Hindawi
Journal of Healthcare Engineering
Volume 2021, Article ID 1550993, 12 pages
https://doi.org/10.1155/2021/1550993

Research Article

A RFID Authentication Protocol for Epidemic Prevention and Epidemic Emergency Management Systems

Xiuqing Chen, Xiao Zhang, Deqin Geng, Lei Zhou, Junshu Chen, and Fan Lu

School of Medicine Information, Xuzhou Medical University, Xuzhou 221000, China

Correspondence should be addressed to Xiao Zhang; changshui@hotmail.com

Received 14 August 2021; Revised 6 October 2021; Accepted 28 October 2021; Published 3 December 2021

Academic Editor: José A. García-Berná

The outbreak of the novel coronavirus has exposed many problems in the auxiliary information system for epidemic prevention and control, which needs to be resolved by using methods such as the antitampering of logistics data and the management and control of epidemic materials. This article discusses the introduction of emerging technologies such as Radio Frequency Identification (RFID), which support privacy protection into the auxiliary information system for epidemic prevention and control. Recently, this paper found that Khwaja et al.'s protocol (RAPUS protocol) is susceptible to database impersonation attacks and reader impersonation attacks. Therefore, this article proposes the enhanced protocol, which not only perfectly solves the problems of the abovementioned protocols but also comprehensively compares multiple protocols. The enhanced protocol has higher efficiency and security. The security of the proposed protocol (RAPUS + protocol) is analyzed by GNY logic and the AVISPA model. The designed scheme can help realize the safety and traceability of epidemic prevention materials and improve the automation and decision-making efficiency of the epidemic prevention.

1. Introduction

Medical Internet of Things (IoMT) needs higher demand for security than the Internet of Things (IoT) when decreasing medical expense and enhancing the medical workpiece ratio. Khwaja et al.'s protocol [1] uses symmetric cryptography to design a robust authentication protocol. In the enforcement of IoMT, RFID is required to create an identity authentication system as a key technology, which can effectually verify patients [2]. It is helpful to design a safe and efficient RFID for protecting user privacy, improving the safety of the IoMT system, and boosting the efficiency of medical staff to inspect and manage patients.

In medical scenes that need to efficiently verify a good deal of tags in a brief period, the employ of traditional per-tag protocols is inefficient and may put off the cure of patients. To solve the problem that uses the solution of homogeneous linear equations as a key to make the authentication data of the tag encipherment to further decrease the expense, Nikkhah et al. [3] proposed the LAPCHS protocol on account of the cloud healthcare system and analyzed and proved the safety of the protocol against various attacks by heuristic security analysis. Sarier et al. [4] proposed a new biometric based on non-transferable certificate scheme, which maintains the privacy and efficiency of biometric identification and can be easily integrated into the current BBIM system based on efficient brand and PS certificate.

Due to the low cost, high stability, and excellent characteristics of noncontact automatic identification of RFID system, it has been used in many fields, such as waste electronic product processing, farm management, and supply chain management [5–7]. In addition, in the field of healthcare, RFID technology is also widely used, such as drug management and vital signs detection [8, 9]. During the epidemic, RFID technology also participated in the establishment of the auxiliary information system for epidemic prevention, with the purpose of solving problems such as the management of epidemic material data and the management of epidemic information. Although the RFID system has many advantages in epidemic prevention and control, it faces the risks of security and privacy due to the usage of bottomed wireless media that enables (T, RE)'s mutual communication.

In order to design the secure RFID authentication solution, many protocols have been put forward to guarantee the security of RFID, but they have all been proved to have problems. In 2019, Khwaja et al. [1] proposed the lightweight authentication protocol. The authors claim that their protocol meets the necessary security requirements and solves most security issues. This paper finds that the protocol [1] is susceptible to database spoofing attacks, reader spoofing attacks, and asynchronous attacks. Therefore, this article proposes the new protocol on this basis, which can not only solve the problems of the abovementioned protocols but also can make the comprehensive comparison of multiple protocols, which has higher efficiency and security. The security of RAPUS + protocol is analyzed formally and informally through GNY logic, security verification tool AVISPA model. Through the above scheme, it is expected to improve the automation and decision-making efficiency of the epidemic prevention auxiliary information system.

This article analyzes the protocol [1] and improves realistic and lightweight certification protocol to guarantee protection against the known attacks:

(1) The protocol [1] is susceptible to database impersonation attacks and reader impersonation attacks

(2) The improved authentication protocols are proposed to resist all known attacks

(3) RAPUS + protocol performs formal and informally security analysis and compares it with relevant existing protocols on security features and performance

2. Related Work

A variety of certification protocols have been put forward to protect RFID systems [10–22], especially for lightweight cryptographic primitives. But many schemes based merely on the lightweight primitives were verified to be insecure, as shown in Table 1.

In 2014, Cho et al. [10] put forward the hash-based protocol. Later, Safkhani et al. [11] pointed out that the protocol [10] cannot withstand DoS attacks and impersonation attacks. In the same year, the ECC-based RFID authentication protocols [12, 13] were proposed to ensure communication security in the medical environment and improve patient safety. However, Farash et al. [14] proved through analysis that the protocols [12, 13] cannot ensure forward secrecy. In 2015, Gope et al. [15] proposed the lightweight protocol. But Khwaja et al. [1] pointed out that their protocol is susceptible to collision, DoS attacks, and stolen attacks. In 2018, Fan et al. [16] proposed the ultralightweight LRMI protocol to protect medical privacy. However, Aghili et al. [17] analyzed that the LRMI protocol cannot withstand traceability attacks and simulation attacks and proposed the SecLAP protocol. However, under the analysis of Safkhani et al. [18], it is found that the protocol in [17] is susceptible to traceability attacks and asynchronous attacks. In the same year, Fan et al. [21] put forward the lightweight authentication scheme on the basis of quadratic. Later, Zhu et al. [22] analyzed and proved that their scheme is susceptible to forward secrecy and impersonation attacks. In 2019, Zhou et al. [19] put forward the protocol on the basis of secondary residues. But the protocol [20] cannot withstand asynchronous attacks. Naeem et al. [23] presented an RFID authentication protocol and suggested an improvement to cater to the correctness and scalability issues. Li et al. [24] presented a mutual-healing group key distribution scheme based on the blockchain which can effectively resist various attacks with small overhead on time and storage. Amin et al. [25] provided an effective solution to solve all existing problems regarding key protocol methods to enhance security. The AVISPA simulation results in the solution ensure that active and passive attacks are protected. Lin et al. [26] constructed a novel secure mutual authentication system and proved the security and privacy requirements, including anonymity, traceability, and confidentiality. Shahidinejad et al. [27] introduced a lightweight authentication protocol for IoT devices named Light-Edge using a three-layer scheme.

Section 3 reviews the protocol [1]. Section 4 demonstrates RAPUS + protocol. In Section 5, the security analysis of the RAPUS + protocol is checked. Section 6 compares RAPUS + protocol with existing protocols. At last, Section 7 summarizes the article.

3. The Analysis of RAPUS Protocol

By examining the limitations of the RAPUS protocol, this section points out that it is susceptible to database impersonation attacks. Table 2 demonstrates the symbols used in the RAPUS protocol.

The doctor and many patients make up every cluster. Patients are moved from one cluster to another. Via the DB Server, the registered patients are authenticated by the doctor and the cluster. The symmetric key K_{rs} is shared between each Doctor and DB. The improved authentication scheme is made up of two parts: the tag registration part and the tag certification part. We have the medical data through the protocol. Besides, we use the decentralization, traceability, and nontampering characters of blockchain technology to guarantee the security of data storage and sharing.

T registrations steps are as follows, as shown in Figure 1.

Step PTR 1. *ID_{Ti} is submitted to the DB by each tag.*

Step PTR 2.

(1) A random number n_s is generated by DB.

(2) DB calculates $K_{ts} = h(ID_{Ti}||n_s) \oplus ID_s$.

(3) DB randomly generates r_i and encrypts it with s_x to calculate one-time alias tag_i's identity $AID = \text{E}_{sx}(ID_{Ti}||r_{Ti})$.

(4) DB authenticates tag_i based on AID_T.

(5) DB stores and delivers M_2 to tag.

Step PTR 3. Tag_i stores the information $M_2 = \{ID_{Ti}, K_{ts}, AID\}$ in its memory after receiving the messages from DB.

Table 1: The issues of lightweight authentication protocols.

Lightweight authentication protocols	Security issues
Cho et al. [10]	DoS and impersonation attacks [11]
Zhao et al. [12], Zhang et al. [13]	Cannot ensure forward secrecy [14]
Gope and Hwang [15]	Collision, DoS, and stolen-verifier attacks [1]
Fan et al. [16]	Traceability attacks and simulation attacks [17]
Aghili et al. [17]	Traceability attacks and asynchronous attacks [18]
Fan et al. [21]	Forward secrecy and impersonation attacks [22]
Zhou et al. [19]	Asynchronous attacks [20]

Table 2: Symbols and definitions of the RAPUS protocol.

Symbols	Definitions
T; S; R	RFID tag; database (DB); reader device
ID_{Ti}; AID_{Ti}; SID; R_j; N_t; N_r	i^{th} tag identity; one-time tag alias identity; shadow identity
K_{ts}; K_{emg}	j^{th} reader identity; Tag random number; reader random number
Tr_{seq}; K_{rs}	Shared key (shared emergency key) of server and tag
r_j	Track sequence number (used by both S and T)
$h(.)$; $\oplus$; $\|\|$	Hash function; the exclusive XOR operation; concatenation

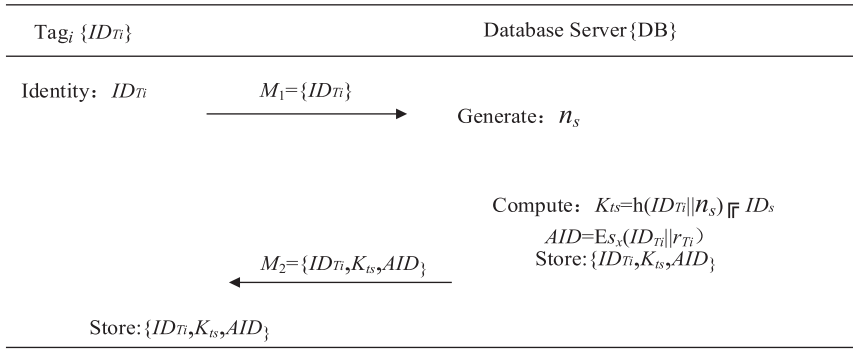

Figure 1: Tags registration phase.

The registered T starts the certification procedure, which is presented in Figure 2. The specific steps are as follows:

Step PTA 1:

(1) Nt is generated by an RFID tag with IDTi.
(2) $N_x = K_{ts} \oplus N_t$ and $V_1 = h(AID_{Ti}||K_{ts}||N_x||R_i)$ are derived.
(3) T delivers $M_{A1} = \{AID_{Ti}, N_x, T_1, V_1\}$ to R_i to start the authentication request.

Step PTA 2:

(1) R_i of the i^{th} cluster verifies the timestamp freshness as $(T_2 - T_1) \le \Delta T$.
(2) N_r is generated and $N_y = K_{rs} \oplus N_r$, $V_2 = h(M_{A1}||N_r||K_{rs})$ is calculated by R_i.
(3) R_i delivers $M_{A2} = \{N_y, R_i, V_2, M_{A1}, T_2\}$ to S.

Step PTA 3:

(1) S proves $(T_3 - T_2) \le \Delta T$ and then stems from $N_t = K_{ts} \oplus N_x$ and $N_r = K_{rs} \oplus N_y$.
(2) $V_1 = h(AID_{Ti}||K_{ts}||N_x||R_i)$ and $V_2 = h(M_{A1}||N_r||K_{rs})$ are calculated and verified by S.
(3) S decrypts AID_{Ti} as D_{Sx} $(ID_{Ti}||r_i)$.
(4) After successful authentication, S calculates $V_3 = h(R_i||N_r||K_{rs})$ and $V_4 = h(K_{ts}||ID_{Ti}||N_t)$.
(5) $AID_{Ti(new)} = E_{Sx}(ID_{Ti}||r_{i(new)})$ is updated and $Z_T = AID_{Ti(new)} \oplus K_{ts}$ is computed by S.
(6) S delivers $M_{A3} = \{V_3, V_4, ZT, T_3\}$ to R_i.

Step PTA 4:

(1) R_i checks the freshness of the timestamp $(T_4 - T_3) \le \Delta T$.
(2) R_i calculates $h(R_i||N_r||K_{rs})$ and verifies its equality with the received V_3.
(3) R_i delivers $M_{A4} = \{V_4, T_4, Z_T\}$ to tag$_i$.

Step PTA 5:

(1) Tag$_i$ checks the freshness of the timestamp after receiving M_{A4}.
(2) Tag$_i$ calculates and renews $AID_{Ti(new)}$=$(Z_T \oplus K_{ts})$, $AID_{Ti} = AID_{Ti(new)}$, if Tag$_i$ successfully verifies the messages $(T_5 - T_4) \le \Delta T$, $V_4 * ? = h(K_{ts}||ID_{Ti}||N_t)$.
(3) Tag$_i$ saves the information.
(4) Otherwise, AID_{Ti} will not update.

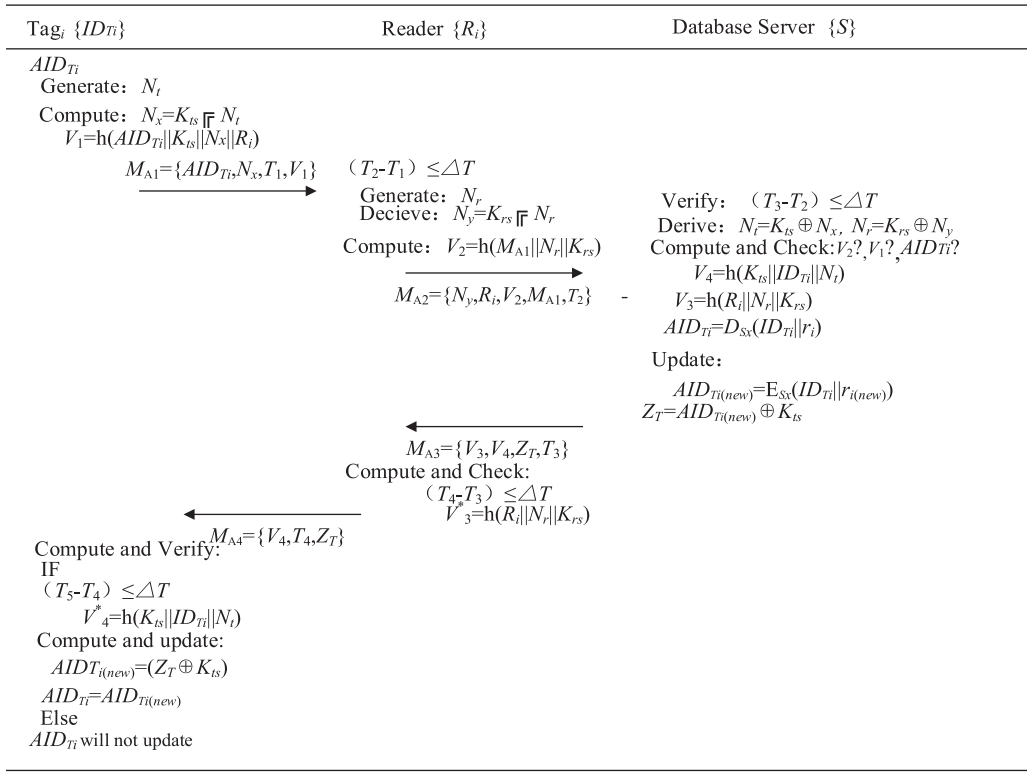

Figure 2: Tags authentication phase.

3.1. Vulnerable to Database Impersonation Attacks for RAPUS Protocol

3.1.1. Phase 1 (Learning). After receiving $M_{A2} = \{N_y, R_i, V_2, M_{A1}, T_2\}$ from the reader, the DB performs as follows:

STEP 1.1. *S proves* $(T_3-T_2) \le \Delta T$ *and then stems from* $N_t = K_{ts} \oplus N_x$ *and* $N_r = K_{rs} \oplus N_y$.

STEP 1.2. $V_1 = h(AI\ DT\ i \| K_{ts} \| N_x \| R_i)$ *and* $V_2 = h(M_{A1} \| N_r \| K_{rs} \| T_2)$ *are calculated and verified by S.*

STEP 1.3. *S* decrypts $AI\ DT_i$ as $DS_x\ (I\ DT_i || r_i)$ in order to verify it.

STEP 1.4. $V_3 = h\ (R_i \| N_r \| K_{rs} \| T_3)$ *and* $V_4 = h\ (K_{ts} \| I\ DT_i \| N_t \| T_3)$ *are calculated by S, after successful verification.*

STEP 1.5. $AI\ DT_{i\ (new)} = ES_x\ (I\ DT_i \| r_{i(new)})$ *is updated and* $Z_T = AI\ DT\ i_{new} \oplus KT_s$ *is computed by S.*

STEP 1.6. *S delivers* M_{A3} *to* R_i.

3.1.2. Phase 2 (Database Impersonation Attacks). To imitate the database, the attacker starts a new session:

STEP 2.1. The attacker eavesdrops Z_T.

STEP 2.2. The attacker maliciously modifies $Z_T' = Z_T \oplus 1$.

STEP 2.3. The reader's verification method V_3 does not check the integrity of Z_T.

STEP 2.4. At this time, the database impersonation attacks succeed.

3.2. Vulnerable to Reader Impersonation Attacks for RAPUS Protocol

3.2.1. Phase 1 (Learning). After receiving $M_{A3} = \{V_3, V_4, Z_T, T_3\}$ from the DB, the reader performs the following steps.

STEP 1.1. R_i checks freshness of the timestamp $(T_4-T_3) \le \Delta T$.

STEP 1.2. R_i calculates $h(R_i \| N_r \| K_{rs})$ and proves that it equals V_3.

STEP 1.3. R_i delivers M_{A4} to tag_i.

3.2.2. Phase 2 (Reader Imitation Attacks). To imitate the reader, the attacker imitates the new routine:

STEP 2.1. The reader continues to send the modified data $Z_T'(Z_T \oplus 1)$ to T.

STEP 2.2. T's validation method does not verify the integrity of Z_T.

STEP 2.3. The reader's impersonation attacks succeed.

3.3. Vulnerable to Asynchronous Attacks

STEP 1. The above two processes lead to the wrong updating of cryptographic key $AID'_{Ti(new)}=(Z' \ T \oplus K_{Ts})$.

STEP 2. In the second round of conversation, T key $AID'_{Ti(new)}$ and T key $AID_{Ti(new)}=(Z_T \oplus K_{Ts})$ stored in the database are inconsistent.

STEP 3. Therefore, it results in asynchronous attacks.

4. The Improved RAPUS + Protocol

RAPUS + protocol is shown in Figure 3.

Step PTA 1:

(1) N_t is generated by RFID tag with ID_{Ti}.
(2) $N_x = K_{ts} \oplus N_t$ and $V_1 = h(AID_{Ti}||K_{ts}||N_x||R_i)$ are exported.
(3) T delivers $M_{A1} = \{AID_{Ti}, N_x, T_1, V_1\}$ to R_i.

Step PTA 2:

(1) R_i of the i^{th} cluster first proves the timestamp freshness as $(T_2 - T_1) \leq \Delta T$, as soon as the request is received from T.
(2) N_r is generated by R_i.
(3) $N_y = K_{rs} \oplus N_r$ and $V_2 = h(M_{A1}||N_r||K_{rs}||T_2)$ are computed.
(4) R_i delivers $M_{A2} = \{N_y, R_i, V_2, M_{A1}, T_2\}$ to S.

Step PTA 3:

(1) S proves $(T_3 - T_2) \leq \Delta T$ and then stems from $N_t = K_{ts} \oplus N_x$ and $N_r = K_{rs} \oplus N_y$.
(2) S calculates and proves $V_1 = h(AID_{Ti}||K_{ts}||N_x||R_i)$ and $V_2 = h(M_{A1}||N_r||K_{rs}||T_2)$.
(3) S decrypts AID_{Ti} as $D_{Sx}(ID_{Ti}||r_i)$ to verify it.
(4) After verifying successfully, S renews $V_3 = h(R_i||N_r||K_{rs}||Z_T)$ and $V_4 = h(K_{ts}||ID_{Ti}||N_t||Z_T)$.
(5) $AID_{Ti(new)} = E_{Sx}(ID_{Ti}||r_{i(new)})$ is updated and $Z_T = AID_{Ti(new)} \oplus K_{ts}$ is computed by S.
(6) S delivers $M_{A3} = \{V_3, V_4, Z_T, T_3\}$ to R_i.

Step PTA 4:

(1) R_i verifies the freshness of the timestamp $(T_4 - T_3) \leq \Delta T$ after receiving M_{A3}.
(2) R_i calculates and verifies $h(R_i \ ||N_r \ ||K_{rs} \ ||Z_T) = V_3$.
(3) R_i delivers $M_{A4} = \{V_4, T_4, Z_T\}$ to tag_i after successful verification.
(4) If not, R_i ends the session.

Step PTA 5:

(1) Tag_i checks the freshness of the timestamp after receiving M_{A4}.
(2) Tag_i calculates and renews $AID_{Ti(new)}=(Z_T \oplus K_{ts})$, $AID_{Ti} = AID_{Ti(new)}$ if Tag_i verifies the message $V_4 * ? = h(K_{ts} \ ||ID_{Ti}||N_t||Z_T)$.
(3) Tag_i saves the information.
(4) Otherwise, AID_{Ti} will not update.

5. The Analysis of RAPUS + Protocol

The security of the RAPUS + protocol is analyzed through formal analysis and explains the informal security features under the GNY logic model and AVISPA model.

5.1. The Informal Analysis. In the following subsections, we analyze the security of the RFID system.

5.1.1. Mutual Authentication between Tag and Server. The DB verifies AID_{Ti} and $V_1 = h(AID_{Ti}||K_{ts}||N_x||R_i)$ in M_1 to authenticate RFID tag. Only the legitimate T can form the effective request M_1, which includes the two parameters. As effective AID_{Ti}, it only knows legal T. Besides, the legal tag only knows (ID_T, K_{ts}). The RFID tag can use V_4 and M_3 in M_4 to authenticate the legitimacy of the DB. The mutual authentication property can be achieved by RAPUS + protocol.

5.1.2. Anonymity. The most basic element of the secure protocol is anonymity. The personal information of the user is protected by a secure scheme so that the adversary has no access to any information. The protocol has achieved strong anonymity. During the registration part, the RFID tag used $M = \{ID_{Ti}, K_{ts}, AID\}$ to identify the S through RFID-Reader.

The messages $M_{A1} = \{AID_{Ti}, N_x, V_1, T_1\}$ have been delivered to the S through a public channel in the authentication part. The adversary cannot attain the identity of the RFID tag even if the adversary gets the message M_1 for the reason that AID_{Ti} is the one-time alias identity of T. The initial identity is kept encoded in AID_{Ti}. It can only be encoded by the DB using K_{ts}. Therefore, the adversary cannot destroy the RFID tag's authentic identity. In this way, we achieve the anonymity of the protocol.

5.1.3. Traceability. A safe protocol can protect any identity information of the participants from illegal users. The traceability of the RFID tag may be caused by identifying information. RAPUS + protocol cannot reveal the login information of the conversation that causes the security attack.

The protocol needs to use (N_t, N_r, r_i). It is impossible for the adversary to achieve any random number in the RFID system because the RFID tag's new one-time alias identity AID_{Ti} has already been used. Therefore, the protocol meets the untraceability.

5.1.4. Backward/Forward Secrecy. It is essential for security protocols to ensure that the information transferred during a phase is not threatened and traced by the adversary, as it may generate defects in the certification phase between T and S. In our proposed scheme, the previous and next sessions will

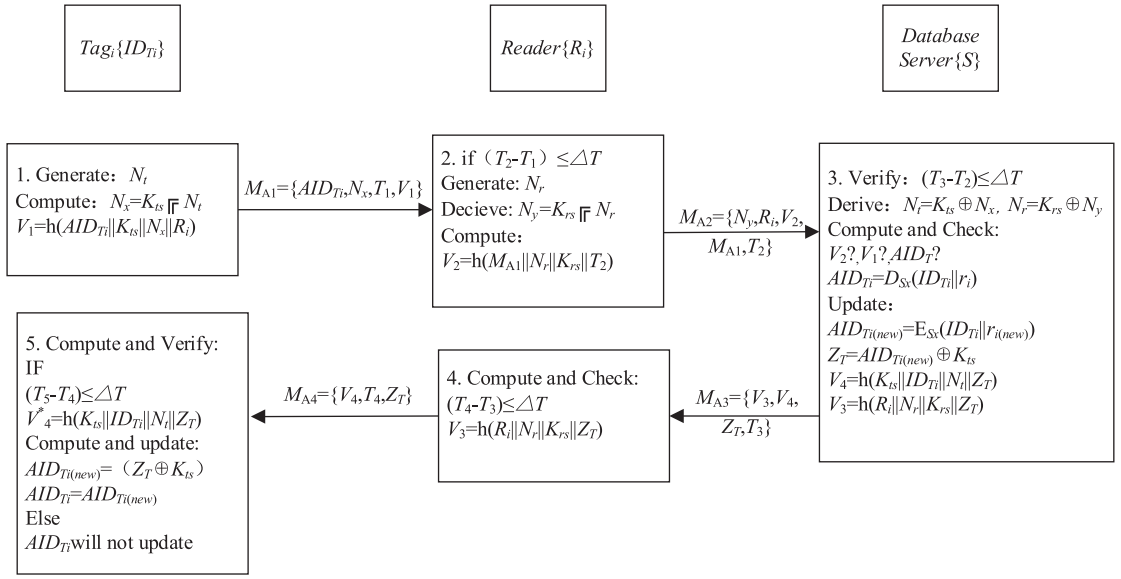

Figure 3: The improved RAPUS + protocol.

not be affected, even if the identity ID_T is lost. The encrypted AID_{Ti} is updated in each new session to ensure it. Therefore, the backward and forward secrecy of the RAPUS + protocol can be guaranteed.

5.1.5. Scalability. In RAPUS + protocol, the detailed procedure is used to verify if any T is not performed by the RFID Server S. Oppositely, S disposes AID_{Ti} to verify T and makes a quick response to T. Therefore, RAPUS + protocol gets more stable.

5.1.6. DoS Attacks. For any random key which is in charge of verification or authentication of T, the protocol is not based on them. Instead, it is on the basis of AID_{Ti}. Moreover, it is well encoded and renewed for each transaction. Hence, the proposed scheme defenses against DoS attack.

5.1.7. Replay Attacks. In the replay attack, to authenticate S, the attacker may postpone and repeat the transferred information. (T, RE, DB) are included in RAPUS + protocol. For authentication, $\{M_1, M_2, M_3, M_4\}$ are exchanged through the public channel. Accessible to the messages, the attackers try to launch the replay attacks.

Nevertheless, due to the messages delivered with the fresh timestamp T, the attempt will fail. The adversary request will be repulsed each time in the event of timestamp's ineffectiveness. Besides, the adversary cannot launch the attacks if it cannot calculate the parameters of the messages, because all messages' parameters are updated by the participants for every new session. RAPUS + protocol is able to resist replay attacks.

5.1.8. Location Tracking Attacks. The authentic identity of the RFID tag is not delivered firsthand. Therefore, it has been delivered in the encoded form for authentication between the RFID tag and S. And only the server can decrypt through its secret key. Besides, in every new session, the unpredictability of messages is continually renewed. Therefore, the adversary cannot seek out the location. Any attempt to find the location will finally become a failure.

5.1.9. Impersonation Attacks. To authenticate the server, adversary A holds up the messages of the valid T and changes it. On this occasion, adversary A needs to issue the legitimate message request including (N_y, R_i, V_2, M_{A1}, AID_{Ti}). In order to achieve it, AID_{Ti} is encrypted and calculated and cannot be forged by adversary A.

Besides, to submit the legitimate request for certification as the valid T, adversary A demands various other timestamps and parameters too. Adversary A is impossible to know the real parameters used for certification. Therefore, it has no ability to verify its validity as T to the DB. RAPUS + protocol for RFID system can resist any forgery attack reluctantly.

5.1.10. Stolen-Verifier Attacks. All the validation and verification keys are encrypted and stored in the DB. Although the data and keys are both stolen from the DB, they cannot be decrypted and extracted by adversary A. Moreover, the original data saved in DB cannot be altered or modified by adversary A. Therefore, the RAPUS + protocol resists the stolen-verifier attacks.

5.2. The Formal Analysis Using GNY Logic. In order to guard against major attacks, the proposal of the security protocol design must be analyzed ahead of execution. The fundamental assumptions are presented in Table 3.

The aims verified by RAPUS + protocol are as follows:

(i) Goal 1: $R_i \mid \equiv tag \overset{AID_T}{\longleftrightarrow} R_i$

(ii) Goal 2: $R_i \mid \equiv T \mid \equiv tag \overset{AID_T}{\longleftrightarrow} R_i$

Table 3: The assumptions used for RAPUS + protocol under the GNY logic.

T_i $\{ID_{Ti}\}$	*Reader* $\{R_i\}$	*Database Server* $\{S_j\}$
$T\mid \equiv \#(N_t)$	$R_i \mid \equiv \#(N_r)$	$S_j \mid \equiv \#(AID_{Ti})$ (r_i)
$T\mid \equiv S_j \Rightarrow r_i$	$R_i \mid \equiv S_j \Rightarrow r_i$	$Sj \mid \equiv R_i \Rightarrow N_r$
$T\mid \equiv R_i \Rightarrow N_r$	$R_i \mid \equiv T \Rightarrow N_t$	$Sj \mid \equiv T \Rightarrow N_t$

(iii) Goal 3: $S_j \mid \equiv R_i \overset{AID_T}{\longleftrightarrow} S_j$

(iv) Goal 4: $Sj \mid \equiv R_i \mid \equiv R_i \overset{AID_T}{\longleftrightarrow} S_j$

(v) Goal 5: $R_i \mid \equiv S_j \overset{AID_T}{\longleftrightarrow} R_i$

(vi) Goal 6: $R_i \mid \equiv S_j \mid \equiv S_j \overset{AID_T}{\longleftrightarrow} R_i$

(vii) Goal 7: $T \mid \equiv R_i \overset{AID_T}{\longleftrightarrow} tag$

(viii) Goal 8: $T \mid \equiv R_i \mid \equiv R_i \overset{AID_T}{\longleftrightarrow} tag$

The protocol messages generated by the parser are as follows:

(i) M_1: $T \longrightarrow R_i$: AID_T, N_x:< N_t >K_{ts}, V_1, T_1

(ii) M_2: $R_i \longrightarrow S_j$: M_1, N_y:< N_r >K_{rs}, R_i, V_2, T_2

(iii) M_3: $S_j \longrightarrow R_i$: V_3, V_4, Z_t:<AID_{Ti}> $*_{Kts}$, T_3

(iv) M_4: $R_i \longrightarrow T$: V_4, T_4, Z_t:< AID_{Ti} >$_{Kts}$

The goals (G_1, G_2, G_3, G_4, G_5, G_6, G_7, G_8, G_9) are made to verify the RAPUS + protocol that has been certified. The sequence of logical assumptions is employed in the parser export to achieve the security goals by considering the various assumptions.

In M_1, T_1 is the timestamp of T. Using the seeing rule, we can get

$$R_i \triangleleft AIDT_i, SID, N_x: \ < N_t >_{Kts}, T1. \tag{1}$$

Applying the message-meaning rule and the previous step result,

$$R_i \mid \equiv tag \mid \sim N_t. \tag{2}$$

Using the freshness-conjuncatenation rule and the previous step results,

$$R_i \mid \equiv tag \mid \equiv N_t \tag{3}$$

According to the jurisdiction rule and the previous step result,

$$R_i \mid \equiv N_t. \tag{4}$$

Applying the previous step result and the session-key rule,

$$R_i \mid \equiv tag \overset{AID_{Ti}}{\longleftrightarrow} R_i \,(\textbf{Goal}1). \tag{5}$$

Using the nonce-verification rule,

$$R_i \mid \equiv tag \mid \equiv tag \overset{AID_{Ti}}{\longleftrightarrow} R_i \,(\textbf{Goal}2). \tag{6}$$

In M_2, T_2 is the timestamp of R_i. Applying the seeing rule, we get

$$S_j \triangleleft M1, N_y: \ < N_r > K_{rs}, T2, V2. \tag{7}$$

According to the message-meaning rule and the previous step result,

$$S_j \mid \equiv R_i \mid \sim N_r. \tag{8}$$

By the freshness-conjuncatenation rule and the previous step result, we get

$$S_j \mid \equiv R_i \mid \equiv N_r. \tag{9}$$

Through the jurisdiction rule and the previous step result,

$$S_j \mid \equiv N_r. \tag{10}$$

Applying the S_{10} and the *SK* rule,

$$S_j \mid \equiv R_i \overset{AID_{Ti}}{\longleftrightarrow} S_j \,(\textbf{Goal}3). \tag{11}$$

According to the nonce-verification rule and the previous step result,

$$S_j \mid \equiv R_i \mid \equiv R_i \overset{AID_{Ti}}{\longleftrightarrow} S_j \,(\textbf{Goal}4). \tag{12}$$

In M_3, T_3 is the timestamp of S_j. Through the seeing rule, we get

$$R_i \triangleleft V3, V4, Z_t < AIDT_{inew} >^{*}_{K_{ts}}, T3. \tag{13}$$

Applying the message-meaning rule and S_{13},

$$R_i \mid \equiv S_j \mid \sim AIDT_{inew}. \tag{14}$$

Through S_{14} and the freshness-conjuncatenation rule,

$$R_i \mid \equiv S_j \mid \equiv AIDT_{inew}. \tag{15}$$

According to the assumption S_{15} and jurisdiction rule,

$$R_i \mid \equiv AIDT_{inew}. \tag{16}$$

Applying S_{16} and the session-key rule,

$$R_i \mid \equiv S_j \overset{AID_{inew}}{\longleftrightarrow} R_i \,(\textbf{Goal}5). \tag{17}$$

Using the nonce-verification rule,

$$R_i \mid \equiv S_j \mid \equiv S_j \overset{AID_{inew}}{\longleftrightarrow} R_i \,(\textbf{Goal}6). \tag{18}$$

In M_4, T_4 is the timestamp of R_i. Applying the seeing rule,

$$tag \triangleleft V4, Zt < AIDT_{inew} \geq >_{ts}, T4. \tag{19}$$

Through the message-meaning rule and S_{19},

$$tag \mid \equiv R_i \mid \sim AIDT'_{inew}. \tag{20}$$

According to S_{20} and the freshness-conjuncatenation rule,

$$tag \mid \equiv R_i \mid \equiv AIDT_{inew}. \tag{21}$$

Applying the jurisdiction rule and S_{21},

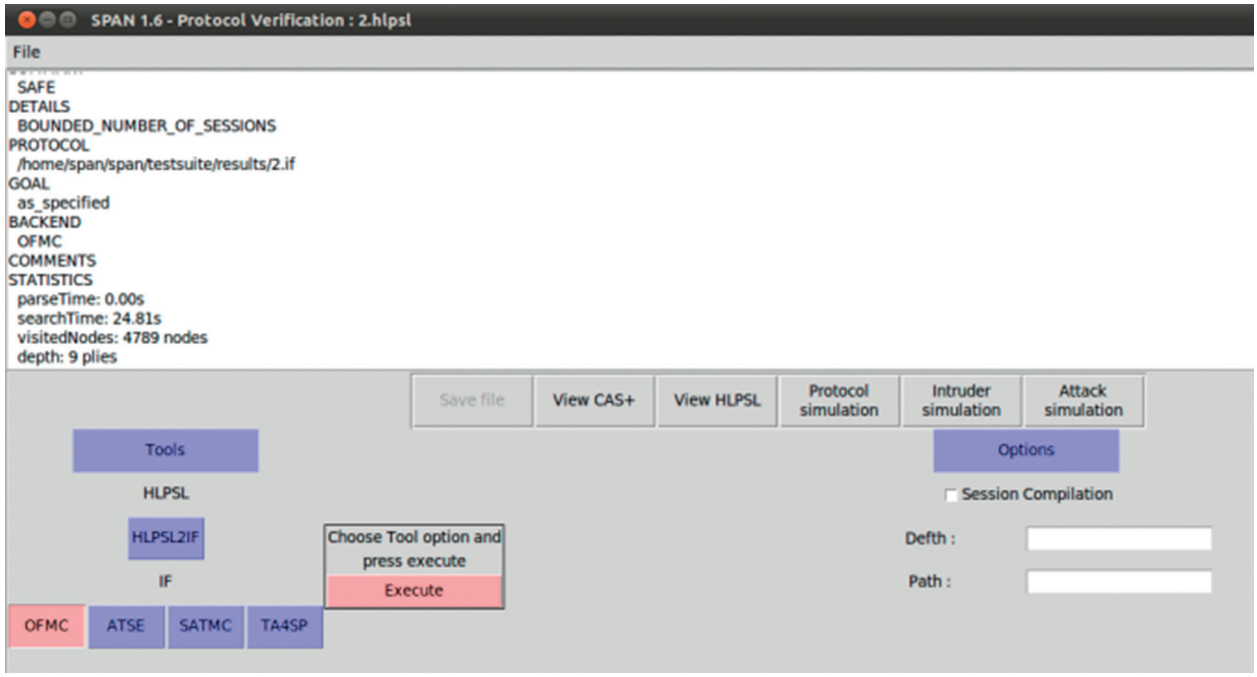

Figure 4: AVISPA execution of RAPUS + protocol.

$$tag| \equiv AIDT_{inew}. \tag{22}$$

By the session-key rule, we get

$$tag| \equiv R_i \overset{AID_{inew}}{\longleftrightarrow} tag\,(\textbf{Goal}7). \tag{23}$$

Finally, according to the nonce-verification rule,

$$tag| \equiv R_i| \equiv R_i \overset{AID_{inew}}{\longleftrightarrow} tag\,(\textbf{Goal}8). \tag{24}$$

As a result, it is proved that (T, R_i, S_j) achieve successful reciprocal certification and obtain the session-key agreement safely.

5.3. The Protocol Verification Using AVISPA Tool. The AVISPA is the formal security protocol analysis tool. It uses the High-Level Protocol Specification Language (HLPSL) to specify the sequence of messages exchanged among different entities. The basic role is the module consisting of the action of each entity. The entities combine multiple basic roles into the composed role to interact with each other. The analyzed protocol's security goals are specified in the goal phase. It has four back ends, including OFMC, CL-Atse, SATMC, and TA4sp, which use different kinds of techniques to show whether the RAPUS + protocol is safe or not. The tool supplies tracking of the steps that lead to the attack and uses the Dolev-Yao intruder model that can eavesdrop, intercept messages, modify passing traffic, or insert bogus data. In our proposed scheme, we describe different entities' actions by defining the basic role and how the entities in the composed role interact with each other. The results present that our proposed scheme is "safe" against OFMC with regard to the security goal in Figure 4. Appendix A shows all source programs by AVISPA.

5.4. Performance Analysis and Comparison. This phase conducts the comparative analysis between the RAPUS + protocol and the existing protocol. First of all, we compare the existing protocol with the RAPUS + - protocol in terms of security requirements. Besides, based on the calculation cost, we compare the RAPUS + protocol with the existing protocol. Lastly, we compare the RAPUS + protocol with existing protocols in regard to model analysis.

5.4.1. Security Requirements. This section analyzes the existing authentication protocols based on symmetric keys from the perspective of security requirements. Table 4 presents the comparisons between the proposed agreement and the existing agreement [1, 10, 15, 28–30].

Table 4 shows the insecurities of existing protocols [1, 10, 15, 28–30]. The result shows that only RAPUS + - protocol can provide all the above security features, such as mutual authentication, untraceability, anonymity, the backward/forward secrecy, scalability, collision attacks, DoS attacks, replay attacks, location tracking attacks, stolen-verifier attacks, database impersonation attacks, and reader impersonation attacks.

5.4.2. Computational Cost. The computation cost analysis of existing related protocols [1, 10, 15, 28–30] with RAPUS + protocol is given in this section. Table 5 presents the analysis of computation cost.

In the protocol proposed in [15], the computational cost of each (T, R, S) is $5Th$, $2Th$, and $7Th$, so the total cost is $14Th$. The protocol proposed in [29] needs $2Th$, $2Th$, and $3Th$ for each (T, R, S), and the total cost is $7Th$. The cost of protocol

Table 4: Security requirements comparisons.

Requirements	[27]	[23]	[28]	[29]	[30]	[10]	[15]	[1]	Ours
SR1	√	√	×	×	×	√	×	√	√
SR2	√	√	×	×	×	√	--	--	√
SR3	√	√	×	×	×	√	--	--	√
SR4	√	√	√	×	×	√	--	--	√
SR5	√	√	×	×	×	√	--	--	√
SR6	√	√	×	×	×	×	×	√	√
SR7	√	√	×	×	×	×	×	√	√
SR8	√	√	×	×	×	×	√	√	√
SR9	--	--	--	--	--	--	--	--	√
SR10	--	--	--	--	--	--	--	--	√
SR11	--	--	--	--	--	--	--	×	√
SR12	--	--	--	--	--	--	--	×	√

SR1: mutual authentication. SR2: tag untraceability. SR3: tag anonymity. SR4: backward/forward secrecy. SR5: scalability. SR6: collision attacks. SR7: DoS attacks. SR8: replay attacks. SR9: location tracking attack. SR10: stolen-verifier attacks. SR11: database impersonation attacks. SR12: reader impersonation attacks. √: yes provides; ×: does not provide.

Table 5: Comparisons of computation cost.

Computation cost	[15]	[29]	[30]	[10]	[28]	[1]	Ours
^{CC}tag	$5T_h$	$2T_h$	$4T_h$	$3T_h$	$2T_h$	$2T_h$	$2T_h$
CC_{Ri}	$2T_h$	$2T_h$	$2T_h$	$2T_h$	$3T_h$	$2T_h$	$1T_h$
CC_S	$7T_h$	$3T_h$	$6T_h$	$5T_h$	$5T_h$	$4T_h + 2T_{se}$	$3T_h + 2T_{se}$
^{CC}Total	$14T_h$	$7T_h$	$12T_h$	$10T_h$	$10T_h$	$8T_h + 2T_{se}$	$6T_h + 2T_{se}$

CC: computation cost; T_h: CC of single hash function; T_{se}: CC of symmetric encryption/decryption.

Table 6: Comparisons of model analysis.

Formal model	[27]	[23]	[28]	[29]	[30]	[10]	[15]	[1]	Ours
BAN	×	×	×	×	×	×	×	×	×
GNY	×	×	×	×	×	√	×	×	√
AVI	√	×	×	×	×	×	×	×	√
ProVerif	×	×	×	×	×	√	×	×	×

demonstrated in [30] is $4Th$, $2Th$, and $6Th$ correspondingly, amounting to $12Th$. In the protocol proposed in [10], each (T, R, S) generates $3Th$, $2Th$, and $5Th$ cost correspondingly, so the total cost is $10Th$. The cost of protocol demonstrated in [28] is $2Th$, $3Th$, and $5Th$ correspondingly, amounting to $10Th$. The protocol proposed in [1] needs $2Th$, $2Th$, and $4Th + 2Tse$ for each (T, R, S), so the total cost is $8Th + 2Tse$. In comparison, T requires $2Th$, the reader requires $1Th$, and the server requires $3Th + 2Tse$, and the total cost is $6Th + 2Tse$ in the protocol proposed in this article. In general, the protocol proposed in this article has a relatively smaller computation cost and is the only one that can withstand all known attacks.

5.5. Comparisons of Model Analysis. This section describes a model analysis of RAPUS + protocol with existing multitag authentication protocols in Table 6.

The results show that most protocols lack or have no model analysis. In the proposed authentication protocol, the secrecy attacks are analyzed by automatic cryptographic protocol verifier tools AVISPA. GNY logic is applied to verify the reciprocal certification.

6. Conclusion

The auxiliary information system for epidemic prevention and control has integrated traditional medical systems with RFID technology. However, the antitampering of logistics data and management and control of epidemic materials are still challenges. In this article, we prove that the RAPUS protocol is susceptible to database impersonation attacks, reader impersonation attacks, and asynchronous attacks. Then, the RAPUS + protocol is proposed. The security analysis of the RAPUS + protocol has been conducted through GNY logic, AVISPA model. Additionally, the comparisons of RAPUS + protocol with the existing protocols prove the superiority in security, computational cost, and model analysis. Based on RAPUS + protocol, the safety and management of epidemic prevention materials will be greatly improved.

Appendix

A. The Source Programs under AVISPA Model

```
role reader(
  R,T,S:agent,
  H:hash_func,
  SND_TR,RCV_TR,SND_SR,RCV_SR:
channel(dy)
)
played_by R
def=
      local
    State:nat,
    R0,DID,C0,RID,C1,R1,
    C2,Tid,C3,TID,OID,C4,
    C5,C6,TS1,TS3,C7,SR,C8,KRC,C9,
    Tidnew,C10,C11,C12:text
const
tag_reader_c3,tag_reader_c7,reader_tag_c7:
protocol_id
init State:=0
transition
(1) State=0/\RCV_SR(start)=|>
    State':=1
    /\R0':=new()
    /\C0':=H(R0'.DID)
    /\C1':=xor(DID,RID)
    /\SND_TR(R0'.C0'.C1')
(2) State=1/\RCV_TR(C2'.C3'.C4'.C5'.C6'.R1')=|>
    State':=2
    /\C7':=xor(C3',xor(H(RID.DID),TS1))
    /\C8':=xor(OID,SR)
    /\SND_SR(TS1.C7'.C8'.H(RID).H(TS1.C7'.C8'.
H(RID).KRC).R1')
    /\witness(R,T,reader_tag_c7,C7')
(3) State=2/\RCV_SR(C9'.H(C9'.KRC))=|>
    State':=3
    /\Tidnew':=xor(R1,Tid)
    /\C10':=xor(Tidnew',SR)
    /\SND_SR(C10'.TS3.H(C10'.TS3.KRC))
(4) State=3/\RCV_SR(C11'.H(C11',KRC))=|>
    State':=4
    /\C12':=xor(H(TID.DID.OID),R1)
    /\SND_TR(C12')
end role
role tag(
  R,T,S:agent,
  H:hash_func,
  SND_RT,RCV_RT:channel(dy)
)
played_by T
def=
      local
    State:nat,
    R0,DID,C0,RID,C1,R1,
    C2,Tid,C3,TID,OID,C4,
    C5,C6,TS1,TS3,C7,SR,C8,KRC,C9,
    Tidnew,C10,C11,C12:text
const  tag_reader_c3,tag_reader_c7,reader_tag_c7:
protocol_id
init State:=0
transition
(1) State=0/\RCV_RT(R0'.C0'.C1')=|>
    State':=1
    /\R1':=new()
    /\C2':=xor(RID,xor(Tid,R1'))
    /\C3':=xor(DID,xor(H(TID.DID.R1'),RID))
    /\C4':=xor(OID,H(RID.R0'))
    /\C5':=H(OID.R0'.C3')
    /\C6':=H(RID.R0'.R1')
    /\SND_RT(C2'.C3'.C4'.C5'.C6'.R1')
    /\witness(T,R,tag_reader_c3,C3')
    /\witness(T,R,tag_reader_c5,C5')
(1) State=1/\RCV_RT(C12')=|>
    State':=2
end role
role server(
  R,T,S:agent,
  H:hash_func, SND_RS,RCV_RS:channel(dy)
)
played_by S
def=
      local
    State:nat,
    R0,DID,C0,RID,C1,R1,
    C2,Tid,C3,TID,OID,C4,
    C5,C6,TS1,TS3,C7,SR,C8,KRC,C9,
    Tidnew,C10,C11,C12:text
const  tag_reader_c3,tag_reader_c7,reader_tag_c7:
protocol_id
init State:=0
transition
(1) State=0/\RCV_RS(TS1.C7'.C8'.H(RID).H(TS1.C7'.
C8'.H(RID).KRC).R1')=|>
```

```
State': = 1
/\C9': = xor(Tid,SR)
/\SND_RS(C9'.H(C9'.KRC))
(2 ) State = 1/\RCV_RS(C10'.TS3.H(C10'.TS3.KRC)) =
|>
State': = 2
/\Tidnew': = xor(C10′,SR)
/\C11': = xor(H(TID.DID.OID),xor(Tidnew',SR))
/\SND_RS(C11'.H(C11′,KRC))
end role
role session(
   R,T,S:agent,
      H:hash_func
      )
   def =
      local
            SSR,RSR,STR,RTR,SRT,RRT,SRS,RRS:
channel(dy)
      composition
reader(R,T,S,H,STR,RTR,SSR,RSR)
      /\tag(R,T,S,H,SRT,RRT)
      /\server(R,T,S,H,SRS,RRS)
end role
role environment()
      def =
      const
            r,t,s:agent,
            h:hash_func,
            tag_reader_c3,ta-
g_reader_c7,reader_tag_c7:protocol_id
      intruder_knowledge = {r,t,s}
composition
      session(r,t,s,h)
      /\session(r,t,s,h)
      /\session(r,t,s,h)
end role
goal
authentication_on tag_reader_c3
authentication_on tag_reader_c7
authentication_on reader_tag_c7
end goal
environment()
```

Data Availability

The data served to support the findings of this study are contained within the article.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work is supported in part by China Postdoctoral Science Foundation (Grant No. 2020T130098ZX) and National Key Research and Development Program (Grant No. 2020YFB1711500).

References

[1] K. Mansoor, A. Ghani, S. Chaudhry, S. Shamshirband, S. Ghayyur, and A. Mosavi, "Securing IoT-based RFID systems: a robust authentication protocol using symmetric cryptography," *Sensors*, vol. 19, no. 21, pp. 40–54, 2019.

[2] J. Kang, K. Fan, K. Zhang, X. Cheng, H. Li, and Y. Yang, "An ultralight weight and secure RFID batch authentication scheme for IoMT," *Computer Communications*, vol. 167, no. 2, pp. 48–54, 2020.

[3] F. Nikkhah and M. Safkhani, "LAPCHS: a lightweight authentication protocol for cloud-based health-care systems," *Computer Networks*, vol. 187, no. 1, pp. 167–169, 2021.

[4] N. D. Sarier, "Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management," *Computers & Security*, vol. 105, no. 5, pp. 125–132, 2021.

[5] R. Przemyslaw, L. Agnieszka, S. Ewa et al., "Welfare health and productivity in commercial pig herds," *Animals*, vol. 11, no. 4, pp. 2263–2278, 2021.

[6] G. Li, M. K. Lim, and Z. H. Wang, "Stakeholders, green manufacturing, and practice performance: empirical evidence from Chinese fashion businesses," *Annals of Operations Research*, vol. 290, no. 1-2, pp. 961–982, 2020.

[7] J. Srinivas, D. Ashok Kumar, and V. Athanasios, "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7081–7093, 2020.

[8] S. Fatty M and A. Ruhul, "A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS," *Information Sciences*, vol. 527, no. 2, pp. 382–393, 2020.

[9] S. Zhang, X. Liu, Y. Liu, B. Ding, S. Guo, and J. Wang, "Accurate respiration monitoring for mobile users with commercial RFID devices," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 513–525, 2021.

[10] J. S. Cho, Y. S. Jeong, and S. O. Park, "Consideration on the brute-force attack cost and retrieval cost: a hash-based radio-frequency identification (RFID) tag mutual authentication protocol," *Computers & Mathematics with Applications*, vol. 69, no. 1, pp. 58–65, 2015.

[11] M. Safkhani, P. Peris-Lopez, J. C. Hernandez-Castro, and N. Bagheri, "Cryptanalysis of the Cho et al. protocol: a hash-based RFID tag mutual authentication protocol," *Journal of Computational and Applied Mathematics*, vol. 259, no. 2, pp. 571–577, 2014.

[12] Z. Zhao, "A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem," *Journal of Medical Systems*, vol. 38, no. 5, pp. 46–273, 2014.

[13] Z. Zhang and Q. Qi, "An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography," *Journal of Medical Systems*, vol. 38, no. 47, pp. 47–23, 2014.

[14] M. S. Farash, O. Nawaz, K. Mahmood, S. A. Chaudhry, and M. K. Khan, "A provably secure RFID authentication protocol based on elliptic curve for healthcare environments," *Journal of Medical Systems*, vol. 40, no. 7, pp. 152–154, 2016.

[15] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," *Computers & Security*, vol. 55, no. 125, pp. 271–280, 2015.

[16] K. Fan, S. Zhu, K. Zhang, H. Li, and Y. Yang, "A lightweight Authentication scheme for cloud-based RFID healthcare systems," *IEEE Network*, vol. 33, no. 131, pp. 44–49, 2019.

[17] S. F. Aghili, H. Mala, P. Kaliyar, and M. Conti, "SecLAP: secure and lightweight RFID authentication protocol for medical IoT future gener," *Computer Systems*, vol. 101, no. 16, pp. 621–634, 2019.

[18] M. Safkhani, Y. Bendavid, and S. Rostampour, "On designing lightweight RFID security protocols for medical IoT," *Computer Networks*, vol. 187, no. 2, pp. 432–442, 2020.

[19] Z. Zhou, P. Wang, and Z. Li, "A quadratic residue-based RFID authentication protocol with enhanced security for TMIS," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 2, pp. 3603–3615, 2019.

[20] M. Safkhani and A. Vasilakos, "A new secure authentication protocol for telecare medicine information system and smart campus," *IEEE Access*, vol. 7, no. 1, pp. 23514–23526, 2019.

[21] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFID protocol for medical privacy protection in IoT," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 101, pp. 1656–1665, 2018.

[22] Z. Zhu, P. Li, H. Xu, and R. Wang, "A novel lightweight authentication scheme for RFID-based healthcare systems," *Sensors*, vol. 20, no. 17, pp. 265–269, 2020.

[23] M. Naeem, S. A. Chaudhry, K. Mahmood, M. Karuppiah, and S. Kumari, "A scalable and secure RFID mutual authentication protocol using ECC for Internet of Things," *International Journal of Communication Systems*, vol. 33, no. 13, Article ID e3906, 2020.

[24] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, "Blockchain based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11309–11322, 2019.

[25] R. Amin, S. Islam, P. Vijayakumar, M. Khurram Khan, and V. Chang, "A robust and efficient bilinear pairing based mutual authentication and session key verification over insecure communication," *Multimedia Tools and Applications*, vol. 77, no. 9, pp. 11041–11066, 2018.

[26] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K.-K. Raymond Choo, "HomeChain: a blockchain-based secure mutual authentication system for smart homes," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 15–27, 2020.

[27] A. Shahidinejad, M. Ghobaei-Arani, A. Souri, M. Shojafar, and S. Kumari, "Light-Edge: a lightweight Authentication protocol for IoT devices in an edge-cloud environment," *IEEE Consumer Electronics Magazine*, vol. 7, no. 9, pp. 1–6, 2021.

[28] J. Yang, J. Park, H. Lee, and K. Ren, "Mutual authentication protocol," in *Proceedings of the Workshop on RFID and lightweight crypto*, pp. 14-15, Graz, Austria, 2005.

[29] C. C. Tan, B. Sheng, and Q. Li, "Secure and serverless RFID authentication and search protocols," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1400–1407, 2008.

[30] S. Cai, Y. Li, T. Li, and R. H. Deng, "Attacks and improvements to an RIFD mutual authentication protocol and its extensions," in *Proceedings of the second ACM conference on Wireless network security*, pp. 51–58, Zurich, Switzerland, March 2009.