International Journal of Database Theory and Application
Vol.9, No.10 (2016), pp.19-32
http://dx.doi.org/10.14257/ijdta.2016.9.10.03

Key Technology Development and Application of High-Security UHF RFID Systems

Pan Tiejun[1], Zheng Leina[2], Wang Ming[3] and Zhu Xiaodong[4]

[1,3]Ningbo Dahongying University
*[*2]Corresponding Author Zhejiang WanLi University*
[4]Zhejiang Fengkun Ltd.
[1]pantiejunmail@126.com, [2]mdsryx@126.com, [3]48342084@qq.com,
[4]ttxnttw@126.com

Abstract

Threats in Internet of things are ubiquitous such as counterfeiting, product piracy and product recall. China is no exception to this trend. The reader SoC (system on chip) chip of Ultra high frequency (UHF) Radio Frequency Identification is the key technology to solve these threats. Due to RF technology, tag data is read and written through wireless transmission directly in the air. In order to avoid tag theft and related backstage database attack, we provide UHF High Security System (UHS-HSS) to prevent the tag data monitoring in third party equipment. UHF-HSS regard UHF RFID reader SoC chip technology as the technology foundation provides chip level security solutions, system level information security service and industry level security applications for the IOT. This paper introduces a complete set of software platforms based on UHF RFID sensors including the underlying Linux operating system and related device driver, IOT platform technology, RFID middle-ware technology and software platform application. It solves the critical problem of security and reliability of UHF RFID applications for the national economy, which is of a great significance for the development of China's Internet of Things technology.

Keywords*: Ultra high frequency RFID, IOT platform, UHF- HSS, security solutions*

1. Introduction

UHF technology has been widely used in recent years, regarded as the most advanced fourth generation of automatic identification technology. It has the advantages of long identification distance, high-recognized rate, quick reading speed, strong anti-interference ability and long serving life. In addition, it can penetrate the nonmetal materials, which has a wide range of use. It is a new management method for automatic acquisition of characteristic data from the object's attribute, status and number in order to realizing digitization and informationization [1]. The typical architecture for UHF application system is composed of UHF tag, which is embedded or attached to an object, UHF reader, antenna and server. UHF tags known as electronic tags are mainly used to store marked data information. The core of UHF tag is an integrated circuit with the function of transmitting and storing information of an object's attribute, status, number *etc.*, whose storage capacity is 1024 bits or more. The electronic tag is usually installed without metal shielding perspective on the surface of the object. Reader is used to read or write data to tag, which meets the need for fast and accurate automatic recognition for moving objects or persons. Its main functions include ①Data is written in the blank tags. ② Reading all kinds of data stored in the tags. ③ Modify or rewrite data in the tags. Antenna is connected to reader mainly sending and receiving data from the tag. [2] Server always provides backend services, including security services such as SSL, encryption *etc.* SoC is the core technology of UHF reader under the present RFID security framework using

ISSN: 2005-4270 IJDTA

encryption for recognizing identification codes and processing memory data. Besides, it transmits energy to electronic tags through antenna, and transmits data through the network to the back-end database safely and reliable. It is the core chip with the most intensive technology and patent in IOT system. Therefore, it is necessary to establish the trust platform system (TPS) for UHF RFID based on PKI mechanism and SoC technology. [3]

2. Background

In the Internet of things technology, Ultra high frequency (840MHz-960MHz) RFID is the main developing direction because of its higher data transmission rate, longer communication distance, lower cost, identifying multiple tags in high moving speed, and flexible coding system. UHF system is widely used in intelligent logistics, intelligent transportation, intelligent home, food and drug security traceability, national defense and other fields for realizing automation and visualization of process control, reducing operation costs, improving operational efficiency, strengthening the quality, which is helpful of developing of traditional industries, increasing the intelligent level of social management, citizen life and public service [4].

Ultra high frequency RFID's current standards, such as EPC C1G2 (American Standard), ISO 18000-6B/6C (International Standard) and ETSI EN 302 208-1 (European standard), are set by the European and American companies. America Company Impinj in addition to the dominance of EPC C1G2 and ISO 18000-6C standard respectively accounts for 86% of the world's reader SoC chip (IndyR1000/R2000), 63% of tag chip and 25% of the reader market. The other three providers of SoC chip of reader are the Microsystems in Austria, the TriQuint in USA, and the Phychips in Korea. With the establishment of the basic technical standards in different countries, one neglected but particularly important issue is placed in front of the whole industry that how to effectively prevent the tag data monitoring in third party equipment in order to avoid the theft of the tag-related backstage database. The Ultra high frequency RFID data encryption technology in China has become more and more urgent in all walks of life. In China's national defense applications, although the Chinese army standard has not provide specific scheme, it explicitly supports the Ultra high frequency RFID data security encryption mechanism and stipulates that military services have to set up their own data encryption system to ensure the absolute security of defense data. [5]

Due to its single product tags, the amount of UHF tag is very huge. Thus, except the data storage function, other functions are as simple as possible, the cheaper the better. At present, the foreign manufacturer's tag cost can be achieved 4 cents (about 0.20 Yuan). Meanwhile, as the passive UHF tag's energy is provided by the reader's wireless transmitter, the limited power supply cannot support the complex algorithm. Furthermore, an active tag's battery life is also limited otherwise the cost of the active tag will increase exponentially. Therefore, it is not a solution to directly add security encryption circuit in UHF tag whose cost is such sensitivity. So that, It is impressive to improve the security of data encryption mechanism for developing a set of UHF RFID High-Security System (UHF-HSS). [6]

UHF-HSS integrates reader SoC chip technology, multi-level data security encryption and authentication methods to establish a series of technical platform covering RFID reader, label, terminal, cloud services and Big data centers, senior security encryption, authentication, tag read write algorithm, tag data dynamic encryption and so on to solve the reliability and accuracy of data operation, the security of data transmission and the leaks during data interception. At the meantime, it aims to continuously meeting the low cost requirement of electronic tag in order to further promote usage of the Ultra high frequency RFID in various fields of the national economy, and to provide high security solutions in the chip level and information security service in the system level. By the

error control coding, dynamic symmetric key authentication and other technical innovations, UHF- HSS solves the serious security problem of UHF RFID widely application, reliability problem of tag information wireless transmission and is expected to reduce the wafer cost by 30%. [7]

UHF- HSS focus on the development technologies of error control coding, data encryption mechanism and dynamic symmetric key authentication, ensuring the network security and the reliability on chip level, module level and system level, in order to innovate the world leading UHF RFID Internet of things technology overall solution platform.

3. UHF-HSS Framework

UHF-HSS supports the Chinese national standard "Information technology, radio frequency identification of 800/900MHz air interface protocol" (GB/T 29768-2013) and the military standard "Protection RFID Air Interface". Besides, through the data encryption module, it develops a set of security and encryption mechanism to ensure Chinese IOT information security. Furthermore, by the error control coding technology, it solves the long troubled technical defects in the UHF RFID application of the reliability of multi tag recognition, and greatly improves the reading efficiency and distance. On the premises of the integration of dynamic symmetric key authentication technology and the requirement of meeting the electronic tag Ultra low cost, it can effectively prevent the leakage of tag data, unauthorized access and the fake tag. It has solved the key problems of safety and reliability on UHF RFID application widely used in the national economy, which has the vital significance to the development of Chinese Internet of things technology. [8]

UHF-HSS Framework has the advanced technologies as follow:

3.1. SoC Chip Design

Chip design uses direct up conversion transmitter structure and zero intermediate frequency orthogonal receiver structure. UHF RFID reader adopted analog front end and integrated 20dBm transmit power amplifier on-chip based on 0.18um SiGe BiCMOS process to achieve the tag remote read. In addition, it solves the leakage problem during information transmission by using the high linearity and low noise passive mixer to improve the receiver’s sensitivity. Furthermore, with the usage of rare integrated chip components, the test result of the receiver is below 20dbm output power and the sensitivity is -75dBm.

Based on the analog front-end chip, a fully integrated UHF RFID reader SoC chip is developed by the same process. It firstly integrated power amplifier of 25dBm to meet the portability and reading distance and reduce the cost of BOM. Receiver RF front-end adopts carrier offset technique, solves the 10dBm self-leakage problem and significantly increases the sensitivity of the receiver. The UHF RFID reader supports dense reading mode and expands the application field. We have designed the industry leading frequency synthesizer with low power consumption and excellent phase noise (phase noise of 200 KHz frequency offset is 125dBc/Hz). Receiver's digital baseband adopts advanced signal processing technology and realizes the demodulation ability of low SNR. In addition, the chip not only supports the EPC C1G2/IS0 18000 6C protocol, but also for the first time is in support of the national standard and the national military standard. It only needs a small number of external components to develop UHF system, which is suitable for large-scale application.

3.2. Software Platform

Based on the SOC chip, we has developed a set of IOT software platforms, including device driver of Linux kernel, IOT platform technology, RFID middleware technology

and the applicable software platform as shown in Figure1. Due to mastering the core technology platform from the bottom layer software to the application layer software, we can form safety mechanism to prevent possible data security problems through the close coordination between the chip, the software and the system [9].

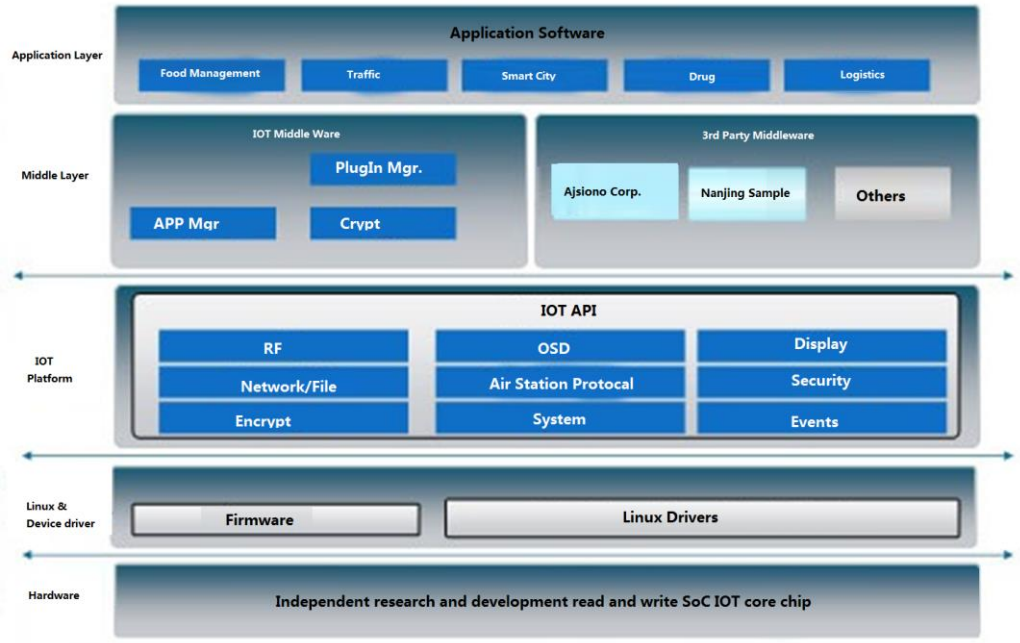

Figure 1. UHF- HSS Framework

3.3. RFID Middleware

In the RFID system, the object name service (ONS) is a process of the RFID reader sending wireless radio frequency identification label to the computer or application system by a string identifying a particular commodity. The Object Name Service system will lock the fixed point grab goods concerned in computer network news, and then provide tracking EPC represents the item's name and its related information, and immediately identify and share the data items in the supply chain, which the efficiently promotes the information transparency.

As showed in Figure 2, the RFID middle-ware plays a mediating role between RFID hardware and applications. It can realize the connection to the RFID reader from a set of generic application program interface (API) provided by the middle-ware in an application program. In this way, even if the storage of RFID tag data database software or back-end application increase or replaced by other software, or read and write RFID reader types increase occurs, the application does not need to modify which solves the complex problem of many-to-many connection maintenance.

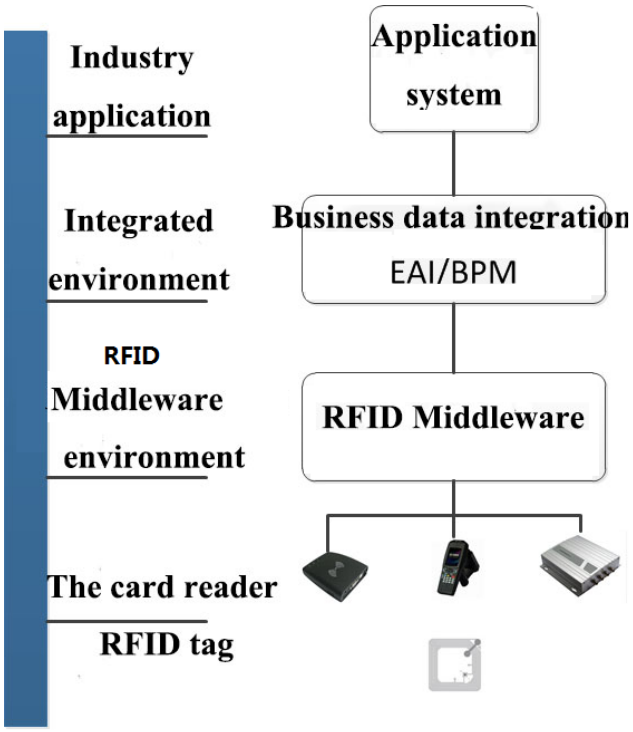

Figure 2. UHF- HSS Middleware Levels

4. Security Mechanism

UHF- HSS solves the security problem of Chinese Ultra high frequency RFID and protects the security of national information. RFID reader SoC chip undertakes data acquisition, data recognition and data processing between the tag and the application system. It relies on radio frequency communication protocol, encryption operation and security mechanism. Trust service platform will help establish a complete security and encryption mechanism in the read and write process of Ultra high frequency RFID (reader signal transmitting - tag signal return - reader decoding) and database query process (reader send tag data to database - database query – send information to reader), UHF- HSS security mechanism and relative implementation technology as follows:

4.1. Error Control Coding

Error control coding technology has used in the existing authentication of tags and reader. Firstly, reader checks the received data reflecting from the UHF tags by CRC. If the check fails, the reader requests data retransmission from tags until it is successfully recognized. Because the tag reflecting signal is usually very weak and susceptible to noise interference, which leads to signal distortion, reading rate declines and system performance deteriorates.

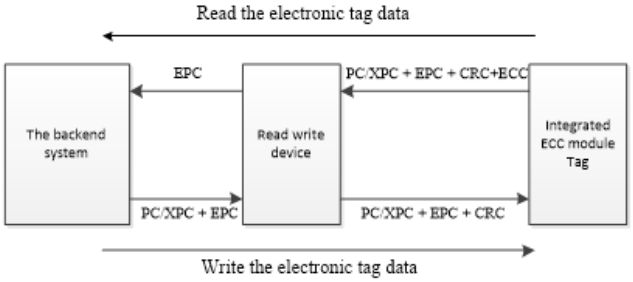

Figure 3. Error Control Coding Technology in the Tag Adds the ECC Module

In order to improve reading and writing success rate, we integrate error correction coding circuit corresponding into the tag as shown in Figure3. At the same time, the reader is also integrated with the error correcting decoding circuit or corresponding software. During the specific implementation process, the tag data add the check code by the CRC circuit firstly, and then the error correcting code is also added to tag data by error correction coding circuit for transitions. While reader firstly deal with error correcting code decoding, and then go through the CRC checks. If the inaccurate code number is in the error correction range of the error correcting code, the reader can correct the tag data. Only the uncorrectable error caused by a plurality of continuous error codes is found by correcting code CRC, and then the reader requests tag retransmission. It greatly reduces the possibility of the read-write device requiring the resending of data. The solution improves the reader's efficiency of reading and writing and reduces the rate of misreading. [10]

However, because this approach demands ECC integrated circuits in the tag, the cost of tag rises affecting its prospects. Then, we has further creative improved the method by integrating the electronic error correcting coding and decoding circuit in the reader to avoiding the tag cost arisen. The implementing steps are as follow as Figure4. Before the reader write the tag data, all the data generate the ECC error code after they pass through the correction circuit, and then they are written into the UHF tag (tag memory space doesn't need to be expanded because of the sufficient storage capacity). When reading the tag, the reader read back the tag data and ECC error correcting codes. The reader firstly decodes error correcting code, and then verifies the CRC. The reader can correct the error codes only if they are in the error correction range.

The workflow of reading the data is shown in Figure4. At first, the tag data is coupled with the check code through the CRC circuit , and then the error correction code by ECC will be sent back to the reader (as for the tag without ECC, it will directly send error correcting code data stored in the storage area by the reader). Thus the data which has been transmitted back to the reader including PC (Protocol Control), EPC (Electronic Product Code), CRC (Cyclical Redundancy Check) and the additional ECC (Error Correction Code). The reader decodes ECC error to correct some errors in the data, and then the CRC parity checks PC+EPC code correctly to confirm the data is correct or not. If the inaccurate code number is within the error correction range, the reader can correct the received tag data. Only the uncorrectable error caused by a plurality of continuous error codes can be found by CRC, and then the reader requests retransmission. This process greatly reduces the retransmission of the same tag, and improves the efficiency of tag reading. In this paper, the error correcting codes adopted BCH code, convolution code or LDPC code.

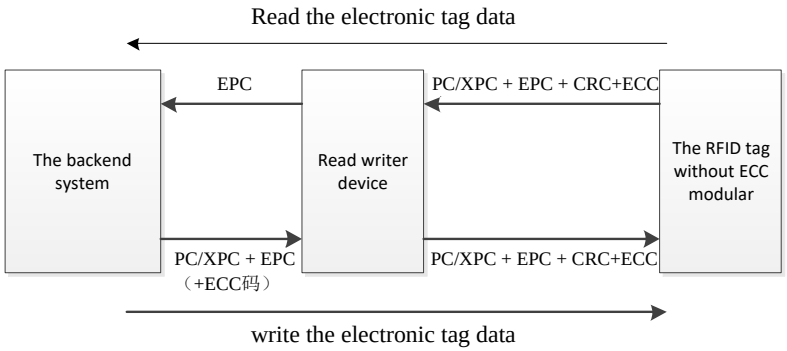

Figure 4. Reader Soc Chip Platform Reads and Writes Tag Mode

4.2. Advanced Security Encryption

While the reader is reading and writing the tag data, the signal read by the reader can be stolen by the third party device since there lacks encryption mechanism and the signal is transmitted via wireless broadcasting. In that manner, user data may be embezzled and bring big loss. Or user may be tracked for the disclosure of sensitive personal information, especially the location privacy. As for applications that are very confidential, such situation cannot be accepted. The reader involved in this project can encrypt the over-the-air data in many different ways according to user's request of different encryption levels.

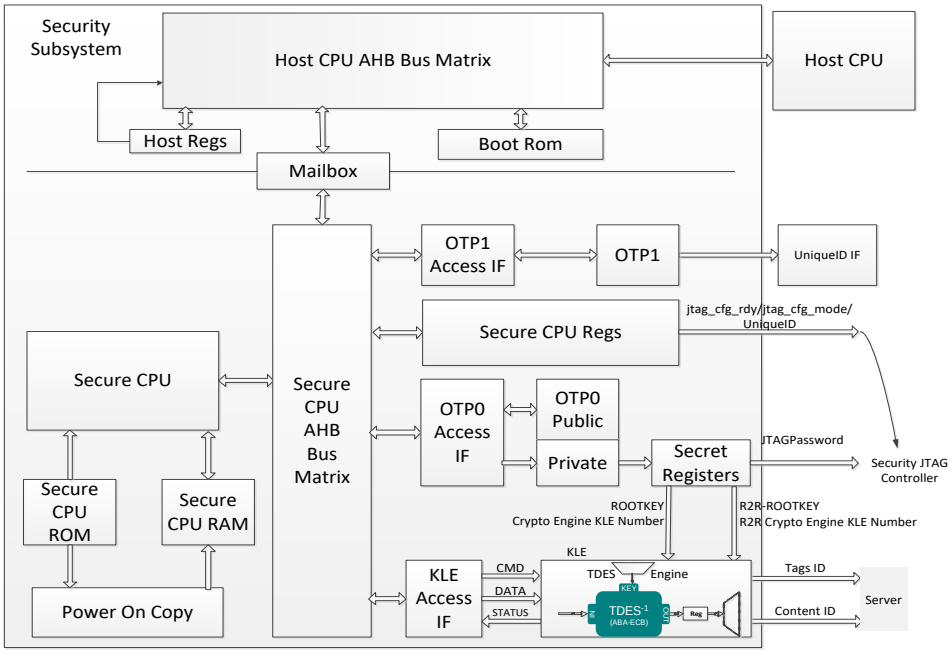

Figure 5. Soc Advanced Security Encryption Diagram Subsystem

As Figure5 shown, the advanced security encryption is supported by Embedded Secure Access Module (ESAM) including Secure Subsystem, Secure CPU *etc*. in the SoC chip of reader:

① ESAM cannot directly access by application software, which has its own security of CPU, ROM and RAM, its built-in encryption engine can realize tag fast data encryption and decryption;

② ESAM supports public - private key authentication mechanism. The industrial public key can be customized written in the chip before leaving factory for industrial user,

industrial users can complete control of data encryption and reader authorization mechanism;

③ Only number of OTP (One-Time-Program) for reader is supported. The end user industries code is written in the SoC chip before leaving factory, which ensure every reader has different ID number, so as to ensure effective authentication and authorization of reader, to prevent third parties reader data inquiry, ensure that the data is not leaked;

④ ESAM supports Advanced Security Encryption. The authentication and writing program ensure that the reader is not cloning. When the system starts up, ESAM can start the reader security subsystem to signature verification the reader program, so that the monitoring party copy FLASH procedure is unable to start in the other SoC chip which ensure the data security. [11]

4.3. Reader Authentication and Tag Anti-Cloning

When the existing UHF reader is working, tag can respond to the reader's query without its owner's permission. It can also be read by the reader nearby on the condition that the user isn't aware. The reader also can directly inquire the data that is relevant to the tag in the backend database. In this way, user data can be illegal embezzled and bring big loss. Data leakage leads to tag being illegally cloned and failing to realize its unique identifier function.

When UHF tags are used in the trace to the source, management and other functions, the information on the tag will be stored in the confidential backend database, which may involve in the production process, inventory management and shipments. The information once obtained by the competitor, the company would suffer. In terms of the factory, the tag database can improve the automatic program of factory production, inventory management, process monitoring. The relevant supervising departments can also monitor economic data via this database. The user hope that they can inquiry about raw materials, manufacture date and quality information through the tag. The current IOT system usually visits the backend database indiscriminately so that it is difficult to realize the multi-level authorization automatic inquiry system.

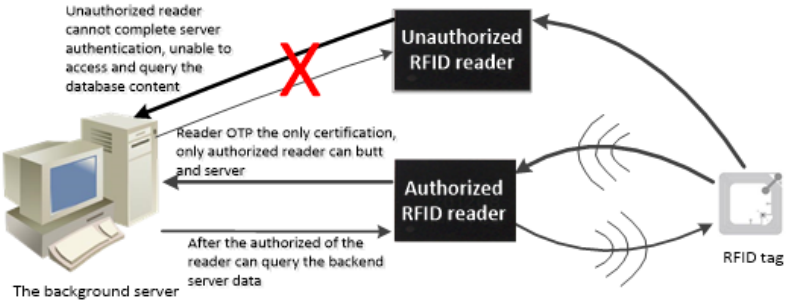

Figure 6. Encryption and Authentication Mechanism

The authentication method will establish an effective multi-level authorization accessing mechanism to access the backend database. It opens the database details on the different levels according to user role to effectively protect sensitive information. [12]

The reader authentication implementation is that: at first, OTP (One Time Password) module is embedded into the reader, the unique number identifying the reader is written into OTP module, and the backend database will hierarchically authorize each reader according to the unique number in the reader. In the second, after reading the tag, the reader connects the backend server via the Internet and then sends the authenticated information including OTP information encrypted by the public key to the backend certification system. The backend certification system decrypts the data via the private

key, and then judge the reader is authorized or not by comparing the tag data from the relative reader with the reader limit list. If failed, the reader can not access the backend database. If success, the authorized reader can inquiry the relevant information in the backend database.

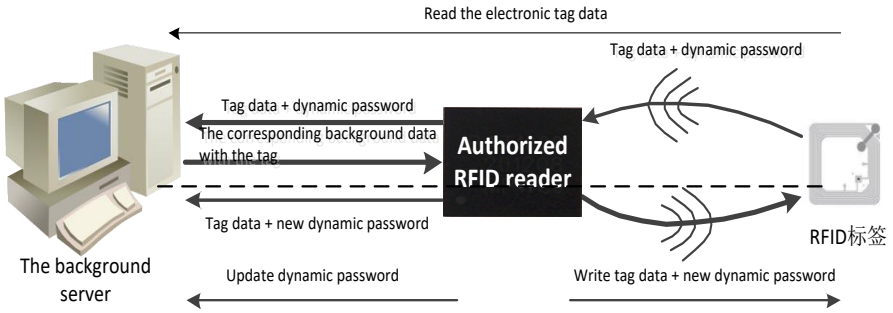

Figure 7. Through Dynamic Password to Realize Tag Anti Cloning

The Tag anti cloning implementation is that: at first, the reader reads the tag data content including dynamic symmetric cryptography password stored in the tag, and then send the data to the background server for dynamic symmetric cipher comparison. If the authentication succeeded, the server sends a response to the reader. In the second, the reader generates a set of new dynamic passwords and rewrites the tag and the backend server, and then the passwords are symmetric dynamic updated. If cloning tag, the attacker could not update dynamic symmetric cipher at the same time. So that, even one time all data in the tag is in a copy cloning, but attacker is unable to update dynamic symmetric cipher in background server, so the cloning is easily be identified by the server as illegal tag, thereby effectively preventing the tag large-scale cloning. [13]

5. System Implementation

UHF-HSS implementation is based on the Soc reader chip, which is a fully integrated, high-performance chip using Jazz 0.18-micron SiGe BiCMOS process, supporting China's national standard "IT RFID 800 / 900MHz air interface protocol" (GB / T 29768-2013), GJB GJB7377.1, ISO / IEC 18000-6C, ETSI 302 208-1. The chip integrates the RF transceiver front-end, base band transceiver, PLL, and power amplifiers, supports DSB-ASK, SSB-ASK, PR-ASK modulation modes. Further more，it has a powerful multi-reader, multi-tag reading, writing and anti-jamming technology and security mechanism. By the National radio Frequency Identification (RFID) system Engineering Research Center testing, its performance reached the level of the market similar products. The purpose of UHF-HSS is a turn-key solution for Hardware aspects, including reader Soc Chip hardware reference design, DC power adapter, USB to UART cable, RF Cable, Antenna and so on, which has the following features. It is shown in Table 1.

Table 1. The Specs of UHF-HSS Full Solution

Items	Specification
RFID Protocol Support (Air Interface protocol)	EPC global C1Gen2 (ISO 18000-6C) with DRM CHINA 800/900MHz UHF RFID Standard
RF Power Output	30dBm, power output range and accuracy
Max Tag Read/Write	Over 9 m with 6dBi antenna(Read)

Distance	
Max Tag Read Rate	Up to 200 tags/second using high performance settings
Antenna connector	2 antenna 50Ohm MMCX connectors supporting 2 mono-static antennas
Physical interface	Providing DC power
	Providing Communication, Control and Debug signals
	Providing GPIO signals, like sensor signals input and indicator signal output
API Support	API Function Library based C
DC power required	DC voltage: 5V ; DC Current: <3A
Local Regulatory	CHINA, ETSI, FCC
Operating Temp	-40~60
Storage Temp	-40~80

Figure 8 shows UHF-HSS's simplified architecture. Fully integrated Reader chip includes transceiver and digital core. Just need simple off-chip components. User can make a Reader Module. MCU communicates with Reader Soc Chip by SPI and be responsible for configuring the chip status, sending commands and receiving data. Besides, MCU can also be used for monitoring and controlling RF parts on the Board, like detecting forward power, reverse power and external's PA Temp and selecting external antenna. Power supply solution is composed of DC/DC and LDO. It can power on the entire chip on the board. Interface defines the signals relevant with External and Host. DC Power Supply connects with DC Adapter. USB and UART are designed to communicate with the Host. Debugging signals are used for Reader Soc Chip and MCU. GPIO is reserved for future use.

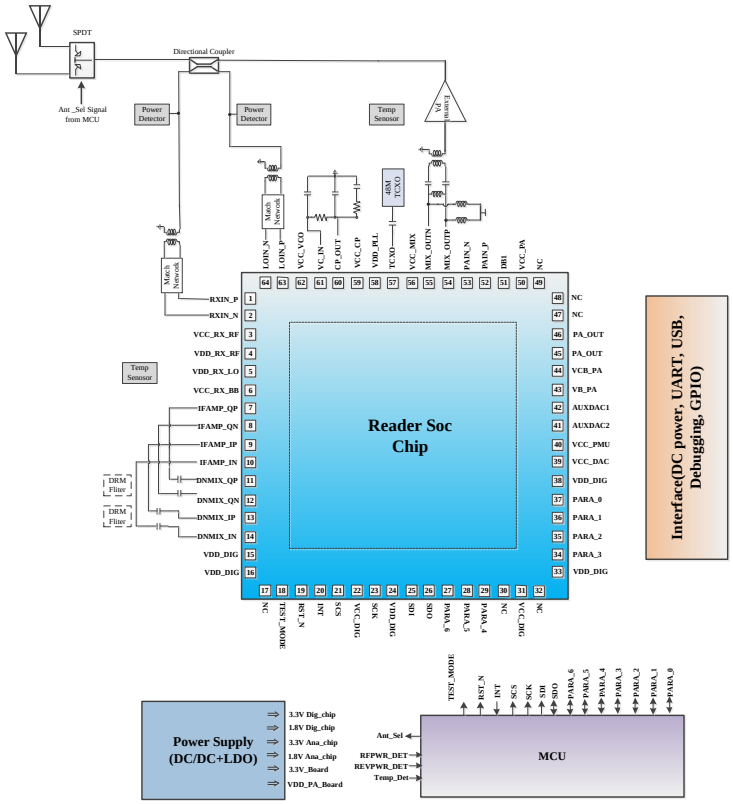

Figure 8. The UHF-HSS's Simplified Architecture

5. Conclusion

Based on the investigation of UHF information security, we had analyzed the existing problems of current UHF information security, given the realization method, and developed the security system. Through the error control coding, dynamic symmetric key authentication technology and much other technical innovation, we have solved the security and reliability problem which had ever prevented UHF technology scale application. UHF-HSS technology will be applied in the fields of vehicle management, automatic identification, Logistics management and other aspects of production. In the future, we will pay more attention to the combine of UHF and mobile Internet. The mobile intelligent device will communicate with UHF reader via interface of Bluetooth, USB and other way, which will be used in the Express and product security, change our life greatly.

Acknowledgments

This paper was supported by Public Projects of Zhejiang Province (No.2015C31092), MOE Project of Humanities and Social Sciences (No. 11YJC790141), Ningbo intelligent team business plan project (Ningbo World Information Technology Development Co., Ltd.), National Students' Innovation and Entrepreneurship Training Program (No.201513001005), Ningbo leader and top-notch talent and Ningbo Wisdom team project, Ningbo DaHongYing College Sciences support project.

References

[1] Y. Sun, Y. Wu and X. Ma, "Modeling and verifying EPC network intrusion system based on timed automata", Pervasive & Mobile Computing. vol. 3, no. 2, **(2015)**, pp. 61-76.
[2] Z. Wang, W. Xin, Z. Xu and Z. Chen. "A Secure RFID Communication Protocol Based on Simplified DES". Proceedings of the 2012 International Conference on Information Technology and Software Engineering, Beijing, China, **(2012)**.
[3] A. W. Xing, H. F. Zheng, W. Bin, Z. X. Dong, and L.Li, "RFID tag antenna, a radio frequency identification tag and a radio frequency identification system", C.N. Patent 201120172872.8X, **(2011)**.
[4] T. Kasper, D. Oswald and C. Paar, "RFID. Security and Privacy", Springer Berlin Heidelberg, Los Angeles, **(2012)**.
[5] M. J. Chae, D. J. Yeager, J. R. Smith and K. Fu, "Maximalist cryptography and computation on the WISP UHF RFID tag", In: Proceedings of the Conference on RFID Security, **(2007)**.
[6] Z. Bin, Z. Hui, Z. X. Dong, and Y.Fei, "Improve the success rate of the RFID tag reading method", C.N. Patent 201310170686.4, **(2013)**.
[7] Z. Bin, Z. Hui, Z. X. Dong, and Y.Fei, "Enhanced RFID information security and privacy protection method", C.N. Patent 201310170371.X, (**2013**) May 10.
[8] Z. X. Dong, and J. Han, "RFID tag antenna, RF power amplifier gain control method", C.N. Patent 201410013886.3, **(2014)**.
[9] P. T. Jun, "City Card System based ID cards". C.N. Patent 200910262685.6, (**2009**) Dec 23.
[10] P. T. Jun, "A DRM system and the distributed key-based security methods", C.N. Patent 201110463007.3, **(2011)**.
[11] P. T. Jun, "A security device operating system with a virtual on-chip devices, systems and methods", C.N. Patent 201210373661.X, **(2012)**.
[12] P. T. Jun, "High security mobile security system for distributed key information and security methods", C.N. Patent 201110329692.0, **(2011)**.
[13] P. T. Jun, "A network security device, multi-application systems and security methods in the PAN", C.N. Patent 201210561978.6, **(2012)**.

Authors

Tiejun Pan, (Henan,1972-) received the MS and PhD degrees in modern mechanical engineering from Zhejiang University, Hangzhou, China, in 1997 and 2001, respectively. He is currently a Master Tutor associate professor in the Department of Computer Science and Information Engineering at Zhejiang Wanli University. His research interests include software engineering, embedded system, theory and application of networked control system.

Leina Zheng, (Liaoning, 1981-) received the MS degree in School of Management from Wuhan University of Technology, Wuhan, China, in 2008. She is currently a Lecturer in the Department of Business at Zhejiang Wanli University. Her research interests include IOT, Mobile Internet, and Innovation & Enterprise education.

Ming Wang, (Jiangxi, 1968-) received the MS degree in University of Jiangxi Education, NanChang, China, in 1991. He is currently a professor at Ningbo Dahongying University. His research interests include IOT, Mobile Internet, and Innovation & Enterprise education.

Xiaodong Zhu,(Jiangsu, 1959-) received the MS and PhD degrees in Solid State Physics from Purdue University, U.S., in 1981 and 1984, respectively. He is currently CEO of Zhejiang Fengkun Ltd.. His research interests include RFID application, IC Design.

