www.sensorsportal.com

Sensors & Transducers

© 2014 by IFSA Publishing, S. L.
http://www.sensorsportal.com

Design of Wireless Point of Sale Based on ZigBee Technology

Xiaoning Jiang, Shaoju Chen,
Zhejiang Gongshang University,
18, Xuezheng street, Xiasha, Hangzhou, 310018, China
Tel.: 0086-15858285447
E-mail: csj_881020@163.com

Received: 20 November 2013 /Accepted: 28 January 2014 /Published: 28 February 2014

Abstract: With the rapid development of Point of Sale technology and modern communication technology, financial Point of Sale terminal system has been started from wired to wireless. Wireless payment technology can used where can't rely on or even no cable network. As one of the most important technologies in the information era, Wireless Sensor Network has been widely used in banking business and other various modem business fields. This paper describes a kind of simple portable Point of Sale terminal based on the ZigBee wireless network [1], which is a low power, low cost, flexible, safe and reliable network. This Point of Sale system can be applied gas stations, liquefied petroleum gas stations and other complex sales environment, and it improves safety of gas station and personnel safety. Simple and user-friendly, this formula design and optimization method greatly improves efficiency and thus has much value for practical application. *Copyright © 2014 IFSA Publishing, S. L.*

Keywords: Point of sale, Wireless network, ZigBee, Security, Gas station.

1. Introduction

Point of Sale (POS) is a kind of multi-functional terminal, which is installed in the credit card specially engaged and accepting network. When it is connected with the computer network, it can provide electronic accounts of automatic operation, for example, consumption, preauthorization, balance inquiries and transfer functions. It has many advantages such as convenience and shortcut and safety and credibility and so on. Such advantages make it indispensable in the field of commercial transaction.

In recent years, the number of POS which we need increases quickly with the development of retail and finance of the bank. However, the overall level of bank cards is still in early stages, which restricts the expansion of bank card business credit. One of the main factors is the shortage of laying hardware devices, leading to fail to the flexible, efficient, fast, safe payment with credit card. How to break through the restriction better has become the urgent task of Banks.

Along with a variety of wireless technology continues to keep developing itself, the use of wireless technology make transmitting financial data possible, and the value of wireless POS business can be fully reflected. Wireless POS application system releases developers from the constraints of space and line, explores the financial services, at the same time, it increases the competitive power of itself and brings a lot of new deposits for development.

However, some sales environments, such as gas stations, liquefied petroleum gas (LPG) stations, are poor and gas concentration is higher in the air, especially in summer, because high temperature contributes to faster release of gasoline refueling [2]. When it reaches a certain concentration, any small spark or invisible electrostatic would cause an explosion. The higher the transmission frequency, the easier it easy to cause sparks. Data show, GPRS transmit frequency of about 4 V, CDMA transmit frequency of about 0.2 V, but due to the changes of temperature, weather, easy to cause the change of gas concentration in the air, it makes use of GPRS or CDMA equipment with unpredictable factors. This kind of explosion has occurred in the world and our country due to the precedent of using mobile phones. Therefore, using a wireless POS device needs to take into account the transmit frequency and a kind of smaller emission frequency wireless POS is a good choice. From resources to maximize the use of point of view, GPRS and CDMA are wide-area wireless networks, is more suitable for larger areas. While the establishment of the above two networks will cause the resource waste in this special environment of the gas station, so these two are not the best choice.

To solve these problems, this paper proposes an approach of wireless POS based on ZigBee wireless network with low power consumption, low cost, flexibility and other characteristics. ZigBee, a low power wireless personal area network protocol, is set by the ZigBee alliance based on IEEE802.15.4 standard [3]. ZigBee is a short-range, low complexity, low power, low data rate, low-cost two-way wireless communication technology, mainly used in the field of automatic control and remote control, and can be embedded in various devices. In short, ZigBee is a kind of wireless networking in order to meet the small cheap equipment and control of wireless network communication technology.

2. Related Works

As a convenient and efficient means of communication, wireless communications has been used in many industries. With the application of advanced wireless communication means, wireless POS products which greatly facilitates the cardholder and widens the applications of POS, is a strong impetus to the bank card business. Currently, wireless POS payment technology types are: wireless LAN access, GSM short message access, GSM wireless dial-up access, GPRS wireless access, CDMA wireless access.

Because restrictions on the radiation is high in gas stations, LPG stations, aircraft and other complex environment, high transmit power modes, such as GSM short message access, GPRS wireless access, CDMA wireless access, are not suitable for these special work environment. Therefore, the only choice is a low-power, low-cost wireless LAN access, this article presents a wireless sensor network based on ZigBee for wireless POS.

In formulating the ZigBee standard, ZigBee Alliance adopted the IEEE802.15.4 as its physical layer and the media access layer specification [3]. On its basis, ZigBee alliance made the data link layer (DLL), the network layer (NWK) and application programming interface (API) specifications [1], and is responsible for the high-level application, testing, and marketing efforts, etc. ZigBee protocol jointly proposed by the five companies: Honeywell, Invensys, Mitsubishi Electric, Motorola and Philips. IEEE802.15.4 Working Group for ZigBee defines three from right of frequency bands: 2.4 GHz (Global application) in the world, 915 MHz (US) and 868 MHz (Europe).

ZigBee uses DSSS technology in place of FHSS technology. Compared with other wireless communication technology such as Bluetooth (Table 1), it has the following characteristics:

Table 1. ZigBee compared with other wireless technology.

Type	Wi-Fi	Bluetooth	ZigBee
Operating Frequency	2.4 GHz, 5 GHz	2.4 GHz	868 MHz, 915 MHz, 2.4 GHz
Transmission rate	11 Mbps, 54 Mbps	720 Kbps,	20 Kbps, 40 Kbps, 250 Kbps
Network node	32	7	65 K
Power	10-50 mA	20 mA	5 mA
Security	Low	High	Middle
Cost	25 $	2-5 $	5 $
Main applications	Date Transmission	Date and Voice Transmission	Monitoring, Control

Low power consumption: ZigBee Alliance website shows, in terms of general battery power, ZigBee products can be used for a few months to several years. It is ideal for those who need a year or even longer before the need to replace the battery device (such as the typical monitoring equipment).

More access devices: ZigBee networks can support a larger number of devices and a longer range between devices than Bluetooth. ZigBee solutions support each network coordinator with 255 active nodes (Bluetooth only eight) and multiple network coordinators can join a large network. ZigBee technology allows contains more than 65000 nodes in a network.

Lower cost: Without the host platform, ZigBee can be realized only with 80C51 sort of low-end processors and a small amount of software. From the antenna to the application, it only takes one chip to achieve. But Bluetooth needs to rely on stronger main processor (such as ARM7), and its chip architecture is more complex.

Lower transmission rate: ZigBee low power leads to the low transmission rate, the original data throughput rate at 2.4 GHz (10 channels) spectrum of 250 Kbps, at 915 MHz (6 channels) spectrum of

40 Kbps, at 868 MHz (channel 1) spectrum of 20 Kbps. Transmission distance is 10 ~ 75 m.

3. The System Scheme

ZigBee-based POS system adopts TI's wireless SoC integrated chip CC2530, which is based on TI's ZigBee2007/Pro protocol stack, i.e., Z-Stack software architecture for wireless ad hoc networks. The entire wireless network is composed of a ZigBee coordinator node, n routing nodes and n terminal nodes [4]. The coordinator initializes a ZigBee wireless network, usually as a ZigBee network gateways are external systems and ZigBee network internal information exchange channel. The primary function of routing nodes is to achieve multi-hop routing. Terminal nodes are connected to the IC card reader for the realization of IC card read and write as well as the related IC card information collection. At the same time information data of terminal nodes are encrypted and transmitted to PC terminal depending on routing nodes and the coordinator node. PC is connected with the coordinator via a serial port in order to realize the upper machine control. System block diagram is shown in Fig. 1.

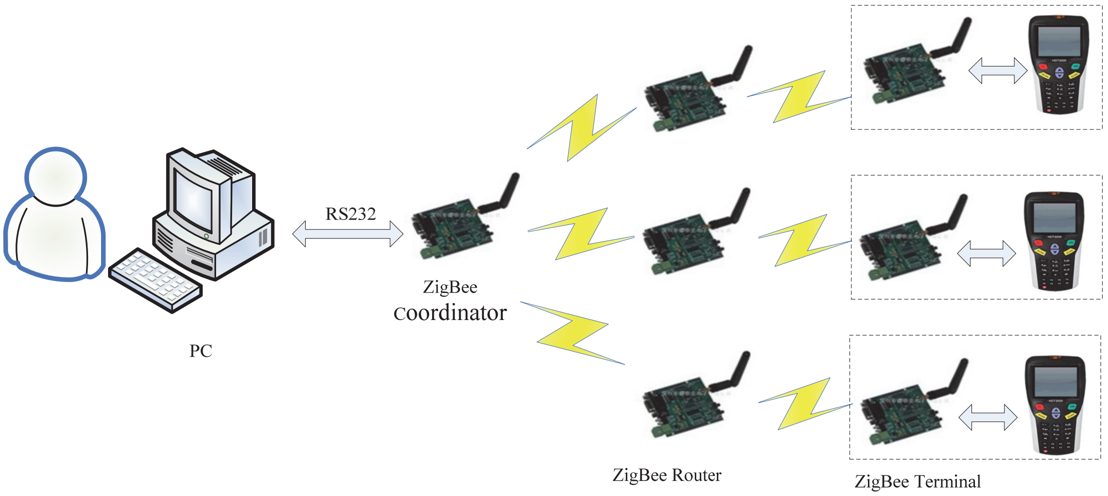

Fig. 1. ZigBee-based wireless POS system block diagram.

3.1. Hardware Design

Hardware part adopts modular design method, divided into CC2530 core board and expansion board. CC2530 core board is designed for a module which can be combined with different expansion boards, including CC2530 chip and its peripheral circuit. This module leads CC2530 main I/O ports combined with an expansion board. According to different functions, expansion board is divided into three boards: coordinator node, routing node and terminal node. Fig. 2 is a block diagram of the hardware design of ZigBee module.

As the role of gateway, coordinator node does not require a direct connection with the IC card, but indirectly through routing nodes for terminal nodes transaction information with IC cards. So you don't have IC card reader module design. Meanwhile, because the coordinator node must remain active, it uses 220 V AC/DC regulated power supply converter module power supply and designs the power switch. UART serial port is completed by the serial level converter chip for connection to the host computer. Download programming interface is used to connect the TI CC DEBUGGER simulator for simulation and downloading the program. Led indicator part used to indicate the node working condition.

Coordinator node's function can meet the function of routing nodes, so the routing nodes' hardware circuit is the same as the coordinator. The main achievement of Zigbee terminal node is capturing smart cards information, therefore a terminal node need a keyboard module and a smart card reader. What's more, the communication protocol between smart card readers and terminal nodes is the ISO7816 protocol.

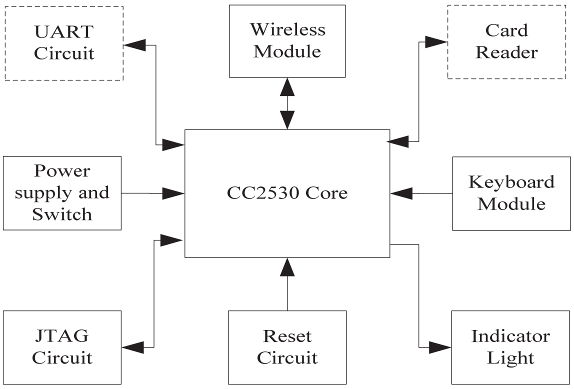

Fig. 2. ZigBee module hardware design diagram.

3.2. The Establishment of the Network

The ZigBee protocol stack consists of physical layer, link layer and network layer. ZigBee network layer has discovered devices and establish a wireless link between devices, and it supports three kinds of topology network: star structure (star), cluster structure (Cluster tree) and mesh structure (Mesh). This realization of the POS system uses the Mesh network structure [5] which network has high reliability and scalability, because it can provide more than one network path.

The mesh network structure is a self-organizing network, which uses a dynamic routing. Dynamic routing refers to the network data transmission paths that are not set in advance, but before the data transmission, searches for all available paths from the network, analyses their position relationship of distance, and then selects one of the paths for data transmission. Similar in network management software, the choice of path uses the gradient method, which is to choose the path of a recent channel transmission, such as transmission barrier, and then use another one a little further path for transmission, and so on, until the data delivery destination. In actual gas station scene, due to environmental complexity and the staff moved a predetermined transmission path may change at any time, or the path is interrupted for various reasons, or too busy to deliver timely. Dynamic routing combined with mesh topology, can solve this problem very well, so as to ensure reliable data transmission, and this is very important in terms of site control in gas station.

In ZigBee protocol stack, the realization of the mesh network is to make ZigBee defined between all sorts of equipment, be connected in the form of mesh network, transmit data and control signals. Because ZigBee application layer in the protocol stack, different vendors provide application framework model is different in the application layer of the ZigBee protocol stack, so we only analyze the network layer and the MAC and physical layer transmission implementation process. This process must use primitives defined in ZigBee layers to provide services. The primitive services have nothing to do with the providers so that it is defined as any other implementation -independent interface to make this method is versatile.

Firstly, you need to complete the establishment of networks. A new network is completed by the coordinator in Z-stack, and uses the *NIME _NETWORK_FORMATION.request* primitive to start the wireless network.

NIME_NETWORK_FORMATION.request (
Sanchannels, // scan channel
ScanDuration, // scan time
BesconOrder, // network beacon frame number
SuperframeOrder, // network frame number
PANID, // network identifier
BatteryLifeExtension)

After building a network, the network layer management entity will find a suitable channel and the identifier PANID which is defined in the new network is written to *macPANID* attribute for the MAC layer properties. Then, select one 16-bit network address that is equal to 0x0000, and set the *macShortAddressPIB* attribute of the MAC layer to make it equal to the selected network address. After this process is completed, the coordinator initialization is completed and routing devices can use *NINE_PERMIT_JOINING. Request* to join the network, and connect with the coordinator node for communication.

NINE_PERMIT_JOINING.request (Permit Duration) // connection time allowed by coordinator
NLME_PERMIT_JOINING. confirm (Status)

When the coordinator completed the network connection, the frame transmission of the network layer uses *NIDE_DATA.request* primitive to issued data transfer request and then uses *NLDE_DATA.confirm* primitive to return the requested results.

NLDE_DATA. request (
DstAddr, //NSDU destination network address
NsduLength, // Number of NUSU bytes
Nsdu, // NUSU
NsdyHandle, // NUSU correlation handle
BroadcastRadius, // Broadcast frames transmission distance allowed
DisoverRoute, // Allow the route discovery or not
SecurityEnable) // Enable the network layer security or not

When primitive *DisoverRoute* parameter is TRUE, the network layer will calculate and search routing paths through the AODV routing algorithm, and establish a routing table entry of equipment, and then create a command frame carrying the payload routing request. All network layer transmission data frame contains a destination address and source address. In the MAC layer, public sub-layer entity sends this data frame to the MAC layer of the connected device by using *MCPS_DATA.request* primitive.

MCPS_DATA.request (
SrcAddrMode, // Source Address Mode
SrcPANID, // Source entity identifier
SrcAddr, // Source Device Address
DstAddMode, // Destination address mode
DstPANID, // Destination entity identifier
DsrAddr, // Destination device address
msduLength, // Entity bytes
msdu, // Entity Data Unit
msduHandle, // Entity handle
TxOptions) // Transmit mode

Finally, you also need the MAC layer would like to send *LAME_SET_TRX_STATE.request* primitive with *TX-ON* state to the physical layer, activate the device transmitters. When the MAC layer receives, it will send a constructed data unit be good data unit to the physical layer by the *PD_DATA. Request* primitive. If the MAC layer receives *PD_DATA.confirm* primitive, this data unit will be sent to the connected destination device by the transmitter unit. At this point, data is transferred to the destination device and the network communication function is completed.

3.3. Security Policy

POS system is mainly used for bank card or other financial IC card transactions. This is a commercial transaction. The POS credit card spending in the process, involves a lot of financial information and personal privacy, and therefore requires more than the IC card transaction information confidential, but also need to take security measures to the users' information. On this point, ZigBee protocol uses the corresponding security policies to avoid data security property being destroyed, that is, to protect data confidentiality, integrity and availability.

The stack architecture of ZigBee standards (Showed in Fig. 3) is defined according to the market and the actual needs. IEEE802.15.4 standards defines the bottom: the physical layer (PHY) and medium access control layer (MAC) layer. On this basis, the ZigBee Alliance defines the architecture of the network layer (NWK) and application layer (APL). And furthermore the application layer includes the application support sub-layer (APS) and the application framework Layer (AF).

From the ZigBee standard stack architecture diagram, it can be clearly seen ZigBee security policies were deployed at the MAC layer and the NWK layer. Hop on the data arrives at its destination, ZigBee MAC layer provides only security mechanism; when in the case of multi-hop, ZigBee is necessary to ensure the safety of high-level dependent.

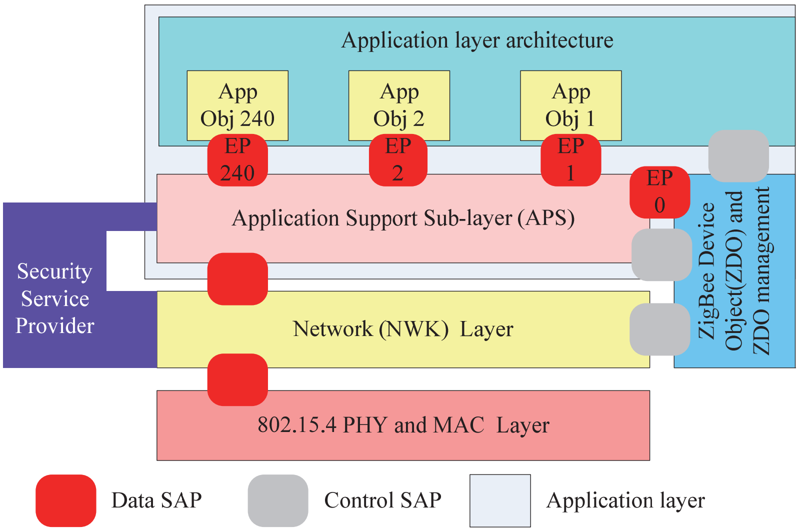
Application layer architecture
App Obj 240
App Obj 2
App Obj 1
EP 240
EP 2
EP 1
EP 0
Application Support Sub-layer (APS)
Security Service Provider
Network (NWK) Layer
802.15.4 PHY and MAC Layer
ZigBee Device Object(ZDO) and ZDO management
Data SAP
Control SAP
Application layer

Fig. 3. The stack architecture of ZigBee.

ZigBee uses AES-128 (key and data block length is 128) [6] of the CCM* encryption mode. CCM* encryption mode is an expansion of CCM (counter with cipher block chaining message authentication code) encryption mode. It consists CCM encryption mode, at the same time can be used alone CTR mode (counter mode) and CBC-MAC (cipher block chaining-message authentication code) mode [7, 8]. CTR mode can be used to ensure secrecy, the use of CBC-MAC mode to ensure data integrity, and above both use both to ensure the confidentiality and integrity. Therefore, it can provide a variety of security solutions, and choose a message integrity code (MIC) of the length (32, 64, 128) according to security needs, to form the security level up to 8. CCM* combination model of CTR and CBC-MAC implementation process is shown in Fig. 4.

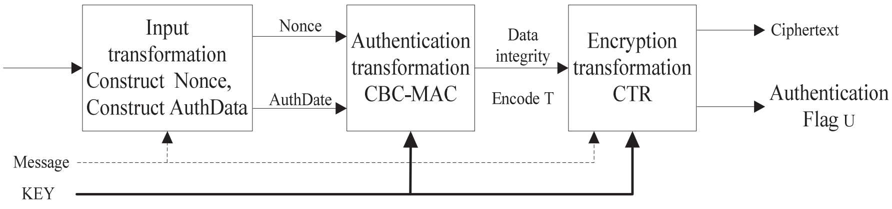
Input transformation Construct Nonce, Construct AuthData
Nonce
AuthDate
Authentication transformation CBC-MAC
Data integrity
Encode T
Encryption transformation CTR
Ciphertext
Authentication Flag U
Message
KEY

Fig. 4. CCM * encryption mode operation.

As in Fig. 4, three kinds of transformation use the following parameters:

- A bit string key, its length keylen is 128;
- The authentication data a;
- The encrypted data m;
- The length of the authentication field *M(0, 4, 6, 8, 10, 12, 14, 16)*;
- The message field length *L(2, 3, ..., 8)*;
- The length of m byte string territory is *l(m)* byte, its value scope is shown in the formula (1).

$$0 \le l(a) < 28L \text{ ,} \tag{1}$$

- The length of random *Nonce N* value domain is *15 - L*, for at any one range when using the same key, *N* value is unique;
- The length of a byte string territory is l(a) bytes, its value scope is shown in the formula (2).

$$0 \le l(m) < 2^{64} \text{ ,} \tag{2}$$

Random value *Nonce N* contains the device source address, the frame count, security control. The length of the three domains is 64,32,8 respectively. Security control field also includes three data fields: security level (3 bits), key identification (2 bits), extended Nonce (1 bit), and another two as reserved for use. There are eight security levels which are no encryption security level, *MIC-32, MIC-64, MIC-128, ENC, ENC-MIC-32, ENC-MIC-64* and *ENC-MIC-128,* and four types of key identifier: the corresponding data key, the network key, the key transmission key, the key loading key. Expansion Nonce indicates the sender's address is set in the frame auxiliary header.

3.3.1. Input Transformation

The purpose is to enter input transformation a and m, forming *AuthData* and *PlainText-Data*, for authentication transformation and encryption transformation, by these following steps:

1) Make sure forming a *L(a)* bytes string.

a) If the formula (3) can be achieved, then *L(a)* is empty;

$$l(a) = 0 \text{ ,} \tag{3}$$

b) As shown in the formula (4), If *l(a)* is in the range, then *L(a)* will encrypt *l(a)* of the two bytes;

$$0 < l(a) < 2^{16} - 2^{8} \text{ ,} \tag{4}$$

c) If *l(a)* ranges from $2^{16} - 2^{8}$ to 2^{32} as shown in the formula (5), then *L(a)* is 0xff, 0xfe, and *l(a)* of the four-byte encoding right connection;

$$2^{16} - 2^{8} \le l(a) < 2^{32} \text{ ,} \tag{5}$$

d) If *l(a)* is shown as the formula (6), then *L(a)* is the 0xff, 0xff, and *l(a)* of the eight-byte encoding right connection (right connection symbol "||").

$$2^{32} \le l(a) < 2^{64} \text{ ,} \tag{6}$$

2) Adding the authentication data as the formula (7), and the data can be divisible by 16.

$$AddAuthData = L(a) \,||\, a \,||\, 0 \text{ ,} \tag{7}$$

3) As shown in the formula (8), it is addition of message data, and the data can be divisible by 16.

$$PlaintextData = m \,||\, 0 \text{ ,} \tag{8}$$

4) The authentication data is shown in the formula (9):

$$AuthData = AddAuthData \,||\, PlaintextData \text{ ,} \tag{8}$$

3.3.2. Authentication Transformation

The purpose is to generate transformed authentication message integrity code, using the CBC-MAC mode [9]. The input parameter is a random value *Nonce N* and authentication data *AuthData*. Their calculation process of message integrity code *T* is shown in Fig. 5.

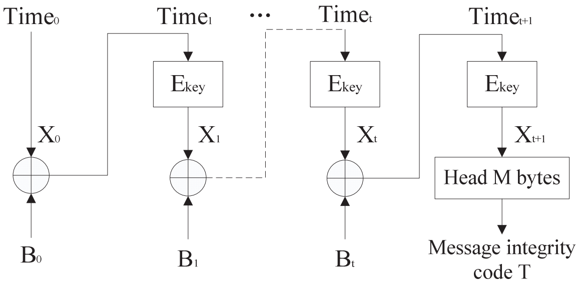

Fig. 5. CBC-MAC mode of operation.

1) To form B_0, namely the formula (10). *Reserved* is 1 bit extension reservation, used for future expansion, and it is set to 0. *Adata* is 1 bit, when *l(a)* is 0, the value is 0, otherwise 1. *L* is 3, and L represents an integer *L* - 1. *M* is 3, when *M* > 0, the value is equal to (*M* - 2) / 2, otherwise 0.

$$B_0 = Reserved \,||\, Adata \,||\, M \,||\, L \,||\, Nonce\ N \,||\, l(m) \tag{10}$$

2) $X_0 := 0^{128}$; 0^{128} stands for that all 16 bytes is 0.

3) X_{i+1}: $= E(Key, X_i \oplus B_i)$ for $i = 0, ..., t$. First decompose *AuthData* to $B_1 \| B_2 \|\ldots \| B_t$, where each data block B_i is a 16-byte string, and then XOR encode X_i and B_i, and then encrypt with Key to form X_{i+1} by the function *E*.

Message Integrity Code *T*: $= left\ (1, M, X_{i+1})$, get previous M bytes from the ciphertext X_{i+1}.

3.3.3. Encryption Transformation

CTR mode is used to encryption transformation, and the encryption process shown in Fig. 6.

Ciphertext block C_i: $= E(Key, A_i)$□M_i, for $i = 1,2,..., t$. Count field is shown as the formula (11), for $i = 0, 1,2, ...$; M_i is the 16-byte message block.

$$A_i = Reserved \| Reserved \| 0 \| L \| Nonce\ N \| Counter\ i \tag{11}$$

Encryption block *S0*: $= E\ (Key, A_0)$.

Encryption Authentication flag *U*: $= T \oplus left\ (1, M, S_0)$.

Ciphertext *C:=left (1,l(m), C1 || C2 || ...|| Ct) || U*.

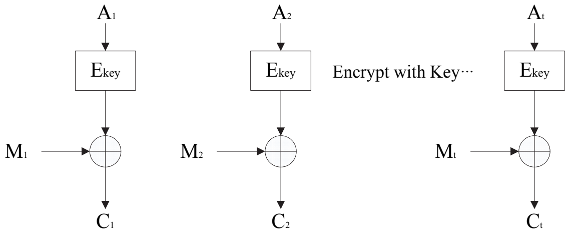

Fig. 6. CTR mode of operation.

4. Performance Evaluation

Considering the objective conditions of gas stations and practical demands, let's analyze the performance of this POS system.

4.1. Convenience Analysis

In the past, customers should get off to charge windows for paying. It is not convenient to customers. Considering the customer's property safety, personal habits and convenience, we can use this ZigBee-based POS to complete payments in the car. What's more, the POS terminal can be accepted by a variety of cards, including debit cards, integral cards and refueling cards, in order to meet the needs of different customers.

4.2. Security Analysis

It seems to be an old conversation topic, but it is a major problem that we have to focus on it. This POS system is based on ZigBee technology so that its security relies heavily on Zigbee technology. As described in the Part 3.3, ZigBee technology enhances security of the protocol stack layers by using the AES encryption algorithm to encrypt the data. AES can be used to protect data payload and prevent the attacker impersonating legal devices, and various applications can be flexible to determine its security properties [10]. Moreover, ZigBee provides data integrity checking and authentication measures, but also establishes the Trust Center security key management mechanisms. The wireless network communication has a good safety protection mechanism with these security measures.

By analyzing the ZigBee security, we have a certain understanding to the strengths and weaknesses of ZigBee security [11], but as many applications for security requirements increase, further research is necessary to enhance security.

4.3. Reliability Analysis

Signal transmission in the wireless environment, there must be many problems, such as large scale decline, shadow fading and multi-path interference and so on. Because ZigBee, Bluetooth and WLAN (IEEE802.11) is to work on 2.4 GHI-SM spectrum, mutual interference is inevitable, thus ensuring reliability is especially important.

In terms of reliability, ZigBee has many aspects to guarantee it [12]. ZigBee uses direct sequence spread spectrum (DSSS) and frequency agility (FA) technology, to a certain extent, for interference resistance, in physical layer. It is stronger than IEEE802.11 on the ability of anti-interference and multi-path. MAC application layer can answer retransmission. In MAC layer, CSMA-CA mechanism allows nodes listen to the channel before sending in order to avoid interference. Meanwhile, when the ZigBee network is subject to some external interruption and can not work, the entire network can dynamically switch to another channel.

In the NWK layer, ZigBee mesh network and redundant routing, ensures the robustness of the network.

4.4. Energy Performance Analysis

Low power consumption is an important feature of ZigBee. In a typical ZigBee sensor network, a common alkaline battery can supply ZigBee devices work six months to two years. Usually ZigBee node is carried by relatively low data rate applications. Without communication, nodes can enter a low-power sleep state; therefore energy may be in the normal working state of the one-thousandth. As the general case, the total running time of sleep most of the time, sometimes working for less than one percent, thus achieving high energy efficiency.

5. Conclusion

This paper presents a ZigBee-based wireless POS system, which adopts ZigBee wireless ad hoc network communication technologies, and uses AES-128 CCM* mode for the encryption and decryption operations of the transmission data. Therefore it has adequate protection of the stability of the data transmission, reliability and confidentiality of the data itself. Furthermore, ZigBee network is a low-power, low-cost, low-rate wireless network, in full compliance with the electromagnetic radiation requirements of gas stations, LPG stations and other complex environment. So this POS system can not only protect the personal safety of staff and the gas station's property during the whole operation process, but also reduce the costs of laying a network of POS system. And it's easy to use and maintain the system.

Although the ZigBee-based wireless POS system has advanced and high usability, the system still has some drawbacks. Currently, the AES encryption algorithm still has certain vulnerability, vulnerable to be intruded by some attacks, so that the algorithm needs to be optimized. The future works are the optimization of AES algorithm and putting forward a hybrid algorithm based on AES, and the influence of different algorithms for the POS system power consumption and security issues.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (61272306), the Public Project of Science and Technology Plan in Zhejiang Province (2012C21001), the Public Project of Science and Technology Plan in Zhejiang Province (2013C31042), and the College Students' Science and Technology Innovation Activities Plan of Zhejiang Province (1130JQ4212058G).

References

[1]. ZigBee Specifications (ZigBee Document 053474r17), *ZigBee Alliance*, January 2008.

[2]. M. Casamirra, Safety studies of a hydrogen refuelling station: Determination of the occurrence frequency of the accidental scenarios, *International Journal of Hydrogen Energy,* Vol. 34, No. 14, July 2009, pp. 5846-5854.

[3]. IEEE Standard 802.15.4-2003, Wireless medium access control and physical layer specifications for low rate wireless personal area networks, *IEEE*, 2003.

[4]. Khusvinder Gill, Shuang-Hua Yang, A ZigBee-based home automation system, *IEEE Transactions on Consumer Electronics*, Vol. 55, Issue 2, May 2009, pp. 422-430.

[5]. Lihua Xu, Yihuai Wang, The design and realize of a ZigBee network, *Control & Automation*, Issue 32, November 2007, pp. 72-74.

[6]. Advanced Encryption Standard (AES), *FIPS PUB* 197, *NIST*, November 2001.

[7]. Xiaopei Nie, The analysis of ZigBee standard's security services architecture, *Net Security Technologies and Application*, No. 2, February 2009, pp. 43-45.

[8]. Li Chunqing, Zhang Jiancheng, Research of ZigBee's data security and protection, in *Proceedings of the International Forum on Computer Science Technology and Applications*, 2009, pp.298-302.

[9]. R. Housley, D. Whiting, N. Ferguson, Counter with CBC-MAC(CCM). (http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm.pdf), August 3, 2009.

[10]. Cristina Alcaraz, A security analysis for wireless sensor mesh networks in highly critical systems, *IEEE Transactions on Systems, Man, and Cybernetics – PART C: Applications and Reviews*, Vol. 40, Issue 4, July 2010, pp. 419-429.

[11]. Aristides Mpitziopoulos, Damianos Gavalas, A survey on jamming attacks and countermeasures in WSNs, *IEEE Communications Surveys & Tutorials*, Vol. 11, Issue 4, 2009, pp. 42-56.

[12]. Pradhumna L. Shrestha, Modeling latency and reliability of hybrid technology networking, *IEEE Sensors Journal*, Vol. 13, Issue 10, October 2013, pp. 3616-3624.