Proceedings of the 2011 International Conference on Machine Learning and Cybernetics, Guilin, 10-13 July, 2011

MUTUAL AUTHENTICATION PROTOCOL BASED ON HASH FUNCTION OF RFID SYSTEMS

LEI-AN LIU [1], XIAO-ZHENG LAI[2], DA-SHUN YAN[1], ZHI-QIANG CHEN[1], LING YANG [1]

[1]College of Computer Science & Engineering, Zhongkai University of Agriculture and Engineering, Guangzhou 510225, China
[2]School of Computer Science & Engineering, South China University of Technology, Guangzhou 510641, China
E-MAIL: gudu420@163.com

Abstract:

Currently, security and privacy issues of RFID systems cause for growing concern, and have become a hot research topic. Physical mechanisms and cryptographic mechanisms are the two main methods to solve these issues. Among cryptographic mechanisms, hash-based mechanism is a vital kind of solution. Analysis on the existing hash-based mechanisms shows there are a variety of security risks, or they are not very suitable for passive RFID systems. In this paper, based on the analysis of the existing hash-based mechanisms, an improved mutual authentication protocol based on hash function is proposed. Through security and efficiency analysis, we can see that our protocol requires lower resources on readers and tags, and it is suitable for passive RFID systems.

Keywords:

RFID; Authentication; Hash function

1. Introduction

RFID (Radio frequency identification) technology is an important automatic identification technology, which uses electromagnetic fields to transmit signals and has been implemented in many areas. Corresponding to its wider application, the security and privacy issues have become increasingly prominent. If these issues are not solved adequately, they will put great influence on the further promotion and application of RFID systems.

RFID systems are composed of three main entities, reader, tag, and the back-end database. These three pieces come together to form a system where any physical item can be tagged and scanned wirelessly. Tags can be divided into three categories: active, passive and semi-active tags. Active tags have their own battery and are usually used on large items, such as cargo containers, or other items that need to be read from a distance. Therefore, it is more expensive than passive tags and semi-active tags. Semi-active tags are also equipped with a power source, but these tags only use the batteries for powering the chip, not for communication. Semi-active tags have a longer range than passive tags and a longer battery life than active tags. Unlike active tags and semi-active tags, passive tags do not have an independent power source, and they obtain the energy required from the electromagnetic field generated by the reader. Typically, passive tags have a long service life, smaller and lighter than active tags, and their read/write distance is closer. In this paper, the case of passive tags is considered. Although there are some security issues of the reader and the back-end database, they have enough energy and computing resources to use conventional cryptographic algorithms to ensure their safety. On the contrary, RFID tags brought security and privacy issues become particularly prominent, even for passive tags, because they do not have enough resources to run conventional cryptographic algorithms. Furthermore, because the communication channel between the reader and tags is a wireless channel, it is very vulnerable to attacks. An attacker can eavesdrop the information transmitted easily. If the information transmitted is in plain text, it will be completely exposed, and even if the information transmitted is in cipher text, malicious tracking attack can be done when there are no appropriate measures. In a word, because of mutual restraint between RFID security and cost, it is still very difficult to design a secure, efficient, low-cost mutual authentication protocol of RFID systems. This study is aimed to provide a stronger protection to the low-cost passive RFID systems.

2. Security requirements of RFID systems

As mentioned above, typically, as computing power and storage capacity is limited, the conventional cryptographic protocols cannot be used directly in RFID systems. In addition, open communication channel between tags and the reader can be tapped easily. Security requirements of RFID systems are as follows:

978-1-4577-0308-9/11/$26.00 ©2011 IEEE

- *Reliability (Authenticity).* In an open RFID system, the attacker can choose a variety of attacks, such as man-in-the-middle attack, DoS attack, replay attack, etc. In order to ensure the reliability of RFID systems, the attacks should be prevented to the greatest extent possible, and the mutual authentication protocols must be used to ensure the authenticity and legitimacy of tags and readers.
- *Confidentiality.* Some information stored in tags is related to the consumer privacy. A secure RFID system must be able to ensure that the information stored in tags can only be read and written by the authorized reader.
- *Integrity.* Data integrity means that the receiver must ensure that the information received has not been modified or replaced during the transmission process. Typically, digital signatures are used to support data integrity, but because of the limited resources of RFID systems, it is difficult to support these expensive cryptographic algorithms. In RFID systems, message authentication code is often used to support data integrity.
- *Availability.* A reasonable solution for the security of RFID systems should provide various services to the authorized users and unauthorized users should be prohibited. The solution proposed can also be applied in the low-cost RFID systems.
- *Privacy.* Typically, the tag itself does not need to store large amounts of data, but only needs to store its identifier in its memory. Therefore, the attacker is likely to track the tag using its fixed identifier, even when the attacker does not know the encrypted content. By tracking the tag, the attacker can learn its location information. If someone carries such a tag, the malicious holder of the reader can track this person. In some cases, it is very dangerous.

3. Related works

Because the size and cost limitations of RFID tags, the design of the security and privacy solutions of RFID systems is a challenging research work. In order to meet the security requirements in section II, many authentication mechanisms have been proposed at home and abroad [1-12]. According to the security mechanisms, these mechanisms are divided into the physical mechanisms and cryptographic mechanisms.

3.1. Physical mechanisms

Physical mechanisms include Killer tag, Faraday cage, Active interference, and Blocker Tag, etc [13-16]. Killer tag method is proposed by Auto-ID Center. The principle of it is: when the physical entity is sold, the tag attached to it is removed and killed. The tag will lose its function and can not be activated again. Therefore, this method reduces the utilization of the tag. Furthermore, access password of Killer tag method is only 8 bits, so a malicious attacker can get the access of the tag with only 2^8computational cost. As we all know, radio waves can be shielded by the container which is made of conductive material. Faraday cage is such a container. When a tag is put into such a container like Faraday cage, no reader can communicate with it, so do the tag. But using this method, an additional physical device is needed, which will increase the cost of RFID systems. In active interference method, the operations of unauthorized readers are hindered, but some legal RFID systems nearby also may be subject to interference. At last, the misuse of Blocker Tag can lead to denial of service attacks. Also, there is an effective range of Block Tag. Therefore, tags existing beyond the effective range cannot be protected. From the above content, we can see that these existing physical mechanisms are not suitable for practical RFID systems, and can only be used for some particular applications because of their inherent flaws.

3.2. Cryptographic mechanisms

Among cryptographic mechanisms, authentication protocols based on hash function is an important category used in RFID system, which mainly contains Hash-Lock protocol [17], randomized Hash-Lock protocol [18] and Hash-chain protocol [19], etc. Hash-Lock protocol is an access control mechanism based on one-way hash function. The reader stores the key Key of every tag, which is associated with $metaID$, and is satisfied with the following function, $metaID = H(Key)$. During the authentication process, the tag uses $metaID$ to instead of its real ID to avoid the leakage of the information. The specific work process of the protocol is shown in Figure 1.

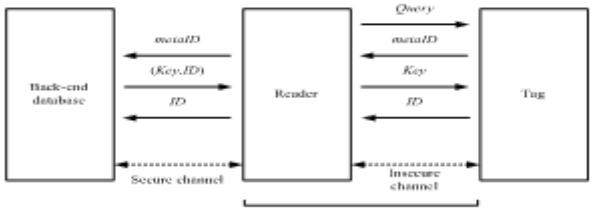

Figure 1. The Work Process of Hash-Lock Protocol

In this protocol, only when $H(Key) = metaID$, the tag sends its *ID* to the reader. Otherwise, the tag will not send its *ID* to the reader. In this way, the illegal reader cannot achieve the information stored in the tag, and the tag cannot be forged too. However, at the beginning of the protocol, when the reader sends *Query* to the tag, the tag will return *metaID* to the reader. So the attacker can still achieve the information of the tag's location by using *metaID*. Besides, the key *Key* is transferred as plaintext through the insecure channel, so it can be captured by the attacker easily. Finally, the *ID* is also transferred as plaintext through the insecure channel, so it can also be captured easily which can be used by the attacker to forge the tag.

As in the Hash-Lock protocol, each time the reader sends a query to the tag, the tag returns the same *metaID* to the reader, which results in tracking problem. In order to overcome this shortcoming, S. A. Weis, et al. proposed a randomized Hash-Lock protocol. The specific work process of the protocol is shown in Figure 2.

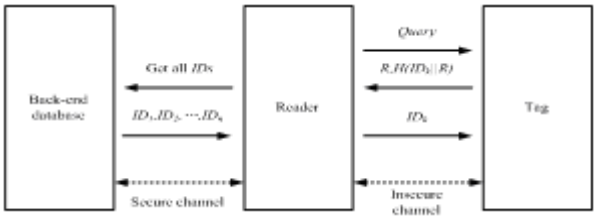

Figure 2. The Work Process of Randomized Hash-Lock Protocol

In this protocol, each time the reader sends a query to the tag, the tag generates a random number *R*. The tag uses this random number *R* and its ID_k to compute with a hash function, and then sends the result to the reader. At each time, the random number is different, so the tracking attack can be avoided. But there are still some flaws in this protocol. Firstly, because the tag needs to generate random numbers, so there must be random number generator in the tag, which will increase the cost of the tag significantly. Secondly, although the location privacy issues have been resolved, because the key and *ID* are all fixed, the attacker can still capture the information by eavesdropping and replay attack and then forge the tag. Finally, this method is not suitable for the case of a large number of tags. Because when the number of tags is large, the calculation of the reader increases sharply, and which will lead to the reducing efficiency and increasing delay of RFID systems.

Ohkubo M. et al proposed a Hash-chain protocol, which is shown in Figure 3 and Figure 4. In this protocol, tags integrate two hash functions, *G* and *H*. The initial value S_1 is stored in the tags and the back-end database. Meanwhile, the back-end database also stores the *ID* numbers of all the tags. For more details, we can see the paper [19].

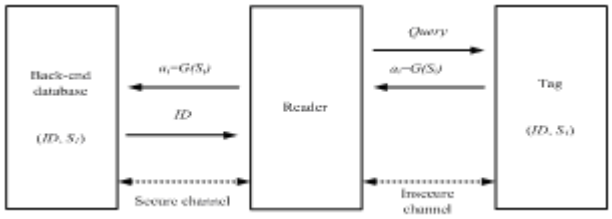

Figure 3. *Tag-to-reader* Authentication Process

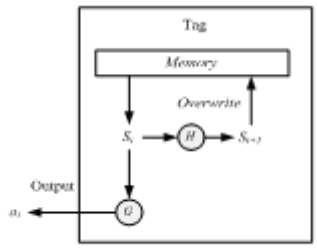

Figure 4. The Update Process of ID Numbers of Tags

In this protocol, the ID number of a tag is updated after a complete authentication process to meet indistinguishability and forward security. But in this protocol, when the tag response to the authentication request, it can not verify the identity of the reader. So when an unauthorized reader sends an authentication request to the tag, the tag will response to it too and an attacker can use this information to deceive the system. In addition, tags need to make two different hash operations, which increase the cost of tags. Furthermore, during each authentication process, each *ID* number must be calculated and compared by the back-end database. So when the number of tags increases, the load of the back-end database will be increased greatly and the efficiency of the system will be decreased sharply and also the system delay will be increased significantly.

4. Proposed protocol and it's security analysis

Analysis of Hash-Lock protocol, randomized Hash-Lock protocol and Hash-chain protocol shows that these protocols have some potential safety problems. In order to solve these problems, we propose a new kind of authentication protocol which is also based on hash function.

4.1. Prior conditions and assumptions

In our protocol, there are two assumptions, one is the channel between the reader and the tag is insecure and the channel between the reader and the back-end database is secure, and the other is tags considered in this paper is passive tags which have very few computing resources. The following notations are used:

r : Random number generated by the reader.

ID_k : ID number of tag *k*.

$H()$: Hash operation.

$||$: Concatenation operation.

At the beginning, each tag stores its *ID* in its memory and integrates a hash function *H*. There is a random number generator in the reader. A pair of data $(ID_k, H(ID_k))$ *(k=1…n, n is the number of tags)* are stored in the back-end database. The back-end database can carry out all kinds of complex operations needed.

4.2. Description of the proposed protocol

The specific work process of the proposed protocol is shown in Figure 5.

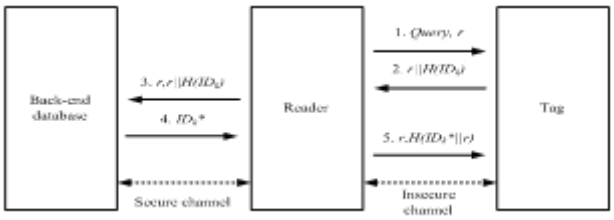

Figure 5. The Work Process of The Proposed Protocol

The work process of the proposed protocol is as follows:

1) Reader generates a random number *r* and sends *r* and *Query* to the tag;
2) The tag uses its *ID* and the number *r* received to calculate and gets the value $r \| H(ID_k)$, and then sends this value to the reader;
3) The reader sends the random number *r* and $r \| H(ID_k)$ to the back-end database;
4) The back-end database uses *r* and the $H(ID_k^*)$ saved to calculate and try to find whether there is a $H(ID_k^*)$ which satisfies the equation $r \| H(ID_k^*) = r \| H(ID_k)$ or not. If $r \| H(ID_k^*) = r \| H(ID_k)$, it means that the tag is a legal one. The *reader-to-tag* authentication process is successful. The back-end database sends ID_k^* to the reader;
5) The reader sends r and $H(ID_k^* \| r)$ to the tag. The tag uses its ID and the received number r to calculate and finds whether $H(ID_k \| r) = H(ID_k^* \| r)$ or not. If the equation is satisfied, it means that the reader is a legal one. The tag-to-reader authentication process is successful. Until now, the mutual authentication process is completed.

4.3. Safety analysis of the proposed protocol

From the work process of the proposed protocol, we can see that the proposed protocol in this paper has all the security features that randomized Hash-Lock protocol has. So it can resist all forms of attack effectively. More detailed analysis will be conducted as follows:

1) The tag does not need to generate random numbers, so the cost of the tag is reduced;
2) The calculation of the reader decreases sharply, and which will improve the efficiency of RFID systems. Reader only requires one time hash calculation in each session, and more calculations are done by the back-end database. Typically, the computing power of the back-end database is very powerful. Therefore, even when the complex calculations are done by the back-end database, it will has less impact on system efficiency;
3) Forward security. As the participation of the random number *r*, the proposed protocol can guarantee the information of each communication between the reader and tags is different. Also, the hash function *H* is a one-way function, so even if the attacker obtains the current data $r \| H(ID_k)$, the historical data of the tag cannot be obtained;
4) Location tracking. In the proposed protocol, the response message of the tag changes in every session and the output of the hash function *H* is unpredictable. So location tracking is impossible.
5) Eavesdropping. Throughout the protocol, the values the adversary can acquire via eavesdropping are r, $r \| H(ID_k)$, $H(ID_k^* \| r)$. Because the random number r changes in every session, it is useless to eavesdrop it. Moreover, $r \| H(ID_k)$ and

$H(ID_k^* \| r)$ are protected by the hash function, so they cannot be exposed by simple eavesdropping. Therefore, this proposed protocol is secure against eavesdropping;

6) Replay attack. As the random number r changes in every session, even if the adversary has acquired the messages of the previous session, it is impossible to obtain authentication from the legitimate reader;
7) Spoofing. As the adversary cannot acquire the *ID* number of the tag, it cannot be disguised as a legitimate tag to communication with the reader. Meanwhile, because of the *tag-to-reader* authentication, the adversary cannot be disguised as a legitimate reader too;
8) Indistinguishability. As the proposed protocol uses the random number r as well as one-way hash function H, it is impossible to anticipate the response message of the tag in every session. Furthermore, it is secure against intended and meaningless requests of an adversary, so it guarantees Indistinguishability.

4.4. Comparison with other existing hash-based protocols

In order to explain the advantages of the proposed protocol more clearly, a comparative analysis of safety and efficiency between the proposed protocol and other existing hash-based protocols is done, as is shown in Table 1 and Table 2. In Table 1, "√" means that the protocol has the properties, and "×" means not.

Table 1. Comparison of Safety Performance

Protocol	Indistinguish-ability	Forward security	Against location tracking	Against eavesdropping	Against replay attack	Against Spoofing
Hash-Lock protocol	×	×	×	×	×	×
Randomized Hash-Lock protocol	√	√	√	×	×	×
Hash-chain protocol	√	√	√	√	√	×
The proposed protocol	√	√	√	√	√	√

A good mutual authentication protocol of RFID systems not only needs to solve security issues, but also needs to consider the consumption of resources. The good protocol does not require RFID tags having a large storage capacity and powerful computing power, which will greatly reduce the cost of tags. Therefore, the total cost of RFID systems will also be reduced greatly, which will facilitate large-scale application of RFID systems. For convenience, we assume the number of tags is n, and the length of one tag is L (The length of all the tags is the same). In Table 2, T_H is the number of hash operations, $T_{\|}$ is the number of concatenation operations, and T_r is the number of r generated by the reader. From Table 2, we can see that in each session of the proposed protocol, the number of computing time of the reader is "$1T_H$, $1T_r$" and more calculations are done by the back-end database, which will improve the efficiency of the entire system compared with Randomized Hash-Lock protocol. Meanwhile, the tag does not need to generate random numbers and only needs to store its ID, so the cost of the tag is reduced. Although compared with Hash-Lock protocol and randomized Hash-Lock protocol, the tag needs to double the hash operation, which is aimed to ensure the security of the whole system. On the whole, the proposed protocol in this paper is better than other existing hash-based protocols.

Table 2. Comparison of Efficiency

Protocol	Computing time			Storage capacity		
	Tag	Reader	Back-end database	Tag	Reader	Back-end database
Hash-Lock protocol	$1T_H$	-	-	$2L$	-	$3nL$
Randomized Hash-Lock protocol	$1T_H$, $1T_r$	nT_H	-	$1L$	-	nL
Hash-chain protocol	$2T_H$	-	$2nT_H$	$1L$	-	$2nL$
The proposed protocol	$2T_H$	$1T_H$, $1T_r$	$nT_{\|}$	$1L$	-	$2nL$

5. Conclusions

Research on the security issues of RFID systems is of great significance. Only the security problems of RFID systems are resolved, can it be applied more widely. Nowadays, there are two kinds of mechanisms to solve these security problems, physical mechanisms and cryptographic mechanisms respectively. Compared with physical mechanisms, cryptographic mechanisms are more effective. Mutual authentication protocol based hash function is a main kind of mutual authentication protocol in RFID systems. In this paper, we proposed a new kind of mutual authentication protocol based on hash function. From the analysis, we can draw a conclusion that the proposed protocol is more effective. In our protocol, we assume that the channel between the reader and the database is secure, but in fact, in many real RFID systems, this assumption is not correct. In addition, we do not consider the ownership transfer problems. In our further work, we will take into account these factors.

Acknowledgements

This paper is supported by the National High Technology Research and Development program (863 program) of China (2008AA04A103) , Guangdong university outstanding young innovative personnel training project, China (LYM10089), the Natural Science Foundation of Guangdong Province, China (9151022501000008) and the Science and Technology Planning Project of Guangdong Province, China (2010B080701001 and 2010A020507001-80).

References

[1] H. Mobahat, "Authentication and lightweight cryptography in low cost RFID", 2010 2nd international conference on software technology and engineering, V2, pp. 123, 2010.

[2] Wang Shaohui, Wang Faxing, "Security analysis of some RFID authentication protocols", 2010 2nd international conference on e-Business and information system security, pp. 1-4, 2010.

[3] L. Kulseng, Zhen Yu, and Yawen Wei, et al, "Lightweight mutual authentication and ownership transfer for RFID systmes", INFOCOM, pp. 1-5, 2010.

[4] Chih-Hung Wang, Shan Chin, "A new RFID authentication protocol with ownership transfer in an insecure communication environment", 2009 9th international conference on hybird intelligent systems, pp. 486-491, 2009.

[5] Rotter, P., "A Framework for Assessing RFID System Security and Privacy Risks", Pervasive Computing, IEEE, 7(2), pp. 70 – 77, 2008.

[6] Soo-Young Kang, Deok-Gyu Lee and Im-Yeong Lee, "A study on secure RFID mutual authentication scheme in pervasive computing environment", Computer Communications, 31(18), pp. 4248-4254, 2008.

[7] Selwyn Piramuthu, "Protocols for RFID tag/reader authentication", Decision support systems in integrated decision support, 43(3), pp. 897-914, 2007.

[8] G. Tsudik, "YA-TRAP: yet another trivial RFID authentication protocol", 4th annual IEEE international conference on pervasive computing and communications workshops, pp.640-643, 2006.

[9] J. Yang, J. Park, and H. Lee et al, "Mutual Authentication Protocol for Low-Cose RFID", Proc. of the workshop on RFID and lightweight cryptography, pp. 17-24, 2005.

[10] S. Karthikeyan, M. Nesterenko, "RFID security without extensive cryptography", Proc. of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 63-67, 2005.

[11] J. Saito, K.Sakurai, "Grouping Proof for RFID Tags", Proc. of the 19th international comference on advanced information networking and applications, pp. 621-624, 2005.

[12] D. Henrici, P. Muller, "Hash-based enhancement of location privacy for radio-frequency indentification devices using varying identifiers", Proc. of the 1st international workshop on pervasive computing and communication security, pp. 149-153, 2004.

[13] Auto-ID Center, "860MHz-960MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical communication Interface Specification Proposed Recommendation Version 1.0.0", Technical Report MIT-AUTOID-TR-007, NOV, 2002.

[14] Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Faraday Cage.

[15] T.Hjorth, "Supporting privacy in RFID systems", master thesis, 2004.

[16] Ari Juels, Ronald L Rivest, and Michael Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy", proceedings of the 10th ACM conference on computer communication security, pp. 103-111, 2003.

[17] S. Weis, "Security and Privacy in Radio Frequency Identification Devices", Massachusetts Institute of Technology (MIT), Massachusetts, USA, 2003.

[18] S. A. Weis, S. E. Sarma, and R. L. Rivest et al, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Inter. Conf. on Security in Pervasive Computing-SPC 2003, pp. 454-469, 2003.

[19] Ohkubo M., Suzuki K., Kinoshita S., "Hash-chain based forward-secure privacy protection scheme for low-cost RFID", Proc. of the 2004 Symposium on Cryptography and Information Security, pp. 719-724, 2004.