Security In the Internet of Things Based on RFID: Issues and Current Countermeasures

Xiao Nie
College of Information Engineering
Guangdong Jidian Polytechnic
Guangzhou, China
brenner@21cn.com

Xiong Zhong
College of Information Engineering
Guangdong Jidian Polytechnic
Guangzhou, China
8977220@qq.com

***Abstract*—In recent years, the internet of things (IOT) has been a focus of research. RFID (Radio Frequency Identification) as a core technology of the IOT also attracted the attention of industry and academia. Security is the key issues for emerging applications of the IOT based on RFID. In order to promote the development of this emerging domain, we firstly in brief introduce the IOT system based on RFID including the components and the work process, and then by means of deeply analyzing the security issues in the IOT based on RFID from two aspects: security features and security threats, we summarize the security issues of RFID into the RFID system security and the communication security. On the basis of these, we discuss the current countermeasures for the security of RFID. In the RFID system, for privacy protection and anti-interference, the corresponding technologies are praised such as Tag killing, Tag sleeping and Tag blocking; in the communication process, the authentication based on HASH is the main method.**

Keywords-the internet of things; RFID; security; untraceability; attacks

I. INTRODUCTION

Nowadays, the "Smart Earth" and the "Experience China" as popular words are widely known, along with the high attention of the governments and the rapid development of related technology, we have approached the era of the IOT (the internet of things). The internet of things refers to a way of connecting objects to the Internet for the purpose of intelligent control and management. The objects are sensed through RFID (Radio frequency identification) or sensors achieving the integration of human society and the information system.

RFID is the core technology to implement the internet of things. So the security issue of RFID is becoming more and more important, in the past decade, a large number of research papers dealing with security issues of RFID technology have appeared. Literature [1] [2] [3] [4] summarized the security issues in the internet of things based on RFID, literature [5][6] paid attention to the privacy models for RFID, literature [7] explained mobile RFID network based on EPC and analyzed threats of the mobile RFID system, this is important to create a secure IOT architecture, literature [8] analyzed RFID technology and its Applications in Internet of Things (IOT) from different layers, the standard of the RFID and the authentication scheme was discussed separately in [12] and [13].

In this paper, we will first introduce the IOT based on RFID in section Ⅱ, then we analyze the security issues in the IOT based on RFID in section Ⅲ, and on the basis of these, we will give the current countermeasures for the security of RFID in section Ⅳ.

II. THE INTERNET OF THINGS BASED ON RFID

A. *The components of the system*

The typical internet of things based on RFID is composed of three major components including RFID system, middleware system and Internet system.

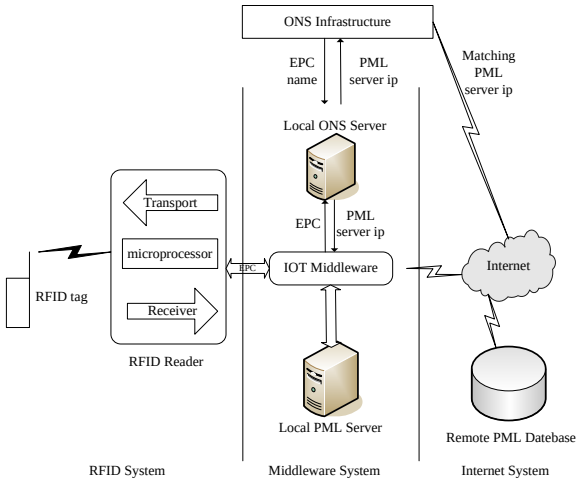

Figure 1. Woking process of IOT based on RFID

RFID system is composed of tags, readers, and antennas. RFID tags are inexpensive wireless devices which can communicate with RFID readers [5]. The sole EPC (Electronic Product Code) saved in each RFID tag is used to identify a target. The reader consists of transport , receiver and microprocessor, which is responsible for reading or writing tag information. The antennas play a role in transmitting radio-frequency signal between the RFID tag and the reader.

The middleware system is called Savant system including Savant server, physical markup language (PML) server, Object naming service (ONS) server.

Internet system usually consists of computer system and network server including PML database etc.

B. How it works

In the internet of things based on RFID, RFID reader is responsible for collecting data from RFID tag with sole EPC code. Through this EPC code the middleware system can find corresponding IP address from the ONS infrastructure on the internet, thereby the relevant information of the object can be obtained from this address. Then the middleware system (Savant system) can process and manage the information. In this process there are local ONS server, local PML server and remote PML server which are in charge of data storage, as shown in the Figure 1.

III. SECURITY ISSUES IN THE IOT BASED ON RFID

A. Security feature

According to the working process of IOT based on RFID, we summarize the security feature in the following.

1) RFID system

In the RFID system, the RFID tag is possible to leak sensitive information of the owner to the unauthorized reader, so the encryption is to be needed to ensure confidentiality; The RFID reader should confirm the information is transported from correct tag, which needs mutual authentications of the reader and the tag. To protect the data integrity, we need to make sure the information hasn't been tampered with during the transmission. Last but not least, RFID system should be able to resist denial of service attack (DOS) and protect users' privacy.

2) Middleware system

In the middleware system, the main security goal is to protect the communication security between the RFID reader and the database server. Meanwhile the database server should be protected to prevent DOS attack. This is a traditional security issue.

3) Internet system.

In the internet system, the traditional network security problems are needed to be solved, for example, how to protect the database from being destroyed and how to guarantee the confidentiality and integrality of data in internet.

B. Security Threats

Through the analysis of the security features in above, we can draw a conclusion: the security issues can be summarized into two aspects. One is the RFID system security including the RFID tag and the RFID reader, the other is the communication security between the RFID reader and the RFID tag and between the RFID reader and the database server. Now we will discuss the security threats from the two aspects, as shown in TABLE I.

TABLE I. THE SECURITY THREATS AND THEIR REASONS

Security threats		The reasons
RFID system	Abuse of tags(tag cloning)	The weakness of tags
	Reader risks	The weakness of readers
	Personal privacy leak	traceability and identification of the tags
	Signal interference	Interference between the tow adjacent band
Communication security treats	Wireless communication risks(search, intercept, monitor, and jam wireless communication signals)	the openness of the wireless signals
	wired communication risks	The openness of the internet
	Denial of Service (DOS)	Malicious attackers

1) RFID system security threat

a) Abuse of tags

RFID tag is small and relatively cheap, and it can be embedded into any object of the users. So it is very difficult to establish security protection system. These weaknesses of the tags will lead that the abuse of tags. For example, the tags can be illegal used by unauthorized users, and when communicating with RFID readers, RFID tags will send a unique *Electronic Product Code* (EPC), this EPC may be collected by attackers, which leads to the tags will be cloned.

b) Readers risks

Once the RFID readers are controlled by an attacker, they can emit the specific electromagnetic wave to destroy the data in the RFID tag.

c) Personal privacy leak

When the tag is scanned, users cannot always know that, this means the tag is tracked without control. Furthermore, since the EPC number in the tag is unique, it is still easy for an attacker to recognize and track tags. In conclusion the traceability and identification of the tags can lead to personal privacy leak.

d) Signal interference

The RFID system adopts two frequency signals including low-frequency signal (125kHz, 225kHz, 13.65MHz) and high-frequency signal (433MHz, 915MHz, 2.45GHz, 5.8GHz), so there is signal interference between the two adjacent band. The signal interference will lead to the data error in the communication between the reader and the tag.

2) Communication security treats

a) Wireless communication risks

In RFID system wireless communication is adopted between the RFID readers and RFID tags. Due to the openness of the wireless signals, it is very easy for an attacker to search, intercept, monitor, and jam wireless communication signals. So encryption and authentication are needed to protect the wireless transmission between the RFID readers and RFID tags.

b) Wired communication risks

Between the RFID readers and the middleware system, data transmission is through the internet. Just like traditional network connection, a serial of security measures will be adopted for assuring the data confidentiality and integrity, and the normal network connection.

c) Denial of Service (DOS)

In both of wireless and wired communication, there are Denial of Service (DOS) . Once attackers control a large number of fake readers and tags, they can make the data

connection to abuse computational resources, and even use up the resources and network bandwidth.

IV. CURRENT COUNTERMEASURES FOR THE SECURITY OF RFID

Now, according to the above threats, we will look into the current countermeasures for the security of the IOT based on RFID, and further detail on privacy protection, mutual authentication between tag and reader(and between reader and database), secure key exchange, and so on.

A. Aiming at RFID system

1) Privacy protection

a) Tag Killing

Tag killing is one of the simplest approaches for the privacy protection. The kill command can put the tag out of action when the users purchased the objects on the points of sale. This method can prevent the tag from being tracked and being carried. Thereby the privacy of the purchasers is protected. Moreover, when the consumers need the tag, they are no use because the operation of killing tag is irreversible. Thus, the scheme of simple execution of killing tags is not feasible.

b) Tag sleeping[10]

As the above, tag killing offers consumers privacy effectively, but it will drop the function of RFID. So we should adopt better method to protect the privacy of the consumers. That is tag sleeping. When the tag needn't to be tracked, it is temporarily put to sleep, when needed it is to be waked up.

c) Blocking tags

Literature [11] proposed a concept called "blocker tags" and established a privacy protection schema with the use of "selective blocking". As a special RFID tag, a blocker tag can stop unwanted scanning of tags in the privacy zone. In this way, instead of killing tags or sleeping tags, the tag will be blocked. This means that there is a modifiable flag bit in the tag. When the bit is set to 1, the tag is not able to be scanned and tracked.

To protect the privacy of the end users, many researchers have proposed other constructive method, such as relabeling approach, re-encryption and "Minimalist" cryptography in [10].

2) Anti-interference [4]

There are three anti-interference measures in the RFID system including data coding, data coding and data integrity check, multiple retransmission and eliminating the false data.

B. Aiming at communication process

1) Authentication

a) Hash-Lock

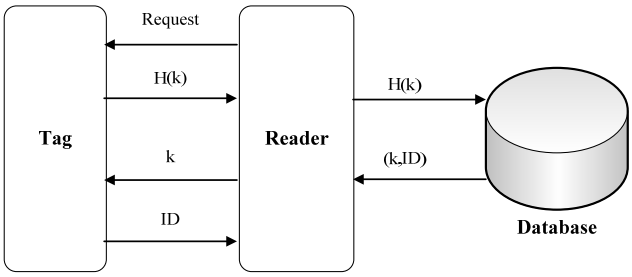

Figure 2. Hash-Lock authentication

This scheme is based on one-way hash function. As shown in figure 2, when the RFID reader sends the request to the tag, the tag will return the H(k), the k is shared key between the tag and the reader, then the reader gets the (k,ID) from the database according the H(k) and sends k to the tag, the tag calculates H'(k) using the k received from the reader, if H(k) and H'(k) is equal, the tag will return ID to the reader. In this way, using H(k) to replace real tag ID prevents the tag being tracked. [1][10]

b) Randomized Hash-Lock

This method is based on random numbers. When receiving the request from the reader, the tag will return a unfixed H(k||R) instead of H(k) , this R is a random number and k is shared key between the tag and the reader. The process is shown in figure 3.

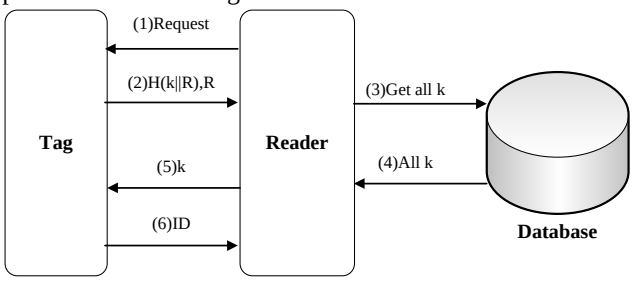

Figure 3. Randomized Hash-Lock authentication

c) Hash Link

Essentially it is based on inquiry/answer mechanism with shared secret. When using two readers with different hashing functions to initiate authentication, the tag always sends different responses. In this agreement, the tag becomes an active tag with independent ID update ability.

d) Other authentication scheme.

Literature [1] listed other authentication based on hash such as ID exchange and distributed RFID Challenge/Answer Authentication. In [9], a security authentication mechanism based on the eID security platform was proposed, and literature [14][15][16] did a lot of work on the RFID security protocols.

2) Protecting the share key

The authentication based on hash needs the share key in the both sides. So it is clearly that protecting the share key is important in the process of authentication. The share key is saved in the tag and in the database of the RFID

reader. Wherever the share key is saved, the encryption is necessary, besides dynamic share key is another method.

To sum it up, the current countermeasures for the security of IOT based on RFID is shown as TABLE II.

TABLE II. THE SECURITY TARGET AND THE CORRESPONDING SOLUTION

Security target		Security Solution
RFID system	Privacy protection	Tag killing Tag sleeping Tag blocking Relabeling Re-encryption
	Anti-interference	Data coding Data coding and data integrity check Multiple retransmission and eliminating the false data.
Communic-ation process	Mutual Authentication	Hash-Lock Randomized Hash-Lock Hash Link ID Change based on hash Distributed RFID Challenge/Answe
	Protecting the share key	Encryption Dynamic share key

V. CONCLUSION

In the past few years, the internet of things has been attracting a great deal of attention, and as the core technology in the sensor layer of IOT, RFID similarly will attract the significant interest for the years to come. In this article, we concisely reviewed the security issues in the IOT based on RFID, and analyzed security features and threats, then we discussed the current countermeasures in this field. From the RFID system and the communication process we give the corresponding solution to the security target. All in all facing the security challenges in the IOT based on RFID, we have a long way to go.

ACKNOWLEDGMENT

Special thanks to the teaching team in Guangzhou.

REFERENCES

[1] Shao Xiwen, “Study on Security Issue of Internet of Things based on RFID,” Proc. IEEE 2012 Fourth International Conference on Computational and Information Sciences(ICCIS), IEEE Press, Aug. 2012, pp. 566–569, doi:10.1109/ICCIS.2012.301.

[2] Dang Nguyen Duc; Hyunrok Lee; Konidala, D.M.; Kwangjo Kim “Open Issues in RFID Security”, in Proc. Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference, Nov. 2009, pp.1-5.

[3] Khoo, B. ,“RFID as an Enabler of the Internet of Things: Issues of Security and Privacy”, in Proc. 2011 4th International Conference on Cyber, Physical and Social Computing, pp. 709 – 712, doi: 10.1109/iThings/CPSCom.2011.83

[4] LI U Li min , X IAO De bao, LI L in , SH UI Hai hong “Information Security and Its Countermeasures of RFID System of Internet of Things Sensing Layer”, JOURNAL OF WUHAN UNIVERSITY OF TECHNOLOGY, Vo l. 32. No. 20. Oct. 2010, pp.79-87.

[5] Ton van Deursen, “50 Ways to Break RFID Privacy,” IFIP AICT(Advances in Information and Communication Technology) Vol. 352, pp. 192–205, 2011.

[6] Serge Vaudenay ,“On Privacy Models for RFID”, Advances in Cryptology – ASIACRYPT 2007, Lecture Notes in Computer Science Vol. 4833, pp. 68-87, 2007.

[7] Tao Yan, Qiaoyan Wen ,“A Secure Mobile RFID Architecture for the Internet of Things”, Proc. IEEE Information Theory and Information Security (ICITIS), IEEE Press, Dec. 2010 ,pp.616 – 619, doi: 10.1109/ICITIS.2010.5689514.

[8] Xiaolin Jia, Quanyuan Feng, Taihua Fan, Quanshui Lei,“RFID Technology and Its Applications in Internet of Things (IOT)”, in Proc. 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), April 2012, pp. 1282 – 1285.

[9] Chen Bing, Dai Yuebo, Jin Bo, Zou Xiang, Zhou Lijuan “The RFID-based Electronic Identity Security Platform of the Internet of Things”, in Proc. 2011 International Conference on Mechatronic Science, Electric Engineering and Computer, pp. 246 – 249, doi: 10.1109/MEC.2011.6025447

[10] Pateriya, R.K.; Sharma, S. “The Evolution of RFID Security and Privacy:A Research Survey”, in Proc. Communication Systems and Network Technologies (CSNT), June 2011,pp. 115 – 119, doi: 10.1109/CSNT.2011.31

[11] Juels, R. L. Rivest, and M. Szydlo, “The blocker tag: Selective blocking of RFID tags for consumer privacy,” in Proc. 8th ACM Conf. Comput. Commun. Security, V. Atluri, Ed., 2003, pp. 103–111.

[12] Korkmaz, E.; Ustundag, A.,“Standards, Security & Privacy Issues about Radio Frequency Identification (RFID)” ,RFID Eurasia, 2007 1st Annual, pp. 1-10, doi: 10.1109/RFIDEURASIA.2007.4368148

[13] Kai Fan, Jie Li and Hui Li “ESLRAS: A Lightweight RFID Authentication Scheme with High Efficiency and Strong Security for Internet of Things”, 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems, pp. 323 – 328, doi: 10.1109/iNCoS.2012.48

[14] Ton van Deursen, Sasa Radomirovi,“Security of RFID Protocols -A Case Study”, Electronic Notes in Theoretical Computer Science 244 (2009) 41–52

[15] Ranasinghe, D.C. , Cole, P.H. ,“Confronting Security and Privacy Threats in Modern RFID Systems”, in Proc. 2006. ACSSC '06. Fortieth Asilomar Conference, Oct. 2006, pp. 2058 – 2064.

[16] Mubarak, M.F.; Manan, J.A.; Yahya, S.,“A Critical Review on RFID System towards Security, Trust, and Privacy (STP)”, proc. IEEE 7th International Colloquium on Signal Processing and its Applications, IEEE press. March 2011, pp. 39 – 44, doi: 10.1109/CSPA.2011.5759839