Advanced Engineering Forum
ISSN: 2234-991X, Vols. 6-7, pp 1129-1134
doi:10.4028/www.scientific.net/AEF.6-7.1129
© 2012 Trans Tech Publications Ltd, Switzerland

Online: 2012-09-26

A Prototype of Fingerprint and ZigBee Based Train Ignition System

P.J.Bharani[a], B.Gopinath [b], R.Goutham [c]

R.M.D Engineering College, R.S.M Nagar, Kavaraipettai - 601206, India

[a] bharanijss@gmail.com, [b] gopee1329@gmail.com, [c] gouthamr5@yahoo.in

Keywords: Fingerprint, ZigBee, Pulse Sensor, ARM Processor, Authentication, Ignition, Train

Abstract. At present, number of vehicles is successfully implementing fingerprint system for authentic ignition. By this system unauthorized accessing of the train or mishandlings can be avoided. The Fingerprint and ZigBee based Train Ignition system can serve as a robust security mechanism and can avoid trains being driven by unauthorized person at any circumstances. Fingerprints are the most widely used form of biometric identification overtime and the critical step in exploring its advantages is to adopt it for use as a form of security in already existing systems, such as trains.

This paper work focuses on the use of fingerprints for train ignition along with the conventional method of using keys. The fingerprint recognition software enables fingerprints of valid users of the train to be enrolled in a database. The developed prototype serves as an impetus to drive future research, geared towards developing a more robust and embedded real-time fingerprint based ignition systems in trains along with ZigBee communication.

Introduction

The authentication presented in this paper consists of two stages. In the first stage, the duty is assigned for the user in the database station and the fingerprint information is transmitted to the train using ZigBee transmitter. In the second stage, the information is received by the ZigBee receiver and is matched with the user. For further security purpose, the receiver retains the information for a certain time after which it gets erased. The ARM processor acts as a control unit for the ZigBee receiver and fingerprint units in the train.

Before any user can ignite the train, his/her fingerprint information is sent from the database station using ZigBee transmitter and is received by the ZigBee receiver in the train. Then the fingerprint is matched against the images in the database while users with no match in the database are prevented from igniting the train.

ZigBee

ZigBee standard is developed by ZigBee Alliance, which has hundreds of member companies, from the semi-conductor industry and software developers to original equipment manufacturers and installers. The ZigBee alliance was formed in 2002 as a nonprofit organization open to everyone who wanted to join.

[1] ZigBee is a low-cost, low-power, wireless mesh networking standard. First, the low cost allows the technology to be widely deployed in wireless control and monitoring applications. Second, the low power-usage allows longer life with smaller batteries. Third, the mesh networking provides high reliability and more extensive range. ZigBee is a standard that defines a set of communication protocols for low data rate short range wireless networking. ZigBee based wireless devices operate in 868MHz, 915MHz and 2.4GHz frequency bands. ZigBee is targeted mainly for battery power applications where low data rate, low cost and long battery life are main requirements.

ZigBee and IEEE 802.15.4: ZigBee wireless networking protocols shown in Figure 1. ZigBee protocol layers are based on the Open System Interconnect (OSI) basic reference model. The bottom two networking layers are defined by IEEE 802.15.4 standard. [2] This standard is developed by IEEE 802 standards committee and was initially released in 2003. IEEE 802.15.4

defines the specifications for PHY and MAC layers of wireless networking, but it does not specify any requirements for higher networking layers. The ZigBee standard defines only the networking, applications and security layers of the protocol and adopts IEEE 802.15.4 PHY and MAC layers as a part of the ZigBee networking protocol. Therefore, ZigBee-compliant device conforms to IEEE 802.15.4 as well.

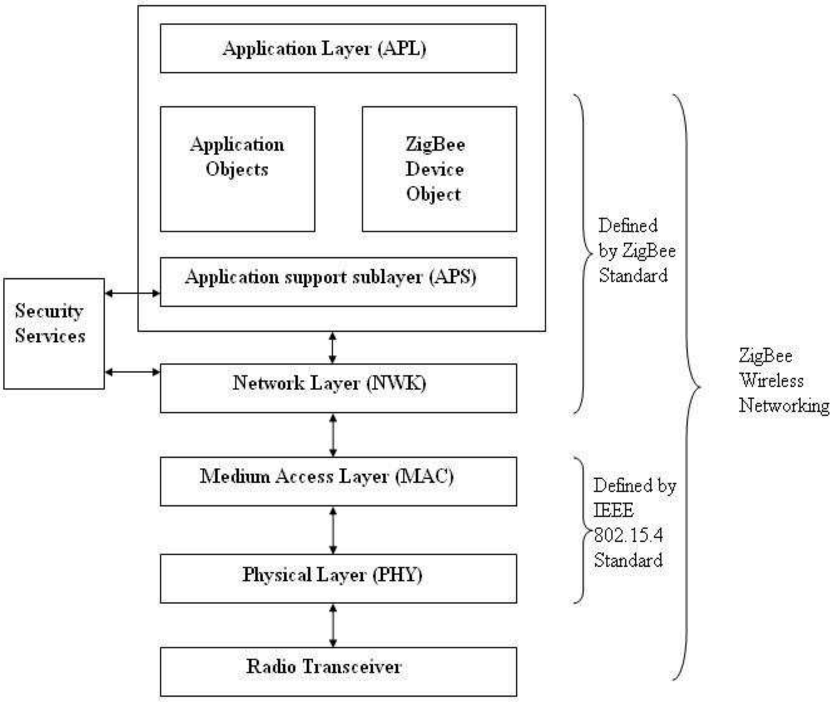
Application Layer (APL)
Application Objects
ZigBee Device Object
Application support sublayer (APS)
Security Services
Network Layer (NWK)
Medium Access Layer (MAC)
Physical Layer (PHY)
Radio Transceiver
Defined by ZigBee Standard
Defined by IEEE 802.15.4 Standard
ZigBee Wireless Networking

Figure 1 ZigBee wireless networking protocol Layers

Interoperability: ZigBee has a wide range of applications; therefore, several manufacturers provide ZigBee -enabled solutions. It is important for these ZigBee based devices to be able to interact with each other regardless of the manufacturing origin. In other words, the devices should be interoperable, which is one of the key advantages of the ZigBee protocol stack. ZigBee-based devices are interoperable even when the messages are encrypted for security reasons.

ZigBee Transmitter: The ZigBee transmitter does major functions like, bit to symbol mapping, symbol to chip mapping, serial to parallel conversion, performing half sine pulse shaping and performing modulation. The receiver performs RF to baseband conversion, sampling and thresholding, parallel to serial conversion and dispreading.

ZigBee Receiver: In the receiver configuration of ZigBee, we are using a MSK demodulator and a multiplier for despreading. This multiplier output contains the baseband data and higher frequency harmonics. The multiplied signal is passed through a low pass filter for avoiding harmonics. This sampled data is passed through a decision device. Decision device is a simple comparator which contains a threshold value for making a decision. If the input to the comparator is greater than the threshold value, it decodes the bit as “1” otherwise it decodes as “0”. Actually 2Mbps data coming from parallel to serial converter contains a small amount of offset delay. We must introduce this offset delay in the PN sequence data while multiplying with 2Mbps data, So that we will get original bit stream without any errors.

The following Figure 2 and Figure 3 show the block diagram for ZigBee transmitter and receiver.

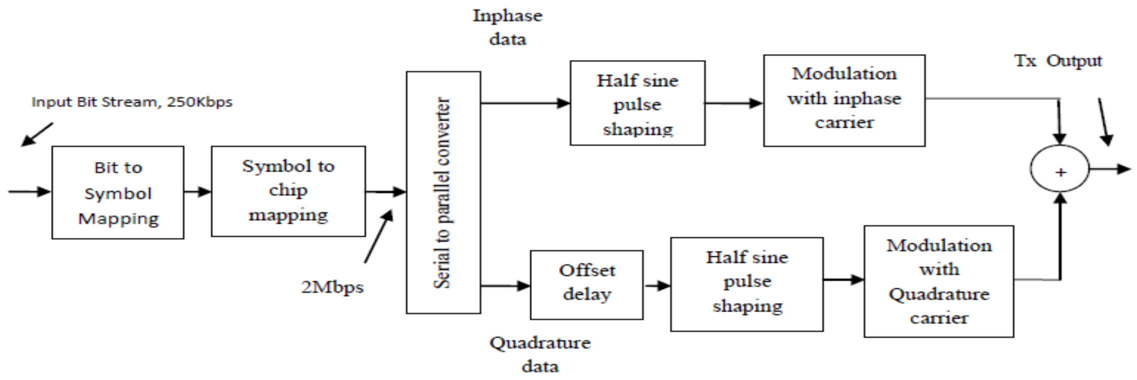

Figure 2 Block Diagram of ZigBee Transmitter

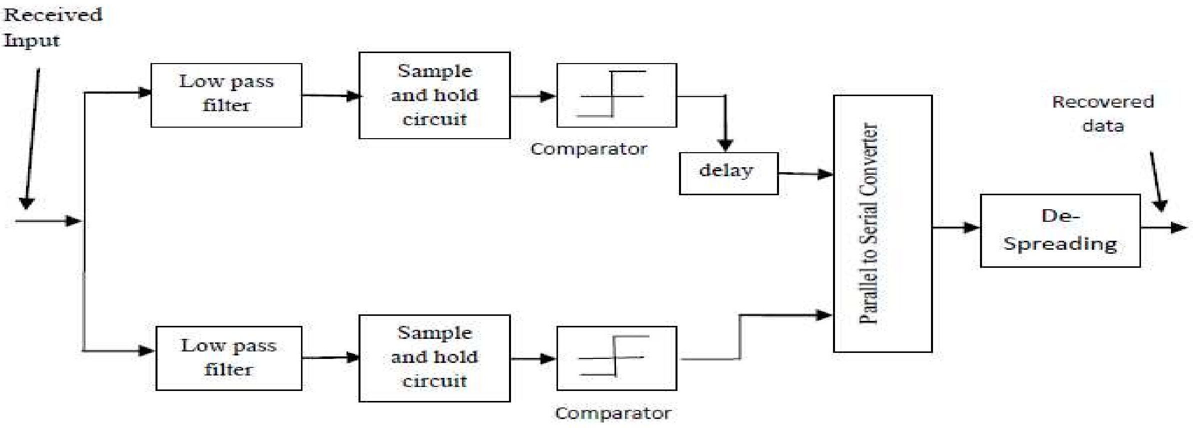

Figure 3 Block Diagram of ZigBee Receiver

Biometric Identification

Fingerprint Reader: In traditional fingerprint access systems, an individual attempting to access a protected resource places their finger on a fingerprint sensor/reader at an access point such as a door or computer. The sensor reads the fingerprint and transmits the image, typically to a server, where it is compared against a database of stored fingerprints. [3] If the live print matches a stored print, the individual is permitted access. Biometrics represents significant security advancements over proximity cards or passwords because they physically prove each user's identity.

Accuracy and Reliability: With biometric finger scanning, misplacing key or not remembering a password doesn't matter. [4] Since the technology uses your fingerprint to either allow or deny access, the only way to lose your key would be to lose your finger, which likely won't happen.

[5] By choosing good model biometric equipment, we can have a security for as long as you need one. It is very secure and reliable since the fingerprints are unique and immutable.

Pulse Sensor: The Pulse Sensor measures subtle changes in light from expansion of the capillary blood vessels to sense your heartbeat. Gently place the sensor on any area of skin (such as a finger or earlobe) and it will transmit pulse data for processing.

Fingerprint reader with pulse sensor: Here a pulse sensor is embedded with the fingerprint reader circuit. This is mainly used for security purpose. If somebody did gain access to an authorized user's prints then the person could trick the scanner. In a worst-case scenario, a criminal could even cut off somebody's finger to get past a scanner security system. So the scanner is made with an additional feature of Pulse sensor to verify that the finger is alive, rather than a mold or dismembered digit.

[5] The Fingerprint reader with pulse sensor is schematically illustrated in Figure 4. The finger is placed in the reader first. The pulse sensor senses for the pulse. If pulse exists, then the finger pattern is captured and compared with the existing database and the result is produced.

Most of fingerprint systems utilize optical or capacitive sensors for capturing fingerprints. These sensors detect difference between ridges and valleys of fingerprints. Optical sensors detect difference in reflection. Capacitive sensors, by contrast, detect difference in capacitance. Some systems utilize other types of sensors, such as thermal sensors, ultrasound sensors. In this paper we examine fingerprint systems which utilize optical or capacitive sensors.

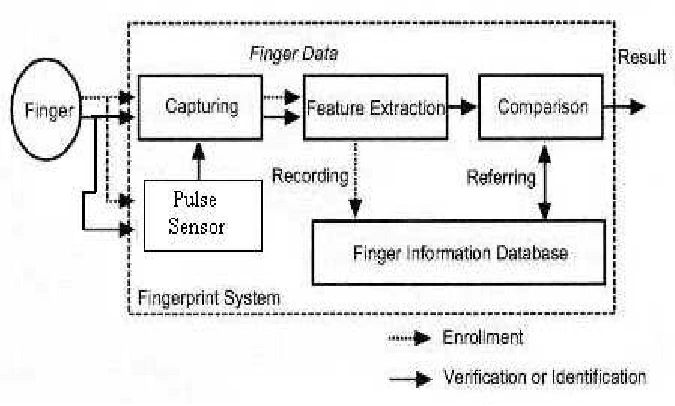

Figure 4 Fingerprint Reader with Pulse Sensor

In the registration process, the system captures finger data from an user with sensing devices, extracts features from the finger data, and then record them as template with a personal information, e.g. a personal identification number (PIN), of the enrollee into a database. We are using the word "finger data" to mean not only features of the fingerprint but also other features of the finger, such as "live and well" features. In an identification or verification process, the system captures finger data from a finger with sensing devices, extracts features, identifies the features by comparing with templates in the database, and then outputs a result as "Acceptance" only when the features correspond to one of the templates.

Fingerprint and ZigBee based Ignition System Design

The prototype comprises of both software and hardware units which are the driving units of the Fingerprint and ZigBee based Ignition System Design which gives secured authentication and ignition mechanism.

Software: The program codes driving the fingerprint recognition software for ignition system control was written in visual basic and ran on a PC. It uses a set of fingerprint images stored in an image folder in its directory. The test images can be enrolled into its database after it has gone through the stages of image enhancement, minutiae extraction and image post-processing (eliminates false minutiae).

Hardware: Figure 5 shows the Fingerprint and Zigbee based Ignition system design. The database information is transmitter using the ZigBee transmitter which is connected with the PC. The information is received by the ZigBee receiver and the image is compared with the image which is captured by the Fingerprint reader where both reader and receiver are controlled by the ARM processor since it has two serial ports for controlling two units. The received data is stored in the memory unit only for a certain time and then it gets erased automatically to provide additional security. [6] The timer and the memory units are programmed in the ARM processor. The ARM processors provide better reliability compared to normal microcontrollers since the memory and peripheral interface features are better in it.

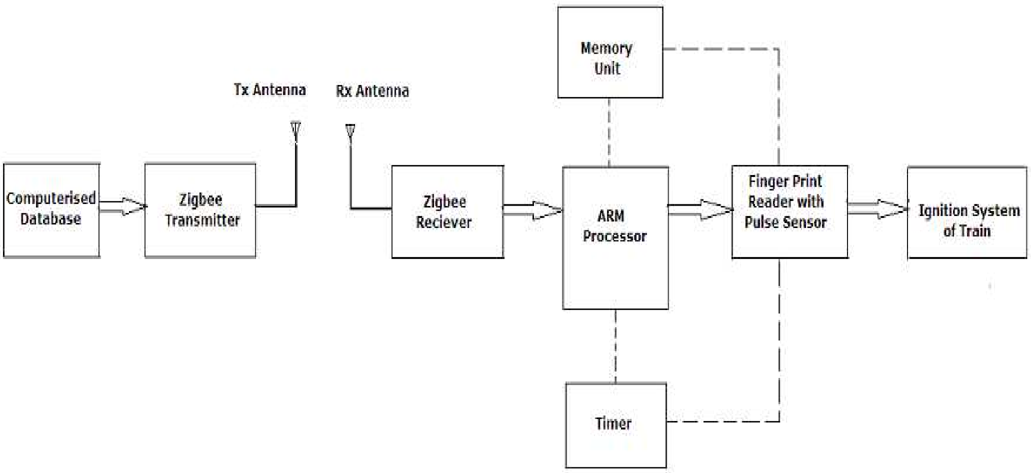

Figure 5 Fingerprint and ZigBee based Ignition System Design

Authentication Procedure

The authentication consists of different stages in which first the users are registered in the database and their details and Fingerprint images are stored. Secondly, when the duty is assigned to the user, his/her information is transmitted to the train by means of ZigBee. The data at the receiver is stored only for a specific time after which it gets erased so that the user can ignite the train only when the duty is assigned and mishandling can be avoided. During train ignition, the user has to provide his/her fingerprint in the fingerprint reader installed in the train. The fingerprint reader with pulse sensor makes sure that pulse is present and only if it is present then the image is captured and sent for comparison with the database. So that any other form of fingerprints like plastic mould, transparent sheets can be avoided. If the image received and the captured images matches, then the train can be ignited using the physical key else the train cannot be ignited.

The Relay transmitter is an amplifier which can be used for restoring the strength of a transmitted signal. If the distance covered by the ZigBee is not enough, then the relay transmitters can be employed for extending the coverage distance of the ZigBee. The databases are available in the main stations alone and if needed it can be installed in all the stations. The database management and duty assignment are done by the authorized person in the station alone. The data when transmitted is secure since we use ZigBee. In future, Encryption methods can be used during transmission so that the data is secure in the air.

Conclusion

The prototype of a fingerprint and ZigBee based train ignition system developed has a specific sequence that must be followed before it can be used to ignite a train. By this sequence the unauthorized users can be restricted form accessing the train. Major accidents due to mishandling by unauthorized users can be avoided by adapting this system and human lives can be saved.

In the results, it can be deduced that the use of biometric security systems offers a much better and foolproof means of restricting the ignition of trains by unauthorized users. Furthermore, it can be logically derived from the findings of this research work that fingerprint images can be used for train ignition system control.

References

[1] ZigBee wireless networks and transceivers by Shahin Farahani.

[2] ZigBee wireless networking by Drew Gislason.

[3] Biometrics by John D. Woodward (Jr.), Nicholas M. Orlans, Peter T. Higgins.

[4] Guide to biometrics by Ruud Bolle.

[5] Encyclopedia of Biometrics by Stan Z. Li, Anil K. Jain.

[6] The defensive guide to the ARM cortex-M0 by Joseph Yiu.