Implementation of a lightweight RFID security authentication protocol system

Ying Zheng¹,*, Mi Zou¹,*, Guobo Hu²

¹Center for Computer Fundamental Education, Jilin University, Changchun 130012, China
²College of Computer Science and Technology, Jilin University, Changchun 130012, China

*Corresponding author e-mail: zhengying@jlu.edu.cn, zoumi@jlu.edu.cn

Abstract. RFID technology is particularly important for the security certification of its system due to the limitations of its own resources. This paper designs and implements an RFID system experimental platform consisting of programmable tags, readers and servers and application software. At the same time, a secure authentication protocol based on one-way hash function and static ID mechanism is proposed. The protocol applies to system performance requirements and security requirements. The results show that the protocol can effectively solve security problems such as eavesdropping, replay attacks, and loss of synchronization. This system helps protocol designers analyze and compare the security protocols of RFID systems, and at the same time fills the gaps in experimental systems in this field.

1. Introduction

RFID technology has been noticed since its introduction, and it is known as one of the top ten technologies in the 21st century. Today, RFID systems have a wide range of applications in today's production and life. However, due to its own characteristics, RFID technology has many hidden dangers in terms of security [1]. Many of these security risks can cause the entire system to paralyze and crash. Research on the security of RFID systems is always one of the most important research directions [2]. This system is a simulation platform built in the laboratory, mainly for the simulation and implementation of data encryption methods during the transmission of lightweight RFID systems. Through this experimental platform, students can directly see the data flow and encryption of the RFID system during transmission. By simulating a newly designed system authentication protocol, the system completed the entire process from system construction, system setup to system application. The application of this experimental platform can better help students understand the working principle and workflow of RFID systems, and also help students design encryption authentication algorithms suitable for RFID systems at all levels.

The application scope of this platform is data encryption based on a hash function, the tag calculation is lightweight, and the tag ID is a static ID. The connection method between the reader and the back-end server is wired and secure channel connection. This system environment has the widest applicable range, the experimental results are the best, and the experimental results are the most intuitive.
2. Composition of lightweight RFID system

2.1. Tags
A tag is a data carrier encapsulated by a chip. It is an electronic device used to exchange data with a reader in an RFID system. Tags generally have a certain amount of storage and computing power [3]. The larger the memory, the higher the computing power and the higher the level of the RFID system. In addition, the tag's working frequency, energy supply and extraction methods, and read / write performance are also important technical indicators.

This system uses a programmable chip card for the label. A single-chip wireless transceiver working in the 2.4-2.5GHz universal ISM frequency band is used. The so-called lightweight system, that is, the tag's storage and calculation capabilities is relatively weak, and it cannot afford a large number of calculation and data transmission tasks. This type of label is the most widely used and relatively inexpensive. The advantage of using such a tag is that it can better prove the security of a lightweight RFID system, and it is also an important part of the system. Since the system is lightweight, the calculations involved in the tag are low-bit hash encryption and bit operations.

2.2. Reader
The reader is the core component of the RFID system and the most complex component in the RFID system. The reader interacts with the tag through the antenna and interconnects with the back-end server through wired or wireless [4]. As a relay station for information interaction in the system, the performance of the reader is the key to determining whether the system is excellent. In general, while we require readers to have certain computing and storage capabilities, we also need to display data.

The reader used in this system is the most basic handheld programmable reader. This reader has comprehensive functions, moderate storage and calculation functions, and plays a good role in data transfer in lightweight RFID systems. This system pays more attention to the security of direct data transmission between the tag and the reader, so the connection between the reader and the background server uses a wired connection. This can greatly improve the security of the entire system and also solve the data transmission Out of sync issue.

2.3. Background server and software system
In general, we usually set the back-end server as a generalized database system. It has a considerable amount of data storage and high computing speed. Much higher in data calculation and response than tags and readers. It is mainly responsible for calculating and storing the data of the tag [5]. Can also archive and trace system data. The composition of this system is shown in Figure 1.

![System composition diagram](image-url)
The background server of this system is served by a common high-performance PC. Use Mysql database to record data. The protocol analysis software is developed based on the Visual Studio platform and C# programming language, which simulates the authentication process of the system, so as to analyze the system security issues more intuitively. The software uses encryption simulation to encrypt the data, and uses MD5 encryption algorithm to simulate the hash function. Use the Random class to generate pseudo-random numbers. Use operation classes to perform bit operations in the protocol. Because the system is based on lightweight operations, we use only sixteen-bit raw data in the software. The data width of the system is also set to sixteen bits. The main function of the software is to identify the tags and reader identifiers, and to display the calculation process of the tags, readers and back-end servers. The server-side protocol authentication software function module is shown in Figure 2.

![Software System Function Module Diagram](image)

**Figure 2.** Software system function module diagram

3. System security certification methods

3.1. Definition

The symbols involved in the agreement are as follows:

- $R_T$: One-time random number generated by the label
- $R_R$: A one-time random number generated by the reader
- ID: Tag identification value
- $\oplus$: XOR operator
- $\|$: Concatenation operator

Condition setting:

1. ID is the identification of the label itself, and the ID of each label is unique and unchanged during the entire label existence authentication process.
2. Tags are low-energy, meaning they only have low storage and computing power.
3. The channel between the tag and the reader, the reader and the background server are all insecure channels.
4. The background server stores an index table of all tag IDs. That is, a valid label must store its ID value in the server before authentication, otherwise it is an illegal label.
5. Compared with tags, the computing and storage capabilities of the background server are powerful.
3.2. Protocol authentication process

Assuming the following is the i + 1 round of authentication, the process is as follows:

1. The reader generates a one-time random \( R_B \) and sends it to the tag.

2. The label generates a one-time random number \( R_T \) and calculate \( M_1 = H(ID \| R_B \!\! \| R_T) \); \( M_2 = H(M_1 \oplus R_T) \+ ID \); Send \( M_1, M_2, R_B, R_T \) to the reader and forward to the background server.

3. Background server computing \( ID = M_2 \oplus H(M_1 \oplus R_T) \); If \( ID = ID' \) exists, the verification label is a legal one, otherwise the authentication fails.

4. Background server computing \( M_3 = H(ID \| R_T) \). If \( ID = ID' \) exists, the verification label is a legal one, otherwise the authentication fails.

5. Label calculation \( M_4 = H(ID \| R_T) \); If \( M_4 = M_3 \) then the tag verification server succeeds, if not equal then verification fails.

The protocol flowchart is shown in Figure 3:

![Figure 3. Protocol execution process](image)

By deploying the protocol on the system, you can see the execution process of the protocol through the software on the background server. Through analysis and comparison of the displayed execution process, the advantages and disadvantages of the protocol can be seen more intuitively. The RFID authentication protocol tag based on the static ID mechanism proposed in this paper only needs to generate a random number and three one-way hash function operations. Since the calculation and storage performance of the background server and the RFID reader is far greater than the calculation and storage performance of the tag, for RFID systems with low energy consumption requirements, the tag’s calculation amount is the real bottleneck of the security authentication protocol. The RFID security authentication protocol based on the static ID mechanism proposed in this paper comprehensively analyzes the calculation amount of the RFID tag and the security performance of the system, and
achieves a good balance between the low cost of the tag and the security of the RFID system. Figure 4 shows the operation of the system software after the protocol design is completed.

4. Conclusion

The main function of the experimental platform designed in this paper is to realize the visibility of the information encryption algorithm of the RFID system during data transmission. Through this experimental platform, students can better understand the RFID system data from the physical layer to the data layer interaction process. This paper also proposes an RFID security authentication protocol based on the static ID mechanism. Through the deployment of the protocol on the experimental platform, the system information encryption process is completed. Through several trials of experimental teaching, the application of the experimental platform has a good effect on the experimental teaching of RFID system.

References:
[1] Desynchronization attack on RAPP ultralightweight authentication protocol[J]. Zahra Ahmadian, Mahmoud Salmassizadeh, Mohammad Reza Aref. Information Processing Letters. 2013 (7)
[2] Tag-ordering polling protocols in RFID systems[J]. Yan Qiao, Shigang Chen, Tao Li, Shiping Chen. IEEE/ACM Transactions on Networking (TON). 2016 (3)
[3] AKF: A key alternating Feistel scheme for lightweight cipher designs[J]. F. Karako?, H. Demirci, A.E. Harmanc?. Information Processing Letters. 2014
[4] Fast Tracking the Population of Key Tags in Large-Scale Anonymous RFID Systems[J]. Xiulong Liu, Xin Xie, Keqiu Li, Bin Xiao, Jie Wu, Heng Qi, Dawei Lu. IEEE/ACM Transactions on Networking (TON). 2017 (1)
[5] Rapid structural condition assessment using radio frequency identification (RFID) based wireless strain sensor[J]. Yunfeng Zhang, Linjia Bai. Automation in Construction. 2015