Zigbee Wireless Vehicular Identification and Authentication System

S. D. Dissanayake, P. P. C. R. Karunasekara, D. D. Lakmanaarachchi,
A. J. D. Rathnayaka, and A. T. L. K. Samarasinghe
Department of Electronic and Telecommunication Engineering
University of Moratuwa, Moratuwa, Sri Lanka 10400
Email:{sds03, ppcrk03, ddl03, ajdr03,}kithsiri@ent.mrt.ac.lk

Abstract— **We propose a Zigbee technology based wireless vehicle identification and driver authentication system consisting of a central database of authorized vehicles, Zigbee RF Vehicle tags, RF tag Reader and RF tag Writer. Zigbee is based on IEEE 802.15.4 standard for Wireless Personal Area Networks (WPANs) that is being used in many commercial and research applications today where it has become an attractive solution for low power and low cost applications. The RF Tag is placed in a vehicle that will be approaching the entrance of an establishment, the RF tag reader is used to communicate with the RF tags and the RF tag writer is used to program or write to the RF tags. Vehicle identification is performed by reading the serial number in the RF tag and driver authentication is done by means of a password entered through the RF tag. Both information are read through the wireless 802.15.4 interface via the RF tag reader and sent to a central database through Ethernet for verification. In order to enhance the data security, 128 bit Advance Encryption Standard (AES) was implemented in the Zigbee interface. This paper is based on a prototype development of the proposed system and it presents hardware and firmware aspects of the design. A vehicle identification device profile was defined and developed using the Microchip Zigbee protocol stack. Hardware implementation of Zigbee RF tags, reader and writer was carried out using Microchip micro-controller PIC18F4620, Chipcon CC2420 RF transceiver and an inverted F-type PCB antenna which was used with the transceiver. The designed application functions in the 2.4 GHz frequency band. The physical layer of the Zigbee stack is implemented in the CC2420 transceiver and the Microcontroller implements the other layers including the application layers of the Zigbee stack. The system was successfully demonstrated at Ratmalana Air-force base with a maximum omni-directional range of 7meters.**

I. Introduction

Zigbee is a recently developed wireless technology used in many commercial and research applications. Based on the IEEE 802.15.4 specification [1], it has become a very attractive wireless connectivity solution due to its open standard, low-cost and low power characteristics [2]. Zigbee is suitable for low data-rate and low power consumption applications [3] in comparison with other wireless techologies such as Bluetooth and WiFi. Applications include home and building automation, industrial control, building management systems, environmental monitoring, vehicle fleet management systems etc.

Intelligent vehicle and fleet management systems are required by large companies, establishments and high security zones with restricted access, to identify, authenticate and manage their vehicle fleet and to control access to outsiders. With the advent of cheap low power commercial RF modules such fully automated management systems are being implemented using wireless technologies. For example [4] presents a novel bus priority control system for the Advanced Public Transportation System (APTS) based on wireless sensor networks and Zigbee, authors of [5] report the use of Zigbee RF nodes for data packet transmission in an intra-car wireless environment, [6] investigates the suitability to Zigbee wireless technology for Intelligent Transportation Systems (ITS).

We have proposed a system using Zigbee wireless RF tags to identify and authenticate vehicles entering into such a premises. Design consists of RF vehicle tags containing authentication information for each vehicle authorized, an RF tag reader, an RF tag writer and a central database containing information about all vehicles authorized to enter the facility. Prototype of the system was demonstrated under real conditions and results conclude that the proposed system is viable.

The rest of the paper will be organized as follows, section II will give details of the system model. An overview of Zigbee protocol and the operation of the proposed system is discussed in section III. Implementation of the system is discussed in section IV. Section V draws concluding remarks.

II. System Model

This section presents an overview of the system and introduces the functionality of each of the individual components.

A. Overview

Fig. 1 depicts the system model. Vehicular RF Tags are installed securely in all vehicles needed to be identified, authenticated and managed. Each vehicular RF tag is programmed to have a unique serial number for identifying it and a password to authenticate the driver. An RF tag reader module is installed near the entrance to the facility. When a vehicle stops at the entrance the reader detects the vehicular RF tag and retrieves authentication information from it. This information is transfered over Ethernet to a central database to verify whether access is granted for a particular vehicle to enter into premises. Furthermore, the driver of the vehicle is authenticated by means of a password entered using a numerical keypad in the vehicular RF tag when prompted by the RF tag reader. Using the information received from the

978-1-4244-2900-4/08/$25.00

central database a human security personnel at the entrance or automated security system can take action to allow or deny the vehicle entrance into the facility.

B. Vehicular RF Tag

Each vehicle would be equipped with a vehicular RF tag having a unique serial number. The vehicular RF tag module would consists of a 2.4 GHz RF transceiver, micro-controller circuitry, power control circuitry, LED indicators and a numerical keypad used to enter password for driver authentication.

C. RF Tag Reader, Writer

The vehicular RF tag reader and writer are implemented as one unit. It comprises of a 2.4 GHz wireless transceiver, micro-controller, power control circuitry, and a debugging and communication interface. This module is connected to a personal computing device (laptop or desktop) through a RS232 interface which is used by the security personnel at the entrance. Communication from there onwards to central database server is done through Ethernet. Depending on the verification sent by the database server, positive or negative, the user at the entrance is presented with the simple decision of whether to allow or deny entrance to a vehicle or to check the identification of vehicle and authentication of a driver manually by engagement if in doubt. Although the human agent in the system between the central database and the tag reader can be removed and the system can be fully automated, we have resorted to implement it with human involvement since most organizations employ security personnel. The RF tag writer is used to program in the unique vehicle serial number and password information into a vehicular RF tag.

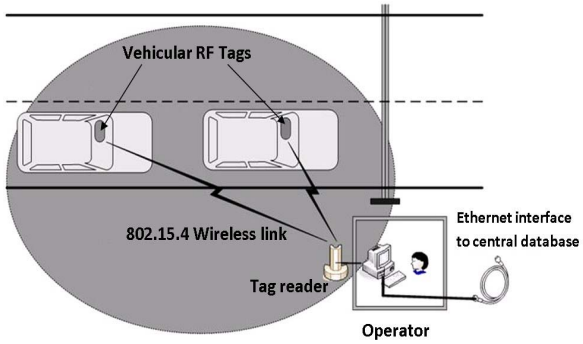

Fig. 1. System Model

III. System Operation

Here an overview of the Zigbee wireless protocol is presented followed by the communication involved in the system operation.

A. Zigbee protocol overview

Zigbee wireless protocol provides means to network a set of autonomous devices each equipped with a IEEE 802.15.4 standard RF transceiver to perform some networked task. The IEEE 802.15.4 wireless standard provides the Physical layer (PHY) and Medium Access Control layer (MAC) for the wireless communication while the Zigbee protocol working on top of it would perform the Network layer (NWK) and Application layer (APL) tasks. The PHY, MAC and NWK layers would handle how the underlying wireless data transmission would be carried out and how the network of RF transceivers would be organized while the APL layer would handle the tasks associated with each autonomous device.

After power up, a set of Zigbee devices would involve in network formation. A device defined as a Zigbee *coordinator* would perform energy scans on the available wireless channels and select an interference free channel for communication. Other devices that wish to join the network would send out *beacon* requests in order to join the network of the *coordinator*. The newly joined child devices to the network can either work as *end devices* or *routers* where the *coordinator* is the parent. *Routers* can permit other devices to join it whereas *end devices* can't; i.e. they are leaf nodes of the network.

In the proposed system a vehicular RF tag takes the role of a Zigbee *end device* while the tag reader & writer module takes the role of Zigbee *coordinator*. Different Zigbee devices implement different *device profiles* defined under the Zigbee protocol stack to suit the application in which they are being used. The Zigbee alliance has defined several *device profiles* for typical applications intended for Zigbee devices, such as home and building automation, industrial control etc [2]. The specification has also provided flexibility to include custom *device profiles* to suit customized applications [1]. We have defined the *vehicle identification device profile* to suit our application as shown in Fig. 2.

B. Tag-Reader communication

Fig. 3 shows the sequence of steps involved in the communication between vehicular Tag and Tag reader. Once a tagged vehicle arrives into the vicinity of the RF tag reader the vehicular RF tag would issue beacon requests to the Tag reader. Tag reader would respond with beacon response and join the RF tag into its network as a child node. Once connected to the personal area network (PAN) of the Tag reader, it would request the vehicle serial number from the tag. After reception of the serial number from the tag the password for driver authentication is requested by the reader which is validated with the central database once received from the tag. After both serial number and password are successfully exchanged the vehicle would leave the Tag readers PAN. A maximum of 10 RF tags can be accommodated in the PAN of the reader. Since tags joining the PAN would leave once they are validated or denied access, this PAN size of 10 is sufficient for the efficient operation of the system.

Similar flow of events occurs when information is written into a RF tag using RF tag writer. Instead of requesting

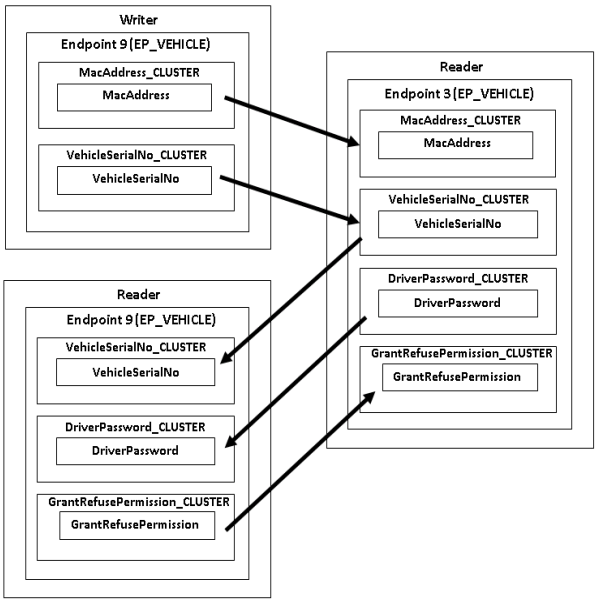

Fig. 2. Vehicle identification device profile

for information from the tag after it joins the PAN of the coordinator, the vehicle serial number and password would be written into it and an acknowledgment would be sent back to the writer.

IV. System Implementation

This section provides the implementation details of the prototype developed. The basic structure of the Zigbee device used in the system is shown in Fig. 4, consisting of a 2.4 GHz transciever and antenna, Microcontroller and power control circuitry.

A. 2.4 GHz RF transceiver

We have used a low cost low power IEEE 802.15.4 compliant RF transceiver CC2420 developed by Chipcon AS to design the RF modem in each Zigbee device. It operates in the frequency spectrum 2.4 - 2.4835 GHz with a 250 kbps data rate. Direct Sequence Spread Spectrum (DSSS) is used as the modulation technique.

Antenna design: An inverted F-type PCB antenna was used with the transceiver. This is a wire monopole where the top section is folded down to be parallel with the ground plane which reduces the antenna height and maintains a resonant wire length. Fig. 5 shows the PCB layout of the RF transceiver.

B. Microcontroller circuit

The microcontroller circuit interfaces with the RF transceiver and controls the operation of the Zigbee device. Microchip microcontroller PIC18LF4620 [7] was used in the design and it houses firmware required to communicate with RF transceiver and perform other house keeping routines of the device, such as taking inputs from numerical key pad, communicating with RS232 interface. The Zigbee protocol stack is implemented in the firmware of the microcontroller.

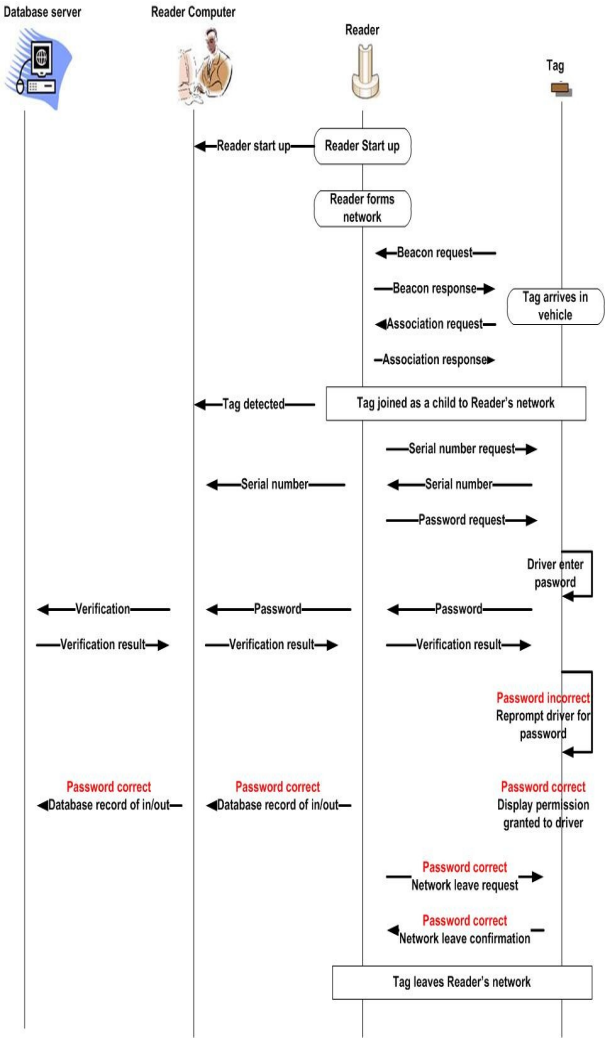

Fig. 3. Communication between tag and tag reader

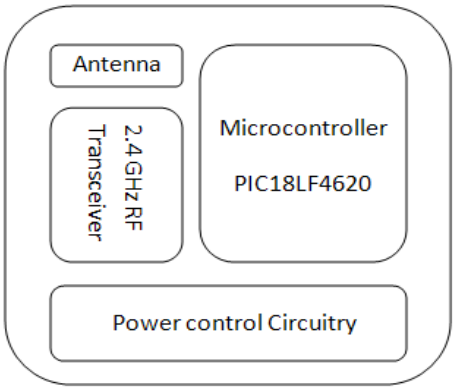

Fig. 4. Hardware modules in Zigbee device (Tag or Reader/Writer)

We used the free Zigbee stack provided by Microchip Inc. [8] for their 8 bit microcontrollers to implement the Zigbee protocol with the vehicle identification device profile. Since the application requires secure communication over wireless

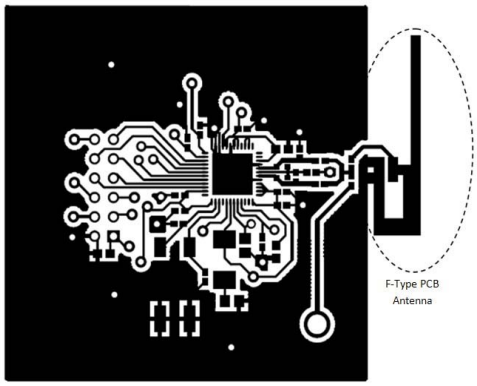

Fig. 5. PCB layout of RF transceiver circuit (top side)

channels, 128 bit Advance Encryption Standard (AES) [9] was implemented in the application layer of the Zigbee protocol stack.

C. Voltage Regulating Circuit

Both reader/writer and vehicular RF tags each require 100 mA under 3.3 V for their operation. Tag was designed to be powered by car battery or 9 volt battery and the reader/writer was designed to be powered by mains electric supply. Fixed positive voltage regulator MC7805 and low-dropout voltage regulator MAX882 were used to convert DC voltage 12 V and 9 V into 5 V and then 5V into 3.3 V respectively.

D. Test Results

The performance of the RF transceiver circuit was investigated using different test modes of the CC2420 transceiver. Fig. 6 show the outputs of the spectrum analyser for different performance tests conducted with the RF transceiver test setup. The plot in the bottom left of the figure shows the output obtained at the RF output pins of the transceiver when the device was programmed to output an unmodulated carrier, a peak at 2.4 GHz frequency can be clearly observed in the spectrum analyzer output. The plot in the bottom right shows the output of the spectrum analyzer when the device was programmed to modulate its carrier with a pseudo random data sequence.

Field tests were carried out at the air force base at Ratmalana, Sri Lanka where the prototype system was setup to authenticate and identify vehicles entering the high security zone of the air force base. Test results carried out revealed that our system has a maximum omni directional range of 7 meters with a clear line of sight path communication.

V. Conclusion

In this paper we have presented a novel Zigbee based vehicular identification and authentication system. We have provided a detailed description of our system referring to the prototype developed. A custom Zigbee device profile was developed to suit the proposed application and was implemented in the Zigbee protocol stack defined by the Zigbee specification. Prototype of the proposed system was field tested and demonstrated at a working environment.

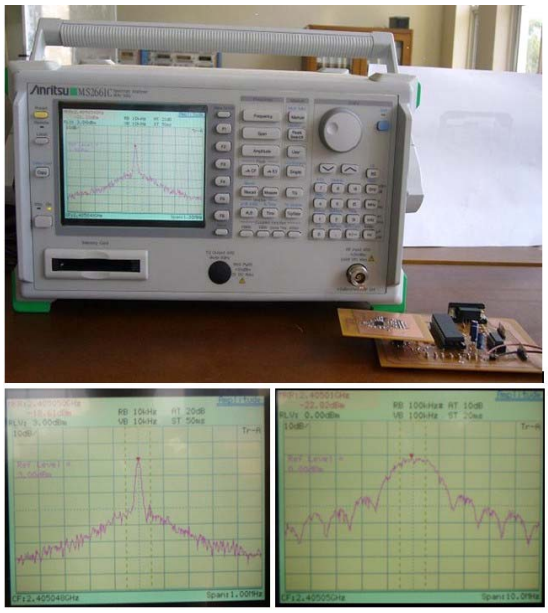

Fig. 6. CC2420 RF output through spectrum analyzer

References

[1] *Zigbee Specification, ZigBee Document 053474r06 Version 1.0*, Zigbee Alliance Std., Dec. 2004.

[2] A. Wheeler, "Commercial applications of wireless sensor networks using zigbee," in *Communications Magazine, IEEE*, vol. 45, no. 4, Toronto, Ont., Canada, Apr. 2007, pp. 70–77.

[3] N. Baker, "Zigbee and bluetooth strengths and weaknesses for industrial applications," *Computing & Control Engineering Journal*, vol. 16, pp. 20–25, Apr./May 2005.

[4] Z. Wu, H. Chu, Y. Pan, and X. Yang, "Bus priority control system based on wireless sensor network (WSN) and zigbee," in *Vehicular Electronics and Safety, 2006. ICVES 2006. IEEE International Conference on*, Dec. 2006, pp. 148–151.

[5] H.-M. Tsai, C. Saraydar, T. Talty, M. Ames, A. Macdonald, and O. K. Tonguz, "Zigbee-based intra-car wireless sensor network," in *Communications, 2007. ICC '07. IEEE International Conference on*, June 2007, pp. 3965–3971.

[6] K. Selvarajah, A. Tully, and P. T. Blythe, "Zigbee for intelligent transport system applications," in *Road Transport Information and Control - RTIC 2008 and ITS United Kingdom Members' Conference, IET*, May 2008, pp. 1–7.

[7] (2008, 01) PIC18F2525/2620/4525/4620 Datasheet 28/40/44-Pin Enhanced Flash Microcontrollers with 10-Bit A/D and nanowatt Technology. Microchip Technology Inc. [Online]. Available: http://www.microchip.com

[8] Y. Y. David Flowers, Kim Otten and N. Rajbharti. (2006, 12) Microchip stack for the zigbee protocol. Microchip Technology Inc. [Online]. Available: http://www.microchip.com

[9] D. Flowers. (2006, 10) Data Encryption Routines for the PIC18. Microchip Technology Inc. [Online]. Available: http://www.microchip.com