information

MDPI

Article

An Improved Two-Way Security Authentication Protocol for RFID System

Baolong Liu *, Bing Yang and Xiaohao Su

School of Computing Science & Engineering, Xi'an Technological University, Xi'an 710021, China; wuliyang3792@163.com (B.Y.); su-xiaohao@foxmail.com (X.S.)

* Correspondence: b.liu@xatu.edu.cn; Tel.: +86-29-8617-3270

Received: 11 March 2018; Accepted: 9 April 2018; Published: 11 April 2018

Abstract: This paper proposes an improved two-way security authentication protocol to improve the security level of Radio Frequency Identification (RFID) system. In the proposed protocol, tags calculate hash value, which is divided into two parts. The left half is used to verify the identity of the tags, and the right half is used to verify the identity of the reader, which will reduce the tag's computation and storage. By updating the tag's secret key value and random number, the protocol can prevent most attacks existing in RFID systems such as data privacy, replay attack, fake attack, position tracking and asynchronous attack. The correctness of the protocol is proved by using Burrows-Abadi-Needham (BAN) logic analysis. The evaluation results show that the scalability of the protocol proposed is achieved with acceptable response time limits. The simulation results indicate that the protocol has significant advantages on performance efficiency for many tags, which provides a reliable approach for RFID system application in practice.

Keywords: RFID system; security protocol; authentication; hash function; BAN logic

1. Introduction

RFID is a non-contact automatic identification technology, and it has been widely used in logistics, identity, electronic tickets, public transport, and other fields. Because RFID tags are limited by storage space, computing power and power supply, some mature authentication protocols cannot be applied directly. The design of efficient, low-cost RFID authentication protocol has become a hot topic of extensive discussion.

So far, a variety of security authentication protocols have been proposed to solve security and privacy issues within RFID sensor networks. There are three major types of RFID security protocols based on unidirectional hash functions: Hash-Lock protocol [1], randomized Hash-Lock protocol [2] and Hash chain protocol [3]. Hash-lock protocol was proposed by Sarma to avoid information disclosure and tracking [1]. In this protocol, the meta ID is used to identify a tag instead of the real tag ID. The protocol does not have a dynamic refresh mechanism for tags, and the meta ID remains unchanged during authentication. The initial condition of the protocol is that both the label and the backend server store the label ID and the identifier meta ID, and the backend server also stores the label key. Because tag's ID is transmitted in clear text over insecure channels, a hostile attacker could obtain the data and forge the label. Therefore, the protocol is vulnerable to counterfeit attacks, replay attacks and tracking attacks [4].

To solve the problem of location tracking in the Hash-Lock protocol, Weis et al. proposed a Randomized Hash-Lock protocol using a pseudo-random number generator. This protocol can avoid tracking the same response value for each tag because their response message is different from the last one [2]. However, the ID value and the key value of the tag have not been changed during the authentication process. This indicates that the attacker can forge the tag by stealing the ID value of the tag [5]. In addition, there is a problem of computation efficiency. When a tag is authenticated, the hash value of the tag ID must be calculated quickly and efficiently, which cannot be adapted to a large authentication system because there is not enough time to authenticate a large number of tags [6]. The system will crash due to a large number of calculations just as in Denial of Service (DoS) attacks.

Hash-chain protocol was proposed based on the challenge-response mechanism [3]. Tags and backend server share an initial secret value. When the reader sends a request to the label for authentication, the label sends a different response to solve the forward security issue. In this protocol, the reader authenticates the identity of the tag, and the tag does not authenticate the identity of the reader. If the response message of the tag is intercepted by the attacker, the attacker will send the value to the reader in the next round, and the forged tag can also be authenticated successfully. So, the protocol is vulnerable to fake and replay attacks.

Yang et al. proposed a lightweight authentication protocol based on hash function and XOR operation [7], and other researchers also proposed improved protocols. However, the static ID authentication protocol was susceptible to forged tag attacks in general [8–12]. For example, the protocol in [7] cannot resist the tracking attack, the forgery attack, the synchronous attack, and the DoS attack [13]. The protocol proposed in [14–16] cannot resist DoS attacks, faked tag attacks and faked reader attacks.

To solve the problem mentioned above, this paper proposes an improved two-way security authentication protocol for RFID systems. In the protocol, the tags calculate the hash value, which is divided into two parts. The left half is used to verify the identity of the tags, and the right half is used to verify the identity of the reader, which reduces the tag's computation and storage. By dynamically updating the tag's secret key for each authentication round, the protocol can prevent most of attacks existing in RFID systems such as data privacy, replay attack, fake attack, position tracking and asynchronous attack. The correctness of the protocol is proved by using BAN logic analysis.

The remainder of this paper is organized as follows: In Section 2, the necessary instructions and authentication process of the proposed protocol are described. The security of the protocol proposed is analyzed and proved using BAN logic in Section 3. A comparison with existing well-known protocols is also made. In Section 4, we performed the simulation of the protocol, and analyzed the protocol's scalability and efficiency. Finally, a conclusion is drawn in Section 5.

2. The Proposed Security Protocol

Through analysis of the mentioned literature review, a new security protocol is proposed in this section. The main idea is to divide the response value of the tag into two parts. One part is used to respond to the reader's query request, and the other is used to verify the legality of the reader. The following is the detailed description.

2.1. Initial Conditions and Related Instructions

The paper assumes that the label is a low-cost passive tag with a small amount of storage capacity and low computing power. Hash function of the RFID application is safe enough, and pseudo-random number is also safe enough. According to the EPC-C1-GEN2 standard, passive electronic tags come with on-chip pseudorandom generator (PRNG), and as the PRNG takes secret of 128 bits as seed value along with random numbers each time, it satisfies the randomness property for the RFID tag. The random number generated in the protocol is also safe enough. The hash function SHA3-224 is recommended in this paper. It is assumed that the communication channel between the tag and the reader is an insecure channel of wireless connection and the channel between the reader and the backend server is a secure channel of wire connection. The notations in the protocol are described in Table 1.

Table 1. The description of notations.

Notations	Description
R_r	Random number generated by reader
R_t	Random number generated by tag
ID	The identifier of the tag
K_i^{old}	The old secret value shared by the *i*th tag and the database
K_i^{new}	The new secret value shared by the *i*th tag and the database
RID	The identifier of the reader
M_L	The left part of the message M
M_R	The right part of the message M
$h(\cdot)$	Hash function
$\oplus$	XOR operation
$\|\|$	Connection operator

2.2. Authentication Process

The main security risk of the static ID-based security protocol is the leakage of the tag ID value. Because of the static security protocol, the tag's ID value always remains unchanged after the authentication is completed, and the attacker conducts multiple actions on the value of the target tag response reader. After the eavesdropping, it is easy to calculate the ID value of the tag; or an attacker can eavesdrop the random value sent to the tag. The pseudo reader sends a query to the tag, and the tag is traced by the response value of the tag. In both cases mentioned above, tags can be easily tracked and the situation is not secure. For the security risks that tags are easily tracked, the response value of the tag is divided into two parts. One part is used to respond to the reader's query request, and the other is used to verify the reader's legality. This not only ensures the security of the tag value but also reduces the amount of tag calculations. An improved RFID authentication process is shown in Figure 1.

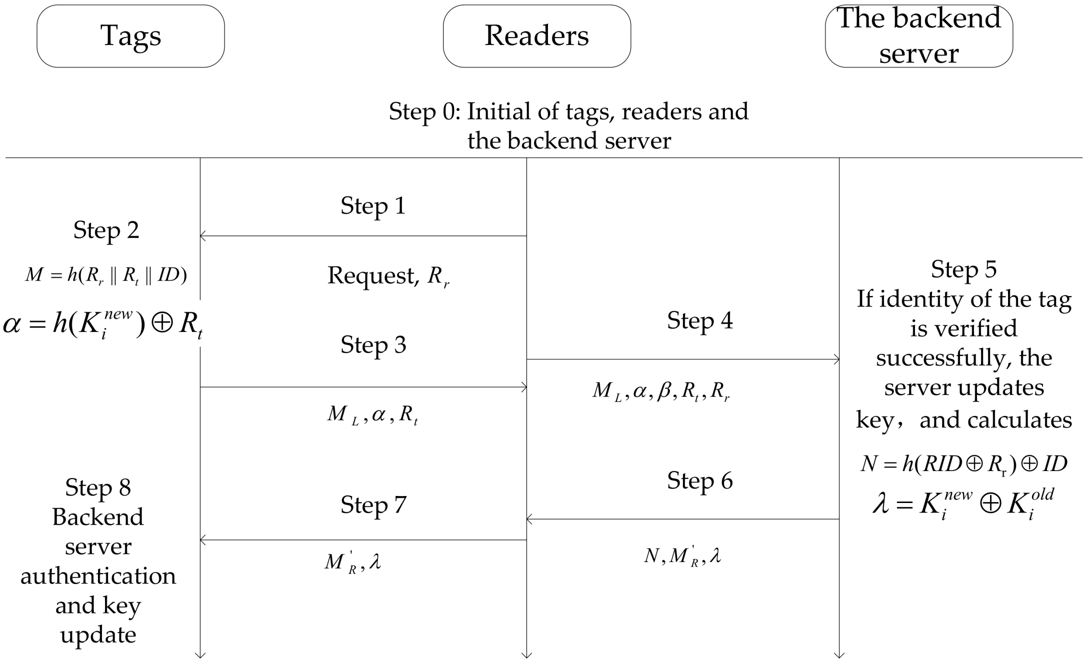
Tags
Readers
The backend server
Step 0: Initial of tags, readers and the backend server
Step 1
Request, R_r
Step 2
$M = h(R_r \| R_t \| ID)$
$\alpha = h(K_i^{new}) \oplus R_t$
Step 3
M_L, α, R_t
Step 4
$M_L, \alpha, \beta, R_t, R_r$
Step 5
If identity of the tag is verified successfully, the server updates key， and calculates
$N = h(RID \oplus R_r) \oplus ID$
$\lambda = K_i^{new} \oplus K_i^{old}$
Step 6
N, M'_R, λ
Step 7
M'_R, λ
Step 8
Backend server authentication and key update

Figure 1. The detailed authentication process.

The specific authentication steps are described as follows.

1. In the initial state, the tags need to store their own identifiers and the secret value ID, K_i^{new}, and readers only need to store their own identifiers RID, and backend database store all readers data RID and tags data ID, K_i^{new}, K_i^{old}.
2. The reader generates a random number R_{r}, and it sends query R_{r} to the tag as an authentication request.
3. After received the reader's request, the tag generates a random number R_{t} using its own identification ID. The tag calculates $M = h(R_r \mid\mid R_t \mid\mid ID)$, $\alpha = h(K_i{}^{new}) \oplus R_t$ (where, $\mid\mid$ is the concatenation operator, $\oplus$ exclusive OR operation), and the M value is divided into two parts, M_L and M_R.
4. The tag sends data M_L, R_t, α to the reader.
5. The reader calculates $\beta = h(RID) \oplus R_{\mathrm{r}}$ after received the message from the tag, and it sends the data M_L, α, β, R_{r}, and R_t to the backend server.
6. After received the message from the reader, the backend server verifies the legitimacy of the identity of the reader, and then the server verifies the legitimacy of the identity of the tag. If the reader and tag identity are legitimate, the server will update the secret value shared by tag and the server, otherwise the server finishes the authentication process. The detailed process is as follows.

   - Verify the legitimacy of the reader: the backend server calculates $\beta \oplus R_{\mathrm{r}}$ and uses the value $h(RID)$ of the reader itself to check whether the equation $h(RID) = \beta \oplus R_r$ is satisfied. The process continues to the next step if the condition is satisfied, otherwise the verification process is terminated.
   - Verify the legitimacy of the tag: The backend database calculates $\alpha \oplus R_{\mathrm{t}}$ to check whether the equation $h(K_i^{new}) = \alpha \oplus R_t$ is satisfied. The process continues to the next step if the condition is satisfied, otherwise the backend server makes an authentication using the previous retained K_i^{old}. The process continues to the next step if the condition is satisfied with retained K_i^{old}, otherwise the verification process is terminated.
   - If the above steps are finished, the backend server calculates $M\prime = h(R_r||R_t||ID)$ according to the tag's data pair stored by it. If there is $M_L' = M_L$, the tag is authenticated, otherwise authentication process is stopped.
   - The tag's secret value is updated in this step, let $K_{\mathrm{i}}^{new} = h(ID \oplus K_i^{old})$ and $K_i^{old} = K_i^{new}$.
   - The tag's secret value remains unchanged.
   - Finally, the backend server calculates the following two values $N = h(RID \oplus R_{\mathrm{r}}) \oplus ID$, and $\lambda = K_i^{new} \oplus K_i^{old}$.

7. The backend server sends the value N, λ, M_R' to the reader.
8. The reader calculates $N \oplus h(RID \oplus R_r)$ that is the tag ID value, and it sends λ, M_R' to tag.
9. When the tag receives the data, it makes a comparison between M_R and M_R'. If M_R equals to M_R', the tag calculates the value $K_i^{old} \oplus \lambda$ as the updated tag's key, otherwise the authentication process is terminated.

The key distribution scheme for above authentication process can be found in existing literature. A certificateless-effective key management (CL-EKM) supports efficient key updates for dynamic wireless sensor networks and ensures forward and backward key secrecy [17]. Similar to CL-EKM, a Hash Graph (HaG) scheme for key pre-distribution among a large set of sensor nodes in a sustainable and secure way was proposed [18]. This scheme is no limit on the total number of generations providing flexible network lifetime. A hierarchical key assignment scheme is provably secure with respect to key indistinguishability and relies on perfect secret sharing [19]. With a proper key distribution scheme, the protocol proposed has a wide application scope.

3. Protocol Analysis

In this section, the basic knowledge of BAN logic is introduced, and BAN logic is deployed to prove the security and feasibility of the new protocol proposed.

3.1. BAN Logical Analysis and Proof of Security

To analyze the security of the proposed protocol, formal analysis using BAN logic is described. BAN logic is basic model logic with primitives which describes the belief of the principle involved in a crypto system [20]. Using the inference rules of the BAN logic, authentication issues between the principles can be dealt with. The BAN logical reasoning steps are divided into three steps as shown in Figure 2, which are: (1) According to the specific description of the authentication protocol, it is expressed in logical language and initialized; (2) According to the established idealized model, the exchanged messages in the authentication protocol are converted into BAN logic language, and the unrelated parts are directly omitted; (3) Based on the initial assumptions in the first two steps and the idealized model established, the BAN logic inference rules can be used to prove whether the improved protocol achieves the desired goal and reaches a conclusion.

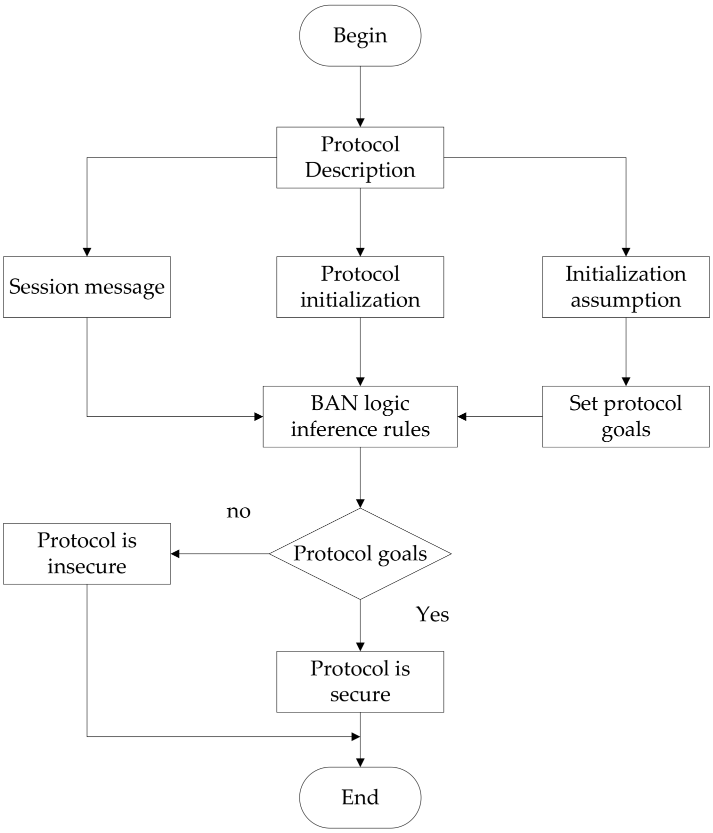

Figure 2. The detailed BAN logic inference steps.

BAN logic includes three sorts of objects: principle, encryption keys and logical formulas. The main construction of BAN logic is described as follows. $P|\equiv X$ denotes that P believes X; $P \lhd X$ denotes that P sees X; $P|\sim X$ denotes that P said X; $\#X$ denotes that the formula X is fresh, that is X has not been sent in a message at any time before the current execution of the protocol. $P \overset{K}{\leftrightarrow} Q$ denotes P and Q may use the shared K to communicate; $\{X\}_K$ denotes that the formula X is encrypted under the key K. The inference rules of BAN logic that are required in the analysis are described below.

1. message-meaning rules R1: $\frac{P\ |\equiv P \overset{K}{\leftrightarrow} Q P \lhd (X)_{\mathrm{k}}}{P\ |\equiv Q\ |\sim X}$;

2. Fresh rules R2: $\frac{P \mid\equiv\# \ (X)}{P \mid\equiv\# \ (X,Y)}$;
3. Logical community rules R3: $\frac{P \mid\equiv Q \mid\sim H(X_1,X_2,\cdots,X_\mathrm{n}),P \lhd X_1,P \lhd X_2,\cdots,P \lhd X_n}{P \mid\equiv Q \mid\sim (X_1,X_2,\cdots,X_n)}$;
4. Belief rules R4: $\frac{P \mid\equiv Q \mid\sim (X,Y)}{P \mid\equiv Q \mid\sim X}$;

In the following analysis, the tag is denoted by *T*. The reader is denoted by R, and the ID of the tag is represented by *IDT*.

3.1.1. Protocol Initialization Hypothesis

Before using the BAN logic to prove the proposed protocol, several necessary initial assumptions need to be given. The following is a list of specific assumptions.

$$\mathrm{P1}:\ R \mid \equiv \#(R_\mathrm{r})$$

$$\mathrm{P2}:\ R \mid \equiv\ R \overset{R_\mathrm{r}}{\leftrightarrow} T$$

$$\mathrm{P3}:\ T \mid \equiv \# \ (IDT)$$

$$\mathrm{P4}:\ T \mid \equiv\ T \overset{R_\mathrm{r}}{\leftrightarrow} R$$

The four initial assumptions are obvious. For assumption P1, because R_r (random number generated by reader) is always fresh, it is believed that the R_r is fresh. Because *IDT* is the identifier of the tag, it certainly believes that *IDT* is fresh. For P2 and P4, *R* and *T* believe that R_r is the communication key between them.

3.1.2. Establish an Idealized Protocol Model

Through above analysis, the idealized protocol can be expressed as the following process

$$\mathrm{M1}:\ R \to T : \mathrm{Query}, R_r$$

$$\mathrm{M2}:\ R \to T : h(IDT||\ R_r\ ||\ R_t)_L\, \alpha = K_i^{new} \oplus R_t R_\mathrm{t}$$

$$\mathrm{M3}:\ R \to T : h(IDT||\ R_r\ ||\ R_t)_R\, \lambda = K_\mathrm{i}^{new} \oplus K_i^{old}$$

where, M_1, α, and λ are expressly transmitted, and they have no effect on the logical attributes of the protocol analysis. The model above can be converted to the following BAN logical language.

$$\mathrm{M2}:\ R \lhd h(IDT, R_r, R_t)$$

$$\mathrm{M3}:\ T \lhd h(IDT\prime, R_r, R_t)$$

3.1.3. The Expectations of the Protocol

The expected objective of this protocol is to achieve:

$$R \mid \equiv T| \ \sim \#(IDT) \tag{1}$$

$$T \mid \equiv R| \ \sim \#(IDT') \tag{2}$$

3.1.4. Proof of the Authentication Process

(1) Proof evidence for objective: $R \mid \equiv T \mid\ \sim \#(IDT)$

With the initial hypothesis P1 and freshness rule: $\frac{P \mid\equiv\#(X)}{P \mid\equiv\#(X,Y)}$, it can be deduced that $\frac{R \mid\equiv\#(R_r)}{R \mid\equiv\#(R_r,R_t,IDT)}$. We can obtain result: $R \mid \equiv \#(R_\mathrm{r}, R_t, IDT)$.

With the protocol massage M2 and the initial hypothesis P2, using the message-meaning rule: $\frac{P\mid\equiv P\overset{K}{\leftrightarrow}QP\lhd(X)_{\mathrm{k}}}{P\mid\equiv Q\mid\sim X}$, we can obtain result: $R\mid\equiv T\mid\sim h(IDT,R_r,R_t)$.

The M2 split message can be seen that $R\lhd IDT, R\lhd R_{\mathrm{r}}, R\lhd R_t$, and using logical community rule: $\frac{P\mid\equiv Q\mid\sim H(X_1,X_2,\cdots,X_{\mathrm{n}}),P\lhd X_1,P\lhd X_2,\cdots,P\lhd X_n}{P\mid\equiv Q\mid\sim(X_1,X_2,\cdots,X_n)}$, we can learn that $R\mid\equiv\ T\mid\sim(IDT,R_{\mathrm{r}},R_t)$.

With belief rule: $\frac{P\mid\equiv Q\mid\sim(X,Y)}{P\mid\equiv Q\mid\sim X}$, the following deduction is reached $\frac{R\mid\equiv T\mid\sim(IDT,R_{\mathrm{r}},R_t)}{R\mid\equiv T\mid\sim IDT}$. The result achieved is: $R\mid\equiv\ T\mid\sim\ IDT$.

From above process we can learn that $R\mid\equiv\ T\mid\sim\#\,(IDT)$, and the objective (1) is proved.

(2) Proof evidence for objective: $T\mid\equiv\ R\mid\sim\#\,(IDT\prime)$

With the initial hypothesis P3, the message M3 and the initial hypothesis P4, using the message-meaning rule: $\frac{P\mid\equiv P\overset{K}{\leftrightarrow}QP\lhd(X)_{\mathrm{k}}}{P\mid\equiv Q\mid\sim X}$, we can learn that: $\frac{T\mid\equiv T\overset{R_r}{\leftrightarrow}RT\lhd h(IDT\prime,R_r,R_t)}{T\mid\equiv R\mid\sim h(IDT\prime,R_r,R_t)}$, and the following result can be obtained: $T\mid\equiv\ R\mid\sim\ h(IDT\prime,R_r,R_t)$.

The M3 split message can be seen that $T\ \lhd\ IDT\prime, T\ \lhd\ R_{\mathrm{r}}, T\ \lhd\ R_t$, using logical community rule: $\frac{P\mid\equiv Q\mid\sim H(X_1,X_2,\cdots,X_{\mathrm{n}}),P\lhd X_1,P\lhd X_2,\cdots,P\lhd X_n}{P\mid\equiv Q\mid\sim(X_1,X_2,\cdots,X_n)}$, the following result can be achieved as $\frac{T\mid\equiv R\mid\sim h(IDT\prime,R_r,R_t),T\lhd IDT\prime,T\lhd R_r,T\lhd R_t}{T\mid\equiv R\mid\sim(IDT\prime,R_r,R_t)}$, which means that $T\mid\equiv\ R\mid\sim\ (IDT\prime,R_r,R_t)$.

With belief rule: $\frac{P\mid\equiv Q\mid\sim(X,Y)}{P\mid\equiv Q\mid\sim X}$, we obtain that $\frac{T\mid\equiv R\mid\sim(IDT\prime,R_{\mathrm{r}},R_t)}{T\mid\equiv R\mid\sim IDT\prime}$, and the final result is that $T\mid\equiv\ R\mid\sim\ IDT\prime$.

From above process we can obtain that $T\mid\equiv\ R\mid\sim\ IDT\prime$, and the objective (2) is proved.

The security protocol proposed in this paper can be deduced using the formal analysis of the BAN logic, so the protocol can effectively achieve the security objectives of the two-way legal authentication of tags and readers in the RFID sensor network.

3.2. Security Comparisons

(1) Data privacy. Each message in the solution is encrypted using hash function and XOR operation. Because of the unidirectional nature of hash function [21], it is difficult for attackers to obtain confidential information such as *ID*, *RID*. In the authentication process, random number is not the same, so the solution can guarantee the security of the label ID information.

(2) Replay attack [22]. Assuming that an attacker has recorded the information sent by the tag in advance, when the reader communicates with the tag again, the attacker is disguised as a legal label to communicate with a reader through the recorded tag information. The value of $M_L, R_{\mathrm{t}}, \alpha$ is associated with the random number of the reader and the tag. Because the random number of each authentication is different, each value of tag response is also not the same, even if the illegal attacker intercepted the previous information, it cannot simulate the value next time. As a result, the tag or reader will not accept the copied information.

(3) Fake attack [23]. It can be seen from above that an attacker cannot obtain private information of a label and a reader, so it cannot disguise as a legitimate label and reader.

(4) Position tracking [24]. The random number of each communication is different, and the transmitted information of the label is different each time, which can effectively prevent the fixed output caused by the location tracking problem.

(5) Asynchronous attack [25]. Because of the static ID security protocol, the label ID information is the same each time, it is impossible to appear asynchronous attack.

(6) Brute-force attack [14]. The hash function SHA3-224 is recommended. When the adversary has acquired R_r, α, $R_t\oplus\beta$, $h(\beta\oplus RID)$, $R_t\oplus K_i^{new}$ via eavesdropping or meaningless requests, a brute-force attack must be performed in order to obtain ID, K_i^{old}, K_i^{new}, via analysis of the messages. If we assume that initially an adversary knows R_r, the complexity of determining ID and K_i^{old} from α is 2^{196}. The number of possible pairs of R_t and β is 2^{96}, and based on the respective β values, the number of estimations for the 64 bits ID and the 128 bits K is 2^{192}.

Therefore, an adversary has requested 2^{388} estimations of ID and K. Based on above analysis, the scheme proposed is sufficiently secure against the brute-force attack.

Table 2 shows the security comparison of protocol proposed with existing solutions. It can be seen clearly that the proposed protocol has the best security performance compared to existing protocols.

Table 2. Security comparisons with other protocols.

Scheme	[1]	[2]	[3]	[26]	[27]	[28]	Proposed Scheme
Data privacy	√	√	√	√	×	√	√
Replay attack	×	×	×	√	√	√	√
Fake attack	×	×	×	×	√	√	√
Position tracking	×	×	√	×	×	√	√
Asynchronous attack	√	√	√	×	×	×	√

√: Satisfies the property, ×: Does not satisfy the property.

4. Evaluation

This section introduces the simulation experiment environment, and the stability and execution efficiency of the proposed protocol are also analyzed.

4.1. Experimental Environment

The simulation of this experiment is implemented by computer programming and developed with Eclipse + JDK. The object-oriented Java is selected as the programming language. The experimental related hardware and software environment is set up as follows.

1. Hardware section

   Processor: Intel Core i5-3230M CPU @ 2.60GHZ RAM: 4GB
   Tag: The passive MIFARE Plus IC card
2. Software section

   OS: Windows 7 Professional
   Simulation tools: Eclipse Java EE IDE for Web Developers (Version: 4.6.3), Java SE Development Kit 8 (Version: 1.8), Network simulator-2, MySQL (Version: 10.1.2531.0, for Win32)

In the experiment, three Java classes of Database.class, Reader.class and Tag.class are used to simulate three main parts of RFID identity protocol, which are backend database, reader, and tag.

According to the definition format of data in the database in the new protocol, Database.class is defined to set the corresponding variables, and the rules are defined for distributing data to the reader in the class. In Reader.class, the rules are defined for distributing data to the backend database and the tags. The Tag.class is defined to set the variables corresponding to the information shared by the backend database according to the format of the tag data definition in the protocol, and we define the rules for responding to the reader in the class.

The simulation sets the hash function that needs to be invoked during protocol execution in SHA3.class. To ensure that the input string can be hash compressed to a fixed-length output in the Reader.class, a pseudo-random number generation function is used to define the random number generated by the reader in Tag.class.

4.2. Scalability

An RFID authentication protocol is said to be scalable if the backend server takes constant time to search a match in its database during the identification of an RFID tag. To analyze the scalability of protocol proposed, a simulation is performed using network simulator-2 (NS-2). The purpose here is not to compare the proposed protocol to existing ones but rather to ensure the scalability is achieved with acceptable response time limits. In this simulation, the performance of proposed protocol is studied in terms of end-end delay. The end-end delay includes two main parts, the network delay and the processing time in the reader, tag, and backend server. The number of tags in the simulation is varied from 10 to 100 thousand and the number of readers is set at 50 and 100. The results of the simulation are presented in Figure 3 and each data point corresponds to the average of 10 simulation runs. As shown in Figure 3, as the number of tags increases the time delay increases. This is along expected lines as the backend server has a complexity of $O(n)$. However, it can be observed that the end-end delay is within acceptable bounds (≈0.5 s) for all cases. In terms of the impact of number of readers, the time delay increases are quite small. The results prove that the protocol proposed is scalable.

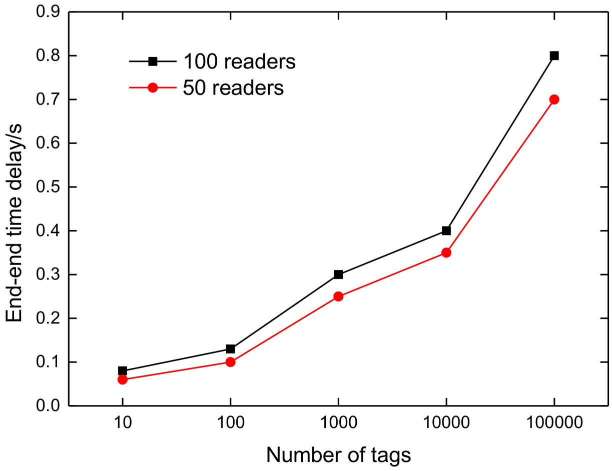

Figure 3. Scalability evaluation.

4.3. Performance Efficiency

The proposed protocol has obvious advantages compared to other protocols in terms of computational complexity. It requires only simple hash operations and XOR operations to avoid other complex and time-consuming operations. The specific comparison is shown in Table 3.

Table 3. Performance properties.

Scheme	Reader	Server	Tag	M	C
[1]	N/A	N/A	1H	4	√
[2]	2mH	N/A	1H	3	√
[3]	N/A	2mH	2H	2	√
[26]	1R	(m + 1)H	3H, 1R	3	√
[27]	1R	5H, 1R	3H	3	√
[28]	1R	(m + 1)H	2H, 1R	3	√
This paper	1R	3H	2H, 1R	3	√

m: No. of tags; H: Hash operation; R: Random number generation; M: No. of message exchanged between tag and reader; C: EPC Compliance.

In Table 3, we compare the performance of the authentication protocols that have been proposed. We observe that the random number of operations on the reader side of the new protocol is only once, and the encryption operation on the tag side is twice. The protocol in reference [2], the cryptographic operation at the reader is twice to the number of tags. In other schemes listed in Table 3, the number of encryptions on the tag side is between one and three times, so the number of encryptions in the new protocol is within an acceptable range. From Table 3, it can be seen that the tag of the new protocol requires two hash operations during the authentication process. They occur when responding to the reader authentication request. $h(R_r||R_t||ID)$ is generated the M value and divide the M value into two parts M_L, M_R. M_L will be sent to the backend server for verification. If the verification is successful, the backend server will send M_R to the tag. In this way, the tag does not need to perform any operation when authenticating the server, which reduces tag-side computations and the number of operations on the server side.

While comparing, all the agreements are in line with EPC standards and, of course, the agreement also meets the standards. Thus, we see that our scheme provides the required security properties while at the same time conforming to EPC standard.

The major factors affecting the performance efficiency are the number of hash computing and the number of comparisons within system [26–28]. The paper takes the number of hash computing and the number of comparison as criteria to make an evaluation as shown in Figures 4 and 5. The compared protocols are the Hash Lock-based scheme, the Hash Chain-based scheme and protocol proposed in this paper. In the process of simulation, we assume the number of tags is x, and there are x entries in backend server corresponding to tags. The simulation selects 200 tags randomly, and makes 20 hostiles accessing randomly, which causes asynchronous data between tags and the backend server. Based on the above settings, the simulation makes 100,000 authentication processing, and the tag's number varies from 200 to 10,000. In the simulation, given a hash length of 224 bits, a 128-bit random number R_t, secret key K_i length of 128 bits and tag ID length of 64 bits, the storage requirements on the tag would be 224 + 128 + 128 + 64 = 544 bits = 68 bytes. For authentication protocol in a RFID system, the higher security, the greater the amount of calculation and power consumption. Other protocols proposed are mainly hashed with SHA3-112, whose hash length is 112 bits. The amount of computation and power consumption of SHA3-112 is much less than that of SHA3-224, but it is not safe enough. In a commercial RFID solution, different hash algorithms can be selected in the proposed protocol according to the actual application requirement.

The simulation results show that when the number of tags is increased, the number of comparison and the number of hash computing in protocol proposed is stable compared to Hash Lock protocol and Hash Chain protocol with the same number of authentication. Because the number of comparison only relates to the number of authentication in our protocol, and the number of hash computing relates to the number of authentication and hostile accessing, with two different parts division, the total number of comparison and number of hash computing are decreased. For many tags, the protocol proposed in this paper has significant advantages.

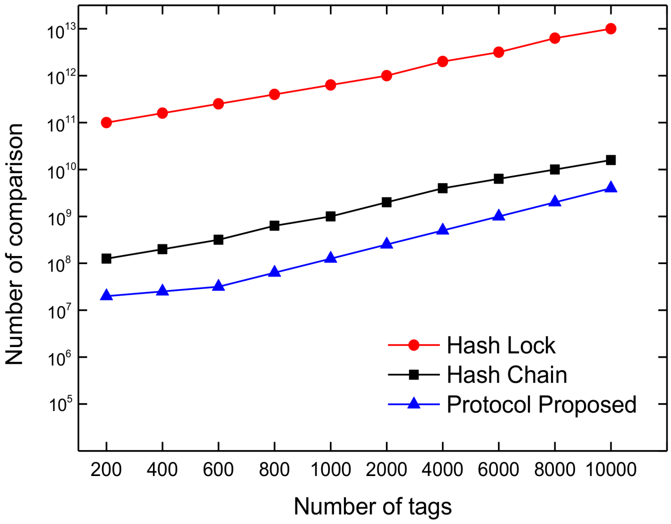

Figure 4. The number of comparison in simulation.

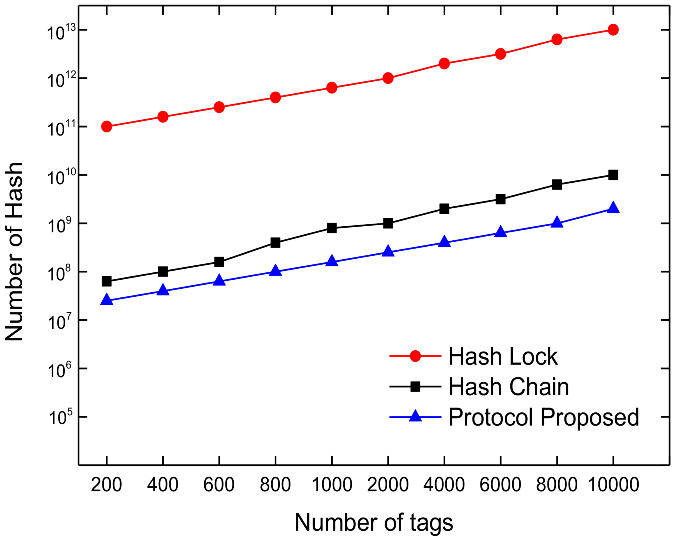

Figure 5. The number of hash computing comparison.

In the proposed protocol, when the backend server authenticates tags, the number of hash operations is a dynamically changing value. Specifically, the backend server obtains the shared secret value ${K_i}^{new}$ between the electronic tag by using the exclusive-OR operation of the random number R_t and $\alpha = h({K_i}^{new}) \oplus R_t$, and then compares the value ${K_i}^{new}$ with the tag value stored by the server. If they are not equal, the server directly terminates the identity authentication of this tag and performs the next electronic tag authentication. In this way, the hash operation of authenticating the tag is only once, and is less than the maximum number of hash operations of the backend server in the protocol. Supposing the sender is determined to be an attacker after a hash function operation, and the subsequent authentication steps are no longer performed, which reduces the number of comparisons. However, the Hash chain and the Hash lock protocol must complete all the hash operations to determine whether a tag is valid or not. When the number of tags is large, the proposed new protocol has obvious advantages in the number of hash operations and the number of comparisons over the hash chain and hash lock protocols.

5. Conclusions

This paper proposes an improved scheme based on hash function to overcome the shortcomings of existing protocols. Through the establishment of the idealized model of the protocol, the BAN logic is used to analyze the protocol, which proves its security in theory. The simulation results indicate that the protocol proposed is scalable and has a better performance. With a properly selected key distribution scheme, the protocol has a wide application scope.

Acknowledgments: This work is partially supported by Science & Technology Program of Shaanxi Province with project "2017GY-196", and the Opening Fund of State and Local Engineering Laboratory of Advanced Network and Monitoring Control with project "GSYSJ2016001".

Author Contributions: Baolong Liu and Bing Yang conceived and designed the protocol; Baolong Liu performed the deduction; Bing Yang simulated the system; Baolong Liu, Bing Yang and Xiaohao Su wrote the paper. All authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sarma, S.A.; Weis, S.E.; Engels, D.W. RFID systems and security and privacy implications. In Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems, Redwood Shores, CA, USA, 13–15 August 2002; pp. 454–469. [CrossRef]
2. Weis, S.A.; Sarma, S.E.; Rivest, R.L. Security and privacy aspects of low-cost radio frequency identification systems. In Proceedings of the First International Conference on Security in Pervasive Computing, Boppard, Germany, 12–14 March 2003; Lecture Notes in Computer Science. Springer: Berlin/Heidelberg, Germany, 2003; Volume 2802, pp. 201–212.
3. Ohkubo, M.; Suzuki, K.; Kinoshta, S. Hash-chain based forward-secure privacy protection scheme for low-cost RFID. In Proceedings of the 2004 Symposium on Cryptography and Information Security, Sendai, Japan, 27–30 January 2004; pp. 719–724.
4. Prosanta, G.; Tzonelih, H. A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. *Comput. Secur.* **2015**, *55*, 271–280.
5. Tan, X.; Dong, M.; Wu, C.; Ota, K.; Wang, J.; Engels, D. An Energy-Efficient ECC Processor of UHF RFID Tag for Banknote Anti-Counterfeiting. *IEEE Access* **2017**, *5*, 3044–3054. [CrossRef]
6. Sundaresan, S.; Doss, R.; Piramuthu, S.; Zhou, W. A secure search protocol for low cost passive RFID tags. *Comput. Netw.* **2017**, *122*, 70–82. [CrossRef]
7. Yang, J.; Park, J.; Lee, H.; Ren, K.; Kim, K. Mutual authentication protocol for low-cost RFID. In Proceedings of the Workshop on RFID and Lightweight Cryptography, Graz, Austria, 14–15 July 2005; pp. 17–24.
8. Cai, Q.; Zhan, Y.; Wang, Y. A minima list mutual authentication protocol for RFID system and BAN logic analysis. In Proceedings of the ISECS International Colloquium on Computing, Communication, Control, and Management, Guangzhou, China, 3–4 August 2008; pp. 449–453.
9. Luo, Z.; Chan, T.; Li, J.S. A lightweight mutual authentication protocol for RFID networks. In Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'05), Beijing, China, 12–18 October 2005; pp. 620–625.
10. Tan, C.C.; Sheng, B.; Li, Q. Secure and server-less RFID authentication and search protocols. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 1400–1407. [CrossRef]
11. Dass, P.; Om, H. A Secure Authentication Scheme for RFID Systems. *Procedia Comput. Sci.* **2016**, *78*, 100–106. [CrossRef]
12. Gope, P.; Amin, R.; Islam, S.H.; Kumar, N.; Bhalla, V.K. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Gener. Comput. Syst.* **2017**, *83*, 629–637. [CrossRef]
13. Cai, S.; Li, Y.; Li, T.; Deng, R. Attacks and improvements to an RFID mutual authentication protocol. In Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec'09), Zurich, Switzerland, 16–18 March 2009; pp. 51–58.
14. Cho, J.-S.; Jeong, Y.-S.; Park, S. Consideration on the Brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol. *Comput. Math. Appl.* **2015**, *69*, 58–65. [CrossRef]
15. Piramuthu, S. RFID mutual authentication protocols. *Decis. Support Syst.* **2011**, *50*, 387–393. [CrossRef]
16. Safkhani, M.; Peris-Lopez, P.; Hernandez-Castro, J.C.; Bagheri, N. Cryptanalysis of the Cho et al. protocol: A hash-based RFID tag mutual authentication protocol. *J. Comput. Appl. Math.* **2014**, *259*, 571–577. [CrossRef]
17. Seo, S.; Won, J.; Sultana, S.; Bertino, E. Effective Key Management in Dynamic Wireless Sensor Networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 371–383.
18. Levi, A.; Sarimurat, S. Utilizing hash graphs for key distribution for mobile and replaceable interconnected sensors in the IoT context. *Ad Hoc Netw.* **2017**, *57*, 3–18. [CrossRef]
19. Castiglione, A.; Santis, A.; Masucci, B. Hierarchical and Shared Key Assignment. In Proceedings of the 2014 International Conference on Network-Based Information Systems, Salerno, Italy, 10–12 September 2014; pp. 263–270.
20. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]

21. Li, Z.; Zhong, X.; Chen, X. A Lightweight Hash-Based Mutual Authentication Protocol for RFID. In Proceedings of the International Workshop on Management of Information, Processes and Cooperation, Hangzhou, China, 23 September 2016; pp. 87–98.
22. Liu, Y.; Feng, S. Scalable Lightweight Authentication Protocol with Privacy Preservation. In Proceedings of the Tenth International Conference on Computational Intelligence and Security, Kunming, China, 15–16 November 2014; pp. 474–478.
23. Jannati, H.; Bahrak, B. Security analysis of an RFID tag search protocol. *Inf. Process. Lett.* **2016**, *116*, 618–622. [CrossRef]
24. Yang, L.; Wu, Q.; Bai, Y.; Zheng, H.; Lin, S. An improved hash-based RFID two-way security authentication protocol and application in remote education. *J Intell. Fuzzy Syst.* **2016**, *31*, 2713–2720. [CrossRef]
25. Zhang, C.; Zhang, W.; Mu, H. A Mutual Authentication Security RFID Protocol Based on Time Stamp. In Proceedings of the 2015 First International Conference on Computational Intelligence Theory, Systems and Applications (CCITSA), Yilan, Taiwan, 10–12 December 2015; pp. 166–170.
26. Yang, X. Research and Design on Authentication Protocol for RFID. Master Thesis, Xidian University, Shaanxi, China, 2014.
27. Xiong, W.; Xue, K.; Hong, P. RFID cryptographic protocol based on two-dimensional region Hash chain. *J. Univ. Sci. Technol. China* **2011**, *41*, 594–598.
28. Lei, H.; Song, H.; Tao, Z. An enhanced 2-pass optimistic anonymous RFID authentication protocol with forward security. In Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing, Beijing, China, 24–26 September 2009; pp. 3692–3695.