Hash-based RFID Mutual Authentication Protocol

Liu Yang[1,2*], Peng Yu[2],Wang Bailing[1], Qu Yun[1], Bai Xuefeng[1]
Yuan Xinling[1] and Yin zelong[1]

[1]Department of Computer Science & Technology
Harbin Institute of Technology at Weihai, Shandong, China
[2]Automatic Test and Control Institute
Harbin Institute of Technology, Harbin, China
**Liuyang322@hit.edu.cn*

Abstract

With the development and application of RFID technology in Internet of Things (IOT), RFID system plays a more and more important role on privacy protection and information security of users. For the safety need of RFID system and the existing shortage of secure authentication protocols, we offer RFID mutual authentication protocol based on variable update. Mutual authentication is executed in RFID system through the characteristics of Hash function, which prevents the phenomenon of counterfeit in internal system. Meanwhile, we adopt the method of periodic updates System initial value to improve the level of security authentication, which overcomes the various safety attacks. The protocol has certain advantages on security capabilities and algorithm complexity with high safety and practicality.

Keywords: *Mutual authentication; Hash; RFID; IOT*

1. Introduction

Internet of Things (IOT) is a New Network which interconnects wireless sensor RFID Information sensing equipment and so on to realize the overall perception of information, reliable transmission and intelligent processing. IOT gets all kinds of information about the physical world mainly through RFID and the sensor and so on, makes information transmission and interactive combined with internet, mobile communication network and so on, analyses and process information with smart computing technologies, which improves the perceptual skill of the physical world and realize intelligent decision-making and control [1]. According to agreed agreement, IOT takes any goods and Internet connection with the RFID device, the infrared sensor, GPS, laser scanner and other information sensing equipment, which makes information exchange and communication to realize intelligent identification, orientation, track, Monitoring and management.

The key technology of IOT is RFID technology which is a synthesis technique blending with radio frequency technology and Embedded Technology. RFID has wide application prospects on Automatic identification, Goods logistics management. It is a kind of Non-contact automatic identification technology on the rise in 1990s, which could identify identified objects automatically, multiple tags and the objects with high speed through the transmission characteristic of radio-frequency signal, space coupling, radar reflection. RFID technology with convenient operation and strong adaptability is the most advanced automatic identification technology at present.

With the widely application of RFID technology, the security of the RFID system is increasingly prominent. The communication between RFID tag and Reader adopts wireless

communication, which is considered unsafe and easily attacked by various ways[2]. The computational power, storage space and electricity supply of RFID tag are very limited. The characteristics and the boundedness of RFID tag bring the security mechanism of RFID system a lot of limitations, especially on security and privacy protection which has seriously hindered the further development of RFID technology and to be a key problem effecting RFID system.

For the security requirement of different RFID tags, many solutions have been proposed at present. These solutions are divided into two kinds of mechanisms [3]: physical mechanism and password system. Physical mechanism is mainly for the RFID tag which is not suitable for the executive password operation or one-time tag, including Kill command mechanism [4], active jamming [5], Blocker Tag [6], Ferrari cage [7] and so on. Although these physical mechanisms could partly ensure the safety of the RFID signal, these methods which are limited used need extra physical equipment and increase the RFID system cost [8]. Therefore, the industry more inclines to password mechanism. Password system mainly takes the method of the mutual authentication between tag and Reader to control the access to the tag, which enhance the security and privacy of the RFID system. More typical security protocols: Hash-lock protocol, randomizing Hash-lock protocol, hash chain protocol, ID change protocol based on Hash, distributed challenge-response protocol and so on [9]. Password system is a good measure solving security and privacy, but the existing scheme has obvious security weaknesses like needing tag and requiring Reader with strong ability of computing power [10]. These authentication protocols all assume that the channel between Tag Reader and back-end data base is secure and don't consider the mobile characteristics of Tag Reader and Tag [11], which doesn't agree with the real development of IOT and ignores the problem about fake and manipulation of legal Reader and legal tag in the internal system, lack of the ability to prevent attacks roundly.

We have summarized the problem about RFID security in the environment of IOT and propose RFID secure authenticated protocol based matrix variable update. The protocol ensures the privacy of information realizes three party mutual authentications, solves the problem that the existing RFID secure authenticated protocol couldn't realize mutual authentication in tag, Reader and Backend database, effectively resists attacks from internal system, updates and deals with initial variables periodically and improve the security of RFID system. Compared with the existing RFID secure authenticated protocol, ours could prevent existing security attacks and it has certain advantages on computational complexity and time complexity. Meanwhile, it has the high safety and practicality.

2. The Structure of RFID System

RFID system has a variety of classifications according to different principles. In the light of its different frequency, RFID system is divided into three categories such as low-frequency system (working frequency: 100-500KHz), mid-frequency system (working frequency: 10-15MHz), high-frequency system (working frequency: 850-950MHz and 2.4-5.8GHz). We also classify RFID system into active system and passive system on the base whether the battery placed in the tag provides energy for Tagged Traffic. On the other hand, RFID system is sort by technology means of reading electronic tag data such as radio emission type, times frequency type, reflection modulation and so on.

RFID system consists of Tag, Reader and Database.

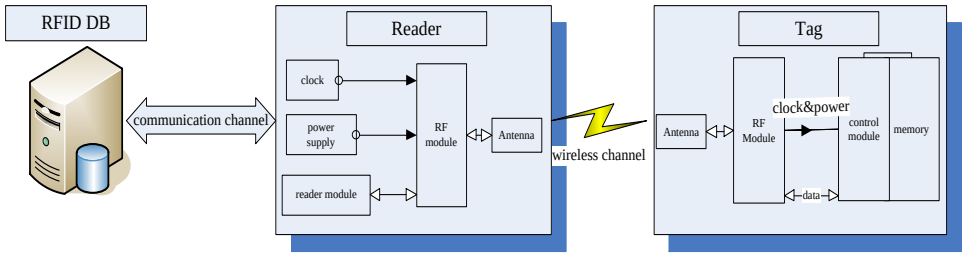

Figure 1.Composition of RFID System

The operating principle of RFID is that RFID is sent outside through radio carrier signal passing the transmitting wire of the RFID Reader. When the RFID tag enters into the transmitting wire's zone of action, the RFID tag will be active and be sent through the antenna. The carrier signal emitted by the RFID tag is received by the receiving antenna and it is sent to the Reader through the antenna. Then the RFID reader sends the received signal to the database after demodulating and decoding the signal. The legality of the Tag is judged by the database which makes decisions by logical operation and takes the corresponding treatment and control for different set. The control actuator runs according to command signals emitted by the database. The computer communication network which accretes monitory points together forms the general control information platform. The platform could design different corresponding software to finish functions we need according to actual different requirements of projects.

3. The Security Issue of RFID

With the development and widely application of RFID technology, the design and perfection of security authentication protocol plays a more important role on protecting the security of information and the privacy of users. The needs of RFID system on security include confidentiality (the reader which is unauthorized couldn't the tag's information), integrality (the system should make sure that information isn't tampered or replaced), availability (ensure that information is used effectively and the system works steadily) and privacy (prevent the attacker from grasping behavior, position and other privacy information of users). Therefore, RFID security issues mainly focus on privacy protection, prevention of attacks on RFID system, safety with RFID technology and so on. Security vulnerabilities mainly include the following situations on RFID system:

Access Violation. The attacker communicates with the tag directly to obtain important information stored in the tag through holding the protocol compatible reader, which result in personal information leaking.

Wiretapping: the attacker could detect communication content of the channel between the reader and the tag with RFID device, because the communication between the reader and the tag, the reader and the database is wireless. Thereby, we can capture the content of forward channel (the reader to the tag) and we also could capture the content of backward channel (the tag to the reader) to make doctoring information attacks, replay attacks, counterfeit attacks and so on

Doctoring information: the attacker transmits information wiretapped to the receiver after deleting and replacing part or whole of information, which results in the error and invalidation of response message. The purpose of attacks mainly includes malicious destruction of legal tags' content, prevention of legal tags' connection establishment and making the receiver believe the message modified is transmitted by a legal user.

Counterfeit attack: In the RFID communication network, the connection between the tag and the reader is by means of wireless channel. The tag must transmit its identity information through wireless channel so that the reader could properly identify its identity, but any message could be bugged in wireless channel. After the attacker gained sensitive information of the tag by illegal means, the real tag's information is copied to the counterfeit tag. When the reader transmits authentication information to the tag, the illegal transmits the tag information copied to the reader so that the tag is in the disguise of legal tag to be passed the reader authentication. Counterfeit attack belonging to active attack is the most popular attack method, which is one of the main hidden troubles faced by system security. The main method to solve the problem about counterfeit attack is the implement of authentication protocol and data encryption.

Replay attack: when the reader (the tag) sends authentication information, the attacker captures the response message. When the reader (the tag) sends authorization request next time, the attacker rebroadcasts the previous transmit information of the tag (the reader) to the reader (the tag) so that the tag (the reader) passes the authentication of the reader (the tag) in purpose of acting as the tag (the reader). The attack threatens the RFID system badly, so we prevent the system from being attack with the method of transmission data encryption.

Location tracking: the illegal sends fixed information to locate the tag in purpose of tracking and locating. The attacker could send inquiring command anywhere and associate the obtained tag's certain information with the identity of the tag (the holder) in condition that the tag returns certain information when queried each time. Therefore, the RFID system should satisfy indistinguishability and forward security. Indistinguishability is undistinguishable ability of the information which one tag sends and what others send. Forward security is that the attacker couldn't verify the tag through obtaining the previous tag sent.

Forward security attack: the attacker captures the tag's output in the communication, and then the previous information sent by the tag could be obtained in relation to current data and history data.

Because of the limitation of storage capacity and computational capacity of the tag and the reader, the attacker sends a lot of requests to the tag with counterfeit. The tag's memorizer will halt in that its memorizer stores a lot of random numbers or reads tags to the limit of tag numbers. On the other hand, the attacker constantly sends authorization request information to the database in purpose of running out of the database's buffer resource, which results in the RFID system communication interrupt.

4. Design of Security Authentication Protocol

In this section, we describe our algorithm for detecting sensors whose readings (measurements) are faulty. Firstly, we illustrate NDHN by using an aggregation session scenario example, and then we present the detection procedure and the algorithm.

4.1. System Initialization Process

1) Information stored in the database (DB): the reader ID(R_1,R_2..R_n), the initial value of each reader R_1（X_1,Y_1）..R_n(X_n,Y_n); System initial value (X,Y); Tag information and tag ID (T1,T2,… Tid); Session key K.

2) Information stored in the reader (R): the reader ID(R_n), the initial value of the reader R_n(X_n,Y_n) System initial value (X); variable L; Tag Rid; the value of Hash(y'||Tid') calculated previously; Session key K.

3) Information stored in tag T: System initial value (X,Y); Tag Tid.

4.2. Authentication process

1) The reader R generates a random number Rr1, calculates Hash(X||Rr1) and sends request and Hash(X||Rr1)|| Rr1 to the tag T.

2) The tag T calculates Hash(X'||Rr1) compared with the Hash(X||Rr1)received after receiving information. If the Hash(X'||Rr1) calculated is equal to the one received, the authentication for the reader R would be accomplished. If the Hash(X'||Rr1) calculated isn't equal to the one received, the message would be gave up. The tag T calculates Hash(Y'||Tid')|| Hash(X'||Rr1||Tr1)||Tr1 and sends it.

3) The reader R judges whether the Hash(Y'||Tid') stored is equal to the Hash(Y'||Tid') after receiving information. The equality of them shows that being queried and stop querying, which prevents the attacker from making DDos attack on the server with repeatedly sending query information. If they aren't equal, the reader calculates Hash(X'||Rr1) compared with the Hash(X||Rr1) received. If the Hash(X'||Rr1) calculated is equal to the one received, the authentication for the tag T would be accomplished. At the same time, the reader R calculates Hash(Y' $\oplus$ Tid')|| Hash(Y_n||Rr2||Rid)||Rr2||Tr1 and sends it to the database DB.

4) The database DB calculates Hash(Y'_n||Rr2||Rid) compared with the Hash(Y_n||Rr2 $\oplus$ Rid) received after receiving information and gets Rid and (X_n,Y_n) to accomplish the authentication for the reader R. If the Hash(Y||Tid) calculated is equal to the one received and Tid has been obtained, the authentication for the tag T would be accomplished. The database DB consults with the reader R about the session key K through a secure channel and calculates K^+(Tid||Rr2||X_n)|| Hash(Y||Tid||Tr1) and sends it to the reader R.

5) The reader R uses the session key K to calculate K^- (K^+(Tid||Rr2||X_n)) for obtaining the ID of the tag T (Tid)after receiving information and accomplishs the authentication for the database DB. After that, R sends the Hash(Y||Tid||Tr1)calculated to the Tag T.

6) The tag T calculates Hash(Y||Tid'||Tr1)compared with the Hash(Y||Tid||Tr1) received. If the Hash(Y||Tid'||Tr1) calculated is equal to the one received, the authentication for the database DB would be accomplished.

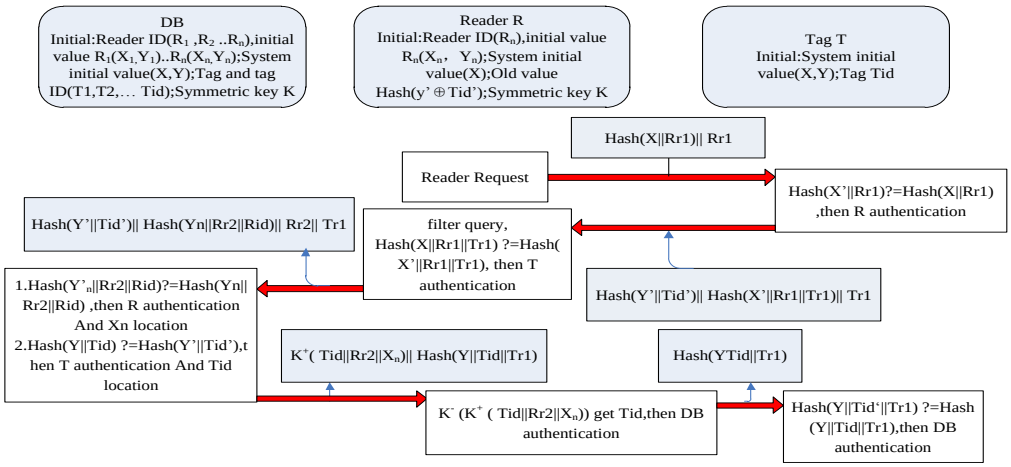

Figure 2. RFID Mutualauthentication

4.3. Update process

Update process is updating relevant variable of the database DB, the reader R and the tag T. The countdown called TTL should be set in the database DB for timing corresponding (X,Y), $R_n(X_n,Y_n)$. Update id renew is also set in the database DB. After the countdown timing is over, specific update process is divided into two kinds: update from the reader R and update from the database DB.

1)Update from the reader

a) When TTL in the reader R is 0, the reader R sends update id renew and $Hash(X_i||Y_i)||Rid||Rr0$ to the database DB.

b)The database DB calculates Rid corresponding $Hash(X'_i||Y'_i)$ compared with $Hash(X_i||Y_i)$. If the $Hash(X'_i||Y'_i)$ calculated is equal to the one received, the authentication for the reader R would be accomplished. The back-up inhere is reserved and the variable of the database DB is updated. (X_n,Y_n) corresponds with (M_n,N_n) and (X,Y) corresponds with (A, B). Then, the database DB encrypts in the use of the session key K consulted with the reader and sends $K^+(M_n||N_n||A||B/Y)||Hash(Xi||DBr||Rr0)||DBr$ to the reader R.

c) The reader R calculates $Hash(X'_i||DBr||Rr0)$ compared with $Hash(X_i||DBr \oplus Rr0)$ after receiving information. If the $Hash(X'_i||Y'_i)$ calculated is equal to $Hash(X_i||DBr \oplus Rr0)$, the authentication for the database DB would be accomplished. The reader R decrypts, keeps the back-up inhere and updates corresponding variables. (X_n,Y_n)corresponds with (M_n,N_n); (L) corresponds with (X), (X) corresponds with (A). The reader R generates a random number Rr1 and send Hash(X'||DBr) ||DBr ||Rr1 to the tag which would be read.

d) The tag T calculates Hash(X||DBr)compared with Hash(L||DBr). If the Hash(X||DBr)calculated is equal to Hash(L||DBr)received, the authentication for the reader R would be accomplished. The tag T calculates Hash(X||Rr1) and sends it to the reader R.

e) The reader R calculates Hash(X||Rr1) compared with Hash(L||Rr1) after receiving information. If the Hash(X||Rr1) calculated is equal to Hash(L||Rr1) received, the authentication for the tag T would be accomplished. The reader R generates a random number Rr2 and sends $(Rr2 \oplus A)||(Rr2 \oplus B/Y)||Rr2$ to the tag which would be read.

f) The tag T gains A with $Rr2 \oplus A \oplus Rr2$; $(Rr2 \oplus Rr2 \oplus B/Y)$*Y gains B and updated (X,Y) is (A,B). The original initial value (X,Y) is reserved and the update is over.

What above has been authenticated before it is updated.

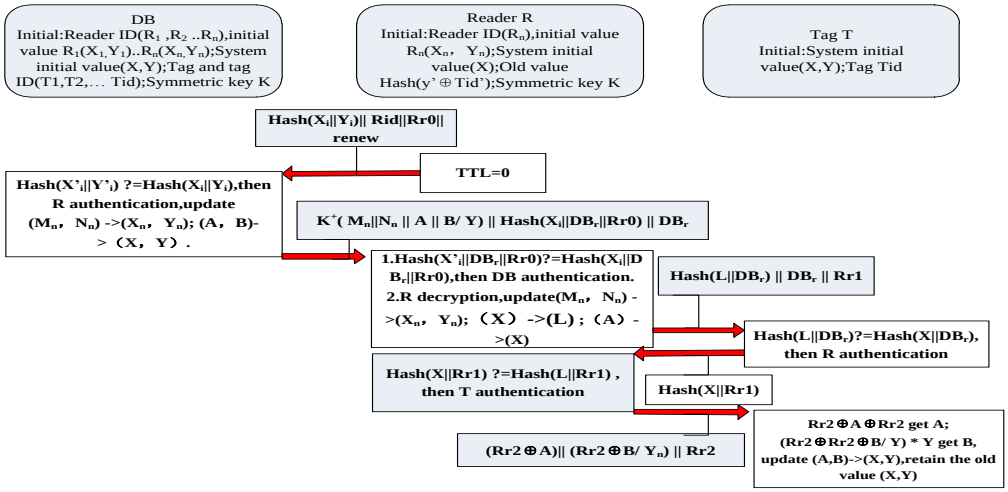

Figure 3. Reader R renew process

2) Update from the database DB

a) When TTL in the database DB is 0, the database DB sends the update id renew and Hash(Xi||DBr)||DBr to the reader R.

b) The reader R calculates Hash(X_i||DBr)compared with Hash(X_i||DBr). If the Hash(X_i||DBr) calculated is equal to the one received, the authentication for the database DB would be accomplished. The reader R sends Hash(Y_i||Rr2||Rid)||Rr2 to the database DB.

c) The database DB calculates Hash(Y'_i||Rr2||Rid) compared with Hash(Y_i||Rr2||Rid) received. If they are equal, the authentication for the reader R would be accomplished. The database updates corresponding variables. (X_n,Y_n) is (M_n,N_n); (X,Y) is (A,B). Then, DB encrypts in the use of the session key K consulted with the reader R. DBr which is a random number sends K^+(M_n||N_n||A||B/Y)||Hash(X_i||DBr||Rr2)||DBr to the reader R and keeps the original back-up of (X,Y)

d) Step 4 to step 6 is accordance with step 4 to step 6 of update from the reader R

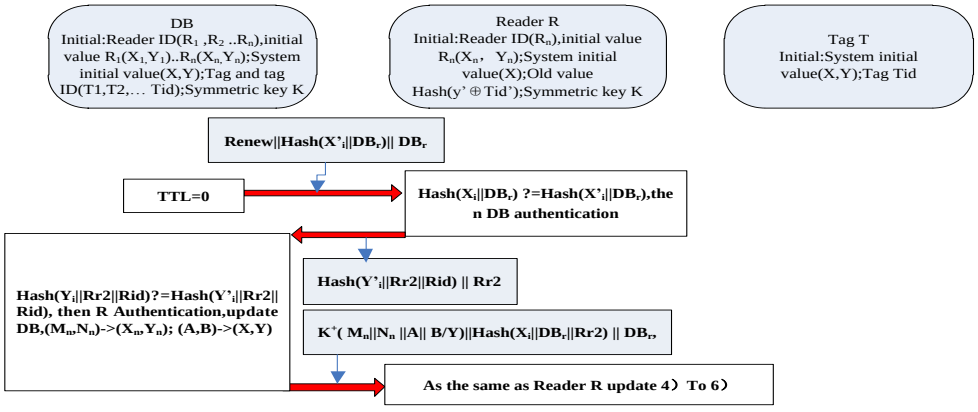

Figure 4. Database Renew Process

5. The Formal Proof of the Protocol

For verifying the security of the protocol, we formally analyses the authentication protocol, adopt GNY [12] logical proof from the hypothesis of the protocol and achieve the beforehand goal.Formally certify objectives

$$T \mid\equiv R \mid\sim \#hash(X \parallel Rr1) \tag{1}$$

$$T \mid\equiv DB \mid\sim \#hash(Y \parallel Tid \parallel Tr1) \tag{2}$$

$$R \mid\equiv T \mid\sim \#hash(X \parallel Tr1 \parallel Rr1) \tag{3}$$

$$R \mid\equiv DB \mid\sim \#K^{+}(X_n \parallel Tid \parallel Rr2) \tag{4}$$

$$DB \mid\equiv T \mid\sim \#hash(Y \parallel Tid) \tag{5}$$

$$DB \mid\equiv R \mid\sim \#hash(Y_n \parallel Rid \parallel Rr2) \tag{6}$$

Objective 1 the proof procedure of $T \mid\equiv R \mid\sim \#hash(X \parallel Rr1)$

Initial assumption $T \mid\equiv \#Rr1,\ T \ni Rr1,\ T \ni X,\ T \mid\equiv T \overset{Rr1}{\longleftrightarrow} R$

Obtained from the rule $\dfrac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y), P \mid\equiv \#(F(X))}$ and $T \mid\equiv \#Rr1$:

$T \mid\equiv \#Rr1 \parallel X$ ……a

Obtained from the rule $\dfrac{P \ni X, P \ni Y}{P \ni (X,Y), P \ni F(X,Y)}$ and $T \ni Rr1,\ T \ni X$

$T \ni Rr1 \parallel X$ ……..b

Obtained from the rule $\dfrac{P \mid\equiv \#(X), P \ni X}{P \mid\equiv \#(H(X))}$ and the thesis a, b

$T \mid\equiv \#hash(X \parallel Rr1)$ ……..…..c

Obtained from rule $\dfrac{P \lhd *H(X,< S >), P \ni (X,S), P \mid\equiv P \overset{S}{\longleftrightarrow} Q, P \mid\equiv \#(X,S)}{P \mid\equiv Q \mid\sim (X,< S >), P \mid\equiv Q \mid\sim H(X,< S >)}$

assumption $T \mid\equiv T \overset{Rr1}{\longleftrightarrow} R$, Message $T \lhd *Rr1, *hash(X \parallel Rr1)$, thesis a, b

$T \mid\equiv R \mid\sim hash(X \parallel Rr1)$ ……..d

Obtained from freshness theorem and thesis c, d

$T \mid\equiv R \mid\sim \#hash(X \parallel Rr1)$

Proof procedures of other objectives 2,3,4,5,6 are in the same with the proof procedure.

6. Analysis of the Protocol's Performance

RFID security mainly reflects in the privacy of users and the security of information. We declare the protocol's security capacity through the following analysis of the protocol against various attacks.

Mutualauthentication: the scheme realizes mutualauthentication mechanism between the tag and the reader, the reader and the database, the database and the tag. After mutualauthentication, the tag Tid would be dealt with to enhance reliability of authentication.

Defence against wiretap: In the scheme, attackers outside of the system couldn't contact with the tag to start the attack, because they don't know the authentication process of the system. Attackers inside of the system couldn't calculate the tag's Tid, even though they could illegally obtain Hash(Y'||Tid), because the reader and the tag' ID are transmitted in hash function forms instead of plaintext forms . Beside, only reader authenticated legally could read the tag's data information so that illegal read is prevented, potential hazard after exposing Tid is avoid and privacy is protected effectively.

Defence against counterfeit: Because the reader only has system initial value in the authentication process, the reader finally obtains the tag's real ID through verifying the combination of the tag's system initial value and X_n obtained with the database's verification of Y_n provided by the reader. The authentication scheme restrains bi-directionally on the reader, the tag and the database ,because random numbers and initial value are changing.

Defence against replay attack: the attacker in the disguise of the reader could retransmit the reader's authentication request previously obtained for the tag on the purpose of obtaining the response message from the tag. From the other Hand, the attacker in the disguise of the tag could retransmit the tag's authentication request previously obtained for the reader, which cheats the reader. In the mutualauthentication process on the tag, the reader and the database with different combinations of random numbers Rr1, Tr1, Rr2 and so on, the scheme makes sure that the data transmitted back and forth is variational and sends or receives random numbers compared, which can defend against and identify the replay attack effectively.

Defence against Dos attack: because the tag and the reader separately record random numbers, we can use them to match with random numbers requested newly. If they are in the cache, they would be given up. At the same time, Dos attacks would be prevented effectively with handling ability of periodically updating (X,Y).

Defence against traffic analysis: Attackers couldn't conduct traffic analysis attacks, because the authentication process and the transmision process adopt the combination of random numbers and the reader and the tag' ID aren't transmitted in hash function forms instead of plaintext forms.

Forward security: In every authentication phase, the values of the tag, the reader, the database add a random number and they attached to messages are transmitted together. Meanwhile, they periodically update (X,Y), because attackers couldn't recall the tag's related history activities information, even though they obtain Hash(Y'||Tid')|| Hash(X'||Rr1||Tr1)||Tr1.

Defence against position tracking attack: the value of the tag's every response on the reader's query Hash(Y'||Tid')|| Hash(X'||Rr1||Tr1)||Tr1 is diffrernt , because the tag adopts different random numbers in dealing with different time requests of different readers and the one-way hash function, the correlation of different ciphertexts is lower and the initial value (X,Y) is changing and updating. We could prevent the attacker from location and tracking based on special outputs so that the attacker difficultly judges whether the request message comes from the same tag, even though position trailing is carried out through capturing data.

In conclusion, the authentication scheme could effectively defend against various attacks in IOT. Table 1 shows the analysis about defense capability of several kinds of common RFID security certificate for different attacks. √ indicates the protocol has the function, × indicates the protocol doesn't have the function.

Table 1. RFID Security Authentication Protocol against Attacks Ability Comparison

authentication protocol	Anti-eavesdropping	Forward security	Anti-denial	Anti-replay attack	Anti-phishing attack	Anti-location track	Anti-traffic analysis	Anti-insider attack	Mutualauthentication
Hash chain	√	√	×	×	×	√	√	×	×
Hash-lock	×	×	×	×	×	×	×	×	×
Random Hash lock	√	√	×	×	×	√	×	×	√
Hash-based ID variation protocol	√	√	×	√	√	√	√	×	√
Distributed challenge-response protocol	√	√	√	√	√	√	×	×	√
Mutual authentication protocol	×	√	√	√	√	√	×	×	√
This protocol	√	√	√	√	√	√	√	√	√

From the comparison, Hash chain protocol, Hash lock protocol and Hash lock protocol couldn't defend against Dos attacks, replay attacks, counterfeit attacks and internal attacks; they are not secure. ID variation based on Hash still doesn't solve Dos attack and internal attack; Distributed query- response protocol, David digital library RFID protocol and Tee mutual identify have a good effect on defense eavesdropping, forward security and position trailing, but they couldn't defend against internal attacks. Nevertheless, the security certificate protocol solves the safety privacy problem of RFID system in the certain degree and it has a good safety.

RFID security protocol not only guarantees privacy and security of information transmission but also synthetically considers the inherent characteristic of the tag and the reader. The characteristic is mainly on the limitation of computational power and memory capacity, which lowers the cost of RFID system. Therefore, we verify the algorithm advantage of the protocol in space complexity and time complexity through the comparison between the protocol and the existing RFID security authentication protocol. The related calculation expressions involved in the protocol are agreed in the following represents Hash calculation; R generates random numbers calculation; XOR represents or calculation; K represents Encryption operation; L represents 128-bit Hash function calculated value.

Table 2. The Complexity of the Algorithm Comparison Table

protocol	time complexity			space complexity		
Authentication protocol	tag	reader	DB	tag	reader	DB
Hash chain	2 H		2nH	1L		2nL
Hash lock	1 H			2L		3nL
Random Hash lock	1 H 1R	nH		1L		2nL
The changes of ID protocol based on Hash	3 H		3H,1R 1XOR	3L		10nL
Distributed challenge-response protocol	2 H 1R	1R	(n+1)H	1L		nL
David RFID protocol	2 H 2XOR	1R	2nXOR	2L		2nL
This protocol	4H,IR	5H 2R,1K	3H,1K	1L	1L	2nL

From the comparison, most protocols all have n order of magnitudes operation and a part of protocols involve several n order of magnitudes operations, which results in the phenomenon that arithmetic speed is slower and nodes consume more energy. The protocol allows the strong computing power database to deal with a number of calculations and its calculation load is lighter than other protocols. Although the calculation load involved in the tag and the reader is a little heavier than other algorithms, it is able to meet the safety need of RFID system overall.

7. Conclusion

The article has analyzed RFID security issues in IOT. We propose the RFID Two-way authentication protocol based on updating variables and securely transmit ID in ciphertext form between the reader and the tag through Hash function characteristic on purpose to guarantee the privacy of information. Meanwhile, we realize three party mutual authentications and solve the problem that RFID security certificate couldn't realize in the tag, the reader and the database so that the internal system counterfeit phenomenon is defended effectively. At the same time, we adopt the method to periodically update system initial value in order to enhance security level and overcome various security attacks. Compared with the existing secure authentication protocols and computational complexity, the protocol has a certain advantage on algorithm complexity and safety performance and it has a higher security and practical applicability.

Acknowledgements

This research was supported by the National Science Nature Foundation of China under Grant No 61170262.

References

[1] Z. Lina, S. Chaoyi and F. Li, "Early warning of the propagation direction of network worms", J. J. Huazhong Univ. of Sci. & Tech. (Natural Science Edition), **(2009)**, pp. 13-16.
[2] H. Gilbert, R. Matthew and H. Sibert, "An active attack against HB+: A provably secure lightweight authentication protocol", IEEElectronics Letters, vol. 41, no. 21, **(2005)**, pp. 1169-1170.
[3] Q. Y. Dai, R. Y. Zhong, M. L. Wang, X. D. Liu and Q. Liu, "RFID-enable Real-time Multi-experiment Training Center Management System", International Journal of Advanced Science and Technology, vol. 7, **(2009)** June, pp. 27-48.
[4] A. Sarma and J. Girao, "Identities in the Future Internet of Things", Wireless Personal Communications, Springer Netherlands, vol. 4, **(2009)**, pp. 258-263.
[5] F. Zhang and X. Sun, "A universally composable secure RFID communication protocol in supply chains", Chinese Journal of Computers, vol. 10, **(2008)**, pp. 1754-1767.
[6] Y. B. Zhou, D. G. Feng, "Design and analysis of cryptographic protocols for RFID", Chinese Journal of Computers, vol. 29, **(2006)**, pp. 581-589.
[7] H. D. Gao, Y. J. Guo, J. Q. Cui, H. G. Hao and H. Shi, "A Communication Protocol of RFID Systems in Internet of Things", International Journal of Security and Its Applications, vol. 6, **(2012)** April, pp. 91-102.
[8] V. Letri and B. Medeirosde, "Universally composable and forward secure RFID authentication and authenticated key exchange", Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, New York: ACM, **(2008)**, pp. 242-252.
[9] M. O. Balitanas and T. -h. Kim, "Review: Security Threats for RFID-Sensor Network Anti-Collision Protocol", International Journal of Smart Home, vol. 4, **(2010)** January, pp. 23-36.
[10] D. Zhenhua, L. Jintao and F. Bo, "Research on Hsah-based RFID security authentication protocol", Journal of Computer Research and Deveolpment, vol. 4, **(2009)**, pp. 583-592.
[11] G. Avoine and P. Oechslin, "A scalable and provably secure hash-based RFID protocol", Proceedings of the 2nd IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2010), Washington, DC, USA, **(2010)**, pp. 110-114.

[12] K. Rhee, J. Kwak, S. Kim and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment", Hutter D., Ullmann M. eds.. Proceedings of the 2nd International Conference on Security in Pervasive Computing (SPC 2009). Lectures Notes in Computer Science 3450.Berlin: Springer-Verlag, **(2009)**, pp. 70-80.

Authors

Liu Yang, Associate Professor, his research fields include Network information Security Technology, Internet of Things Security Technology, etc. He has participated in many projects of Ministry of Information Industry and National Science, and he has published over 20 academic papers in journals and conferences both home and abroad.

Wang Bailing is working for Harbin Institute of Technology (abstract as HIT) as an associate professor. He got the Ph.D. degree from HIT in 2006. His research is mainly on information security, network security, parallel computing.