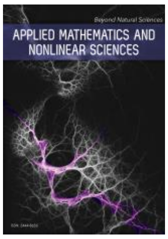
sciendo Applied Mathematics and Nonlinear Sciences, 9(1) (2024) 1-14



Applied Mathematics and Nonlinear Sciences

https://www.sciendo.com

Anti-Collision and Security Protocol of Logistics Warehouse Labels by Integrating RFID and Chaotic Encryption Algorithm

Yunhai Gu[1], Fei Xia[1], Weihua Wang[1], Song Yang[1,†], Yuqiong Ye[1]

1. Information Management Department, Hongta Group Chuxiong Cigarette Factory, Chuxiong, Yunnan, 675000, China.

Submission Info

Communicated by Z. Sabir
Received March 6, 2023
Accepted June 5, 2023
Available online November 25, 2023

Abstract

RFID technology application has made multi label collisions and security privacy issues increasingly prominent in logistics warehousing. A solution that combines RFID and chaotic encryption algorithm has been proposed and applied to anti-collision and security protocols for logistics warehousing labels to address these issues. Firstly, optimization analysis was conducted on the anti-collision of warehouse system labels using chaotic sequences. By comparing different types of labels, it was determined that the 6TypeB label has good anti-collision ability. On this basis, a bidirectional security authentication protocol based on a chaotic encryption algorithm for 6TypeB labels was studied. The data privacy and security of tags can be effectively protected by this protocol. Finally, a detailed analysis was conducted on the performance of 6TypeB logistics warehousing labels used. The 6TypeB system has an average label recognition rate of 73%, an average transmission efficiency of 95.31%, and an average memory usage rate of 93%. Meanwhile, the average stability of the bidirectional security authentication protocol based on the 6TypeB label system is 92.08%. By utilizing 6TypeB, data privacy and security of RFID can be significantly improved, leading to a new application direction for anti-collision and security of logistics warehousing labels.

Keywords: Chaos encryption algorithm; Radio frequency identification technology; Logistics warehousing; Anti collision; Security protocol.
AMS 2010 codes: 05C85

†Corresponding author.
Email address: yangsong90262023@163.com

ISSN 2444-8656
https://doi.org/10.2478/amns.2023.2.01246

1 Introduction

The demand for label information management in the logistics warehousing (LW) industry is increasing with the promotion of IT. With the expansion of the logistics scale, label information collision and data security have become a serious problem [1-2]. In order to solve this problem, many researchers have combined RFID technology with a Chaos encryption algorithm (CEA) to improve the anti-collision ability and data security of 6TypeB label information. RFID technology is capable of tracking and managing items, but in large-scale applications, conflicts and collisions between labels can result in information loss and confusion. In order to solve this problem, the 6TypeB label system has emerged, which reduces the occurrence of collisions by coordinating and separating labels [3-4]. However, this method still cannot completely avoid the occurrence of collisions. Therefore, integrating RFID technology and CEA can help further improve the anti-collision ability and data security of label information. CEA is an encryption technology based on Chaos theory, which has high uncertainty and randomness. By confusing and encrypting chaotic sequence (CS) with label data, the security of label data can be effectively improved.

Meanwhile, the randomness of CS can also be used to adjust the sending time and frequency of labels to avoid collisions [5-6]. The research examines how to utilize RFID technology and CEA to enhance the anti-collision and data security of LW6TypeB label information. By coordinating and encrypting labels, collisions can be reduced, and label data's privacy and security can be safeguarded.

The research first introduces the current status of research on RFID tag technology in the field of tags. Secondly, research was conducted on anti-collision and security protocols based on the 6TypeB label system. Then, the performance of the 6TypeB label system was verified through simulation experiments. Finally, the experimental results were summarized, and the benefits and drawbacks of the research methods were evaluated.

2 Related works

RFID 6B pallet label is a type of label that uses RFID technology to identify and track pallets. It can be utilized extensively in fields like logistics, warehousing, and supply chain management. Many domestic and foreign scholars have studied anti-collision protocols for RFID to prevent label information from colliding in warehouses. Liang X and other scholars proposed a probability-based query tree protocol to reduce information collisions in RFID systems. The protocol consists of an inverse probability function, a total time slot function, and a mapping table.

The recognition efficiency of this protocol is closer to the optimal value, and its performance is superior to other anti-collision protocols [7]. Huang Z et al. found that prior knowledge of the number of labels is crucial for anti-collision protocols in time slot systems. A physical layer algorithm was proposed to detect the number of labels in collision slots based on this. A mean shift algorithm was first used to analyze the scattered signal, and then the algorithm's performance was verified through simulation experiments. The proposed solution is more efficient than the current MAC layer methods in terms of low estimation error with a high SNR range [8]. Wang X's investigation has revealed that RFID can be significantly impacted by collisions with multiple tags. An effective label recognition algorithm - enhanced adaptive tree time slots were proposed by them to address these issues. By performing binary splitting recognition on multiple labels, this method will update the optimal number of labels through an early observation mechanism. This algorithm's system throughput can reach 0.46, which is superior to the existing methods [9]. Kumudham R et al. constructed three selective time slot Aloha anti-collision protocols and analyzed the application effect of RFID in warehouse labels by comparing the anti-collision performance of these three-time slots. The anti-collision protocol that was built has a high practical value in tracking warehouse cargo, as it can display real-time information through mobile programs.

Through research, Li XN discovered that RFID can classify and recognize information labels in LW. Based on this, a recognition (RFID) system was constructed as the main research object, and an automatic identification model for goods in LW was established based on RFID technology. Among 600 stored goods, the RFID system has better performance and stability in the automatic identification of goods in LW, and the experimental results are of great significance [10-11]. A mathematical model with dual objectives was proposed to improve the storage and delivery efficiency of warehouse products. Öztürkoğlu Ö et al. constructed a heuristic algorithm storage channel through the practical application of this mathematical model. This model and heuristic algorithm offer better storage utilization and shorter distances compared to the company's method when two targets have the same weight [12]. Li T et al. proposed a deep learning framework-based detection algorithm to address the identification and positioning of unmanned forklifts and warehouse pallets. By obtaining tray information and data, labels were created and trained in the experiment using a database. The improved tray detection algorithm has an accuracy of 92.7% and a detection speed of 42 frames per second, which can meet the efficiency and accuracy requirements of tray detection during use [13]. Long W et al. found that pallets are a sustainable and cost-effective industry, but due to the limited data information on pallets, it is not easy to achieve large-scale applications. To address this problem, they proposed an end-to-end bidirectional authentication system that utilizes blockchain and IoT technology to transfer data and pallets. Research utilizes labels, positions, and specific objects to achieve pallet rotation. The system provides low bandwidth constraints and a high probability of recovering the full data payload [14].

Overall, RFID plays a very important role in the development of modern LW, but in practical applications, there are still issues such as high costs, limited read and write distances, and privacy security. Therefore, based on the summary of existing technologies, an LW label anti-collision and security protocol based on the 6 Type B label system was constructed, aiming to provide more ideas for the application of the 6 Type B label system.

3 Construction of A Tag Anti-Collision and Security Protocol Model Integrating RFID and CEA

6 Type B label system is a label system that uses Radio Frequency Identification (RFID) technology and can simultaneously read a large number of labels. Anti-collision research is necessary to prevent collisions and interference between labels.

3.1 Anti-Collision Optimization Algorithm for System Tags Integrating RFID and CS

In the LW industry, anti-collision of label information is a very important issue. The application of the 6TypeB label system in warehouse pallet information can prevent various label information collisions during the process of goods entering and leaving the warehouse. The time spent on goods entering and leaving the warehouse can be reduced, and storage efficiency can be improved. When using 6TypeB labels, it is first necessary to determine the type of label used in the 6TypeB label system and the required label information. This information encompasses the name, specifications, quantity, production date, and other relevant details of the product. It is necessary to install hardware devices for the 6TypeB label system on the tray, including readers, antennas, and labels. To ensure accurate label reading, it is important to consider the installation position of the reader and antenna to maximize signal coverage. The programming tool of the 6TypeB label system was used to program and configure the label, which allows for setting the unique number, storage space, read and write permissions, etc. of the label. In addition, labels can also be associated with product information.

Then, mark the location of the electronic label on the tray and use glue or other fixing methods to fix the label on a tray, ensuring that the label position is fixed and not easy to falls off. Finally, before the system officially runs, it is necessary to test and calibrate the 6TypeB label system [15-16]. The testing mainly involves evaluating the label's reading and writing functions, reading range, and accuracy. Integrating RFID and CS using 6TypeB tags can be used for further research on tag anti-collision. The anti-collision structure of the 6TypeB label system can be seen in Figure 1.

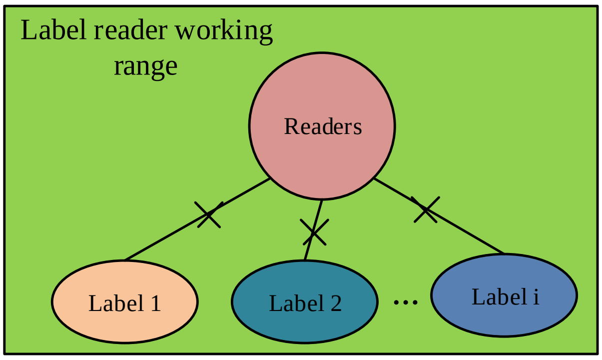


Figure 1. 6TypeB tagging system anti-collision structure diagram

In the operation of the warehouse label system, when the value of the time slot counter is equal to the time slot value selected inside the label, this label will respond to the inquiry request command issued by the reader. If the tag is successfully recognized, the reader will send a command requesting the tag to exit the current RFID communication system. However, if the value of the slot counter is not equal to the randomly selected slot value, it indicates a communication failure between the reader and the tag. The tag randomly selects a time slot to send a response in a frame number. The selection process is completely random, resulting in no fixed rules to follow for labels. Therefore, neither readers nor other devices can predict when the tag will send a response. The security and reliability of RFID communication systems are enhanced by this random selection method. By randomly selecting time slots, communication conflicts and interference can be reduced, thereby improving the overall performance and efficiency of the system. In addition, randomly selecting time slots can also prevent potential attackers from predicting the behavior of tags and increase the system's anti-interference ability. To select the same time slot probability for multiple labels in the 6TypeB label, formula (1) can be used to represent it.

$$B_{N,1/F}(r) = N(\frac{1}{F})^{r}(1-\frac{1}{F})^{N-r} \tag{1}$$

In formula (1), F stands for the number of time slots in the label. N stands for the number of tags within the recognition range of the tag reader. r stands for the probability value of the same time slot corresponding to the selected label. When the tag reader completes a long period of recognition for a frame, the random probability of selecting a tag with just one time slot can be calculated using formula (2).

$$a^{F,N} = F \cdot B_{N,1/F}(r) = N(1-\frac{1}{F})^{N-1} \tag{2}$$

At this point, the system throughput rate of 6TypeB label can be calculated, indicating that the selected label has been successfully recognized. The system throughput is calculated using formula (3).

$$S = \left(\frac{N}{F} - \frac{N}{F^2}\right)^{N-1} \tag{3}$$

By taking the derivative of the system throughput, formula (4) can be obtained.

$$\frac{dS}{dN} = \frac{1}{F}\left(1-\frac{1}{F}\right)^{N-1}\left[1+N\ln\left(1-\frac{1}{F}\right)\right] \tag{4}$$

In formula (4), dS stands for the number of successful time slots. dN stands for the total length of the time slot. If $\frac{dS}{dN}$=0 in formula (4), the relationship between N and F can be calculated, which can be represented by formula (5).

$$N = \left[-\frac{1}{\ln\left(1-\frac{1}{F}\right)}\right] \tag{5}$$

If RFID system in label system reaches the maximum label recognition rate and labels number is also large, the connection between N and F can be further calculated, which can be represented by formula (6).

$$F = \frac{1+1/N}{1+(1/N-1)} \approx N \tag{6}$$

When $F = N$, tag recognition rate obtained by fusing RFID and CS on the basis of 6TypeB tags reaches the maximum value. At this point, the maximum value can be represented by formula (7).

$$A = \lim_{N\to\infty}(1-1/N)^{N-1} \tag{7}$$

From the above analysis, CS is a random and unpredictable sequence that can be used to generate unique identifiers. A CS generator was designed in the experiment to ensure that each label has a unique identifier during the communication process. A new identifier can be generated by combining RFID and CS. This fusion enables the identifier to be transmitted to the reading device during the communication process, which can decompose the fused identifier into RFID identification column identifiers through a decryption algorithm. When multiple labels transmit identifiers simultaneously, the reading device can determine whether they are the same label by comparing the CS part of the identifier. If the CS part is the same, it indicates that a collision may have occurred, and the reading device can send a feedback signal to the label requesting it to resend the identifier. By integrating RFID and CS, the security and reliability of the system can be enhanced by anti-collision of label information, ensuring that each label can be transmitted and recognized normally. The warehouse's operation status and inventory information can be determined by analyzing the data uploaded by the labeling system. Based on these analysis results, the layout and logistics process of the warehouse can be optimized to improve the operational efficiency and management level of the warehouse. Figure 2 shows the anti-collision process of integrating RFID and CS tags using the 6TypeB tag.

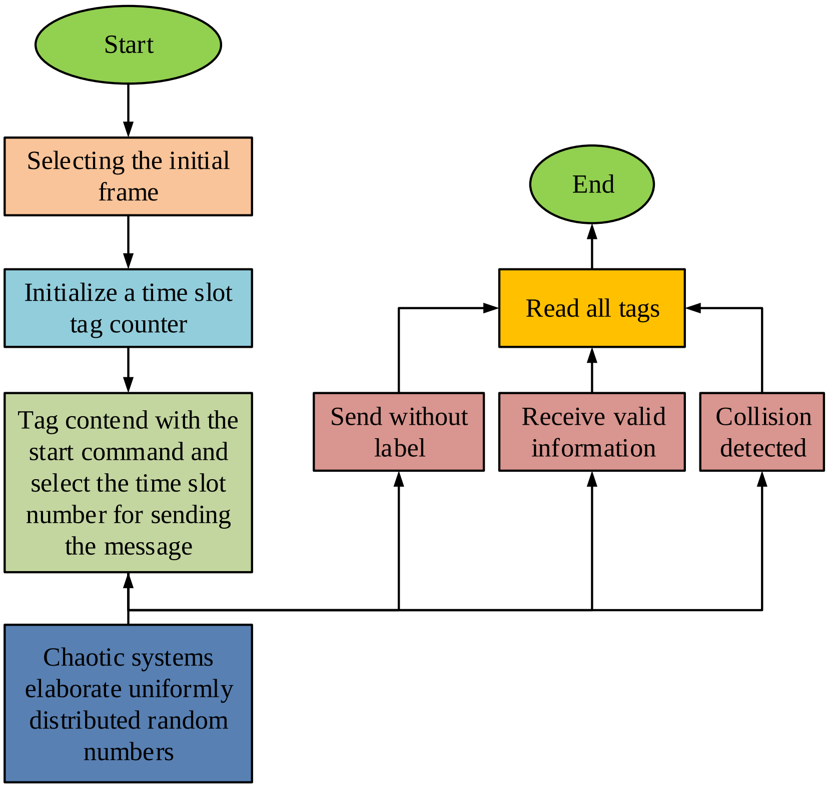


Figure 2. 6TypeB tag based on the fusion of RFID and chaotic sequence tag anti-collision flow chart

3.2 Bidirectional Security Authentication Protocol Integrating RFID and CEA

The 6TypeB standard protocol provides a variety of security mechanisms for data security during communication, including authentication, data encryption, and data integrity checks. Through these mechanisms, it can be ensured that unauthorized third parties do not obtain data during the communication process, and it can be verified whether the data has been tampered with during transmission. Identity verification is a mechanism that ensures communication security and ensures that only genuine readers and integrated circuit cards are able to communicate. Data encryption is a crucial method for safeguarding data security. Encrypting data during communication can prevent unauthorized third parties from stealing it. This way, even if the data is stolen, unauthorized third parties cannot decrypt it, protecting the confidentiality of the data. To confirm if data has been tampered with, a data integrity check is a mechanism. Data transmission can result in data being tampered with. Through the data integrity check mechanism, it can verify whether the data has been tampered with during the transmission process. If the data has been tampered with, the system can detect it and take necessary measures to ensure the integrity of the data.

The study of integrating RFID and CEA for bidirectional security authentication protocol was proposed by researchers to further investigate the security of the 6TypeB label system. Bidirectional authentication involves mutual identification between tags and readers. During this process, a single random key is employed for encryption, with each key being used only once. This encryption scheme is regarded as an ideal and unbreakable encryption method. By using bidirectional authentication between tags and readers and one-time encryption, both user privacy and tag cloning issues can be addressed simultaneously. Through the above security mechanisms, the 6TypeB standard protocol can effectively protect data security during communication. Authentication, data encryption, Data integrity check and other mechanisms can ensure that unauthorized third parties do not obtain the data in the communication process and can verify whether the data has been tampered with in the transmission process. The bidirectional security authentication protocol that incorporates RFID and CEA can enhance the security of the system by addressing user privacy and label cloning issues. Figure 3 shows the bidirectional authentication process based on the 6TypeB label system.

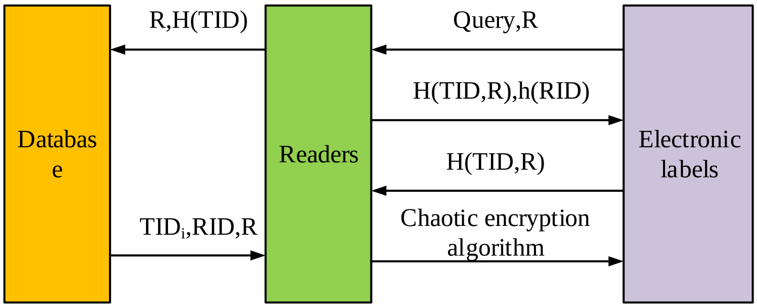


Figure 3. Flow chart of two-way authentication based on 6TypeB tagging system

This study utilizes the unique identifier of the RFID system itself as a key value for chaotic system encryption to study the security of the 6TypeB label system. At this point, it is assumed that the tag, reader, and random number are all 16-bit binary numbers composed of [0,1]. If they are not 16-bit binary numbers, they can also be calculated using the real number calculation method in chaotic systems. The calculation factor of real numbers in chaotic systems can be calculated using the formula (8).

$$\frac{x_0}{TID * RID} = 1.525 * 10^{-5} \tag{8}$$

In formula (8), x_0 stands for the initial value of the chaotic coefficient. TID stands for labels number. RID is the corresponding value for reader. Figure 4 shows the process of integrating CEA.

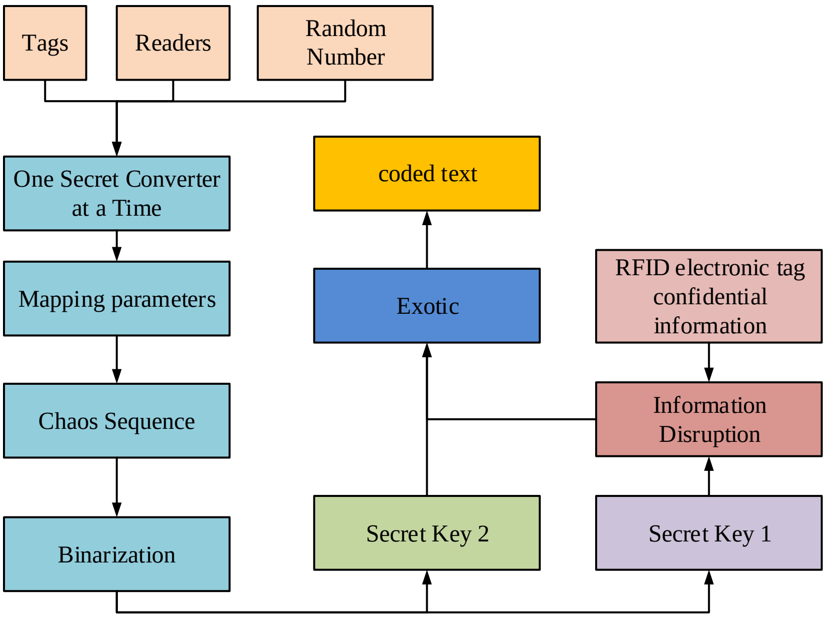


Figure 4. Flow chart of fusing RFID with chaotic encryption algorithm

After obtaining chaotic coefficients, it is necessary to analyze the randomness and independence of the sequence. The randomness and independence of sequences are both prerequisites and foundations for ensuring the security of encryption algorithms. Firstly, it is necessary to test the frequency of the

6TypeB label system. Assuming that the sequence is randomly distributed, it can be represented by formula (9).

$$S_i = \sum_{1}^{i} x_1 + x_2 + \cdots + x_i \tag{9}$$

In formula (9), x_i stands for each numerical value participating in the statistics in the sequence. On this basis, the statistical values of the random distribution can be calculated using formula (10).

$$V = \frac{|S_i|}{\sqrt{t}} \tag{10}$$

In formula (10), t stands for the statistical number in the binary sequence. Using run test to determine the randomness in data, assuming that the sequence used is independently distributed, the corresponding mean can be represented by formula (11).

$$E(r) = \frac{2n_1 n_2}{n_1 + n_2} \tag{11}$$

In formula (11), n_1 stands for the number of means that subtract from binary sequence value to negative. n_2 stands for the number of means that subtract from a binary sequence value to be positive. The variance at this point can be represented by formula (12).

$$Zr = \frac{r - E(r)}{\sqrt{D(r)}} \tag{12}$$

In formula (12), $D(r)$ stands for a variance value. According to the significance level judgment criterion, the research has previously set the assumption that the sequence is independently distributed. To further verify the randomness and mutual independence of CS, the study also carried out a series of tests, including intra-group frequency test, maximum run test, Discrete Fourier transform test, CUSUM test, random offset test, etc. Through a series of tests, research has verified the randomness and mutual independence of CS. Therefore, the 6TypeB label system can be applied to encrypt and scramble confidential data. This will provide certain guarantees for the security of data and prevent data leakage and unauthorized access. In summary, Figure 5 shows the process of integrating RFID and CEA bidirectional security authentication protocols based on 6TypeB standard protocol.

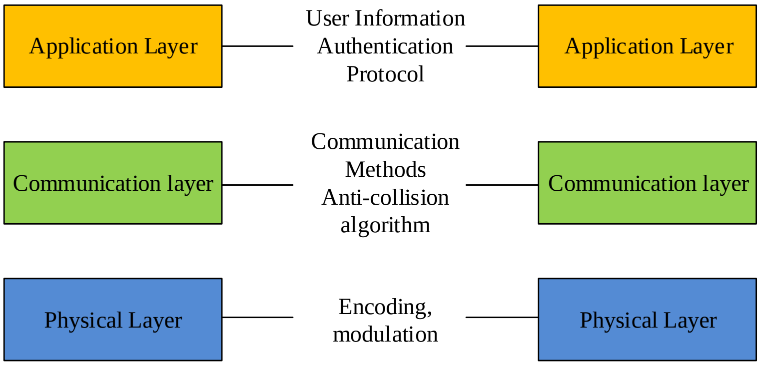


Figure 5. Two-way security authentication protocol structure based on the existing 6TypeB standard protocol

4 Application Analysis of Tag Based-Anti-Collision and Bidirectional Security Protocol

to verify the anti-collision performance of the 6TypeB label. This study analyzed the time gap, label recognition efficiency, and label storage capacity. Different authentication protocols are also used to verify the performance of the 6TypeB tag.

4.1 Analysis of the Application Performance of 6 Type B Label for Collision Prevention

To verify the 6TypeB label's performance in terms of the time slot number occupied by each label, this study compared it with traditional label methods. Different frame lengths were taken in the experiment, and Figure 6 shows the comparison results.

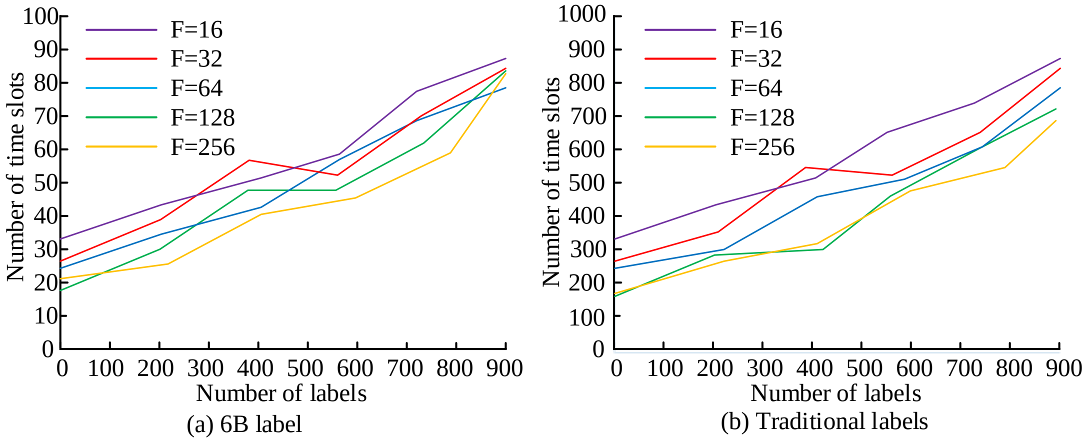


Figure 6. Comparison of frame length test results of two different labeling methods

Compared with Figure 6 (a) and (b), in the 6TypeB method and traditional label method, as frame length increases, the time required for the number of time slots continues to increase. In the case of the same frame length, the time required for 6TypeB labels to recognize label numbers is shorter, and traditional label methods will greatly increase the time required to recognize the same label number. This indicates that 6TypeB has significant advantages in terms of time consumption and recognition ability compared to traditional labeling methods. This study examined the anti-collision rate and recognition ability of two methods in label recognition by comparing them separately in Figure 7.

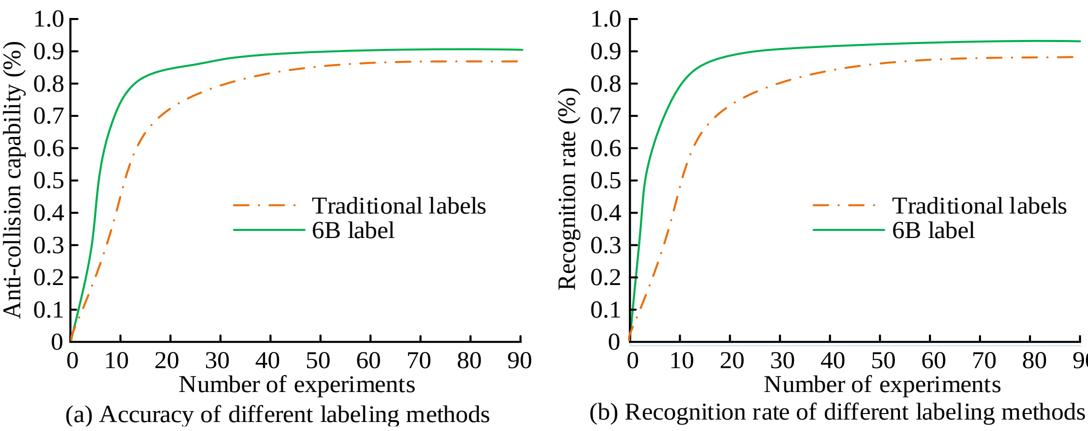


Figure 7. Comparison results of anti-collision rate and recognition rate of two labeling methods

According to Figure 7 (a), both labeling methods have good anti-collision capabilities, with an average of 91.03% for 6TypeB and 83.67% for traditional labels. According to Figure 7 (b), under the same number of labels, 6TypeB label has stronger information recognition ability, with an average recognition rate of 92.84%, while the average information recognition rate of traditional label methods is 81.36%. This indicates that the 6TypeB tag has stronger collision prevention ability and better recognition ability. To further verify the anti-collision ability of 6TypeB, the throughput of 6TypeB system was tested. Comparative indicators were chosen from different frame lengths in the experiment. Figure 8 shows the throughput comparison results of the 6TypeB system under different frame lengths.

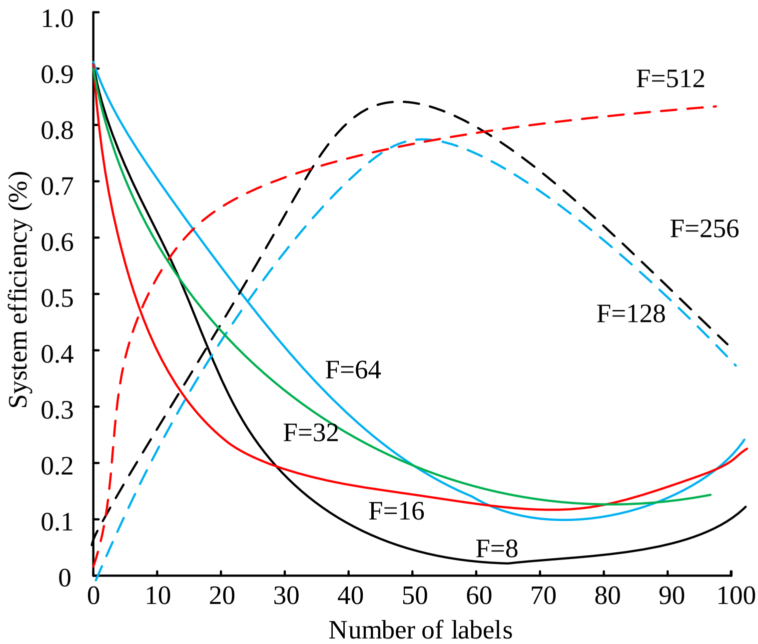
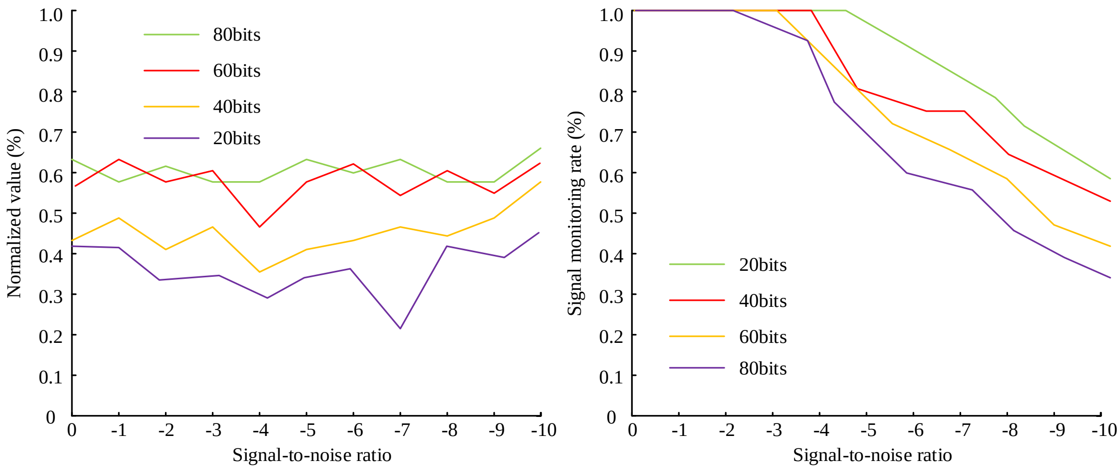


Figure 8. Throughput comparison results of 6TypeB system with different frame lengths

In Figure 8, as frame length increases, the label recognition rate of the 6TypeB system maintains an average of around 73%. When the frame length value is 8-16, the maximum efficiency of system label recognition is greater than 40%. The reason for this situation is that the generation of random numbers leads to the selection of time slot labels, which reduces the probability of collisions and reduces idle gap numbers. In other frame lengths, the efficiency of the 6TypeB system has been improved based on traditional labeling methods.

4.2 Performance Analysis of Bidirectional Security Authentication Protocol Based on 6 Type B Labels

To verify the encoding length, normalization, and signal monitoring rate of the 6 Type B label under different signal-to-noise ratios, the threshold was set to 0.7 at different signal-to-noise ratios (SNRs). Figure 9 shows the comparison results of different signal-to-noise ratios.



(a) The relationship between coding length and normalized value for different signal-to-noise ratios

(b) Coding length versus signal detection speed for different signal-to-noise ratios

Figure 9. Results of normalized values versus signal detection speed at different signal-to-noise ratios

According to Figure 9 (a), under different SNRs, the frame length is longer, and its correlation value is larger. An increase in the SNR value leads to an increase in its normalized value. The normalized average values of 20-80bits are 0.39, 0.42, 0.53, and 0.59, respectively. According to Figure 9 (b), the detection rate of signals with different encoding lengths shows a decreasing trend under different SNRs. The fastest decline is at 80 bits, while the slowest is at 20 bits. The probability of label signals being successfully detected is significantly correlated with SNR and encoding length, as indicated. As the SNR and encoding length increase, the accuracy of their correlation values increases, leading to an increase in the probability of successfully detecting the signal. To verify the anti-interference ability of the bidirectional security authentication protocol based on the 6TypeB label system, the random protocol and Hash lock protocol were compared with the constructed authentication protocol. Figure 10 shows the results of the anti-interference comparison.

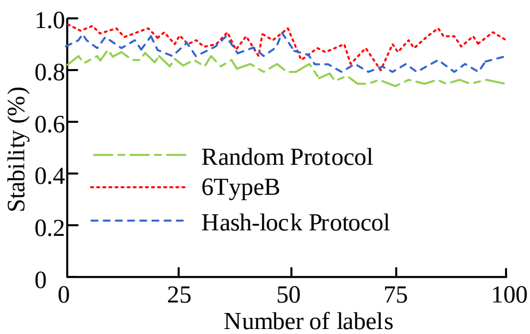


Figure 10. Comparison results of tagging system stability under different authentication protocols

The stability of the three authentication protocols fluctuates to varying degrees when labels are added in Figure 10. The strongest anti-interference capability is based on the bidirectional security authentication protocol of the 6TypeB label system, with an average stability value of 92.08%. The Hash lock protocol has an average stability value of 87.26%. The average stability value of the random protocol is 80.26%. The bidirectional security authentication protocol based on the 6TypeB label system has strong anti-interference ability and certain research value, as indicated by this. To better demonstrate the performance of the 6TypeB label system, simulation experiments were conducted on the 6TypeB label using attack datasets. These datasets were utilized to verify its transmission efficiency performance in Figure 11.

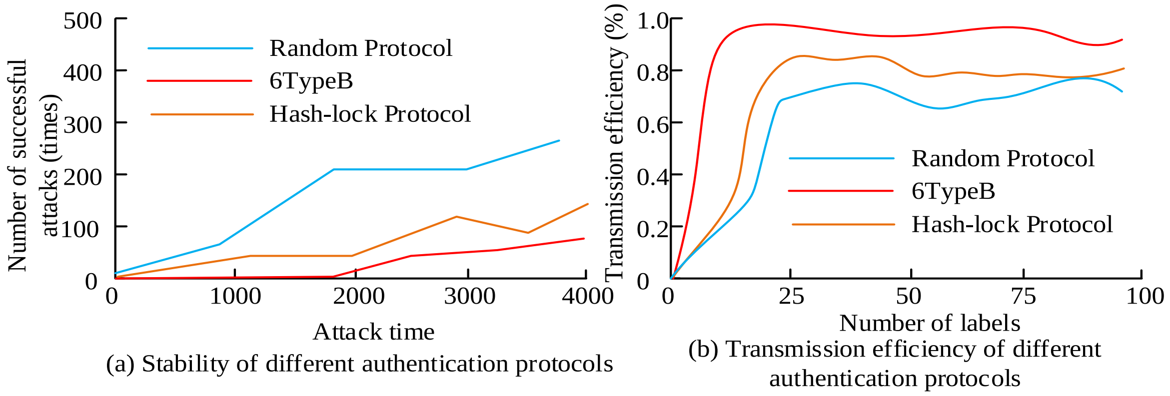


Figure 11. Comparison results of stability and transmission efficiency of different authentication protocols

In Figure 11 (a), as attack time in the dataset increases, successful attacks number also increase. The random protocol has the highest number of successful attacks, followed by the hash lock protocol. 6TypeB appears to be successfully attacked when the attack time is 1873 seconds. Compared to the other two, it has a strong anti-attack capability and high-security performance. As the number of labels in the dataset increases, the transmission efficiency of the three protocols also increases, as shown in Figure 11 (b). Out of these, 6TypeB has an average transmission efficiency of 95.31%, Hash lock protocol has an average transmission efficiency of 80.66%, and random protocol has an average transmission efficiency of 72.91%. It can be concluded that 6TypeB has both high-security performance and good transmission efficiency. To verify the storage performance of the 6TypeB tag, this study used the memory and storage utilization required by three protocols as comparison indicators to determine the performance of different tags in Figure 12.

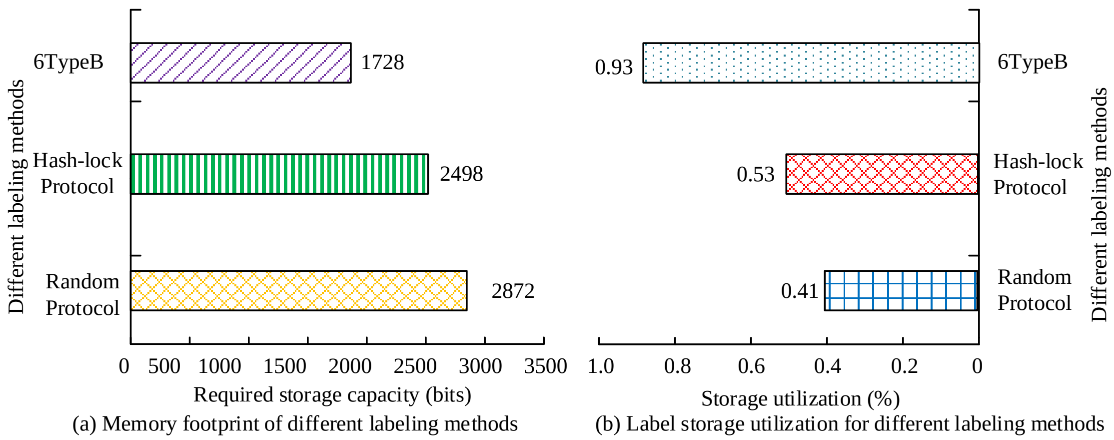


Figure 12. Comparison of memory footprint and utilization results for different labeling methods

According to Figure 12 (a), the memory required for the three labeling methods is the same. The memory required for 6TypeB is 1728 bits, while the memory required for the Hash Lock Protocol and Random Protocol is 2498 and 2872 bits, respectively. According to Figure 12 (b), the memory usage rate of 6TypeB is as high as 0.93, while the memory usage rates of the Hash lock protocol and random protocol are 0.53 and 0.41, which are significantly lower than the usage rate of 6TypeB. This indicates that 6TypeB has better application performance because it requires less memory and can reduce storage costs while also having higher memory utilization, saving costs and effectively utilizing existing configurations.

5 Conclusion

To address the collision and security issues of tray label information in the LW system, a solution for collision prevention and security protocol of 6TypeB label information data in LW has been proposed. The initial investigation focuses on the anti-collision of label information based on the 6TypeB label. Then, a more in-depth study was conducted on the security of the 6TypeB label system, and a bidirectional security authentication protocol was studied by integrating RFID and CEA. Finally, simulation experiments were used to verify the relevant performance of the 6TypeB tag. 6TypeB has an average anti-collision capacity of 91.03% and an average recognition rate of label recognition information of 92.84%. The bidirectional security authentication protocol of the 6TypeB label system has an average stability of 92.08%. This indicates that the 6TypeB tags application can improve tag information processing efficiency in LW, and the implementation cost of this scheme is relatively low, making it suitable for large-scale LW systems. However, there remains a lack of clarity in this study, and there is still room for improvement in the reading distance and speed of warehouse label information. By combining RFID technology with the next step, label information transmission capacity can be further optimized. Through technological upgrades and improvements, the processing efficiency and security of label information in LW systems can be further improved.

References

[1] Dong, G., Zhang, W., Xuan, S., Qin, F., Tan, H. (2020). An Improved Binary Search Anti-Collision Protocol for RFID Tag Identification. Computers, Materials & Continua, 65(2):1855-186.

[2] Pal, K. (2019). Algorithmic solutions for RFID tag anti-collision problem in supply chain management. Procedia Computer Science, 151(2): 929-934.

[3] Huang, Z., Su, J., Wen, G., Zheng, W., Chu, C., Zhang, Y. (2019). A Physical Layer Algorithm for Estimation of Number of Tags in UHF RFID Anti-Collision Design. Computers, Materials & Continua, 61(1):399-408.

[4] Wei, S., Zhang, X., Xue, W. (2019). RFID Anti-Collision Algorithm Based on Tag Best Response Probability Estimation//BASIC & CLINICAL PHARMACOLOGY & TOXICOLOGY. 111 RIVER ST, HOBOKEN 07030-5774, NJ USA: WILEY, 124: 317-317.

[5] Huang, Z., Ma, H., Wang, S., Shen, Yl. (2021). Accurate Item Recommendation Algorithm of itemrank based on tag and context information. Computer Communications, 176(3): 282-289.

[6] Nath, S., Som, S., Negi, M. C. (2021). Cryptanalysis of a novel bitwise xor rotational algorithm and security for iot devices. International Journal of Knowledge-based and Intelligent Engineering Systems, 25(1): 139-147.

[7] Liang, X., Guo, Y. (2019). A probability-based anti-collision protocol for RFID tag identification. Wireless Personal Communications, 107(1): 57-79.

[8] Huang, Z., Su, J., Wen, G., Zheng, W., Chu, C., Zhang, Y., Zhang, Y. (2019). A Physical Layer Algorithm for Estimation of Number of Tags in UHF RFID Anti-Collision Design. Computers, Materials & Continua, 61(1):399-408

[9] Wang, X., Zhang, M,. Lu, Z. (2019). A Frame Breaking Based Hybrid Algorithm for UHF RFID Anti-Collision. Computers, Materials & Continua, 59(3):873-883

[10] Kumudham, R., Ganesh, E. N., Rajendran, V. (2020). Testing anti-collision algorithm for tracking purpose using RFID in IOT technology. Journal of Critical Reviews, 7(15): 4587-4592.

[11] Li, X. N. (2020). Automatic identification management of goods in warehouse logistics based on RFID technology. Telecommunications and Radio Engineering, 79(13):1167-1176

[12] Öztürkoğlu, Ö. (2020). A bi-objective mathematical model for product allocation in block stacking warehouses. International Transactions in Operational Research, 27(4): 2184-2210.

[13] Li, T., Huang, B., Li, C., Huang, M. (2019). Application of convolution neural network object detection algorithm in logistics warehouse. the Journal of Engineering, 2019(23): 9053-9058.

[14] Long, W., Wu, C. H., Tsang, Y. P., Chen, Q. (2021). An end-to-end bidirectional authentication system for pallet pooling management through blockchain internet of things (BIoT). Journal of Organizational and End User Computing (JOEUC), 33(6): 1-25.

[15] Saderova, J., Rosova, A., Sofranko, M., Kacmary, P. (2021). Example of warehouse system design based on the principle of logistics. Sustainability, 13(8): 44-58.

[16] Setiawan, A., Kristina, L. R., Kurniawan, R. C. (2021). THE ALGORITHM OF GOOD PLACEMENT ON THE SHELF BY CONSIDERING THE WEIGHT AND VOLUME OF THE GOODS TO THE CENTRE OF MASS. Journal of Industrial Engineering Management, 21(6): 208-217.

[17] Hale, B. (2020). User-mediated authentication protocols and unforgeability in key collision. International Journal of Information Security, 19(6): 609-621.

[18] Wang, C., Shao, X., Meng, Y., Gao, J. (2021). A physical layer network coding based tag anti-collision algorithm for RFID system. Computers Materials & Continua, 66(1): 931-945.

[19] Baha'A, A., Thompson, D. R., Alma'aitah, A., Jia, D. (2022). Using dummy data for RFID tag and reader authentication. Digital Communications and Networks, 8(5): 804-813.

[20] Raghib, A., Majd, B. A. E. (2019). Hierarchical multiobjective approach for optimising RFID reader deployment. International Journal of Mathematical Modelling and Numerical Optimisation, 9(1):70-88.

About the Author

Yunhai Gu was born in Chuxiong, Yunnan, P.R. China, in 1982. He obtained a Master's degree from Hefei University of Technology in China. Mr. Gu is currently working at Hongta Group Chuxiong Cigarette Factory. His main research direction is Information management.

Fei Xia was born in Honghe, Yunnan, China, in 1983. He received his bachelor's degree from Kunming University of Science and Technology in China. Mr. Xia is currently working at Hongta Group Chuxiong Cigarette Factory. His main research direction is Information management.

Weihua Wang was born in Chuxiong, Yunnan, P.R. China, in 1976. He obtained a Master's degree from Kunming University of Science and Technology in China. Mr. Wang is currently working at Hongta Group Chuxiong Cigarette Factory. His main research direction is Information management.

Song Yang was born in Mouding, Yunnan, P.R. China, in 1974. He obtained a master's degree from Kunming University of Science and Technology in China. Mr. Yang is currently working at Hongta Group Chuxiong Cigarette Factory. His main research direction is Network and Network Security.

Yuqiong Ye was born in Chuxiong, Yunnan, P.R. China, in 1984. She obtained a bachelor's degree from Kunming University of Science and Technology in China. Ms. Ye is currently working at Hongta Group Chuxiong Cigarette Factory. Her main research direction is Information management.