Interference Issues and Mitigation Method in WSN 2.4GHz ISM Band: A Survey

N. Azmi[1, 2], L.M. Kamarudin[1, 2], M. Mahmuddin[3], A. Zakaria[1], A.Y.M. Shakaff[1], S. Khatun[2], K. Kamarudin[1], M.N. Morshed[2]

[1]Centre of Excellence for Advanced Sensor Technology, Universiti Malaysia Perlis, Perlis, Malaysia
[2]School of Computer & Communication Engineering, Universiti Malaysia Perlis, Perlis, Malaysia
[3]College of Art & Sciences, Universiti Utara Malaysia (UUM), Kedah, Malaysia
noraini.azmi88@gmail.com, latifahmunirah@unimap.edu.my

Abstract— **Current lifestyles promote the development and advancement in wireless technologies, especially in Wireless Sensor Networks (WSN) due to its several benefits. WSN offers a low cost, low data rate, flexible routing, longer lifetime, and low-energy consumption suitable for unmanned and long term monitoring. Among huge WSN applications, some key applications are smart houses, environmental monitoring, military applications, and other monitoring applications. As a result, ubiquitous increase in the number of wireless devices occupying the 2.4GHz frequency band. This causes a dense wireless connection followed by interference problem to WSN in the 2.4GHz frequency band. WSN is most affected by the interference issue because it has a lower data rate and transmission power compared to WLAN. Despite efforts made by researchers, to the author's knowledge, the interference issue is still a major problem in wireless networks. This paper aims to review the coexistence and interference issues of existing wireless technologies in the 2.4GHz Industrial, Scientific and Medical (ISM) band.**

Keywords— Coexistence, Frequency Spectrum, IEEE 802.15.4, Interference, WSN, 2.4GHz ISM band

I. Introduction

Wireless Sensor Networks (WSN) consist of a large number of wireless sensor devices (also known as motes) that is small in size, low cost, flexible routing, low power consumption with longer lifetime. Motes are designed for low data rate application such as Wi-Fi environmental monitoring, healthcare monitoring, medical applications, security, home automation, biodiversity monitoring, weather monitoring, forest monitoring, and military applications. WSN physical and MAC layer is governed by the IEEE802.15.4 (also known as Zigbee), henceforth, the IEEE802.15.4 and Zigbee will be used interchangeably in this paper. IEEE802.15.4 shares the 2.4GHz radio frequency with other wireless networks such as Wi-Fi, Bluetooth, microwave oven, Wireless USB, and cordless phone. Therefore, there is a tough competition among the wireless technologies in order to acquire the frequency spectrum resources and often WSN is at the loose end due to its low transmission power compared to other wireless technologies.

The Federal Communications Commission (FCC) fragmented the frequency band for specific devices. The 2.4GHz frequency band is selected exclusively for Industrial, Scientific and Medical (ISM) purposes, allowing various wireless devices to operate in this frequency region. The ubiquitous increase of wireless devices operating in the 2.4GHz frequency band raised various issues, particularly in coexistence and interference between different wireless technologies. Moreover, neither resource planning nor bandwidth allocation can be guaranteed due to the non-proprietary nature of the 2.4GHz frequency band. To better understand the issue, Fig. 1 shows the available wireless communication technologies (often classified into several categories according to their specific application and transmission range) and the allocation of the 2.4GHz ISM frequency band. Various ongoing studies are conducted to investigate and analyze the interference problem in the search for a better solution to improve the Quality of Service (QoS) of the network.

This paper aims to review the interference effect and the available methods to mitigate the interference issues, particularly for WSN operating in the 2.4GHz frequency band. The remainder of this paper is organized as follows: Section II review the existing interference mitigation in wireless standard, Section III illuminates the coexistence issues and Section IV review the available solutions to mitigate the interference issue.

II. Existing Interference Mitigation Scheme Employed in Wireless Standard

Wireless devices such as wireless sensors, smartphones, tablet, netbook, and laptop mostly utilize the existing wireless technologies such as IEEE802.15.1/Bluetooth, IEEE802.11/ Wi-Fi, IEEE802.15.4/Zigbee, IEEE802.15.3/WirelessUSB, 3G/4G, and GPS/GPRS. The following Sections and Tables highlight the features of different wireless technologies and the existing interference mitigation scheme incorporated in the standard.

A. WLAN/ IEEE802.11a/b/g/n

Wi-Fi[1] is the name dedicated by the Wi-Fi Alliance to the IEEE802.11 suite of standards. The IEEE802.11 defined the initial standard for Wireless Local Area Networks (WLAN).

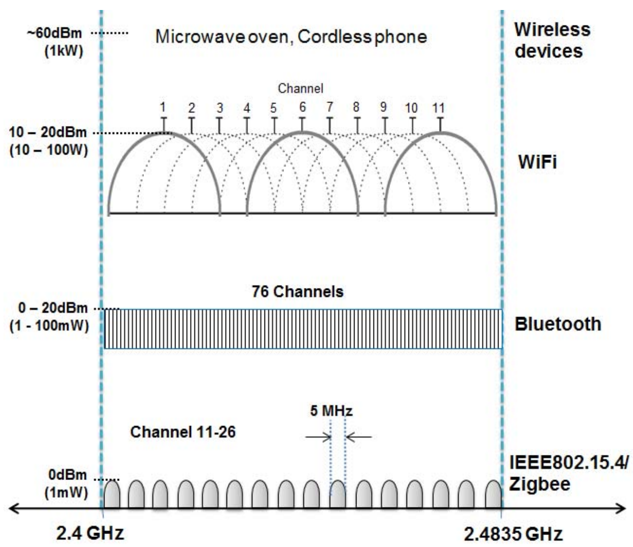

Fig. 1. Spectrum consist of Wifi, Bluetooth and WSN

The comparison between each Wi-Fi extension is presented in Table I. Wi-Fi employs Carrier Sense Multiple Access (CSMA) together with collision avoidance algorithm known as CSMA/CA to overcome the interference problem[2]. The CSMA scheme is also widely used in other technologies apart from Wi-Fi. In order for the Wi-Fi and WSN to coexist, several wireless standards incorporate the CSMA as interference mitigation method in the Physical and MAC layer. However, based on the empirical result obtained in a study by Huang et al. [3], the CSMA scheme seems inadequate to fully utilize the Wi-Fi white spaces between the Wi-Fi frames due to the Wi-Fi bursty character.. Moreover, the Clear Channel Assessment (CCA) in CSMA only sense the carrier of IEEE802.11 modulated signals hence, Wi-Fi do not defer their transmission even when there is ongoing WSN transmission because Wi-Fi transmitter unable to detect signals from WSN[3].

B. Bluetooth/ IEEE802.15.1

IEEE802.15.1/Bluetooth is a specification for Wireless Personal Area Network (WPAN) and it is widely used for short range communication such as information sharing between mobile phones or laptops[4]. Bluetooth incorporates Frequency Hopping Spread Spectrum (FHSS) as a method to overcome packet collision. Bluetooth occupies the 2.4GHz frequency band that is divided into 76 individual channels with only 1MHz wide. The signal deterministically changes its center frequency at the rate of 1600Hz over the 79 center frequencies in order to avoid the interference problem. Thus, over time the Bluetooth signal actually occupies 79MHz. The FHSS later improved to Adaptive Frequency Hopping (AFH) algorithm where the hopping algorithm includes 'Blacklisting' capability in which Bluetooth devices able to classify each channel as good, bad, or unknown. Bluetooth also has higher data rate compared to WSNs hence enabling live audio streaming. On the contrary, Bluetooth suffer from energy depletion because it consumes higher energy in comparison with WSN[5]. Table II shows three different classes for Bluetooth. Each class differs in terms of transmission range and energy consumption as the longer distance requires higher energy consumption compared to the shorter distance.

C. Microwave oven/ Cordless phone

Microwave oven operates at 2.5GHz radio waves to heat food because water, sugar and fats absorbed the waves at this length. The absorbed radio waves are converted directly into atomic motion, which causes the food to heat up [2]. Most microwave oven emits microwave across the 2.4GHz ISM band while heating food, causing interference to devices operating in the 2.4GHz ISM band for communication. Although, the effect of microwave oven on IEEE802.15.4 result in an enlarged of packet drop, however the percentage of packet drop less than 10% is still acceptable [6] [7].

D. WirelessUSB

WirelessUSB was initially designed for Personal Computer components such as mouse, and keyboard. Similar to Bluetooth, WirelessUSB is made of 76 channels and each channel with 1 MHz bandwidth[2]. WirelessUSB utilizes the DSSS instead of FHSS even though it has the same number of frequency channel as Bluetooth (see Table III). Besides that, unlike Bluetooth, WirelessUSB utilize Frequency Agility to overcome interference, where it uses a fixed channel for transmission and only change the channel when the link quality dropped under unacceptable threshold.

E. 2.4GHz Cordless Phones

Most of the 2.4GHz cordless phone use Direct Sequence Spread Spectrum (DSSS) technique while some use FHSS to reduce the interference effect[8][9]. For cordless phone that use DSSS, the phone has a built-in button that allows the user to manually change the channel in the event when the signal is interfered by other wireless system. On the other hand, phone that utilizes FHSS does not require users to manually change the channel because the FHSS technique will constantly change the operating channel automatically[2].

F. Wireless Sensor Network

WSN as the name suggests, is a network comprises of sensors that communicate with each other wirelessly. WSN is low cost and affordable wireless sensor suitable for most low data rate monitoring. The IEEE802.15.4 is a standard defined specifically for low data rate wireless sensor applications and the low power consumption characteristic enables the nodes to operate for a period of time powered only by a battery [5]. IEEE802.15.4 [10] defines two sub-layers consist of physical (PHY) layer and medium-access-control (MAC) layer. IEEE802.15.4 physical layer specifies the physical operation of the device such as receiver sensitivity, channel rejection, number of channels, energy detection, and link quality indication. While, the IEEE802.15.4 MAC control the access to radio channel, employs CSMA/CA to avoid collision (interference), security, flow control, and retransmission. Other network protocols were developed on top of IEEE802.15.4. Among the protocols are ZigBee, WirelessHART, and ISA100. WirelessHART, for instance, is a standard developed on top of the IEEE802.15.4 and employs the combination of frequency hopping with TDMA however, with additional features such as blacklisting technique in order to overcome the interference problem. IEEE802.15.4 also employs DSSS scheme in order to ensure the coexistence of the signal with other network. Another scheme adopted in IEEE802.15.4 to ensure successful packet delivery in the presence of interference is retransmission capabilities (minimum of 3 retries). However, this incurs extra energy consumption that inevitably shortened the lifetime of the sensor node.

The Zigbee protocol built atop of the IEEE802.15.4 OSI stack provides additional supports of network and application layer in terms of security and user interface. Unlike Bluetooth, Zigbee does not change the operating channel upon experiencing heavy interference. Hence, Zigbee relies on the low data rate (low duty cycle) and utilizes the collision avoidance algorithm similar to IEEE802.11/Wi-Fi to reduce the collision among Zigbee nodes and minimize packet loss rate affected by the interference from other wireless devices. Some of the new features incorporated in ZigBee are intended to promote coexistence capability with other networks. According to [8], Zigbee Pro currently have the ability to change its operational frequency while it is operating which is known as frequency agility[9]. Table IV presents the comparison between Wi-Fi, Bluetooth and Zigbee technologies.

III. COEXISTENCE ISSUES BETWEEN WSN & OTHER TECHNOLOGIES

A number of approaches have been proposed to encourage the coexistence between different wireless technologies. The majority of studies conducted focused on the effect of specific interference source on WSN individually or separately such as in [11][12], and only a few studies investigate the performance of WSN under heavy interference from various types of interference sources simultaneously such as in [6].

WSN is susceptible to interference caused by other 2.4GHz wireless system (e.g. IEEE802.11b/g WLAN, Bluetooth and Cordless Phone) because they are higher in transmission power compared to WSN. The mutual interference between WSN and other wireless technologies is unsymmetrical, for instance the WSN is vulnerable to WLAN interference and not vice versa[13]. From the past decade, there are several simulation and experimental study conducted to investigate the effect of other wireless technologies on WSN. According to [6], if the same transmission frequency is selected, the interference effect of IEEE802.11 on IEEE802.15.4 is very critical in comparison with the effect from other wireless systems such as microwave oven, Bluetooth, and cordless phone. Overlapping channels between WSN and Wi-Fi destroyed more than 92% of WSN frame[6]. Bluetooth, microwave oven and, cordless phone contributes to enlarged WSN packet error rate, however, the level below 10% is considered as not critical[6].

Garoppo et al. [12] study the effect of mutual interference between Wi-Fi, Bluetooth, and Zigbee towards the performance of the wireless technologies. The experimental

TABLE I: IEEE802.11A/B/G/N PROTOCOLS EXTENSION COMPARISON

Parameter	802.11a	802.11b	802.11g	802.11n
Frequency	5.3, 5.8 GHz	2.4 GHz	2.4 GHz	2.4/ 5GHz
Channels	1-13	1-13	1-13	1-13
Bandwidth (MHz)	20-22	20-22	20-22	20-40
Modulation	OFDM	CCK/ DSSS	OFDM	OFDM
Range (m)	~30 - 35	~30 - 38	~30 - 35	~60 - 70
Data Rate	54Mbps	11Mbps	54Mbps	108Mbps
TX Power	~100mW	~100mW	~100mW	~100mW

TABLE II: IEEE802.15.1 (BLUETOOTH)

Parameter	Bluetooth Classes		
	Class 1	*Class 2*	*Class 3*
Frequency	2.4GHz		
Channels	79		
Bandwidth	1 MHz		
Modulation	FHSS		
Signal range	100m	10m	1m
Max data rate	1 Mbps	1 Mbps	1 Mbps
Max output power	100mW (+20dBm)	2.5mW (+4dBm)	1mW (0 dBm)

TABLE III: WIRELESSUSB

Parameter	WirelessUSB
Operating frequency	2.4 GHz
Transmission Channels	79 channels
Bandwidth per channel	1 MHz
Modulation Technique	DSSS
Maximum data rate	62.5 kbps

TABLE IV: COMPARISON BETWEEN DIFFERENT WIRELESS TECHNOLOGIES

Standard (Technology)	IEEE802.11 /Wi-Fi	IEEE802.15.1 /Bluetooth	IEEE802.15.4 /Zigbee
Channels	11	79	16
Data Rates	11Mbps, 54Mbps	1Mbps	250Kbps
Throughput	11000(kb/s)	720(kb/s)	20 –250(kb/s)
Bandwidth	22 MHz	15MHz (Dynamic)	3MHz (Static)
Transmission Range (m)	1 – 100	1 – 10	1 - 100
Transmit Power	100mW	1-100mW	1mW
Power Consumption	Medium	Low	Ultra Low
Battery Life (days)	0.5 – 5	1 –7	100 –1000
Network Size	32 nodes	7 nodes	>64000 nodes
Frequency Modulation	CCK, OFDM	Gaussian Frequency Shift Keying (GFSK)	BPSK, O-QPSK
Spread Spectrum Technique	DSSS	FHSS	DSSS
Channel Access	CSMA-CA, Dynamic channel selection (DCS)	Master slave scheme, AFH	CSMA-CA, Energy Detection but no DCS

study performed between pairs of technologies and simultaneous interference among the three systems. A drawback of the experimental test conducted is that it does not include other wireless devices such as microwave oven, WirelessUSB, and cordless phones. The result from that study showed that Wi-Fi is unaffected by the presence of neither Bluetooth nor Zigbee. On the contrary, Zigbee and Bluetooth suffer from the interference by Wi-Fi as the frame error rate (FER) dropped with an average of 41% and 68% respectively. The result also showed that the position of WSN and the interferer significantly affect the performance of the WSN.

In a similar study, Guo et al. [14] found that microwave oven contributes minor impact on Zigbee packet error rate (PER) compared to Wi-Fi and Bluetooth. Besides that, the effect of microwave oven on Zigbee heavily depends on the distance of the microwave oven (interferer) and the receiver as the PER drops from 8.20% to 2.06% when the distance between the receiver and microwave oven is 0.5m and 7m respectively. Guo also summarizes several aspects that must be taken into account when predicting the performance of Zigbee communication in the presence of different interferer. Among the aspect summarized are the type of interference source, distance between transmitter and receiver, and also distance between interferer and receiver. However, this study only focuses on one interferer at a time, hence does not reflect the interference issues in the real environment where a number of different wireless devices coexist and interfere with each other.

In another experimental studies conducted to investigate the effect of Bluetooth interference on WSN shows that the packet loss rate due to the Bluetooth interference is approximately 3% [15] and can go up to 9-10% [6]. Table V shows the packet loss experience by WSN in the presence of different wireless technologies.

Each wireless devices operates at slightly different frequency though they are sharing the same frequency band[11]. Other than that, Wi-Fi bandwidth is about 22MHz which covers approximately four WSN channels, hence, affect the QoS of the WSN in the occurrences of heavy Wi-Fi network traffic. Hou et al. [11] studied the effect of Wi-Fi on Zigbee utilizing different setup: Wi-Fi connection via Access Point (AP) and via point-to-point (Ad-hoc) configuration. The findings from that study agrees with the results from other studies as Zigbee experiences packet losses in the presence of heavy IEEE802.11/Wi-Fi traffic depending on the network setup; approximately 33% (via Ad-hoc) and 56% (via AP). According to Hou, packet loss is not permissible, especially in mission critical application such as in military or medical applications where a packet might bring the difference between life and death. In medical application such as ECG monitoring, the critical readings need to be successfully transmitted to the medical assistance and doctors immediately. Any delay such as waiting duration for free channels and retransmission is not acceptable, thus, a new method or algorithm needs to be formulated.

The interference effect of WLAN on Zigbee does not only depends on the location and distance of Zigbee nodes to Wi-Fi devices but also affected by Wi-Fi packet sizes[16] and the ongoing activity/task of Wi-Fi devices[17]. Boano et al. [18] perform experimental study to investigate the effect of Wi-Fi traffic on Zigbee packet. The results from the study shows that Wi-Fi activities such as radio streaming, file transfers and video streaming contributes to approximately 15%, 90% and 30% Zigbee packet loss rate respectively. The enlarged in Zigbee packet loss rate often followed with the increased in the network traffic due to retransmission[17]. The re-transmission will increase Zigbee energy consumption and frequency spectrum occupancy, which leads to a serious interference problem.

TABLE V: WSN PACKET LOSS RATE IN THE PRESENCE OF OTHER WIRELESS TECHNOLOGIES

Technologies	WSN Packet loss rate	Source(s)
Wi-Fi	~90% (File transfer)	[18] [6]
	~30% (video streaming)	
Bluetooth	3-10%	[15][6]
Microwave oven	0.5-2% (worst case scenario, mote placed on top the microwave oven)	[6]

TABLE VI: COEXISTENCE & INTERFERENCE STUDIES

Source	Wireless Devices in the Study	Parameters
[12]	Wi-Fi, Bluetooth, Zigbee	Frame error rate (FER)
[14]	Wi-Fi, Bluetooth, Zigbee, Microwave oven	Link Quality Indicator (LQI), Received Signal Strength Indicator (RSSI), Packet error rate (PER)
[11] [31]	Wi-Fi, Zigbee	Packet loss rate
[16]	Wi-Fi, Zigbee	PER, RSSI
[3]	Wi-Fi, Zigbee	Packet delivery rate (PDR)
[32]	Wi-Fi, Bluetooth, Zigbee	Packet error rate (PER)

Interference from the adjacent channels (frequency bands) is another important factor that must be taken into consideration when investigating the interference effect on the performance of WSN. WSN is not only susceptible to external interference from other wireless technologies but also highly affected by interference from the adjacent channels[19]. Even though, there is no overlapping between adjacent channels in IEEE 802.15.4, work by [20] shows the presence of interference due to spurious emissions introduced by the O-QPSK coding.

IV. EXISTING INTERFERENCE MITIGATION METHOD

Traditionally, by licensing the frequency bands only the primary user is authorized to transmit in that specific frequency bands[12]. The frequency licensing approach is not only exceptionally costly but also caused low utilization of the licensed frequency band because only the primary user is allowed to use that allocated channel regardless the minimal transmission. Hence, this approach is not a viable and efficient solution to the interference problem.

There are a number of schemes devised to reduce; if not possible to eliminate the interference between wireless devices from happening. The schemes ranging from time sharing, DSSS, CSMA, and exploiting different channels. Despite these advancements and efforts, interference is still a big issue, especially when two or more devices attempt to transmit data simultaneously. Besides, devices that share the 2.4GHz frequency band using different standard and protocols, and each of them propose a different way to mitigate interference and collision. Besides that, challenges in solving the interference problem is due to the differences in the physical layer of each wireless device. Bluetooth, Zigbee, and Wi-Fi utilize different modulation schemes, different packet sizes, with different packet type, format and headers. Due to these reasons, Zigbee cannot issue a packet to 802.11 devices indicating that it wishes to transmit data. Hou, et al. [11] proposed a hybrid device that have both IEEE802.15.4 and IEEE802.11 device transmitters. The hybrid device will act as an intermediate connector between both protocols. Hou, et al. [11] incorporate Clear-to-Send (CTS) in the interference solution and the test shows that the packet drop of WSN decreased significantly, as low as 3% and 14% for different setups; infrastructure based 802.11 and ad-hoc network respectively.

Different methods and algorithms have been developed in order to mitigate the interference issue and ensure the coexistence between different types of wireless technologies (see Table VII). Each solution differs in terms of computational cost, computational complexity, and performance. Recently, cognitive radio techniques gaining great interest as the devices able to scan the environment to dynamically select and utilize the channel that offer the least interference[21][22]. Yun et al. [23], proposed a cognitive radio utilizing channel switching scheme to avoid interference among the IEEE802.15.4 and other wireless technologies. The problem with cognitive radio technique is that there is no guarantee that the primary user (licensed band owner) communication would not be affected. This study only provides theoretical measurement, thus further experimental test is required to analyse the effectiveness of the proposed theory.

A number of studies incorporated the concept of channel hopping in Bluetooth into the interference solution for WSN. Yoon, et al. [24] proposed Adaptive Channel Hopping (ACH), while Mahalin, et al. [25] introduce the Adaptive Interference Avoidance Scheme. Other available interference mitigation method is Interferer Classification (IC). According to Chowdhury, each transmission protocols implement different transmission cycles, for instance, WLAN devices rely on the opportunity to gain control over the channel when the channel is vacant while microwave ovens runs at a fixed, pre-determined duty cycle (range of 30-50%). The abilities to recognize different type of interferer helps WSN to select a suitable channel for its transmission[26]. Currently, studies involving wireless sensor network are mostly based on single radio per node. There are several channel classification used for wireless ad-hoc networks such as fixed-channel assignment, semi-dynamic channel assignment and dynamic channel assignment[27]. Nevertheless, different wireless systems operate in the same frequency band uses different modulation and channel access schemes hence introducing challenges to solve the interference problem (refer Table IV). A study by Vanheel et al. [28] suggest that the reduction in power will have positive effect on the frequency spectrum. This is possible for low data rate applications that require small throughput and bandwidth, but unlikely for high data rate applications that requires high bandwidth and throughput such as file transfer, video and voice streaming.

TABLE VII: EXISTING INTERFERENCE MITIGATION FOR WSN

Techniques	Source(s)
Transmit power control	[28]
Adaptive clear channel assessment (CCA)	[33]
Dynamic frequency selection / switching	[13], [23], [24]
Adaptive time slotted channel hopping	[34]
Adaptive interference avoidance scheme	[25]
Interferer classification	[26]
Request to send (RTS)/ Clear to send (CTS)	[11]

At this point in time, most WSN nodes perform energy scanning initially before forming a network and choose the best channel during that instant. As the transmission progress, the WSN did not change the channel even when experiencing heavy interference hence reduces the performance of WSN. Researchers begin to realize that channel selection can be implemented in WSN similar to Bluetooth frequency hopping. As a starting point, the algorithm for channel selection should use low processing resource and memory, consume small computational power, and robust. Several studies proposed channel selection algorithms and techniques; however, the validated algorithm via simulation and experimental study is for proof of ideas only. A real-life implementation of channel selection is not yet available to the author's knowledge.

For example, in a study by Hassan, et al [13], he proposed an interference mitigation algorithm utilizing vector mapping. A footprint is obtained by measuring the RSSI on each WSN channel (channel 11 until channel 26) when Wi-Fi is injected with heavy traffic (video streaming). The channel selection is then performed by mapping the footprint vector to the present measured vector (RSSI on each WSN channel) and then the best channel with the lowest energy level is selected. This method is superior in terms of accuracy; however it requires high processing resources to perform the extensive mathematical calculations. In another study, Zheng, et al. proposed channel assignment method utilizing Tabu Search algorithm to determine the best transmission channel for WSN[29]. Zhang proves that the algorithm is successful via simulation test. Although, channel selection is a permissible solution to solve the interference problem as proposed by several studies[13][29][30], there is several setbacks that must not be overlooked. According to Yao et al. [30], when sensor nodes decided to change the current working channel detect upon experiencing heavy interference, the communication will be suspended until the all sensor nodes in the network re-associates with the base station again. Any attempt for data transmission within the re-association period will result in data loss. Besides that, most existing interference mitigation methods typically perform energy scanning only at the base station (receiver side). This solution is believed to be inefficient if the network deployed is based on the ad-hoc topology consisting of scattered sensor nodes. Sensor nodes that are placed near interference source experienced greater interference effect compared to the sensor nodes that are located further away from interference source [6].

V. SUMMARY & FUTURE SUGGESTION

WSN is among the future wireless technologies that promote the Internet of Things (IoT). Despite that, the literature review shows that there are various open issues that must be fulfill in order to have a successful wireless sensor network with good QoS. Interference issue is crucial in determining the performance of the WSN, hence must not be overlooked. Although, the studies on the interference problem have been conducted since the beginning of wireless system, to the author's knowledge, there is no definite method found to completely eliminate the interference issue. At present, the idea of channel selection emerged as one of the solution that can be utilized so solve the interference issues. Hence, more studies should be conducted in this area to create a better methods, algorithms and solutions.

ACKNOWLEDGMENT

This research is supported by an ERGS9010-00036 grant, "Sight, Scent and Sound of Nature: A Bio-indication of Healthy Forest". Thanks to the anonymous reviewers who provided insightful comments that helps to improve this paper.

REFERENCES

[1] W. Lehr and L. W. McKnight, "Wireless internet access: 3G vs WiFi?," *Telecomm. Policy*, vol. 27, no. 5–6, pp. 351–370, Jun. 2003.

[2] R. Kandiar, "Interference mitigation challenges and solutions in the 2.4 to 2.5-GHz ISM band," no. 001, pp. 1–14, 2011.

[3] J. Huang, G. Xing, G. Zhou, and R. Zhou, "Beyond co-existence: Exploiting WiFi white space for Zigbee performance assurance," *18th IEEE Int. Conf. Netw. Protoc.*, pp. 305–314, Oct. 2010.

[4] M. Blom, M. Ekstrom, J. . Castano, and M. Linden, "Bluetooth energy characteristics in wireless sensor networks," *3rd Int. Symp. Wirel. Pervasive Comput.*, pp. 198–202, May 2008.

[5] S. Zacharias and T. Neve, "Technologies and architectures for multimedia-support in wireless sensor networks," *Smart Wirel. Sens. Networks, InTech*, pp. 373–394, 2010.

[6] A. Sikora and V. F. Groza, "Coexistence of IEEE802. 15.4 with other systems in the 2.4 GHz-ISM-Band," in *IEEE Instrumentation and Measurement Technology Conference (IMTC)*, 2005, vol. 3, pp. 1786–1791.

[7] A. Sikora, "Compatibility of IEEE 802.15.4 (Zigbee) with IEEE 802.11 (WLAN), Bluetooth, and Microwave Ovens in 2.4GHz ISM Band," vol. 37, no. 10, pp. 23–31, Aug. 2004.

[8] G. Thonet and P. Allard-jacquin, "ZigBee – WiFi coexistence white paper and test report," vol. 1, no. 38, pp. 1–38, 2008.

[9] ZigbeeAlliance, "ZigBee and wireless radio frequency coexistence," 2011.

[10] IEEE 802.15 Working Group, "IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks Specific Requirements Part 15.4 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for ." 2003.

[11] J. Hou, B. Chang, D. Cho, and M. Gerla, "Minimizing 802.11 interference on Zigbee medical sensors," 2009.

[12] R. G. Garroppo, L. Gazzarrini, S. Giordano, and L. Tavanti, "Experimental assessment of the coexistence of Wi-Fi, ZigBee, and Bluetooth devices," *2011 IEEE Int. Symp. a World Wireless, Mob. Multimed. Networks*, pp. 1–9, Jun. 2011.

[13] M. N. Hassan, L. M. Kamarudin, and A. Zakaria, "Mitigating interference in a heterogeneous wireless network using channel selection," vol. 7, pp. 3766–3774, 2013.

[14] W. W. Guo, S. Member, W. M. Healy, and M. Zhou, "An experimental study of interferenceimpacts on ZigBee-based wireless communication inside buildings," pp. 1982–1987, 2010.

[15] M. Bertocco, G. Gamba, A. Sona, G. Gradenigo, and B. Padova, "Is CSMA/CA really efficient against interference in a wireless control system□? An experimental answer," pp. 885–892, 2008.

[16] M. Petrova, J. Riihij, and M. Petri, "Performance study of IEEE 802.15.4 using measurements and simulations," vol. 00, no. c, pp. 487–492, 2006.

[17] N. Baccour, D. Puccinelli, T. Voigt, A. Koubaa, C. Noda, H. Fotouhi, M. Alves, H. Youssef, M. A. Zuniga, C. A. Boano, and K. Römer, "External radio interference," in *Radio Link Quality Estimation in Low-Power Wireless Networks*, Heidelberg: Springer International Publishing, 2013, pp. 21–63.

[18] C. A. Boano, T. Voigt, C. Noda, K. Römer, and M. Zúñiga, "JamLab□: Augmenting sensornet testbeds with realistic and controlled interference generation," pp. 175–186, 2011.

[19] L. Lo Bello and E. Toscano, "Coexistence issues of multiple co-located IEEE802.15.4/ZigBee networks running on adjacent radio channels in industrial environments," *Ind. Informatics*, vol. 5, no. 2, pp. 157–167, 2009.

[20] E. Toscano and L. Lo Bello, "Cross-channel interference in IEEE 802.15.4 networks," in *2008 IEEE International Workshop on Factory Communication Systems (WFCS 2008)*, 2008, pp. 139–148.

[21] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surv. Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[22] A. He, K. K. Bae, T. R. Newman, J. Gaeddert, K. Kim, R. Menon, L. Morales-tirado, J. J. Neel, Y. Zhao, J. H. Reed, and W. H. Tranter, "A survey of artificial intelligence for cognitive radios," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1578–1592, 2010.

[23] J. Yun, B. Lee, J. Li, and K. Han, "A channel switching scheme for avoiding interference of between IEEE 802.15.4 and other networks," *Int. Multi-symposium Comput. Comput. Sci.*, pp. 136–139, 2008.

[24] S.-U. Yoon, R. Murawski, E. Ekici, S. Park, and Z. H. Mir, "Adaptive channel hopping for interference robust wireless sensor networks," *2010 IEEE Int. Conf. Commun.*, pp. 1–5, May 2010.

[25] N. H. Mahalin, H. S. Sharifah, S. K. S. Yusof, N. Fisal, and R. A. Rashid, "RSSI measurements for enabling IEEE802.15.4 coexistence with IEEE802.11b/g," pp. 1–4, 2009.

[26] K. R. Chowdhury and I. F. Akyildiz, "Interferer classification, channel selection and transmission adaptation for wireless sensor networks," in *IEEE International Conference in Communication (IEEE ICC 2009)*, 2009, pp. 1–5.

[27] Ö. Durmaz Incel, "Multi-channel wireless sensor networks: protocols, design and evaluation," 2009.

[28] F. Vanheel, J. Verhaevert, and I. Moerman, "Spectral interference study of WiFi on wireless sensor networks," in *University of Ghent Faculty of Engineering Sciences PhD Symposium, Ghent, Belgium*, 2007, p. 108.

[29] T. Zheng, Y. Qin, D. Gao, and H. Zhang, "A novel channel assignment method using Tabu Search based on graph theory in Wireless Sensor Networks," *2010 3rd IEEE Int. Conf. Broadband Netw. Multimed. Technol.*, pp. 1079–1083, Oct. 2010.

[30] F. Yao, S.-H. Yang, and W. Zheng, "Mitigating interference caused by IEEE 802.11 b in the IEEE 802.15. 4 WSN within the environment of smart house," in *2010 IEEE International Conference on Systems Man and Cybernetics (SMC)*, 2003, pp. 2800–2807.

[31] B. Polepalli, W. Xie, D. Thangaraja, M. Goyal, H. Hosseini, and Y. Bashir, "Impact of IEEE 802.11n operation on IEEE 802.15.4 operation," *2009 Int. Conf. Adv. Inf. Netw. Appl. Work.*, pp. 328–333, May 2009.

[32] S. Shin, H. Park, S. Choi, and W. Kwon, "Packet error rate analysis of ZigBee under WLAN and Bluetooth interferences," *IEEE Trans. Wirel. Commun.*, vol. 6, no. 8, pp. 2825–2830, Aug. 2007.

[33] W. Yuan, J.-P. M. G. Linnartz, and I. G. M. M. Niemegeers, "Adaptive CCA for IEEE802.15. 4 wireless sensor networks to mitigate interference," in *WCNC 2010*, 2010, pp. 1–5.

[34] P. Du and G. Roussos, "Adaptive time slotted channel hopping for wireless sensor networks," in *Computer Science and Electronic Engineering Conference (CEEC2012)*, 2012, pp. 29–34.