A New Zigbee Backoff Approach for Home Healthcare Devices

Halikul Lenando, Azizul Lau
Faculty of Computer Science & Information Technology,
Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia.
cool@unimas.my

***Abstract*—Most of Healthcare Monitoring System (HMS) used ZigBee, one of the Wireless Sensor Network technologies that offer better mobility, low power consumption and better network scalability. However, ZigBee-based devices face overlapping channel with Wi-Fi devices which cause interference when deployed under the same operating frequency. In this paper, we proposed a new ZigBee algorithm based on Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) to minimize the Wi-Fi interference using experimental approach. Further elaboration highlights the approach, experiment set-up and the analysis metrics for the ZigBee and Wi-Fi coexistence issues. By minimizing the effect of Wi-Fi interference, it will improve the ZigBee transmission reliability which critically required for developing a reliability HMS application. A fragmentation packet management can be considered in the future development to improve packet allocation for large type packet to avoid collision with Wi-Fi packets for better HMS application performance.**

***Index Terms*—ZigBee; MicaZ; Coexistence; CSMA-CA; Smart Home; Healthcare Monitoring.**

I. INTRODUCTION

Health Monitoring System (HMS) is one type of medical system used in healthcare application today to monitor patient health parameters to improve their health condition. HMS goals to facilitate medical application in increasing monitoring accuracy, produce high quality of monitoring data, and less medication error [1]. Besides, HMS deployment also not limit to the medical center or hospital only. It can be deployed in multiple environments like home, and outdoor environments allow patient for self-monitoring that give an advantage for people that live alone. For example, Smart Home introduced as home environment indoor health and safety automated monitoring solution that targeted in assisting elderly and disabled people as stated in [1]. It also aids the medical team in early disease detection as the patients are continuously monitored 24/7 in their home. While for an outdoor solution, HMS can be integrated as part of Smart City that also assists elderly and disabled peoples in the case of emergency that happens within the Smart City network.

As mentioned before, HMS can be used to facilitate medical application as a modern Health Monitoring System is mostly computerized health parameters observation and acquisition for health diagnosis. Data acquisition achieved by using smart monitoring device approach in the form of wearable and remotely monitoring devices to collect patients' health parameters [1]. The health parameters are fetched automatically from the patient without any human intervention. The information fetched is accumulated digitally in local or online data repositories for diagnosis and research purposes. Patient common measured health parameters are heart rate, body temperature, blood pressure, etc. In HMS, those parameters are important because each of the parameters can be related to each other. For example, the system [2] proposed is more for elderly fall detection which elderly heart rate and body position parameter are crucial to being measured. Fall detection depends on those two parameters where a sudden changed of body position with increasing of heart rate can be predict as falling and caused an emergency alert to be triggered to the caretaker.

Health parameters in HMS are also monitored in real time fashion. This is to prevent outlier and to obtain reliable results [4]. Continuity and accuracy in data acquisition are fundamental issues for real-time monitoring. It requires a reliable communication system. Basically, in HMS, sensor node is used to obtain data and sink node is for processing data. Communications between nodes is done via wirelessly which to provides mobility to the monitored patient or users.

ZigBee is a Wireless Body Area Network (WBAN) technology. It has small size of data transfer, low power consumption time and better network scalability which is suited for the medical application. Zigbee is a protocol with used IEEE 802.15.4 as its baseline and implemented on low powered devices manufactured by various manufacturer [15]. ZigBee supports 250 Kbps theoretical bandwidth which makes it suitable technology in sending smaller data. Moreover, ZigBee devices are capable running time up to 17 months with optimized power configurations which is less cost for power maintenance. It also provides better network scalability due to it Mesh Network capability where the ZigBee device able to detect the present of new sensor nodes and reroute data from an origin node to the sink node. Those three important features of ZigBee make it suitable for HMS application based.

Despite the aforementioned advantages, ZigBee is subject to interference from the overlapping operating channel with Wi-Fi devices which also used 2.4 GHz bands [12,14]. Most of the Wi-Fi router or device has a power range from 5-20 dB which is higher than the ZigBee maximum transmission power (0 dB). A high Wi-Fi transmission power can give serious impact on ZigBee device performance which affects the reliability of the ZigBee communication when overlapping channel occurs. In recent studies, when ZigBee network deployed in the area with moderate Wi-Fi traffic it can cause packet delivery delay problem due to high jitter time [5,6,11]. Moreover, different way of deploying CSMA-CA protocols with the different back off duration also potentially lead to significant performance depreciate for

ZigBee devices [13]. This problem is vital to be investigated as HMS requires real-time data transmission and highly accuracy information.

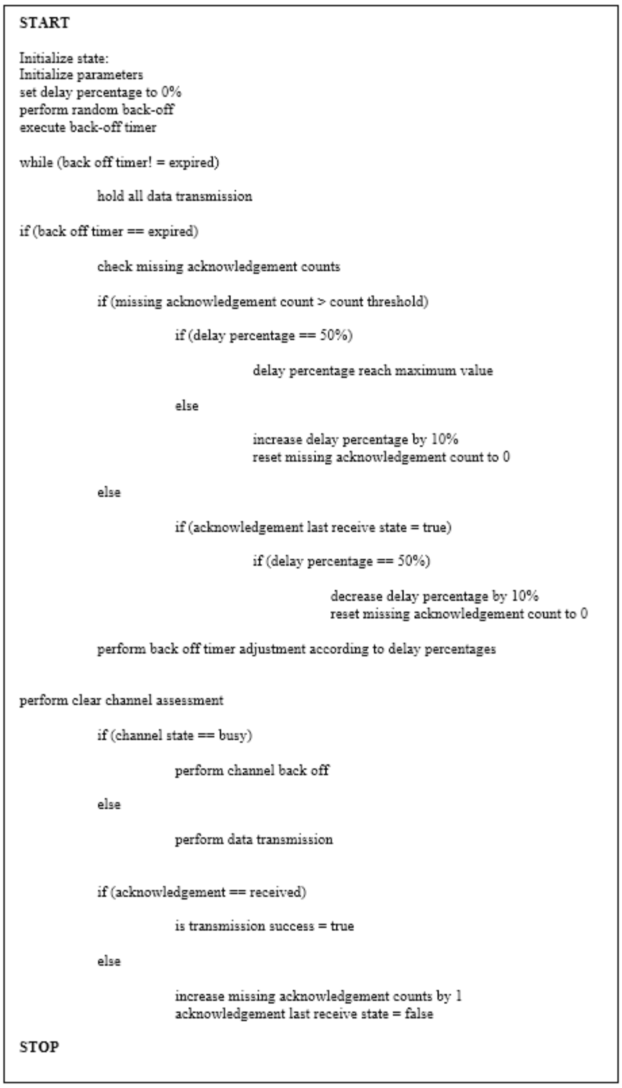
There are number of related studies to minimizing ZigBee and Wi-Fi coexistence by using Frequency Domain Approach, Packet Size Rectification Approach, Back Off Mechanism Alteration Approach and Dynamic approach. A Frequency Adaptation under Frequency Domain Approach proposed to manage and to reduce the packet loss and retransmission rate by only switching ZigBee channel when the channel interference threshold is reached to a certain level. Another proposed Frequency Domain Approach Studies, a Frequency-Based Interference Avoidance proposed to minimize interference effect by utilizing Packet Error Rate parameter (PER) in [8]. The algorithm proposed by selecting the best ZigBee channel based on channels that have lower measured PER when the current link quality is drop to a certain level. The study is carried by the experimental method by different scenarios involving background interferences, emulated Wi-Fi interference and Real-Life interference using Tmote Sky devices. Packet Dummy Byte technique to reduce packet loss due to packet collision with Wi-Fi packets proposed in [9]. Based on their analysis, the main reason of packet loss in ZigBee is the packet header is currupted which causes the packet could not be processed at the receiver side. Controlling the load for Wi-Fi to adjust the guarantee delay for ZigBee is examine in [5]. The proposed algorithm, allow ZigBee coordinator to perform a channel scan to find which Access Point (AP) utilization is higher in the current channel.

In this paper, we propose a new CSMA-CA algorithm for ZigBee that satisfies the delay requirement for data delivery by improving the current ZigBee Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA). An experimental based approach is used to analyze the current ZigBee CSMA-CA performance in moderate to high Wi-Fi traffic to formulate a new lightweight protocol. The rest of this paper is organized as follows. Section 2 introduces a proposed solution for new back off algorithm. Section 3 provides an experimental approach for investigating the interference in detail. Section 4 concludes the paper.

II. Proposed Solution

We propose a solution to increase the chance for ZigBee to find white space between Wi-Fi packets when performing data transmission in the high traffic channel. It can be achieved by minimizing the delay value based on some missing acknowledgment from the sink node or base station and also the link quality measurement.

Figure 1 shows the general flow of the proposed study, where the algorithm involves adjustment of the back-off timer values based on the missing acknowledgment counts from the base station to the sensor node. The number of missing acknowledgment indicates transmission state. Those missing acknowledgment counts are assign by percentage class which can be used to produce the back off timer value.



```
START

Initialize state:
Initialize parameters
set delay percentage to 0%
perform random back-off
execute back-off timer

while (back off timer! = expired)

        hold all data transmission

if (back off timer == expired)

        check missing acknowledgement counts

        if (missing acknowledgement count > count threshold)

                if (delay percentage == 50%)

                        delay percentage reach maximum value

                else

                        increase delay percentage by 10%
                        reset missing acknowledgement count to 0

        else

                if (acknowledgement last receive state = true)

                        if (delay percentage == 50%)

                                decrease delay percentage by 10%
                                reset missing acknowledgement count to 0

        perform back off timer adjustment according to delay percentages


perform clear channel assessment

        if (channel state == busy)

                perform channel back off

        else

                perform data transmission


        if (acknowledgement == received)

                is transmission success = true

        else

                increase missing acknowledgement counts by 1
                acknowledgement last receive state = false

STOP
```

Figure 1: Enhanced Back-Off Delay Management

The idea of this solution is to increase the probability of ZigBee's packet that can be allocated into the white space as shown in Figure 2. Therefore, a back off timer is adjusted for each time the ZigBee's packet (acknowledgment) collides with the Wi-Fi's packet. The packet will fit into the white space when the back-off timer reaches the optimal value.

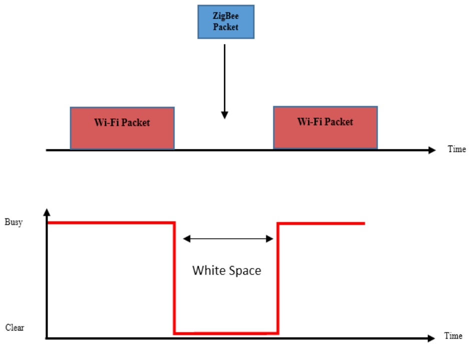


Figure 2: Channel White Space

III. Experimental Approach for Zigbee and Wi-Fi Coexistence Analysis

The study is conducted based on an experimental approach. We deployed MicaZ OEM (Figure 4) for this experiment. We also used packet generator tool to emulate Wi-Fi interference while MicaZ motes establishing a communication. This allows us to vary the interference levels to see its impact on ZigBee communication.

A. Hardware Setup

We setup a point to point communication between sensor node (Figure 3) and a base station. We also set-up an Access Point (Figure 5) in the ZigBee deployment area to create an interference issue face by ZigBee equipped system in real life. Table 1 and 2 below shows the MicaZ mote configuration for the experiments.

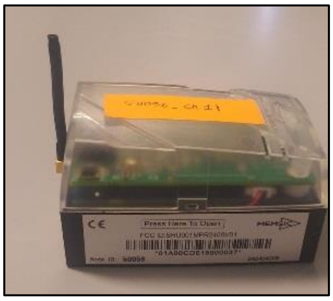


Figure 3: MicaZ Sensor Node (Radio Module with Sensor Board)

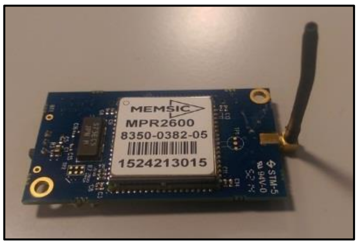


Figure 4: MicaZ OEM Edition Radio Module (MPR2600)

Figure 5: Wi-Fi Router TP-Link W8968 used in our experiment

Table 1
Parameter Set-Up of Sensor Node

Sensor Node Configuration	
Channel Assigned	20
Bandwidth Range	2.449 – 2.451 GHz
Packet Send Interval	5.5s
Transmit Power	0 dB (Max)
Route Mode	Low Power
Sensor Board Sampling Value	1000
Maximum Allowable Packet Size	65 bytes

Table 2
Wi-Fi Parameter Set-up

Wi-Fi Set-up Configuration	
Channel Assigned	9
Bandwidth Range	2.441 – 2.463 GHz
Transmit Power	20 dB
Bandwidth	20 MHz

B. Software / Tools

We used *Iperf 2.0* packet generator in an experiment involving Wi-Fi interference. *Iperf* is a tool used to measure maximum TCP bandwidth, allowing the tuning of various parameters and UDP characteristics. *Iperf* metrics in TCP are namely: time transfer and transfer rate while UDP metrics are namely: time transfer, transfer rate, bandwidth, jitter and packet loss. For our experiments, we used UDP packet to increase traffic load in the Wi-Fi connection.

We used one workstation PC equipped with Wi-Fi adapter as a server and one notebook as a client. The experiment with Wi-Fi interference is conducted with three different bandwidths which are 2,4 and 8 Mbit as shown in Table 3.

Table 3
Iperf 2.0 parameters

Packet Generator Configuration	
Channel Assigned	Iperf Packet Generator
Type of Packet Generated	UDP
Bandwidth	2 / 4 / 8 Mbit
Communication Setup	Client > Server Connection

We also used *Xsniffer* (MEMSIC) with sniffer node (Figure 6) to record all the ZigBee communications and also it`s node health state. *Xsniffer* is an application used to perform diagnostic for Wireless Sensor Network devices especially MicaZ. One MicaZ is assign as the sniffer node which intercept all communication between sensor node and base station. What is most important, this software able to record the transmission statistic which provides us important information like MicaZ mote transmission pattern, type of packet sent, size of the packet, number of packet loss, number of retransmission, number of hops and others.

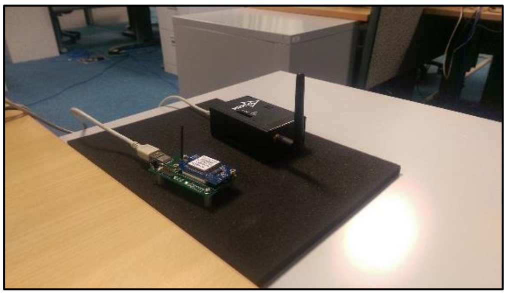


Figure 6: Sniffer node (Left) placed near the base station (Right) for better packet interception

C. Experiment Setup

Our experiment was performed with two categories where the first category of our experiment conducted with low Wi-Fi traffic in the deployment area. The other experiment conducted with moderate to high traffic volume. Each of categories will have three scenarios based on varies distance between the sensor node and the base station (Table 4). Same with the other categories which also execute with three scenarios so we can compare the ZigBee devices performance without and with Wi-Fi interferences with three different distances.

Table 4
Scenarios by Distances

Scenarios	
No of Scenario	Distance (Meter)
Scenario 1	3.35
Scenario 2	7.38
Scenario 3	12.40

The experiment area that we used to conduct experiment is 249.47 m^2 (square meters). Figure 7, 8 and 9 shows the location of sensor node based on scenarios. Wi-Fi router is place same location with the base station.

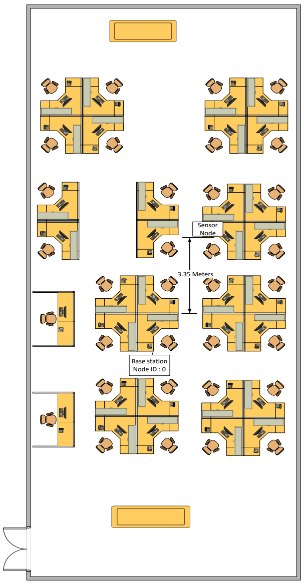


Figure 7: Scenario one with sensor node distance 3.35 meters

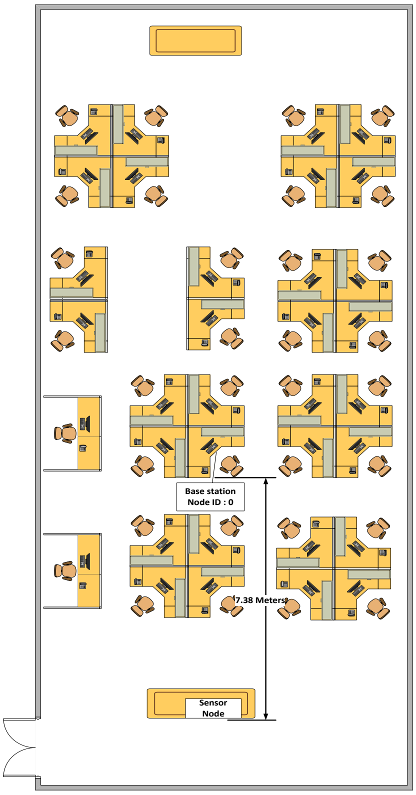


Figure 8: Scenario two with sensor node distance 7.38 meters

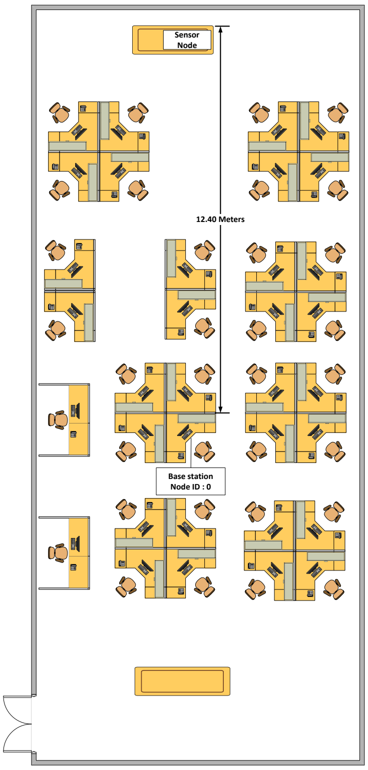


Figure 9: Scenario three with sensor node distance 12.40 meters

D. *Experiment Procedures*

Both of client and server computer will have *iperf* set-up. For our experiments, we use notebook (Asus N550JV) as our client and one workstation as server (Dell Precision T3600) (Refer Figure 10). For the server side, we configure it to receive UDP packets from the client continuously. While for client side, we configure the client to send UDP packet with 3 different bandwidths as mentioned before. The *iperf* packet generator will be executed concurrently with ZigBee experiment to reproduce the interference problem.

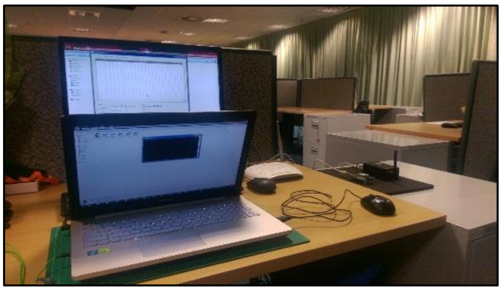


Figure 10: Client (Notebook) and Server (Workstation)

We run the experiments for the non-overlapping and overlapping channel for 20 trials each scenario in one category. Each trial, we conduct the experiment within 6 minute interval. Also, each experiment we enable data logging feature in *Xsniffer* application which allows us to measure Round Trip Time (RTT) of each packet sent from the sensor node to the base station.

E. *Analysis Metrics*

In analysis part, we need to measure average Round Trip Time (RTT) for each trial. We use basic Equation (1) to measure each packet RTT.

$$RTT = T_{ack} - T_{sent} \quad (1)$$

In Equation (1), we subtract the timestamp for received acknowledge (T_{ack}) of that packet with a timestamp of the packet when it sent from the sensor node (T_{sent}) to obtain single Round Trip Time. Moreover, average of Round Trip Time can be calculated by divide sum Round Trip Time with the sum of packet counts (Σ_{pkt_count}) as shown in Equation (2). Each of the average Round Trip Time for each trial from each scenario will be recorded. Performance comparison with each scenario can be compared to average Round Trip Time from each scenario obtained.

$$AVG_{RTT} = \Sigma_{RTT} \div \Sigma_{pkt\_count} \quad (2)$$

Other than Round Trip Time, we also measure the Packet Delivery Ratio (PDR) to see how bad can Wi-Fi interference affect the packet delivery in ZigBee. PDR is measured by identifying how many packets generated from the sensor node (ΣPkt_{sent}) is successfully received by the base station after the connection with base station established. The Equation (3) and (4), shows how we calculate the PDR in a percentage format.

$$\Sigma Pkt_{rcv} = \Sigma Pkt_{sent} - \Sigma Pkt_{loss} \quad (3)$$

$$PDR = (\Sigma Pkt_{rcv} \div \Sigma Pkt_{sent}) * 100 \quad (4)$$

The Transmission Efficiency is also taken into account. Transmission Efficiency is the measurement how many numbers of retransmission in one experiment because retransmission consumes more time and reduce battery lifetime the sensor node. Packet retransmission occurs when sensor node doesn`t receive an acknowledgment from the base station for a certain amount of time. After the acknowledgment timer had expired, sensor node will resent the packet for multiple times before it discarded the packet and count as packet loss. The higher the retransmission rate will lead to low transmission efficiency and vice versa. Equation (5) shows the calculation to obtain the transmission efficiency by utilizing number transmission and the total packet sent from the sensor node.

$$Efficiency = 100 - ((\Sigma Pkt_{xmit} \div \Sigma Pkt_{sent}) * 100) \quad (5)$$

Our analysis will use Round Trip Time, Packet Delivery Ratio and Transmission Efficiency to evaluate the ZigBee communication performance for the whole experiments.

IV. Conclusion

The new propose lightweight ZigBee protocol is managing the back off period in the current ZigBee CSMA-CA protocol. Alteration of CSMA-CA protocol is required due to an inefficient back off mechanism which led to high round trip time and also packet loss. An efficient of back off mechanism reduces the back-off delay in ZigBee communication thus minimizes the round-trip time delay. The experimental approach has been outlined to analyse the interference. The Algorithm is design to give us more solid analysis result in the experiment later. So, we realize that minimize coexistence interference between ZigBee and Wi-Fi can be quite challenging in Wireless Sensor Network, however it is worth to solve it. Fragmentation packet management also offer a better solution in managing packet structure for large type packet which reduce chance of packet collision. This is our next step once this research is completed.

Acknowledgment

The authors would like to acknowledge and thank Universiti Malaysia Sarawak for providing the funding for publication.

References

[1] Baig, M. M., & Gholamhosseini, H. Smart health monitoring systems: an overview of design and modelling. *Journal of Medical Systems, 37*(2), 2013, pp. 1-14.

[2] Hussain, A., Wenbi, R., da Silva, A. L., Nadher, M., & Mudhish, M, Health and emergency-care platform for the elderly and disabled people in the Smart City. *Journal of Systems and Software*, *110*, 2015, pp. 253-263.

[3] Das, D., Pal, A., Tewary, S., Chakraborty, S., & Gupta, S. D, A Smart and Wearable Cardiac Healthcare System with Monitoring of Sudden Fall for Elderly and Post-Operative Patients. *IOSR Journal of Computer Engineering (IOSR-JCE) Vol 16, Issue 2, Ver VIII,* Mar-Apr 2014, pp. 126-133.

[4] Dhar, S. K., Bhunia, S. S., & Mukherjee, N, Interference aware Scheduling of Sensors in IoT enabled Health-care monitoring system. In Emerging Applications of Information Technology (EAIT), 2014 Furth International Conference of IEEE, pp. 152-157.

[5] Kim, Y., Lee, S. and Lee, S, Coexistence of zigbee-based wban and wifi for health telemonitoring systems. *IEEE journal of biomedical and health informatics*, *20*(1), 2016, pp. 222-230.

[6] Dahham, Z., Sali, A. and Ali, B.M, An efficient backoff algorithm for IEEE 802.15. 4 wireless sensor networks. *Wireless personal communications*, *75*(4), 2014, pp. 2073-2088.

[7] Yazdi, E. T., Willig, A., & Pawlikowski, K, Frequency adaptation for interference mitigation in IEEE 802.15. 4-based mobile body sensor networks. *Computer Communications*, *53*, 2014, pp. 102-119.

[8] Tytgat, L., Yaron, O., Pollin, S., Moerman, I., & Demeester, P, Analysis and experimental verification of frequency-based interference avoidance mechanisms in IEEE 802.15. 4. *IEEE/ACM Transactions on Networking*, *23*(2), 2015, pp. 369-382.

[9] Du, T., Wang, Z., Makrakis, D., & Mouftah, H. T, Protective Dummy-byte Preamble Padding for improving ZigBee packet transmission under Wi-Fi interference. In *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, March 2015, pp. 1918-1923.

[10] Du, T., Wang, Z., Makrakis, D., & Mouftah, H. T, Adaptive Preamble Padding with Retransmission Control for ZigBee network under Wi-Fi interference. In 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), August 2015, pp. 981-986.

[11] Ishida, S., Tagashira, S., & Fukuda, A, AP-assisted CTS-blocking for WiFi-ZigBee Coexistence. In 2015 Third International Symposium on Computing and Networking (CANDAR), December 2015, pp. 110-114.

[12] Lee, T. H., Hsieh, M. C., Chang, L. H., Chiang, H. S., Wen, C. H., & Yap, K. M, Avoiding collisions between IEEE 802.11 and IEEE 802.15. 4 using coexistence inter-frame space. In *Advanced Technologies, Embedded and Multimedia for Human-centric Computing* (pp. 1185-1193). Springer Netherlands.

[13] Cherkaoui, Soumaya, "Adaptive 802.15. 4 backoff procedure to survive coexistence with 802.11 in extreme conditions." In *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 556-561. IEEE, 2016.

[14] Yuan, W., Wang, X., Linnartz, J. P. M., & Niemegeers, I. G, Coexistence performance of IEEE 802.15. 4 wireless sensor networks under IEEE 802.11 b/g interference. *Wireless Personal Communications*, *68*(2), 2013, pp. 281-302.

[15] “Demystifying 802.15.4 and ZigBee” ZigBee White Paper by Digi.