Sensors & Transducers

© 2014 by IFSA Publishing, S. L.
http://www.sensorsportal.com

RFID Cryptographic Protocol Based on Cyclic Redundancy Check for High Efficiency

[1] Nian Liu, [1,*] Ye Yin, [1] Xiangnong Wu, [2] Long Ye

[1] College of Information and Mechanical Electrical Engineering, Shanghai Normal University,
Shanghai 200234, China
[2] College of Information and Computer, Shanghai Business School,
Shanghai 201400, China
[1] Tel.: 13918621989, fax: 021-67827111
[1] E-mail: shidayinye@163.com

Received: 10 January 2014 /Accepted: 7 April 2014 /Published: 30 April 2014

Abstract: In this paper, RFID encryption protocol is proposed based on the security problems in wireless signal channel. In order to solve the privacy issues of electronic tags, the most commonly way is to improve algorithms based on Hash function. However, there are some problems that can only play roles in some specific domains. Due to the limitations in various kinds of algorithms, in this paper we put forward a new kind of agreement. When it is required to locate target labels accurately and rapidly in a movement environment, using this agreement can achieve high efficiency through combining the Hash function, the two division search algorithm and CRC check. The results show that this algorithm can accurately identify the tags with merits of low cost, execution rate and anti-attack ability etc. *Copyright © 2014 IFSA Publishing, S. L.*

Keywords: Radio frequency identification, Security protocol, Anti-attack capability, Cyclic redundancy check, High efficiency.

1. Introduction

Radio frequency identification (RFID) system is a non-contact wireless communication technology, which is used to automatically identify the target and access to relevant information through radio frequency signals [1]. In the field of wireless communication, RFID has been widely applied because of its low-cost and convenience. At the same time, the security issues of the label information face a lot of hidden dangers [2]. Aimed at RFID security issues, there have been a lot of researches at home and abroad, such as Hash-Lock protocol, Hash-Chain protocol, SPA protocol, AES algorithm etc [3]. However, these cryptographic security protocols have some drawbacks to some extent. Due to these inadequacies, in this paper we propose a new RFID encryption security protocol, which designed to achieve a low-cost system with high security and improved efficiency of identifying label.

2. The Security Issues

In the actual application environment, via the Internet or LAN, the reader of RFID connects with the backend server and communicates with tags through a wireless channel. Generally it is believed that the formal channel is secure, while the latter is not. That is to say, the data transmitted between reader and tags is susceptible to be attacked and eavesdropped by assailants. It is an important issue to design a reliable information security mechanism. Otherwise, you cannot protect the RF-tag data effectively [4].

The RFID security problems are mainly about the authentication, confidentiality and integrity. The cost of tag, on the other hand, may directly affect the performance of RFID security. Only with reliable security mechanisms, we can achieve the efficient protection to the security threats of low-cost tags [5]. A good security protocol must have an advantage in information processing complexity, and provide enough anti-attack ability in replay, tracking, counterfeiting, insertion and de-synchronization [6].

3. The Usual Protocols

Here, we introduce some commonly used security authentication protocol.

3.1. Hash-Lock Protocol

As is shown in Fig. 1, Sarma proposed the Hash-Lock protocol in 2003. It uses Hash (ID) to reply the real message ID and to avoid the information being leaked or tracked [7].

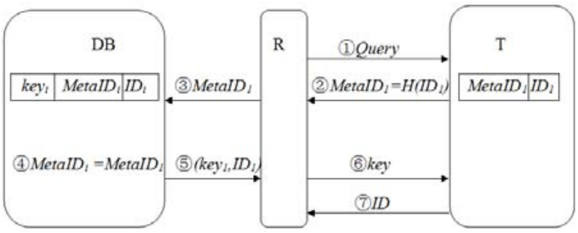

Fig. 1. Hash-Lock protocol.

In this protocol, the tag T uses Hash function to encrypt the self-information ID. The backend server DB sequentially searches $(H(ID_i), Key_i, ID_i)$ which matched with H(ID) in the target tag, so as to complete the verification. The Hash-Lock protocol can achieve privacy protection. In the process of communication, even if the attacker sized H(ID), he cannot decipher the tag ID information [8]. However, H (ID) remains the same all the time, it is easy to be tracked and positioned. The assailants can easily replicate a same tag to make repeatedly attack to the reader, resulting in an increased computation of the backend server and even channel congestion [9].

3.2. Hash-Chain Protocol

Differently from the defects of Hash-Lock protocol, Hash-Chain protocol is based on the shared inquiry-response mechanism [10]. It guarantees the security of frontal channel. The Hash-Chain protocol is shown in Fig. 2:

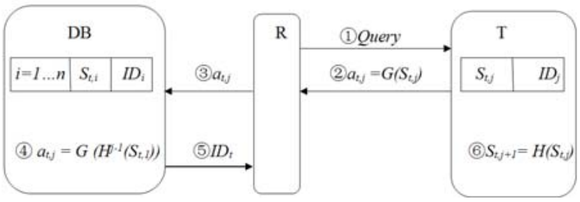

Fig. 2. Hash-Chain protocol.

In this protocol, T uses two Hash functions: The encrypted ID information $G(S_{t,j})$ and the updated density value $H(S_{t,j})$. Hash-Chain protocol remains the one-way channel security of Hash-Lock protocol. At the same time, owing to the random update of $S_{t,j}$, even if the attacker intercepts $G(S_{t,j})$, he cannot make position tracking and replay attacking [11]. However, this protocol uses two Hash functions, which may make more computation and slower execution efficiency of the backend server [12].

3.3. SPA Protocol

The SPA protocol, which is based on the tree structure to reduce the complexity of authentication, is proposed by Molnar and Wagner. All labels are distributed in leaf nodes of a k degree balance tree. The depth of the tree is $\log_k N$, and the value of each branch is a random number $k_{i,j}$, where i is the layer of the label in the tree, and j is the branch number. It can uniquely identify one group target value through the branch node path. The structure of k degree tree is shown in Fig. 3:

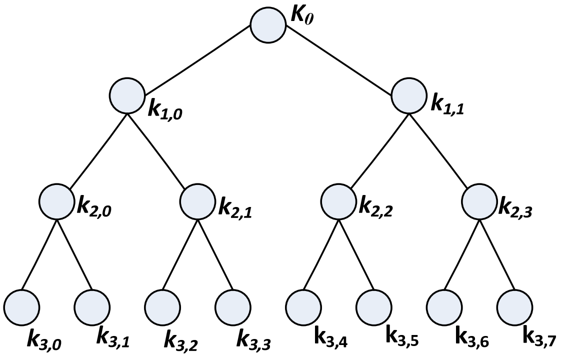

Fig. 3. Structure of k degree tree.

In this protocol, the system needs to confirm the information from the root node to branch node to ensure which branch layer the target lies in. To find the i-th value k_i of the secret group of label, system only needs to search from j secret values $(k_{i,0}, k_{i,1}, \ldots k_{i,j})$ in the i-th layer of the tree, which reduces the time complexity to $\Theta(\log N)$, and greatly improves the running speed of the backend server.

However, just due to this bifurcation characteristic of tree structure, the attacker can easily follow the track of another label which shares the same path as this one [14].

In this protocol, the system confirms the information from the root node to branch node, to ensure which branch layer the target lies in. To find the i-th value k_i of the secret group of label, system only needs to search from j secret values $(k_{i,0}, k_{i,1}, ... k_{i,j})$ in the i-th layer of the tree, which reduces the time complexity to $\Theta(\log N)$, and greatly improves the running speed of the backend server. However, just owing to this bifurcation characteristic of tree structure, the attacker can easily follow the track of another label which shares the same path of this one [14].

4. The Proposed Protocol

According to the characteristic of the Hash function, any alteration or replacement of the original plaintext data will get a different result. With the frontal Hash-based security protocols, based on the shared inquiry-response mechanism, the security of the RFID system can be increased. However, the backend servers can search the secret value k_i from the N messages $(k_0, k_1, ... k_{N-1})$, which makes the time complexity of the system too high. This would not be suitable for large-scale tagging systems. With the tree-based security protocols we can improve the search efficiency by constructing a code tree structure. However, this feature leads to that any two tags share a common code value at least. There would be obvious security vulnerability – due to the leakage of one message, the tags in the same path can be easily tracked.

Based on the problems of the previous security protocols, with proposal in this paper we can improve the Hash function security protocol combining with binary search algorithm and cyclic redundancy check code. We can also achieve the security communication and reduce the time complexity. This protocol most probably provides much more comprehensive advantages in safety properties, anti-attack ability, low cost and high execution rate etc.

4.1. The Mathematical Principle

Suppose that there are n(n≥1) ordered integers stored in the array list. list[0]≤list[1]≤…≤list[n-1]. We need to find that whether searchnum is in this list. If it exists, just return searchnum=list[i], or return -1.

In orderly search algorithm, we sequentially compare searchnum with list[i] from front to back, until we find the value for searchnum=list[i]. It spends clock time $\Theta(1)$ to cycle a while statement language. By this way, the mathematical time complexity of backend server is $\Theta(n)$.

In binary search algorithm, suppose that left and right represent the endpoint of the list, and the number of tags is n. At first, we set that left=0, right=n-1, middle=(left+right)/2. Each time we compare searchnum with list[middle], the length of the list would be reduced to half of the original value. The cycle would not be stopped until we find the middle that meets searchnum=list[middle].

As we can see, the binary search algorithm can effectively reduce the computation of backend server. It can reduce the time complexity to $\Theta(\log n)$, lower the workload, and improve the search efficiency with high rate of identification.

4.2. Cyclic Redundancy Check Code

Cyclic Redundancy Check code (CRC) is a kind of calibration method that checks the correctness of data communication. It starts from the data itself, and verifies the data rely on the agreement from of mathematics. CRC can directly test whether an error is occurred. If it does, the recipient may notify the sender to resend the data again.

In CRC, the sender sends m-bit information data T(x), and the recipient receives the data D(x).If T(x)=D(x),there is no error in the transmission process. CRC appends R(x), a k-bits binary parity information, at the end of the data T(x). There is a special relationship around the parity information R(x), the generator polynomial g(x), and the information data T(x). Once any date goes wrong, this special relationship may be broken up. Therefore, we can verify the correctness of data by checking this relationship.

In the CRC-8 international standard, the generator polynomial is $g(x) = x^8 + x^5 + x^4 + 1$. The sender moves T(x) left to k bits, and then makes XOR operation with g(x). The remainder is the check number R(x). On the other hand, the recipient makes the inverse operation for the information data. If the finally result has a remainder, the data T(x) must have been tampered in the transmission channel, or it is correct.

4.3. Improved RFID Security Protocol

The backend server uses CRC-8 to check the information which is sent back by reader. If the attacker illegally tampers the tag information in the wireless communication path, CRC-8 can immediately pick out the illegal label, and return it back without any handles. In this way, the system can avoid searching for the error label, and greatly reduce the workload.

On the other hand, after the CRC-8 proving the correctness of the tag information, the backend server does the position search work. As to the Hash security protocol, it searches the target from all labels one by one. The algorithm complexity is $\Theta(n)$. But for binary search algorithm, the comparison between searchnum and list[middle] can greatly reduce the search time. It can quickly find the target, and the time complexity is $\Theta(\log n)$. On condition that the number of tag N is large, the binary search algorithm may have higher execution speed.

Combining CRC-8 with binary search algorithm can prevent tampering attacks effectively, avoid occupying the resource of backend server, and reduce the time complexity. At the same time, relative to the tree protocol, it can avoid the connection between the tags and thus prevent the attack of label location tracking.

The implementation process of the protocol is shown in Fig. 4:

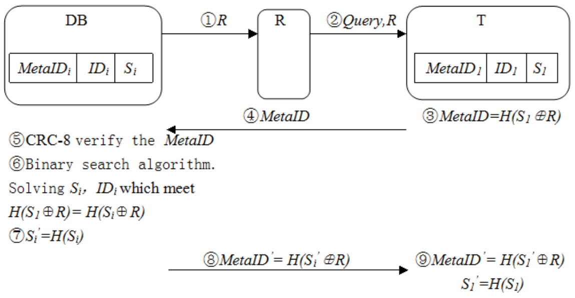
DB
$MetaID_i$ | ID_i | S_i
①R
R
②$Query,R$
T
$MetaID_1$ | ID_1 | S_1
④$MetaID$
③$MetaID=H(S_1 \oplus R)$
⑤CRC-8 verify the $MetaID$
⑥Binary search algorithm.
Solving S_i, ID_i which meet
$H(S_1 \oplus R)= H(S_i \oplus R)$
⑦$S_i'=H(S_i)$
⑧$MetaID'= H(S_i' \oplus R)$
⑨$MetaID'= H(S_1' \oplus R)$
$S_1'=H(S_1)$

Fig. 4. Improved RFID security protocol with high efficient.

The implementation process is as follows:

1) When the system DB needs to search for a tag, it generates a random number R, and sends it to the reader;

2) Reader sends the information Query and R to the tag T, which is in the range of the reader identification;

3) The tag T makes XOR operation between R and its own secret value S_1, then calculates its Hash function value: $MetaID = H(S_1 \oplus R)$;

4) T sends MetaID to reader, and continues to DB;

5) DB verifies the value MetaID by CRC-8 method. If it exists remainder, verification is wrong, which means that the information sent by T is tempered by attacker. If so, just sends it back and process over. Or the authentication is passed.

6) On condition that the step (5) is passed, we search DB by binary search algorithm. In $(H(S_i \oplus R), ID_i)$, find the value S_i that meets $H(S_1 \oplus R) = H(S_i \oplus R)$.

7) Update the secret value: $S_i' = H(S_i)$.

8) Calculate $MetaID' = H(S_i' \oplus R)$. DB sends $MetaID'$ to reader, and continues to T.

9) Verify $MetaID' = H(S_1' \oplus R)$. If it success, the authentication is passed. Update the value $S_1' = H(S_1)$.

5. Performance Assessment

In this paper, the encryption security protocol combines Hash function encryption and binary search algorithm. The one-way security of Hash function can guarantee the safety of the label information effectively, and achieve the anti-attack capability of eavesdropping, information leakage and data occultation. At the same time, it combines with the updated keys, avoiding the label problem of being copied and position tracking. The protocol based on Hash function can reduce the design complexity of label with low cost and easy production.

On the other hand, CRC-8 prevents the information being tampered in wireless channel. It avoids the illegal label occupying the process of backend server. In the end, this scheme uses binary search algorithm, which greatly improves the time complexity. This proposed security protocol shows comprehensive advantages in security, low cost, efficiency and complexity, etc.

5.1. Security Analysis

The proposed scheme can improve the work efficiency. When there are a large number of tags, it achieves target location capabilities, and can ensure the security of the communication process.

1) Reduce cost:

The random number generator is in the backend server, which reduce the design complexity of the tags and the reader.

2) Anti-illegal to read:

Only certified reader is able to get the information of the label. This protocol makes use of the one-way security of Hash function. The attacker cannot reverse the label value S_1 even if he intercepts the information $MetaID = H(S_1 \oplus R)$.

3) Data integrity:

Any intervention or replacement to the original plaintext data will get a different result. This can guarantee the data integrity.

4) Anti-retransmission:

The random number R, produced by the backend server, makes the information $MetaID = H(S \oplus R)$ difference in each certification process. The attacker cannot camouflage tags to cause retransmission.

5) Anti-intervention:

CRC-8 can verify the value of metaID, which can guarantee the correctness of the information in the transmission path. This method reduces the time to validate illegal labels.

6) Lower time complexity:

Supposed that the legal number is N, the time complexity of Hash protocol is $\Theta(n)$. In this paper, with the binary search algorithm the times of searching the target can be reduced. The time complexity is $\Theta(\log n)$. The larger the N is, the higher of the speed in the execution.

7) Two-way authentication security:

When DB searches the target, it compares with the value $MetaID = H(S_1 \oplus R)$, which realizes the safety of the forward channel from the reader to the tags. On the contrary, the tag compares with $MetaID' = H(S_1' \oplus R)$ and the security of backward channel can be guaranteed.

8) Anti-tracking:

Update the value R and S. Even if the attacker intercepts much information of the tags, he cannot find the relevant rule or the related historical activity information.

5.2. Performance Evaluation

This scheme combines with Hash function and binary search algorithm. It can promise the anti-attack capability of retransmission, counterfeit, replication, intervention, insertion, denial of service and two-way security and location tracking etc.

We make comprehensive comparison among Hash-Lock protocol, Hash-chain protocol, SPA protocol and this proposed protocol. Their characteristics of security, complexity, and executive efficiency are show in Table 1.

Table 1. Security comparisons.

	Hash Lock	Hash Chain	SPA	This paper
Intervention	N	Y	N	Y
Two-way authentication	N	N	Y	Y
Retransmission	N	Y	Y	Y
Intercept	N	Y	Y	Y
Location tracking	N	Y	N	Y
Update key	N	Y	Y	Y
Timecomplexity	$\Theta(n)$	$\Theta(n)$	$\Theta(\log n)$	$\Theta(\log n)$

(N denotes it has no anti-attack capability in this performance. Y denotes it has the anti-attack capability)

By comparing with the directly search, tree-search and binary search algorithm, there would be obvious differences.

In direct search algorithm, we suppose that there are N labels. To find the target searchnum, we need one search at least and N searches at most. So the overall complexity of the worst situation is $\Theta(n)$. In tree-search algorithm, the depth of the δ degree tree is $\log_\delta N$. Each label stores a password group [S1, S2 …, SL],which is the path value from root node to leaf node. In the i-th layer, there just need δ/2 search times, which means that the certification times for each tag is δ*L/2. In this algorithm, the process of searching tags is just searching the branch node of the tree. The time complexity is reduced to $\Theta(\log n)$. In this paper, by comparing searchnum with list[middle], the length of the array would be cut down to half. The complexity of the best situation is $\Theta(1)$, and the worst is $\Theta(\log n)$.

Simulated by MATLAB, there are different time complexities in the curves shown in Fig. 5.

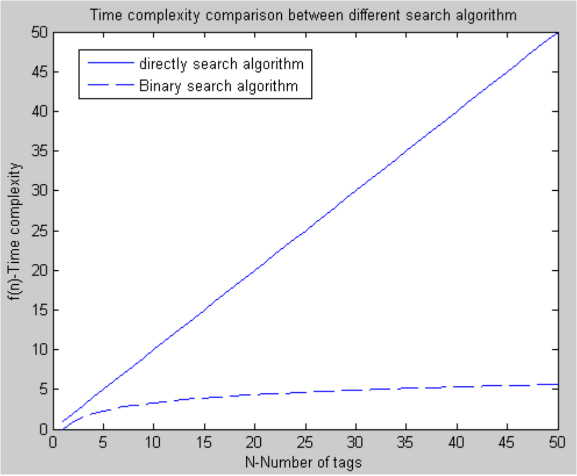

Fig. 5. Time complexity comparison of different search algorithm.

It can be seen from Fig. 5 that the complexity of binary search algorithm is less than the direct search. Especially in the environment with large number labels, this comparison of complexities will be more obvious. The binary search algorithm can greatly reduce the computation of the backend server, and effectively improve the execution efficiency.

6. Conclusions

In the application of location in large venues, due to the large number of tags within the recognition scope of the reader, the targets mixing and attacker invasion are easily occurred. We usually need to locate the target tag accurately and quickly. It means that we need to guarantee the anti-attack security capability with low-cost of the tags, besides the high execution efficiency.

In this paper we improve the normal RFID security protocol, which combines with the one-way security of Hash-function, updating keys, binary search algorithm and CRC verification. In the security part of information, with our new proposal the retransmission and intervention can be prevented. Thus it reduces the time of identifying wrong labels. Additionally, it reduces the time complexity of the server. This protocol has comprehensive advantages in security property, time complexity and low cost. It provides a makeup for the problem of time complexity in the inquiry-response mechanism security protocol, and a solution to the security problem in the tree structure protocol. It has potential applications in the low-cost label environment.

Acknowledgements

Authors are grateful to the anonymous reviewers for their helpful comments. They also wish to note that the research work is supported by the National Natural Science Foundation of China (No. 61101209), Shanghai Normal University key project (A7001-12-002006), the Venus project of Shanghai Business School (QMX2012-14), Supported by General Program of Shanghai Natural Science Fund (No. 13ZR1430400), and Supported by Innovation Program of Shanghai Municipal Education Commission (No. 14YZ070).

References

[1]. Jeremy Landt, The history of RFID, *IEEE*, Vol. 24, Issue 4, 2005, pp. 8-11.

[2]. Wang Qinghua, Xiong Xiaozhong, Tian Wenhao, et al., Low-Cost RFID: security problems and solutions, in *Proceedings of the International Conference on Management and Service Science (MASS)*, 2011, pp. 1-4.

[3]. B. R. Ray, M. Chowdhury, J. Abawajy, Critical analysis and comparative study of security for networked RFID systems, in *Proceedings of the 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2013, pp. 197-202.

[4]. A. N. M. Noman, M. Rahman, C. Adams, Improving security and usability of low cost RFID tags, in *Proceedings of the Ninth Annual International Conference on Privacy, Security and Trust (PST)*, 2011, pp. 134-141.

[5]. D.-Z. Sun, J.-D. Zhong, A hash-based RFID security protocol for strong privacy protection, *IEEE Transactions on Consumer Electronics*, Vol. 58, Issue 4, 2012, pp. 1246-1252.

[6]. Lei'an Liu, Zhiqiang Chen, Ling Yang, Yi Lu, Research on the security issues of RFID-based supply chain, in *Proceedings of the International Conference on E-Bussiness and E-Government (ICEE)*, Guangzhou, China, 2010, pp. 3267-3270.

[7]. M. R. Rieback, B. Crispo, A. S. Tanenbaum, The evolution of RFID security, *IEEE Pervasive Computing*, Vol. 5, Issue 1, 2006, pp. 62-69.

[8]. Piao Chunhui, Fan Zhenjiang, Yang Chunyan et al, Research on RFID security protocol based on grouped tags and re-encryption scheme, in *Proceedings of the IEEE International Conference on Wireless Communications, Networking and Information Security*, 2010, pp 568-572.

[9]. Dong Seong Kim, Taek-Hyun Shin, Jong Sou Park, A security framework in RFID multi-domain system, in *Proceedings of the 2nd International Conference on Availability, Reliability and Security ARES*, April 2007, pp. 1227-1234.

[10]. R. K. Pateriya, Sangeeta Sharma, The evolution of RFID security and privacy: a research survey, in *Proceedings of the International Conference on Communication Systems and Network Technologies CSNT*, 2011, pp. 115-119.

[11]. Y. Yang, J. Gu, C. Lv, Q. Jiang, W. Ma, Security analysis of Kulseng et al.'s mutual authentication protocol for RFID systems, *IET Information Security*, Vol. 6, Issue 4, 2012, pp. 239-248.

[12]. Yan Fang, Liu Bingwu, HuoLingYu, Yang Xi, Research and design of a security framework for RFID system, in *Proceedings of the International Forum on Information Technology and Applications (IFITA)*, Vol. 2, 2010, pp. 443-445.

[13]. Tzipora Halevi, Nitesh Saxena, Shai Halevi, Tree-based HB protocols for privacy-preserving authentication of RFID tags, *Journal of Computer Security*, Vol. 19, Issue 2, 2011, pp. 343- 363.

[14] A. K. Bashir, S. H. Chauhdary, S. C. Shah, M. S. Park, Mobile RFID and its design security issues, *IEEE Potentials*, Vol. 30, Issue 4, 2011, pp. 34-38.