Automatization of the Shop2box System with Bluetooth

Mikael Soini, Reino Aarinen, Lauri Sydänheimo, Markku Kivikoski

Abstract—**In this paper, a shop2box system is presented in which a customer can order over the Internet grocery that is delivered to a receiving box leased by the customer in his or her neighborhood. The aim of this paper is to focus on a Bluetooth application designed for the shop2box system and on its possibilities. The task of this application is to identify the system devices by automatically forming an authenticated Bluetooth link between the devices. After the identification, the deliveryman can open the receiving box for delivery and the customer can collect the order when convenient. This paper will cover the application device characteristics and the most important protocols in respect of the application's function. Also, the key items of the Bluetooth technology will be presented briefly.**

Index terms—**Bluetooth, Electronic Grocery Shopping, Home Delivery, Security**

I. Introduction

A. Shop2box System

The shop2box system is aimed at saving the consumer's time by eliminating daily visits to the store. Grocery buying on the Internet through the shop2box system is quite similar to the usual Internet grocery buying. The major difference is that products are not delivered directly to the consumer, but to a receiving box, which he or she owns or leases. Consequently, deliveries can be carried out at any time and the consumer's presence is not required. The consumer is not obliged to change his or her schedules, and the transport company can plan the delivery routes and times as optimal as possible so that the customer still receives the products by the agreed time. In the future grocery chains will avoid unnecessary transport between warehouses and stores if the consumer adopts this kind of Internet shopping/delivery service. The receiving box of the shop2box system is an intelligent refrigerator-freezer that is located near the consumer. The receiving box is located either in the consumer's home yard or, e.g. in the parking hall near his or her working place. [1]

Manuscript received November X, 2002. This work was supported by Tekes under Kilavi project.

M. Soini is with the Rauma Research Unit, Electrical Engineering Department, Tampere University of Technology, Rauma 26100, Finland (e-mail: mikael.soini@tut.fi)

R. Aarinen is with the Hollming Ltd, Electronics, Rauma 26100 (e-mail: reiska@hollming.fi)

L. Sydänheimo is with the Rauma Research Unit, Electrical Engineering Department, Tampere University of Technology, Rauma 26100, Finland (e-mail: lauri.sydanheimo@tut.fi)

M. Kivikoski is with the Electrical Engineering Department, Tampere University of Technology, Tampere 33101, Finland (e-mail: markku.kivikoski@tut.fi)

B. Development of the Delivery Process

In the shop2box system, the wireless technology is used for opening receiving box doors. At present the customer and the deliveryman can open the box by means of a mobile phone. The objective of this research work is to study the Bluetooth technology and to apply it in the box door opening process. At first Bluetooth is used to simplify the work of the deliveryman.

The objective is to create an automatic data secure Bluetooth link between the delivery van terminal and the receiving box on the delivery van's arrival in the range. This kind of connection is called ad-hoc connection that is established when the need arises without predetermined network infrastructure. In spite of that, a spontaneous network of this kind has to able to distinguish devices and perform required authentication and access control between devices [2]. When the Bluetooth link is formed, the control card of the receiving box opens the box electronic lock and the deliveryman places the ordered products in the box. So the doors will open without the deliveryman's participation in the process. Bluetooth replaces the inconvenient and time-consuming use of ordinary keys or text messages in door opening. The deliveryman does not need to write a SMS message in a particular format and, after sending it, await door opening. Furthermore, the use of ordinary keys prevents progress towards a more automatic system that is needed when operating as a part of a data network (e-activity). Different user interactions cannot be registered and verified with the system using mechanical keys. Also, key possession and control of a large amount of keys have turned out to be a problem in the early stage use of the shop2box system.

II. Bluetooth Technology Overview

Bluetooth is short-range radio technology that enables voice and data packet transmission. The most important application fields for Bluetooth are mobile devices and embedded systems. That being the case, Bluetooth chips must be low-cost, small-sized and low-power. Open standard Bluetooth operates practically worldwide.

Bluetooth operates in the license free 2,4 GHz Industrial, Scientific, Medicine (ISM) band. In the ISM band, a set of 79 hop carriers has been defined at 1 MHz spacing. In its operation Bluetooth uses FHSS method (Frequency Hopping Spread Spectrum) in which the transmission frequency is changed after every packet. The hopping frequency sequence

defines the transmission frequency between the devices. The Bluetooth physical channel is formed from successive transmission frequencies. For Bluetooth duplex data transmission, the TDD (Time Division Duplex) is used in which the physical channel is shared by piconet devices on a time division basis. The Bluetooth physical channel is divided in time slots of 625 µs in length. Depending on the packet type, each packet can be composed of 1, 3 or 5 time slots. The Bluetooth system uses GFSK modulation (Gaussian Frequency Shift Keying) to send data. This enables implementing low-cost radios.

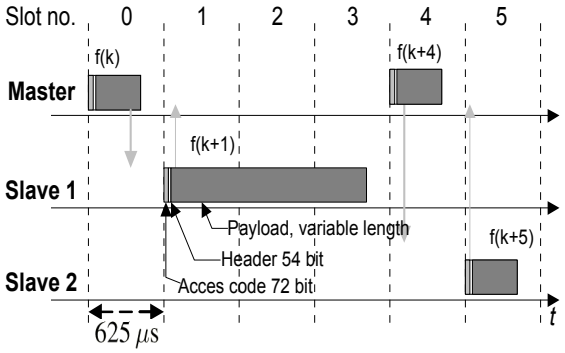

Fig. 1. TDD and packets

Bluetooth devices can be connected in an Ad-hoc fashion that is called a piconet. When a piconet is formed, one device acts as a master while up to 7 devices act as active slaves. Besides active slaves, a piconet can accommodate devices in different low-power modes. The above-mentioned frequency hopping sequence of the channel is defined by the master ID parameters and its phase from the master clock. All piconet devices use the same physical channel for data transmission, as a result only one device can transmit data/voice at a time in the piconet. Since master transmits every second packet in the piconet, the piconet slaves are permitted to perform every second transmission. The slave that has been address by the master in the preceding master-to-slave slot is permitted to transmit in the next slave-to-master slot. Maximum 3 channels are reserved for voice transmission with assigned time slots; consequently, voice transmission has a higher priority than data packets. The master can transmit data packets to the slaves either in point-to-point or in point-to-multipoint mode.

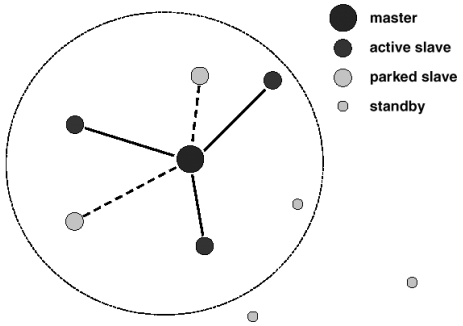

Fig. 2. Piconet

Different low-power modes (sniff, hold, park) can be used when data is not transmitted to maintain the synchronization to the piconet. In low-power modes, shortening the device duty cycle in the piconet reduces the power consumption; as a result, the device is for most of the time in low-power sleep mode.

Bluetooth devices' transmission power is 1…100 mW, which correspondingly provides ideal transmission distances of about 10…100 m. These distances shorten in interference conditions when several devices, such as a microwave oven, WLAN (Wireless Local Area Network) and RFID (Radio Frequency Identification), operate at the same frequency. As distances grow bigger and/or interference increases, Bluetooth transmission speed decreases. The ideal maximum transmission speed in Bluetooth is 721 kbps in asymmetric and 432 kbps in symmetric link when using packets of 5 time slots in length with a minimum amount of control data. In practice transmission speeds are approximately 250 – 350 kbps depending on transmission distance, transmission power, geometry of environment and other techniques in the ISM band. [3, 4, 5, 6]

III. Bluetooth in Shop2box System

A. Bluetooth Devices

Similar Bluetooth cards are used both in the receiving boxes and delivery vans. Cards are based on CSR (Cambridge Silicon Radio) BlueCore01b chips [7]. GigaAnt Mica SMD (Surface Mounted Devices) circuit board antennas are utilized as antennas. (With these antennas, a transmission distance of several meters may be achieved between devices.) These above-mentioned chips are a step towards a single-chip solution in which all components required for Bluetooth may be implemented with one chip. Due to the single-chip solution, the surface area required for Bluetooth may be reduced. The low-cost CMOS (Complementary Metal Oxide Semiconductor) technology is used in single-chip solution implementation [8].

Bluetooth cards replacing the serial port are configured as master or slave devices, which simplifies the system operation. The Bluetooth card in the delivery van is connected to the computer of the van through a serial port (RS232) and it acts as the Master. The Bluetooth card of the receiving box is connected in the same way to the receiving box control card and is configured as a slave.

In this paper, the master and slave configurations are presented in respect of GAP (General Access Profile). When not having an active connection with the Bluetooth card of the receiving box, the delivery van is in a limited inquiry mode and inquiries new devices which are in a limited discoverable mode. It is not possible to initiate a connection with the master because it does not respond to inquiries of other Bluetooth devices (non-discoverable mode), whereas the receiving box is set to non-

discoverable mode only when having an authenticated link with the delivery van. Otherwise the receiving boxes are in the limited discoverable mode and respond to all inquiries (general and limited). The receiving box does not need to inquiry other devices or initiate connections with other devices, so it does not support inquiry function. [9]

The receiving box and delivery van Bluetooth cards are paired in advance (pairing), which simplifies future connections ”in the field”. Therefore, the delivery van does not need a separate user interface for entering the PIN code that is required in pairing procedure. In pairing, a link key is created between Bluetooth devices to be used for Bluetooth link authentication. The used link key type is a combination key [3], which means that a different link key is used in different boxes. This provides a better security level in comparison with the unit key solution. Besides the link key, the delivery van Bluetooth card needs the Bluetooth card IDs of the receiving boxes for the creation of authenticated Bluetooth link. This information about the receiving boxes located along the route of the delivery van are saved in the FLASH memory of the delivery van Bluetooth card.

B. Bluetooth Protocol Description

Fig. 3 shows the box door opening process of the shop2box system on the level of the Bluetooth protocol [3].

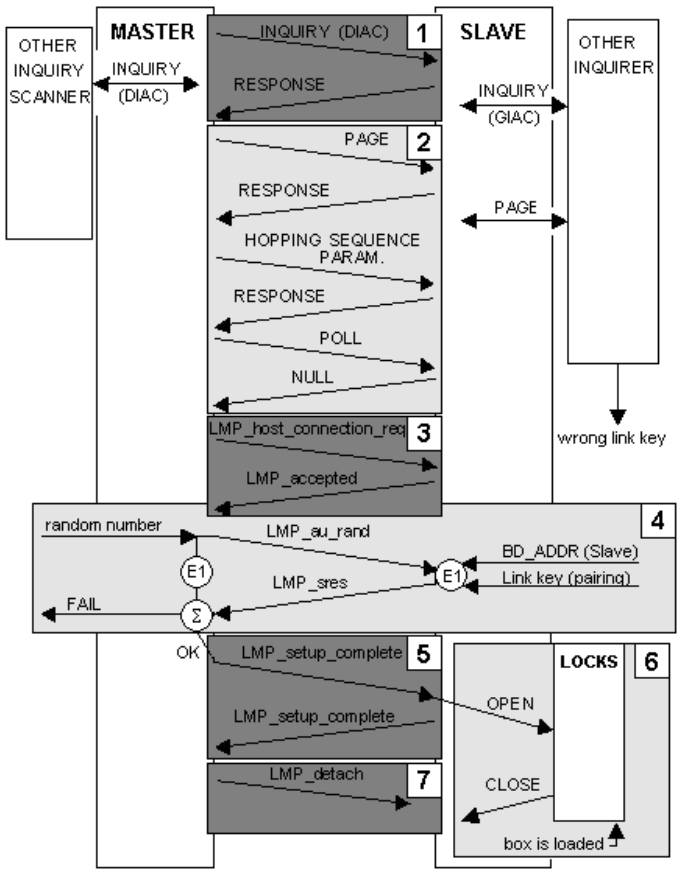

Fig. 3. Forming the connection

Step 1.
32 (16+16) frequency channels are used in the inquiry in accordance with abnormal hopping sequence that does not contain source information. ID packets contain an inquiry access code (IAC) that may indicate which device class should respond. The inquiring master sends out two ID packets of half time slot in length in every second time slot and listens to the responses in every second. In this way the connection setup is speeded up. In the inquiry, an ID packet train of 10 milliseconds (fig. 4) is sent at first 16 frequencies with repetition for 256 times. At the next 16 frequencies the procedure is repeated.

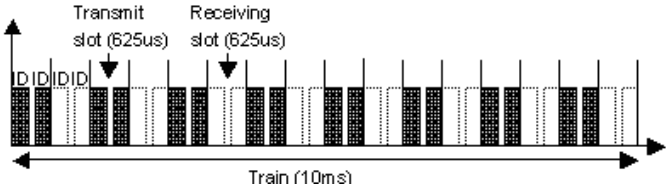

Fig. 4. ID-train

Devices that are in the *Inquiry scan* state listen to inquiries for 11,25 ms every 1,28 s and after that change the frequency channel. Having received an ID message, the destination will respond in a random time period to the source with an *inquiry response* that is a FHS packet in which the master can read the destination Bluetooth device address (BD_ADDR) and clock information. The connection between the devices can be set up with this knowledge. A Dedicated Inquiry Access Code (DIAC) is used in this application. With the DIAC the delivery van discovers only these dedicated receiving boxes in the range, not, e.g. any mobile phones. The receiving box Bluetooth card may also receive other ID packets containing general IAC (GIAC). These ID packets are responded although the receiving box Bluetooth card is in the limited discoverable mode. [5, 9]

Step 2.
The connection is established with the paging procedure. The paging has no essential differences from the inquiry, but the train is only repeated for 128 times. In the page state, the hopping sequence of ID packets and their phase are defined by the slave device parameters (BD_ADDR + clock). The page state is entered first by the master by sending an ID packets (slaveID) as in the step 1. These ID packets contain slave Device Access Code (DAC). The slave that has entered the Page scan state listens to these ID packets in regular time intervals. When the slave receives a slaveID packet that is meant for it, it will respond with an identical slaveID packet.

Next the master then sends its own BD_ADDR and clock parameters to the slave (a FHS packet), and, after the response of the slave (slaveID), the connection parameters defined by the master are switched to. These parameters are master BD_ADDR that defines both frequency hopping sequence and CAC (Channel Access Code) that identifies the piconet.

Besides, the master clock defines the sequential phase, in other words, timing. This procedure establishes the connection between the devices. This is verified with a master POLL message that is responded by the slave with, e.g. a NULL message. [5]

Step 3.
In this application, the master requires a connection above the LMP layer because SPP (Serial Port Profile) is used. SPP uses upper protocol layers, e.g. RFCOMM. An LMP_host_connection_req message is needed for the connection request to application layers. When the slave receives this message, the application is informed and it can accept or reject the connection request (LMP_accepted/ LMP_not_accpted).

Step 4.
When a positive response is received to the LMP_host_connection_req message, a data secure link can be formed. The authentication procedure requires an link key that is formed in the pairing procedure. Since the pairing procedure is performed already in device configuration, the link key already exists when the step 4 is entered. Therefore authentication eliminates the possibility of connection setup by outsiders (Fig. 3, other inquirers) with the receiving boxes.

The master initiates the authentication procedure by issuing a random number (EN_RAND), in other words, a challenge to the slave. Both devices calculate with the E_1 algorithm [3] a response, SRES. The response is derived from the slave BD_ADDR, the link key and the random number created by the master. The slave then sends its calculated response to the master that compares the calculated responses and approves authentication in case the results coincide. The Bluetooth security characteristics are limited in the lower protocol layers described here. Requirements to use more developed secure procedures (public keys, certificates) call for application layer solutions. [5, 6, 9]

Step 5.
After authentication, the logical connection between the devices is formed and acknowledged by the master with an LMP_setup_complete message. The slave acknowledges this by sending the same message to the master [3]. Now, if needed, data can be sent between the device applications. In this system, data can be sent between the serial port emulators of both ends if need should arise. AT commands, which are familiar from the transmission between modems, can be utilized in data transmission. Only the connection setup is required at this stage.

Step 6.
The connection is set up and the box control card gives the electric lock an order to open up. The driver can place the ordered products in the box.

Step 7.
The box doors have been open and the connection between the Bluetooth cards of the delivery van and the receiving box can be closed. The master terminates the Bluetooth link with an LMP_detach message.

IV. Future Application Scenarios

In the future scenario of the shop2box, the use of Bluetooth is scaled, besides receiving box door opening, to other functions as well. The data secure Bluetooth link, which is described in this paper, can replace the use of GSM in customer operations with the receiving box. In another scenario delivery vans can be identified by the loading platforms of a distribution center using Bluetooth, and accordingly send them information on, e.g. delivery route. Also, receiving box maintenance can be carried out using Bluetooth. On arrival of a serviceman to the box he is identified and he will automatically receive information on, e.g. box temperature. Actual data transmission is also required for these applications. This is implemented with application programs; in other words, the Bluetooth link setup remains unchanged.

Bluetooth is not the only option for the implementation technology when developing the shop2box system. RFID (Radio Frequency Identification) is aimed at short-range device identification and represents a respectable competitor due to its low cost. When using RFID, the device identification is performed using a RFID tag that is located in the receiving box. The tag is activated by the power from the operating device (passive RFID tags) and the identification can be carried out [10]. The RFID technology may also be used to supplement Bluetooth in delivery. In that case products to be delivered will be provided with RFID tags that contain information on, e.g. product storage. On the basis of that piece of information the deliveryman is able to place groceries in the right section of the receiving box opened with Bluetooth, in other words, in refrigerator, freezer or grocery [1].

V. Conclusion

The objective of this research work is the automatization of the last link in the shop2box system delivery chain, in other words, the delivery to receiving boxes of grocery that has been ordered over the Internet. Besides simplicity, this door opening process using Bluetooth requires simple data secure characteristics that can be achieved with Bluetooth. To ensure security the Bluetooth cards of the delivery van and the receiving boxes share a common link key that enables the establishment of an authenticated connection between the van and the boxes. Only after the authenticated link is set up, the box doors will open. The authenticated link forming procedure is entered on arrival of the van in range of an active receiving box.

When the amount of receiving boxes increases in the same area, the cards that are based on BlueCore01/02 can be changed to support point-to-multipoint mode, which enables the connection setup with several receiving boxes at a time. Communication between the shop2box system and the receiving boxes must be developed more intelligent so that the receiving boxes know on the basis of the delivery van Bluetooth ID whether to enter the inquiry_scan mode. This eliminates unnecessary connections between the delivery van and boxes that are not needed at the moment.

REFERENCES

[1] Reino Aarinen, Markku Kivikoski, Lauri Sydänheimo, " Shop2box Concept and Radio Frequency Identification," To Appear: Proceedings of the 2002 IEEE Conference on Systems, Man and Cybernetics, Hammamet, Tunis, 2002

[2] Laura Marie Feeney, Bengt Ahlgren, Assar Westerlund, "Spontaneous Networking: An Application-Oriented Approach to Ad Hoc Networking," IEEE Communications, vol. 39, no. 6, 2001, pp. 176-181

[3] Bluetooth Special Interest Group, "Bluetooth spesification v1.1, Volume 1: Core," http://www. bluetooth.com, 2001

[4] Jennifer Bray, Charles F. Sturman, "Bluetooth connect without cables," Prentice Hall, 2001

[5] Palowireless, Bluetooth Resource Center. http://www.palowireless.com/bluetooth/

[6] J.Haartsen, "The Bluetooth Radio System," IEEE Personal Communications, vol. 7, no. 1, 2000, pp. 28-36

[7] Cambridge Silicon Radio (CSR), Bluecore01b datasheet. http://www.csr.com/bc01datasheet.pdf

[8] Cheryl Ajluni, "Single-Chip Radio Solution Goes Blue," Wireless Systems Design, vol. 6, no. 3, 2001, pp. 31-34

[9] Bluetooth Special Interest Group, "Bluetooth spesification v1.1, Volume 2: Profiles," http://www. bluetooth.com, 2001

[10] RFID (Radio Frequency Identification). http://www.aimglobal.org/technologies/rfid/