



Enabling Coexistence of ZigBee and WiFi

Sunil Jacob, PhD
Professor, ECE Department
SCMS School of Engineering and Technology
Karukutty, Angamaly, Cochin,
Kerala

Priyanka Ravi
Mtech student
SCMS School of Engineering and Technology
Karukutty, Angamaly, Cochin,
Kerala

ABSTRACT

Spectrum scarcity is known to be main obstacle to scaling of wireless network capacity. Spectrum sharing is a solution to this problem. The unlicensed ISM band is getting crowded by WLAN and WPAN users and devices. Spectrum sharing within the devices of same network is not a problem. But coexistence of WLAN and WPAN (eg: WiFi and ZigBee) is a challenging problem. Spectrum sharing among these networks will surely improve spectrum utilization. WiFi and ZigBee uses 2.4 GHz ISM band. Different methods had been adopted to improve the coexistence of ZigBee and WiFi. Some methods are discussed here. Each of them has some disadvantages. To tackle these challenges a new system called WiseBee is used which help in the coexistence of ZigBee and WiFi. It uses a single antenna sink without changing WiFi and ZigBee design. The sink works in following steps: The signal from the RF front end will be processed firstly. If the WiFi interference is detected, system will process the WiFi decoding and use decoded data for accurate channel coefficient estimation. After that, the WiFi signal is removed by interference cancellation module, where the residual signal can be used for ZigBee decoding. Then we find out a channel for ZigBee transmission.

General Terms

Coexistence, interference recognition, channel selection

Keywords

802.11, 802.15.4, interference, coexistence, spectrum sharing, heterogeneous networks, WiFi, ZigBee

1. INTRODUCTION

Spectrum scarcity is known to be main obstacle to scaling of wireless network capacity. Spectrum sharing is a solution to this problem. The ISM spectrum is so crowded that it is shared by different wireless networks. Allowing spectrum sharing among these networks will surely improve spectrum utilization. However it also creates great challenge, especially the coexistence of incompatible MAC/PHY protocols. Two such networks, WiFi (IEEE 802.11) and ZigBee (IEEE 802.15.4), that operate in the 2.4 GHz license-exempt band have received considerable attention. WiFi is designed for Internet access, video streaming, etc., whereas ZigBee targets low duty-cycle monitoring and control applications such as healthcare and home/industrial automation. They are expected to run simultaneously in close proximity, e.g., inside a residential or office or hospital building. However, recent measurement studies have shown that ZigBee's performance is severely degraded in the presence of moderate to high WiFi traffic [9]. This can cause severe interference and can also reduce communication reliability [1], [5], [6].

Several types of solutions have been proposed to address the cross technology coexistence. They are basically divided into

three categories. The first category is to do centralized frequency planning beforehand; separating different technologies in nonoverlapping spectrums. The second approach requires the wideband devices to vacate the spectrum used by narrowband devices. The third approach uses different ZigBee protocols to ensure ZigBee networks interference free from WiFi networks in time domain.

Unfortunately, such solutions cannot be deployed in urban monitoring scenario for several reasons. First WiFi networks in urban are uncontrolled and unpredicted which makes centralized coordination and modification of WiFi devices infeasible. Secondly protocol solutions either consume computational resource or require network coordination leading to great overhead. Thirdly, some solutions require re-programming of ZigBee nodes and reduce the performance of WiFi networks, which are not feasible in large-scale and long-term urban monitoring scenario [15].

Above mentioned challenges can be tackled using WiseBee system. It uses a single antenna sink without changing WiFi and ZigBee design [1]. The sink works in following steps: The signal from the RF front end will be processed firstly. If the WiFi interference is detected, system will process the WiFi decoding and use decoded data for accurate channel coefficient estimation. After that, the WiFi signal is removed by interference cancellation module, where the residual signal can be used for ZigBee decoding. Then we find out a channel for transmission.

We develop following contributions in this paper.

- We revisit the coexistence problem in ZigBee and WiFi.
- We propose an interference removal scheme for coexistence of ZigBee and WiFi.
- We also propose a method to find out the channel for the transmission of ZigBee data.

The remainder of the paper is arranged as follows. In section 2, we provide background on ZigBee and WiFi systems. Section 3 analyses different types of interference. We discuss about related works in section 4. In section 5 we discuss about WiseBee system. We discuss about simulations in section 6, while section 7 discuss about future work and conclusion. The section 8 concludes the paper.

2. ZIGBEE VERSUS WIFI

WiFi and ZigBee share the same 2.4 GHz frequency band. Such technologies usually operate in proximity and have to co-exist with each other. WiFi uses same frequency band that is used by ZigBee however WiFi uses higher power level, compared with ZigBee. The characteristics of both differ greatly resulting in asymmetric coexistence problem. The

output power of 802.15.4 device is as low as 0dBm where as the output power of 802.11 devices is 15dBm or above. When both are used together ZigBee yield a smaller spatial footprint and hence less visible to WiFi [1]. So ZigBee presence is not sensed by WiFi and can lead to collision. The sensing slot for 802.11 networks is 20 μ s while 802.15.4 sensing slot is 320 μ s. When sensing a busy channel ZigBee resumes its backoff and clear channel assessment and then aborts after five consecutive attempts. WiFi remains in backoff and sensing until it finds an idle slot for transmission. Also each backoff in ZigBee consists of two contention windows ie. transmitter ensures an idle channel for two slots before sending data where as WiFi needs only one idle slot. Since WiFi clear channel assessment duration is much shorter, WiFi transmitter can easily pre-empt ZigBee. When ZigBee and WiFi use the channel at the same time, interference problem appears which causes loss of data being transmitted. This will result in retransmission in both ZigBee and WiFi until successful transmission is achieved [14]. This causes delay and mitigation in delivery ratio for both technologies. Moreover ZigBee need to wait longer to get free medium for transmission and with expected packet loss and retransmission faster draining of sensor battery is expected [7].

The interference between WiFi and ZigBee has been extensively studied in both the industry and the research communities. Under light WiFi traffic, ZigBee suffer less from collision with WiFi and can recover loss via retransmission. However, under moderate to high WiFi traffic, ZigBee performance is severely degraded [12]. With the proliferation of WiFi devices and high-rate applications, the amount of WiFi traffic in a typical home or enterprise environment will keep increasing, thus severely affecting the reliability of ZigBee WPANs for monitoring and control applications.

On the other hand, ZigBee seldom interferes with WiFi since it targets low duty-cycle applications with low channel occupancy. Moreover, WiFi has much higher transmit power, which forces ZigBee nodes to backoff, and can dominate the ZigBee interference.

3. TYPES OF INTERFERENCE

Basically there are two types of interference. They are symmetric interference and asymmetric interference [1]. In symmetric interference, due to ZigBee activities the WiFi transmitter will go to backoff. Here header of ZigBee packet is corrupted. Asymmetric interference happens when the ZigBee power is too low to be detected by WiFi. In this case WiFi activities can corrupt any bit of ZigBee packet [10]. Two methods can be used to avoid such interference-Static channel assignment and dynamic channel assignment. In static channel assignment 802.11 occupies fixed number of channels. ZigBee uses those channels which are unused by WiFi. But this may not work as planned due to the high WiFi traffic. In dynamic channel assignment scheme different nodes in a sensor network or same nodes over different points in different time will use different channels to avoid interference from nearby WiFi sources. But it has two challenges. Initially the WiFi traffic has to be detected and then coordinate channel selection among senders and receivers.

3.1 Spatial collision hazards

3.1.1 Asymmetric Interference

Due to the difference in transmit power levels, there exists a “gray region” where ZigBee can hear WiFi, but WiFi is

unaware of ZigBee and can arbitrarily interrupt its transmission so called asymmetric interference. To combat asymmetric interference, a simple solution is to employ a proxy signaler with higher transmit power to send the busy tone [14].

3.1.2 Hidden Terminal

It occurs when WiFi and ZigBee transmitter cannot hear each other. It can also be alleviated using a proxy signaler visible to WiFi transmitter.

3.2 Temporal Collision Hazards

3.2.1 Partial Carrier Sensing

In addition, collision can occur in the time domain when a WiFi packet is partially sensed by ZigBee and is insufficient to trigger its backoff. This happens when WiFi packets are partially sensed during the long sensing period of ZigBee, when WiFi starts transmission near the end of the ZigBee sensing duration [14].

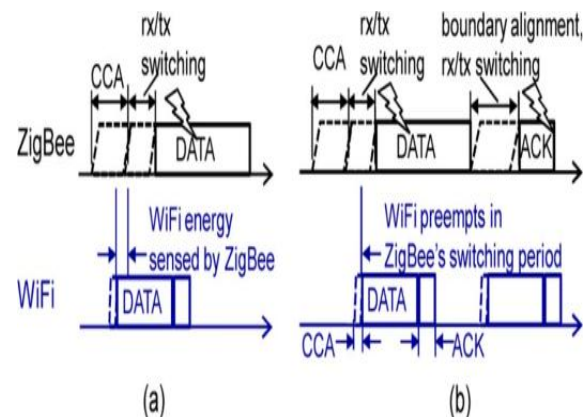


Fig 1: Collision hazards in the temporal domain. (a) Partial carrier sensing. (b) WiFi pre-emption

3.2.2 Non-CSMA Transmission and WiFi Pre-emption

Packets sent without sensing, such as GTS, acknowledgement and beacons will be corrupted when encountering an ongoing WiFi session.

Secondly WiFi can pre-empt a ZigBee transmission when its carrier sensing falls in the receiver/transmitter switching time of ZigBee transmitters. These two cases are essentially due to the long response time of ZigBee [14].

4. RELATED WORK

Different mechanisms were adopted to improve the coexistence of ZigBee and WiFi.

1) In case of symmetric interference due to ZigBee activities the WiFi transmitter will go to back off. Here header of ZigBee packet is damaged. In symmetric region, damage occurs to the packet header. To compensate this simple method can be used. In this method multiple headers can be transmitted in a single packet. So even if first header is damaged, second header will be received correctly. In asymmetric region forward error control code can be used to correct bit errors. RS code is best against burst errors.

These techniques are integrated in to a protocol called Buzz-Buzz [10]. It can improve the packet delivery rate by about 70% and also reduces the packet retransmission rate. So the

interference of ZigBee with WiFi can be reduced. In this method interference between WiFi and ZigBee is discussed in bit level. In FEC, transmitter applies an error correction code to the data to be transmitted. So the message is converted to an encoded form. The receiver then applies the reverse transformation to recover the original message from the encoded message.

2) The characteristics of ZigBee and WiFi differ greatly resulting in asymmetric coexistence problem. To begin output power of 802.15.4 device is as low as 0dBm where output power of 802.11 devices is usually 15dBm or above. Next although both technique require a listen before send prior to every transmission, the sensing slot for 802.11 is 20 μ s while 802.15.4 slot is much larger at 320 μ s. Experimentally it was observed that while doing a listen before send it can harm 802.11 transmission. Collision between the 802.15.4 packet and 802.11 packet occurs only at the beginning of 802.11 packet. Indeed during the remainder of the 802.11 packet no 802.15.4 transmission happen proving that 802.15.4 does backoff for 802.11. However the responsiveness of 802.15.4 sensing is too slow to avoid collision with start of an 802.11 packet. 802.15.4 backoff sensing slot is 320 μ s which is large compared to 20 μ s sensing slot for 802.11. An 802.11 packet starting during sensing slot will not be detected quickly and therefore each network listen before send algorithm is insufficient to avoid inter network collision.

3) Metronome is another system which allows heterogeneous networks to coexist well [8]. Metronome provides a flexible and expressive policy language that allows network operator to specify constraints on receiver performance metrics such as throughput or loss rate. Metronome thus configures each transmitter with appropriate channel, bandwidth, transmission power settings automatically.

Metronome implements three concepts to detect signals and interference across heterogeneous networks:

- i) a flexible policy frame work for computing good transmitter settings.
- ii) a matched filter-based detection for separating out signal power of one particular network from interference of all networks.
- iii) mobile monitors for collecting multiple spatially distributed samples of signals and interference levels around the receiver.

Metronome uses a monitor. The monitors continuously sample the energy across the band and use a parameterized matched filter for separating signal power of different networks and periodically send the information to the policy server. The policy server uses this information to calculate the interference contributions of each transmitter. The policy server then runs an optimization procedure. Using this individual transmitter interference information it determines the best transmit power and channel settings for the participating transmitters. The server sends these settings to the transmitters, which modify their behavior accordingly. There are few challenges in Metronome. The filtering technique must be flexible. Secondly monitor must be able to capture interference levels experienced at receivers. But because of RF propagation characteristics, the interference measurement at monitor can differ from interference at the receiver. Thirdly mobile monitor is used to solve this. When mobile monitors are used, expense will be more

4) Adaptive radio channel allocation is used for supporting coexistence of 802.15.4 and 802.11 [2]. The basic idea of this scheme is to make the interference affected nodes to switch to a new clean channel. When packet is entering or leaving to the interference part of the routing path, radio channel is switched to a new channel or back to the old channel. The overhead for switching radio channel is very small. The adaptive scheme improves the performance and is especially advantageous for large scale multi-hop sensor networks.

Each node holds a switching table and all the nodes have the same entries in their table at the beginning. When interference is detected in this area, the node looks up the switching table to find a new channel. The same table is used to go back to previous channel, when interference is finished.

The adaptive scheme uses three mechanisms: Interference Detection, Group Formation, and demolition. Each 802.15.4

node checks for interference on the current channel using the Interference Detection. It can be called periodically or on demand. In case of interference, the node enters into Group Formation (GF). During GF, the nodes in the same interference area form a group and a new channel is selected as the current channel for the group. When the current interference is diminished, the group removed and its current channel is switched back to the previous one.

5) A distributed adaptation strategy is proposed to minimize the impact of 802.11 interference [3]. Here a distributed algorithm is used to optimize the ZigBee performance under varying 802.11 interference. In the first method used here, nodes randomly pick a channel every period. Packets are then forwarded to any other node within the communication range that happened to pick the same channel. In the second method a scanning based approach is used. Each time current channel and the channel randomly selected is considered and its performance is accessed. Then the channel with good performance is always considered. In the second method it need to scan current channel and an extra channel. So energy cost is doubled.

6) A mechanism called CCS is used. CCS stands for cooperative carrier signaling which enables coexistence of ZigBee and WiFi. Here a separate node called signaler is used. Signaler have higher power than normal ZigBee transmitter. So WiFi can detect ZigBee transmitter's presence by detecting busy tone. The busy tone persists throughout the data and acknowledgement round trip. The main difficulty of CCS is that signalers busy tone should occur concurrently with data transmission. To overcome this difficulty a temporal channel hopping mechanism is used [13], [14].

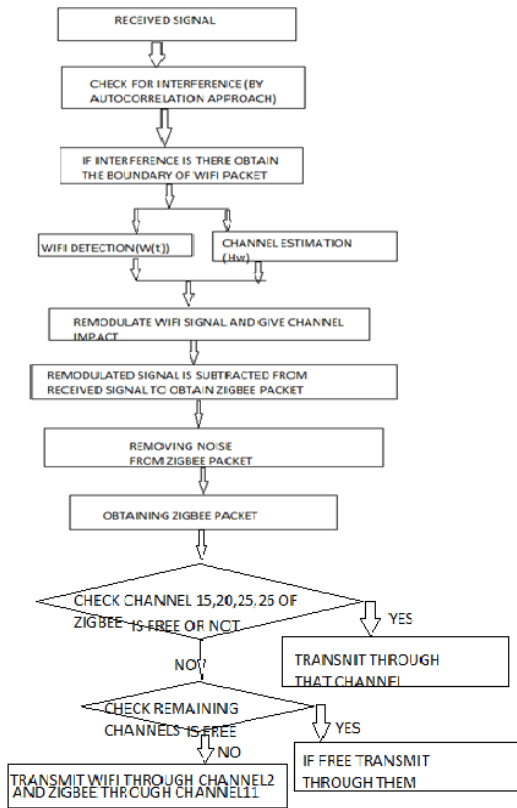


Fig 2: Steps involved in WiseBee system

5. DESIGN

In this section we present an overview of WiseBee system. In this system ZigBee signal can be decoded in presence of WiFi interference. Here initially RF front end receives the ZigBee packet with interference. Then the system checks whether WiFi interference is present or not. It is done by using autocorrelation approach. The autocorrelation output can be represented as

$$C = \sum_{K=0}^{L-1} r(n+k)r^*(n+k+L)$$

where r^* is the conjugate of the t^{th} sample. In order to obtain a normalized result, we need to find

$$P = \sum_{K=0}^{L-1} r(n+k+L)r^*(n+k+L)$$

$$K=0$$

The final autocorrelation result is

$$Mn = (C)^2 / (P)^2$$

When WiFi packet is there the value of Mn will be high. After identifying that WiFi packet is present, next step is to obtain the boundary of the WiFi packet. Boundary can be easily obtained because there is much difference in the power of WiFi and ZigBee packet. Once the boundary of the WiFi packet is obtained initially we consider ZigBee signal as background noise and standard WiFi decoder is used to decode the WiFi packet. Then the channel coefficient is also estimated. Then WiFi signal is remodulated and channel impact is applied to it. Thus obtained signal is then subtracted

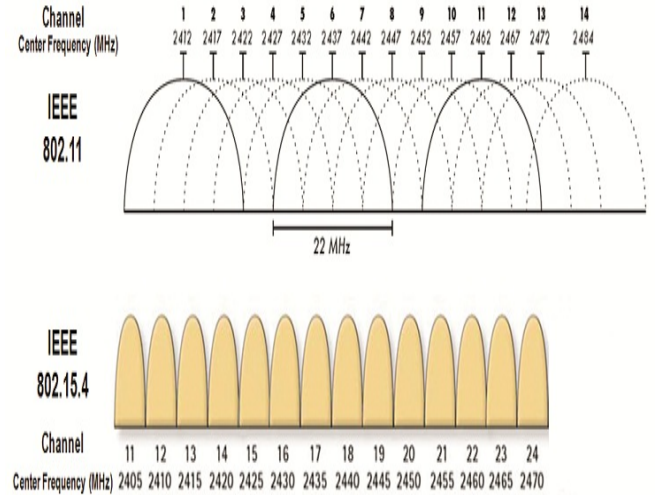
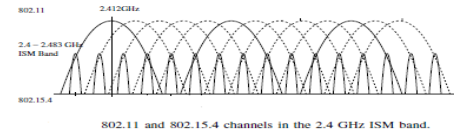


Fig 3: 802.11 and 802.15.4 channels in 2.4GHz

from the mixed signal. From the remaining signal we can use standard ZigBee decoder to extract ZigBee packets.

The next step is to transmit the ZigBee packet. Fig 3 shows WiFi and ZigBee channels in 2.4 GHz ISM band. Channel 1, 6 and 11 are the nonoverlapping and commonly used channels of WiFi. Channels 15, 20, 25 and 26 of ZigBee are those channels which come outside nonoverlapping channels. So initially we check whether these channels are free or not. If any of these channels are free, we transmit using that channel. If none of these channels are free, we then check the remaining channels of ZigBee i.e. channel 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24. If any of these channels are free, we transmit through it, otherwise we adopt another method. Along with the ZigBee packet we also have WiFi packet. So we are sending this WiFi packet through channel 2 of WiFi. So channel 1 of WiFi will be free. Within the channel 1 of WiFi comes the channel 11 of ZigBee. So ZigBee packet can be transmitted through channel 11 of ZigBee. Here we selected channel 2 of WiFi because the number of overlapping WiFi channels are less than if we move to the center. Here the main advantage is that we have WiFi packet with us. So it can be used to transmit the ZigBee packet. WiFi packet will serve the purpose of a jamming signal and so ZigBee packet can be transmitted without WiFi interference.

6. SIMULATIONS

In this section we show the simulations obtained. Initially we created ZigBee in simulink and obtained BER. ZigBee with WiFi as interference was also done in simulink and BER was obtained.

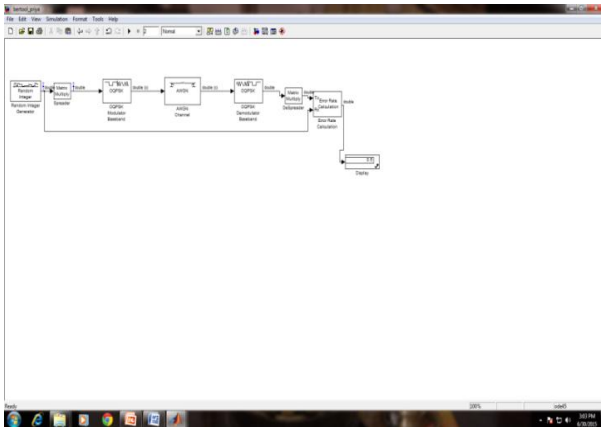


Fig 4: Simulink block for ZigBee

Matlab codes were also generated for ZigBee. There the number of errors obtained was 55. When coding was done for ZigBee with WiFi interference the number of errors increased to 72. From the simulations done in Simulink and Matlab it is very clear that ZigBee performance is getting degraded due to the presence of WiFi. So WiseBee system is used. When WiseBee system is used, we are able to obtain the ZigBee packet from the mixed signal. After doing the coding for WiseBee system the number of errors has been reduced to 61. Figure 8 gives command window output for WiseBee system.

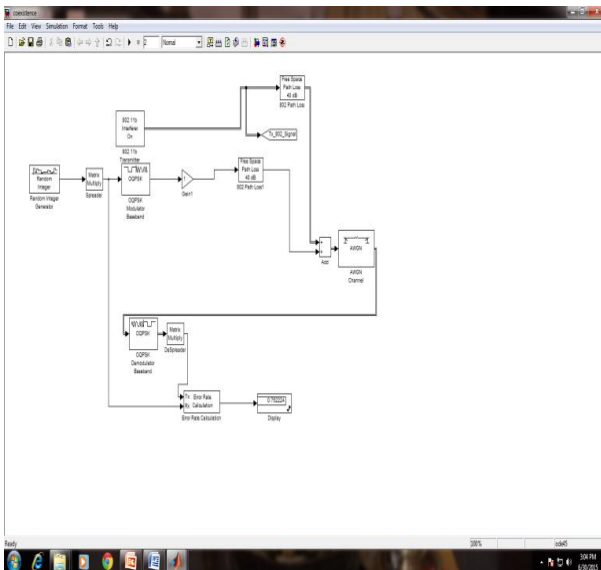


Fig 5: Simulink block for ZigBee with WiFi as interference

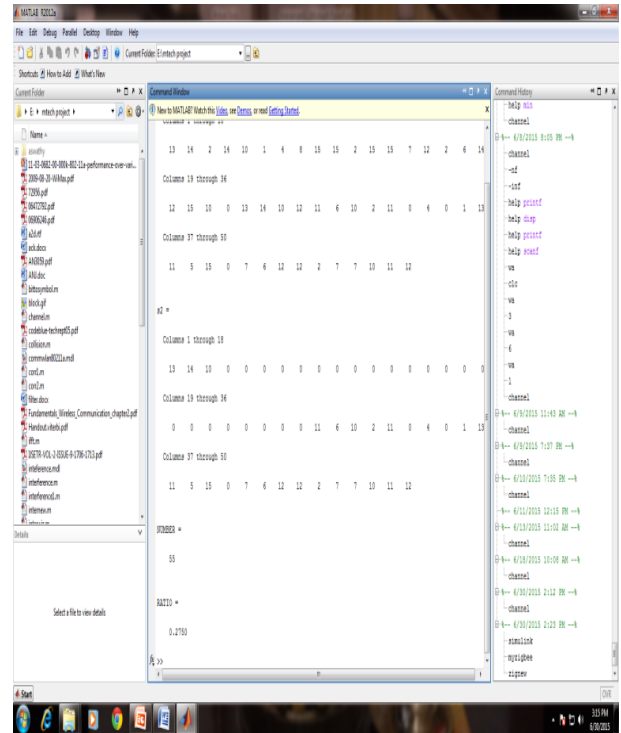


Fig 6: Command window output for ZigBee

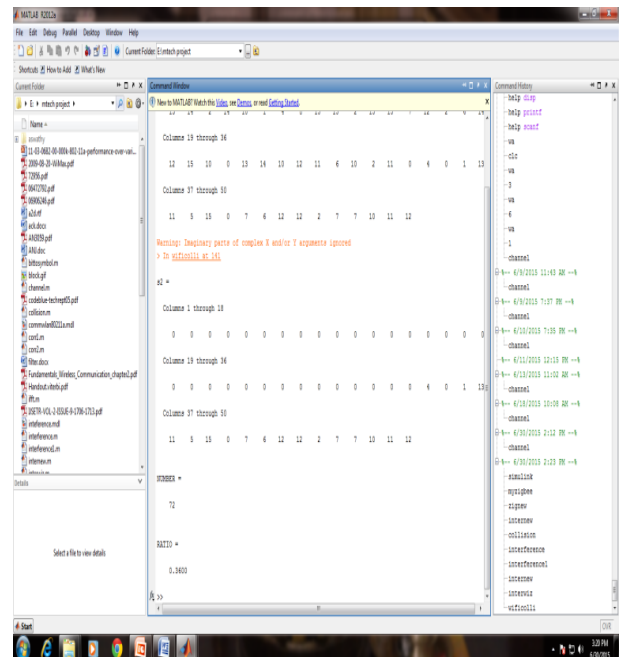


Fig 7: Command window output for ZigBee with WiFi as interference

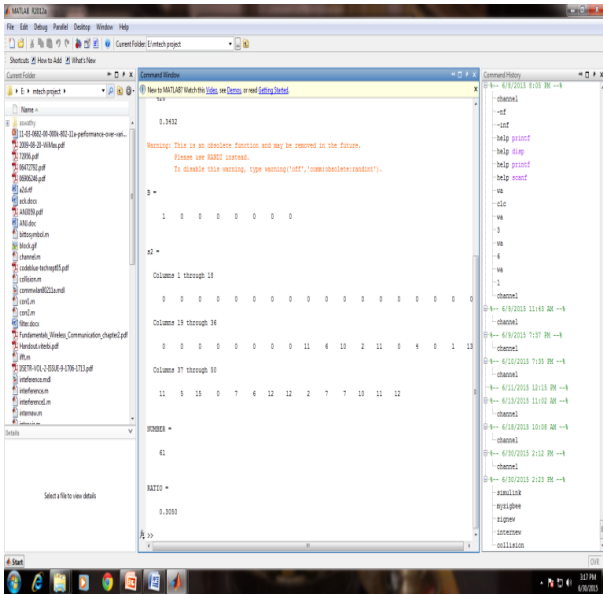


Fig 8: Command window output for Wise Bee system

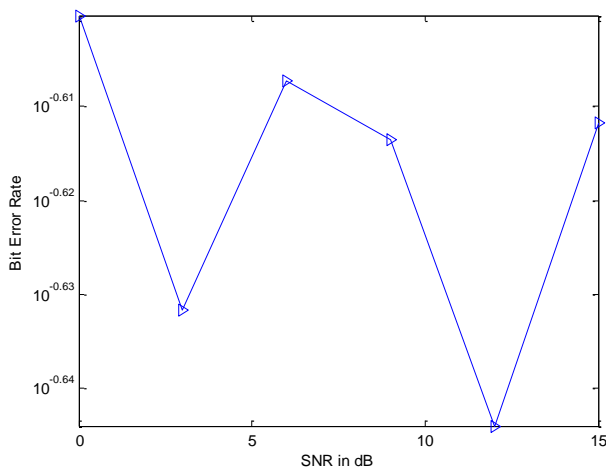


Fig 9: BER VS SNR for ZigBee

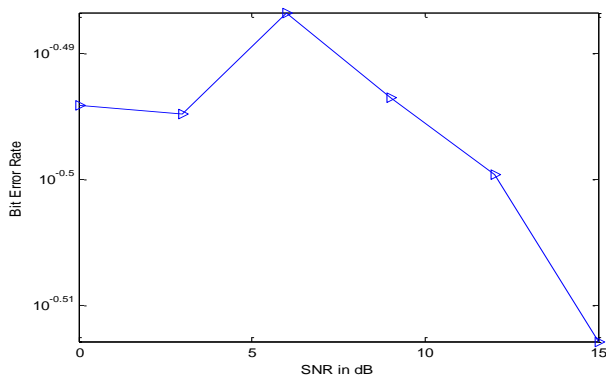


Fig 10: BER VS SNR for ZigBee with WiFi as interference

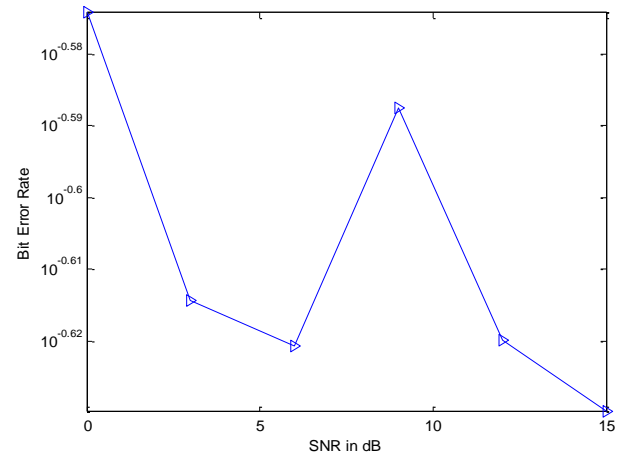


Fig 11: BER VS SNR for Wise Bee system

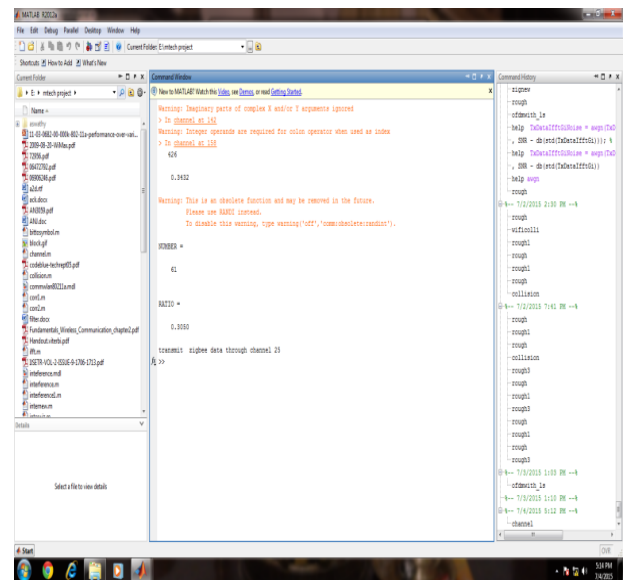


Fig 12: Command window output showing transmission of ZigBee packet

In a communication system quality of a transmission is usually quantified by BER or PER.

$$\text{BER}=1-(\text{NRX}/\text{NTX})$$

NRX is the total number of correctly received bits and NTX represents total number of transmitted bits. PER is

the ratio of the incorrectly transferred data packets divided by number of transferred packets.

$PER=1-(1-BER)^N$ where N is the number of bits in packet. Here we have plotted BER VS SNR for ZigBee, ZigBee with WiFi as interference and for WiseBee system.

By all these simulations it is very clear that in case of WiseBee system, we can obtain the ZigBee packet from mixed signal and BER can be reduced .After obtaining the ZigBee packet we then check the channel for transmission of ZigBee packet and found that channel 25 is free for transmission. Figure 12 shows the channel obtained for the transmission of ZigBee packet.

7. DISCUSSION AND FUTURE WORK

From the above simulations it is very clear that by using WiseBee system, we are able to obtain ZigBee packet from the mixed signal and BER has been reduced. Here after we have obtained the ZigBee packet, we are searching a channel for ZigBee transmission. If none of the channels are free, we transmit WiFi packet which we have through channel 2 of WiFi. So anyway channel 1 of WiFi will be free. So ZigBee packet will be transmitted through ZigBee channel 11 because this channel comes within channel 1 of WiFi. Here main advantage is that we don't want to find out another jamming signal to make other WiFi users aware of ZigBee transmission. So our ZigBee packet is anyway protected from other WiFi transmission. All we discussed here is focussed on one hop network. Extension of it to multihop can be done in future. Also the WiFi packet which we obtained from mixed signal have more errors compared to original WiFi packet. Here greater importance is given to ZigBee packet. Here if we are able to reduce errors in WiFi packet we will be able to recover WiFi packet with much throughput improvement. It can be done as the future work.

8. CONCLUSION

Prior studies have revealed that ZigBee performance is getting degraded due to the presence of WiFi. In this paper we suggested a new system called WiseBee system in which we are able to recover ZigBee packet from the collided signal of ZigBee and WiFi packet. Also we are finding a channel for transmission of ZigBee packet without WiFi interference. Our evaluations have shown that WiseBee system can improve the throughput for ZigBee networks. Our future work is to extend the system to multihop.

9. REFERENCES

- [1] Howitt and J. Gutierrez, "IEEE 802.15.4 low rate wireless personal area network coexistence issues," in *Proc. IEEE Wireless Commun. Netw. (WCNC 2003)*, pp. 1481–1486.
- [2] C. Won J H Youn, H. Ali, H. Sharif and J. Deogun, "Adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b," in *Proc IEEE VTC*, 2005, Vol.4; pp. 2522-2526.
- [3] S. Pollin, M. Ergen, M. Ergen, M. Timmers, L. Van Der Perre, F. Catthoor, I. Moerman, and A. Bahai, "Distributed cognitive coexistence of 802.15.4 with 802.11," in *Proc Crowncom*, 2006, pp.1-5.
- [4] M. Petrova, L. Wu, P. Mahonen, and J. Riihijarvi, "Interference measurements on performance degradation between collocated IEEE 802.11g/n and IEEE 802.15.4 networks," in *Proc ICN*, 2007, p.93
- [5] R. Gummadi, D. Wetherall, B. Greenstein and S. Seshan, "Understanding and mitigating the impact of RF interference on 802.11 networks," in *Proc ACM SIGCOMM*, 2007, pp.385-396.
- [6] S. Pollin, I. Tan, B. Hodge, C. Chun, and A. Bahai, "Harmful coexistence between 802.15.4 and 802.11: A measurement-based study," in *Proc. CrownCom*, 2008, pp.1-6.
- [7] R.C Shah and L. Nachman, "Interference detection and mitigation in IEEE 802.15.4 networks," in *Proc ACM/IEEE ISPN*, 2008, pp. 157
- [8] R Gummadi, H. Balakrishnan, and S. Sehan, "Metronome: coordinating spectrum sharing in heterogeneous wireless networks," in *Proc. 1st COMSNETS* 2009, pp. 157-166.
- [9] J-H Hauer, V. Handziski and A. Wolisz, "Experimental study of the impact of WLAN interference on IEEE 802.15.4 body area networks," in *Proc EWSN*, 2009, pp.17-32.
- [10] C-J .M. Liang, N.B Priyantha, J. Liu, and A. Terzis, "Surviving WiFi interferences in low power ZigBee networks," in *Proc. ACM Sen Sys*, 2010, pp.309-322.
- [11] Choi, J. Jain, M., Srinivasan, K. Levis, P., and Katti. S, "Achieving single channel full duplex wireless communication," in *Proc. ACM Mobicom* (2010), 1-12.
- [12] Peizhong Yi, Abiodun Iwayemi, Chi Zhou, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications" *IEEE Transactions on smart grid*, Vol. 2, No.1, March 2011.
- [13] X. Zhang and K. G. Shin, "Enabling coexistence of heterogeneous wireless systems: case for ZigBee and WiFi," in *Proc. ACM MobilHoc*, 2011.
- [14] XinYu Zhang and Karang G. Shin, "Cooperative carrier signaling: Harmonizing coexisting WPAN and WLAN devices," *IEEE Transactions on networking*, vol.21, no.2, April 2013.
- [15] Yubo Yan and Panlong Yang, "WizBee: Wise ZigBee coexistence via interference cancellation with single antenna," *IEEE Transactions on Mobile Computing*, 2013.