Design and Development of Network for Housing Estate Security System

Awacharin Nachin*, Somsak Mitatha*, Kobchai Dejhan*,Patchanon Kirdpipat * and Yoshikazu Miyanaga**
* Faculty of Engineering
King Mongkut's Institute of Technology Ladkrabang
Bangkok 10520, Thailand
Tel: +66 27392400, Fax: +66 27392404
E-mail: knawacha@kmitl.ac.th , kmsomsak@kmitl.ac.th ,kobchai@telecom.kmitl.ac.th and patchanon@hotmail.com
** Hokkaido University, Japan
Email: miyanaga@ice.eng.hokudai.ac.jp

Abstract: This paper presents the design and development of network for housing estate security system. The system can cover up to 961 houses which can be up to 1,200 meters long transfer rate of 9,600 bps. This system uses checking and warning the abnormal situation. More over this system has ability to control switch on/off the electrical equipment in the house via AC line control system. The system consists of 4 parts. The first part is a security system of each house using MCS-51 microcontroller as a central processing unit scan 32 sensors and control 8 appliances and send alarm. The MCS-51 microcontroller received control signal via telephone used DTMF circuit. The second part is distributed two levels master/slave network implementing after RS-485 serial communication standard. The protocol its base on the OSI (Open Systems Interconnection) 7 layers protocol model design focus on speed, reliability and security of data that is transferred. The network security using encrypt by DES algorithm, message sequence, time stamp checking and authentication system when user to access and when connect new device to this system. Flow control in system is Poll/Select and Stop-and-Wait method. The third part is central server that using microcomputer which its main function are storing event data into database and can check history event. The final part is internet system which users can access their own homes via the Internet. This web service is based on a combination of SOAP, HTTP and TCP/IP protocols. Messages are exchanged using XML format [6]. In order to save the number of IP address, the system uses 1 IP address for the whole village in which all homes and appliance in this village are addressed using internal identification numbers. This proposed system gives the data transfer accuracy over 99.8 % and maximum polling time is 1,120 ms.

Keywords: House, Security, Network, Protocol,Control, Webservice

1. Introduction

At present situation, everybody goes to work outside, nobody looks after the house. This paper proposes to use computer as security system in order to check and warning the abnormal situation. At the same time, its can be used to switch on/off the electrical equipment in the home. The proposed system can be operated via 3 networks namely, telephone network, LAN and Internet. Therefore, this proposed system can be used without the higher cost.

2. The system design

The working of the system is divided into 4 parts. First part is House Security Control, not only silent alarm. Second part is communication network in the village. Third part is security server in village control center. Fourth part is Internet system that allowed users to control via the Internet. The overview of the system is in Fig.1.

There are 961 houses at maximum. Each house is connected to telephone system. The communication network is in Master/Slave design divided to two classes, 1 Center Control and 31 node controls. The security server is micro-computer that connected to Center Control and connected to the internet.

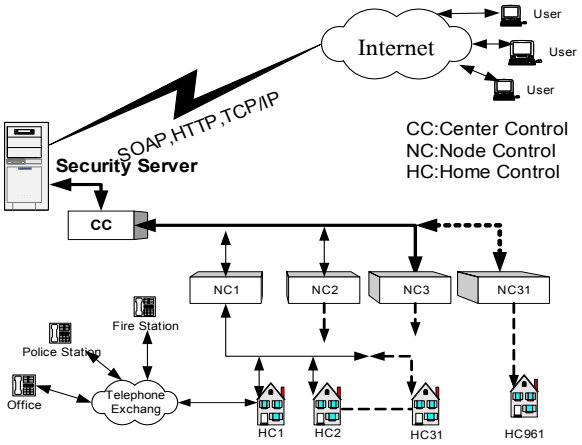

Fig.1 Integrate System

3. House Security Control

The microcontroller 89C51 is used as processing unit connects to multiplexer SN74LS42N to expand the control port and I/O port. So each house control can have up to 32 sensors and can control 8 home appliances via AC line control system.The House control consists of 4x3 keypad, LCD module with 4 rows 16 characters. It also has module to store the program and data with 32 Kbytes of memory and 72 bits for input/output. The connecting part with telephone consists of hook switch circuit which consists of

telephone-DTMF connecting circuit, DTMF decoder and sound recorder, as show in Fig.2.

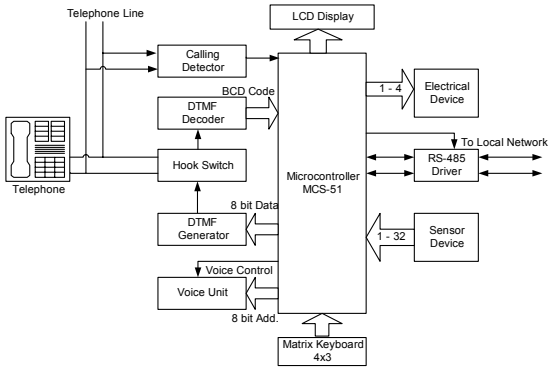

Fig. 2 Block diagram of home security System

The AC line control system uses FSK (Frequency Shift Keying) technique. The transmitter consists of Parallel to Serial Circuit, FSK Modulator and FSK Demodulator Circuit and AC Coupler. The Receiver of home appliances consists of AC Coupler Circuit ,FSK Modulator and FSK Demodulator Circuit , Microcontroller and Device Control Circuit. The solid state relay was used to control 220 V AC at 10 A maximum in Device control circuit. Block diagram of AC Line control system shown in Fig .3 and Fig.4.

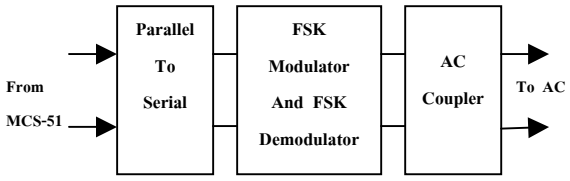

Fig 3. The Transmitter

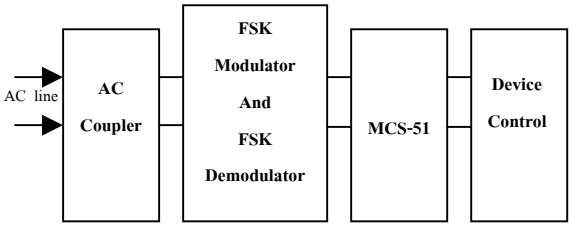

Fig 4. The Receiver

4. Network System

4.1 Protocol Layer

The protocol is base on the ISO Open Systems Interconnection (OSI) seven layers network protocol model. The Seven Layers are show in Fig.5.

The seven layers are divided into two classes, lower class and upper class. The lower class consists of OSI's layer 1-3 used in network structure, data framing, flow control and error detection. The upper class consists of OSI's layer4-7 used in data packet, data security and application.

7	Application	Sensor Checking,Divice control
6	Presentation	DES,Time Stamp,Message Sequence
5	Session	Dialog control,Synchronization
4	Transport	Connection Control,Flow control
3	Network	Logical Addres
2	Data link	Data Framing,Addressing,Checksum,Poll
1	Physical	RS-485,1,200 m.,master/slave 2 level,Half-duple

Fig.5 Protocol Layers

4.2 Physical layer.

The network system is master/slave type with RS-485 standard in order to connect with 32 points maximum. This network system is two layer types, each layer consists of 1 Master as controller which can be divide the home in each village to be 31 lines, each line has maximum 31 houses. Thus, this system can be used for 31x31=961 houses, maximum distance from Master control device is 1,200 meters and transmission rate is up to 9,600 bps in half-duplex[5]. The master device connects to microcomputer by RS-232 standard. The network system show in Fig.6.

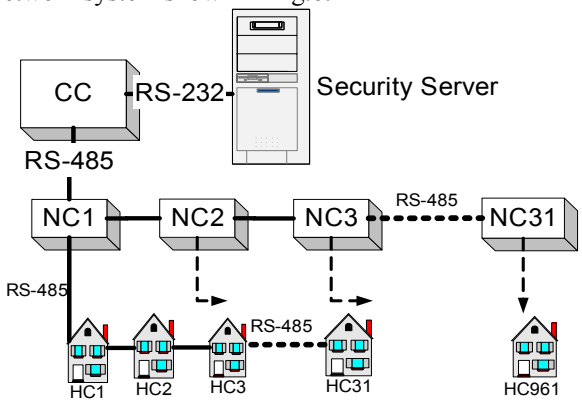

Fig.6 Network System

4.3 Data link layer

4.3.1 Data link control

Signal transmits in network uses method Poll/Select , as shown in Fig. 7.

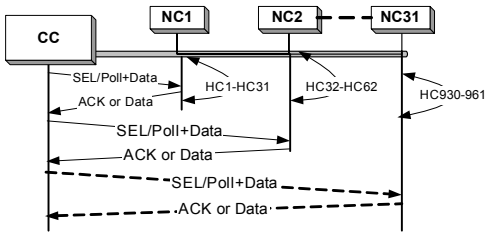

Fig.7 Poll/Select

SEL/Poll and Data signal were sent together. When the user wants to check the status of network, CC will send Poll signal to NC, then NC will return ACK and Data signal back to CC. When the user in

each house wants to send control signal to NC, HC will send SEL and Data to NC, then NC will return with ACK signal. The system was distributed into two levels, CC (Center Control) controls NC (Node Control) level, and each node of 31 NCs control HC independently, node by node. Stop-and-wait is used as flow control which has Stop-and-Wait ARQ (Automatic Repeat Request) as error control.

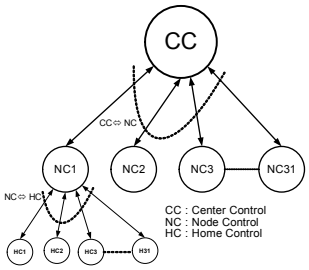

Fig.8 Signal Transmission

4.3.2 Data Framing

The data frame can be categorized to 5 categories as in Fig.9.

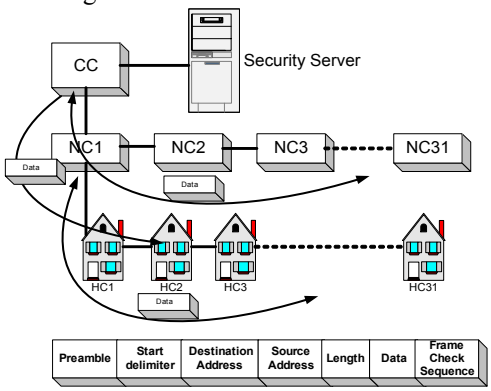

Fig.9 Data Frames

The data frame consists of Preamble, Start delimiter, Destination address, Source address, Length of frame, Data and Frame check sequence.

4.3.2.1 Data frame from HC to NC (HC->NC)

This frame is sent from HC to NC to reports the status of house and electrical home appliance. The frame structure is as below figure.

HC	CMD	DT1	DT2	STS1	STS2	FCSq

HC: house address in each node (1-31)
CMD: command, there're have 3 modes
1: check status of NC
2: check status of HC
3: control the node
4: control home appliance
DT1-DT2: status of 16 sensors divided to 2 groups
Each group consists of 8 sensors. The value of DT can be evaluated from the equation (1)

$$DT = \sum 2^{n-1} \text{ ----------(1)}$$

n : number of sensors which alerted
e.g. sensor 1,5,6 alerted.
DT1 = $2^{1-1}+2^{5-1}+2^{6-1} = 2^0+2^4+2^5 = 1+16+32 = 49$

STS1-STS2: status of 16 home appliances divided to 2 groups, each group consists of 8 devices. The value of STS can be evaluated from the equation (2)

$$STS = \sum 2^{n-1} \text{ ----------(2)}$$

n : number of working appliance
e.g. appliance 1,3,5 are working.
STS1 = $2^{1-1}+2^{3-1}+2^{5-1} = 2^0+2^2+2^4 = 1+4+16 = 21$
FCSq : for checking of frame sequence

4.3.2.2 Data frame from NC to HC (NC->HC)

This frame is sent from NC to HC to control home appliance and check the status of sensors. The frame structure is as below figure.

HC	CMD	STS1	STS2	FCSq

4.3.2.3 Data frame from NC to CC (NC->CC)

This frame is sent from NC to CC to inform the abnormal situation in network. The frame structure is as below figure.

NC	HC	CMD	DT1	DT2	STS1	STS2	FCSq

4.3.2.4 Data frame from CC to NC (CC->NC)

This frame is sent from CC to NC to control the devices in network. The frame structure is as below figure.

NC	CMD	NSTS	FCSq

NSTS: command for control the node.
0: off 1: on (operated)

4.3.2.5 Data frame from CC to HC (CC->HC)

This frame is sent from CC to HC to control home appliance and check sensors'status. The frame structure is as below figure.

NC	HC	CMD	STS1	STS2	FCSq

4.3.3 Error detection

Frame checksum is used to checking the integrity of received data. It's stored in 2'complement form of summation of entire data except the Start Byte as in Fig.10.

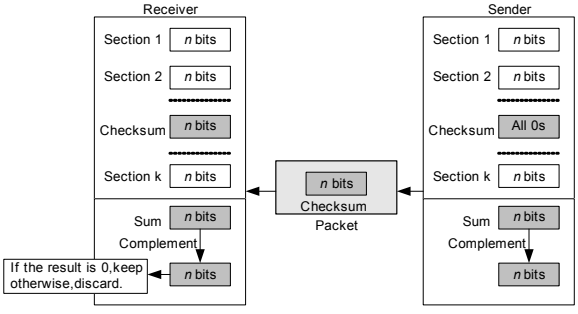

Fig.10 Checksum

4.3.4 Protocol

This system uses asynchronous protocol with Start Byte, The Byte Count of entire byte in frame except start byte and Checksum as Fig.11. The terminated checking of transmission used the Byte Count since it's faster than using Stop Byte.

Start	Byte Count	Data Frame	Checksum

Fig.11 Data frame addition for controlling

Logical address according equation

Logical address = [(NC-1)*31]+HC

When: NC: Node number 1 to 31

HC: Home number 1 to 31

Example node number is 3 home number is 20 then

Logical address = (3-1)*31+20 = 82

5. Data security

The system analyses and protect in risk and attacks.

5.1 Wiretapping

Cracker tap data from network when them understand description in data formant and flow control them can attack the system. The system protect by data encryption via DES Algorithm[3]. DES is data encryption which is not too much complex, and the key is changed in appropriate term.

5.2 Reply Attack

Cracker taps and replies data in network. Data is valid format but is invalid time. The cracker can attack system by reply data to network. It can protect by Time Stamp checking and message Sequence checking as in Fig.12.

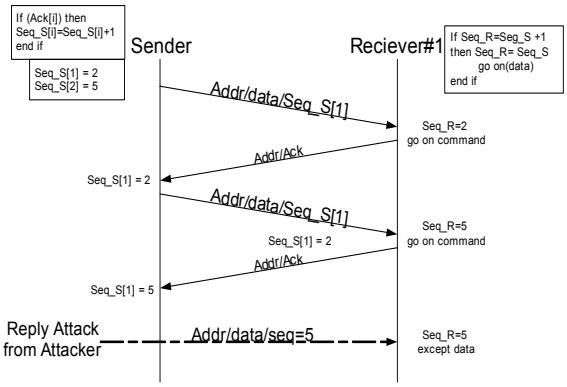

Fig.12 Add Sequence to Data Frame

5.3 Duplicate copied hardware

Cracker can duplicate HC, NC and CC and attack system by duplicate hardware .The protection by user must authentication checking all devices that connect to this system needs to be register for encryption key that being used in the network.

6. Village Security Server

The system requires microcomputer with MS-Windows2000 server to control the system. The application program that used for controlling is written in VB.NET language and store data into MS-SQL server 2000 by ADO.NET. User authentication is used for security of database. User interface is provides in GUI. Fig.13. Database store user data that consists of house plan and event log.

Fig.13 Software user interface

7. Internet System

User can access their homes via Internet work on Web Service technology. This web service is based on combination of SOAP, HTTP and TCP/IP protocols. Messages are exchanged using XML format. In order to save the number of IP address, the system uses 1 IP address for whole village in which all home and appliances in this village are addressed using internal identification numbers and it is treated as 1 service in the internet. Every system that on standard of Web Service, such as ICQ, MS-MSN, etc. ,can use this system, as show Fig.14.

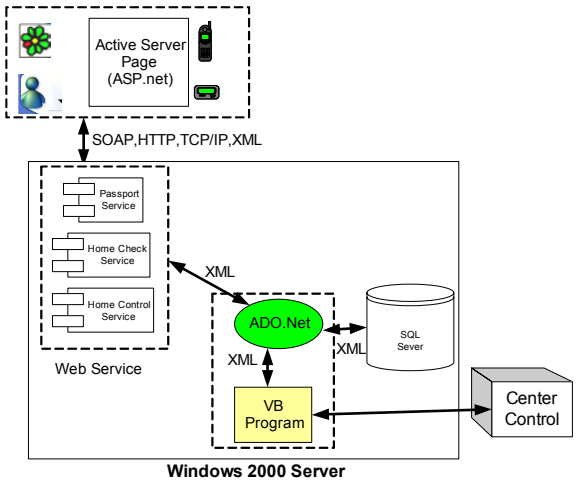

Fig.14 Internet System

The systems have 3 services.

Passport: Authentication and check permission user to access system

Home checking: Check sensor status

Home control: Control electrical device

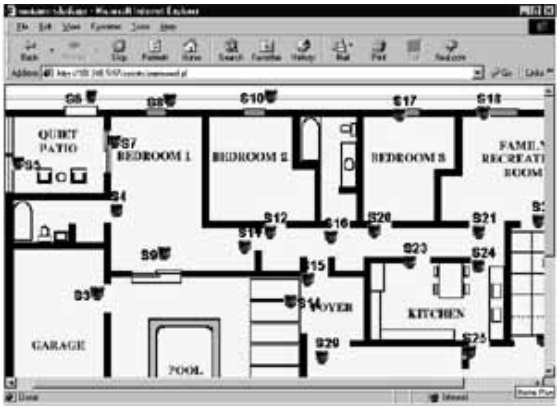

Fig.15 Web Application

8. Experiment

We test the proposed network by spreading 10,000 packets through the networks and only 1 packet is error. So the data transmission accuracy of this proposed system is 99.99%.

9. Conclusion

The Village Security system can control 961 houses with maximum distance from Center Control 1.2 kms and transmission rate up to 9,600 bps. The system is divided into 31 sub-nodes with master/slave RS-485 standard. The transmission ensured by Acknowledge frame and Response time. DES encryption algorithm, Time stamp checking, Message sequence are used to provide data security. The user can access the system via internet by standard of web service which treats each device in house as 1 service. Every system that base on web service standard can use this system. The system is large network system with high security in data communication. And also can be expanded and worked with the other network in the future. It doesn't depend on device or application program. In addition , it is not too expensive.

Fig.16 Testing System

10. Reference

[1] Sin-Min Tsai, Shyi-Shiou Wu, Shya-Siow Sunand Po-Ching Yang, "Integrated Home Service Network On Intelligent Intranet" , IEEE Transactions on Consumer Electronics, Vol. 46 No. 3, August 2000, pp 499-504

[2] Awacharin Nachin and Somsak Mitatha, "Housing Estate Security System via Computer Network," Asia-Pacific Symposium on Broadcasting and Communication; Bangkok, Thailand, December 2000 , pp 389 - 392

[3] William Stallings, "Network Security Essentials Application and Standards", Prentice Hall, 2000

[4] Behrouz A. Forouzan, "Data Communication and Networking, Second Edition", McGraw-Hill, 2000

[5] Jan Axelson, "Networks for Monitroing and Control Using an RS-485 interface", MICROCOMUTER JOURAL, July/August, page 36, 1995

[6] Thuan Thai, "Hoang Q. Lam NET Framework Essentials", O'Reilly, First Edition, 2001