UNIVERSITY
OF GÄVLE

FACULTY OF ENGINEERING AND SUSTAINABLE DEVELOPMENT

Cyclic Redundancy Check for Zigbee-Based Meeting Attendance Registration System

Xiaoying Ma & Yuelong Cheng

July 2012

Bachelor's Thesis in Electronics

Bachelor's Program in Electronics/Telecommunications

Examiner: Per Ängskog

Supervisor: Per Landin

Acknowledgements

During the period of preparing the dissertation, a great many technical problems are encountered. Firstly, we would like to express our sincere gratitude and admiration to our supervisor Per Landin, our teacher Niklas Rothpfeffer and examiner Per Ängskog for their generous help and useful suggestions. Meanwhile, all the teachers are highly appreciated to impart knowledge to us such that we can accomplish the dissertation.

Abstract

The research accomplished in this dissertation is focused on the design of effective solutions to the problem that error codes occur in the ZigBee-based meeting attendance registration system. In this work, several different check algorithms are compared, and the powerful error-detecting Cyclic Redundancy Check (CRC) algorithm is studied. In view of the features of the meeting attendance registration system, we implement the check module of CRC-8. This work also considers the data reliability. We assume use retransmission mechanism to ensure the validity and completeness of transmission data. Finally, the potential technical improvement and future work are presented.

Table of contents

1 Introduction

Along with the increasingly rapid pace of life and frequent information exchanges, the communication among human, social groups and even the governments is brought close to a relaxed, effective, easily manageable and controllable manner. Under the circumstances, meeting systems are emerging in rapid succession. The gradual utilization of meeting systems makes the communication among human easier and more manageable. In order to make meeting attendance registration systems more effective, convenient and mobile, increasing research attention has been paid to wireless meeting attendance registration systems (according to reference 2 and 19). However, wireless telecommunication is apt to cause data loss and data error. Hence, the research accomplished in this dissertation is mainly focused on the design of CRC check, an effective solution to the problem that error codes occur in wireless meeting attendance registration systems, such that the validity and completeness of transmission data is ensured.

1.1 Current Situation of Meeting Attendance Registration Systems

Nowadays, various meetings are held more frequently, and the number of attendees is getting larger and larger. Currently, the meeting sponsor mainly adopts manual registration. Nevertheless, manual registration not only makes it more difficult for management but also results in high labor costs. In addition, it takes more time to handle the registration information after the meeting is over, and mistakes easily occur in the report forms. Therefore, the utilization of meeting attendance registration systems will change the way of our work and enhance efficiency. With the development of meeting service, it is quite necessary to implement an effective and user-friendly meeting attendance registration system.

Currently, besides manual registration, some large and high-level conferences also use the following attendance registration manners: Bar Code Check-in, Magnetic Stripe Card Check-in, Multimedia Check-in, etc. However, the abovementioned attendance registration systems generally communicate via wired transmission, which will result in inconvenience. In order to make the meeting attendance system more advanced and perfect, this dissertation adopts wireless communication.

1.2 Conference Registration System Scope

Personal Identification System is a technical innovation that was introduced to the 9th International Conference on Reliability, Maintainability and Safety, Guiyang, China, 12-15th, June, 2011. In this system, the main function is Automatic sign module: Identify the identity of participants that by read the RFID Card.The background of our thesis is based on the conference. Due to the number of participant is large and the traditional registration system cannot be moved, it is not convenient if the conference place has changed. We come up with an idea of wireless communication registration system to solve the problem. We want to design a Zigbee wireless system instead of the data line between reader system and attendance system. The system is conclude three big parts, they are: Zigbee communication, CRC (Cyclic redundancy check) and backstage process. As the project member we only take part in the transmission part: CRC. The CRC has improved the secrecy and reliability of the system.

1.2.1 Included

Investigation And Selects Error Check Algorithm: We will compare several Error Check Algorithm, and list their advantages and disadvantages. We think the CRC is the most suitable check for the system.

CRC Algorithm:

1)we will study and investigate the theory of CRC from the book and internet.

2)we will design the CRC program on computer based on the theory.

Implementation: We will design the CRC module and realize it by software. To check if the CRC algorithm is consistent with the calculated result. So we will make a simulation of CRC operation to get the matching result.

Software: The software have been used are Microsoft virtual studio 2008 and C++ language.

C++ language is a very commonly used computer programming language as well as a generalized programming language, which supports many kinds of programming styles, such as proceduring programming, data abstraction, object-oriented programming and icon-making. C++ language can be well combined with C language. Even at present, most C language programs are completed under the Integrated Development Environment (IDE) of C++. Facing most object-oriented languages, C++ is of quite high performance. And C++ does not require a complicated programming environment.

Visual Studio is a development environment developed by Microsoft, which is the most popular application development environment based on Windows platform. Now, the Version 9.0 has been released, namely Visual Studio 2008.Microsoft Visual Studio 2008 enables developer to rapidly create applications of high quality, better customer experience and close connection, fully showing the idea of Microsoft to develop intelligent client-side applications. In virtue of Visual Studio 2008, the information acquisition and analysis will become more simple, convenient and fast and the business decision will become much more effective.

Therefore, this system uses C++ language and Microsoft virtual studio 2008.

1.2.2 Not Included

Integration: The integration of CRC and Zigbee module is done by other project members.

Hardware: Done by other members.

Retransmission Mechanism is error correction. It is not included, but in the future development we will intend to do this.

1.3 Factors affecting wireless communication

In the process of wireless communication, there are various different environmental factors that affect the information transmission：“

- *Quality of transmitter and receiver. Generally speaking, the greater the power output of the transmitter is, the wider the signal coverage is. And higher sensitivity of the receiver will tolerate longer distance transmission and make signals more stable. Meanwhile, it should be mentioned that antenna is also a key source that affects transmission range. Since the antenna bandwidth and gain of common portable interphones is a bit low (generally within 10 dB), they are vulnerable to environmental obstacles.*
- *Accessory: Power. Transmitter and receiver should retain adequate power, or the quality of communication would be degraded. Especially, transmission cannot proceed normally in some extreme situations.*
- *Environmental factors. A key difference between wireless and wired communication facilities is that the former are much more vulnerable to environment. In general, the distance marked in products is the test value in theory. In different transmission conditions, the real transmission distance will differ quite considerably. If there are many obstacles between transmitters and receivers such as tower blocks, elevators, etc., transmission distance would be significantly shortened and communication quality would be degraded. Additionally, the existence of electromagnetic wave also influences the quality of wireless communication.*”[1]

Therefore, it is necessary to use a check system needed in wireless communication to ensure that the received information is correct.

2 System Description

2.1 System Framework

The system framework of conference registration is show in figure 1, this is the Zigbee system Location of schematic. Zigbee system between reader system and attendance system, the sender is at reader system, and the receiver is at data library computer.

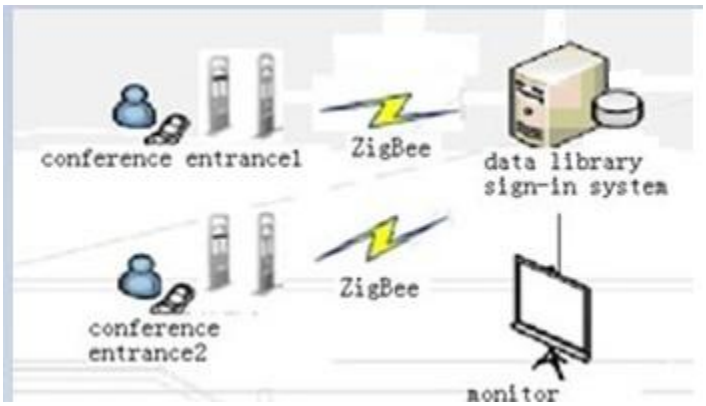

Figure1

2.2 ZigBee

2.2.1 ZigBee Technology

"*ZigBee is a specification for a suite of high level communication protocols using small, low-power digital radios based on IEEE 802.15.4 standard. This specification is defined by IEEE wireless personal area networks (PAN) and called IEEE 802.15.4 (ZigBee) technology standard*" [2]. The key advantages of ZigBee are short distance, low complexity, self-organization, low power, low data rate, and low cost [3].

2.2.2 Current Situation of Wireless Communications

Today wireless network is becoming the leader in communication choices among users [2]. "*Wireless network refers to any type of computer network that is not connected by cables of any kind. It is a method by which homes, telecommunication networks and enterprise installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunication networks are generally implemented and administered using a transmission system called radio waves* [4]." Due to the avoidance of wired medium such as twisted pair cable, coaxial cable and optical fiber, the network is really brought close to an ideal world where the information is portable.

The typical wireless telecommunications network is made up of a sending terminal, a receiving terminal and a wireless receiver. The sending terminal is also called radio transmitters including data source, modulator, radio-frequency (RF) source, RF power amplifier, antenna and power supply, while the wireless receiver consists of data receiving circuit, RF demodulator, encoder, RF low-noise amplifier, antenna and power supply . The data is transmitted from the sending terminal to the receiving terminal via radio waves. Then, the data will be processed and checked such that users acquire the correct message.

The scope of wireless communication is quite wide, and there are several different classification approaches.

"*Firstly, according to the transmission medium, it can be divided into optical communication, microwave communication and sound wave communication, etc. Secondly, according to the frequency band, it includes the following categories: ISM band wireless communication, military band wireless communication and aviation band wireless communication, etc. In addition, according to the communication protocol, it can be categorized into the following eight basic varieties: wireless local area network (WLAN), Bluetooth, HomeRF, Wi-Fi, WiMAX, UWB, wireless USB and ZigBee* [2]."

The main purpose of this dissertation is to design a check system for a ZigBee-based wireless meeting attendance registration system to improve its reliability.

"*ZigBee is a pronoun of IEEE802.15.4 specification* [5]." "*The technology defined by the ZigBee specification is intended to be a short-distance, low-power, wireless telecommunication. The name ZigBee is originated from the waggle dance of honey bees. Bees, after zigging and zagging around in the fields, return to the hive, and perform what some call the waggle dance to communicate the distance, direction and type of food to others in the hive. After receiving a waggle-dance indication, bees fly off directly to the source of food. That is to say, honey bees build the communication network of the colony using the waggle dance* [6]."

The key features of ZigBee include short distance, low complexity, self-organization, low power, low data rate, and low cost. These advantages including allow ZigBee to be applied to industrial automation and remote control fields. It can be integrated into various devices.

"*In a word, ZigBee is a short-distance, low-cost, low-power, wireless mesh network standard, and is a leading technology in the market* [6]."

2.2.3 Technical Advantages and Disadvantages of ZigBee

Compared with other wireless communication technologies, ZigBee has the following advantages: "

a) Low power. In sleep mode, 2 AA type batteries can last up to 6-24 months or even longer for a single node. This is the strong advantage of ZigBee. Under the same condition, Bluetooth can work several weeks, while WiFi can only work several hours.

b) Low cost. The requirement for telecommunication controller is reduced by greatly simplifying the protocol (less than 10 percent of Bluetooth). The predictive calculation is based upon 8051 8-bit microcontroller. The host nodes with full function need 32KB flash memory, and sub-function nodes only need 4KB flash memory. Besides, ZigBee is exempted from protocol patent fee. The price of each chip is about two dollars.

c) Short time-delay. ZigBee has the advantage of fast response. In general, it only takes the system 15ms to switch from sleep to work mode, and 30ms to connect the web, resulting in lower electric energy consumption. However, Bluetooth needs 3-10s and WiFi needs 3s.

d) High capacity. The ZigBee network layer natively supports both star and tree typical networks, and generic mesh networks. For each network, one host node is tasked with its creations, and each host node can govern 254 sub-nodes at most. Meanwhile, host nodes can also be supervised by nodes at the next higher level. It should be noted that a large network can accommodate up to 65000 nodes.

e) High Safety. Concretely, ZigBee provides three security levels. The lowest level is with no security setting. The middle-level adopts access control list (ACL) to prevent the illegal data acquisition, and the highest level uses advanced encryption standard (AES 128) to flexibly determine the safety attributes.

f) License-free frequency bands. ZigBee adopts direct-sequence spread spectrum technology. The license-free frequency bands of ZigBee include Industrial, Scientific and Medical (ISM) band, Global 2.4 GHz band, USA 915 MHz band and Europe 868 MHz band.

g) *Short Distance. The transmission scope is mainly between 10 and 100m. After increasing RF transmitting power, the scope could be increased to 1 to 3km. This scope means the distance between the joint nodes. If the routing and the connection of the nodes, the transmission distance will be further* [6].”

But the ZigBee also has following disadvantage:

“*Low Speed. ZigBee works at the low speed of 20-250kbps, providing the raw data throughput rates of 250 kbps(2.4GHz), 40kbps (915 MHz) and 20kbps(868 MHz), which could meet the needs of low-speed data transmission* [6].”

2.2.4 ZigBee Network Topology

ZigBee has 3 types of network topologies. The structures of these network topologies are given in Figure 2. The advantage of Star network is designed to be simple. The advantage of Mesh network is signal transmission performance well. The advantage of Cluster Tree network is coverage wide. For each network, one host node is tasked with its creations, and each host node can govern 254 sub-nodes at most. Meanwhile, host nodes can also be supervised by nodes at the next higher level. It should be noted that a large network can accommodate up to 65000 nodes [6].

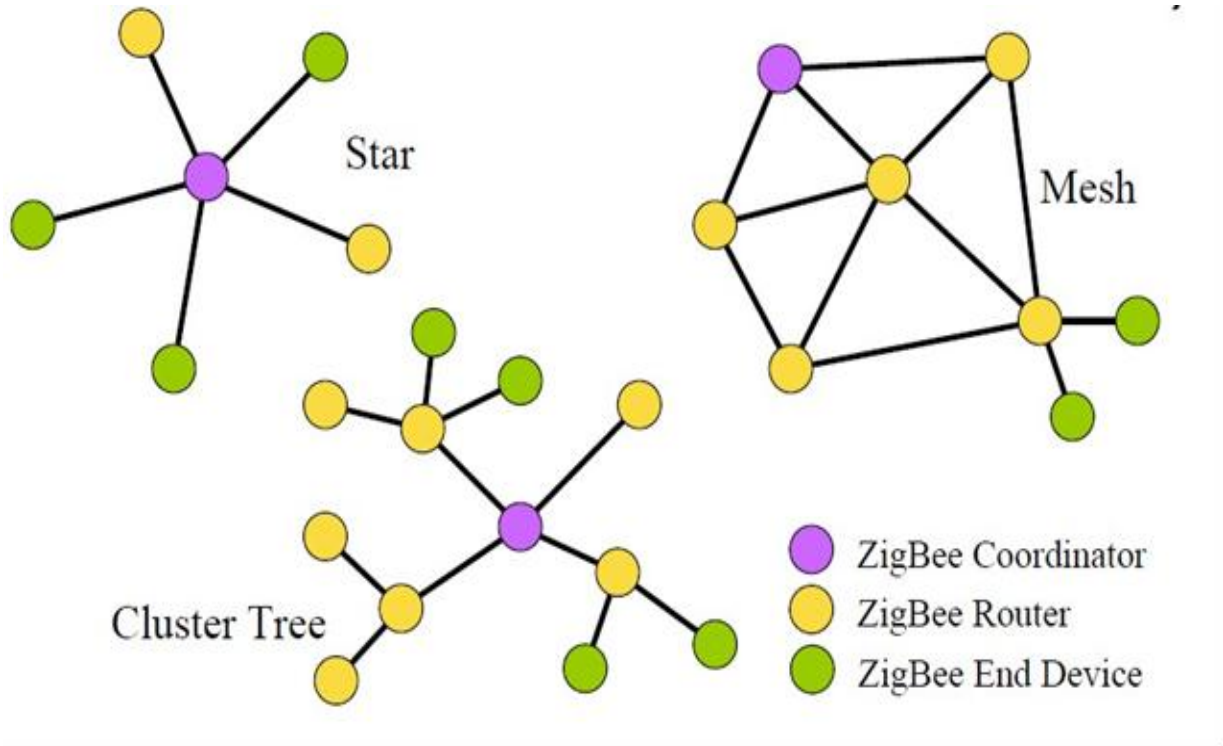

Figure 2

In the point-to-point network (our system is simple and no child nodes, it's a point-to-point network), any two devices can mutually communicate as long as one is in the range of the other's wireless signal [7]. The network coordinator in the point-to-point network is mainly used to manage the information of the link status and authenticate the identities of devices.

2.3 Improvement of System Reliability

The utilization of advanced ZigBee in the meeting attendance system realizes wireless transmission and makes the system more flexible, convenient and movable. However, how to improve the reliability of the meeting attendance system?

The key of the meeting attendance system is to guarantee the accuracy of the signal transmission. In the process of information transmission, the information will become incorrect due to disturbances and transmission system defects. In wireless transmission, noise is always affect signal. When we receive the data, the data is always including noise. For example, the noise will make the information 1 will become 0 or 0 will become 1. Data communication schematic diagram show in figure 3[8]. Therefore, error-correcting code technology should be used to improve the system reliability.

The common error-correcting code technologies include:

- Parity Check

- Block Character Check
- Hamming Check
- Cyclic Redundancy Check

"*All the above are based on a basic method. First, the sending terminal works out the check code of the transmitted information by some algorithm, then sends the information and the check code. According to the same algorithm, the receiver works out the check code, then compares it with the received check code. From the comparison result, users can judge whether the received information is correct or not* [8]."

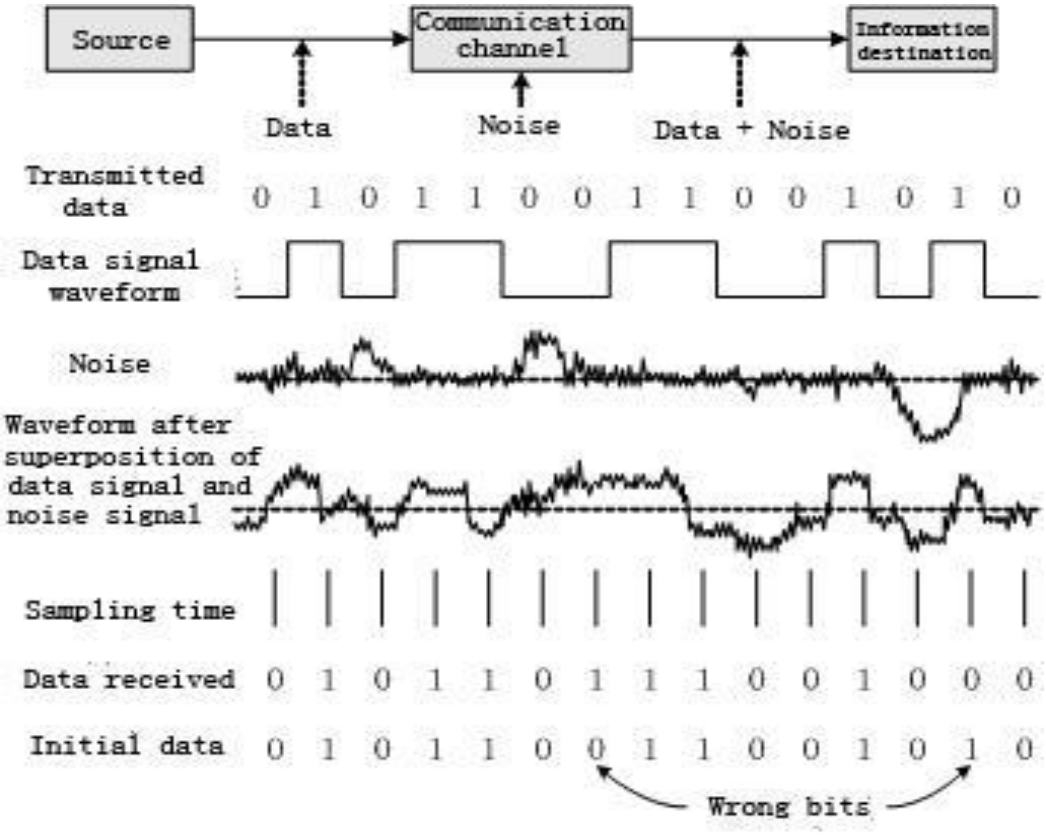

Figure 3

2.3.1 Parity check code

Parity check is a common used error-detecting method. "*It is a simple and widely used method of increasing the minimum distance of the binary transmission system. The parity check could be described as: adding a parity bit to each code word to form the singularity or odevity check. It could identify the incorrect code element since the parity check will become singularity. The parity check code could make the number of 1 in the codes become odd (singularity check) or even (odevity check) by adding a parity bit, then the code*

distance becomes 2. Since the parity check is based on the parity of the number of 1 in the code, the errors of even number cannot be detected [9]." Take the ASCII code (0110000) of 0 for example. If the first bit from the right hand side is wrong after transmission, i.e. 0 changes to 1, the receiver will still consider it as a legal code (0110001) (the ASCII code of 1). If a singularity parity bit is added to the left hand side, the code will be 10110000. If the first bit at the right hand side is wrong after transmission, the code will be 10110001. Then, the number of 1 becomes even, which indicates that the code is illegal. However, if two bits are wrong (the first and second bits for example), the code becomes 10110011. The number of 1 is five which is still an odd number. In this case, the receiver will still consider the code to be legal (the ASCII code of 3). Thus, the parity check could not detect this kind of error.

Advantages of parity check：

Low cost. The arithmetic coding implementation of Parity check is simple and less programming code. The parity check is usually used to check data in the process of the storage reading-writing or the transmission in bytes. Since when error occurs in one byte code, the probability that one bit becomes error is larger than that of two-bit error, the parity check code is effective for checking one byte code.

Disadvantages of parity check：

- If the sum of the error bits in the data is an even number, the error cannot be found.
- Parity can only detect the error, but not be determined.
- Parity can only detect the error, but the error cannot be located, not to mention being corrected.

2.3.2 BCC check code

"Obtain BBC check code by XOR all data with a given initial value (usually 0). Connect the check code to the end of communication data, and then transmit them together" [9]. Once the data is received, the receiver will also make a XOR to obtain the check code. If the latter check code is the same as the received code, then it is indicated that the received data is correct.

Advantages of BCC check：

BCC check implementation simple, and accurate than Parity check.

Disadvantages of BCC check:

BCC check cannot detect the error bits order.

2.3.3 Hamming Check

Hamming code is a multiple (duplex) parity check. It codes the information in logical form to make the error detecting and correction possible. "*All transmitted code words are composed of the original information and the additional parity check bits. Every parity bit is coded at the special position of the transmitted code word. Any bit error will cause changes of the values of the several relevant check bits. Hence, Hamming code cannot only detect errors but also locate the error bits. This provides the basis for automatic error correction* [8]." However, hamming code check can only detect up to 2 and correct up to 1 bit errors.

Advantages of Hamming check:

Hamming check is not only the ability to detect errors, but also gives the exact location where the error.

Disadvantages of Hamming check:

Because the Hamming check can only detect and correct 1 bit error. So if there are multiple errors, these errors cannot be detected.

2.3.4 Cyclic Redundancy Check (CRC) and Its Superiority

Cyclic Redundancy Check (CRC): "*Connect n bits of check code to the end of the K-bit information code to construct the whole code with N bits. Therefore, such codes are also called (N, K) code. For a given (N, K) code, it could prove that there exists a polynomial G(x) with the highest power of N-K=n* [10]." According to G(x), the check code of the K-bit information could be generated, and G(x) is called the generated polynomial of the CRC code.

The generation process of check code: Assume that the transmission information is represented by information polynomial C(x). Shift C(x) to the left by n bits, and it will be $C(x)* x^n$. In this way, the right n bits of C(x) will be empty, and these are the locations for the check code. The remainder of $C(x)* x^n$ divided by G(x) is the check code.

Normally, the k is very large in data communication and network. One frame is composed of one thousand or even several thousands of data bits, then the n-bit check positions will be generated with CRC code [8]. In general, let n be 16, and the standard 16-bit polynomials include CCITT CRC16=$x^{16}+x^{12}+x^5+1$ and ANSI CRC16=$x^{16}+x^{15}+x^2+1$ [11].

Advantages of CRC check:

CRC check error detection capability is strong, and its performance better than other check algorithm, CRC is able to check multiple bit errors.

Disdvantages of CRC check:

CRC can only check for errors, but cannot correct the error.

2.3.5 Comparison

By the comparison among the above four check algorithms, it can be found that the parity check can be easily used but the errors can be considered as correct with a high probability. Hamming code can correct and detect errors, but it can only detect up to 2 and correct up to 1 bit errors. The error detecting capacity of CRC code is strong. Therefore, this paper chooses CRC check.

3 CRC（Cyclic Redundancy Check）

3.1 Theory

3.1.1 CRC（Cyclic Redundancy Check）Technology

The most effective error-correcting scheme that is commonly used is CRC check. CRC check is a mathematical method used for synchronous data transmission, and could capture 99.95% of the transmission errors [8]. CRC is the remainder obtained by using one byte data flow to divide another byte data flow with binary division (without carry, using XOR to replace subtraction). The dividend is the binary representation of the information data flow for which the checksum shall be calculated and the divisor is a predefined (short) binary number with the length of n+1, which is normally represented by the factors of polynomials. Before conducting the division, n zeros shall be added at the end of the information data. The principle of CRC is to connect n-bit check code to the end of the K-bit information code to construct the whole code of N bits. Therefore, such code is called (N, K) code. For a given (N, K) code, it can be proved that there exists a polynomial G(x) with the highest power of N-K=n. According to G(x), the check code of the K-bit information could be generated, and G(x) is called the generation polynomial of the CRC code.

Check process of CRC：the transmitter calculates the cyclic redundancy code of the transmitted binary data and sends it to the receiver together with the original data; by recalculating cyclic redundancy code of the received data and comparing with the received cyclic redundancy code, the receiver can judge whether the received data is correct or not. If they are the same, it can be said that the received data is correct. Otherwise, the received data is wrong [12].

3.1.2 Mathematical Principle of CRC

CRC check code is the remainder obtained by dividing the data by a certain constant number (for example, in ANSI-CRC16, the number is 18005_{hex}) [13].

The question is what to be transmitted is a series of byte data but not a single data, and how could we change a series of numbers into one data? The answer is simple. For example, if the bytes are B1 and B2, the corresponding number is B1B2. If there are three bytes, B1, B2 and B3, the corresponding number is B1B2B3. If the number is 01_{hex}, 02_{hex} and 03_{hex}, the corresponding number is 10203_{hex}. The rest should be calculated in the same way. If there are a lot of bytes, the corresponding number will be very large, but, fortunately, CRC only needs the remainder instead of the quotient.

From the above principle we can roughly know the accuracy of CRC. If error codes occur, the probability of losing them is 1/256 in CRC8, 1/65536 in CRC16 and 1/ (2^{32}) in CRC32, which is a very small value [14]. Therefore, if the scale of the data is small, the CRC8 will be sufficient.

There is another question here. If the dividend is smaller than the divisor, the remainder will be the dividend itself. For example, if only one byte is to be transferred, then its CRC is itself. To avoid such case, the byte should be shifted before the division so as to make it larger than the divisor. The question is how many bits should be shifted? In fact, it depends on the fixed divisor. The number of bits shifted to the left should be fewer than that of the divisor 1 bit.

The CRC polynomial standard divisors should meet the following requirements:
1. Generate a polynomial of the highest and lowest bit must be 1.
2. When any bit of the transmission of information occurs error, the remainder of information divide generator polynomial is not 0.
3. Different bit error occurs, the remainder will different.
4. Use the remainder continues do division, should make the remainder cycle.

The standard divisors are listed as follows [14]**: "**

- *CRC8: the polynomial is $x^8+x^5+x^4+1$, and the corresponding number is 131_{hex}. Shift 8 bits to the left.*
- *CRC12: the polynomial is $x^{12}+x^{11}+x^3+x^2+1$, and the corresponding number is $180D_{hex}$. Shift 12 bits to the left.*
- *CCITT CRC16: the polynomial is $x^{16}+x^{12}+x^5+1$, and the corresponding number is 11021_{hex}. Shift 16 bits to the left.*
- *ANSICRC16: the polynomial is $x^{16}+x^{15}+x^2+1$, and the corresponding number is 18005_{hex}. Shift 16 bits to the left.*
- *CRC32: the polynomial is $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x^1+1$, and the corresponding number is $104C11DB7_{hex}$. Shift 32 bits to the left.***"**

Mathematical Principle of CRC is show in figure 4. For example, a 15-bit binary number C=101001110100001 will be transmitted in the data transmission. Such number could be represented by $C(x) = x^{14} + x^{12} + x^9 + x^8 + x^7 + x^5 + 1$, where the value of the kth bit in C corresponds to the factor of x^k in C(x). Multiply C(x) by x^n, i.e. add n zeros after C, and divide C(x) by the n-order polynomial G(x). Then the binary code, P, of the (n-1)-order remainder P(x) is the CRC code. The division of C(x) and G(x) could be realized by using C and G to complete XOR calculation. We choose the polynomial is G=100110001, so n=8. Then add 8 zeros after C and divide G. The remainder P=00000111 is the CRC code.

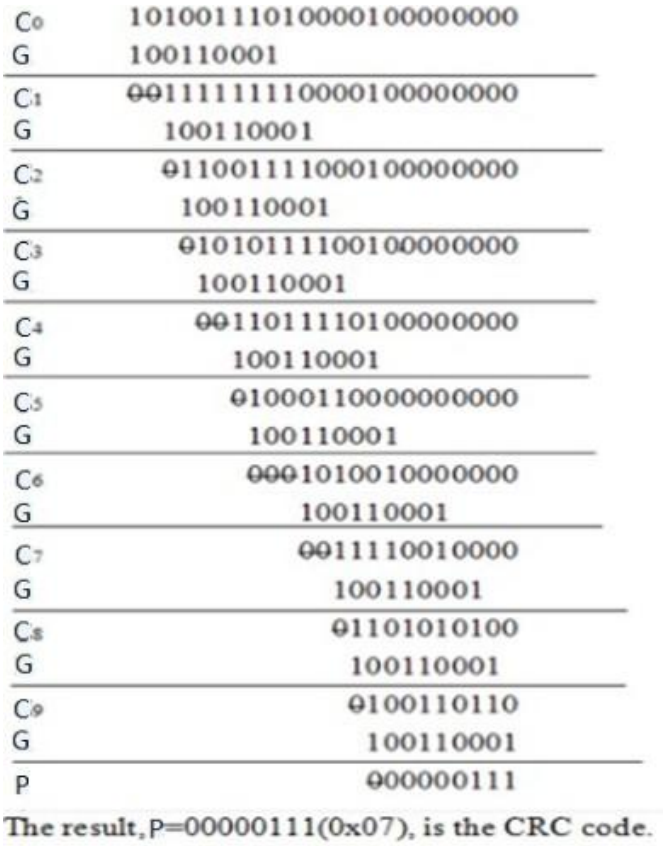

Figure 4

3.1.3 Retransmission Mechanism of Error Communication

In the wireless network communication, conflict will lead to data loss, while channel quality and electronic noise will introduce errors [15]. These phenomena will affect the reliability of data. Although data error can be detected by CRC check and other methods, this paper assume the problem of data loss in the communication via retransmission mechanism.

There always exists the transmission of some control information in the transmission of any practical application information among communication facilities. The application information is conveyed to the destination in a safe, reliable and efficient way according to the established communication protocol. “Handshaking protocol is to make two facilities have a mutual confirmation before transmission [16].”

The schematic diagram of retransmission mechanism is show in figure 5. Illustration of the retransmission means :

(a) Shows when the receive data is correct, the receiver send ACK back to sender.

(b) Shows when the receive data is error, the receiver send NAK back to sender, the sender will send the data once again until receive ACK.

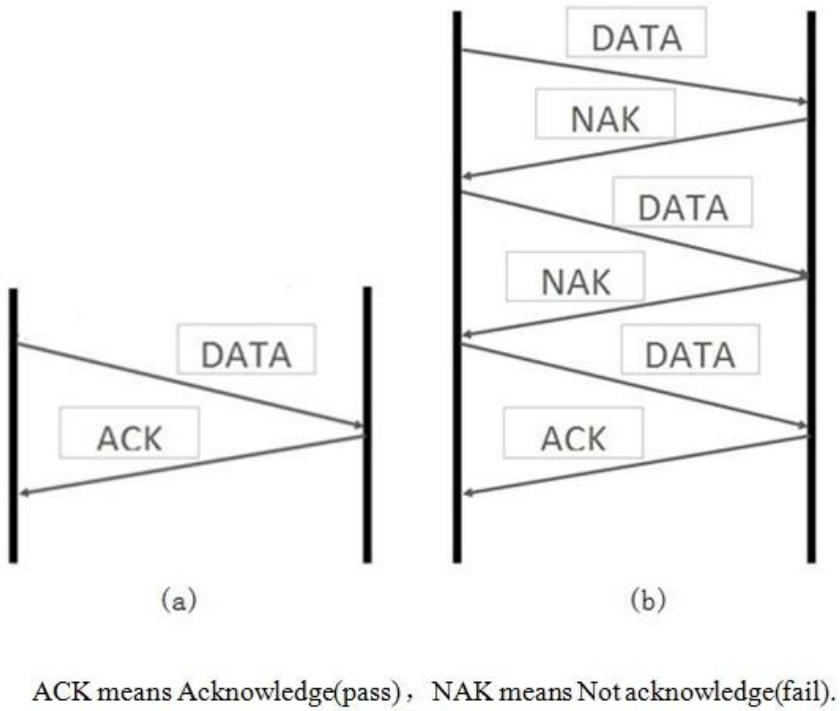

Figure 5

3.2 Implementation

3.2.1 System operation environment

- Operating System: Windows 7
- Development Platform: Microsoft Visual Studio 2008
- Development Language: C++

3.2.2 CRC Module Design

The CRC algorithm is to input the original data into a checking formula and generate a certain-length check code which is then added to the end of the original data to form a new datum. For serial input-output systems, the cyclic calculation of the check code is required until all the data calculation is completed.

3.2.2.1 Why choose CRC algorithms used in current systems?

CRC algorithms, implemented in embedded systems, can be classified into two categories: one is the direct calculation method, and the other is the look-up table method [17]. Why do we choose the first one?

The look-up table method calculates check values by bytes. When calculating, the result is obtained by XOR operation between the data from a given table , rather than finding the remainder after modulo-2 [18]. This method is simple and fast , but its code readability is poor. The table is in appendix A.

In contrast, the direct calculation method calculates by bits. This method, which is the most flexible, can check data of any length and is applicable to the cases insensitive to speed. In this system, as long as the response time of data is maintained in milliseconds, human cannot feel the time difference. Therefore, in light of implementation convenience and code readability, the direct calculation method is adopted.

3.2.2.2 Working Principle for Error Detection of CRC Code

The error detection of CRC code considers the bit sequence of the message to be processed as the coefficients of a binary polynomial C(x). After C(x) is divided by the generated polynomial G(x) previously agreed by the transmitter and receiver, the resulting remainder P(x) is added to the original message as the CRC check code and sent to the receiver together. The receiver divides the received message D(x) by the same G(x). If the remainder equals P(x), then the transmission is correct (C(x) is same as D(x)). Otherwise, an error has occurd in the transmission. In this case, the data should be retransmitted by the sending terminal and the CRC check should be restarted until no error occurs.

Several points in the check process should be noted:

- Binary (modulo 2) algorithm is employed in the CRC calculation, i.e., no carry in summation and no borrow in subtraction, which in fact is to perform XOR operation between two operands.
- Before the CRC calculation, the polynomial C(x) represented by the transmission message multiplies x^n, where n denotes the maximum power value of G(x)). For the binary multiplication, $C(x)* x^n$ means shifting C(x) n bits to the left to store the remainder P(x). Therefore, the actually transmitted message is represented by $C(x)* x^n +P(x)$.
- The first and last coefficients of the generated polynomial G(x) must be 1. The process of CRC check is shown in Figure 6.

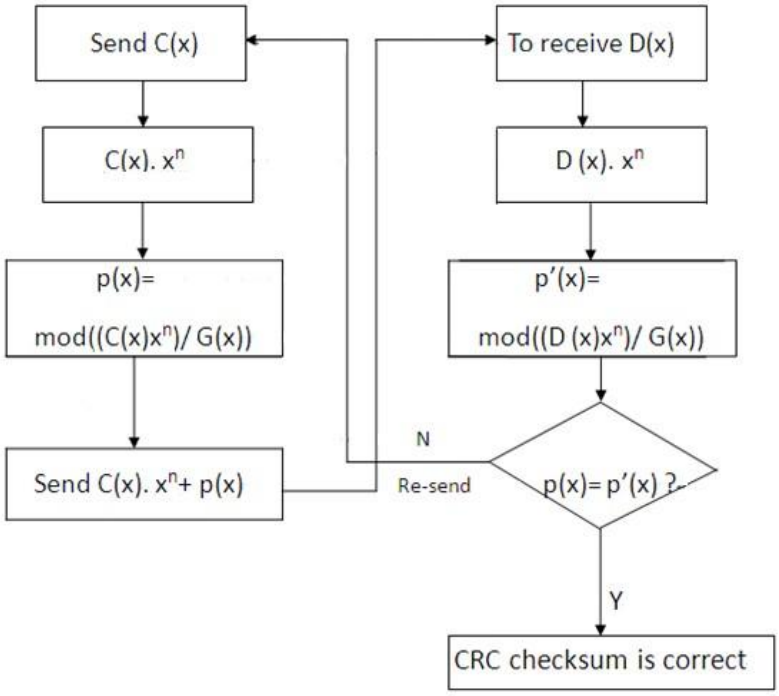

Figure 6

3.2.2.3 Comparison Among Different CRC Algorithms

CRC algorithms include [14]**:** "

- *CRC8: the polynomial is $x^8+x^5+x^4+1$, and the corresponding number is 131_{hex}. Shift 8 bits to the left.*
- *CRC12: the polynomial is $x^{12}+x^{11}+x^3+x^2+1$, and the corresponding number is $180D_{hex}$. Shift 12 bits to the left.*
- *CCITT CRC16: the polynomial is $x^{16}+x^{12}+x^5+1$, and the corresponding number is 11021_{hex}. Shift 16 bits to the left.*
- *ANSICRC16: the polynomial is $x^{16}+x^{15}+x^2+1$, and the corresponding number is 18005_{hex}. Shift 16 bits to the left.*
- *CRC32: the polynomial is $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x^1+1$, and the corresponding number is $104C11DB7_{hex}$. Shift 32 bits to the left.*"

How to Choose Suitable CRC Algorithm?

The CRC error detection capacity is evaluated by undetected probability, i.e., the probability that error cannot be identified. Generally speaking, the undetected probability of CRC is less than $1/(2^n)$, where n denotes the length of redundancy bits. CRC16 is qualified in the case of few data, while CRC32 is usually used for the check of the entire document. When choosing CRC algorithm, CRC-32 algorithm with large-scale computation is not employed since some programs have to be operated in Single Chip

Microcontroller Module. However, the error rate of CRC-8 algorithm is 1/256, this system is enough. Therefore, this system chooses CRC-8 algorithm.

3.2.2.4 Designing Principle of CRC-8 Code Check

The polynomial of CRC-8 is $x^8+x^5+x^4+1$ and the corresponding number is Ox131.

Since the ordinary division method is complicated and the remainder may be more than 8 bits, the modulo-2 division is used in the algorithm, i.e., using XOR operation to replace the subtraction. Thus, the borrow issue can be neglected. Because the highest bits of the dividend and the divisor are 1, and the result of XOR operation will be zero, the remainder can be limited within 8 bits. Therefore, only 8-bit XOR operation is needed in practice. The polynomial code generated by the CRC8 is 0x31. The modulo 2 division can be summarized as the shift operation for the dividend from high to low bit by the binary rule, and then the check of each bit. If the quotient is 0, the treatment is unnecessary. If the quotient is 1, the XOR operation should be conducted between the next 8 bits and the divisor polynomial. The final quotient should be eliminated, and the resulting remainder is the required CRC code.

3.2.2.5 Software Design and Implementation of CRC-8 Check

The software design flow of CRC-8 is show in figure 7. CRC-8 Code implementation see appendix B.

1) At first, one byte of 0 should be added to the end of the data block to be transmitted (CRC buffer).

2) If the highest bit of the fist 8-bit byte is 1, conduct the XOR operation between 8 bits in the CRC register and the highest bit of the sum of the rest bits and the next data. Then, save the result into the CRC buffer.

3) If the highest bit is 0, then import the highest bit of the next data. If 1, then repeat Step 2.

4) Repeat Steps 2 and 3 until the eight shifts are completed. This ends an 8-bit data processing.

5) Repeat Steps 2-4 until all the data processing is completed.

6) The final content of the CRC buffer is the CRC value.

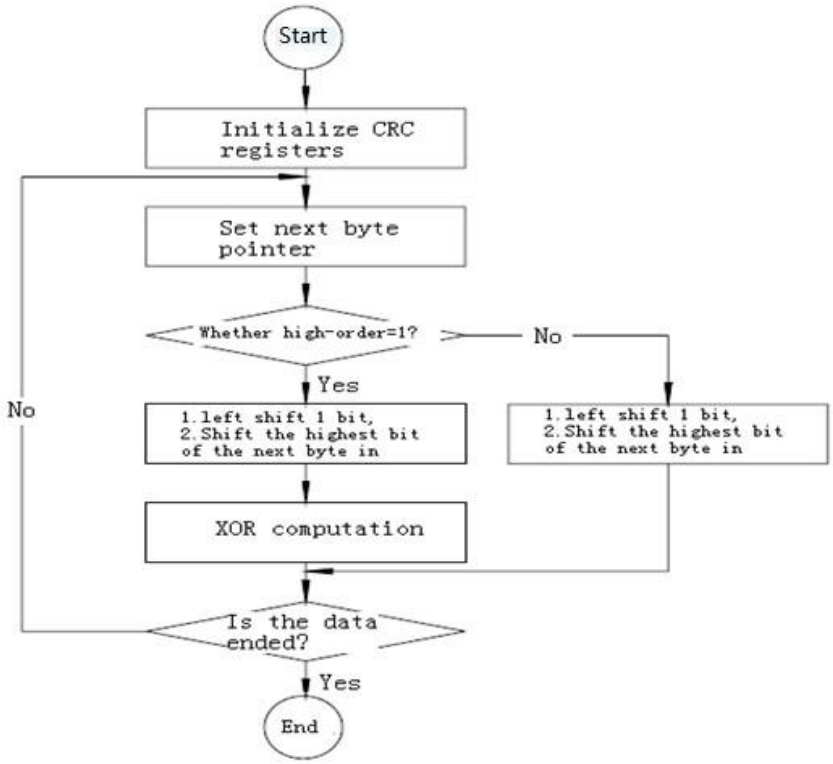

Figure 7

3.2.3 Retransmission Module Design

After the receipt of data, the receiving terminal obtains a hexadecimal check value according to the CRC check. Compare it with the transmitted code value. If they are equal, no error occurs in the transmission and a correct-receiving response signal will be transmitted to the sending terminal; otherwise there is error code in the received message, and response signal demanding retransmission will be sent to the sending terminal. This is known as Automatic Repeat-reQuest (ARQ) mode [16]. After investigation, it would be better to let the retransmission times be 3. Too many times of retransmission result in a long-time occupation of the channel and influence the communication of other units and itself. On the contrary, if the retransmission times are few, correct receipt is unavailable when the channel suffers from strong disturbances and is unstable. The retransmission modular schematic is show in figure 8.

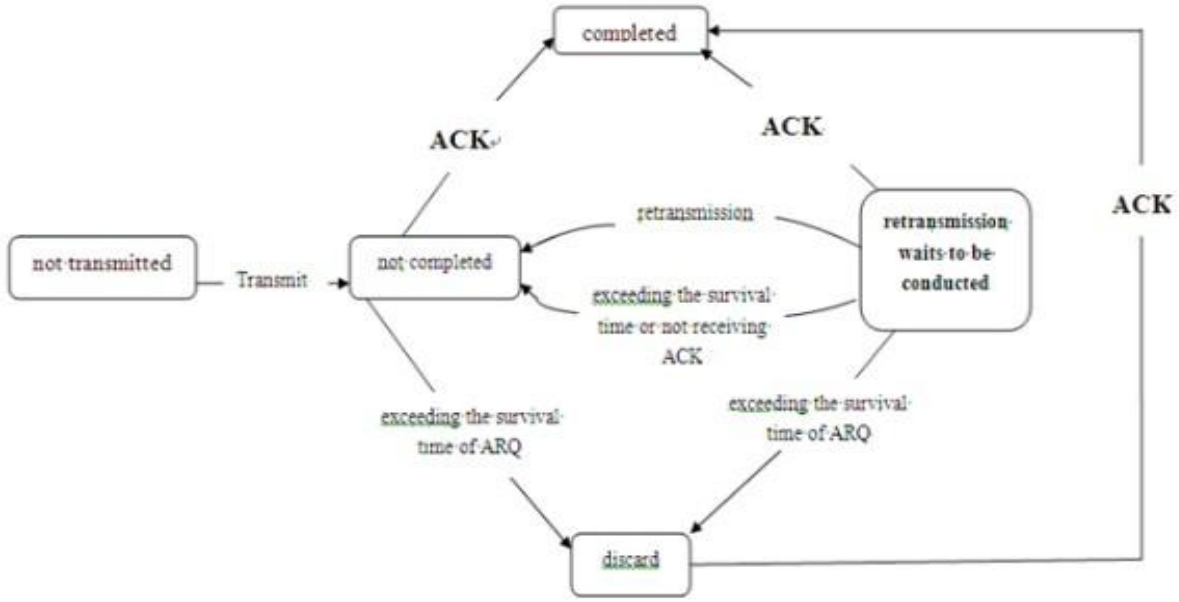

Figure 8

Conclusion: For the future development, this retransmission could better to feedback the error information. If the error occurred in the transmission, the system could resend the last information automatically, so people don't need to do it again by hand. But the module is too complex for this application, and there exceed knowledge for us. If once the card failed, just retry until the card get passed.

4 Simulation

Assume the information that needed check is {1,2,3}. After convert the binary code is 0000 0001 0000 0010 0000 0011. The polynomial that we choose is $x^8+x^5+x^4+1$. After convert the binary code is 1 0011 0001. We calculate the check result by hand first(following the Fig.7). Calculate the check result by hand is show in figure 9.

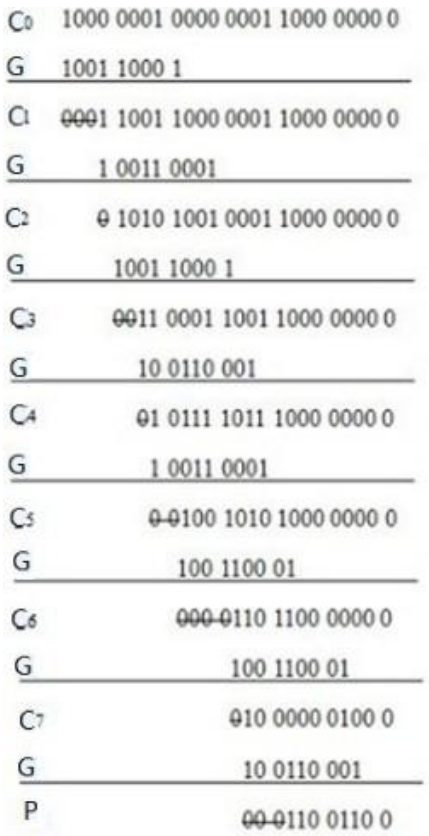

Figure 9

The remainder is 1100 1100.

Then we use the CRC8 program that we designed to operating.Call the CRC8 program that named CHECK_CRC8, and entry the information that needed to check. The whole program is show in appendix C.

The screen shot after a test run with the same input data as above is in Figure 10.

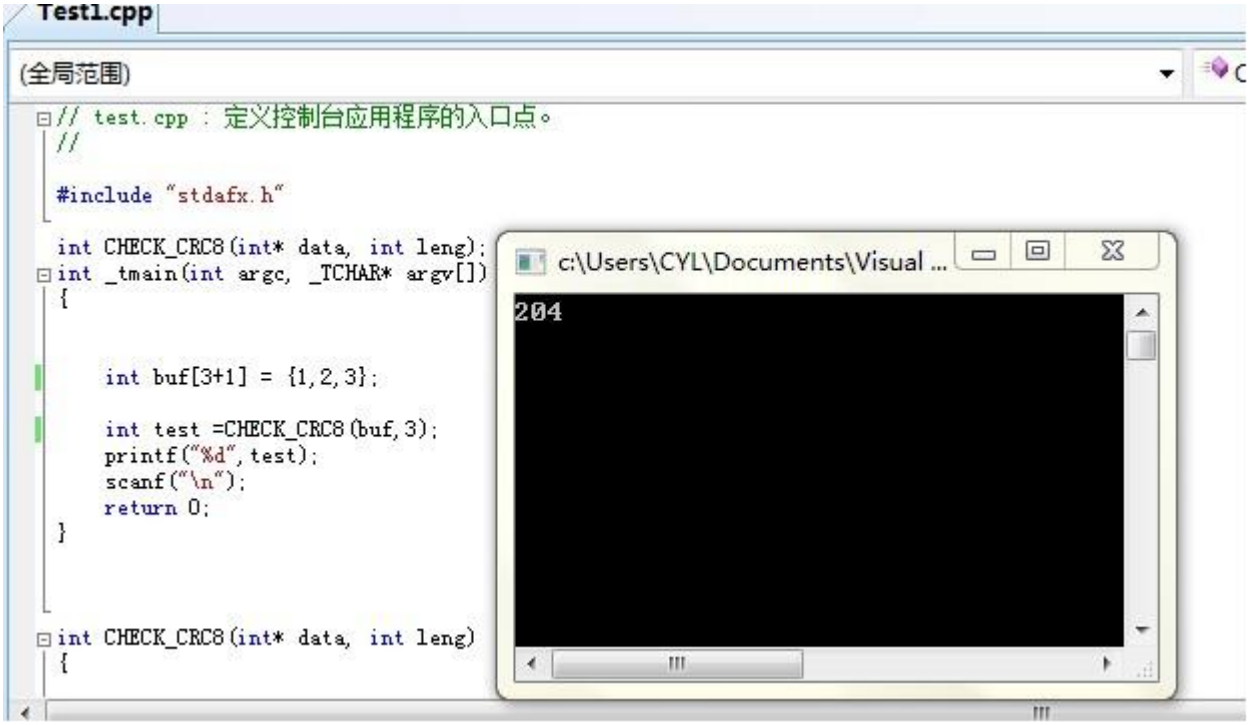

Figure 10

The result is 204. After convert the binary code is 1100 1100. Then it equal the result by hand.

More test results are show in this table:

Input	**Manual Result**	**Program Result(dec)**	**Convert to Binary**	**Match**
1,2,3 **(0001 0000 0010 0000 0011)**	**1100 1100**	**204**	**1100 1100**	**Yes**
8,9,10 **(1000 0000 1001 0000 1010)**	**0100 1010**	**74**	**0100 1010**	**Yes**
11,21,31 **(1011 0001 0101 0001 1111)**	**1110 1100**	**236**	**1110 1100**	**Yes**

5 Discussion

5.1 Problems in the implementation of CRC check module

5.1.1 When the CRC check fails, how to solve data loss?

Constrained by channel characteristic and various disturbances, errors are inevitable in the data received by the receiving terminal during communication, which influence the data reliability. Therefore, we adapt the concept of ARQ.

On the other hand, retransmission needs to occupy channels, which may cause more channel congestions and conflicts. Moreover, retransmission consumes more energy, which greatly influences the performance of wireless network that restricts energy consumption. Therefore, in order to guarantee the validity of data, we need to handle the following problems: whether to retransmit, how many times to retransmit and how to choose when retransmitting.

Through by investigation we have found that three retransmissions can meet the requirements of both performance and security.

5.2 Next Research Direction

5.2.1 Error Correcting Function of CRC algorithms

In this dissertation, only the error detecting function of CRC check is employed in systems, but its error correcting function is not.

The future work should include the utilization of the error correcting function of CRC check. By this way, we can guarantee the completeness of the data to some extent at the receiving terminal. Then, the burden on the data link and the communication delay can be reduced, and the overall performance of the system can be improved.

When the receiving terminal receives CRC codes, the generated polynomial G(x) will be divided by 2. The relationship between the resulting remainder and the error bits only depends on the code system and the generated polynomial, but independent of the code (information bits) to be measured.

If any bit of the cyclic code is wrong, the remainder of G(x) modulo 2 is not 0. Adding 0 to the remainder and then continuing this process, we will see that the remainders cycle in some order. So we

can find a one-to-one relationship between the remainder and error bit. The corresponding relationship between remainder and error bit is show in figure 11.

	CRC digit received							remainder	error bit
digit position	A7	A6	A5	A4	A3	A2	A1		
correct	1	0	1	0	0	1	1	000	none
wrong	1	0	1	0	0	1	0	001	1
	1	0	1	0	0	0	1	010	2
	1	0	1	0	1	1	1	100	3
	1	0	1	1	0	1	1	011	4
	1	0	0	0	0	1	1	110	5
	1	1	1	0	0	1	1	111	6
	0	0	1	0	0	1	1	101	7

Figure 11

If the first bit is wrong, the remainder is 001. Adding 0 and repeating the division, we obtain the second remainder 010. Continuing this process, we will obtain 100, 011, ..., which cycle. This is the origin of the name "cyclic code". Such feature is valuable. If the remainder obtained is not 0, we add 0 to the remainder to continue module-2 division and, at the same time, cyclically shift the checked code to the left. When the remainder is 101, the error bit also shifts to the position of A7. Through an XOR gate, it can be moved back to A1 in the next shift after being corrected. In this way, we do not need any decoding circuit to provide correction conditions for each bit as in Hamming check.

The CRC algorithm can only detect single-bit errors. For example, CRC8 can only check 8-bit data.

5.2.2 Optimization of ARQ

a) Currently, the time between retransmission data is mainly determined by the major cycle times, which cannot control time intervals exactly. In the future investigation, the retransmission time control can be done by timers of Microcontroller and the accuracy can be guaranteed to the level of microsecond.

b) Considering temporary communication errors, such as that the receiving terminal does not give any response signal to the sending terminal because of instantaneous busyness, it is suggested to reduce receiving delay by reducing the first retransmission time and to increase the retransmission times in several seconds as much as possible. In this way, the transmission can be achieved after several seconds such that users cannot feel the delay.

c) For abnormal network errors (i.e., unable to connect to receiving terminal), retransmission can be paused until the connection returns to normal.

Reasonable configuration of ARQ can effectively improve the receiving delay. For some errors caused by network and user factors, decreasing the first retransmission time and increasing retransmission times can significantly decrease the active retransmission delay and improve the optimization effect. However, in some cases it is also possible that the optimization effect is not obvious. Taking the system load condition into consideration, we can increase the retransmission times of the former and decrease the retransmission times of the latter, so as to reduce the influence on exchange and wireless network loads.

The optimization of ARQ is only a remedial measure for exchange and abnormal cases of wireless network. Therefore, to improve the receiving delay of short messages as much as possible, we need to combine the optimization of exchange and wireless network.

6 Conclusion

- In this dissertation, as a part of the Zigbee-based meeting attendance registration system, a detecting system has been designed to deal with the errors in wireless transmission of data information.
- After comparison study of several different check algorithms, we have chosen the CRC check owing to its powerful detection capability. Moreover, according to practical situations, a CRC-8 check module has been designed.
- In view of data reliability, we study the ARQ to guarantee both the validity and the completeness of data.
- We have also discussed the future investigation, especially the improvement in performance and flexibility.

References

[1] Factors Influencing Wireless Communication Quality
http://wenku.baidu.com/view/124654c7aa00b52acfc7ca8f.html [acc.2012-07-12]

[2] Houda Labiod, Hossam Afifi, Constantino De Santis, *Wi-Fi, Bluetooth, Zigbee and WiMax*, Published by Springer, Netherlands. 2007.

[3] *IEEE.802.15.4, Part 15.4*: Wireless Medium Access Control (MAC) and Physical Layer (PHYl) Specifications for Low—Rate Wireless Personal Area Networks (LR-WPANs). October 2003

[4] Wang Ping, Wang Quan, Wang Heng and Xiang Min. *Radio Communication Technology for Measurement and Control* [M]. Beijing. Publishing House of Electronics Industry. 2008.

[5] Chipcon, *Packet Sniffer for IEEE802.15.4 and ZigBee[S]*. User Manual. Oslo. Norway, Oct. 2004

[6] Li Wenzhon and Duan Chaoyu, *The Introduction and Practice of ZigBee Wireless Network Technology*, Beijing: Press of Beijing University of Aeronautics and Astronautics2007.

[7] Dr.S.S.Riaz Ahamed , *THE ROLE OF ZIGBEE TECHNOLOGY IN FUTURE DATA COMMUNICATION SYSTEM*, Professor & Head, Dept of Computer Applications, Mohamed Sathak Engg College, Kilakarai & Principal, Sathak Institute of Technology, Ramanathapuram, TamilNadu, India-623501.
http://www.jatit.org/volumes/research-papers/Vol5No2/5Vol5No2.pdf [acc.2012-07-12]

[8] Fuchang WANG, Xiaoming PAN, *Experiment of Communication Theory*, Tsinghua University Press, China, 2007

[9] Jeffrey S. Beasley, Gary M. Miller, *Modern electronic communication*, Ninth Edition. Pearson/Prentice Hall, cop. New Jersey.2008

[10] Walma, Mathys IC3N, *Pipelined Cyclic Redundancy Check (CRC) Calculation*, Computer Communications and Networks, 2007 Proceedings of 16th International Conference on; Honolulu, HI, 2007

[11] Ping`an ZHANG, *An Analysis of the Principle and Performance of 16- bit Circulation Redundancy Check (CRC)*, Shanxi Science and Technology, 2005(5)

[12] Guogu YAN, *C Language Realization of a Rapid Algorithm of CRC checks*, Science 2010, the seventh issue, p.128.

[13] Cheng, C.Parhi, K.K. "High-Speed Parallel CRC Implementation Based on Unfolding, Pipelining, and Retiming" *IEEE transactions on circuits and systems. II, Express briefs*, EI SC I 2006 10

[14] Evgeni Stavinov "*A Practical Parallel CRC Generation Method*", Circuit cellar, 2010 Jan. TN.234

[15] *On-line CRC calculation and free library* http://www.lammertbies.nl/comm/info/crc-calculation.html [acc.2012-07-12]

[16] Suoping LI, Shijun LU "*Delay Performance of SW-ARQ System with Limited Number of Retransmission Based on Adaptive Frame-Size Technique*", School of Science, Lanzhou Univ. of Tech., Lanzhou 730050, China

[17] Yan Sun, Min Sik Kim "*A Pipelined CRC Calculation Using Lookup Tables*" 2010, 7th, IEEE Consumer Communications and Networking Conference (CCNC 2010). Las Vegas, Nevada, USA

[18] Zulin WANG, "*Table Look up Algorithm and Implementation of the Cyclic Redundancy Check Mode*", Journal of Beijing University of Aeronautics and Astronautics (August 1996 vol.22, the 4th issue)

[19] Zhijie GUAN, "*The Design and Realization of the Meeting Attendance Registration System*", TongJi University Software College, Master's Degree Thesis, 20090601

Appendix A

CRC Remainder Table

{/* CRC Remainder table */

0x00, 0x5e, 0xbc, 0xe2, 0x61, 0x3f, 0xdd, 0x83, 0xc2, 0x9c, 0x7e, 0x20, 0xa3, 0xfd, 0x1f, 0x41, 0x9d, 0xc3, 0x21, 0x7f, 0xfc, 0xa2, 0x40, 0x1e, 0x5f, 0x01, 0xe3, 0xbd, 0x3e, 0x60, 0x82, 0xdc, 0x23, 0x7d, 0x9f, 0xc1, 0x42, 0x1c, 0xfe, 0xa0, 0xe1, 0xbf, 0x5d, 0x03, 0x80, 0xde, 0x3c, 0x62, 0xbe, 0xe0, 0x02, 0x5c, 0xdf, 0x81, 0x63, 0x3d, 0x7c, 0x22, 0xc0, 0x9e, 0x1d, 0x43, 0xa1, 0xff, 0x46, 0x18, 0xfa, 0xa4, 0x27, 0x79, 0x9b, 0xc5, 0x84, 0xda, 0x38, 0x66, 0xe5, 0xbb, 0x59, 0x07, 0xdb, 0x85, 0x67, 0x39, 0xba, 0xe4, 0x06, 0x58, 0x19, 0x47, 0xa5, 0xfb, 0x78, 0x26, 0xc4, 0x9a, 0x65, 0x3b, 0xd9, 0x87, 0x04, 0x5a, 0xb8, 0xe6, 0xa7, 0xf9, 0x1b, 0x45, 0xc6, 0x98, 0x7a, 0x24, 0xf8, 0xa6, 0x44, 0x1a, 0x99, 0xc7, 0x25, 0x7b, 0x3a, 0x64, 0x86, 0xd8, 0x5b, 0x05, 0xe7, 0xb9, 0x8c, 0xd2, 0x30, 0x6e, 0xed, 0xb3, 0x51, 0x0f, 0x4e, 0x10, 0xf2, 0xac, 0x2f, 0x71, 0x93, 0xcd, 0x11, 0x4f, 0xad, 0xf3, 0x70, 0x2e, 0xcc, 0x92, 0xd3, 0x8d, 0x6f, 0x31, 0xb2, 0xec, 0x0e, 0x50, 0xaf, 0xf1, 0x13, 0x4d, 0xce, 0x90, 0x72, 0x2c, 0x6d, 0x33, 0xd1, 0x8f, 0x0c, 0x52, 0xb0, 0xee, 0x32, 0x6c, 0x8e, 0xd0, 0x53, 0x0d, 0xef, 0xb1, 0xf0, 0xae, 0x4c, 0x12, 0x91, 0xcf, 0x2d, 0x73, 0xca, 0x94, 0x76, 0x28, 0xab, 0xf5, 0x17, 0x49, 0x08, 0x56, 0xb4, 0xea, 0x69, 0x37, 0xd5, 0x8b, 0x57, 0x09, 0xeb, 0xb5, 0x36, 0x68, 0x8a, 0xd4, 0x95, 0xcb, 0x29, 0x77, 0xf4, 0xaa, 0x48, 0x16, 0xe9, 0xb7, 0x55, 0x0b, 0x88, 0xd6, 0x34, 0x6a, 0x2b, 0x75, 0x97, 0xc9, 0x4a, 0x14, 0xf6, 0xa8, 0x74, 0x2a, 0xc8, 0x96, 0x15, 0x4b, 0xa9, 0xf7, 0xb6, 0xe8, 0x0a, 0x54, 0xd7, 0x89, 0x6b, 0x35, }

Appendix B

```
byte GetCRC(byte *data, int leng)
{
   byte buf[leng + 1];
   byte key = 0x31;    //Abandon the highest-digit x8 of the simple code of x8+x5+x4+1 to attain
   byte crc1, crc2;
   int ptr = 0;
   int i;
   int count = leng;
   buf[leng  - 1] = 0;
   memcpy(buf,data,leng );
   crc1 = buf[ptr++];
   while (--count >= 0)
  {
    crc2 = buf[ptr++];
    for (i = 0; i < 8; i++)
   {
     if (((crc1 & 0x80) >> 7) == 1)// the highest digit is
     {
       crc1 = (byte)(crc1 << 1); // Shift the high digit
       if (((crc2 & 0x80) >> 7) == 1)// if the high digit of crc2 is
       {
         crc1 = (byte)(crc1 | 0x01); //crc1 Low digit change
                    }
       crc1 = (byte)(crc1 ^ key);// XOR computation
       crc2 = (byte)(crc2 << 1); // Shift high digit
                 }
       else
       {
        crc1 = (byte)(crc1 << 1); // Shift high digit
        if (((crc2 & 0x80) >> 7) == 1)// if the high digit of crc2 is
        { crc1 = (byte)(crc1 | 0x01); //crc1 low digit change
         }
                 crc2 = (byte)(crc2 << 1); // shift high digit
       }
     }
   }
         return crc1;
```

Appendix C

```
#include "stdafx.h"

int CHECK_CRC8(int* data, int leng);
int _tmain(int argc, _TCHAR* argv[])
{
                int buf[3+1] = {1,2,3};
                int test =CHECK_CRC8(buf,3);
                printf("%d",test);
                scanf("\n");
                return 0;
}

int CHECK_CRC8(int* data, int leng)
{

  int buf[255+1];
  int key=0x31;
  int crc1,crc2;
  int i;
  int ptr=0;
  int counter=leng;
  for(int c = 0;c<256;c++)
  {buf[c] = 0;}
  memcpy(buf,data,leng*(sizeof(int)));
  crc1=buf[ptr++];
  while(--counter>=0)
  {
    crc2=buf[ptr++];
    for(i=0;i<8;i++)
    {
      if(((crc1&0x80)>>7)==1)
      {
        crc1=(int)(crc1<<1)&0xFF;
          if(((crc2&0x80)>>7)==1)
          {
            crc1=(int)(crc1|0x01);
          }
          crc1=(int)(crc1^key);
                                                  crc2=(int)(crc2<<1);
      }
      else
```

```
        {
          crc1=(int)(crc1<<1)&0xFF;
            if(((crc2&0x80)>>7)==1)
            {
              crc1=(int)(crc1|0x01);
            }
                                                    crc2=(int)(crc2<<1);
        }
      }
    }
        return crc1;
}
```