The Design and Realization of a Lightweight RFID Mechanism Integrating Security and Anti-collision

Yu Songsen
School of Computer, South China Normal University, Guangzhou 510631, China
yss8109@163.com

Peng Yun
College of Computer Information Engineering, Jiangxi Normal University, Nanchang 330022,China
pengyunmail@126.com

Yang Jian
College of Automation, Guangdong University of Technology, Guangzhou 510090, China
jimmyyoungyj@163.com

Zhang jiajing
School of Computer, South China Normal University, Guangzhou 510631, China
627051098@qq.com

***Abstract*—RFID security and RFID anti-collision are research hotspots of RFID technology in the internet of things, most of the existing studies took them as separated parts and researched them individually. This paper attempts to deal with them as a whole, with a strategy integrating lightweight random key double-authentication and dynamic slot-ALOHA protocol. The processing mechanism, performance comparison and algorithm realization are given in this paper. The new mechanism not only maintains the advantage of rapid tag identification, but also has the ability to resist re-transmission attack, tracking-attack, blocking-attack, tampering-attack and so on. It has a high safety and practicality.**

***Index Terms*—RFID security, RFID anti-collision, Lightweight, double-authentication, slot-ALOHA**

I. INTRODUCTION

RFID security and RFID anti-collision is a hot issue in the study of RFID technology. The typical security protocols for RFID system include: Hash-Lock protocol, Randomized Hash-Lock protocol, Hash chain protocol, ID change protocol based on gallimaufry, David's digital library RFID protocol, distributed RFID inquiry - response authentication protocol, LCAP protocol, once again encryption mechanism and etc.[1]

There are extensive studies on RFID anti-collision. According to the method used, RFID anti-collision algorithms can be classified into four types: space division multiplexing (SDMA), time division multiplexing(TDMA), frequency division multiplexing (FDMA) and code division multiplexing(CDMA).The algorithm based on TDMA which is currently a research hotspot includes two types: tag-driven (asynchronous), and reader-driven (synchronous). Tag-driven algorithms are mainly ALOHA series of algorithms; reader-driven algorithms which assorts the collision by reader can be further divided into Q learning algorithm, tree algorithms, PULSE protocol, LLCR algorithm, IRCM algorithms and so on.[2]

To date, RFID security and RFID anti-collision are are generally taken to be different parts and are tackled independently. Some scholars have started to pay attention to put security and anti-collision studying together. Zhang-Hui [1] proposes an anti-collision algorithm for a new RFID security architecture, Gustaw Mazurek, Carlo Mutti, Zhi-Guo Ding, Wang Ping[3-6] propose CDMA mechanism to merge them, which can make full use of the confidentiality, anti-jamming and multi-access communications capability of CDMA. But its dilemma lies in that it is very difficult to choose spreading codes which fully meets the autocorrelation and cross-correlation. Additionally the hardware cost of the tag is higher.

Taking into account the RFID tags limitations of computing power, storage space, cost, power supply and so on, this paper proposes an lightweight approach which merges the random key double-authentication and dynamic slot-ALOHA protocol. The new mechanism maintains the rapid identification of the tag. It can also resist a variety of attacks including re-transmission attack,

Supported by Foundation of production and research of Ministry of Education and Guangdong Province (2009B090300073), Scientific and technological project in Guangdong Province (2008B010200037), National medium and small-sized enterprise innovation fund (09C26214415217), and National college students innovative experiment project [teaching 2009-47]

doi:10.4304/jsw.6.7.1235-1240

tracking-attack, blocking-attack, tampering-attack and so on. It has a high safety and practicality.

II. CONVENTIONS OF THE PROCESSING MECHANISM

A Instructions sending from the reader

The reader sends three kinds of instructions: the frame starting instruction (Start instruction), the certification instruction (Certify instruction) and the time-slot continuance instruction (Continue instruction).

Start (Rr, Slots-num): the frame starting instruction is used to begin a frame, needing to set a random number and the total number of time slots.

Certify (M2): the certification instruction is used to return the M2 data and perform identification operation when the reader successfully received the M1 data.

Continue: the time-slot continuance instruction is used to decrease the time-slot register value of a active tag by one, which means the the tag is sent into the next slot.

B Instructions replying from the tag

There are three types of the tag instructions: the data response instruction (Response instruction), the authentication success instruction (Idty_succ instruction) and the authentication failure instruction (Idty_faul instruction).

Response (M1, Rt): the data response instruction is used to send the M1 message and random numbers back to the reader.

Idty_succ: the authentication success instruction indicates that the tag successfully identifies the information from the reader. After sending this instruction the tag comes into silence state.

Idty_faul: the authentication failure instruction indicates that the tag does not identify the information from the reader successfully. After sending this instruction the tag comes into suspending state, and is not waked up until the reader sends the next frame starting instruction.

C The tag data storage area

RFID tag data storage area is divided into four parts. The reserved area stores 32 bits access password(access password) and 32 bits destruction password (kill password). The EPC area stores 32 bits EPC,16 bits protocol control code(PC),16 bits cyclic redundancy check code of EPC values and PC values. The TID(tag ID) area stores 32 bits tag identifier and 32 bits all the additional information. The user area stores other information of the user.

At the beginning each tag and back-end database share the EPC of the tag, named EPCx and EPCi respectively. When the product comes into the sale stage, it generates passwords which shared by the tag and the back-end database, named PWx and PWi. It is stored in the tag and the back-end database respectively. The 16 bits cyclic redundancy check code calculating from EPCx value and PC value, is expressed as CRC (EPCx, PC) and is stored into EPC storage area. It is used for verification when sending data. In which: Ra means 16 bits binary number inputted by the user; Rr means 16 bits binary random number generated by the tag reader; Rm means 16 bits binary random number generated by the tag; CRC (a, b) means 16 bits cyclic redundancy check code calculated from a and b; $\oplus$ means XOR; $\oint$ means connecting operation which can connect the two 16 bits binary number into a 32 bits binary number [9].

III. PROCEDURE OF THE PROCESSING MECHANISM

The procedure of the processing (mechanism X) is as follows:

Step one: the reader generates a random number named Rr, sets a frame total time-slot number named Slots-num, makes the current time-slot number named Slots-cur equaling to Slots-num, and sends a Start (Rr, Slots-num) instruction to the tags in the area.

Step Two: When the tag receives the Start instruction it also generates a random number named Rm. The tag makes the Rm mode Slots-num as the tag owned time-slot, and stores it into the time slot register named Slots-temp. Then it will calculate Rt = Ra $\oplus$ Rm, Kx = (Rr $\oint$ Rt) $\oplus$ PWx and M1 = (CRC (EPCx, PC) $\oint$ Rr) $\oplus$ Kx.

Step Three: the tag that its Slots-temp is 0 will response by instruction Response (M1, Rt).

Step four: so according to the data the reader receives from the tags, there are three cases:

(1)If there is no signal, indicating that no tag reply, the reader lets the idle time-slot counter C_0 increase 1, and turns to the eighth step.

(2) If the reply data is invalid, indicating that there is a conflict, the reader lets the conflict time-slot counter C_k increase 1, and turns to the eighth step.

(3) If the reply data is valid, indicating that there is a single tag replying, the reader lets the single tag time-slot counter C_1 increase 1, and goes into the fifth step that is the certification process.

Step Five: the reader inquiries the EPCi and PWi ($1 \le i \le n$) in the back-end database, whether there is the EPCi and PWi that makes M1 $\oplus$ Ki = (CRC (EPCi, PC) $\oint$ Rr) ? Where Ki is equal to (Rr $\oint$ Rt) $\oplus$ PWi.

if the value matches, the reader will calculate Ki = (Rt $\oint$ Rt) $\oplus$ PWi and M2=(CRC(EPCi, PC) $\oint$ Rt) $\oplus$ Ki, and send a instruction Certify (M2) to the tag, then turn to the sixth step. Otherwise, it means the authentication failure, the reader will set the fail status bit named faul_deat, and turn to the tenth step.

Step Six: the tag receives the M2 message, verifies whether (if) M2 $\oplus$ Kx=(CRC(EPCx, PC) $\oint$ Rt) is true? Where Kx equals to (Rt $\oint$ Rt) $\oplus$ PWx. if the result matches, it gets across certification. The tag returns instruction Idty_succ, comes into silence state and turns to the ninth step. Otherwise, it means authentication failure. The tag returns instruction Idty_faul and continues to the seventh step.

Step seven: the tag sets itself to suspending state, and is not waked up until the reader sends the next frame starting instruction.

Step eight: if the reader receives Idty_faul instruction, it set the fail status bit faul_deat.

Step nine: the reader makes the current time-slot variable Slots-cur decrease 1. when its value is not 0, the reader sends a time-slot continuance instruction Continue. Otherwise, it means a frame is end, the reader will re-estimate the total time-slot number of the next frame, and turn the first step. If the collision slot does not exist in the frame and the faul_deat is 0, the whole process is ended.

Step ten: the tag makes its time-slot register variable Slots-temp decrease 1, and turns to the third step.

The procedure is shown in figure 1, figure 2.

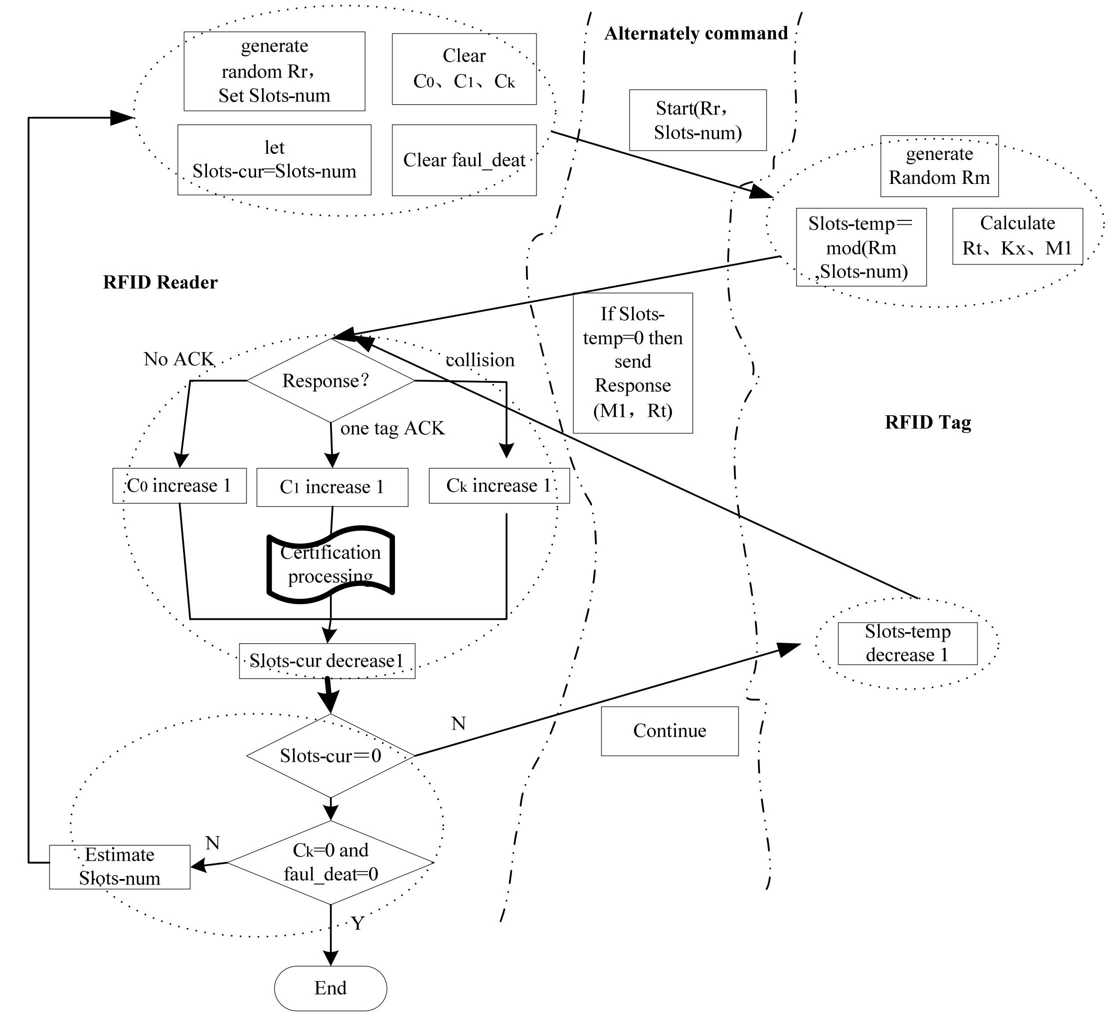

Figure1 The procedure of integration processing mechanism

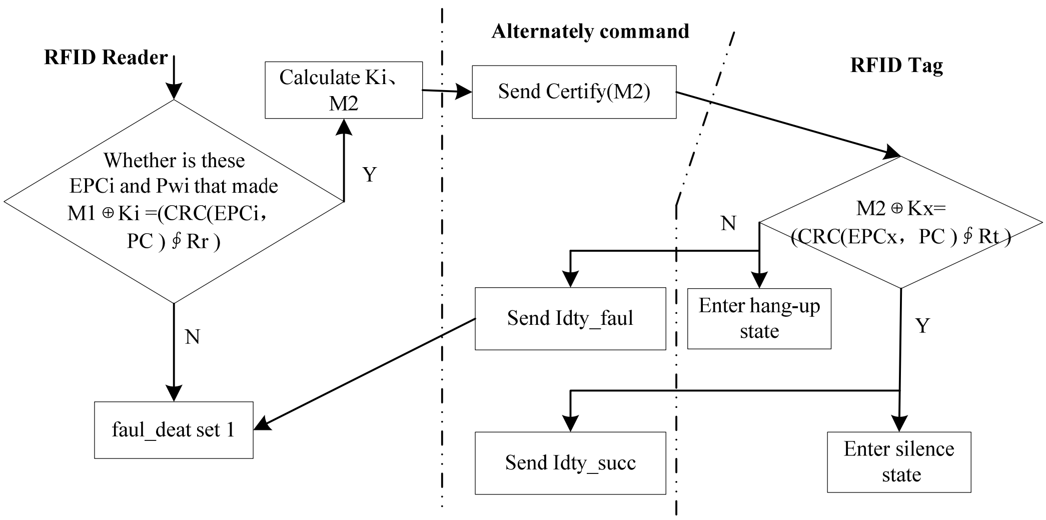

Figure2 The authentication part of integration processing mechanism

The selection of the optimal number for time-slot of the next starting frame can be estimated by the number of idle time-slots C_0, conflict time-slot number C_k and the single-tag time-slot number C_1. The optimization model can see Vogt method [7].

$$n(N) = C_1 + 2 * C_k \quad (1)$$

A simple way is shown in Table 1[8]. Table 1 lists the maximum goal number (high) and the minimum goal number (low) when the system uses different frame time-slot numbers by statistical methods, as the threshold value, the range in which corresponds to an optimal frame time-slot number. In the reading process, it only need judge the current time-slot estimate value is in which corresponding threshold range, then determines whether need to re-allocate the new frame time-slot number.

TABLE1 THE OPTIMAL FRAME TIME-SLOT NUMBER PATTERN TABLE

N	1	4	8	16	32	64	128	256
low				1	10	27	56	112
high				9	30	63	127	∞

Ⅳ. PERFORMANCE ANALYSIS

The integrating RFID processing mechanism adopts MOD operation, XOR operation, connecting operation and CRC operation in the identification procedure. The operation type and operation quantity for a successful identification under normal circumstance are listed in Table 2. Both the values for the reader and tag are included. (Note: The searching EPCi and Pwi operation is done in the back-end database, thus these operations need not to be considered in the performance analysis).

TABLE2 THE RESPECTIVE OPERATION TYPE AND OPERATION QUANTITY

	mode operation	XOR operation	link operation	CRC operation
Reader		2	2	1
Tag	1	5	4	2

Because the MOD operation, the XOR operation and the connecting operation are very simple, those operation times can be negligible. The main time will be spent on the CRC operation. But the CRC operation can be implemented by a corresponding shifting logic circuit designed in the tag, therefore its computing time is will be short too.

The communication instructions between the tag and the reader are mainly: Start(Rr,Slots-num), Response (M1,Rt), Certify (M2), Continue, Idty_succ and Idty_faul. Because of interacting simplicity, the data traffic quantity is not high.

In this mechanism the EPC code information is hidden in identification. The message have already been encrypted that inquiries and answers between the tag and the reader. If the listener monitors the entire process, he can only get encrypted information. In order to get the tag information he needs to get the corresponding secret key. Because the same probability is very low after the random numbers do XOR operation each other, and block mechanism or self-destruct mechanism can be appropriately adopted if necessary, so this mechanism can resist spoofing-attack, replay -attack, as well as tracking-attack.

In conclusion, Table 3 shows performance comparison of several common RFID security and anti-collision protocols, in which √ and × respectively mean a protocol has or has not the corresponding function.

TABLE3 PERFORMANCE COMPARISON OF SEVERAL COMMON RFID SECURITY AND ANTI-COLLISION PROTOCOLS

	frame-slots dynamic adjustment	hide EPC code	randomly generate ID code	double-authentication	tag needs a lot of memory unit	possess anti-collision function	possess Security function
ISO18000-6	×	×	×	×	×	√	×
EPC Gen2	×	√	√	×	×	√	×
dynamic slot-ALOHA	√	×	×	×	×	√	×
Randomized Authentication Key[9]	×	√	√	√	×	×	√
ZHANG Hui[1]	×	√	×	√	×	√	√
Gustaw Mazurek[3]	×	√	×	√	√	√	√
Liang Biao[10]	×	√	×	√	√	√	√
Wang Ping[6]	×	√	×	√	√	√	√
Carlo Mutti[11]	√	√	×	√	√	√	√
Fusion mechanism(this paper)	√	√	√	√	×	√	√

Ⅴ. SIMULATION AND IMPLEMENTATION

The RFID processing mechanism can be implemented by the corresponding program, its implementation using

similar language is as follows.
Part of the reader
Main()
{repeat
{Randomly generate a random number Rr;
Set an initial value to total frame number Slots-num;
Let the current time-slot number Slots-temp is equal to Slots-num;
Clear time-slot counter C_0、C_1、C_k;
Clear status bit faul_deat;
Call Start(Rr，Slots-num) function; //start a frame processing
Case Answer of tag
{ no signal: idle time-slot counter C_0 increase 1;
Conflict: conflict time-slot counter C_k increase 1;
Receiving a valid data M1: single tag time slot counter C_1 increase 1, and call identify() function to come into the certification process.
};
If receiving Idty_faul
Set faul_deat;
Current time-slot number Slots-temp decrease 1;
If Slots-temp!=0
Call Continue() function; // To the next slot
Else
{ If (C_k ==0)& & (faul_deat==0)
Exit(0)； //The whole process is over
Else
Estimate the new total time-slot number Slots-num of the next frame;
}
} until(1)

identify() function
{ Search each of the EPCi and PWi (1≤i≤n) in the database;
Calculate Ki=(Rr ∮ Rt) ⊕ Pwi;
If M1 ⊕ Ki ==(CRC(EPCi，PC) ∮ Rr)
{ Calculate Ki=(Rt ∮ Rt) ⊕ Pwi;
Calculate M2=(CRC(EPCi，PC) ∮ Rt) ⊕ Ki;
Call Certify(M2) // Send authentication data to the tag
}
Else set faul_deat
}
}．
Part of the tag
Main()
{
If receive a Start instruction
{Generate a random number Rm;
Let time-slot register Slots-temp is equal to mod(Rm,Slots-num);
Calculate Rt=Ra ⊕ Rm, Kx=(Rr ∮ Rt) ⊕ PWx;
Calculate M1=(CRC(EPCx,PC) ∮ Rr) ⊕ Kx;
If Slots-temp==0
Call Response(M1，Rt);
}；

If receive a Certify instruction
{ Calculate Kx =(Rt ∮ Rt) ⊕ PWx;
if M2 ⊕ Kx==(CRC(EPCx，PC) ∮ Rt)
Send Idty_succ instruction, and come into silence state;
Else
Send Idty_faul instruction
}；

If receive a Continue instruction
{ Slots-temp decrease 1;
If Slots-temp==0
Call Response(M1，Rt);
}
}

Ⅵ. CONCLUSION

To research the RFID security and the RFID anti-collision as a whole is a good attempt. Based on the study of existing RFID security protocols and RFID anti-collision algorithms, this paper proposes a processing mechanism integrating lightweight random key double-authentication and dynamic slot-ALOHA protocol. The mechanism is simple, practical, and compatible with EPC Gen2 standards. compared with the other security protocols and anti-collision protocols, the new mechanism has a low complexity and tag-cost. It can not only effectively solve the problem of quickly identifying tags, but also can resist a variety of attacks including re-transmission attack, tracking-attack, blocking-attack, tampering-attack and so on. It has a high safety and practicality.

REFERENCES

[1] ZHANG Hui,HOU Chao-huan,WANG Dong-hui，An Anti- collis ion Algorithm for a New RFID Security Architecture，Micro Computer Information，2008.24.

[2] Yang Jian，Research of Anti-collision Algorithms in RFID System，Sun Yat-sen university PhD thesis，2009.p4-6

[3] Gustaw Mazurek，Active RFID System With Spread-Spectrum Transmission，IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING, VOL. 6, NO. 1, JANUARY 2009

[4] Carlo Mutti，CDMA-based RFID Systems in Dense Scenarios: Concepts and Challenges，2008 IEEE International Conference on RFID The Venetian, Las Vegas, Nevada, USA，April 16-17, 2008

[5] ZhiguoDing，Research and Realization on Key Technologies of RFID，A dissertation for doctor’ s degree，University of Science and Technology of China，2009，P113～122

[6] Wang Ping,Hu Ai-qun,Pei Wen-jiang，The Design of Anti-collision of UHF RFID System Based on CDMA，Journal of Electronics & Information Technology，Vol.29 No.11 2007

[7] Vogt H．Efficient object identification with passive RFID tags[A]．International Conference on Pervasive Computing[C]．LNCS，Springer-Verlag，2002
[8] Wu Jing,Xiong Zhang,Wang Ye，Multiple object anti-collision RFID technology with dynamic slot allocation，Journal of Beijing University of Aeronautics and Astronautics，2005 V01．31 No．6
[9] Cai Qingling, Zhan Yiju, Shi Binning，A Mutual Authentication Protocol of Randomized Key Based on EPC C1G2 RFID, TELECOMMUNICATIONS SCIENCE ,2007 23(4)
[10] Liang Biao,Hu Ai-qun,Qin Zhong-yuan，A Novel Design for RFID Anti-collision Technique，Journal of Electronics & Information Technology，Vol.29 No.9 2007
[11] Carlo Mutti，CDMA-based RFID Systems in Dense Scenarios: Concepts and Challenges，2008 IEEE International Conference on RFID The Venetian, Las Vegas, Nevada, USA April 16-17, 2008

YU Song-sen was born in Fengcheng, China in 1972. He received the B.Sc. degree in electrical engineering in 1990 and the M.Sc. degree in computer in 2003 from NanChang University, NanChang, China. In 2006, he received the Ph.D. degree from Guangdong University of Technology, Guangzhou, China.

In july 1994, He joined the School of Computer at NanChang University, initially as a Teaching Assistant, a lecturer and subsequently as an Associate Professor. He was a Research Assistant from 2006 to 2008 in the School of Technology at SUN YAT-SEN University. Since 2009, he has been in School of Computer at the South China Normal University. His research interests are in the areas of Internet of things, RFID anti-collision, RFID security and wireless sensor networks. He has more than 20 publications in the above areas and is actively taking charge or participating in several R&D projects of the china.

He has been a Assessors of the Sciencepaper online of china, Transportation and Logistics Association of Jiangxi Province and Guangzhou Science and Technology Projects.

Peng Yun received the B.E. degree in electronic engineering from Nanchang University,Nanchang,P.R.China, in 1994 and the M.E. degree in computer software and theory from Jiangxi Normal University,Nanchang,P.R.China,in 2002. He was a Teaching Assistant from 1994 to 1999 in the Department of Applied Physics at Jiangxi Science & Technology Normal University and a Lecturer from 2002 to 2007 and currently an Associate Professor in the Computer and Information Engineering College at Jiangxi Normal University. His interests include artificial intelligence,data mining and software engineering.

Yang Jian received the B.S and M.S degrees in biomedical engineering from Northeastern University, Shenyang, China, in 2003 and 2006, respectively, and the Ph.D. degree in communication and information system from Sun Yat-sen University, Guangzhou, China, in 2009. Since 2009, he works as a lecturer at Guangdong University of Technology, Guangzhou, China. His research interest covers RFID anti-collision, RFID network and ad hoc wireless network.

Zhang jiajing undergraduate of School of Computer, South China Normal University, His research interests include RFID and wireless communication.