_a} \| T_{a0}\right)\right.$$
$$\oplus h\left(PID_t \| (R_t\right), R_t$$

T may respond to $A(R_a)$ by mistake. $A(R_a)$ obtains R_t and $h(PID_t\|R_t)$, then authentication will continue.

In the Next Session

A intercepts messages sent to *T* and disguises as a tag T_a first:

$$R\rightarrow A(T_a)\not\rightarrow T: h\left(PID_R \| R_r\right), h\left(PID_R \| T_0\right), R_r$$
$$A(T_a)\rightarrow R: h\left(PID_{R_a} \| R_{r_a} \| h\left(PID_{R_a} \| T_{a0}\right)\right.$$
$$\oplus h\left(PID_t \| R_t\right), R_t$$
$$R\rightarrow \text{server}: h\left(PID_R \| R_r\right), h\left(PID_R \| T_0\right),$$
$$h'\left(PID_t \| R_t\right)\oplus h\left(PID_R \| R_r \| T_0\right), R_r, R_t, T_0$$

R obtains $h'(PID_t\|R_t)$ from $h\left(PID_{R_a} \| R_{r_a} \| h\left(PID_{R_a} \| T_{a0}\right)\right.$ $\oplus h\left(PID_t \| R_t\right)$ using PID_R, R_r and T_0. The server verifies that PID_R is valid and it finds $h'(PID_t\|R_t)$ has no matching value, because the probability that PID_R equals PID_{Ra} is negligible. $Server \not\Rightarrow A(T_a)$, the authentication will fail.

In the Worse Conditions

If DB responds to $h(PID_R\|R_r\|T_1)$, $h\left(PID'_t \| PID_R \| R'_t \| k_{ij}\right)$ and $h\left(PID'_t \| R'_t\right)\oplus k_{ij}$ to *R* by mistake and *R* obtains k''_{ij} from $h\left(PID'_t \| R'_t\right)\oplus k_{ij}$ using $h'(PID_t\|R_t)$ and forwards them to *A*:

$$server\rightarrow R: h\left(PID_R \| R_r \| T_1\right), h\left(PID'_t \| PID_R \| R'_t \| k_{ij}\right),$$
$$h\left(PID'_t \| R'_t\right)\oplus k_{ij}$$
$$R\rightarrow A(T_a)\rightarrow T: h\left(PID'_t \| PID_R \| R'_t \| k_{ij}\right), h\left(PID'_t \| R'_t\right)$$
$$\oplus k_{ij}, h\left(PID_R \| R_r \| k''_{ij}\right)$$

A obtains k'_{ij} from $h\left(PID'_t \| R'_t\right)\oplus k_{ij}$ using $h(PID_t\|R_t)$ and k'_{ij} is not equal to k_{ij}, since $h(PID_t\|R_t)$ is not equal to $h\left(PID'_t \| R'_t\right)$. A cannot obtain PID_t from $h\left(PID'_t \| R'_t\right)\oplus k_{ij}$ using $h(PID_t\|R_t)$ R_t and k'_{ij}. In order to get PID_t, A forwards those messages to *T*.

After *T* receives those messages, it gets k'_{ij} from $h\left(PID'_t \| R'_t\right)\oplus k_{ij}$ using $h(PID_t\|R_t)$ like *A*. It computes $h\left(PID_t \| PID_{R_a} \| R_t \| k'_{ij}\right)$ with PID_t, PID_{R_a}, R_t and k'_{ij}, then compares it with $h\left(PID'_t \| PID_R \| R'_t \| k_{ij}\right)$. The tag finds that these two are not equal and the authentication will be interrupted.

In this protocol, access lists are available for preliminary verifications and random numbers are valid for one time. So the protocol can resist the spoofing attack.

Tracking Attack

The tracking attack is a passive attack, it traces tags through malicious readers. Some malicious readers send the same query to a tag. If the tag responds to the same message, the attacker may trace the certain tag and achieve its related information (Ren *et al*., 2013).

Under the attack, the attacker A performs the following actions:

$$A(R_i)\rightarrow T: h\left(PID_{R_1} \| R_{r_1}\right), h\left(PID_{R_1} \| \mathrm{T}_0\right),$$
$$R_{r_1}; h\left(PID_{R_2} \| R_{r_2}\right), h\left(PID_{R_2} \| \mathrm{T}_0\right), R_{r_2} \ldots\ldots\ldots$$

The tag finds there is no matching entry in the access list L_R. The authentication will terminate.

In worse conditions, *T* responds to these readers by mistake:

$$T\rightarrow A(R_i): h\left(PID_{R_1} \| R_{r_1} \| h\left(PID_{R_1}\right)\right)\oplus h\left(PID_t \| R_{t_1}\right), R_{t_1};$$
$$h\left(PID_{R_2} \| R_{r_2} \| h\left(PID_{R_2}\right)\right)\oplus h\left(PID_t \| R_{t_2}\right), R_{t_2} \ldots\ldots\ldots$$

All response messages are different, since the random numbers $\left(R_{t_1}, R_{t_2}, R_{t_3}\ldots\ldots\right)$ are varying and $\left(R_{r_1}, R_{r_2}, R_{r_3}\ldots\ldots\right)$ are the same situations. Hence, the attacker cannot trace the certain tag by these response messages.

In other words, if the attacker collects the transferring messages by a certain tag in the past sessions, it cannot find two same messages. It cannot track specific tags because random numbers generated by readers and tags are different in each session.

Therefore, the protocol can resist the tracing attack.

DOS Attack

DOS attack is an active attack. The attacker launches a lot of requests with false address. The system has no sufficient resources to process the normal communication because most of the resources are allocated to handle these malicious messages. The goal of the attacker is not to achieve the sensitive data, but to destroy the normal communication.

Like (Ning *et al*., 2011; Ren *et al*., 2013), two approaches (the access list and the access control) are adopted to provide protection in this protocol. Access lists (L_R, L_T) are used for quick search and preliminary check.

Under the attack, the attacker A may perform the following actions:

$$A(R_i) \to T : h\left(PID_{R_1} \parallel R_{r_1}\right), h\left(PID_{R_1} \parallel T_0\right),$$
$$R_{r_1}, h\left(PID_{R_2} \parallel R_{r_2}\right), h\left(PID_{R_2} \parallel T_0\right), R_{r_2} \ldots\ldots\ldots$$

A sends several requests with wrong PID_R to one tag. The tag can quickly identify all illegal readers by the access list L_R. The access control is applied by random/pseudorandom numbers (R_r, R_t, PID_R, PID_t). The legal server and tag can refuse the request with the same pseudorandom identifier and random numbers in a certain time, because they keep the last received and pseudorandom identifiers as temp lists. The legal reader can do that by keeping (R_t, $h(PID_t \| R_t)$).

If the attack continually replays legal requests attained from the former session to a tag (or a reader or server), the tag (or the reader or server) can deny the requests through access control. Hence, the attacker cannot interfere with the normal communication.

All in a word, the DOS attack can be resisted in this protocol.

In the protocol, an attacker cannot obtain tag's identifier even it correctly guesses the random number R_t. So the protocol offers anonymity. Table 1 shows the security comparison with other related protocols for lightweight RFID systems.

Performance Analyses

In this section, we will compare the proposed scheme with some other protocols in terms of performance, including storage requirement, the computation overhead and communication overhead.

The performance comparison between this protocol and other related protocols of lightweight RFID systems is shown in Table 2. Like (Fan *et al*., 2018; Zhao, 2014; Zhang and Qi, 2014; Niu *et al*., 2014; Doss *et al*., 2013). The protocol assumes that the channels between readers and servers are insecure since they work in mobile RFID system. KAAP and SAAP assume that the channels between readers and server are secure in RFID system.

Storage Requirement

As it is known that the tag's storage is limited relative to the reader and the server. Only the using of tag storage in Table 2 is concerned. Each tag stores the TID ID_T, access list L_R and pseudorandom identifier PID_T in the protocol. It is the same as most related protocols.

For the sake of simplicity, it is noted that all the components are assumed L-bits size and the length of keys, hash function value and random numbers are ignored in Table 2.

Computation Cost

In the authentication process, each reader performs a Random Number Generation (RNG) operation and a one-way hash function and the server performs a one-way hash function. Each tag in the protocol needs to perform three bitwise XOR, one RNG operation and one hash function. Since *XOR* consumes little resource, *XOR* operation and other simple operations are ignored here. In general, a server and reader are not limited to the computing resources and Table 2 only shows the tag computation cost of the protocol, which is obviously more than (Fan *et al*., 2018) and less than (Niu *et al*., 2014).

Table 1: Security comparison

	Anonymity	DOS	Spoofing	Replay	Tracking	Internal forgery	Desynchronization
Rhee *et al.* (2005)	√	×	√	√	√	×	×
Niu *et al.* (2014)	√	√	×	√	√	×	√
Fan *et al.* (2018)	√	√	×	√	√	×	√
Ning *et al.* (2011)	√	√	√	√	√	√	√
Ren *et al.* (2016)	√	√	√	√	√	√	√
The protocol	√	√	√	√	√	√	_

√: provided; ×: not provided; _ : not exist

Table 2: Performance comparison

	Rounds	Tag storage	Tag Computation	Communication cost	SA
Rhee *et al.* (2005)	5	3L	3H	5L	Y
Niu *et al.* (2014)	5	3L	5R	4L	N
Fan *et al.* (2018)	11	L	R	7L	N
Ning *et al.* (2011)	5	3L	R+2E	2L	Y
Ren *et al.* (2016)	5	3L	R+H	3L	Y
The protocol	5	3L	R+2H	0L	N

R: RNG operation; H: Hash operation; E: Encryption operation; L: Length of identifier/access list; SA: Security Assumption on channels

Communication Overhead

In terms of communication overhead, "round" represents the number of communication rounds in the whole authentication process in Table 2. “Communication cost” represents the resource consumption on the channel between the tag and the reader. Supposed that the identifier of a reader or a tag has the same length L, communication cost of this protocol is 0 L. It is less than other related protocols.

Based on the previous analysis, the protocol has middle complexity in storage requirement and computation cost and its communication overhead is obviously less than other related protocols.

Conclusion

To minimize medical errors and overall manage, more and more medical systems adopt RFID technology. The tags in medical systems usually contain some sensitive or personal data. Leakage of whole or part of the data may damage the people’s privacy and seriously affect their physical and mental health.

Most of the existing protocols lack the idea of classified security protection for RFID-based medical systems. These protocols are difficult to be directly applied and other protocols assume the channels between readers and servers are safe.

A classified protection protocol is proposed for RFID-based medical systems without the assumption that the channels between readers and server are safe. The scheme allows different participants to access the authorized tag data in the medical systems. Readers, tags and servers are mutually authenticated. Readers can change their roles freely, so the protocol has better scalability.

The protocol uses timestamp, access list, mutual authentication mechanism and random access control mechanism to strengthen security and privacy protection. Based on formal analysis, the design correctness of the protocol is verified by GNY logic. According to the analysis of attack model, the protocol can resist all kinds of attacks: Internal attack, replay attack, tracking attack, spoofing attack and DOS attacks.

Performance analysis shows that the protocol has less communication overload, similar storage requirements and acceptable computation load compared with other related protocols. Therefore, the new protocol is suitable for RFID-based medical application.

The new protocol cannot detect the patient. In the future, we will focus on personnel detection of patient status in the scheme and develop several programs to simulate further certification.

Acknowledgement

This work is supported by Zhejiang Provincial natural science foundation of China (NO. LQY18F020001), Zhejiang Province key R&D program projects of China (NO. 2019C03096).

Author’s Contributions

Xueping Ren: Has conceived and designed the experiments, data analysis, manuscript writing and publication.

Ming Jiang: Has reviewed and revised the manuscript.

Ethics

Authors should address any ethical issues that may arise after the publication of this manuscript.

References

Ahamed, N. N., Karthikeyan, P., Anandaraj, S. P., & Vignesh, R. (2020, March). Sea Food Supply Chain Management Using Blockchain. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 473-476). IEEE.

Alotaibi, B. (2019). Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review. IEEE Sensors Journal, 19(23), 10953-10971.

Álvarez López, Y., Franssen, J., Álvarez Narciandi, G., Pagnozzi, J., González-Pinto Arrillaga, I., & Las-Heras Andrés, F. (2018). RFID Technology for management and tracking: E-health applications. Sensors, 18(8), 2663.

Burrows, M., Abadi, M., & Needham, R. M. (1989). A logic of authentication. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 426(1871), 233-271.

Cha, S. C., & Yeh, K. H. (2018). A data-driven security risk assessment scheme for personal data protection. IEEE Access, 6, 50510-50517.

Chen, D., Zhang, N., Qin, Z., Mao, X., Qin, Z., Shen, X., & Li, X. Y. (2016). S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol. IEEE Internet of Things Journal, 4(1), 88-100.

Doss, R., Sundaresan, S., & Zhou, W. (2013). A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems. Ad Hoc Networks, 11(1), 383-396.

Fan, K., Jiang, W., Li, H., & Yang, Y. (2018). Lightweight RFID protocol for medical privacy protection in IoT. IEEE Transactions on Industrial Informatics, 14(4), 1656-1665.

Gong, L., Needham, R. M., & Yahalom, R. (1990, May). Reaso Ning about Belief in Cryptographic Protocols. In IEEE Symposium on Security and Privacy (pp. 234-248).

He, D., Chan, S., Zhang, Y., & Yang, H. (2013). Lightweight and confidential data discovery and dissemination for wireless body area networks. IEEE journal of biomedical and health informatics, 18(2), 440-448.

Mehra, V., Sarvari, P., & Ruban, N. (2018, December). RFID Based Secured, Remotely Accessible Personal Medical Data Base Including the Medicinal History. In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-4). IEEE.

Ning, H., Liu, H., Mao, J., & Zhang, Y. (2011). Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems. IET communications, 5(12), 1755-1768.

Niu, B., Zhu, X., Chi, H., & Li, H. (2014). Privacy and authentication protocol for mobile RFID systems. Wireless Personal Communications, 77(3), 1713-1731.

Rahman, F., & Ahamed, S. I. (2014). Efficient detection of counterfeit products in large-scale RFID systems using batch authentication protocols. Personal and ubiquitous computing, 18(1), 177-188.

Rasheed, A., Hashemi, R. R., Bagabas, A., Young, J., Badri, C., & Patel, K. (2019, April). Configurable anonymous authentication schemes for the Internet of Things (IoT). In 2019 IEEE International Conference on RFID (RFID) (pp. 1-8). IEEE.

Ren, X., Jiang, M., Wu, T., Xu, X., & Ge, Y. (2016). A Scalable Authentication Protocol with Classified Protection in RFID-based Systems. Adhoc & Sensor Wireless Networks, 31.

Ren, X., Xu, X., & Li, Y. (2013). An One-way Hash Function Based Lightweight Mutual Authentication RFID Protocol. JCP, 8(9), 2405-2412.

Rhee, K., Kwak, J., Kim, S., & Won, D. (2005, April). Challenge-response based RFID authentication protocol for distributed database environment. In International Conference on Security in Pervasive Computing (pp. 70-84). Springer, Berlin, Heidelberg.

Safkhani, M., & Vasilakos, A. (2019). A new secure authentication protocol for telecare medicine information system and smart campus. IEEE Access, 7, 23514-23526.

Sanchez, V., Ro, R., Kent, L., Navas, J., Diyan, O., Roussel, C., ... & Zhan, J. (2019, January). ScanAlert: electronic medication monitor and reminder to improve medical adherence. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0537-0543). IEEE.

Sun, Z., & Wei, M. (2019, July). PUF-based Anonymous RFID system Ownership Transfer Protocol. In 2019 Chinese Control Conference (CCC) (pp. 6367-6373). IEEE.

Youssef, W., Zaid, A. O., Sami, M., & Kammoun, M. H. (2019, October). RFID-based System for Secure Logistic Management of Implantable Medical Devices in Tunisian Health Centres. In 2019 IEEE International Smart Cities Conference (ISC2) (pp. 83-86). IEEE.

Zhang, K., Liang, X., Ni, J., Yang, K., & Shen, X. S. (2016). Exploiting social network to enhance human-to-human infection analysis without privacy leakage. IEEE Transactions on Dependable and Secure Computing, 15(4), 607-620.

Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X., & Luo, H. H. (2015). Security and privacy for mobile healthcare networks: from a quality of protection perspective. IEEE Wireless Communications, 22(4), 104-112.

Zhang, Z., & Qi, Q. (2014). An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. Journal of medical systems, 38(5), 47.

Zhao, R., Wang, D., Zhang, Q., Chen, H., & Huang, A. (2018, June). CRH: A Contactless Respiration and Heartbeat Monitoring System with COTS RFID Tags. In 2018 15th Annual IEEE International Conference on Sensing, Communication and Networking (SECON) (pp. 1-9). IEEE.

Zhao, Z. (2014). A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem. Journal of medical systems, 38(5), 46.