A Model Using Open-Source Hardware and Software to Assess Wi-Fi Affects Zigbee's Performance

Dalibor Dobrilovic, Milica Mazalica, Goran Gecin
University of Novi Sad, Technical Faculty "Mihajlo Pupin" Zrenjanin
Djure Djakovica bb
23000 Zrenjanin
Serbia
dalibor.dobrilovic@tfzr.rs

ABSTRACT

Given the increasing use of wireless technologies in the Internet of Things and Wireless Sensor Networks, the issue of how these technologies can work together and be compatible becomes crucial. Wi-Fi and ZigBee technologies have established a strong foothold in the market and are widely used in various systems due to their extensive applications. It's vital to assess how one technology might impact another. This paper introduces a method using open-source hardware and software to evaluate how Wi-Fi affects ZigBee's performance. The testing setup is constructed using Arduino microcontroller boards. This document outlines the experiment, the setup, the approach, the tools for data collection and analysis, the insights from the experiments, and how these findings will shape future research. The findings in this paper provide a detailed understanding of the impact of IEEE 802.11 networks on the performance of IEEE 802.15.4 networks when operating within similar frequencies. The study shows that at a distance of about 12 meters, Wi-Fi can influence the performance of ZigBee, particularly when there is a frequency difference of 7 MHz or less.

Keywords: Wireless Sensor Networks, IoT, IEEE 802.11 Networks

1. Introduction

In the past decade, the Information and Communication Technology (ICT) systems have considerable changes in their appliance. The rapid and widespread development of wireless technologies influenced the creation of new environments and innovative ways of utilization of novel technologies. The growing appliance of wireless technologies leads to the creation of Wireless Sensor Networks (WSN) and the Internet of Things (IoT). These circumstances accompanied by the rapid growth in numbers of connected devices put in focus the question of various technologies' coexistence and interoperability, and make this question extremely important. The measurement of interference in the 2.4 GHz band is particularly important, because many technologies, such as

IEEE 802.11 (Wi-Fi), ZigBee, Bluetooth Low Energy (BLE), 6LoWPAN, and WirelessHART [1], operate in the 2.4 GHz band, as a part of Industrial, Scientific, Medical (ISM) band.

Wi-Fi and ZigBee technologies already have a long-lasting presence in the market, and due to their good performances are deployed in numerous systems. It is very likely that in the industrial, office, and even residential facilities, especially in indoor environments, these two technologies can operate side by side. That's why it is extremely important to measure how one technology impacts the performance of the other. So it is very interesting to build a low-cost portable platform for measuring the interference and to use it in various locations where these two networks coexist.

The methods for measuring the interference include the usage of specific equipment. This paper has presented the approach of using open-source hardware for measuring the interference effects of Wi-Fi to ZigBee. This paper describes the low-cost and easy-to-use experimental platform, methodology, and tools used for collecting and analyzing data, as well as the experience gained during the experiments, and their influence on future work. Considering that Arduino and open-hardware components are used for the platform, the platform is modular and easy to expand.

This paper is structured as follows. After the introduction, a brief reference of similar research in measuring and analyzing the interference is presented. Then, a brief overview of IEEE 802.11 and ZigBee technology is given, together with a brief description of other technologies operating in the same band as BLE and others. Next, the experiment and the devices and tools used for this experiment are described. After the experiment, the results are presented, followed by a discussion. At the end of the paper, the concluding remarks are given.

2. Related Work

One of the most popular standards used in wireless sensor networks for connectivity is ZigBee. It is one of the standards of communication protocols for low-data-rate short-range wireless networking which operates in 868MHz, 915 MHz, and 2.4GHz frequency bands with a maximum data rate of 250Kbits per second. This standard is focused on low energy consumption and because of this, it is targeted for battery-powered applications which required low data rate, low cost, and long battery life [2].

ZigBee is applicable in a variety of scenarios such as home and building automation, e-health and personal health care, smart energy, smart grid, smart industry, industrial asset management, etc. It is based on IEEE 802.15.4 standard, same as many other standards such as ISA100.11a, WirelessHART, 6LoWPAN, 802.15.4g Wi-SUN, etc. All of these standards are targeted for a variety of WSN applications. Some specific appliances of ZigBee technology can be in the industry for environmental and structural monitoring, teledosimetry in nuclear power plants, condition-based maintenance, etc.

In this section, the ZigBee and Wi-Fi technology basics, their mutual interference as well as the interference with other technologies, particularly with the BLE are presented.

2.1. ZigBee and Wi-Fi Technology Overview
The ZigBee is based on IEEE 802.15.4 standard [3]. This standard defines the operation of low-rate wireless personal area networks (LR-WPANs) at the physical (PHY) and media access control (MAC) layer. The standard dates back to 2003. It defines the use of 27 channels at the physical layer. The channels are numbered from 0 to 26. Channels operate in 868 MHz bands (channel 0), 915 MHz bands (channels 1–10), and 2.4 GHz bands (channels 11–26). In the 2.4 GHz band, channel spacing is 5 MHz and the center frequency of channel 11 is 2.405 GHz, and 2.480 GHz for channel 26 [1]. The ZigBee channel allocation is presented in figure 1a and figure 1b.

The other wireless technology which is in the focus of this paper is defined with IEEE 802.11 standard. This standard is part of the IEEE 802 set of Local Area Network (LAN) technical standards. It is designed for the specification of a physical layer (PHY) and medium access
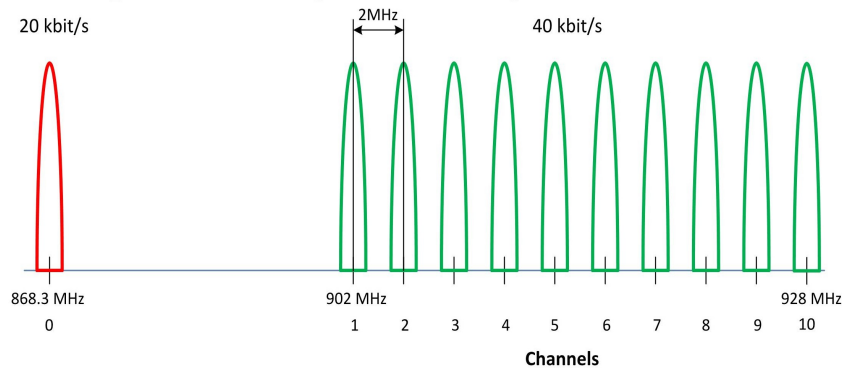
Figure 1a). ZigBee channels in 868 and 915 MHz band
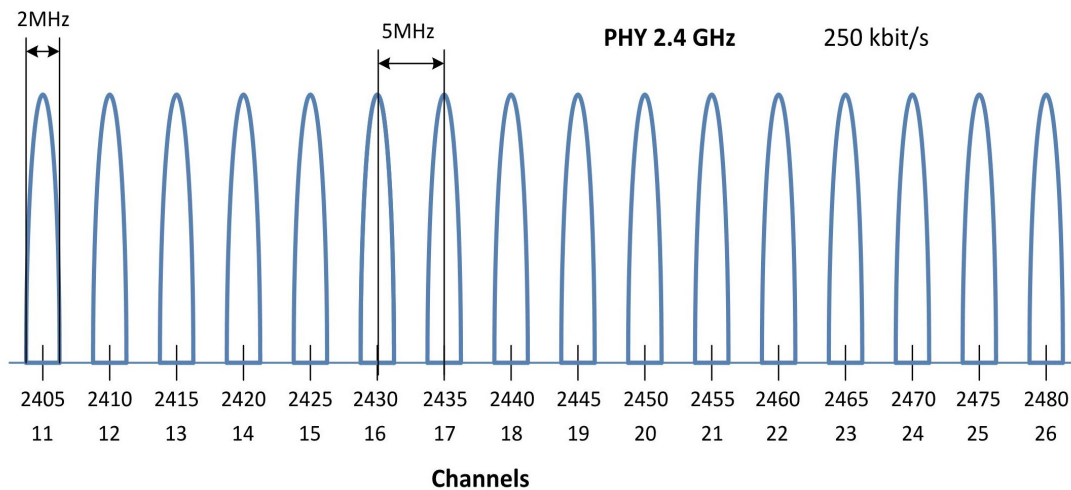
Figure 1b). ZigBee channels in 2.4 GHz band

control (MAC)protocols for Wireless Local Area Networks (WLAN). The standard has several amendments and it serves as a basis for wireless network products using the Wi-Fi of Wireless Fidelity product brands. IEEE 802.11 is designed for and used in consumer Internet applications, and for home and office appliances. Nowadays, the devices such as laptops, tablets, printers, smartphones, network access storage, and others have integrated Wi-Fi interfaces and use them for Internet and local network connectivity. [1]

The 802.11 family consists of a series of standards. The first standard 802.11-1997, was published in 1996. The first applicable wireless networking standard was 802.11b, then followed by 802.11a, 802.11g, 802.11n, and recently with 802.11ac [4], 802.11ah [5], and 802.11ax [6]. IEEE 802.11a standard uses a 5 GHz band and it is not in use nowadays. IEEE 802.11ah operates in the sub gigahertz band and IEEE 802.11ac in the 5 GHz band. The standards 802.11b, 802.11g, 802.11n, and partially 802.11ax use the 2.4 GHz ISM band. Here the interference with other standards operating in 2.4 GHz might occur. The majority of Wi-Fi networks are 802.11b/g/n. The IEEE 802.11 physical layer uses 14 channels in the 2.4 GHz range. Channels are spaced with 5 MHz between their central frequencies. The last channel (14) has 12 MHz spacing from channel 13. Channel 14 is only allowed in Japan, channels from 1 to 13 are allowed in the majority of countries including Europe, Asia, Africa, and South America. In North America channels 1 to 11 are allowed for usage. The IEEE 802.11 channels allocation in the 2.4 GHz band is presented in figure 2.
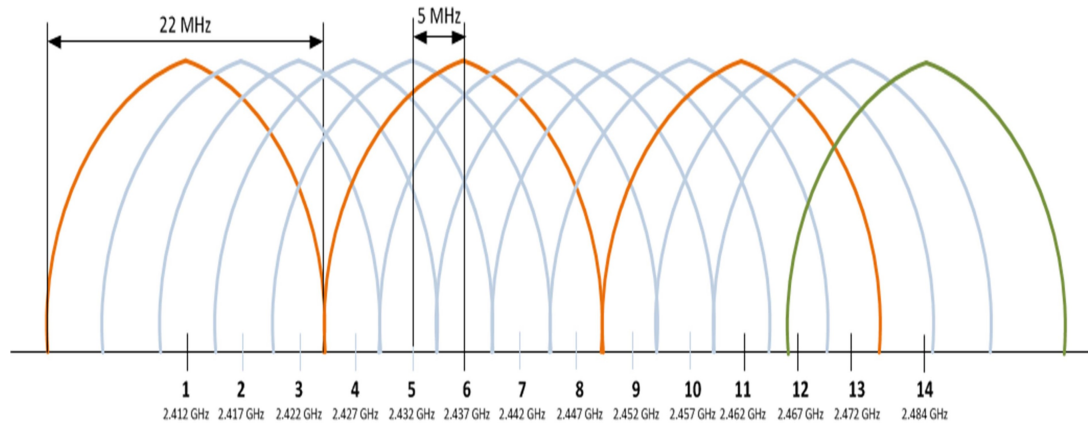
Figure 2. IEEE 802.11 channels frequency allocation in 2.4 GHz

2.2. Research on ZigBee and Wi-Fi coexistence

In paper [7] is presented evaluation and influence of ZigBee topology and coexistence between ZigBee and Wi-Fi network on quality of service performance. The two scenarios are simulated in [7]: the first scenario evaluates ZigBee network topology, and the second analyzes coexistence between ZigBee and Wi-Fi network. The results of this research show that the tree topology gives the highest throughput for the ZigBee network, while the mesh topology has the lowest throughput. The star topology (in wireless LAN) has the highest throughput, but when it is paired with ZigBee mesh topology it has the lowest HTTP page response time. The paper [7] also shows that the coexistence between Wi-Fi and ZigBee networks results in interference and decreased throughput in the ZigBee network.

The paper [8] shows that inter-technology interference can be detected by Wi-Fi devices for monitoring and calculating the statistics of receiver errors. This paper presents two methods for recognizing the source of interference based on Artificial Neural Networks and hidden Markov chains.

The paper [9] deals with a cooperative channel control method to improve the sink arrival rate of ZigBee packets allowing smaller degradation of Wi-Fi throughput in coexisting ZigBee and Wi-Fi networks. Also, this paper evaluates this method using evaluation criteria such as the satisfaction rate of ZigBee devices and Wi-Fi throughput.

In paper [10] is investigated Wi-Fi impact on Industrial IoT networks (SmartMesh IP), because both networks operate in the same 2.4 GHz frequency. The result of this research shows that with the very high Wi-Fi interference, and even when the latency and power consumption increase, the end-toend reliability of the network stays at 100%. The paper [10] shows that TSCH (Time Slotted Channel Hopping) technology at 2.4 GHz such as SmartMesh IP is suitable for an industrial environment where Wi-Fi is used.

The paper [11] presents an experimental investigation about interference between Wi-Fi and ZigBee networks and gives answers to the question of how to avoid this cross-interference between them. The results show that ZigBee channel switching and AP radio power adjusting are not effective ways to reduce the interference from Wi-Fi. Also, this paper gives a solution for this problem which is based on time-slot resource scheduling. This can help in the elimination of interference and guarantee network performance.

The paper [12] presents an analytical model to evaluate the performance of ZigBee under Wi-Fi interference in the practical smart home scenario. This model is based on the Markov chain and indoor path loss model. The analytical results of the simulation show that improvements in ZigBee network performance can be achieved with the reasonable deployment of Wi-Fi and ZigBee devices.

2.3. ZigBee and Bluetooth, and other technology coexistence

Together with the Wi-Fi, it is interesting to give an overview of the interference of ZigBee with other popular technologies. The Bluetooth and its newer variants are the most interesting because of their wide appliance. Bluetooth systems also operate in the 2.4 GHz ISM band. The Bluetooth uses the frequency hopping spread spectrum (FHSS).

Bluetooth until version 4.0 of standard uses 79 frequency channels separated by 1 MHz. The transmitted signal bandwidth is 1 MHz. The frequency of the channel is changed using a pseudorandom sequence with the maximum number of hops in Bluetooth of 1600 hops per second. The newer versions of Bluetooth, starting with version 4.0, e.g. Bluetooth Low
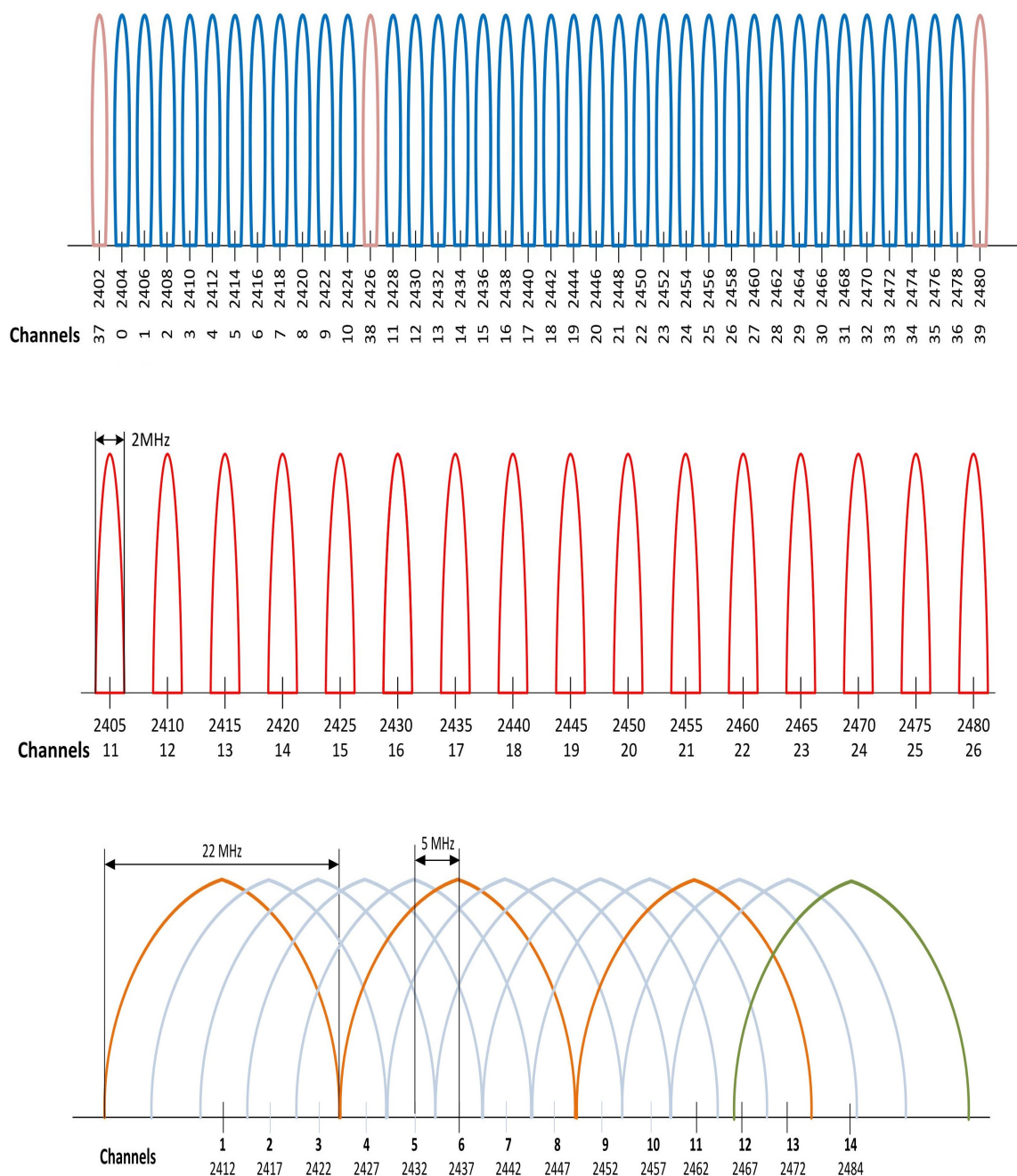
Figure 3. BLE, ZigBee, and Wi-Fi channel overlapping

Energy (BLE) also use the 2.4 GHz ISM band. BLE spectrum is divided into 40 channels, with 2 MHz channel spacing. 37 are data channels and 3 are advertising channels. The channel overlapping of ZigBee (IEEE 802.15.4), IEEE 802.11, and BLE in the 2.4 GHz band is presented in figure 3. [13]

Multiple papers have been published on the interference of Bluetooth and Wi-Fi networks and other devices using the 2.4 GHz ISM band. All of them evaluate different scenarios in the means of types and the number of interference sources.

The research [14] presents the results of the experiment in which ZigBee controlled robots remotely. The system was exposed to the combined effect of a WLAN, two Bluetooth piconets, and two microwave ovens. Measurements performed using a spectrum analyzer showed most interferences were caused by microwave ovens followed by WLAN. The experiment concluded that long delays in robot operation were caused by CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) used by ZigBee to determine channel availability during high interference.

Research published in [15] outlines the effect of Bluetooth on two types of network modes available in 802.15.4 standard: beaconed and non-beaconed. The evaluation was based on PER (Packet Error Rate). The tested scenario consisted of a single Bluetooth piconet and single 802.15.4 master-slave pair. The 802.15.4 devices were tested with a distance of 1 through 10 meters while the Bluetooth piconet was 1m away from the 802.15.4 end device. Results showed that PER in nonbeaconed mode was consistently higher than in beaconed mode, but non-beaconed mode exhibited a lower increase due to interference than beaconed mode. The effect of interference significantly diminished after 3m marks.

Papers [16, 17] discuss the performance of the ZigBee network under the interference of multiple Bluetooth and WLAN networks. Analysis was performed with simulation. The simulation was based on a mathematical model for calculating PER based on the number of interfering networks. Results from [16] align with [15] that the effect of a single Bluetooth piconet is greatly reduced after 3m. When multiple piconets are preset, PER is below 10-4 only when the number of piconets is less than 8 and the distance is 4m or greater. Simulations performed in [17] show the combined effect of WLAN and Bluetooth on ZigBee. With one WLAN and up to 20 Bluetooth piconets, PER is in the acceptable range when the distance from WLAN is more than 7 meters and more than 3 from Bluetooth. If more than one WLAN is present, PER will remain high even it is above 10 meters distance. This behavior is attributed to the high transmission power of WLAN networks compared to ZigBee.

The implementation of BLE technology in the testing platform presented in this paper is not supported yet. But considering the level of BLE utilization, it is in a plan for future expansion and will be included in future work.

3. Experiment

In the presented related work variety of experimental platforms are used. ZigBee and Wi-Fi interference is analyzed in [7] using OPNET Modeler simulation software with two scenarios. In [8], ZigBee, LTE-U, or microwave oven interference is investigated using commodity Wi-Fi cards. The interference analyses are performed using QualNet 7.1 simulation software for improving ZigBee packet arrival rate by controlling both the Wi-Fi and ZigBee channels in [9]. The focus of the research presented in [10] is ZigBee/Wi-Fi interference in Industrial IoT networks. In the experiment, one DC2274 SmartMesh IP manager and 47 DC9025 SmartMesh IP motes are used. For research presented in [11] the designed heterogeneous gateway that integrates Wi-Fi and ZigBee, called WiZi gateway is deployed. Research [12] deals with ZigBee/Wi-Fi interference Smart Home environments. In this paper is proposed an analytical model and usage of the OPNET simulation tool. Finally, research [13] examines the interference of ZigBee/Wi-Fi in robot cars where two different wirelessly remote-controlled systems are used. For measurement, Rohde Schwarz FSH6 (model .26) Handheld Spectrum Analyzer (100 kHz - 6 GHz) with an Empfanger receiver, made for measuring signals between 5003000 MHz bands, is used.

Researches [15-17] investigate Bluetooth and Wi-Fi interference primarily. In [15] the IEEE 802.15.4 motes are Jennic Sensor Board JN5121. For Bluetooth devices, one laptop computer with USB Bluetooth (v1.1 0dBm class 3) adapter is employed as Master and one cellular phone with Bluetooth interface as Slave. For monitoring, the Chipcon evaluation board CC2420EB is used in combination with the Chipcon Packet Sniffer software. In [16] ZigBee performance under interferences of Multiple Bluetooth Piconets is analyzed using OPNET simulation software. In [17] ZigBee performance under WLAN and multiple Bluetooth piconets interferences are examined with the simulator.

The experiment performed in this study is based on open-source hardware and software components, freeware software tools, and scripts developed for data processing. Besides its low cost compared to the presented solutions, this platform is very scalable and easy to deploy in different scenarios. Its scalability comes from Arduino UNO modularity and the possibility of connecting multiple communication modules such as Wi-Fi, Bluetooth, BLE, LoRa, LoRaWAN, SigFox, etc, Considering the low costs of Arduino components and the wide supporting community (forums, example codes, wiring schemes, etc,) it is possible to design multiple prototype devices in a short time and to deploy them at the places where the system should be implemented. In this section hardware and software components used for measurement, experiment setup, and methodology are explained.

3.1. Measurement Hardware and Software
The platform for data collection in this experiment consists of several hardware and software components. It is built on an Arduino UNO Rev3 microcontroller unit and XBee communication modules supporting ZigBee technology. Arduino UNO Rev3 is very frequently used in academic environments as a low-cost, reliable, and scalable platform for testing, researching, and prototyping. The configuration used in this experiment is presented in table 1. The platform is used in past research with positive experiences [18, 19]. The two XB modules integrated with Arduino UNO Rev3 were used in the experiment, one as a transmitter (Tx), and one as a receiver (Rx).

No.	Component	Description
1	Arduino UNO Rev3	Microcontroller unit
2	XBee Shield	Expansion module
3	XBee ZB module with RP-SMA connector	ZigBee Communication module
4	2.4 GHz Antenna 3 dBi	External Antenna

Table 1. Configuration of the test device based on Arduino

The Tx microcontroller unit presented in table 1 has the role of ZigBee remote node, It is configured as a ZigBee router in AT command mode. The receiver (Rx) is based on the same platform but configured as a ZigBee coordinator. The PAN ID is set to 1001 (manually defined unique ZigBee Personal Area Network identifier) and communication channels are set to 11, 13, 15, 17, 19, 21, 23, 25, and 26 for each test run respectively. The main function of the Arduino UNO devices is to simulate wireless nodes and to generate traffic. Following the experience with previous experiments, the duration of the test run is set to about 20.000 packets with an interval of 100ms between each packet. So 20,000 packets are sent from Arduino in each test run, from XBee router (Tx) to XBee coordinator (Rx). A simple program for accepting the data packet is written for this experiment. The IEEE 802.15.4 traffic analyses are made with the use of Texas Instruments SmartRFTM Packet Sniffer [20]. It is a free software application for monitoring, displaying, and capturing radio packets of IEEE 802.15.4 and other technologies such as ZigBee, BLE, RF4CE, and SimpliciTI. The packets are captured,

decoded, displayed, and later logged by Packets Sniffer in binary file format. In this experiment is used TI CC2351 USB Dongle for ZigBee Traffic capturing and all captured traffic is saved in SmartRFTM Packet Sniffer as PSD file format. The PSD file format is described in the Texas Instruments Web site and the SmartRFTM Sniffer documentation [18]. In brief, this format stores captured packets byte by byte in a format compatible with the ZigBee frame format, and both formats are stored in the same file. Every packet is saved as a sequence of 151 bytes, if the packet is shorter than 151 bytes, the rest of the bytes will have the value 0. The script for further processing of PSD files is created for the creation of statistical data.

For measuring the Wi-Fi signal, the Vistumbler [21] free software is installed. It is used in combination with TP-Link 722N USB wireless adapter with an external antenna with 5dBi gain. The Vistumbler is used to collect data of active Wi-Fi access points in the nearby areas. The most valuable access point data are the channel of the AP and its signal strength. The collected data are presented in table 5.

3.2. Experiment Setup

The experiment is performed in a relatively large indoor space (amphitheater). Besides the ZigBee Tx (Arduino UNO XBee module) and Rx nodes (same configuration), a Wi-Fi access point is used. The distance between Rx and Tx nodes was about 15m, the distance between Tx and AP was 6.5m, and the distance between Tx and AP was about 11m. The distance of AP1 from Rx is about 8.2m, and from Tx is about 21m. The location of AP and AP1 are fixed and those nodes are an integral part of institutional LAN. The locations of Rx and Tx are chosen randomly at the positions where the interference can be expected from both Wi-Fi access points (AP and AP1) equally. The AP, because of its position in the same room where the Rx and Tx are is planned as the primary interfering node, while the AP1 is chosen as a secondary interfering node. The deployment of the nodes is presented in figure 4.

To reduce the time needed for the test, only odd channels are used (11, 13, 15, 17, 19, 21, 23, and 25), and last channel 26, because it is completely out of the Wi-Fi channel frequency. Each test run is made by sending around ZigBee 20.000 packets. The laptop for capturing ZigBee packets with SmartRF^{TM} Packet Sniffer and Wi-Fi data with Vistumbler is placed near the Rx location (figure 4).

The indoor space used in this test can be considered a suitable environment for such experiments. It combines the indoor environment, with the larger open space. In the amphitheater, the furniture is made of seats and desks of about the same height. Except for the walls, there are no other obstacles in the room. Considering all these environments completely differs from the environments used in related researches.
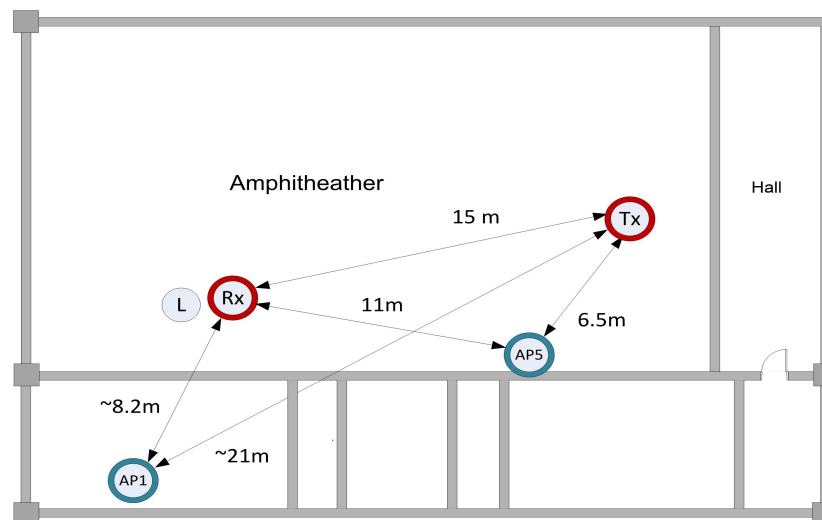

Figure 4. The deployment of devices in the experiment

4. Results

The results of 9 test runs (one run per channel) are given in table 2. This table shows the number of ZigBee channels for each test run, the central frequency of the ZigBee channel, the overlapping Wi-Fi channel, the central frequency of overlapping Wi-Fi channel, the frequency range of the Wi-Fi channel, number of the packets sent, and the number of packets with errors. The number of errors is the lowest for ZigBee channel 26, which is completely out of Wi-Fi overlapping frequencies, and the highest number of packet errors is for ZigBee channel 15, which overlaps with Wi-Fi channel 4.

Channel	Frequency	Overlapping	Central Frequency	Frequency Range (MHz)	Packs. Sent	No. of Errors
11	2405	1	2412	2401–2423	20271	123
13	2415	2	2417	2406–2428	21689	125
15	2425	4	2427	2416–2438	20576	194
17	2435	6	2437	2426–2448	20414	122
19	2445	8	2447	2436–2458	20187	113
21	2455	10	2457	2446–2468	20350	148
23	2465	12	2467	2456–2478	21689	131
25	2475	-	-	-	20331	103
26	2480	-	-	-	20254	56

Table 2. Test run data by ZigBee channel in comparison with Wi-Fi channels

The measurement results, obtained with TI SmartRF^{TM} Packet Sniffer are shown in table 3. The presented data are as follows: ZigBee channel, average Received Signal Strength Indicator (RSSI) per test run (one per channel), RSSI standard deviation, the maximum value of RSSI, the minimum value of RSSI, and throughput in Kbytes. The valuable parameter for this research is throughput. The comparison of the average RSSI with the results of the measurements from the similar researches in the other related works is not compared, because it is a complex task and to large extent, it depends on the parameters such as indoor environment, wall configuration, furniture deployment, antenna gain, output power, data availability and many more. Taking these parameters into consideration will require extensive research and should be in the focus of completely separated research.

The lowest throughput is measured for the ZigBee channel 21 (0.68 Kbytes), and then channel 23 (1.27 Kbytes) both overlapping with Wi-Fi channel 11. The next lowest throughput is for ZigBee channels 15 and 13 (1.59 and 1.65 Kbytes respectively) because of overlapping with Wi-Fi channel 4. Other channels have similar throughput ranging from 1.74 to 1.81 Kbytes.

Channel	RSSI Avg.	RSSI Std. Dev.	RSSI Max.	RSSI Min.	Throughput (KBytes)
11	-64.79	2.208709	-61	-85	1.77
13	-65.46	2.365181	-60	-73	1.65
15	-69.2	1.775225	-66	-75	1.59
17	-65.68	1.284681	-62	-68	1.81
19	-73.53	6.337532	-64	-87	1.81
21	-72.67	4.25302	-60	-97	0.68
23	-63.83	1.487328	-60	-69	1.27
25	-64.36	1.558356	-61	-68	1.74
26	-61.01	1.020621	-59	-65	1.77

Table 3. Test run data by ZigBee channel with RSSI and throughput

The additional data for each test run by the ZigBee channel is given in table 4 where the total bytes transferred, the number of disconnections from the network, and test time in minutes are given. A significant number of disconnections is only detected at ZigBee channel 21 (a total of 14) where the Wi-Fi interference is the strongest.

| ZigBee Channel	Total Bytes Transferred	No. of Disconnection	Test Time
11	902,576	0	8.29
13	979,676	0	9.67
15	905,392	0	9.26
17	916,310	1	8.22
19	900,313	0	8.11
21	900,372	14	21.64
23	979,157	4	12.54
25	910,840	0	8.51
26	909,131	0	8.37

Table 4. Additional test run data by ZigBee channel with No. of disconnections and test time

The data for IEEE 802.11 access points are presented in table 5. The AP ID5 has the strongest signal, and this is the AP located in the same amphitheater where the experiment took place at a distance of 6.5m from Tx, and 11m from Rx. The next strongest signal was from AP ID1, at Wi-Fi channel 4, which is located at a distance of 8.2m from the laptop and RX station and about 21 m from Tx in the room separated with walls from the amphitheater. The table contains data such as AP ID, operating channel, average RSSI, RSSI standard deviation, the maximal value of RSSI, and the minimal value of RSSI in decibels. The data are cumulative for all test runs.

AP ID	Channel ID	RSSI Avg.	RSSI Std. Dev.	RSSI Max.	RSSI Min.
1	4	-61.89	16.24607	-42	-95
2	1	-86.08	4.482173	-75	-92
3	1	-86.45	7.45686	-76	-92
4	1	-85.18	5.344492	-64	-95
5	11	-46.85	6.005166	-32	-68
6	1	-85.63	5.254699	-74	-95
7	6	-80.19	6.760392	-10	-95
8	11	-79.52	7.2724	-57	-95
9	2	-87.31	8.775867	-66	-95
10	6	-80.66	5.680779	-10	-95
11	11	-80.73	6.020162	-69	-95
12	11	-80.78	6.198567	-68	-95
13	3	-86.78	4.646646	-76	-95
14	1	-84.25	5.929563	-69	-95
15	1	-87.44	6.644916	-74	-95
16	6	-80.31	7.971245	-70	-88
17	64	-83.4	8.793518	-76	-90
18	9	-85.16	8.021899	-73	-95
19	11	-81.38	8.951728	-70	-89

Table 5. Measurement information by ZigBee channel

The visual presentation of ZigBee channel throughput is shown in figure 5. The throughput is the lowest for channels 21 and 23 respectively, and next for channels 13 and 15 respectively. Again, channels 21 and 23 are closest to the AP ID5 with the strongest RSSI (average value -46.85dB). Channels 13 and 15 are closest by frequency to the AP ID1 with an average RSSI -61.89 dB. According to these test results, Wi-Fi at a distance of about 12m can result in a decreased ZigBee throughput when the central frequency difference is equal to or lower than 7 MHz.

Channel 11

Channel 13

Channel 15

Channel 17

Channel 19

Channel 21

Channel 23

Channel 25
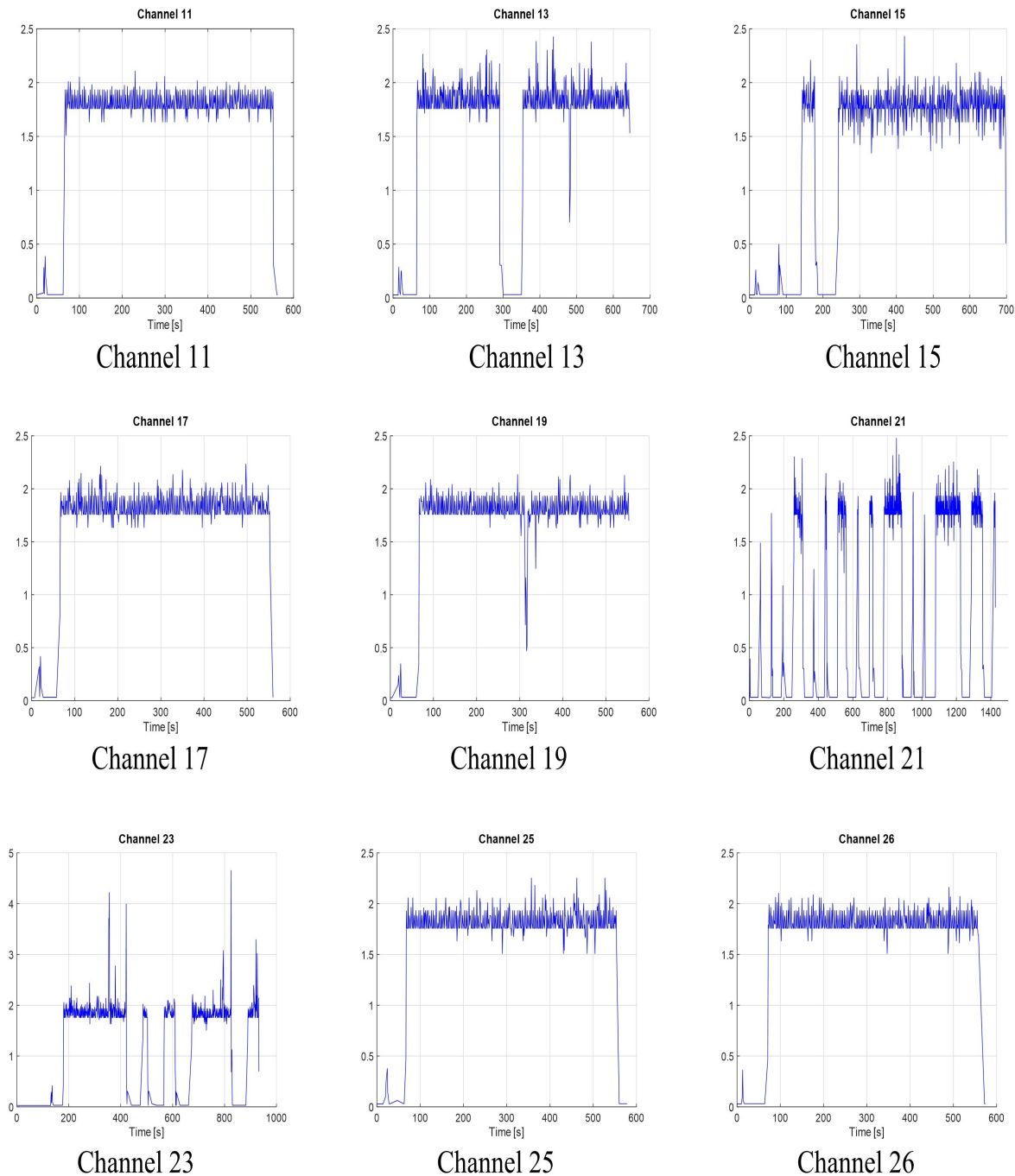
Channel 26

Figure 5. Test run throughput by ZigBee channel

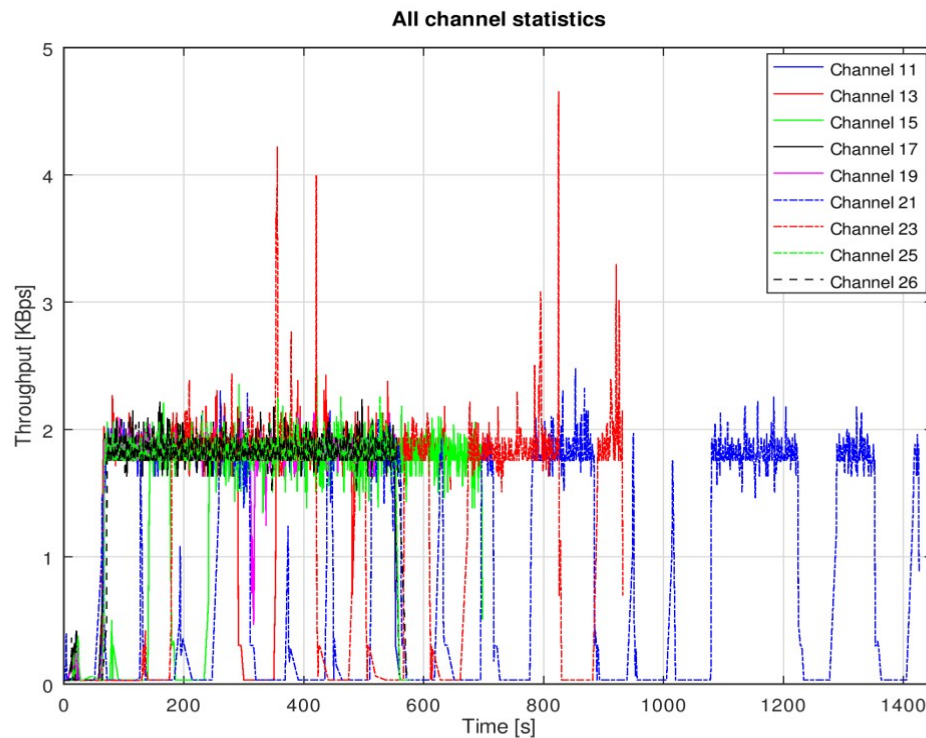The cumulative throughput for all channels is given in figure 6.

Figure 6. Comparison of throughput of all ZigBee channels

5. Conclusion

This paper targets the important issue of ZigBee and Wi-Fi interference. The importance of this issue rises with the growing importance and implementation of systems such as wireless sensor networks and the Internet of Things. In those systems, ZigBee and Wi-Fi are used frequently. In tackling this problem, this paper evaluates the usability of open-source hardware, and software components to build a low-cost and effective platform for measuring interference.

Besides its low cost comparing to the presented solutions, the platform presented in this paper is very scalable and easy to deploy in different scenarios. Its scalability comes from Arduino UNO modularity and the possibility of connecting multiple communication modules. Considering the utilization of low-cost components and Arduino wide supporting community it is possible to generate multiple prototype devices in a short time and to deploy them at the places where the designed systems are going to be implemented. The platform proved itself to be effective, and the results of the conducted experiments detect the effects of Wi-Fi interfering with the existing ZigBee networks. The testing platform collected data for detailed analyses, giving the information of the IEEE 802.15.4 network performance. Channel 21 operating in 2,455 MHz has the lowest average throughput of 0.68 Kbytes and the highest number of disconnections (14). Channel 23 operating in 2,465 MHz has the next lowest throughput of 1.27 Kbytes and a lower number of disconnections (4). With these test results, it is shown that when Wi-Fi is deployed at the distance of about 12m it can significantly affect the ZigBee throughput when the central frequency difference is equal to or lower than 7MHz. The recommendation for the deployment of ZigBee devices in proximity of Wi-Fi networks is to avoid overlapping channels when it is possible. In case when such avoidance is not possible the difference between the central frequencies of two networks should be greater than 7 MHz.

Considering the open-source ch aracteristic of the platform, its scalability, and the availability of the components, the platform should be easily adapted. The plan for future work is an integration of additional interfering technologies, such as BLE. The other direction of the research can be focused on using multiple interfering devices and the creation of complex testing environments with a high level of control of factors with the influence to the interference, and with the controlled intensity of traffic.

Acknowledgment

References

[1] Wilamowski, B. M., Irwin, J. D. (2016). *Industrial communication systems*. CRC Press.

[2] Farahani, S. (2008). ZigBee wireless networks and transceivers. Newnes. https://doi.org/10.1016/B978-0-7506-8393-7.00008-X

[3] IEEE. (2006). IEEE 802.15.4-2006 – IEEE standard for information technology – Local and metropolitan area networks – Specific requirements – Part 15.4: *Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (WPANs)*.

[4] IEEE. (2013). IEEE standard for information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications – Amendment 4: Enhancements for very high throughput for operation in bands below 6 GHz (IEEE Std 802.11ac(TM)–2013). https://doi.org/10.1109/IEEESTD.2013.7797535

[5] IEEE. (2017). IEEE standard for information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications – Amendment 2: Sub 1 GHz license exempt operation (IEEE Std 802.11ah–2016). https://doi.org/10.1109/IEEESTD.2017.7920364

[6] IEEE. (2021). IEEE 802.11ax – 2021 – IEEE approved draft standard for information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications – Amendment 1: Enhancements for high efficiency WLAN.

[7] Arif, S., Supangkat, S. H. (2014). Simulation and analysis of ZigBee – WiFi interference. In Proceedings of the 2014 International Conference on ICT for Smart Society (ICISS) (pp. 206-210). https://doi.org/10.1109/ICTSS.2014.7013174

[8] Croce, D., Garlisi, D., Giuliano, F., Tinnirello, I. (2014). Learning from errors: Detecting ZigBee interference in WiFi networks. In Proceedings of the 2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET) (pp. 158-163). https://doi.org/10.1109/MedHocNet.2014.6849119

[9] Nishikori, S., Kinoshita, K., Tanigawa, Y., Tode, H., Watanabe, T. (2017). A cooperative channel control method of ZigBee and WiFi for IoT services. In Proceedings of the 14th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-6). https://doi.org/10.1109/CCNC.2017.7983071

[10] Rincon, F., Tanaka, Y., Watteyne, T. (2018). On the impact of WiFi on 2.4 GHz industrial IoT networks. In Proceedings of the 2018 IEEE International Conference on Industrial Internet (ICII) (pp. 33-39). https://doi.org/10.1109/ICII.2018.00012

[11] Wang, X., Yang, K. (2017). A real–life experimental investigation of cross interference between WiFi and ZigBee in indoor environment. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 598-603). https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.94

[12] Jiang, H., Liu, B., Chen, C. W. (2017). Performance analysis for ZigBee under WiFi interference in smart home. In Proceedings of the 2017 IEEE International Conference on Communications (ICC) (pp. 1-6). https://doi.org/10.1109/ICC.2017.7997161

[13] Liberg, O., Sundberg, M., Wang, Y.-P. E., Bergman, J., Sachs, J. (Eds.). (2018). Chapter 9 – The competitive Internet of Things technology landscape. In Cellular Internet of Things (pp. 327-360). Academic Press. https://doi.org/10.1016/B978-0-12-812458-1.00009-5

[14] Suhonen, J., Haataja, K., Paivinen, N., Toivanen, P. (2008). The effect of interference in the operation of ZigBee and Bluetooth robot cars. In Proceedings of the 2008 4th IEEE/IFIP International Conference on Central Asia on Internet. https://doi.org/10.1109/canet.2008.4655307

[15] Herrera, M. M., Bonastre, A., Capella, J. V. (2008). Performance study of non-beaconed and beacon-enabled modes in IEEE 802.15.4 under Bluetooth interference. In Proceedings of the 2008 The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (pp. 144-149). https://doi.org/10.1109/UBICOMM.2008.22

[16] Shin, S. Y., Kang, J. S., Park, H. S. (2009). Packet error rate analysis of ZigBee under interferences of multiple Bluetooth piconets. In Proceedings of VTC Spring 2009 – IEEE 69th Vehicular Technology Conference (pp. 1-5). https://doi.org/10.1109/VETECS.2009.5073765

[17] Fang, F., Sun, J., Han, Y., Zhu, H. (2012). Performance analysis of ZigBee under WLAN and multiple Bluetooth piconets interferences. In Proceedings of the IET International Conference on Information Science and Control Engineering 2012 (ICISCE 2012) (pp. 1-7). https://doi.org/10.1049/cp.2012.2357

[18] Dobrilovic, D., Stojanov, Z., Brtka, V., Èoviæ, Z., Bilinac, N. (2014). Software application for analyzing ZigBee network performance in university courses. In Proceedings of the 2014 IEEE 12th International Symposium on Intelligent Systems and Informatics (SISY) (pp. 73-77). https://doi.org/10.1109/SISY.2014.6923560

[19] Dobrilovic, D., Odadzic, B., Stojanov, Z., Sinik, V. (2014). Testing ZigBee RF module applicability for usage in temperature monitoring systems. In Proceedings of the 2014 22nd Telecommunications Forum Telfor (TELFOR) (pp. 415-418). https://doi.org/10.1109/TELFOR.2014.7034436

[20] Texas Instruments Incorporated. (2010). SmartRF™ Packet Sniffer user manual.

[21] Vistumbler. (n.d.). Open source WiFi scanner and channel scanner. Retrieved April 2021 from https://www.vistumbler.net/