**Special Issue for International Conference of Advanced Materials Engineering and Technology (ICAMET 2013), 28-29 November 2013, Bandung Indonesia**

**Advances in Environmental Biology**, 7(12) October Special Issue 2013, Pages: 3775-3782

# Integration and Deployment of IEEE 802.15.4 Wireless Sensor Networks with a Wireless Mesh Backhaul Network

**M.N. Hassan, L.M. Kamarudin, A.Zakaria, RB Ahmad**

*School of Computer and Communication Engineering University Malaysia Perlis*

ARTICLE INFO

***Article history:***
*Received 11 September 2013*
*Received in revised form 21 November 2013*
*Accepted 25 November 2013*
*Available online 3 December 2013*

***Key words:***
*Wireless Sensor Networks, IEE802.15.4, WLAN, WMN, IEEE802.11g, , Zigbee, MICAz motes, Pervasive Computing.*

ABSTRACT

This paper describes the deployment of a IEEE802.15.4 Wireless Sensor Network (WSN) in a campus network and integration with IEEE 802.11a/g Wireless Mesh Network (WMN) for the backhaul. The first problem discussed is the integration of the WSN with the WMN. This research utilises the Motorola IAP4300 – Intelligent Access Point for its WMN backhaul communication and the Crossbow MIB600 Ethernet gateway and MPR2400-MICAz for the WSN. Secondly it explores the issue of coexistence between IEE802.11g and IEEE802.15.4 that is utilising the same industrial, scientific and medical (ISM) radio band of 2.4GHz. This paper describes our deployment and integration experience and provides results which will be of interest to industry and research professionals.

## INTRODUCTION

Numerous deployments of wireless sensor networks (WSNs) for applications such as environmental monitoring have been published in recent years. One challenge using the WSN for this particular application is the short range of the sensor nodes. One option is to use a Wireless Mesh Network (WMN) as the backhaul for transporting the data to a central server. The integration of the WSN with the WMN expands the communication range and allows mobility of the devices. WSN's can be used for forming the underlying sensing and network infrastructure in pervasive computing environments.

The difficulty of deploying a Wireless Sensor Network (WSN) is a problem which should not be overlooked, argues the analysis at Cantab Wireless Ltd., Cambridge, UK [1]. For example in this research we found that the Crossbow MIB600 Ethernet gateway used as a sink for the MPR2400-MICAz motes could not be connected directly to the Motorola IAP4300-802.11a/g WMN campus backhaul. The aim of this research is then focused on the coexistence issues of IEEE802.11g and IEEE802.15.4 that are operating on the same ISM 2.4Ghz radio band. The research conducted in [2] concluded that despite its low transmit power and simple modulation technique, IEEE 802.15.4 shows a robust behaviour against interference of other 2.4 GHz systems and even in the worst case conditions for frequency overlap, local distance and high traffic load for interference, some time slots remain for a successful transmission of IEEE 802.15.4 traffic. In [3] & [4] the impact of coexistence of these ISM bands are evaluated analytically and by using simulation.

In this paper, experiments are conducted where the number of packet drops and packet retries are monitored and experimentally analyzed under a realistic network load environment and involving a scenario where the WSN was under interference of a WLAN. Following on from these experiments the throughput has been measured for the WLAN under the interference of the WSN. The experiments will provide useful information and guidance for network engineers and service providers. The impact of coexistence on the network performance is demonstrated through this series of experiments and should help network engineers better understand the process of network performance and inherent optimisation of service provision. For future work, our research will embark on a simulation study on the impact of coexistence on both networks by introducing coexistence model of IEEE 802.15.4 and IEEE 802.11g to expose the interactive behaviour between these two

**Corresponding Author:** MN Hassan, L.M., School of Computer and Communication Engineering Universiti MalaysiaPerlis
E-mail: najmuddin@unimap.edu.my

standards. A comparison between the deployed testbed and simulation can then deduce and more accurately explain their coexistence performance under a wider range of network conditions.

*WSN Background:*

It is observed that the widespread use of WSNs has been slowed down by the immaturity of the WSN industry. This analysis was concluded in a report; "Over 1 billion wireless sensors to be sold in 2014" [1]. It also suggests that WSNs are often proprietary systems, which are not compatible with each other and cannot exchange data. It will also require considerable expertise to deploy and operate a WSN. The difficulty of designing and installing a WSN is a serious problem which should not be overlooked. Simple wireless sensor nodes may soon cost only $10 or so, but designing, deploying, testing, and calibrating the network may easily cost more than the cost of the WSN hardware. This situation has to change before the WSN business can truly take off. Massachuset Institute of Technology (MIT) Technology Review lists sensor networks as one of "Ten emerging Technologies that will Change the World" [5]. With the development of wireless communication technology, the combination of wireless communication and data acquisition becomes a new trend of networked acquisition systems. Among these kinds of wireless technology, WSN has attracted a lot of interest and visibility due to its huge application space. WSNs are a form of wireless ad-hoc network which connect embedded sensors, actuators, processors and in which each node consists of a wireless communication device. It allows rapid deployment, flexible installation, fully mobile operation and prevents the cable wear and tear problem. WSN will play an increasingly important role in constructing complex industrial data acquisition systems.

WSNs can be used for forming the underlying sensing and network infrastructure in pervasive computing environments. A WSN consists of a collection of sensor nodes and a sink node connected through wireless channels, and can be used for building distributed systems for data collection and processing, covering the functions of on-field signal sensing and processing, network data aggregation and self organized wireless communication [6].

However sensor networks have severe resource constraints. An example of a commercially available sensor is the Crossbow MICAz mote utilising ISM band 2.400MHz – 2.385MHz, 16 Channels, Chipcon CC2420 Direct-Sequence Spread Spectrum (DSSS) RF transceiver, IEEE 802.15.4, Zigbee Alliance compliant, [7] that features slow under-powered Atmega 1281 micro-controller with 4KB of RAM, 512KB of program memory, an AES cryptographic hardware module, and runs the (micro) operating system TinyOS. Sensors like this one can be used to build large sensor networks for a variety of applications in different areas including indoor and outdoor environmental surveillance, habitat monitoring, seismic and structural monitoring, intelligent building, power monitoring, health monitoring, intelligent transportation, object tracking, precision agriculture, factory and process automations, military systems etc. They can also be used to provide relay network to facilitate rescue operations in wide open hostile areas, to fulfil perimeter surveillance duties, to operate in severe environmentally constrained scenarios for commercial purposes, for instance, to measure the concentration of metal such as nodules of manganese in the ocean bed [8].

Although their limited size makes them attractive for use in a number of situations, at the same time their size affects resources such as the energy, computational power, and storage available. Other challenges and limitations are the error-prone wireless medium. Since sensor networks can be deployed in different situations, the requirements of each different application may vary significantly. Researchers must take into consideration that the wireless medium can be greatly affected by noisy environments, and thus the signal attenuates in regard to the noise. Note that an adversary can intentionally interfere and cause enough noise to affect the communication. In an environment such as healthcare, it is vital to ensure that communication is on time to respond to emergencies. Fault tolerance and adaptability are other attributes which are important in providing a robust WSN. If a sensor node fails due to a technical problem or deletion of its battery, the rest of the network must continue its operation without a problem. Researchers must design adaptable protocols so that new links are established in case of node failure or link congestion. Furthermore, appropriate mechanisms should be designed to update topology information immediately after the environment changes so as to minimize unnecessary power consumption.

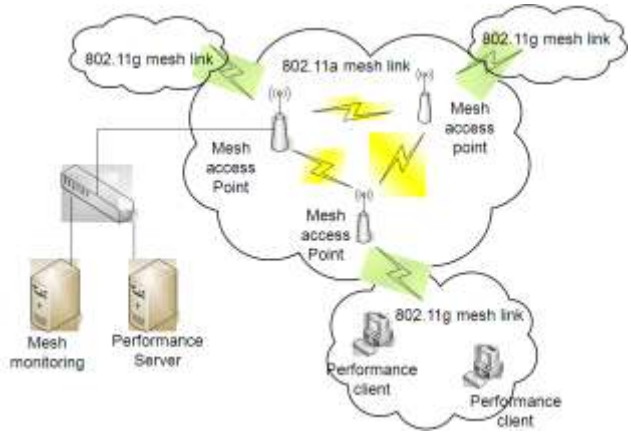


**Fig. 1:** WMN connection setup for the Motorola IAP-4300

The Motorola Intelligent Access Point (IAP)-4300 used in the backhaul network is available either in a single radio configuration with a 2.4 GHz WiFi radio (802.11b/g) or in a two radio configuration with an additional 5.8, 5.4 or 4.9 GHz (802.11a) radio. In a single radio configuration, the 2.4 GHz radio is used for both client access and node-to-node mesh links. In the two radio configuration, the 5.8 or 5.4 GHz radio is dedicated for node-to-node mesh traffic, while the 4.9 GHz radio is used for client access. Additionally, the 5.8 or 5.4 GHz radio can be configured to provide client access using the 802.11a standard [9]. In our campus network the IAP-4300 has been configured to form a two radio configuration WMN backhaul as shown in figure 1. In this configuration Wi-Fi service can be delivered in the 802.11g 2.4GHz band while data backhaul is accomplished in the 802.11a 5.4GHz band. This eliminates the interference and capacity limitations of using the same band for both service and backhaul. Similar work was being carried out in [10] however using different device for WSN and WMN backhaul. The test was using Cisco 1510 802.11b/g outdoor mesh access points, an Emerson 1420 wireless gateway attached to a Cisco 1510 mesh access point, and a mixture of eight Emerson Smart Wireless 802.15.4 field devices.

*WSN deployment and Integration with WMN:*

The MPR2400CA-MICAz (figure 2) motes were used as the primary nodes for transmission or retransmission (multi-hop) of data to the MIB600 Ethernet gateway or also known as a sink. The capability of MICAz motes to allow Over the Air Programming (OTAP) is an added advantage of WSN flexibility and wide range application. We utilised the MIB600 Ethernet (figure 3) as the network gateway as it provides Ethernet (10/100 Base-T) connectivity for communication and has the capability for an in-system programming of the motes. The MIB600 Ethernet gateway is embedded with UDS-10/Cobox 5.x Ethernet module by Lantronix®, Inc. USA. The Ethernet module used a method called serial tunneling, whereby the UDS-10 encapsulates the serial data into packets and transports it over Ethernet. From our investigation, in order for the Crossbow gateway to operate the baud rate needs to be set at 115200bps for channel 1 and 57600bps for channel 2 with the right corresponding Port number. Channel 1 is used for communication and is accessible through Port number 10002 and Channel 2 is for programming the ISP Micro Controller through Port number 10001. It is also noted that programming the MIB600 directly via a PC through channel 2 requires a 10/100 base-T crossover UTP connection. By using the MIB600 Ethernet gateway, allows the integration with other wired networks or with IEEE 802.11b/g wireless networks for expansion. In this research the WSN was connected to the Motorola IAP-4300 IEEE 802.11a/g WMN as a backhaul. MTS310CA (figure 4) was used as the external sensor transducer. It was designed as a general measurement platform for the integration with the motes. The MTS310CA is equiped with light, temperature, microphone, buzzer, 2-axis accelerometer, and 2-axis magnetometer. Figure 5 illustrates the end-to-end application block diagram.

**Fig. 2:** MPR2400CA-MICAz mote

**Fig. 3:** MIB600 Ethernet Gateway

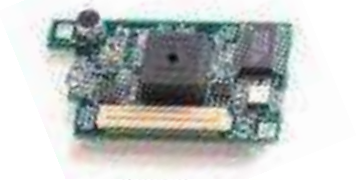

**Fig. 4:** MTS310CA sensorboard


**Fig. 5:** End-to-end application block diagram

*Coexistence on 2.4Ghz:*

The IEEE 802.11g WLAN and IEE802.15.4 WSN are operating on the same ISM frequency allocation of 2.4 GHz; hence the issue of coexistence arises. Figure 6 shows the RF channel spectrum of IEE802.15.4 against IEEE802.11g. WLAN channels are wider in frequency than WSN. This means that WLAN occupies more RF spectrum per channel than WSN. Furthermore WLAN transmit power at a maximum 20dBm (100mW) to insure compliance to regulatory domain power limits regulatory and WSN max power transmission at 0dBm (1mW). Table 1 shows the correlation between channel and frequency allocation of the IEEE 802.15.4 WSN. To gauge the interference level, experiments were carried out to ensure the interoperability of WSN and WLAN in close proximity in an outdoor environment. The experiments were carried out to gauge the percentage packets dropped and retries by WSN motes from channel 11 to channel 26 under the existence of IEEE802.11g WLAN and as for the WMN a series of TCP throughput tests were carried out from the wireless station within the radius of the WSN. The tests have been carried out using 3 motes within the same radius range from the gateway to capture different signal strength from the AP. The tests were carried out in 3 control environments:

a. WSN with absence of WMN
b. Coexistence of WSN and WMN without load
c. Coexistence of WSN and WMN with load

All communications are normally acknowledged in IEEE802.15.4. Each device, on receipt of a message, has a brief window in which it is required to send back a short message acknowledging receipt. The transmitting device will wait to hear this response, commonly known as ACK. If it does not hear the ACK, it will assume that the message was not received, and will retry its message again. This process repeats until the message and ACK are both received or until, usually after a few tries, the transmitter gives up and reports a failure.

Xmesh allows up to 8 retransmissions before the message is dropped. The percentage of retries is calculated as:

***[ (number of packet Tx / number of packet Rx) -1 ] x 100***

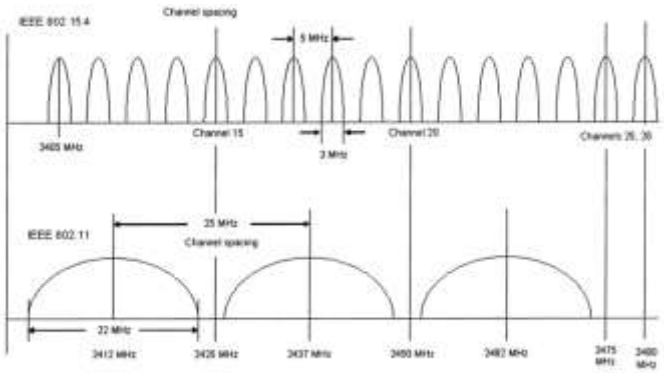


**Fig. 6:** 802.15.4 and 802.11g channels [11]

**Table 1:** IEEE 802.15.4 Channels. All frequencies are in GHz

| Channel | Lower Frequency | Central Frequency | Upper Frequency |
|---|---|---|---|
| 11 | 2.404 | 2.405 | 2.406 |
| 12 | 2.409 | 2.410 | 2.411 |
| 13 | 2.414 | 2.415 | 2.416 |
| 14 | 2.419 | 2.420 | 2.421 |
| 15 | 2.424 | 2.425 | 2.426 |
| 16 | 2.429 | 2.430 | 2.431 |
| 17 | 2.434 | 2.435 | 2.436 |
| 18 | 2.439 | 2.440 | 2.441 |
| 19 | 2.444 | 2.445 | 2.446 |
| 20 | 2.449 | 2.450 | 2.451 |
| 21 | 2.454 | 2.455 | 2.456 |
| 22 | 2.459 | 2.460 | 2.461 |
| 23 | 2.649 | 2.650 | 2.651 |
| 24 | 2.469 | 2.470 | 2.471 |
| 25 | 2.474 | 2.475 | 2.476 |
| 26 | 2.479 | 2.480 | 2.481 |

*Testbed :*

Experiments have been carried out by using the testbed sketched in figure 7, which consist of an IEEE 802.15.4 WSN and IEEE 802.11g WLAN operating in close proximity. Moteview was used to extract data to the database and it also has the ability to display live data information in a modular visualisation. PostgreSQL is an open source database within the moteview application. Three motes were deployed in the testbed. The motes were deployed in a topology with fixed radius(r) of 7 meters. The WMN AP was situated 70 meters apart from the gateway. The range was selected as a compromise of the standard given range for 802.11g ; maximum operating range of 30 meters (100feet) at 54Mbps to 90 meters (300 feet) at 1Mbps in an outdoor environment. It is important to include that the measurements have been performed in an open outdoor test environment with the potential occurrence of external interference and collateral phenomena such as reflections from near metallic objects and structures. To properly account for this phenomenon, different positions of sensor nodes have been considered. To compare the performance of the WSN deployment under the interference from WLAN, the WLAN was fixed to transmit on channel 6 (2437MHz) and variably changing WSN channel from 11 – 26. Xmesh application was downloaded to the motes. The RF power on the motes was set to high power (0dBm). The route update is set at 36 sec interval with packet size of 36 bytes and payload size of 29 bytes all of which are the default configuration for the xmesh. The XMTS310CA sensorboard were configured to display all the sensors available hence providing high data transmission from the motes to the gateway.

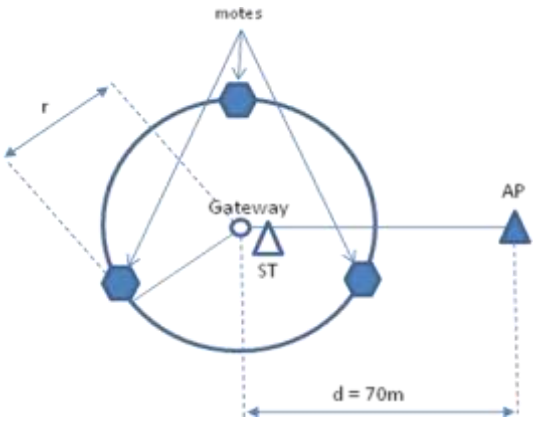


**Fig. 7:** Adopted testbed

Figure 8 below shows a graphical view of temperature reading taken from the motes. Three different colour lines are reflected from three different motes. The readings are quite similar in range as they are within the 7 meter radius and relatively stable.

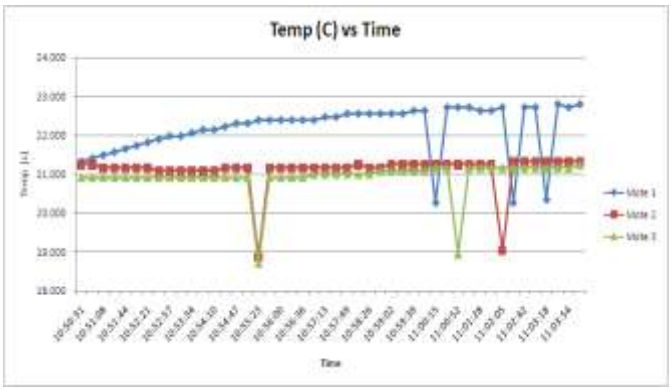


**Fig. 8:** Temperature data gathered from MicaZ motes

*Results:*

The experimental setup has confirmed that WSN are able to connect to the gateway and provide live data despite the presence of WMN in close proximity. The empirical data collected proves that the overlapped channels do have an impact on WSN. Loading the WMN with TCP traffic shows a greater impact to the WSN compare to the no load test. The overlapped WSN channel 16 – 19 has significant implication to the number of packets dropped; within the range of 9.09% -27.97%. Despite the 8 retries before the packet is considered dropped, these figures provide information on the severity of the interference.

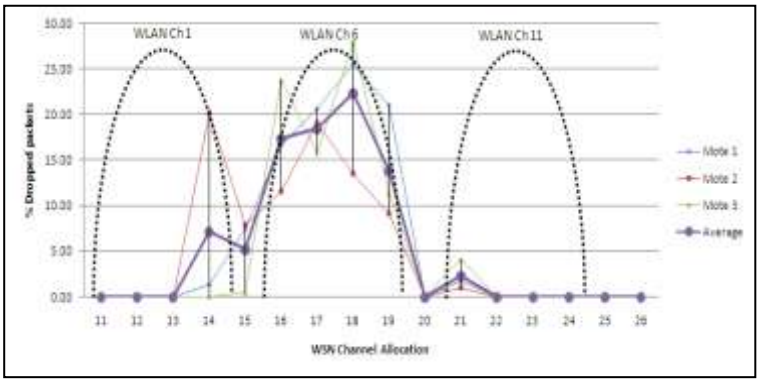


**Fig. 9:** Percentage of WSN dropped packets

The clear non-overlapping channels; 15, 20, 25 and 26; no of packets dropped are supposed to be 0% as it doesn't fall into any operating WLAN channels. Interestingly experiment on channel 15 shows that some

interference occurred making a small value of dropped packets. Evidently channel 11-14 and channel 21-24 are supposed to be out of interference because the WLAN is fixed on single channel 6 (2437MHz). However Channel 14 and 21 shows a very small visible reading of dropped packets. Figure 9 depicts the percentage of WSN dropped packets.

In the analysis of percentage number of retries for the packets in WSN, It is observed that the percentage number of retries is increasing in the overlapped channel in the range of 111.36% - 294.74%. Meaning in a severe case, a packet is resent four times before it is acknowledged by the receiver. Adjacent channels close to the operating channel 6 in the WLAN are also implicated, including clear non-overlapping channels 15 and 20. Figure 10 shows a graphical representation of the percentage number of retries for the packets in WSN.

The WLAN throughput measurements are taken using IxChariot (Ver 5.40). The Motorola IAP-4300 WMN average throughput is at 13.219Mbps (Max: 20.000Mpbs and Min:1.105Mbps) without WSN in operation and upon the introduction of WSN in its environment the Average throughputs in the presence of WSN are between 12Mbps – 13Mbps. Figure 11(a) and 11(b) shows one of the throughput comparison charts. The results are recorded with the WSN operating on channel 16 at frequency 2430MHz which has the highest possibility of interference with WLAN functionality which was set to channel 6 at frequency 2437MHz.

The impacts of coexistence between IEEE 802.15.4 and IEEE 802.11g at this stage of the experiment are clear.

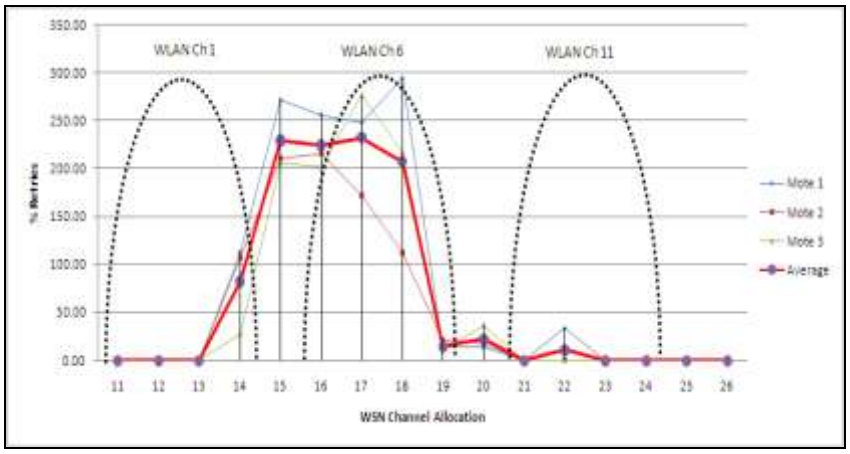


**Fig. 10:** Percentage of packet retries in WSN

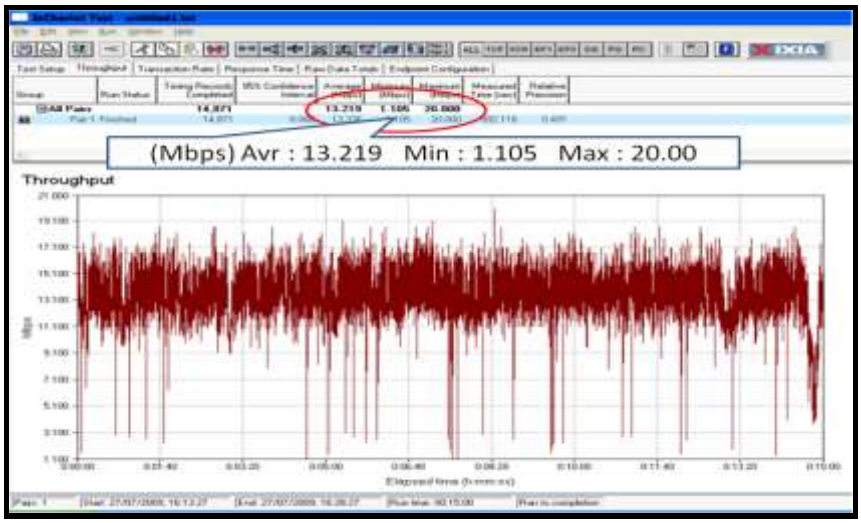


**Fig. 11(a):** Throughput of WMN without the presence of WSN

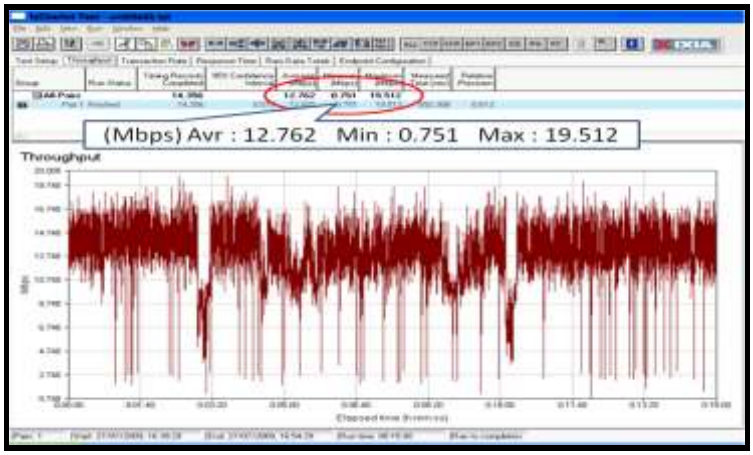


**Fig. 11(b):** Throughput of WMN (channel 6 at 2437MHz) with the presence of WSN (channel 16 at 2430MHz).

*Conclusion and Future Works:*

In this research project, we have evaluated the integration of IEEE 802.15.4, Zigbee Alliance compliant WSN over IEEE 802.11a/g Motorola IAP-4300 WMN as the backhaul. We found that the connectivity can be established by configuring the MIB600 Ethernet module and by associating through a bridge before traversing on the WMN backhaul. The packet delivery rates shows that when WSN and WMN channel overlap the WSN packet delivery rate is reduced from 100%. When the channels are separated further in frequency, the packet rate degradation is reduced. As expected, the degradation are more pronounced in areas with strong presence of WLAN signals.. Coexistence of IEEE802.15.14 WSN and IEE802.11g WLAN can be cautiously addressed through careful channel selection and assignment.

For future work, our research will focus on the impact of coexistence under a wider range of operating conditions. To do this, simulation models will be developed in OPENT.

## REFERENCES

[1] Juha Korhonen, 2008. “Over 1 billion wireless sensors to be sold in 2014”, News from Cambridge, published 11 September, available online at: http://www.cambridgenetwork.co.uk/news/article/default.aspx?objid=51236

[2] Wei Yuan, Xiangyu Wang, Jean-Paul M.G. Linnartz, 2007. A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g, Communications and Vehicular Technology, pp: 1-5.

[3] Sofie Pollin, Mustafa Ergen, Antoine Dejonghe, Liesbet Van der Perre, 2006. Francky Catthoor, Ingrid Moerman, Ahmad Bahai, “Distributed cognitive coexistence of 802.15.4 with 802.11”, Proc. Cognative Radio Oriented Wireless Networks and Communications, pp: 1-5. available online at: http://wow.eecs.berkeley.edu/ergen/docs/robustcrowncom.pdf

[4] Howitt, I., J. Gutierrez, 2003. “IEEE 802.15.4 low rate-wireless personal area network coexistence issues”, Proc. Wireless Communication Network Conference, 3: 1481-1486.

[5] MIT Technology Review, 2003. “10 Emerging Technologies That Will Change the World”, available online at: http://www.technologyreview.com/read_article.aspx?id=13060&ch=infotech

[6] Wang, M.M., J.N. Cao, Jing Li, Sajal K. Dasi, 2008. “Middleware for Wireless Sensor Network : A survey”, Journal of Computer Science and Technology, 23(3): 305-326, springer boston.

[7] MPR-MIB Users Manual, Revision A, 2007, available online at: http://www.xbow.com

[8] Roberto Di Pietro, Luigi V. Mancini, Alessandro Mei, 2006. “Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks”, 12(6): 709-721, Springer Netherlands

[9] IAP4300 – Intelligent Access Point for MOTOMESH Duo, available online at: http://www.motorola.com/business/US-EN/IAP4300_US-EN.do?vgnextoid=068151dab7877110VgnVCM1000008406b00aRCRD

[10] Rajiv Singhal, Cisco Systems, Eric Rotvold, Emerson Process Management, “Coexistence of wireless technologies in an open, standards-based architecture for in-plant applications”. Available online at: http://www2.emersonprocess.com/siteadmincenter/PM%20Central%20Web%20Documents/cisco_emerson_coexistence-paper_070914.pdf

[11] Leopaldo Angrisani, Matteo Bertocco, Daniele Frotin, Alessandro Sona, 2008. “Experimental Study of Coexistence Issue between IEEE 802.11b and IEEE802.15.4 Wireless Networks”, IEE Transactions on Instrumentation and Measurement, 57: 8.