

Implementation of ZigBee in Network Devices

Sameer Ahmad Bhat
IT Skills Dept. KSU
Riyadh Saudi Arabia,

Majid Ramzan
IT Skills Dept. KSU
Riyadh Saudi Arabia,

Tahir Rashid Hakeem
IT Skills Dept. KSU
Riyadh Saudi Arabia,

ABSTRACT

Today, computer networks are the backbone for all types of data communications. These computer networks rely on devices that connect different nodes in a network to each other by means of communication links. The devices that connect nodes in a network typically are active most of the times. Sometimes there arise situations when network devices stop responding due to overload or device malfunctioning. Because of that network administrator is unable to access or troubleshoot the devices. Therefore it becomes necessary to visit the actual device site location and manually reset the device configurations to its original factory settings. In order to restore, the devices usually provide a web based interface or hardware reset button usually on the device itself. Because the web interface is lost due to device freezing or overload, there needs to be an alternate access for the devices. This paper identifies the freezing problem in networking devices and values the potential of ZigBee for addressing these problems through the design and implementation of flexible automation architecture using a PIC microcontroller with a reset circuit. The proposed system provides an alternate to web interface for network devices and ensures a proper authentication for the system.

General Terms

Computer Networks, Zigbee, protocols, ZigBee.

Keywords

Zigbee, device freezing, microcontroller PIC16FXX.

1. INTRODUCTION

In computer network systems, equipment issues frequently occur because of the devices not having the ability to correspond well with an alternate. Now and then it gets important to reset the system settings to restore them to their original manufacturer settings. Thus, practically all network devices provide the restore facility for this purpose. The devices provide an electronic interface or support some provision system to restore original manufacturer settings. A hard reset, otherwise called a factory reset or master reset, restores a device to the state it was in when manufactured. This hard reset deletes all settings, applications, and user information from a device.

A Network troubleshooter may reset the system unit for a few reasons. Most regularly discovered reasons are

- The administrator cannot remember password.
- Compromised Wireless security key.
- Internet connectivity issues due to malfunctioning of the network device.

Restore function starts from a web interface or by an application program or directly by holding the provided restore button typically located on the device itself. A few

occasions give us an understanding where a network device freezes and it gets difficult to impart by means of the web interface. Thus, control over the network device is lost. Resetting and reconfiguration of the network device then turns into a monotonous task and is just possible through a Hardware reset. This reset operation for a network device raises some essential issues like –

- Initially, it needs an individual to visit the device site, with the goal that the individual physically resets the unit by pushing a reset button found typically on the device.
- Second, there is no authentication system, as the device is once in a while receptive to unknowns who without breaking the security make inconvenience in a dynamic system by resetting the device. (Authentication is just available in web/software interface for the devices).
- Third, it clears the memory and reboots the machine persuasively. This reasons information defilement and in some cases completely damages the devices.

This paper gives an ideal answer for the manual reset issue of network devices by including a hardware embedded inside the device itself. The system provided –

- Initially, validates an individual before a hardware restore.
- Second, it permits an individual to restore the system unit remotely without approaching to the actual location of the device.

The fundamental parts of the system are PIC16F84 microcontroller, XBee and Reset circuit. GUI based interface is developed for the system which enables a client to perform device restore after authentication.

2. SYSTEM DESCRIPTION

The designed system gives an alternate approach to restore the network devices by an application program. The system components include - Zigbee communication system, a microcontroller for authentication process, and a reset circuit.

The system consists of following components –

2.1.1 Hardware platform

- ZigBee wireless communications technology
- Micro-controller PIC16F84
- Reset Circuit

2.1.2 Software platform

- An application program

ZigBee is a new low power consumption and low transmission rate wireless communication technology within

short distance and simple structure [1]. Its transmission distance is about tens of meters and uses 2.4 GHz and 900 MHz frequency bands. Ranging the transmission rate from 20 Kb/s to 250 Kb/s average, ZigBee can achieve duplex communication. Its network architecture embeds Master / Slave attributes. Compared with Wi-Fi, WiMax, GPS, Zigbee is more suitable for localization in complexity indoor environment by virtue of the mentioned features. Zigbee technology meets people's information requirements on the indoor localization such as an airport, warehouse, mine and so on. [2]

ZigBee can be configured in following three modes -

- Network (ZigBee) Coordinator
- Full Function Device (FFD),
- Reduced Function Device (RFD).

In the *Network coordinator mode*, the Zigbee stores information of the overall network. This storage of information relating to the network needs much more memory and the processing, computing power. For this type of configuration, there can be only one coordinator node for the network. This node is responsible for initializing the network, selecting the appropriate channel, and permitting other devices to connect to its network. It can be even responsible for routing traffic in a ZigBee network.

In the *Full Function Device (FFD)* mode, the nodes support the protocols of the wireless standard defined for WSN. The nodes can take the responsibility of a Network Coordinator. Using the extra memory and the computing power they may also serve as the network routers and can be used at the edge of the network to works like a network edger devices [3]. This mode enables them to collect the information from the real world e.g. from different sensors. A router is able to pass on messages in a network, and is also able to have child nodes connect to it, whether it be another router, or an end device. Router functions are only used in a tree or mesh topology, because in a star topology, all traffic is routed through the center node, which is the coordinator. Routers can take place of end devices where in such cases the routing functions of the devices become useless. If the network supports beaconing, then a router can sleep when inactive, periodically waking up to notify the network of its presence.

In the *Reduced Function Device (RFD)* mode, the node provides the function as per its name. This mode offers the limited functionality and is generally used for the Network Edge Devices with very low power consumption. The power saving features of a ZigBee network can be mainly credited to the end devices [3]. These nodes are not used for routing traffic. They sleep for the majority of the time, expanding battery life of such devices. These nodes carry just enough function to talk to parent nodes, which can be either a router or a coordinator. An end device does not have the ability to have other nodes connect to its network through the end device, as it must be connected to the network through either a router, or directly to the coordinator. [4]

PIC16F84 belongs to the mid-range family of the PIC® microcontroller devices [5]. Fig 2 shows the internal architecture of PIC16F84 microcontroller.

The program memory contains 1K words, which translates to 1024 instructions, since each 14-bit program memory word is the same width as each device instruction. The data memory (RAM) contains 68 bytes. Data EEPROM is 64 bytes.

There are also 13 I/O pins that are user-configured on a pin-to-pin basis. Some pins are multiplexed with other device functions. These functions include:

- External interrupt
- Change on PORTB interrupt
- Timer0 clock input

Data Memory Organization

The data memory is partitioned into two areas. The first is the Special Function Registers (SFR) area, while the second is the General Purpose Registers (GPR) area. The SFRs control the operation of the device. Portions of data memory are banked. This is for both the SFR area and the GPR area. The GPR area is banked to allow greater than 116 bytes of general purpose RAM. The banked areas of the SFR are for the registers that control the peripheral functions. Banking requires the use of control bits for bank selection. These control bits are located in the STATUS Register. [5]

The PIC16F84 is programed to receive data via serial data. The pic receives instruction from the application provided to the user and controls the hardware reset circuit for restoring. The flowchart for the PIC program is shown in fig 3.

The **Reset Circuit** as shown in Fig 1, consists of PIC16F84 microcontroller, a transistor and an Opto-coupler. The microcontroller is programed with one of its pins configured in output mode. The configured pin drives a transistor, which further activates the opto-coupler. The Opto-coupler isolates the voltage levels of reset circuit and the device circuit. The pins of Opto-coupler are connected in parallel with the reset switch, to perform switching. The transistor drives the Opto-coupler the 5v supply same supply, used for the microcontroller.

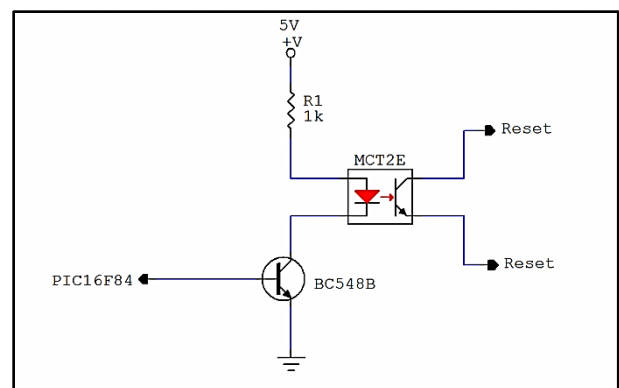


Fig 1: Reset Circuit diagram

3. IMPLEMENTATION

The system uses the GUI application program designed for users, to communicate with the PIC16F84 via ZigBee wireless communication interface. After running the application, the system first authenticates a user.

The user first runs the application. This application communicates with the PIC controller via the Zig-Bee wireless interface. Here in our system the ZigBee is configured as Reduced Function Device, in order to demonstrate the system. The application after receiving the password from the user, communicates with the PIC controller to validate the user. A default password is stored initially in the EEPROM memory in the PIC controller. This password can be later changed via the application program.

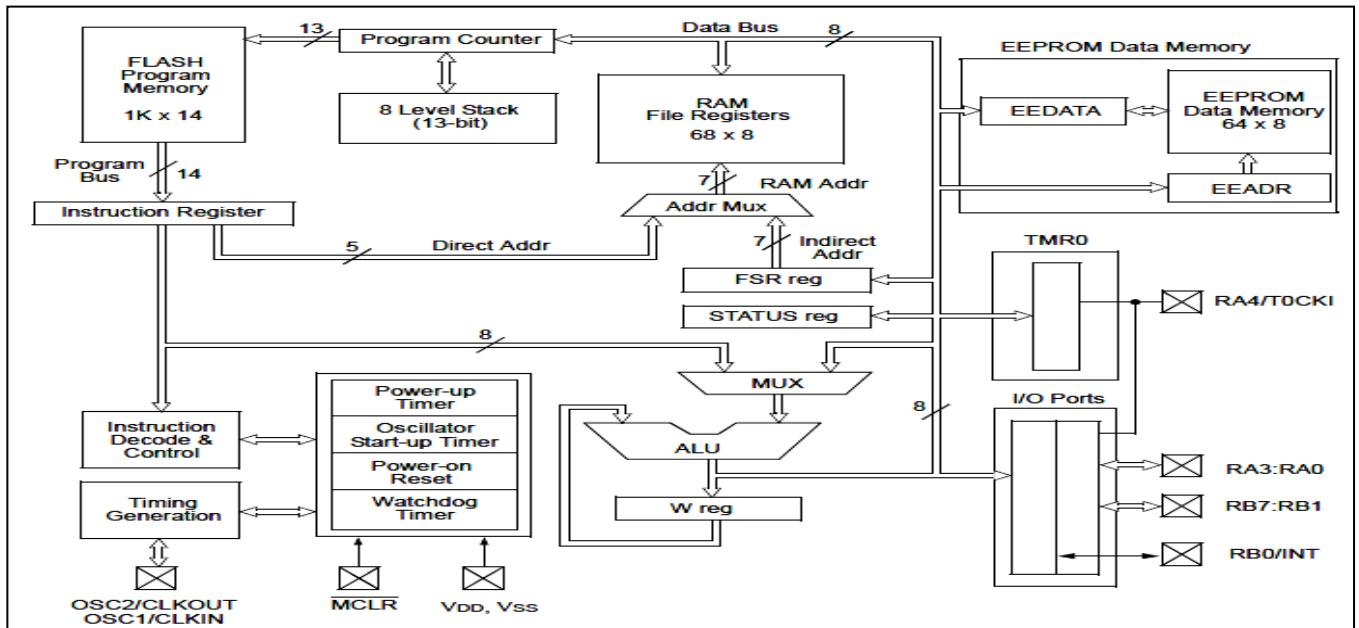


Fig 2: Architecture of PIC16F84

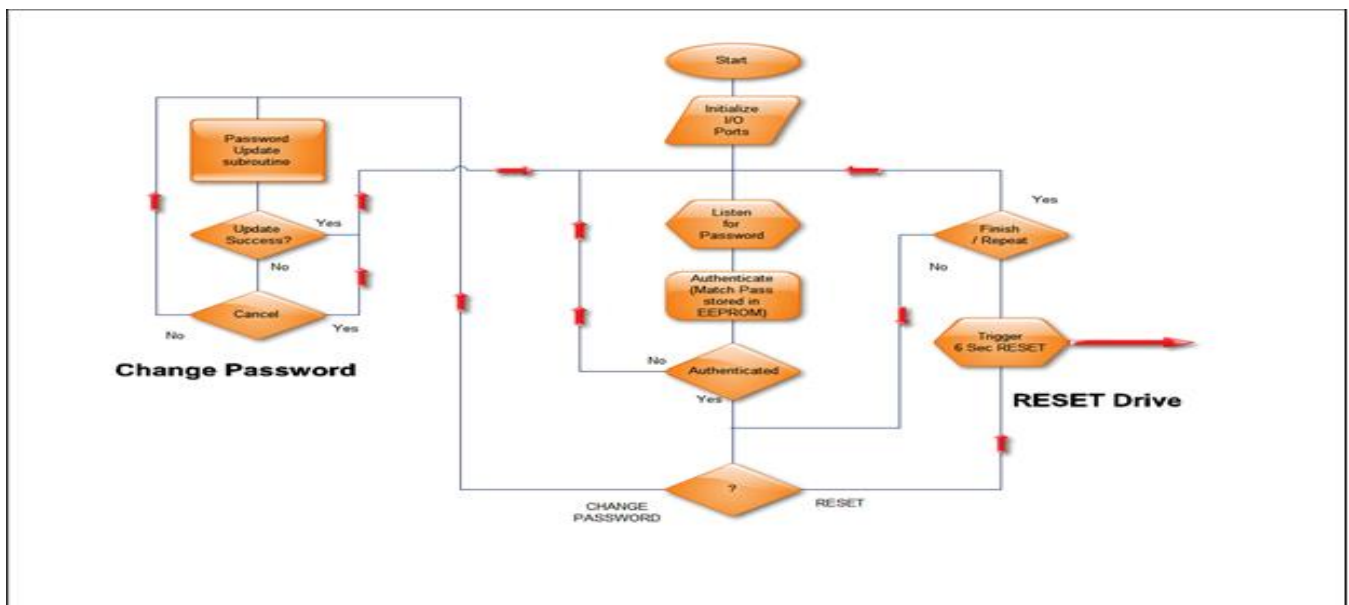


Fig 3: Flowchart for PIC16F84 program

Once the PIC controller authenticates a user, it provides two choices to the user. The first choice allows a user to change the authentication password. The second choice is to reset the network device. The Change Password option is typically the same, as it asks for an old password and the new one. When a user selects the second choice, the program in the PIC16F84 generates a 6-Second trigger pulse. This pulls one of the pins configured for triggering to High state, which further drives a transistor configured as switch. The transistor conducts due to trigger supplied by the PIC controller, shorts the reset switch for 6-sec duration via the Opto-coupler MC2TE. This resets the network device to original factory settings- erasing all settings, applications, and user data from it. Fig 4 shows the block diagram of the complete system.

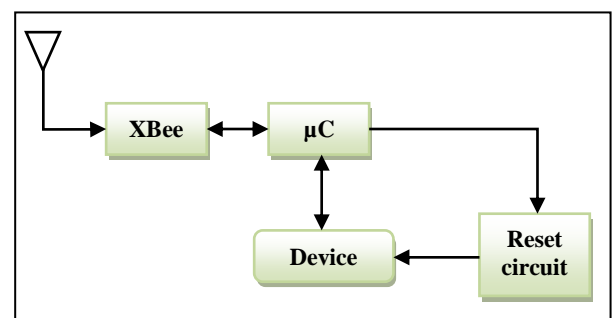


Fig 4: Block diagram

Thus, the proposed system ensures the device reset and furthers the web interface then allows the access to the network device. The user can now apply all the desired settings for the device and can set a new username and password in the device internal configuration. The proposed system avoids the manual resetting of network devices and protects them from unauthorized access, ensuring a better and reliable communication in the networks. device. The user can now apply all the desired settings for the network device and can set a new username and password in the router internal configuration. Hence, the proposed system avoids the manual resetting of network devices and protects them from unauthorized access, ensuring a better and reliable communication in the networks.

4. CONCLUSION

In this paper, a reset control system for resetting network devices to their original settings through a ZigBee interface is proposed. ZigBee as a new attractive wireless technology can be used in several applications such as sensor interconnecting, monitoring, and automating different systems in home, hospitals, manufactories, and agriculture. This paper implements the control architecture for ZigBee and PIC16FXX microcontroller, functions, and protocol.

The paper provides a simple and efficient solution to the manual reset problem in the networking devices. It focuses on the freezing problem of network devices and provides a soft solution with a little cost. The designed hardware circuitry can be embedded within the network device. This will enable a user to have control of a network device via ZigBee interface if the Web interface fails to respond. Later the system can be modified to include a more complex authentication system and extend the range of device control system by implementing the ZigBee as Full Function Device (FFD) or as Reduced Function Device (RFD). This will enable a network administrator to control all the devices from one location, as all the nodes in a network are usually connected to each other by means of communication links

5. REFERENCES

- [1] Zigbee Alliance. (2006, Dec) Zigbee specification: Zigbee document 053474r13. [Online]. www.zigbee.org
- [2] Mian Chen Xinran Li, "Research of the Wireless Localization Technology Based on ZigBee," *Conference Publishing Services*, p. 3, 2012.
- [3] Shahin Farahani, "ZigBee Wireless Networks and Transceivers," *Elsevier*, p. 360, September 2008.
- [4] Ms.Dharmistha D. Vishwakarma, "IEEE 802.15.4 and ZigBee: A Conceptual Study," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 1, no. 7, p. 4, September 2012.
- [5] Microchip Technology Inc. (1998, January) PIC16F8X-18-pin Flash/EEPROM 8-Bit Microcontrollers. English.
- [6] B. Yuksekkaya, "A GSM, Internet and Speech Controlled Wireless Interactive Home," *IEEE*, p. 7, 2006.
- [7] Website, <http://www.zipsms.com/schoolSMS.aspx>.
- [8] Intark Han, Kwang-Roh Park, Wan-Ki kPark, "ZigBee based Dynamic Control Scheme for Multiple Legacy IR Controllable Digital Consumer Devices," *IEEE Transactions on Consumer Electronics*, vol. 53, no. 1, FEBRUARY 2007.
- [9] Anna Trifonova, "MOBILE LEARNING - REVIEW OF THE LITERATURE," p. 9, March 2003.
- [10] Lamboder Jena, Aarti Pradhan Sushruta Mishra, "Networking Devices and Topologies: A Succinct Study," vol. 2, no. 11, p. 11, November 2012.
- [11] Juing-Huei Su, "The Design and Implementation of a Low-cost and Programmable," *IEEE*, p. 6, 2006.
- [12] Rajkalpesh R.Jaiswal and Sunil R.Sansare Shreyas M.Patankar, "Information retrieval system using SMS," *Emerging Trends in Computer Science and Information Technology -2012(ETCSIT2012)*, p. 4, 2012.
- [13] Dr.A.K.Jain Raj Kumar Singh, "Research Issues in Wireless Networks," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 4, p. 5, April 2012.
- [14] Carelin Felix and I. Jacob Raglend, "Home Automation Using GSM," *International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011)*, p. 5, 2011.
- [15] E. Ferro and F. Potorti, "Bluetooth and Wi-Fi wireless protocols: A," *IEEE Wireless Commun*, vol. 12, no. 1, p. 16, Feb 2005.
- [16] B.P. and E.B. Swanson Lientz, "Software Maintenance Management," *Addison-Wesley Longman*, 1980.
- [17] Li Yan, Lu Hu Ji Zhengzhou, "The Implementation of Wireless Sensor Network node Based on ZigBee," , 2008, p. 4.
- [18] Texas Instruments Incorporated, "MCT2, MCT2E," 1995.
- [19] BelBel, "SMS advantages and disadvantages," <http://www.studymode.com/essays/Sms-Short-Messaging-Service-Advantages-450483.html>, 2010.
- [20] Muhammad Asif, "Mobile student information," *Emerald*, p. 11, 2010.
- [21] Dr.S.S.Riaz Ahamed., "THE ROLE OF ZIGBEE TECHNOLOGY IN FUTURE DATA," *Journal of Theoretical and Applied Information Technology*, p. 7, 2005 - 2009.
- [22] "Computer Network Routing with a Fuzzy Neural Network," *Behzad Mahjour Shafiei, Mohammad Amin Saeed, Farshid Iranmanesh, Fariborz Iranmanesh*, no. ISSN 1995-0756, p. 5, 2012.