BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LXI No. 3/2009	267 - 274	Seria Tehnică

Bluetooth Solution Proposed in Control Networking

Silviu Popovici

Petroleum – Gas University of Ploieşti, 39 Bucureşti Blvd., Ploieşti, ROMÂNIA
e-mail: silviu_p@upg-ploiesti.ro

Abstract

The main objective of this paper is to propose some solutions in control networking environment based on Bluetooth wireless technology. The research is based on desk WPAN proposed for security reason and is focused on Bluetooth connectivity and propose a management infrastructure for sensitive data.

Key words: *Bluetooth, wireless, PAN, connectivity, profiles.*

Introduction

Bluetooth technology is a cable replacement solution for mobile devices. This technology is designed for short and medium distances and is based on RF (Radio Frequency) technology like RFID and 802.11 wireless networks. Most users think the Bluetooth is just a simple wireless connection dedicated to gadgets like music players, portable video devices, etc. Bluetooth is more than that. It's a technology wide used in wireless networking, medical care, industrial environment and more other domains. Bluetooth technology is the only one technology who sold over 2 million unit devices in 10 years.

Bluetooth short history

The name of the Bluetooth it is English version of name Blátönn or Blåtand, the name of the king Harald I of Denmark and Norway. Like name, Bluetooth logo is analogous to the modern Latin letters H and B: (for *H*arald *B*luetooth)  and  put together [9].

Bluetooth specification was initially defined in 1994 by Jaap Haartsen and Sven Mattisson, two employees of Ericsson Mobile.

On May 20, 1998 it was announced a new working group Bluetooth Special Interest Group (SIG), with the main scope of Bluetooth specifications release. First versions of Bluetooth were 1.0 and shortly after 1.0B. This version had many problems and products from different producer were inoperable. Latest Bluetooth 1.1 version was recognized like IEEE 802.15.1-2002 Standard and provided fixes for many errors and added support for non-encrypted communication.

Version 1.2 of Bluetooth specifications added major improvement for faster connection and discovery, adaptive frequency-hopping spread spectrum, higher transmission rate and introduced support Host Controller Interface. This version was rated as IEEE Standard 802.15.1-2005.

In November 2004 it was released version 2.0 of Bluetooth specifications which introduces the EDR (Enhanced Data Rate) concept for faster data transfer. Bluetooth 2.1+EDR adopted in July 2007 by Bluetooth SIG introduced more interesting features: extended inquiry response, encryption pause resume, secure simple pairing and automatic creation of secure Bluetooth connections.

The future of this technology is represented by version 3.0 – Seattle, announced for adoption in first semester of 2009. The main features of these specifications will be the topology management thought automatic piconet configurations, Bluetooth information point with broadcast channel, and the alternate MAC/PHY which will provide an alternate connection via low power Bluetooth connection for idle devices or via low power per bits radio when a huge amount of data has to be transmitted. The efforts will be concerned into three distinctive directions: Bluetooth low energy, Bluetooth high speed (up to 480Mbps using UWB – Ultra Wide Band techniques) and Bluetooth low cost [1].

How Bluetooth works

Physically, Bluetooth operate in RF technology into an unlicensed ISM band at 2,4 GHz and implies a Frequency Hoping Spread Spectrum (FHSS) technology to combat interferences and fading. A simple FHSS communication algorithm looks like this: step 1: emitter sends a request over a predefined frequency or over a control channel; step 2: receptor responds with an number known as seed packet; step 3: emitter uses a number as variable into a predefined algorithm which calculates the sequence of frequencies which must be used; step 4: emitter sends a synchronization signal within first frequency from calculated sequence to ensure the accuracy of receptor calculus; step 5: the communication begins between devices and both part change frequency in calculated order from the same point in the same time [7].

This technology uses 79 channels of 1 MHz each, from 2402 MHz up to 2483 MHz, and modulations is based on Gaussian Frequency Shift Keying (GFSK). Basically, data rate is 1Mbps and with EDR enabled Bluetooth data rate is up to 3 Mbps.

Distances for transmission are divided in three classes: up to 1 meter – class 3 devices, up to 10 meters class 2 and up to 100 meters for class 1 devices [3].

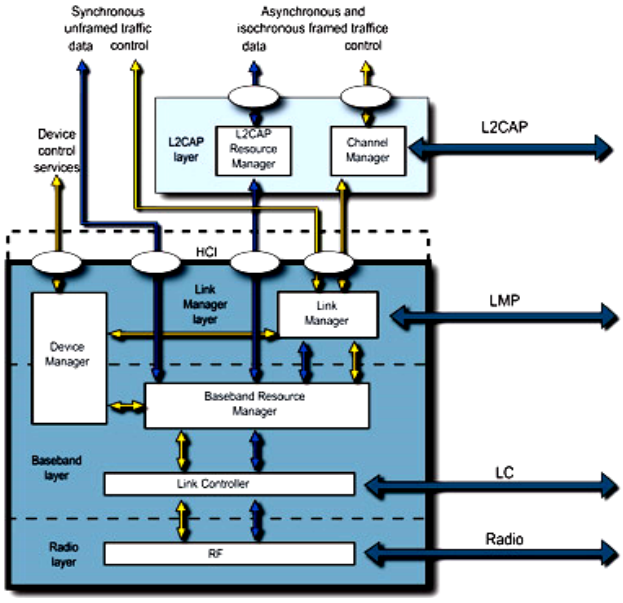

Fig. 1. Bluetooth layers and protocol stack [3].

The philosophy of Bluetooth technology consists in profile concept: every service has one profile associated. At present there are defined 22 profiles like: Advanced Audio Distribution Profile (A2DP), Dial-Up Network Profile (DUN), File Transfer Profile (FTP), Human Interface Device Profile (HID), Personal Area Networking Profile (PAN), Service Discovery Application Profile (SDAP), Service Port Profile (SPP), Synchronization Profile (SYNC) and more others. [5] Also, core Bluetooth specification uses layer and protocol stack concept as seen in figure 1. The layers are, from bottom to the higher level: Radio – provides physical information about communication channels and time to hope interval,

Base Band (BB) - specifies or implements the medium access and physical layer procedures between Bluetooth devices, Link Manager (LM) - used to control and negotiate all parameters of the operation for Bluetooth connection between two devices, Host Controller Interface (HCI) which provides a command interface to the BB and LM layers and Logical Link Control and Adaptation (L2CAP) with capabilities of support for higher level protocol multiplexing, packet segmentation and reassembling [4].

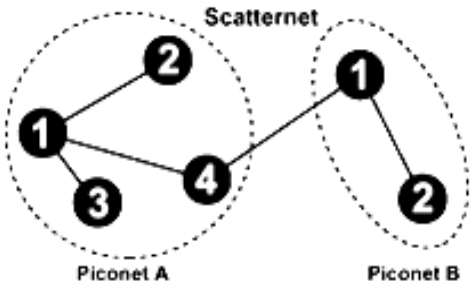

Fig. 2. Bluetooth piconets and scatternet.

Bluetooth communication topology is designed to act as a piconet. These mean two devices who want to initiate a connection must be synchronized first, and they act like master-slave communication. One master device could control up to 7 active devices and up to 127 parked devices. Parked devices are the devices that are in idle state. These could be instantly reactivated at a synchronization signal. If we have multiple piconets and one slave from a piconet act like a master in other piconet we say we have a scatternet (figure 2). The most important layer of communications in Bluetooth is L2CAP, which manage multiple types of connections. The needed protocols are RFCOMM, BNEP, SDAP and SSP [6].

Bluetooth security

Today's wireless desiderate is that the data are being invisibly sent from device to device and this data need to be securely sent. Bluetooth wireless technology is concerning on security while making connections between devices.

Developers of the Bluetooth wireless technology products have some options for implementing security. There are three modes of security for Bluetooth access: non-secure, service level enforced security and link level enforced security.

For devices and services there exist different security levels. Devices have two security levels: "trusted device" and "untrusted device". A trusted device has already been paired with other devices, and has unrestricted access to services [2].

For services there are defined three levels of security: services that require authorization and authentication, services that require authentication only and services that are open to all devices.

Bluetooth PAN scenarios for industrial environment

Industrial plants have many devices connected in different ways. It could be simple data collecting units, intelligent devices (sensors with built-in intelligence, single-loop controllers or programmable controllers) and supervisory systems (used for data logging and supervisory control). For interconnection these types of devices use different communication protocols and media. In some cases they may be replaced with Bluetooth technology.

Bluetooth could be used to connect these devices. It also describes some specific requirements on the Bluetooth technology for this area. Possible scenarios for industrial use of Bluetooth are divided in four distinct categories.

Serial cable replacement

The purpose of this scenario is to be an alternative for wired RS232, RS422 or RS485 connection. In this case two options are provided. First is to use an external Bluetooth adapter connected to a serial port of device. Second option is to use embedded adapters, connected internally. Bluetooth adapters emulate serial port and transfer data using the RFCOMM protocol. Another cable replacement option is addressing to the advanced devices that have built-in support for TCP/IP and WEB server. In this case PAN Profile is used and the Bluetooth stack is embedded in device. These permit HMI (Human Machine Interface) devices with PAN profile to access WEB interface of the device [8].

Combine Bluetooth and Internet technologies

This scenario supposes a Bluetooth adapter is attached to the device. The adapter communicates with industrial device using an industrial protocol like Modbus. The device has also embedded WEB/WAP server. The WEB/WAP pages are accessed through Bluetooth via PAN and could be used to display dynamic data and to modify parameters [8].

Industrial Access Points

Industrial Access Points (AP) require creating a wireless island with Bluetooth devices already connected to an existing wired network (figure 3).

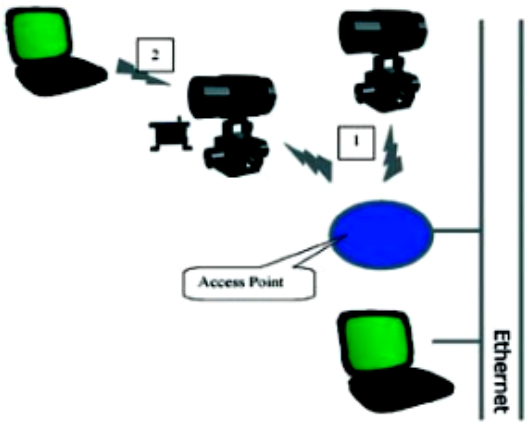

Fig. 3. Bluetooth Access Point Communication [8].

The wired network could be a standard Ethernet network or an industrial network. In this scenario more options may be used. For the first the wired network could be standard Ethernet, devices have embedded WEB servers and the pages are accessed via AP, which has a WEB interface with all connected devices. Another option is described as the AP acts like a dial-in AP using a modem or a GPRS technology. Data is transferred using a high level Bluetooth protocol. The other option is to have support for PAN and embedded WEB server into AP. In this case data are accessed from a Bluetooth device using a HMI. The communication protocol is on top of the Bluetooth stack and could invoke Bluetooth on L2CAP level [8].

Wireless sensors and actuators

Sensors and actuators could be of different types. Some of them may have high level built-in intelligence and other could be simple input-output devices. In these conditions requirements could differ. Intelligent devices could include local functionality to maintain the process running if Bluetooth connection is lost. That is done by dividing control algorithm one part for supervisory control executed into a remote host and one part executed locally in device (designed for critical control). That could consist in a performance solution when the requirements are higher than Bluetooth performance. Also different processes have different requirements for Bluetooth solutions [8].

Industrial Requirements on Bluetooth

The Bluetooth technology of today fits many current industrial applications, but there are some additional industrial requirements that will enhance the Bluetooth possibilities.

Industrial applications require support for an enhanced Quality of Service (QoS). Time stamping is an important issue. The Bluetooth module used in industry should be able to work from –40 to +80 degree Celsius, and must have a robust design. Power consumption is also a major issue since power is normally not available. A pure battery solution is, in some cases, not attractive. Alternative power solutions must be considered [8].

Proposed solution for control network based on Bluetooth concept

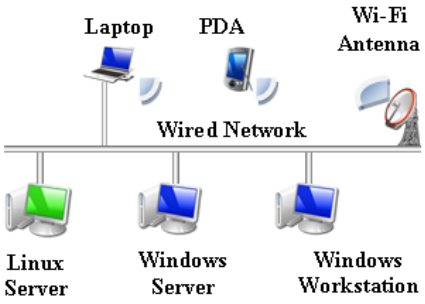

Fig. 4. Typical control network infrastructure.

Basically, a coordinator level on an industrial network looks like in the figure 4. That implies a large infrastructure of wired network based on different protocols, dedicated to the industrial applications and devices.

I propose, for the supervisor sections of the network, an architecture based on ad-hoc Bluetooth network. That means all devices could communicate each other based on Bluetooth PAN Profile. To see if my solution is working I do it some experiences using the cable replacement scenario.

Hardware infrastructure tested solution

To test those concepts I used three different computers, two with Intel solution and one based on AMD architecture. The Intel computers were provided one with simple Pentium 4 processor and one with dual core Pentium processor.

Fig. 3. Proposed and tested PAN architecture.

The AMD based solutions computer was installed with an AM2 Sempron processor. All computers involved in tests have USB support embedded. I also used two different portable computers: one with Bluetooth 2.0 support provided by manufacturer and one mini laptop with USB support. The other portable component was assured by a HP Ipaq PDA running Windows Mobile with wireless and Bluetooth 2.0 support. Finally, for desired tests I choose three Bluetooth class 1 USB dongles: two Yakumo dongles with Bluetooth 2.0+EDR and one Belkin dongle with Bluetooth 2.1+EDR.

Software support testing solutions

For the computers I chose the next roles: one Linux server, one Microsoft Windows 2003 server and a Microsoft Windows Vista Business workstation. The portable computers were installed one with Microsoft Windows XP SP2 and one with Microsoft Windows Vista Business operating systems. The Linux server was installed using Gentoo 2008 r1 distribution and Bluez, Bluetooth Linux core support. For Windows based computers and server I used IVT BlueSoleil application and Widcom \ Broadcom Bluetooth application.

Preparing testing environment

To be ready for testing solution, first it must set up individual computers and laptops to act like Bluetooth PAN device. To build the ad-hoc network, particular settings must be done in each type of device.

Setting up Linux Bluetooth Access Point

After Linux based distributions are installed in the server the kernel must be recompiled. The next modules must be enabled: Bluetooth subsystem support, Bluetooth device drivers and USB support for Host – side. After that BlueZ packet will be installed and configured. It's a good practice to set up the hcid.conf and rfcomm.conf files to accept and provide secure connection.

Optionally, in rfcomm.conf file a particular channel could be set for each device. Bluez application suite offer tools for testing services and connectivity (figure 7).

```
dtic007 / # hcitool scan
Scanning ...
        00:0A:3A:86:19:73       EEEPC_SILVIU
        00:1C:C4:FD:6A:8D       Sly_Pocket_PC
        00:02:72:C0:53:F2       gringo
dtic007 / # l2ping 00:0A:3A:86:19:73
Ping: 00:0A:3A:86:19:73 from 00:02:72:C0:53:F6 (data size 44) ...
44 bytes from 00:0A:3A:86:19:73 id 0 time 60.88ms
44 bytes from 00:0A:3A:86:19:73 id 1 time 19.68ms
44 bytes from 00:0A:3A:86:19:73 id 2 time 7.73ms
44 bytes from 00:0A:3A:86:19:73 id 3 time 9.72ms
44 bytes from 00:0A:3A:86:19:73 id 4 time 20.72ms
44 bytes from 00:0A:3A:86:19:73 id 5 time 7.73ms
44 bytes from 00:0A:3A:86:19:73 id 6 time 20.74ms
44 bytes from 00:0A:3A:86:19:73 id 7 time 14.73ms
44 bytes from 00:0A:3A:86:19:73 id 8 time 14.74ms
44 bytes from 00:0A:3A:86:19:73 id 9 time 10.72ms
^C10 sent, 10 received, 0% loss
dtic007 / # l2ping 00:1C:C4:FD:6A:8D
Ping: 00:1C:C4:FD:6A:8D from 00:02:72:C0:53:F6 (data size 44) ...
44 bytes from 00:1C:C4:FD:6A:8D id 0 time 37.89ms
44 bytes from 00:1C:C4:FD:6A:8D id 1 time 11.67ms
44 bytes from 00:1C:C4:FD:6A:8D id 2 time 12.72ms
44 bytes from 00:1C:C4:FD:6A:8D id 3 time 17.72ms
44 bytes from 00:1C:C4:FD:6A:8D id 4 time 31.74ms
44 bytes from 00:1C:C4:FD:6A:8D id 5 time 83.71ms
44 bytes from 00:1C:C4:FD:6A:8D id 6 time 32.73ms
44 bytes from 00:1C:C4:FD:6A:8D id 7 time 12.73ms
44 bytes from 00:1C:C4:FD:6A:8D id 8 time 12.75ms
44 bytes from 00:1C:C4:FD:6A:8D id 9 time 33.72ms
^C10 sent, 10 received, 0% loss
dtic007 / # l2ping 00:02:72:C0:53:F2
Ping: 00:02:72:C0:53:F2 from 00:02:72:C0:53:F6 (data size 44) ...
44 bytes from 00:02:72:C0:53:F2 id 0 time 45.80ms
44 bytes from 00:02:72:C0:53:F2 id 1 time 12.69ms
44 bytes from 00:02:72:C0:53:F2 id 2 time 11.72ms
44 bytes from 00:02:72:C0:53:F2 id 3 time 39.72ms
44 bytes from 00:02:72:C0:53:F2 id 4 time 29.75ms
44 bytes from 00:02:72:C0:53:F2 id 5 time 47.72ms
44 bytes from 00:02:72:C0:53:F2 id 6 time 11.72ms
44 bytes from 00:02:72:C0:53:F2 id 7 time 8.72ms
44 bytes from 00:02:72:C0:53:F2 id 8 time 8.74ms
44 bytes from 00:02:72:C0:53:F2 id 9 time 30.73ms
^C10 sent, 10 received, 0% loss
dtic007 / # hcitool inquiry
Inquiring ...
        00:1C:C4:FD:6A:8D       clock offset: 0x228a    class: 0x3a0110
        00:02:72:C0:53:F2       clock offset: 0x4189    class: 0x020104
        00:0A:3A:86:19:73       clock offset: 0x0d60    class: 0x3e010c
dtic007 / # hcitool device
Devices:
        hci0_   00:02:72:C0:53:F6
```

Fig. 7. Bluetooth testing tools on Linux Server.

Finally IP address must be set and pan daemon must be set too to listen for connection and act like NAP (Network Access Point) master or client. In this moment we will have a working Linux Bluetooth box.

Installing Windows based machine and servers

Since Windows XP SP2 Microsoft enabled Bluetooth support in operating systems core. But some Bluetooth devices are not recognized from Windows. In this case is necessary to install firmware drivers and application. Unrecognized devices are installed as standard devices and some services aren't available. For our tests after, Windows base operating system was installed, I installed BlueSoleil application which provides drivers and support for many type of USB Bluetooth dongles to use with Yakumo dongle. For Belkin dongle I installed Widcom \ Broadcom application suite. Like for the Linux machine, each Windows based device must have set an IP address in the same network class. It is a good idea to not let the dynamic address allocation active on devices. IP address must be static allocated and manually configured.

Preparing PAN environment

To install the ad-hoc PAN is necessary to follow some steps. First, devices must be paired. After that, devices must be set invisible and undiscoverable for security reason. Next step is to discover available services for every device. PAN service must be installed and connection could be made.

Paired devices will recognize each other after pairing process is done. A good practice is to set a strong passkey for paired devices. Another way is to build a short data base with devices: names, MAC address, IP address and services. That could be stored in each device, but these require skills to build particular programs for connections.

Finally, before connecting devices one with other, even in Windows and Linux machines must be created rules in firewall to accept PAN connection. After that connections could be made. Last step is to interconnect devices. Now, the ad-hoc Bluetooth PAN is build and we could test the solution.

Testing solutions

Particular settings must be made in different servers and workstations depending on service which will be accessed. For test purpose I used a web based sever hosted into a Win2k3 server.

For this I created a rule in server firewall to accept incoming connections on port 80. Depending on the desired security level, rules could be created for each particular device which may request access to the server. In this way, connections may be limited to desired devices. I connected to the web server from various clients created on Bluetooth PAN and it worked (figure 8). In the same time in every Bluetooth device I created rules for ICMP requests and answers, so it was possible to test connections with ping application.

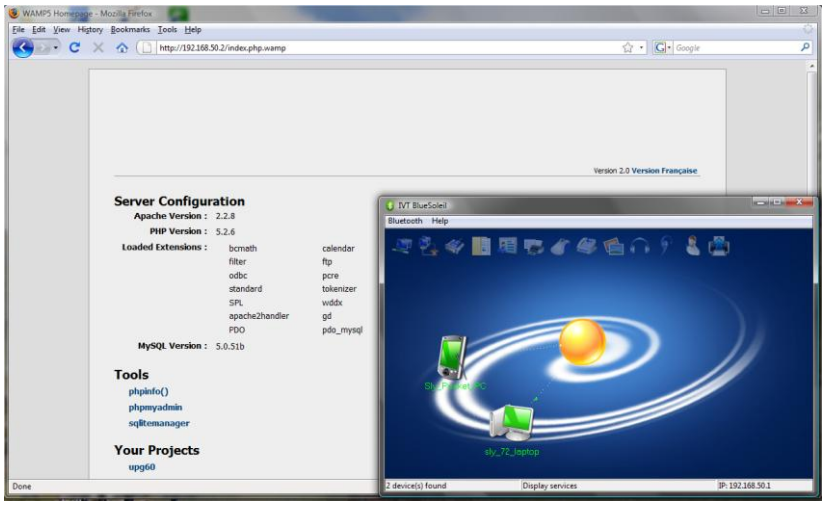

Fig. 8. Web page visited on hosted server via Bluetooth PAN

That worked too for me. Some devices could fail in sending requests and receiving answers if one or more of these steps are skipped. After tests, ICMP services must be blocked for security reason. If these services remain active, although the discoverability of devices is turned off, devices may respond on ICMP scanner requests and the network could be discovered from unwanted users.

Conclusions

Following the results of my tests I propose an ad-hoc Bluetooth PAN solution for part or entirely of control network. It is possible to build Bluetooth islands into control network environment. Depending on area of controlled network could be used combined technologies wireless and wired. If it's choosing usage of Bluetooth wireless technologies, then the solution must be well documented: device compatibility, class of devices and software used. Good start

points are *www.bluetooth.com* and *www.bluetooth.org*, web sites of Bluetooth SIG, which contain complete lists of tested devices and software in conformity with the Bluetooth standard. In the mean time it is recommended for control network environment to use class 1 Bluetooth devices. This will allow a straight radio signal for short distances even in perturbed environment. Next generation of Bluetooth devices will complete the robustness with speed, but, also, will be compatible with "old" devices. In this way the solutions will be extensible and flexible.

References

1. Foley, M. – *How Bluetooth and 802.11 will team up to deliver high speed wireless connections.* Wireless Net DesignLine, Bluetooth SIG, 2008.
2. *** – *Core Specification v2.1 + EDR – How it Works – Security.* http://www.bluetooth.com/Bluetooth/Technology/Works/Security, Bluetooth SIG, 2009.
3. *** – *Core Specification v2.1 + EDR – How it Works Core System Architecture*. http://www.bluetooth.com/Bluetooth/Technology/Works/Core_System_Architecture.htm, Bluetooth SIG, 2009.
4. *** – *BLUETOOTH SPECIFICATION Version 2.1 + EDR, Bluetooth Qualification Program Reference Document (PRD).* http://www.bluetooth.com, Bluetooth SIG, (26 July 2007).
5. *** – *Core Specification v2.1 + EDR – How it Works Profiles Overview*. http://www.bluetooth.com/Bluetooth/Technology/Works/Profiles_Overview.htm, Bluetooth SIG, 2009.
6. Muller, N. – *Bluetooth Demistified.* McGraw-Hill, Telecom, 2001.
7. *** – *Frequency-hopping spread spectrum*. http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum, WIKIPEDIA The free Encyclopedia, 2009.
8. Connect Blue – *Industrial use of Bluetooth*. Connect Blue AB, Sweden, 2001.
9. *** – *Bluetooth*. http://en.wikipedia.org/wiki/Bluetooth, WIKIPEDIA The free Encyclopedia, 2009.

Soluţie Bluetooth propusă pentru reţele industriale de control

Rezumat

Principalul obiectiv al acestei lucrări este acela de a propune unele soluţii de conectivitate pentru reţelele industriale de control bazat pe utilizarea tehnologiilor Bluetooth. Cercetările şi testele sunt concentrate pe conceptul de reţele fără fir construite ad-hoc, arhitectură propusă din motive de securitate. De asemenea, testele sunt concentrate pe studiul conectivităţii Bluetooth, propunându-se o infrastructură pentru reţele industriale de date cu caracter sensibil.