Acta Technica *62* No. 2B/2017, 597–606

Anti-collision algorithm and security authentication mechanism of radio frequency identification system[1]

Jinyan Liu[2], Quanyuan Feng[2]

Abstract. Radio frequency identification (RFID) is a non-contact automatic identification communication technology. Based on the requirement analysis of anti-collision algorithm and security authentication function of radio frequency identification system in this paper, the improved binary search anti-collision algorithm and the RFID security authentication protocol based on Hash function and state locking were proposed respectively, so as to ensure the promotion of the efficiency and security of radio frequency identification system. The results show that the improved binary search anti-collision algorithm has a shorter data transmission length, and is more efficient for large-scale object label recognition, and the RFID security authentication protocol based on Hash function and state locking can avoid illegal attack and complete tag authentication effectively through Hash function, symmetric encryption, ID updating and K value.

Key words. Anti-collision algorithm, RFID, binary search, hash function.

1. Introduction

With the innovation of information technology, it is possible to establish communications between object information through information sensing devices, identification systems and the Internet, so as to realize the automatic and intelligent system of information system in the development of modern industry [1]. Radio frequency identification (RFID) system, as an important component of the perception layer in the architecture of Internet of things, is the key module to support the Internet of things. RFID technology allows contactless and unique identifying objects, and the Internet of things transfers this information from the sense layer to the application layer through the network layer, so that the interconnected neural net of things is formed.

[1]This work is supported by the National Natural Science Foundation of China under Grant 61531016.

[2]School of Information Science and Technology, Southwest Jiaotong University, Chengdu, Sichuan, China, 610031

Compared with other identification technologies, RFID technology can adapt to long distances, and it can make a batch and other advantages, so it has been widely concerned and applied to the logistics, access control and other industries [2]. Although the RFID technology in the world has been widely studied and applied, there are still some problems such as high costs of electronic tags, overlapping aliasing of multiple labels and information security, which restricts the popularization and promotion of RFID technology. Based on this, the research on anti-collision algorithm and security mechanism of RFID technology was launched in this paper, so as to improve the operation efficiency of RFID system and guarantee the security of data and channel.

2. State of the art

In RFID system, information collision refers to the superposition of multiple tag information when multiple tags are identified at the same time, thus, it is difficult for readers to recognize the tag information, which seriously reduces the operation efficiency of RFID system [3]. The anti-collision algorithm based on RFID system is built on the principle of time division multiplexing (TDMA), and scholars have also done a lot of researches on anti-collision algorithms of RFID system, but in the past research on anti-collision algorithm, it will still face such problems. On the one hand, some anti-collision algorithms have too long recognition times and high requirements on the moving speed of tags, so the efficiency is too low; on the other hand, if it simply increases the recognition efficiency by increasing the amount of control in a timely manner, it will result in a substantial increase in operating costs [4]. Therefore, it is an urgent problem for RFID system to improve the operation efficiency without increasing the system cost.

The security authentication mechanism of RFID system is concerned with many aspects, such as system security protection and privacy protection. Only by ensuring the data security of RFID system, can the effective application of Internet of things be realized [5]. In order to prevent the illegal attack on RFID system and the leakage of information of individuals, goods and enterprises, it is necessary to realize the encryption of information and the security authentication of users through security protocol. There are more mature security protocols, such as DES and AES, but what cannot be ignored is that these security protocols can guarantee the operation safety of system to a certain extent, and there is also an increase in costs resulting from the increased logical processing units. At the same time, limited to the calculation and storage capabilities of the tag, it is difficult for the existing security protocols to be popularized in applications of the RFID system. Therefore, lightweight security protocol is also the focus of RFID system research.

2.1. Methodology

2.2. An improved binary search anti-collision algorithm

In this paper, through the study of the current status of RFID system operations and the application of the survey results, it is found that the binary search algorithm has high recognition rate for electronic tags, which is more suitable for large-scale identification of objects. Therefore, in this paper, a binary search anti-collision algorithm was used as the object of study, and on this basis, the improved binary search anti-collision algorithm was analyzed and studied.

The binary search algorithm requires Manchester encoding (Manchester) to provide accurate bit locations for multiple electronic tags to enter the identification area, so that the tag search can then be carried out according to the corresponding rules [6]. The encoding setting map is listed in Table 1.

Table 1. Electronic tag encoding settings

Tag number	Coding (8-bit)
Label 1	01010101
Label 2	01010111
Label 3	01110101
Label 4	01100110
Label 5	01010100

In this study, the sleep counting method was adopted; then, the search time of the reader was then shortened by identifying an electronic tag state. The anti-collision command in this algorithm is divided into request command Request (x, m), activation command Active, removing command Unselect and Read-Data and so on [7]. The function of the request command is to detect the difference between the high value of the tag conflict and the binary value of the 1 bit. If the value is consistent, it will be answered and returned, otherwise, the label is converted to sleep, and the corresponding sleep level is 1 or 1.; the activation command is used to reduce the sleep label, and make it become the standby state by reducing the 1 sleep level of the sleeping tag; the removing command is to change the selected label into "silent", without responding to the commands issued by the reader [8]. In this study, the tag code was set as 8 and the number was 5, as shown in Fig. 1.

When the tag enters the identification area, a request command is issued to all tags in the area. The diagram is shown in Fig. 1, and the process is as follows:

The first request command: for the label entering the reading area, the system sends the Request (NULL, 8) command to it, and then the UID data obtained is 01XX01XX. The maximum collision bit index is 5, which is used as the parameter setting for the second request command, and at the second time, it executes the Request (0, 5) command.

The second request command: after the execution of the first command, the standby fifth-bit response labels are numbered Label, 1, Label 2, and Label 5. The UID data obtained at this time is 010101XX, and the maximum collision bit index

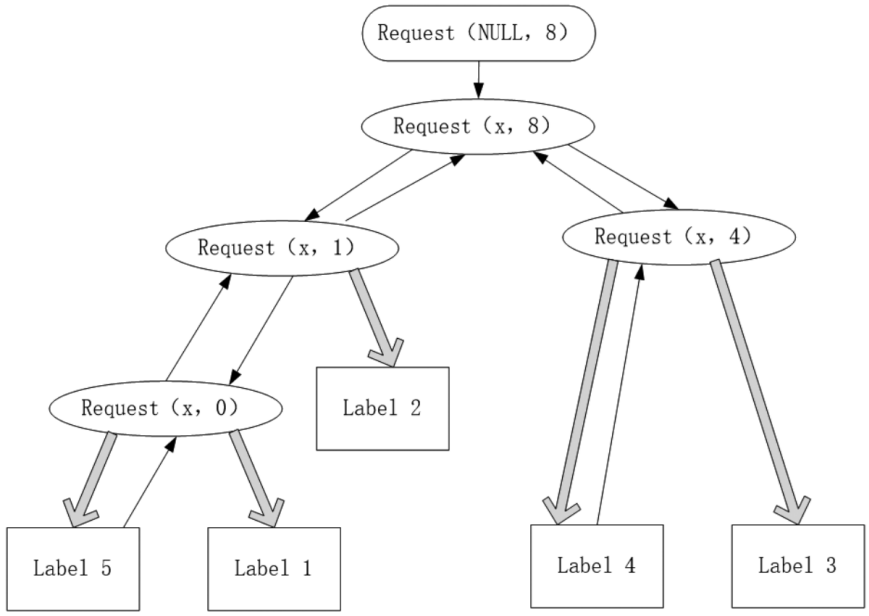

Fig. 1. Collision algorithm identification schemes

is 1, so the Request (0, 1) command is required for the third time. In addition, the command sets label 3 and label 4 to be in a sleeping state (the fifth is 1), and the label 1, label 2, and label 5 still keep a standby state.

The third request command: at this point, label 1 and label 5 which are on a standby state will respond to the Request (0, 1) command issued by the reader, and the maximum collision bit index is 0, and the fourth request command can be executed. The command parameter is Request (0, 0). In addition, the value of the sleep level of label 2 is 1, and label 3 and label 4 are added to 1.

The fourth request command: the execution process has no collision and can be accurately identified, and it will execute other commands in turn, and it will also execute the living command Unselect at the end of the execution and place it in "silent". When a tag is correctly identified, the system sends the activation command Active to all tags, and the dormant degree of corresponding labels has been reduced by 1, and the rebound strategy has been taken. Unlike the beginning, the first parameter is 1.

The fifth request command: the system sends a request command to each tag, and at this time the parameter is set as Request (1, 0), which means that the label whose zeroth digit value is 1 should make a response. Comparing the coding of the five tags, it is found that each of them does not produce collisions, so that the tags can be correctly identified and other operations can be performed sequentially.

The sixth request command: the command parameter is Request (1, 1), and Label 2 responds to the reader and can be correctly identified.

The seventh request command: the command that the system sends to the tag is

Request (1, 5), and when both Label 3 and Label 4 make a response (both of which are standby labels with the fifth digit value of 1), and the maximum collision bit index is 4, which is the parameter of the next request command.

The eighth request command: according to the above operation, the operation result shows that the request command is Request (0, 4), and Label 4 makes a response (the encoding is a standby label with the fourth digit value of 0), and the collision does not happen.

As shown in Fig. 1, the binary tree structure has 4 sub-nodes behind the root node of the tree structure to ensure the accurate identification of each tag. It is characterized by bidirectional search between root nodes and sub nodes, and it reduces the number of searches that are required for multiple tag identification in the anti-collision algorithm design [13]. In the process of the identification of the 5 tags set by the experiment, it can be found that the number of searches is 9, and $S(5) = 2(5\text{-}1) + 1 = 9$. Thus, the binary search anti-collision algorithm requires the number of searches that are required to identify the n tags should be $S(n) = 2(n-1)+1 = 2n-1$.

As shown in Table 2, it is the improved binary search anti-collision algorithm and the binary search algorithm [14]. Compared with the dynamic binary search algorithm, it has a shorter data transmission length and greatly improves the recognition efficiency of the anti-collision algorithm [15]. With the increase of the number of identification tags, the efficiency advantage of this algorithm is more obvious.

Table 2. The sum of the length of the transmitted binary data

Algorithm	The total length of the transmitted binary data
The binary search algorithm	$L_1 = \frac{m(m+1)}{2} N$
The dynamic binary search algorithm	$L_2 = \frac{m(m+1)}{2} \frac{N+1}{2}$
The improved binary search algorithm	$L_3 = (2m-1) \times \log_2^N + 1$

2.3. Research of RFID security authentication protocol based on Hash function and state locking

Radio frequency identification (RFID) needs to add secure and lightweight security protocols to ensure the security and efficiency of the identification system [9]. According to the characteristics of Hash function in RFID security authentication, in this paper it was combined with the state locking module organically. The authentication system is characterized by mutual authentication between the reader and the tag [10]. The legitimacy of the tag is validated by the backend database [11]. In the process of authentication, new ID and key values are constantly formed, which can prevent illegal attacks and avoid information leakages and system paralysis [12].

The schematic diagram of the authentication protocol is shown in Figure 2, and the authentication procedure is as follows:

1. It generates random number r and then passes it to the data to form cipher text and request authentication through the encryption algorithm.

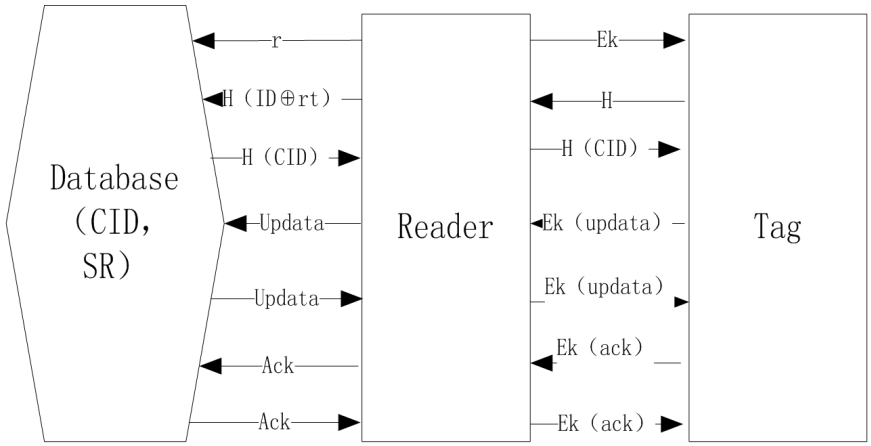

Fig. 2. The schematic diagram of authentication protocol based on Hash function and state locking

2. Database accepts the r value, and then the tag extracts Query and the r value is transmitted to the reader by encryption.

3. H (ID source RT) value is sent to the back-end database.

4. It is necessary to query the CID field, so as to judge whether the numerical values of H (ID source RT) and H (CID source RR) are unanimous.

5. H (CID) is forwarded to the tag to determine whether the H (CID) and the H (ID) values are consistent, or it will pass the authentication, otherwise, the authentication fails.

6. The update data is extracted, and passed to the database.

7. The CID value is updated.

8. The key of the reader is updated.

9. The label ID and key are updated.

10. The ack value is extracted and passed to the database. After setting the SR value to 00, the ack value is passed to the reader.

11. When the tag extracts the ack message, the ST is set to 00.

The meanings of particular symbols in agreement are listed in Table 3.

3. Result analysis and discussion

3.1. Algorithm simulation analysis

The binary search algorithm and the improved binary search anti-collision algorithm were simulated by using MATLAB software. In the simulation experiment, the tag length is 16 bits, as shown in Fig. 3, left part. When the number of processing tags is 10, the binary search algorithm searches 80 times, while the improved binary search anti-collision algorithm searches only 19 times, and search times are reduced by 76 % after improvement; when the number of processing tags is 80, the

binary search algorithm searches 159 times, while the improved binary search anti-collision algorithm searches only 726 times, and search times are reduced by 76 % after improvement. Therefore, the improved binary search anti-collision algorithm can effectively reduce the number of searches with equal number of tags, and improve the operational efficiency. At the same time, as the number of tags increases, the number of search decreases, and it has more advantages in improving the efficiency of large-scale tagging.

Table 3. The meaning table of symbol in the agreement

Sequence number	Symbol	Meaning
1	K	shared key
2	ID	Tag identification number
3	ST	Label state
4	rt	Tag stored in the random number
5	r	Reader stored in the random number
6	CID	Backend database to store the current tag identification number
7	SR	State of the reader
8	PID	Backend database to store the last tag identification number
9	Rr	Random Numbers are stored in the database background
10	Random ()	Random function
11	E()	Symmetric encryption algorithm
12	D()	Nverse execution of symmetric encryption algorithm
13	H()	Hash function
14	Updata	Both sides agreed updates
15	Ack	Both sides agreed confirmation
16	II	Join operation
17	$\oplus$	Exclusive or operation

In Fig. 3, right part, the binary search algorithms and the improved binary search anti-collision algorithms are used for tag identification, and sums of the length of the binary data positively rise with the increase of the number of tags. But from the slope of the two curves, the improved binary search anti-collision algorithm can obviously reduce the total length of binary data transmission. When the number of processing tags is 80, the binary search algorithm has a total binary data length of 14328, while the improved binary search anti-collision algorithm searches only 854 times, and the total length of the improved binary transmission data is reduced by

94 %, which greatly improves the recognition efficiency of the anti-collision algorithm.

The improved algorithm can effectively reduce the number of searches and the total length of binary data transmissions, thus greatly improving the channel saving. In recent years, with the development of computer and Internet, the logistics industry and the new business model have been developing rapidly, which makes it difficult for people to identify, collect and record the information of goods, and it is hard to satisfy the pursuit on efficiency in the information age, moreover, manual labor can also greatly waste labors and cause unavoidable operational errors. The improved binary search anti-collision algorithm can better reflect the advantages of the algorithm when dealing with a large number of larger labels, which can effectively improve the processing efficiency of RFID system and solve the interference problem of simultaneous responses of multiple tags in the operation of RFID system, thus avoiding manual operations in the identification process to the greatest extent.

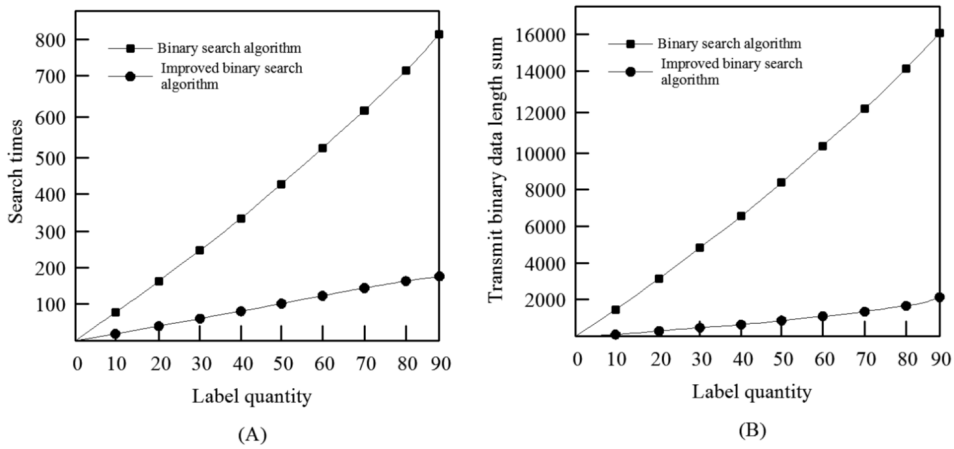

Fig. 3. Number of searches (left) and the total length (right) of transmission data

3.2. Security analysis of the security authentication protocol

In the previous analysis of the security authentication process (Fig. 2), the authentication protocol has high data confidentiality, tag anonymity, forward security and mutual authentication. Among them, the data confidentiality is manifested in the identification process of the tag system, and the data involved is encrypted by the encryption algorithm or Hash function, which ensures the confidentiality of the information passed by the tag and reader [16]. The anonymity of the tag means that the information received by the reader is changing constantly and randomly, which also means that the intercepted label information is erratic for the attacker; the function of the forward security is to update the ID and K values of the tag synchronously, so that even if the attacker has obtained the ID and K values of the current tag, it is also difficult to reverse the tag information before it is launched; the mutual authentication shows that readers and labels need to complete mutual

information comparisons in this secure authentication protocol, so as to realize the mutual authentication and complete the information reading.

In addition, this security authentication protocol also has the following two advantages: on the one hand, the timely updating of ID and K values of the tag ensures that it is difficult for the attacker to retrieve the ID value of the tag again when the reader has finished identifying the tag, that is, the reader will not be re-authenticated; on the other hand, the protocol can lock each step of the system, and the operation of the state is unique. Even if the attacker steals all the information, it is difficult to find the status of the reader's identification on the tag, and the attacker's illegal instructions will not be responded. RFID security authentication protocol based on Hash function and state lock integrates many modules, such as information encryption, status lock and background database, which ensures that every program in the system is locked into a specific state in the process of security authentication. While realizing the mutual authentication between the reader and the tag, the information security risk of the RFID authentication system is effectively avoided by updating the label ID and K value.

4. Conclusion

The optimization of anti-collision algorithm and the construction of security authentication mechanism are two important aspects in the research of radio frequency identification technology. In the research of the improved binary search anti-collision algorithm, it is found that the improved binary algorithm has shorter data transmission length compared with the binary search algorithm and the dynamic binary search algorithm, which greatly enhances the recognition efficiency of the anti-collision algorithm, and with the increase of the number of identification tags, the efficiency advantage of this algorithm is more obvious. At the same time, the research of RFID security authentication protocol based on Hash function and state locking can effectively protect the information security of each process of RFID system in the process of label authentication, and through the application of background database, the updating of label ID and K value and the locking of label status, data confidentiality, label anonymity, forward security and mutual authentication are realized at the same time, which effectively reduces the risk of information security caused by illegal attacks. But limited to the research time and effort, the binary search algorithm in anti-collision algorithm and the RFID security authentication protocol based on Hash function and state locking were discussed and simulated in this paper, and the application research of RFID system was not done. There may be a short board in the design and connection of other components of the RFID system, which will affect the practical performance of the algorithm, and further researches are needed.

References

[1] X. Liu, B. Xiao, K. Li, J. Wu, A. X. Liu, H. Qi, X. Xie: *RFID estimation with blocker tags.* IEEE/ACM Transactions on Networking *25* (2017), No. 1, 224–237.

[2] Y. H. Chen, S. J. Horng, R. S. Run, J. L. Lai, R. J. Chen, W. C. Chen, Y. Pan, T. Takao: *A novel anti-collision algorithm in RFID systems for identifying passive tags.* IEEE Transactions on Industrial Informatics *6* (2010), No. 1, 105–121.

[3] J. Zhao, N. Li, D. A. Li, R. Bai, B. Zhu, X. Liu: *Collision alignment: An RFID anti-collision algorithm assisted by orthogonal signal detection and analogy principle.* Telecommunication Systems *66* (2017), No. 1, 131–144.

[4] J. Su, X. Zhao, D. Hong, Z. Luo, H. Chen: *Q-value fine-grained adjustment based RFID anti-collision algorithm.* IEICE Transactions on Communications *E99.B* (2016), No. 7, 1593–1598.

[5] K. C. Shin, S. B. Park, G. S. Jo: *Enhanced TDMA based anti-collision algorithm with a dynamic frame size adjustment strategy for mobile RFID readers.* Sensors (Basel) *9* (2009), No. 2, 845–858.

[6] H. P. Zhang, J. J. Li, Z. L. Chen, B. Wang: *A rapid anti-collision method for RFID tag identification.* Applied Mechanics and Materials *738–739* (2015) 1123–1128.

[7] X. Tan, H. Wang, L. Fu, J. Wang, H. Min, D. W. Engls: *Collision detection and signal recovery for UHF RFID systems.* IEEE Transactions on Automation Science and Engineering *PP* (2016), No. 99, 1–12.

[8] D. J. Deng, H. W. Tsao: *Optimal dynamic framed slotted ALOHA based anti-collision algorithm for RFID systems.* Wireless Personal Communications *59* (2011), No. 1, 109–122.

[9] X. Q. Yan, Y. Liu, B. Li, X. M. Liu: *A memoryless binary query tree based successive scheme for passive RFID tag collision resolution.* Information Fusion *22* (2015), 26–38.

[10] H. Safa, W. El-Hajj, C. Meguerditchian: *A distributed multi-channel reader anti-collision algorithm for RFID environments.* Computer Communications *64*, (2015), 44–56.

[11] C. T. Nguyen, A. T. H. Bui, V. D. Nguyen, A. T. Pham: *Modified tree-based identification protocols for solving hidden-tag problem in RFID systems over fading channels.* IET Communications *11* (2017), No. 7, 1132–1142.

[12] S. L. Garfinkel, A. Juels, R. Pappu: *RFID privacy: An overview of problems and proposed solutions.* IEEE Security & Privacy *3* (2005), No. 3, 34–43.

[13] X. Liu, X. Xie, K. Li, B. Xiao, J. Wu, H. Qi, D. Lu: *Fast tracking the population of key tags in large-scale anonymous RFID systems.* IEEE/ACM Transactions on Networking *25* (2017), No. 1, 278–291.

[14] C. Wang, Z. Shi, F. Wu: *An improved particle swarm optimization-based feed-forward neural network combined with RFID sensors to indoor localization.* Information *8* (2017), No. 1, paper 9.

[15] F. Zhu, B. Xiao, J. Liu, L. J. Chen: *Efficient physical-layer unknown tag identification in large-scale RFID systems.* IEEE Transactions on Communications *65* (2017), No. 1, 283–295.

[16] Z. Zhou, L. Shangguan, X. Zheng, L. Yang, Y. Liu: *Design and Implementation of an RFID-based customer shopping behavior mining system.* IEEE/ACM Transactions on Networking *25* (2017), No. 4, 2405–2418.

Received September 12, 2017