International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 209-216
http://dx.doi.org/10.14257/ijsia.2015.9.6.20

Research on the Authentication of Radio Frequency Identification based on the Hash function

Bai Zhi and He Yi-Gang

College of Electrical and Information Engineering,
Hunan University, Changsha, China
Zhibaichshn@163.com

Abstract

As a kind of accurate, rapid and real – time data acquisitions and processing technology, RFID can give unique identification to entity object, has been widely used in various industries, such as manufacturing, sales, transportation and so on. But with its widely application, many relevant problems, especially the safety issues of RFID system and the low cost issue of label have been raised more and more attention by people; therefore, a new and more appropriate security authentication protocol becomes necessary. In this paper, firstly introducing several now available security authentication protocols, and analyzing their strengths and drawbacks, then proposed a new authentication scheme based on Hash function, doing security properties and feasibility analysis of it in theory, and proving that the security properties of this scheme is more efficient, and it is more applicable to meet the needs of people through test at last.

Keywords: *Hash function; RFID; authentication protocol; security*

1. Introduction

RFID (radio frequency identification) is the general term for technology which uses radio wave to distinguish the single object automatically. As a kind of accurate, rapid and real–time data acquisition [1] and processing high technology, RFID can give unique identification to entity object, has been widely used in various industries, such as manufacturing, sales, transportation and so on. But with its widely application, many relevant problems, especially the safety issues of RFID system and the low cost issue of label have been raised more and more attention by people, especially in logistics, the demand of RFID tag is huge, so that the low cost of RFID will be much suitable. What's more, as a result of the unauthorized reader's reading and collecting the electronic tag information within its role scope, many consumers' privacy information are revealed to some extent. In a word, when enjoying the much convenience brought by RFID, but at the same time, we have to face with and dispose of the numerous security problems of the RFID. Therefore, this paper introduces several now existing security authentication protocols, and according to the deficiency of these protocols putting forward a new and improved security authentication scheme based on Hash function and also doing theoretical analysis of the feasibility of this scheme [2].

2. The RFID System and its Security Requirements

The RFID system: Radio frequency identification (RFID) system is a kind of non-contact automatic identification technology which automatically identifies target object and obtain the relevant data of it through radio frequency signal in the open system environment. It has many advantages, and is widely used in transportation logistics, security and other fields [3].

RFID system mainly includes three parts: RFID tags, reader and the back-end database.

ISSN: 1738-9976 IJSIA

The structure is shown in Figure1.

1) RFID tags: on the identified items, stores the information of the item, and in non-contact way to read the information on the label through the reader.

2) Reader: it can use the radio frequency identification technology to read the information stored on the label, and the information would be uploaded to the back-end database, and managing through the database.

3) Database: has a powerful ability to do data analysis and storage, and store information of the labeled item.

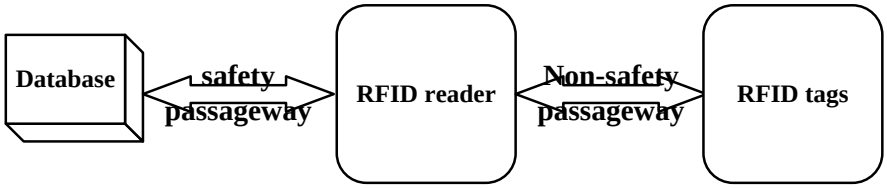

Figure 1. The Structure of Structure

Safety requirement:

1) Security and integrity of the data. Guaranteed the information transmitted between reader and label is encrypted, so that the attacker is unable to analyze the real sense from intercepting information. At the same time to ensure that the information transmitted is complete, and it must be against tampering, both sides can distinguish [4].

2) Privacy protection. Privacy protection mainly refers to prevent labels' user from tracking. Illegal reader sends a query command on the label, and the talisman located the user through the specific respond sound of the label.

3) Anti replay attacks. If attacker filches effective information of the label through illegal means, and after a period of time and then passed to the reader, getting through by reproducing to cheat the reader certification.

4) Anti forgery and deny. Making sure that the attacker cannot get through the certification by the forgery of either party of the label and reader [5].

At present, there are two main methods to solve the security problem of RFID, they are: physical mechanisms and cryptographic mechanism. And physical mechanism includes faraday cage, blocker tag, active jamming and so on. But these physical methods increase the extra amount of physical device or element, which is not only inconvenient, but also increase the cost.

3. Related Research on the RFID Security Protocol

So far, there are various security authentication protocols about the security and privacy issues between reader and tags in RFID sensor network. There are 3 typical protection protocols of RFID security and privacy based on one-way Hash function: Hash-lock protocol randomized Hash protocol and Hash chain protocol.

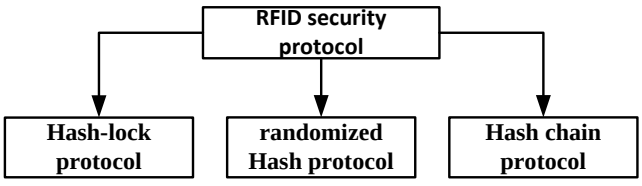

Figure 2. The Constitution of the RFID Security Protocol

3.1. Hash-lock Protocol

It was a kind of RFID security protocol proposed by Sarma, to avoid information

leakage and being tracked, the real ID of label was replaced by metaID, namely metaID = Hash (key) [6]. And initially the label is locked; the backstage data store the secret key of each label, including metaID, ID and key. Certification process is shown in Figure 3.

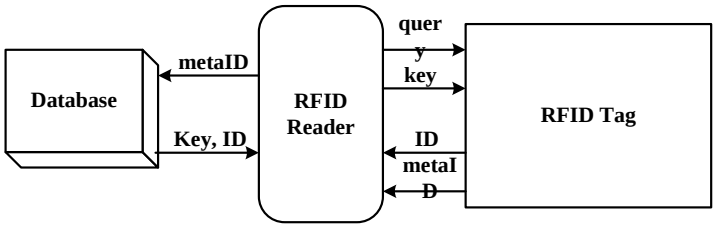

Figure 3. The Certification Process of Hash-lock Protocol

The protocol uses the hard tightness of the one-way Hash function to encrypt the transmitted information, so to some extent solving the privacy preserving of access control. However, because the data metaID each tag answered is fixed, so the protocol cannot prevent the position tracking attacks; and the ID in plaintext form transferred in an insecure channel, an attacker can easily get the label information, vulnerable to the retransmission attack and spoof attack, does not have the indiscernibility [7].

3.2. Randomized Hash- lock Protocol

In order to solve the position tracking problem in Hash- lock protocol, Weis proposed the randomized Hash- lock protocol. It adopted ask - response mechanism which is based on the random number, is the improved form of Hash- lock protocol. [8] In the label, not only Hash function is embedded, but also pseudo random number generator, so that to ensure the unpredictability of transmission number by adding random numbers and the background database stores identities of all the tags. The specific validation process is showed in Figure 4.

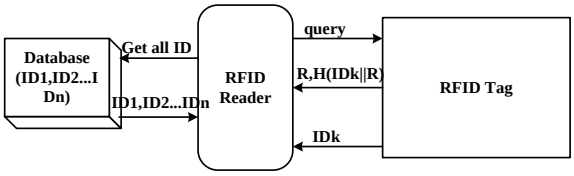

Figure 4. The Specific Validation Processes of Randomized Hash- lock Protocol

These protocols solve the position tracking problem of the label successfully by using the unpredictability of random number. However, because of the low cost and limited computation ability of the label, the integration of pseudo random number generator in the label is not realistic, implementation is more difficult, In addition, the identified tag ID certification was still transmitted through insecure channel, the retransmission and spoof attack are still not coped.

3.3. Hash Chain Protocol

The method of Hash chain is proposed by NTT laboratory, it is based on the shared secret challenge - response protocol. The tags in the protocol integrated with two different Hash functions H and G. Tags and background data libraries all stored the initial value, background database stores all the standard ID sign, constantly refresh the tag dynamically in the authentication process. And the authentication process is shown in Figure 5.

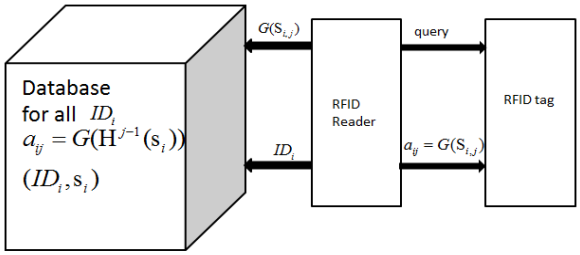

Figure 5. The Authentication Process of Hash Chain Protocol

By adding label ID dynamically refresh mechanism, the protocol satisfies the indiscernibility and forward security, and also has strong anti-guess and anti-analysis ability [9]. However, Hash protocol is one-way authentication protocol, only authenticate the tag, not for reader, if an attacker masquerading as a legitimate reader, it is vulnerable to suffer the replay attack and spoofing attacks. In addition, the protocol requires two different hash functions G and H, which increasing the production cost of the Tag intangibly, the computation library in background data is very big.

4. The Design a New RFID Security Protocol based on Hash Function and its Application in Authentication Research of FRID

Aiming at the deficiency in the above protocols, someone has put forward many security mechanisms which are based on the password techniques in the study of RFID security mechanism [10]. Among all these encryption based security mechanism, design of RFID security protocol based on the Hash function has attracted much attention. Therefore, no matters from the demand side or from the low cost hardware implementation of Hash label. Hash function is most suitable for the RFID authentication protocol. This protocol can be divided into two categories: static and dynamic mechanism of ID mechanism [11]. It is also a three rounds protocol, as is shown in Figure 6.

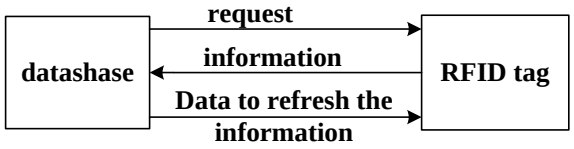

Figure 6. The Three Rounds Protocol

4.1. Authentication Protocol Design

The initial conditions and the related instructions: In the initial state, tags and readers only need to memory its own logo, respectively are ID_x and ID_y. The backstage database store all the tags and $(ID_x, H(\mathrm{ID}_x))$ $(ID_y, H(\mathrm{ID}_y))$ data of the reader. Among them, $\mathrm{H}(\bullet)$ refers to the encrypted data by Hash function. Tag is a passive tag with low cost, having small storage capacity and low computing power, the Hash function is safe enough for RFID, pseudo random number is also safe enough [12].

The authentication steps: RFID authentication scheme which based on Hash functions is shown in Figure 7.

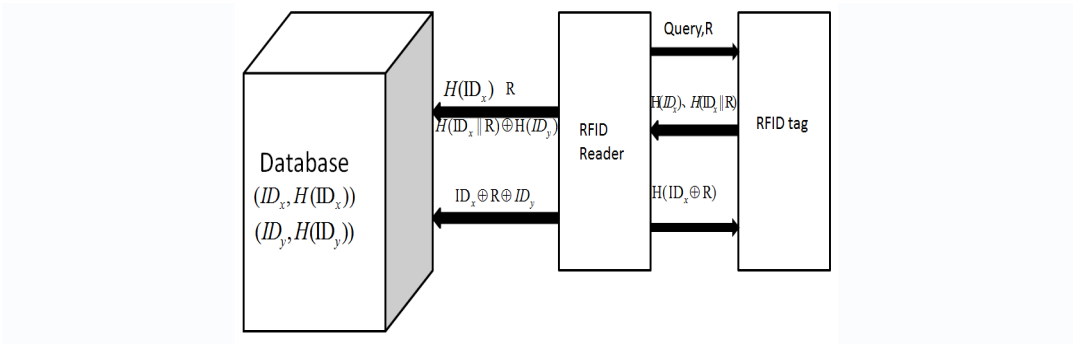

Figure 7. RFID Authentication Scheme which based on Hash Functions

The specific validation process is as follows:

(1) Reader generates a random number R, and sent Query and R to the label as the authentication request;

(2) Label uses own identification ID_x and the random number R calculates $H(\mathrm{ID}_x)$ and $H(\mathrm{ID}_x \| \mathrm{R})$ ($\|$ is the series symbol), and $\mathrm{H}(ID_x)$、$H(\mathrm{ID}_x \| \mathrm{R})$ will be sent to the reader as a response [13];

(3) Reader uses Hash function to encrypt its own identity ID_y and comes $H(\mathrm{ID}_y)$ and differentiates with $H(\mathrm{ID}_y \| \mathrm{R})$ which label sent or operates the $H(\mathrm{ID}_x \| \mathrm{R}) \oplus \mathrm{H}(ID_y)$, and at last, the reader will sent R, H $\mathrm{H}(ID_x)$、$H(\mathrm{ID}_x \| \mathrm{R}) \oplus \mathrm{H}(ID_y)$ to the backstage database [14];

(3) The backstage database will calculate $\mathrm{ID}_x \oplus \mathrm{R} \oplus ID_y$ and turn it to the reader;

(4) Reader will work out their label ID according to its own ID_y and the random number R, and sends it to label [15];

(5) labels will differentiates its identification ID and R, and operating $\mathrm{ID}_x \oplus \mathrm{R}$, and then calculate the $\mathrm{H}^*(\mathrm{ID}_x \oplus \mathrm{R})$, comparing values $\mathrm{H}(\mathrm{ID}_x \oplus \mathrm{R})$ obtained and the calculated value $\mathrm{H}^*(\mathrm{ID}_x \oplus \mathrm{R})$ if they are equal, the reader is legitimate, otherwise, reader is an illegal reader, tag does not respond [16].

5. Security Properties Analysis and Performance Comparison of the Protocol

5.1. Safety Properties Analysis

(1) Forward security: assuming that the attacker intercepted output of a label, and because of the one-way Hash function of the difference of random number R, the attacker cannot be back to this value according to historical data of labels, so this protocol has good forward security [17].

(2) Anti position tracking. Due to the random number R is updated after each change, so in the process of certification, the response $H(\mathrm{ID}_x)$ and $H(\mathrm{ID}_x \| \mathrm{R})$ in the label are different every time, thus effectively preventing the attacker tracking according to the specific output.

(3) Anti hacking attack. Because of the one-way of Hash function, randomness of R

and uniqueness of ID, the attacker eavesdroppers $H(\mathrm{ID}_x \| \mathrm{R}) \oplus \mathrm{H}(ID_y)$ also cannot read.

(4) Anti impersonation attack. Because the fake key lacks the Key, so when the reader asks, will not properly respond the encrypted $H(\mathrm{ID}_x \| \mathrm{R}) \oplus \mathrm{H}(ID_y)$, and will not pass the authentication. So, the protocol has security to the counterfeit attack. The illegal is not informed of the label and reader identification, so it is unable to masquerade as legitimate label and reader [18].

(5) Indiscernibility: towards the tag responding output, due to the use of one-way Hash function random number R, so that even if the attacker gains the output of multiple tags, and also cannot distinguish the output of each one; even getting the output of the same, also cannot distinguish the output of which time of the label.

(6) Anti replaying attack. Because in the communication process, we add the random number R, and each message authentication is new every time, even if an attacker intercepted a message $H(\mathrm{ID}_x \| \mathrm{R}) \oplus \mathrm{H}(ID_y)$ or $\mathrm{H}^*(\mathrm{ID}_x \oplus \mathrm{R})$, he will not simulate the call in next time, effectively prevent the replaying attack [19].

5.2. The Analysis of the Performance Compared with the Last Protocols:

In order to clearly contrast the characteristics of improved new protocol and other protocols in security, the following table gives a detailed comparison. Among them, "+" represent in accord with the requirements; while " — " means disagree with the requirement [20].

Table 1. The Analysis of the Performance Compared with the Last Protocols

Security index protocol	Forward security	Position tracking	impersonation attack
Hash-lock protocol	+	—	—
Randomized Hash-lock protocol	+	+	—
Hash chain protocol	+	+	—
Protocol in our paper	+	+	+

Table 2. The Analysis of the Performance Compared with the Last Protocols

Security index protocol	Indiscernibility	replaying attack
Hash-lock protocol	—	—
Randomized Hash-lock protocol	+	—
Hash chain protocol	+	—
Protocol in our paper	+	+

By analysis in theory, we can find that: random Hash lock protocol and Hash chain protocol all have N amount level computation, which makes the computation amount high, having an effect on the cost and speed of RFID system. While in our new security protocol, the backstage database only need to perform 2N recording search, and once Hash operation. Compared with the existing protocols, the speed of the scheme is more fast, What's more, because the storage capacity of tag is 1L, and also do not need a random number generator, which can greatly reduce the cost of the tag [21].

In addition, because the most computation and location are carried by the backstage database and with high efficiency, tags and readers in this protocol do not need to save identification information, finding the corresponding records and the most calculation process are implemented by the backstage database, with continuously increased number of tag and reader, the computation time of the backstage database increases slowly, therefore, this agreement also can be applied to the situation where number of tag and reader are much.

6. Conclusions

RFID technology is the best expression in pervasive computing idea. It not only has the incomparable advantage than the traditional technology, but also is launched in many new and valuable commercial fields. While the limited computing and storage resources of tags have brought a variety of security problems to RFID, which is also one of the key problems faced by RFID technology in its widely deployed. A lot of researches have been launched to solve these problems, after put into practice, we find that RFID security protocol based on Hash function is an important method in realization and protection of the security of the RFID system, is also one of the hot research topics at present in this field. This paper introduces several now existing security authentication protocols, and according to the deficiency of these protocols putting forward a new and improved security authentication scheme based on Hash function. After test, we prove that this scheme solve the various security and privacy problems existing between reader and tag in FRID sensor networks effectively, has the advantages of lower cost, higher efficiency and higher security. And at last, through the theoretical analysis proves its security properties, which further makes it the higher utility value in practical application.

References

[1] T. F. L. Porta, G. Maselli and C. Petrioli, "Anticollision protocols for single-reader RFID systems: temporal analysis and optimization", IEEE Trans Mobile Comput, vol. 10, **(2011)**, pp. 267-279.
[2] C. Xu, "Application of Multi-information Fusion Positioning Technology in Robot Positioning System", Journal of Multimedia, vol. 9, no. 3, **(2014)**, pp. 271-350.
[3] S. Wu, H. Jiang, D. Feng, L. Tian and B. Mao, "Improving availability of RAID structured storage systems by workload outsourcing", IEEE Transactions on Computers, vol. 60, no. 1, **(2011)**, pp. 64-79.
[4] W. Chunyi and L. Chichung, "A grouping-based dynamic framed slotted ALOHA anti-collision method with fine groups in RFID systems", Proceedings of the 5th International Conference on Future Information Technology, Busan: IEEE, **(2010)**, pp. 1-5.
[5] Y.-H. Shao, N.-Y. Deng and Z.-M. Yang, "Least squares recursive projection twin support vectormachine for classification", Pattern Recognition, **(2012)**.
[6] D. Dui-jian, A. Yong, M. Rong-Zeng and Y. Yue-peng, "Based on the collision of AS3992 Q algorithm analysis and improvement", Journal of sensors and micro systems, vol. 11, no. 03, **(2013)**, pp. 7-10.
[7] F. Shuo, G. Fei, X. Yan-ming and L. Heng, "An improved RFID tag collision algorithm", Microcomputer information, vol. 12, no. 1, **(2011)**, pp. 49-52.
[8] L. Lu, C. Hong-ming and H. Yi-gang, "A new type of RFID joint collision algorithm", Microcomputer information, vol. 26, no. 29, **(2010)**, pp. 145-146.
[9] D. Huifang, L. Jinqiao and D. Chunhui, "RFID multi-tags anti-collision algorithm with adaptive Q leading to the maximum throughput", Proceedings of the Third Pacific-Asia Conference on Web Mining and Web-based Application, Guilin: IEEE, **(2010)**, pp. 166-169.
[10] W. Mingliang and Y. Shun, "Improvement of anti-collision algorithm for RFID system based on TDMA", 2010 international conference on computational problem-solving (ICCP), **(2010)**, pp. 336-342.
[11] H.-T. Ceong, H.-J. Kim and J.-S. Park, "Discovery of and Recovery from Failure in a Costal Marine

USN Service", Journal of information and communication convergence engineering, vol. 10, no. 1, **(2012)**, pp. 11-20.
[12] H.-S. Lee, S.-H. Lee, S.-K. Kim and S.-I. Bang, "Adaptive Group Separation Anti-Collision Algorithm for Efficient RFID System", Journal of the institute of electronics engineers of Korea, vol. 46, no. 5, **(2009)**, pp. 48-55.
[13] W.-Y. Yeo and G.-H. Hwang, "Efficient anti-collision algorithm using variable length ID in RFID systems",ICICE Electronics Express, vol. 7, no. 23, **(2010)**, pp. 1735-1740.
[14] M. R. Rieback, P. N. D. Simpson and B. Crispo, "RFID malware: Design principles and examples", Pervasive and Mobile Computing, **(2006)**.
[15] S. Li, Y. Geng, J. He and K. Pahlavan, "Analysis of Three-dimensional Maximum Likelihood Algorithm for Capsule Endoscopy Localization", 2012 5th International Conference on Biomedical Engineering and Informatics (BMEI), Chongqing, China, **(2012)** October, pp. 721-725.
[16] Y. Geng, J. He, H. Deng and K. Pahlavan, "Modeling the Effect of Human Body on TOA Ranging for Indoor Human Tracking with Wrist Mounted Sensor", 16th International Symposium on Wireless Personal Multimedia Communications (WPMC), Atlantic City, NJ, **(2013)** June.
[17] C.-S. Kim, B.-I. Jang and H.-K. Jung, "Performance Analysis of Anti-collision Algorithm for Tag Identification Time Improvement", International Journal of Software Engineering and Its Applications, vol. 8, no. 3, **(2014)**, pp. 1-10.
[18] L. Zhihan and T. Su, "3D seabed modeling and visualization on ubiquitous context", SIGGRAPH Asia 2014 Posters, ACM, **(2014)**, pp. 33.
[19] L. Zhihan, L. Feng, S. Feng and H. Li, "Extending Touch-less Interaction on Vision Based Wearable Device", Virtual Reality (VR), 2015 iEEE. IEEE, **(2015)**.
[20] L. Zhihan, L. Feng, H. Li and S. Feng, "Hand-free motion interaction on Google Glass", SIGGRAPH Asia 2014 Mobile Graphics and Interactive Applications, ACM, **(2014)**, pp. 21.
[21] C. Zhong, S. Müller Arisona, X. Huang, M. Batty and G. Schmitt, "Detecting the dynamics of urban structure through spatial network analysis", International Journal of Geographical Information Science, vol. 28, no. 11, **(2014)**, pp. 2178-2199.
[22] W. Li, J. Tordsson and E. Elmroth, "An aspect-oriented approach to consistency-preserving caching and compression of web service response messages", Web Services (ICWS), 2010 IEEE International Conference, IEEE, **(2010)**, pp. 526-533.
[23] Y. Geng, J. He and K. Pahlavan, "Modeling the Effect of Human Body on TOA Based Indoor Human Tracking", International Journal of Wireless Information Networks, vol. 4, **(2013)**, pp. 306-317.

Author

Bai Zhi(1975-), was born in HuNan, China, in 1975. Dr. Hunan University, main research field: RFID chip circuit design and anti collision analysis and optimization.

