Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, 2015, *9,* 483-490

Open Access

Hash based Server/Serverless Adaptive and Mutual Authentication Protocol of RFID

Wang Guowei, Jia Zongpu* and Peng Weiping

School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, Henan 454000, China

Abstract: To solve the problems about securities, absence of calculation pertinence, incapability of making the most of the reader's computation and storage capacity that emerged in Radio Frequency Identification (RFID) authentication protocols, the paper proposes a Hash function based server/serverless adaptive and mutual authentication protocol of RFID based on the analysis of RFID authentication protocol that using a backend server and without using a backend server. The protocol can automatically switches between the RFID authentication protocol with or without a backend server according to the application range of RFID tags. The BAN logic proof, security and efficiency performances analysis and comparison with other similar RIFD protocols presented by the paper show that the protocol can effectively meets the security requirements of RFID authentication protocols.

Keywords: Authentication protocol, Hash, RFID, Server/Serverless Adaptive.

1. INTRODUCTION

RFID is a technology that enables the non-contact, automatic and unique identification of objects using radio waves [1]. With the rapid development of Internet of things (IoT) technology, RFID plays a more and more important role in industries such as production, retail, and logistics etc., which makes the security problem of RFID became one of the most challenges in aspects of identity authentication and privacy preservation fields [2]. The attacks against the RFID system mainly include forging of a tag or a reader, eavesdropping, tracing, physical attack, replay attack, and the denial of service attacks etc.. In response to these attacks, RFID security technology can be divided into physical methods and cryptography-based mechanisms [3]. As an encryption algorithm in cryptography and a special one-way function, Hash function require only a few gate chips for implementation but can provides confidentiality and message authentication. Therefore, it is applicable to the RFID authentication protocol of IoT.

Generally, RFID system consists of backend server, reader, and tag [4]. These entries have asymmetric computing and storage properties because the backend server and reader are provided with high computing and storing capacity, while tag, especially passive tag, only bears limited computing and storing capacity. In addition, the data communication between reader and backend server can be ensured since it is in the security monitoring range, while the wireless data communication between reader and tag is vulnerable to attacks. Therefore, in order to improve the execution efficiency and preserve data privacy, most Hash function based RFID authentication protocols use a common method that backend server decrypts the encrypted tag information forwarded by the reader and compares one by one with the tag information stored in the backend server to confirm the legitimacy of the tag. However, tags in RFID system often need to be authenticated by multiple readers in practical applications. For example, in the RFID system of food supply chain, reader of local region is more possibly to identify the RFID tags carried by local food, while less possibly to identify the tags carried by the food from other regions. However, most of existed RFID authentication protocols lack pertinence since almost all the tag information are computed and compared. The enlarged calculation range increases the overhead and reduces the execution efficiency of these protocols. In addition, in these protocols, reader fails to give the full play to its computing and storing performance because it is merely acted as a transfer station.

In this paper, we investigated the FRID mutual authentication protocols with and without a backend server, our main contributions can be summarized as:

1) A server/serverless adaptive RFID mutual authentication protocol that can automatically switches between the RFID authentication protocol with and without a backend server.

2) A novel approach that can gives full play to the calculation and storage ability of the reader and realizes the pertinent authentication and calculation on tag.

The paper is divided into 8 sections. The next section discusses the background and related work involved in RFID authentication protocols that using a backend server and without using a backend server. Section 3 details the whole progress of the proposed protocol. Section 4 illustrates the logic analysis and proof of the protocol. Analysis on security

1874-110X/15

and efficiency performances of the protocol are presented in section 5.The concluding section presents a summary of the paper and future work. Section 6 is conflict of interest and section 7 is acknowledgements. Finally, section 8 lists the references.

2. RELATED WORKS

The Hash-Lock protocol, random Hash-lock protocol, and Hash-chain protocol respectively presented in literatures [5-7] are the most classic RFID authentication protocols with a backend server. Hash-Lock protocol replaces the real ID of tags by metaID. Since metaID keeps constant in the protocol process and the real ID of the tag is transmitted in plaintext, this protocol is vulnerable to tracing and replay attack. Random Hash-lock protocol is an improvement of Hash-Lock protocol that uses random numbers for challenge and response, this protocol can prevents the position tracing on tag but fail to avoid replay attacks since the tag ID is still transmitted in plaintext. In additional, all the tag IDs need to be sent to reader in the authentication process and thus increases the load and communication overhead on reader, which limits the practicality of the protocol. Hash-chain protocol can provides forward security via dynamic refreshing of tag. However, since Hash chain protocol is a one-way authentication protocol, it is vulnerable to reader camouflage and replay attack. On the basis of the research on the three kinds of protocol above, researchers around the world have proposed a number of improved protocols. Literature [8] presented a Hash function-based mutual RFID authentication protocol that realized by sending the encrypted random number generated by the tag to the backend server. Unfortunately, in the fifth step of this protocol, the adversary could replaces the $R_t \oplus s_{j+1}$ by using a random number to initiate synchronization attacks. In addition, this protocol has forward security problem because the encrypted information of a tag in the last authentication process can be distinguished from the former in given conditions.

Using trusted third-party and access list, literature [3], literature [9], and literature [10] presented several serverless RFID authentication protocols. These protocols establish a certification center and initialize the reader with a unique identity and access list. The access list comprises all the tag information allowed to be accessed, which includes a secret key and an identification flag. In the process of the authentication, the tag information in the access list requires Hash computation and comparison to confirm the legitimacy of a tag. In the protocol proposed in literature [3], the secret key that respectively stored in the reader and tag need to be updated. However, at the third step of this protocol, in case of the communication interrupting or blocking induced by reader's power off or human attack, de-synchronization will appears because the secret key of reader was updated while the tag has no information to update the secret key, and thus the reader will not able to identify or authenticate the tag in the future sessions, so this protocol is vulnerable to de-synchronization attack. Meanwhile, at the second step, reader identifies the tag according to the former p bits of the Hash code of the tag, which reduces the anti collision capability of Hash function. In addition, the protocol has key exposure problem because the adversary can calculates the updated key though the captured transmission data. The reader of the protocol presented by literature [9] needs to transverse and compute all the tag information stored in the reader. If the tag amount is too large, the computation efficiency will turns low as the increasing of the searching difficulty and Hash computation. At the forth step of the protocol proposed in literature [10], the anonymity of the tag is not guaranteed. Aiming at the low efficiency of reader traversing and computing, literature [11] presented an optimization algorithm. In this protocol, according to the response information of the tag, reader eliminates the entries mismatching with the tag through an iteration method until matched entries of the tag is retrieved. By each authentication, about 1/4 of the entries can be excluded. This protocol improves the traversing efficiency of the reader to a certain extent, but the traversal algorithm covers all RFID tags and thus is not pertinent.

3. THE AUTHENTICATION PROTOCOL PROPOSED BY THIS PAPER

3.1. Assumptions

The RFID authentication protocol proposed in this paper is based on the following assumptions that are consistent with the communication conditions of RFID systems:

1) Tags are the passive tags with limited computing ability while the backend server and reader have high computation capacity.

2) The communication channel between the reader and the backend server is secure, the data transmitted between the reader and the backend server is credible.

3) The communication channel between the reader and tag is insecure.

4) The one-way Hash function and pseudo random number used in the protocol are secure.

3.2. Initialization

During initialization, the tag contains a one-way Hash function, a pseudo random number generator and a secret key; the reader contains a same one-way Hash function, a same pseudo random number generator, and a access list for storing the secret tag keys in fixed length; the backend server stores all the tag keys of the RFID system.

Additionally, the RFID system can initializes some keys of tag that need to be authenticated multiple times into the access lists of certain readers according to business scope, which integrates these readers and tags into a serverless RFID system. And also, the RFID system can initializes an empty access list in the reader, the secret key of the tag will be automatically saved in the access list during the process of the authentication.

3.3. Notations Used in the Protocol

Table **1** shows the notations and related descriptions used in the protocol.

Table 1. The authentication process of the protocol.

Notation	Description
$H()$	One-way Hash function
L	Access list in reader
S_t	Random number of tag
S_r	Random number of reader
K	Secret key of tag
K_t	Secret key stored in tag
K_r	Secret key stored in reader or backend server
$\|\|$	Connection computation
Query	Authentication request

3.4. The Authentication Process of the Protocol

Step 1: Reader generates a random number S_r and sends the number to the tag together with the authentication request *Query* .

Step 2: After receiving the authentication request, tag produces a random number S_t and calculates $H(K_t \| S_r)$, then sends $H(K_t \| S_r)$ and S_t as responses to the reader.

Step 3: Reader traverses the access list and calculates $H(K_r \| S_r)$, then compares with $H(K_t \| S_r)$. If there is a K_r making $H(K_r \| S_r) = H(K_t \| S_r)$, the tag is legal. Then $H(K_r \| S_t)$ is calculated and sent to the tag and Step 6 begins. If $H(K_r \| S_r) = H(K_t \| S_r)$ is unavailable, reader forwards the $H(K_t \| S_r)$, S_r, and S_t to the backend server through secure channel.

Step 4: Backend server traverses the database and calculates the $H(K_r \| S_r)$. The result obtained is compared with $H(K_t \| S_r)$, if there is a K_r making $H(K_r \| S_r) = H(K_t \| S_r)$, the tag is legal and is identified for the first time. After $H(K_r \| S_t)$ is calculated by the backend server, the K_r and $H(K_r \| S_t)$ are transmitted to the reader through secure channel.

Step 5: Reader stores the received K_r to access list and sends $H(K_r \| S_t)$ to the tag.

Step 6: Tag calculates the $H(K_t \| S_t)$, then compares it with the received $H(K_r \| S_t)$. In the case of $H(K_t \| S_t) = H(K_r \| S_t)$, the authentication is successful. Otherwise, the reader is illegal and the authentication fails.

Fig. (**1**) illustrates the whole authentication process of the protocol.

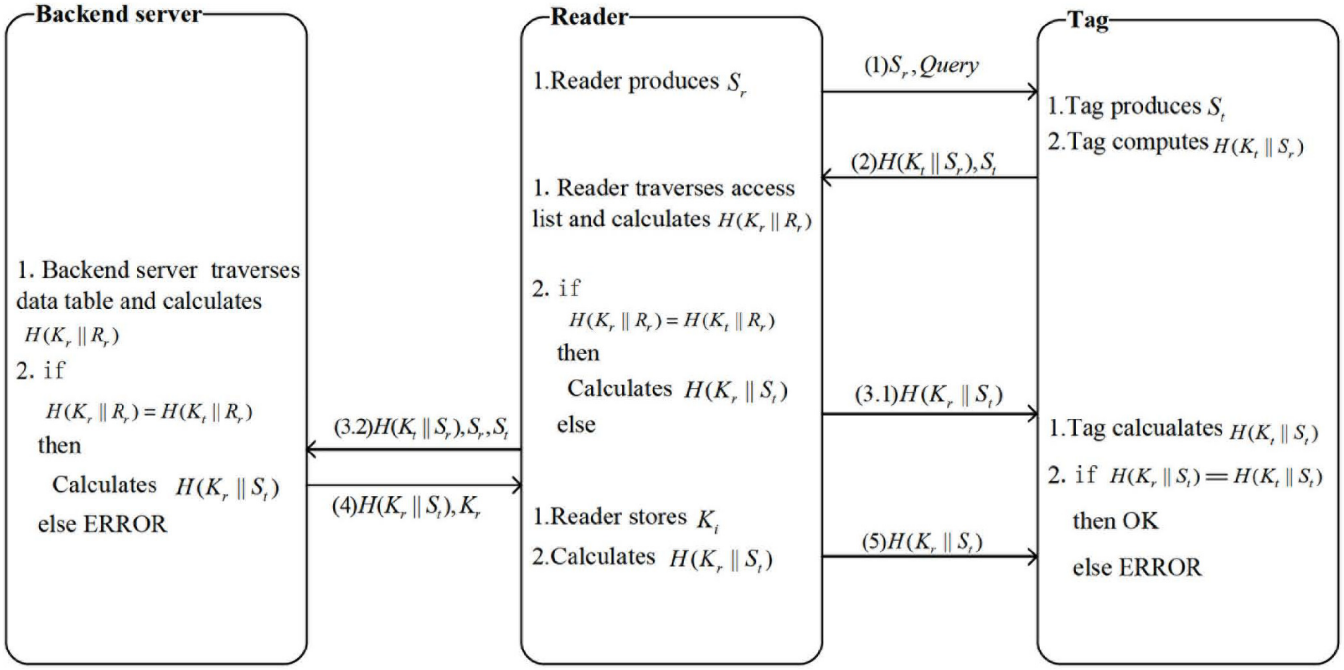

Fig. (1). The authentication process of the protocol.

4. THE LOGIC ANALYSIS AND PROOF OF THE PROTOCOL

4.1. About BAN Logic

The provable security of the authentication protocol is to prove that the protocol can achieve specific security goals using certain model in premise of defining appropriate security objectives and establishing appropriate models [12]. The most widely used formal analysis methods on authentication protocol mainly include the logic analysis methods based on knowledge and belief. The BAN logic is a logic rule for deducing new belief basing on basic and available beliefs [13]. In BAN logic, the protocol is firstly converted into the formulas for the protocol idealization, then conducted reasonable initial assumptions. On the basis of the protocol idealizations and reasonable assumptions, the logical rules are used to deduce whether or not the protocol can achieve desired goal [14]. In this paper, the BAN logic is used to formally prove the security of the authentication protocol.

Table **2** presents the basic expressions and their descriptions.

Table 2. Expression of BAN logic.

Expression	Description
$P \mid\equiv X$	P believes X
$P \lhd X$	P has received X
$P \mid\sim X$	P has sent X
$P \mid\Rightarrow X$	P controls X
(X,Y)	X connects Y
$\#(X)$	X is fresh
$\{X\}_K$	Ciphertext of X encrypted by key K
$< X >_Y$	X integrates secret Y
$P \xleftrightarrow{K} Q$	Shared K between P and Q

BAN logic includes 19 basic logical rules from 7 classes, the 5 used in this paper as following:

Message-meaning rule:

$$\frac{P \mid\equiv Q \xleftrightarrow{K} P, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X} \quad \text{(R1)}$$

Random number verification rule:

$$\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X} \quad \text{(R4)}$$

Jurisdiction rule:

$$\frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X} \quad \text{(R5)}$$

Trust polymerization and trust projection rule:

$$\frac{P \mid\equiv Q \mid\equiv (X,Y)}{P \mid\equiv Q \mid\equiv X} \quad \text{(R8)}$$

Fresh transmission rule:

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)} \quad \text{(R15)}$$

4.2. The Reasonable Assumptions for the Protocol

The reasonable assumptions are constructed for the analysis of the protocol as follows:

$$R \mid\equiv \#(S_r) \quad \text{(P1)}$$

$$T \mid\equiv \#(S_t) \quad \text{(P2)}$$

$$T \mid\equiv \#(S_r) \quad \text{(P3)}$$

$$R \mid\equiv \#(S_t) \quad \text{(P4)}$$

$$R \mid\equiv R \xleftrightarrow{S_r} T \quad \text{(P5)}$$

$$T \mid\equiv T \xleftrightarrow{S_t} R \quad \text{(P6)}$$

$$R \mid\equiv T \Rightarrow K_t \quad \text{(P7)}$$

$$T \mid\equiv R \Rightarrow K_r \quad \text{(P8)}$$

Where, R refers to the reader; T represents the tag, S_r is the random number generated by the reader; S_t is the random number generated by tag; K_t is the tag key stored in the tag in the communication process; K_r is the tag key stored in the reader or backend database in the communication process.

4.3. The Establishment of Idealized Model for the Protocol

In the idealization process of BAN logic, information that forwarded or transmitted in plaintext is independent from the analysis of security. Therefore, in the authentication protocol proposed in this paper, step 1 can be emitted in the idealization process, meanwhile, the communication channel between reader and backend server are reliable and the information forwarded by reader in the channel can be neglected. Since the backend server and reader in the step 3 and step 4 have similar operations, only one of the steps is executed in the authentication process. Therefore, the idealized model of the protocol can be described as follows:

$$T \rightarrow R : H(K_t \,||\, S_r) \quad \text{(M1)}$$

$$R \rightarrow T : H(K_r \,||\, S_t) \quad \text{(M2)}$$

The model can be converted into the following BAN logic idealized model:

$$R \lhd \{(K_t, S_r)\}_{S_r} \quad \text{(M1)}$$

$$T \lhd \{(K_r, S_t)\}_{S_t} \quad \text{(M2)}$$

4.4. The Security Goals of the Protocol

Because the reader or backend server authenticates the tag by using the random number K_t, and the tag authentications the reader via the random number K_r, the security goals can be set as follows:

$$R \mid\equiv K_t \tag{G1}$$

$$T \mid\equiv K_r \tag{G2}$$

4.5. Proof of the Protocol

The proof of G1 as follows:

According to rule R15 and assumption P1, we can get $\frac{R \mid\equiv \#(S_r)}{R \mid\equiv \#(K_t, S_r)}$, that is:

$$R \mid\equiv \#(K_t, S_r) \tag{1}$$

In accordance with rule R1, assumption P5 and idealized M1, we can get $\frac{R \mid\equiv R \xleftrightarrow{S_r} T, R \triangleleft \{(K_t, S_r)\}_{S_r}}{R \mid\equiv T \mid\sim (K_t, S_r)}$, that is

$$R \mid\equiv T \mid\sim (K_t, S_r) \tag{2}$$

According to (1) and (2) and rule R4, $\frac{R \mid\equiv \#(K_t, S_r), R \mid\equiv T \mid\sim (K_t, S_r)}{R \mid\equiv T \mid\equiv (K_t, S_r)}$ is obtained, that is:

$$R \mid\equiv T \mid\equiv (K_t, S_r) \tag{3}$$

According to rule R4 and (3), we can get $\frac{R \mid\equiv T \mid\equiv (K_t, S_r)}{R \mid\equiv T \mid\equiv K_t}$, that is:

$$R \mid\equiv T \mid\equiv K_t \tag{4}$$

According to rule R5, (4), and assumption P7, $\frac{R \mid\equiv T \mid\Rightarrow K_t, R \mid\equiv T \mid\equiv K_t}{R \mid\equiv K_t}$ is obtained, that is:

$$R \mid\equiv K_t \tag{5}$$

Now G1 is proved, the proof of goal G2 can be achieved in similar way, the proof is not repeated in this paper.

5. ANALYSIS ON PERFORMANCES OF THE PROTOCOL

RFID authentication protocol should ensures the security firstly, on which the higher the execution efficiency, the higher the practical value. The performance of the protocol proposed in this paper is analyzed from aspects of security and efficiency. In this section, we will present the security analysis and evaluate the efficiency performance of our protocol.

5.1. Security Analysis

1) Confidentiality. In the protocol, the secret information transmitted in insecure channel between tag and reader is encrypted by one-way Hash function. Although the random numbers generated by the reader and tag are transmitted in plaintext, the adversary is incapable of solving the tag key K even if he obtains the random numbers and the output value of Hash function due to the irreversibility of the one-way Hash function. The confidentiality of the tag key is ensured.

2) Resistance to tracing attacks. The adversary camouflages reader and sends random number S_r and authentication request *Query* to the tag to get the response $H(K_t \| S_r)$, which is used to trace the tags. Since S_r and S_t are random numbers and are different in each authentication process, the output value of the tag response $H(K_t \| S_r)$ are also disparate in each authentication process. Therefore, the protocol can effectively prevents the position tracing problems brought by the fixed output of the tag. Meanwhile, even if the adversary acquires the responses of multiple tags in authentication process, he does not know the responses come from which tag. In case of obtaining the responses of the same tag, the adversary is unable to distinguish the response is sent at which authentication process.

3) Resistance to forward security and replay attack. In the protocol, the adversary can obtains the random number generated by the reader, the authentication request *Query*, the tag response $H(K_t \| S_r)$, random number generated by the tag, the $H(K_r \| S_t)$ fed back by the reader or the backend database. However, attributing to the difference of S_r and S_t, it is impossible for the adversary to recall the historical data according to the information obtained in the authentication process, or, to simulate the data needed by the next authentication according to the current information obtained. Therefore, the protocol has forward security and anti replay attack ability.

4) Mutual authentication. In the protocol, after the reader sends random number S_r and the authentication request *Query* to the tag, tag conducts calculation and responses $H(K_t \| S_r)$ and S_t to the reader or backend database. In accordance with the tag key initialized by the system, the reader or backend database calculates and verifies the consistency of tags to confirm the legitimacy of the tag. Subsequently, the reader sends $H(K_r \| S_t)$ to the tag. According to the secret key and the random number S_t generated during the initialization, tag verifies the consistency of the reader. Since the key K of the tag is encrypted by one-way Hash function via a random number, the confidentiality of tag is ensured. Therefore, the identify verification on both reader and tag avoids the forgery on the reader or tag.

5) Resistance to denial of service attack (DoS). In the protocol, the reader needs to traverse the access list and calculate $H(K_r \| S_r)$, then verify the consistency of the tag response $H(K_t \| S_r)$ received. If the given condition is met, the protocol has no need of connecting with the backend server and there is no denial of service attacks; if given

condition fails to be met, the protocol needs to connect with the backend server for authentication. In this process, tag response information is sent by the reader after judgment instead of being directly transmitted to the backend server, the denial of service attack for backend server by forgery on large number of tags can be avoided.

6) Resistance to de-synchronization attacks. In the protocol, de-synchronization attacks are absent since the tag key *K* does not needs to update.

According to the above analysis, the security performances comparison of our works with other similar RFID authentication protocols are shown in Table **3**. Where × denotes that the security attributes cannot be satisfied, √ denotes that the security attributes can be satisfied; @ represents the security attributes not having existence.

5.2. Efficiency Analysis

The factors related to the efficiency of RFID authentication protocol mainly include storage requirements, computational cost, communication traffic, and sessions [15]. Suppose that the length of the K (key of tag) and Hash code are both set as l, h is encryption operation of Hash function, x represents the exclusive-or(XOR) operation, s represents the computation of the random number; n is the total number of tags in RFID system; r is the total number of readers, m is the number of the tag key stored in the reader. The computational cost refers to the Hash encryption computation, XOR computation, and random number computation of the reader, backend server, and tag for one whole authentication progress. Sessions are also the number of session required in one whole authentication progress.

1) Storage requirements. In the protocol, the tag needs to store its key K_t, the reader needs to store the K_r of m tags; the backend server needs to store the key K of all tags.

2) Computational cost. The tag needs two Hash computations h and one random number generation computation s, computation cost of the tag is $2h+s$. Since the protocol is server/serverless adaptive, if it does not needs to connect the backend server, the reader needs $m/2$ Hash computation on average, an additional Hash computation h, and a random number generation calculation s. Thus the computation cost of reader is $(m+2)h/2+s$. If the backend server need to be connected, the reader has a computation cost of $mh/2+s$. The backend server needs $n/2$ of Hash computation on average, therefore, the computation cost of backend server is $nh/2$.

3) Sessions. In the protocol, there are 5 sessions when connecting with the backend server, and 3 sessions without connecting with backend server.

4) Communication traffic. If the backend server need to be connected, the max communication traffic is emerged at step 3, which is $3l$. If it does not needs to connect the backend server, the max communication traffic is emerged at step 2, which is $2l$.

As shown in Table **4**, in similar protocols with a backend server, as a forward station to transmit data, the reader can not completely utilizes the storing capacity. In detail, the protocols proposed in literature [5] and literature [7] does not take any advantage of computing capacity of the reader. On contrast, the protocol proposed in this paper can makes full use of the computation and memory ability of the reader and backend server. As compared to the protocol that needs Hash computation on all the tags in the RFID system proposed in literature [6], the reader in our protocol conducts Hash computation on the tags in specific range, the computation and storage costs are completely acceptable for the reader. In addition, the tag in our protocol needs two Hash computation, which is more than the protocols proposed in literature [5] and literature [6], however, the security in the protocols proposed in literature [5] and literature [6] cannot fully guaranteed. Finally, other performances of the protocol in this paper are equal to or lower than those of other similar protocols.

Compared to similar protocols without a backend server, the tag merely requires a storage requirement of $1l$ in our protocol, but in protocols of literature [3], literature [9] and literature [10] the storage requirement is rl. Therefore, our protocol is suitable for the passive tags with small storage capacity. In addition, because the number of tags is much

Table 3. Security performances comparison.

Security performances	With a backend server				Without a backend server			Server/Serverless Adaptive
	[5]	[6]	[7]	[8]	[3]	[9]	[10]	Our works
Confidentiality	×	×	√	√	×	√	×	√
Tracing	×	√	√	√	√	√	√	√
Forward security	√	√	√	×	√	√	√	√
Replay attack	×	√	×	√	×	√	×	√
DoS	√	×	×	√	×	×	@	√
De-synchronization	@	@	×	×	×	@	@	@
Mutual Authentication	×	×	×	√	√	√	×	√

Table. 4. Efficiency performances comparison.

Efficiency performances	With a backend server					Without a backend server			
	[5]	[6]	[7]	[8]	Our works	[3]	[9]	[10]	Our works
Tag's storage	*2l*	*1l*	*1l*	*1l*	*1l*	*rl*	*rl*	*rl*	*1l*
Reader's storage	-	-	-	-	*ml*	*nl*	*nl*	*nl*	*ml*
Server's storage	*3nl*	*nl*	*2nl*	*3nl*	*nl*	-	-	-	-
Tag's computation	*1h*	*1h+s*	*2h*	*2h+3x+s*	*2h+s*	*1h+x+s*	*2h+s*	*2h+x+s*	*2h+s*
Reader's computation	-	*nh*	-	*s*	*mh/2+s*	*nh/2+2x+s*	*nh/2+s*	*nh+s*	*(m+2)h/2+s*
Server's computation	-	-	*nh/2*	*(n/2+1)h+2x*	*nh/2*	-	-	-	-
Communication traffic	*3l*	*2l*	*1l*	*3l*	*3l*	*3l*	*2l*	*3l*	*2l*
Sessions	*6*	*5*	*4n*	*5*	*5*	*3*	*3*	*4*	*3*

more than the number of readers in RFID system, so the computational cost and storage of reader in our protocol is better than that of literature [3], literature [9] and literature [10]. Finally, the storage of tag, communications and sessions are equal to or lower than that of other protocols. Although the computational cost of tag in our protocol is $2h+s$, which is more than that in literature [3], but the additional $1h$ is acceptable for a tag in RFID system.

In general, since the key of tag stored in the reader are pertinent, it only need to retrieve and compute the tags automatically stored in the reader in limited range. Because of the limited retrieving range and computational cost, the retrieve and computation efficiency is improved by $\frac{n-m}{n}\%$. Since the tag number m stored in the reader can be initialized into a reasonable fixed number according to the business requirements, the more tags in the RFID system, the higher the execution performance of the protocol. Besides, other performances of the protocol in this paper are equal to or lower than those of other similar protocols.

In addition, according to the initialization condition of the system, our protocol can automatically connects with the backend server for authentication when a tag was authenticated at first time. In the next authentication, since the tag has been stored in the reader automatically, the authentication can be completed without connecting the backend server. Therefore, the disadvantages can be effectively avoided because the protocol can automatically switched between the RFID authentication protocol with and without a backend server.

As a result, the protocol proposed in this paper is applicable to the RFID system with large amount of tags.

6. CONCLUSION

This paper proposed a server/serverless adaptive RFID mutual authentication protocol that could automatically make judgments on whether or not to connect the backend server for authentication according to the business scope of the tag. Through the security performance analysis, efficiency performance analysis and BAN logic proof, the protocol can meets main security requirements faced by current RFID systems with high execution efficiency and flexibility. While in practice, the number of the tag stored in the reader was set during the system initialization, our works is insufficient to deal with the matters of data overwriting when the tag number exceeds the upper range. Given these results we identified a few points which will be part of future work. The most important one is designing a counter to make the reader automatically overwrite the tags that are not usually authenticated.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

The research of this paper was supported by science and technology key project of Henan province (132102210123) and science and technology key project of education department of Henan province (13A520321). The authors thank the research team for the valuable discussions and suggestions.

REFERENCES

[1] R. Doss, S. Sundaresan and Wanlei Zhou, "A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems", *Ad Hoc Networks*, vol. 11, pp. 383-396, 2013.

[2] Y.P. Liao and C. M. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol", *Ad Hoc Networks*, vol. 18, pp. 133-146, 2014.

[3] Z. Yan, T. Chi and M. Chen, "New serverless authentication protocol for RFID", *Application Research of Computers*, vol. 31, pp. 1-4, 2014.

[4] H. Li, W. Xia, G. Deng and R. Wang, "Security analysis of a PUF based ultra-light weight mutual authentication RFID protocol-PUMAP", *Transactions of Beijing Institute of Technology*, vol. 33, pp. 1259, 2013.

[5] S. E. Sarma, S. A. Weis and D. W. Engels, "Radio frequency identification: secure risks and challenges", *RSA Laboratories Crypto Bytes*, vol. 6, pp. 2-9, 2003.

[6] S. A. Weis, S. E. Sarma, R. L. Rivest and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", In: *Proceedings of the 1st International Conference on Security in Pervasive Computing*, pp. 201-212, 2004.

[7] M. Ohkubo, K. Suzuki and S. Kingships, "Hash-chain based forward-secure privacy protection scheme for low-cost RFID", In: *Proceedings of Symposium on Cryptography and Information Security*, pp. 719-724, 2004.

[8] J. S. Cho, S. S. Yeo and S. K. Kim, "Securing against brute-force attack: a hash-based RFID mutual authentication protocol using a secret value", *Computer Communications*, vol. 34, pp. 391-397, 2011.

[9] M. Deng, Y. Wang G. Qiu and L. Zhou, "Authentication protocol for RFID without back end database", *Journal of Beijing University of Posts and Telecommunications*, vol. 32, pp. 59-62, 2009.

[10] C. C. Tan, B. Sheng and Q. Li, "Secure and serverless RFID authentication and search protocols", *IEEE Transactions on Wireless Communications*, vol. 7, pp. 1400-1407, 2008.

[11] R. Di. Pietro and R. Molva, "An optimal probabilistic solution for information confinement, privacy and security in RFID systems", *Journal of Network and Computer Applications*, vol. 34, pp. 853-863, 2011.

[12] D. G. Feng, "Research on theory and approach of provable security", *Journal of Software*, vol. 16, pp. 1744, 2005.

[13] M. Liu, Y. Wang and X. Zhao, "Research on RFID security authentication protocol based on hash function", *Chinese Journal of Sensors and Actuators*, vol. 24, pp. 1320, 2011.

[14] B. Zhang, X. Ma and Z. Qin, "Design and analysis of a lightweight mutual authentication protocol for RFID", *Journal of University of Electronic Science and Technology of China*, vol. 42, pp. 428, 2013.

[15] Z. Ding, J. Li and B. Feng, "Research on hash based RFID security authentication protocol", *Journal of Computer Research and Development*, vol. 46, pp. 589, 2009.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014