

Design of Information Security System Based on RFID

Zhang Hua

Department of Information Engineering, Guangzhou Institute of Railway Technology,
Guangdong Guangzhou 510430, China

Received: 30 November 2013 /Accepted: 22 December 2013 /Published: 30 December 2013

Abstract: With the wide application radio frequency identification (RFID) technology, RFID technology will become the most widely used radio-technology since phone appeared. However, the security risks come into being. The growing number of businesses and users worry about the security and privacy protection issues of RFID system. In this paper, we analyze the RFID system security risks in detail and summarize some related countermeasures. According to these, we design a kind of information security system based on RFID, in which we do some researches on security mechanisms and security protocols of RFID system. Finally, we build a safety assessment model of the system which provides safety support for RFID system. *Copyright © 2013 IFSA.*

Keywords: RFID, Information security, Security assessment model, Safety mechanism.

1. Introduction

The radio frequency identification (RFID) system uses wireless radio frequency technology to identify objects in the open system environment. One of the advantages of such identification is without physical contact, or any other visible contact. Nowadays, RFID system has been regarded as an effective technology for pervasive computing environment [1]. RFID technology, combined with the Internet, communication technology and so on, is widely used, which can implement worldwide object tracking and information sharing. RFID technology can be used in logistics, manufacturing, and public information service, which can significantly improve the management and operational efficiency and reduce costs. With the enhancement and perfection of the related technology, the RFID industry not only becomes a new growth point of national economy and newly developing high-technology, but also listed as national research hot-spot and research focus.

However, with the development and application of RFID technology, the security problems of RFID system are gradually revealed and have attracted people's attention. Currently, RFID information security caused the concerns all over the world. With the world's efforts, the aspects of technical research, system development, product testing, standard formulating and so forth have made positive progress. In order to verify and ensure the safety of the RFID system, RFID system and evaluation technologies are also gradually aroused the attention of researchers [2].

In this paper, we mainly discuss the RFID system and its information safety model. Firstly, the conception and background of RFID system and information security are studied. Then, the security mechanism and safety evaluation model based on RFID system are researched, including the designs of information security protocols and security evaluation model. Finally, conclusions that the effects of the information security system can be implemented are made.

2. The Brief Introduction of RFID System and Information Security

RFID technology, also called electronic tag, is a communication technology that can identify a specific target, read and write related data by radio signals without establishing mechanical or optical contact between recognition systems and specific objectives. Generally, RFID system uses low frequency (125 K~134.2 kHz), high frequency (13.56 MHz), ultra-high frequency, passive technology and so on [3].

2.1. The Construction and Characteristic of RFID System [4]

RFID technology is an automatic identification technology that began to rise in the 1990s. First we talk about the operation principle of RFID shown in Fig. 1.

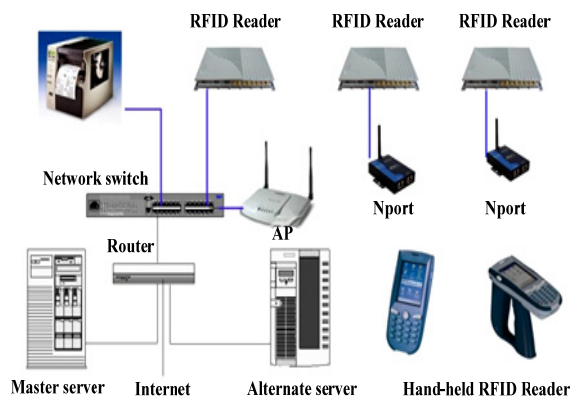


Fig. 1. The construction of RFID system.

From the aspect of basic information transmission principle, RFID technology is based on transformer-couple model (energy and signal transmission between primary point and secondary point) in low frequency band, while it is based on space-couple model of a radar target detection (radar transmits electromagnetic signals, and returns target information to the radar receiver after meeting the target.) Harry Stockman published “communication by using reflective power” which laid the theoretical basis of the RFID technology.

The basic working principle of RFID technology is not complex: after tags entering into a magnetic field, receiver sends radio frequency signal. Namely, it sends out the product information (passive tag or passive label) stored in the chip with induction current energy, or actively sends out a certain frequency’s signal (Active Tag). Reading device reads the information and decodes it, and then sends the information to the central information system for data processing.

A complete set of RFID system consists of three parts: reader, electronic tag and application software. Among them, reader and electronic tag are called transponder. Its working principle is that the reader sends specific frequency radio wave energy to transponder to drive transponder circuit for data transmission. The reader will receive and decode data in turn, and then do the corresponding data processing.

From the aspect of communication and energy induction between RFID card-reader and electronic tag, it can be divided into inductive coupling and backscatter coupling. In generally, most of the low-frequency RFID systems use the first method, while the high-frequency RFID systems use the second method.

The reader can be divided into read device and read/write device depended on the differences between the using structure and technology, which is the center of RFID system’s information controlling and processing. The reader generally consists of coupling module, transceiver module, control module and interface unit. Half-duplex communication is used in information exchange between the reader and transponder, meanwhile the reader provides energy and timing sequence for passive transponder through the coupling method. In the practical applications, it can realize the functions of object identification information collection, processing and remote transmission and so on via the Ethernet or WLAN. Transponder is a kind of information carrier in RFID system. At present, transponder mostly consists of coupling elements (coil, micro-strip antenna, etc.) and passive microchip units.

2.2. The RFID Information Security Issues

According to the working principle of RFID system, the RFID security risks focus on readers and tags with respect to the reader and background-server. The best way to analyze the security problems existing in the system is to stand on the attackers’ spots and figure out their simplest, most effective and most insidious methods to attack RFID systems. Thus we can be able to find out the loopholes in the system at the lowest cost [5]. Generally, attackers attack the RFID application systems from two aspects: 1) the information transmission between the reader and the back-end database; 2) the wireless communication between the reader and the tag, as well as tag itself. The latter one is the focus of our study. As the RFID technology requires the low cost of the hardware itself, some good approaches cannot be applied directly in this technology. This is the reason why RFID technology doesn’t widely replace barcode labels. Assume the first aspect safe and focus on the second aspect. The second aspect can be divided into the following two aspects: 1) internal personnel divulge the secrets of the reader and tags; 2) external attacks, namely take advantages of the hardware and

software to attack the reader and electronic tags to obtain valuable information [6].

2.2.1. Secret Divulgence of the RFID System from Internal Personnel and its Solving Strategy

There are two ways for insiders to leak the confidential information of RFID system. One is that radio frequency label entities are stolen to provide for lawbreakers. Then the lawbreakers remove the chip package by physical means in a lab environment and use the microprobe to obtain sensitive signal, so that they carry out the complex attacks of RF tag remodeling. The other one is that the insiders offer the key to lawbreakers. As for the solution of this threat, we need to tighten up the internal management and raise the awareness of security risks for insiders.

2.2.2. External Attack and its Solution Strategy

Assuming no insider leaks, the external attacks of attackers will become the main factors of influencing RFID security. That is taking advantages of the hardware and software to attack the reader and electronic tags to obtain valuable information. This is the emphasis and difficulty of our research. As for the designed systems based RFID technology, there are usually two kinds of external attacks: one is the active attack (tampering with information, falsifying information, reproducing information and interrupting information); another is the passive attack (tracking tag to monitoring goods circulation, interfering with the normal work of the reader and tag and intercepting the delivering information of tags). The seven types of attacks above are the most common attacks seen in RFID technology applications in the commercial sphere. Fig. 2 shows the information requirements of the seven types of attacks.

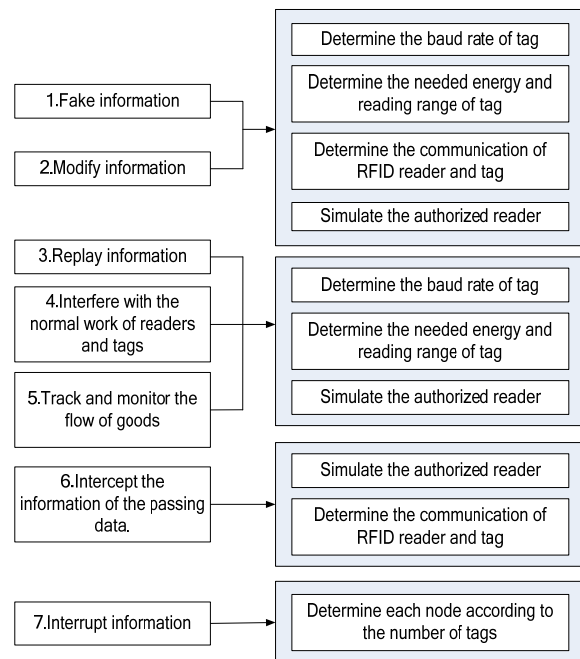


Fig. 2. The information requirements of the seven types of attacks.

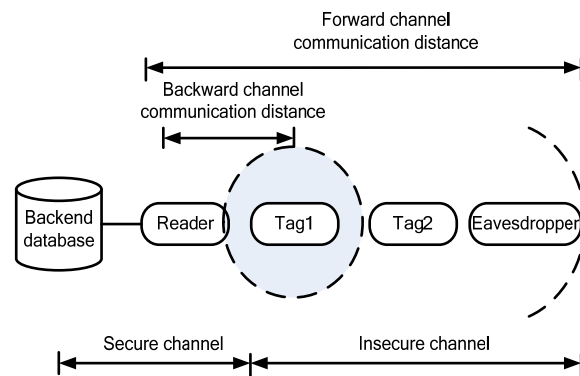


Fig. 3. The communication model of RFID system.

The back-end database can be run on the database system of any hardware platform which can be selected by users themselves according to their actual needs. In general, assuming its powerful computing and storage capacity, it contains all the tag information. Actually, tag reader is a wireless transmitter and receiver device with antenna and its processing power and storage space are relatively large. RFID tag is a kind of miniature circuit equipped with antenna. Tag is usually without the microprocessor and consists of thousands of logic gate circuits. As a result, it is really a challenge to integrate encryption or signature algorithm into such equipment. The communication distance between tag and tag reader is influenced by multiple parameters, especially the communication frequency.

According to its energy source, the tag can be divided into three major categories: passive tag, semi-passive tag and active tag. Their characteristics show in Table 1.

3. RFID System Security Mechanisms

According to the previous chapter about the introduction of RFID and its existing security problems, we will discuss RFID security mechanisms in detail.

3.1. The Communication Model of RFID System

The communication model of RFID system shows in Fig. 3.

Table 1. The classification and characteristic of Tag.

	Energy source	Transmitter	Maximum distance (m)
Passive tag	Inactive mode	Passive	10
Semi-passive tag	Internal battery	Passive	100
Active tag	Internal battery	active	1000

According to its function, tag can be divided into five categories: Class 0, Class 1, Class 2, Class 3 and Class 4. Their functions enhance in turn, showed in Table 2.

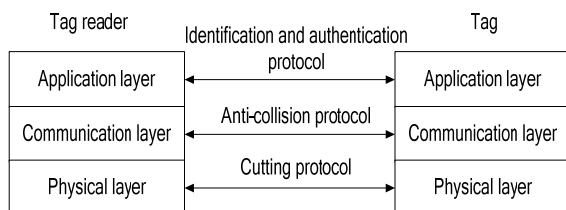
Table 2. The assortment and function of Tag.

Type	Energy source	Alias	Storage	Characteristic
Class 0	Inactive mode	Anti-theft	None	EAS function
Class 1	Arbitrary	EPC	Read-only	Only for identification
Class 2	Arbitrary	EPC	Read/write	Data logging
Class 3	Internal battery	Sensor tag	Read/write	Environmental sensor
Class 4	Internal battery	Intelligent particle	Read/write	Adhoc network

The channel from tag reader to tag is called “forward channel”, and the channel from tag to tag reader is called “backward channel”. As the wireless power between tag reader and tag varies greatly, the communication range of forward channel is much greater than that of backward channel. This inherent asymmetric channel will naturally have great impact on the design and analysis of RFID system security mechanism.

Generally speaking, we usually do the basic assumptions: the communication channel between tag and tag reader is not secure, while the communication channel between tag reader and backend database is safe. This is considered much easier to design, manage and analyze RFID system.

ISO/IEC 18000 standard defines two-way communication protocol between tag reader and tag. Its basic communication model shows in Fig. 4.

**Fig. 4.** The basic communication model.

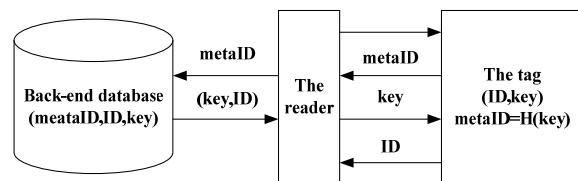
As we can see from the above figure, the communication model of RFID system consists of

three layers that are from bottom to top: physical layer, communication layer and application layer. The physical layer focuses on the electrical signal, such as channel allocation and physical carrier and so on. Communication layer defines the method of data exchange in two-way method between tag reader and tag, of which the most important issue is to resolve the conflict when multiple tags simultaneously access a tag reader. The application layer is used to solve the related contents of the top-level application, including certification, identification and data representation of application layer etc. In general, the RFID security protocol refers to the application layer protocol.

3.2. RFID Security Protocol

1. Hash-Lock protocol

The Hash-Lock protocol [7] is a kind of access control mechanism based on one-way Hash Function. This protocol uses $\text{metaID} = H(\text{key})$ instead of the real tag's ID to identify, which can hide the real tag's ID and avoid information leak. In order to make the mutual authentication successful, it is required to store the three sets data of metaID, ID and key into the back end database. Also the ID and key are stored into the read only memory (ROM). The process of this protocol shows in Fig. 5.

**Fig. 5.** The Hash-lock protocol's process.

As we know in the process of agreement, the protocol uses metaID to response the reader's request. Due to $\text{metaID} = H(\text{key})$ is not the real tag's ID, illegal readers cannot copy the tag or attack it. However, when asked to respond, the tag's response message is the same, which makes the attacker able to track the connection. In addition, the signal in radio communication may be tracked at any time. At the final step in this agreement, the tag ID number is transmitted in plaintext form to the reader, which obviously gives the attackers chance to steal tags' information, or even copy the tags. Therefore, Hash-lock protocol's security and privacy are weak.

2. Hash chain protocol

Hash chain protocol [8] is the improved agreement for Hash-lock protocol. In essence, this protocol is based on a shared secret inquiry-response protocol. This protocol uses a dynamic refresh mechanism to prevent tracking. Its implementation method mainly adds two Hash function in the tag. Similar to Hash-lock protocol, this protocol stores the

tag's ID and $S_{t,1}$ ($S_{t,1}$ is the tag's initial key value, each tag's $S_{t,1}$ is different.) in the back-end database and saves $S_{t,1}$ in the ROM of the tag. The protocol's process shows in Fig. 6.

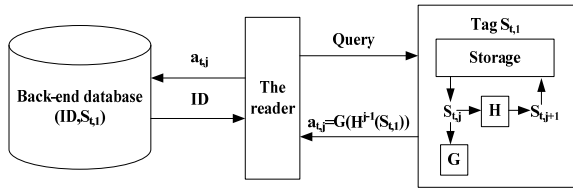


Fig. 6. The Hash chain protocol's process.

From the protocol's implementation process, we can know that the back-end database receives the tag's output $a_{t,j}$ from the reader. Meanwhile, calculate each $S_{t,1}$ according to the tag ID and the initial key (ID, $S_{t,1}$) in the database, and then check if $a_{t,j}$ and $a_{t,j}^*$ are equal. If they are equal, we can determine the tag ID. This method meets no-connection and forward security. The above G is a one-way function. So attackers can obtain the tag's output $a_{t,j}$, but cannot obtain $S_{t,j}$ from $a_{t,j}$. The output of G is a random value, thus the attacker can only know the tags' output but cannot link $a_{t,j}$ and $a_{t,j+1}$. In addition, H is also a one-way function. Even if the attack can tamper the tag and obtain the secret value, he still cannot get $S_{t,j}$ from $S_{t,j+1}$. In other words, this protocol has better defense capability of tracking and eavesdropping attack. However, when the tag responses authentication request, it cannot authenticate the reader. At the time an unauthorized reader sends inquiry request to the tag, the tag will also responds message, the attacker could use this information to deceive the tag will also responds message, the attacker could use this information to deceive the system.

3. Random Hash-lock protocol [9].

In order to avoid connection tracking, the RFID tags' response should not be fixed but random. The reader send inquiry request, the tag will send out a changing metaID. Each tag and reader share an authentication key ID_k . When the reader send inquiry request to the RF tag, the RF tag generates a pseudo random number r_k and output $(r_k, H(ID_k || r_k))$, among which H means Hash function and $||$ represents concatenation. When the reader obtains all the tags' random numbers and $(r_k, H(ID_k || r_k))$ it calculates the Hash value according to the received R and all ID_k value stored in the backend database. If the Hash value matches the Hash value sent to the RFID tags, the reader identifies the RFID tag's ID_k and sends it back to the reader. The protocol process shows in Fig. 7.

Because every time when asked, the output of RFID tag has changed, so this method can prevent tracking and being connected. But this method is not suitable for the users who have a large number of RFID tags. This is because the authorized reader

identifies a radio tag, it needs to search and calculate all the tags' ID_k .

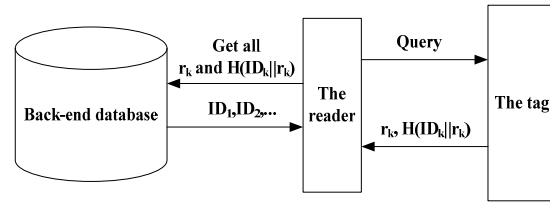


Fig. 7. The random Hash-lock protocol's process.

4. The improved security authentication protocol in this article

The protocol process is as follows.

Aiming at the shortcomings of the above agreement, an improved random Hash-Lock protocol is proposed.

Respectively, use R for representing the reader, T for tags, D for database, ID_R and ID_T for the identifier of the identity. The protocol process is as follows.

- 1) $R \rightarrow T$: Query;
- 2) $T \rightarrow R$: ID_R, r_1 ;
- 3) $R \rightarrow D$: ID_R, r_1 ;
- 4) $D \rightarrow R$: $H(K || ID_R || r_1), r_2$;
- 5) $R \rightarrow T$: $H(K || ID_R || r_1), r_2$;
- 6) $T \rightarrow R$: $ID_T \oplus H(K || ID_R || r_2)$;
- 7) $R \rightarrow D$: $ID_T \oplus H(K || ID_R || r_2)$;
- 8) $D \rightarrow R$: ID_T .

This improved protocol's process shows in Fig. 8.

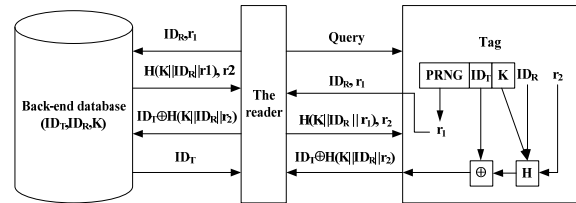


Fig. 8. The improved protocol's process.

The instruction of this protocol:

When generating tags, besides the common tag data ID_T , each tag has a unique random tag data ID_R , as well as the key K for authentication. ID_T , ID_R and K are respectively stored in the tags and the back-end database.

1) The reader enquiries requests to the tag.

2) After receiving the quest, the tag uses pseudo random number generator (PRNG) to generate a random number r_1 and sends the (ID_R, r_1) to the reader in order to identify the reader.

3) The reader sends (ID_R, r_1) to the back-end database.

4) After receiving (ID_R, r_1) , the back-end database will search K according to ID_R and calculate $H(K, ID_R || r_1)$. Then it produces a new random number r_2 and sends it to the reader.

5) The reader forwards $H(K \parallel ID_R \parallel r_1)$ and r_2 to the tag.

6) The tag uses the self-saved ID_R to calculate $H(K \parallel ID_R \parallel r_1)$ which will be compared with the received $H(K \parallel ID_R \parallel r_1)$. If equal, then the legal status of the reader can be confirmed. And then the tag uses its own preserved ID_T , ID_R and received r_2 to calculate $ID_T \oplus H(K \parallel ID_R \parallel r_2)$ which will be sent to the reader.

7) The reader forwards $ID_T \oplus H(K \parallel ID_R \parallel r_2)$ to the back-end database.

8) Due to the stored (ID_T, ID_R) in the back-end database, the ID_T can be obtained by one Hash operation and XOR. Then the database searches the data and judges if there is ID_T . If yes, send the ID_T to the reader.

This improved Protocol security and efficiency analysis are as follows.

The first five steps of the protocol are for the tag's authentication to the reader and the latter three steps are for the reader's identification to the tag. With the advantages of the existing agreements, the improved protocol is able to resist all kinds of attacks and achieve good security.

1) Anti-eavesdrop: during the interaction between the reader and tag, the data has been randomly blinded off. Because of each chosen different random number, the data is always different when delivered. Then by the one-way Hash function, attackers cannot get any valuable information from the interactive data.

2) Prevent replay-attack: even if the attacker has collected the data in the process of the interaction between the tag and reader, after implementation of the agreement in the course of reproduction, it cannot pose a threat to the agreement. This is because it uses random number to ensure data freshness in the interaction of the reader and tag. The data collected by attackers has lost its timelines. The tag or back-end database can easily test out whether it is the fresh news, so that this protocol can prevent replay attacks.

3) Anti-tracking: the signal delivered between the reader and tag in the agreement is changing, because of the random numbers that we choose are different each time, as well as the randomness of Hash function. Thus, it is difficult for attackers to track tags and attack the users' location privacy.

The efficiency and application of the improved protocol: when in the execution of the agreement, the tag implements one pseudo-random number generation computing operation and twice Hash operation and the read doesn't do these operations. The back-end database does the same operations like the tag. Also, the back-end database needs only one Hash operation and one single search. As a result, this improved protocol has the advantages of operational efficiency and low cost. Meanwhile, with the increasing in the number of tags, the storage and computation increase. However, the calculated amount is obviously just a linear function with the tag's function. Thus, this protocol is suitable for large-scale systems.

5. The measures for security protocol

1) Prevent the tag frequency detection. For instance, killing tag principle theory is to make the tag lose its function, so as to prevent the labels and carriers being tracked. According to Faraday cage principle, putting tags in the conductive container can prevent label to be scanned. Namely, passive tags can't receive signals and gain energy. The signal emitted by active tags cannot be issued. Therefore, Faraday cage can be used to prevent privacy offenders scanning the label information. Active jamming: actively interfering with radio signals is another kind of shielding label method. Tag users can prevent RFID readers being operated through an active broadcast radio signal device. Block tags: stop label principle is achieved by using a special anti-collision algorithm of preventing label interference. The reader reads the command and gets the same response data invariably, so that the tags are protected.

2) Prevent the reading range of energy detection of tag. For instance, the clipped tag is a new type of tag which is developed by IBM for RFID privacy issues. Users can rip off or scrape the RFID antenna and shrink the reading range of labels so that tag cannot be read easily. Despite the antenna cannot be reused if adopting the clip tag technology, the reader can still be read within a close range.

3) Prevent the detection of security protocols and stealing of authentication key. The first is to certify a strict security protocol. For example, Hash-lock protocol is for the sake of avoiding information leakage and tracing. It uses the pseudo ID instead of the real tag ID. Randomized Hash-Lock protocol adopts an inquiry-response mechanism based on random number. In essence, Hash chain protocol is also based on a shared-confidential inquiry-response protocol. When using two readers with different hash functions to launch a certification, the tags always send different responses. In this protocol, the tag has become an active tag with the capability of ID self-updating. The ID change-protocol based on Hash is similar to Hash chain protocol, in which the ID exchange information is different in each response. The system uses a random ruler to dynamically refresh the tags and labels, meanwhile update the information of the last answer and the last successful answer so that the protocol can resist attacks. David's Digital Library RFID protocol is based on pre-shared secret pseudo random function which is used to achieve certification. Distributed RFID inquiry-response certification protocol is suitable for distributed database RFID certification, which is a typical two-way inquiry-response authentication protocol. The computing resources and storage resources of RFID based on re-encryption mechanism are very limited, so very few people design the RFID security mechanisms based on public-key cryptosystem. The second is to protect related authentication keys, which contains Hash Lock, Random Hash Lock, Hash Chain, and Renewal Key Value Random Hash Lock and so on.

4) Prevent RFID reader frequency detection, such as the changing frequency.

5) Prevent the RFID reader and the back-end system interface being counterfeited, which mainly uses security protocols and network security policies.

6) Supervise all the nodes and find out which one send the most information. It mainly uses the method of dispersing the sending packets and not focusing on one or two nodes. Also it can use fake packets and nodes to confuse the attackers.

4. The Design of Security Assessment Model-Based on the Analytic Hierarchy Process and Fuzzy Comprehensive Evaluation

As for the information security risk assessment of RFID systems, the main difficulty is the quantitative process of the qualitative indicators. As a result, we propose a kind of method based on the analytic hierarchy process and fuzzy comprehensive evaluation model, which can effectively solve this problem [7, 8, 10-12]. The analytic hierarchy process can calculate the related weight of impacting information security risk factors. And then rank the weight values of various factors so that we can make a horizontal comparison, in order to provide a strong basis to take relevant measures. Fuzzy comprehensive evaluation obtains the risk level of the information system according to experts' evaluation of information system. Thus, we can improve understanding the relevance and urgency of information system security risk and take effective security measures to ensure the security of network information system. The information security evaluation model based on this method shows in Fig. 9.

4.1. Analytic Hierarchy Process

Analytic Hierarchy Process (AHP), which is proposed by Professor TL Saaty (an American operational research expert), is a simple, flexible and practical method with multi-criteria decision. It has the following algorithm steps:

Step 1: build the hierarchy model.

Step 2: construct the judgment matrix. By making a comparison of each indicator's relative importance in the same level, we can obtain the relative weight ratio that is called plus. The judgment matrix is constructed in this way and shown in the following equation.

$$A = \begin{bmatrix} 1 & \frac{w_1}{w_2} & \dots & \frac{w_1}{w_n} \\ \frac{w_2}{w_1} & 1 & \dots & \frac{w_2}{w_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{w_n}{w_1} & \frac{w_n}{w_2} & \dots & 1 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \quad (1)$$

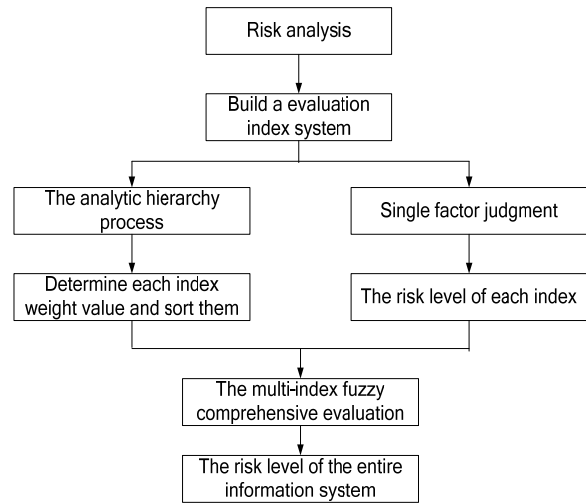


Fig. 9. The information security evaluation model.

The judgment matrix A is an $n \times n$ square matrix and its principal diagonal is 1, which satisfies

$$a_{ij} = \frac{1}{a_{ji}}, i \neq j, i, j = 1, 2, \dots, n, a_{ii} = 1, a_{ij} > 0,$$

where a_{ij} is the relative weight ratio of two factors i and j .

Step 3: calculate the weight value. The calculating method shows as follows.

Scale each column vector of matrix A .

$$\bar{a}_{ij} = \frac{a_{ij}}{\sum_{k=1}^n a_{kj}} \quad (i = 1, 2, \dots, n) \quad (2)$$

After scaling judgment matrix by column, make a sum by line.

$$\bar{W}_i = \sum_{j=1}^n \bar{a}_{ij} \quad (i = 1, 2, \dots, n) \quad (3)$$

Scale the vector $\bar{W} = [\bar{W}_1, \bar{W}_2, \dots, \bar{W}_n]^T$.

$$\bar{W}_i = \frac{\bar{W}_i}{\sum_{i=1}^n \bar{W}_i} \quad (i = 1, 2, \dots, n) \quad (4)$$

Step 4: consistency checking.

Calculate the maximum characteristic root:

$$\lambda_{\max} = \sum_{i=1}^n \frac{(AW)_i}{nW_i} \quad (5)$$

Calculate the consistency indicators:

$$CI = \frac{\lambda_{\max} - n}{n - 1} \quad (6)$$

Calculate the consistency proportion:

$$CR = \frac{CI}{RI} \quad (7)$$

If $CR < 0.1$, the consistency of the judgment matrix is acceptable.

4.2. The Fuzzy Comprehensive Evaluation [9]

Fuzzy comprehensive evaluation is to make the overall evaluation of the things with a variety of properties or factors influencing their overall pros and cons. Hierarchy model with single layer or multi-layer must have two key steps: 1) determine the fuzzy relation R . R is a fuzzy mapping from the factor set x to the judgment set y ; 2) calculate the fuzzy judgment subset $B=AR$. Due to many factors that need to consider, there is a certain kind of hierarchy in a complex system. As a result, we must use the method of hierarchical stepwise judge, namely fuzzy multi-level comprehensive evaluation method.

The steps of the fuzzy multi-level comprehensive evaluation method are as follows.

Assume the factor set $X = \{x_1, x_2, \dots, x_n\}$, x_i means the factors need to be considered in a problem. Let the judgment set $Y = \{y_1, y_2, \dots, y_m\}$, y_m represents the judging level.

Step 1: divide the factor set X . In the formula above, $x_i = \{x_{i1}, x_{i2}, \dots, x_{ik_i}\}$, $i = 1, 2, \dots, n$. x_i contains k_i factors.

Step 2: single factor judgment.

According to the initial model, comprehensively evaluate the k_i factors in $x_i = \{x_{i1}, x_{i2}, \dots, x_{ik_i}\}$.

Assume that the important degree of the factor set x_i is the fuzzy subset A_i , and that the evaluation matrix of the k_i factors in x_i is R_i . Then we can obtain the formula as follows.

$$B_i = A_i \circ R_i = (b_{i1}, b_{i2}, \dots, b_{im}), i = 1, \dots, n$$

In the formula above, B_i is the single factor judgment of x_i .

Step 3: comprehensive multi-factor judgment.

The important degree of the factor set $X = \{x_1, x_2, \dots, x_n\}$ is the fuzzy subset A , $A = (A_1, A_2, \dots, A_n)$. And the overall evaluation of A is R as follows.

$$R = \begin{bmatrix} B_1 \\ \vdots \\ B_n \end{bmatrix} = \begin{bmatrix} A_1 \circ R_1 \\ \vdots \\ A_n \circ R_n \end{bmatrix}$$

Finally, we can obtain the overall comprehensive multi-factor evaluation results, namely,

$$B = A \circ R$$

The formula above is the comprehensive judgment result of $X = \{x_1, x_2, \dots, x_n\}$.

4.3. The Information Security Evaluation Model and its Effect

The information security risk analysis need to identify four elements, and each element includes many sub-elements. In order to highlight the focus of the risk assessment, we need to appropriately simplify the evaluation index system of the information system risk. The index system shows in Fig. 10.

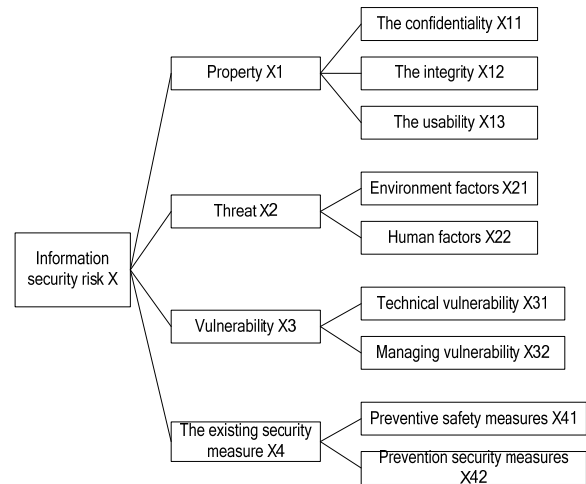


Fig. 10. The information security evaluation index system.

In the evaluation indicator system in the figure above, the confidentiality means the degree of providing or disclosing the information to unauthorized individuals, process or other entity. The integrity is to ensure that information and information system are not altered or destructed by unauthorized persons. The usability represents that the authorized entities are able to access and use the data or resources as required. Environment factors means environmental conditions or natural disasters. Human factors denote that external people's vandalism or insiders' leak. Technical vulnerability involves all levels' problems of the physical layer, network layer, system layer and application layer and so on. Managing vulnerability can be divided into technical management and organizational management. The former is related to the specific technical activities, and the latter is related to the management environment. Preventive safety measures can reduce the threat possibility of security events with the usage of the vulnerabilities. Protective security measures can decrease the impact of security problems.

The difficulty of quantitative assessment of qualitative indicators in the assessment is solved by using the analytic hierarchy process and fuzzy comprehensive evaluation to assess the security risk of the information network system. With this method, we can calculate the relative risk degree and the information network risk rating of the elements. By confirming the level of risk, we can improve the understanding of information systems security risk, determine the relative risk degree of the elements, control risk, reduce risk and transfer risk.

5. Conclusion

The scientific and effective security assessment of the RFID system is one of the important measures to ensure the system's security. In this paper, the basic construction of the RFID system is firstly introduced. Then the information security requirements and security issues of RFID system are analyzed. According to this we study the safety communication mechanisms and establish a kind of information security assessment model in RFID system based on AHP and fuzzy comprehensive evaluation. How to scientifically and effectively evaluate the security of RFID systems will be the further work in this direction.

References

- [1]. Zhou Yong-Bin, Feng Deng-Guo, Design and analysis of cryptographic protocols for RFID, *Chinese Journal of Computers*, Vol. 29, No. 4, 2006, pp. 581-589.
- [2]. Mi Zhi-Qiang, Yang Shu, RFID information security policy analysis, *Logistics Engineering and Management*, Vol. 31, No. 5, 2009, pp. 147-148.
- [3]. Luo Chun-Bin, Peng Yan, Yi Bin, Overview on RFID technology and application, *Communication Technology*, Vol. 42, No. 12, 2009, pp. 112-114.
- [4]. Jiang Fa-Qun, Wang Xiao-Qin, Chen Lu-Ping, Research on the security and testing of RFID system, *Network and Computer Security*, No. 1, 2011, pp. 39-43.
- [5]. Wang Xiao-Mei, Zhang Zhao-Hui, Risk analysis of RFID networks, *Journal of University of Electronic Science and Technology of China*, Vol. 38, No. 1, 2009, pp. 65-68.
- [6]. Sun Pei-Yan, Tian Wei-Ping, Yang Shu-Qing, Analysis on problems that affect RFID data security, *Computer Development & Applications*, Vol. 22, No. 5, 2009, pp. 13-16.
- [7]. Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels, RFID systems and security and privacy implications, in *Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems CHE'2002*.
- [8]. Miyako Ohkubo, Koutarou Suzuki, Shingo Kinoshita, Hash-chain based forward-secure privacy protection scheme for low-cost RFID, in *Proceedings of the Symposium on Cryptography and Information Security SCIS'2004*.
- [9]. S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, Security and privacy aspects of low-cost radio frequency identification systems, in *Proceedings of the Security in Pervasive Computing 2003*, Vol. 2802 of *Lecture Notes in Computer Science*, 2004, pp. 201-212.
- [10]. Xiao Long, Qi Yong, Li Qian-Mu, Information security risk assessment based on AHP and fuzzy comprehensive evaluation, *Computer Engineering and Applications*, Vol. 45, No. 22, 2009, pp. 82-85.
- [11]. Luo Heng-Feng, Zhu Jian-Hong, Li Jin-Hua, Yang Xiao-Ming, Li Qian, Safety evaluation index system and model for RFID system, *Electronic Product Reliability and Environmental Testing*, Vol. 27, No. 5, 2009, pp. 56-59.
- [12]. Zhu Lingbo, Dai Guanzhong, An information security model based on fuzzy synthesis evaluation, *China Information Security*, No. 8, 2006, pp. 13-15.