Performance Evaluation of Zig Bee Using Multiple Input Single Output (MISO) Architecture in the Secured Environment

Hari Kumar Choudhari, Akhilesh A. Waoo, P. S. Patheja, Sanjay Sharma

Abstract: ZigBee is a protocol stack created specifically for control of sensor networks which is built on IEEE 802.15.4, this standard works for low data rate wireless personal area networks (WPAN). The IEEE 802.15.4 standard works on PHY and MAC Layer. The IEEE 802.15.4 has become the preferable PAN system for wireless sensor networks and many software and hardware platforms are based on it. The implementation and performance analysis of this standard is needed to understand the conceptual limitations of it. This standard is designed for low data rate, low power consumption, long battery life. The implementation & performance analysis of this standard is needed to understand the conceptual limitations of it. In this paper we have tried to improve Error rate performance and other affected factors of Zigbee Personal Area Network (PAN) using multiple transmitters on existing system with OQPSK modulation in AWGN channel environment..Here in ZigBee we are applying MISO architecture with ECC 160 Encryption/Decryption method. The idea to use both of the schemes to apply in the IEEE 802.15.4 standard comes from that ECC 160 has features of low power consumption, more enough security and very less complexity as compare to RSA 1024, AES and IBE. The Multi transmitter scheme consumes high power compare to existing system. Hence we got a solution for that to save some amount of energy in the ZigBee Upper Layer. From the simulation results we have found that our proposed multiple transmitters scheme (MISO) gives very better results on low SNR values comparatively with the existing Single Input Single Output (SISO) approach together with the ECC 160 Encryption / Decryption in ZigBee based wireless sensor network.

Keywords - MISO, ZIGBEE, Physical Layer, OQPSK, BER, SNR. ECC 160

I. INTRODUCTION

ZigBee is a specification for a suite of high level communication protocols based on the IEEE 802.15.4 physical and MAC layers. The specification is developed by a group of industry players, the ZigBee Alliance. Some of the commercial applications of WSNs using ZigBee are in the area of home and building automation, remote control or health care monitoring [2] IEEE 802.15.4 Standard provides for very low complexity, very low cost, very low power consumption, and low data rate wireless connectivity among low-cost devices.

The data rate is high enough (250 kb/s) to meet a set of applications but is also scalable down to the needs of sensor and automation requirements (20 kb/s or below) for wireless communications. In addition, one of the alternate PHYs provides precision ranging capability that is accurate to one meter. Multiple PHYs are defined to support various frequency bands including [1]

i. 868–868.6 MHz
ii. 902–928 MHz
iii. 2400–2483.5 MHz
iv. 314–316 MHz, 430–434 MHz, and 779–787 MHz band for LR-WPAN systems in China
v. 950–956 MHz in Japan.

The major standardization bodies in the WSN area are the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF) and the HART communication foundation. Notable standards and specifications are:

A. IEEE 802.15.4 Standard:

This standard [4] specifies the PHY and MAC layer for low-rate WPANs. Many platforms are based on this standard and other specifications, such as ZigBee and wireless HART specifications, are built on top of the standard covering the upper layers to provide a complete networking solution. Some of the main characteristics of the IEEE 802.15.4 are[15]:

- 250 kbps, 40 kbps and 20 kbps data rates.
- Two addressing modes, 16-bit short and 64-bit IEEE addressing.
- CSMA-CA channel access.
- Automatic network establishment by the coordinator of the network.
- Power management control.
- 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz ISM band and one channel in the 868 MHz band.

B. Wi-Fi Compatibility:

The 2.4 GHz band, which ranges from 2400 MHz to 2483.5 MHz, is a worldwide band allocated to wireless LAN devices governed by IEEE 802 standards:

- *IEEE 802.11 – WiFi standard*
- *802.15.1 – Bluetooth*
- *802.15.4 – ZigBee.*

Manuscript published on 30 May 2013.
***Correspondence Author(s)**

Hari Kumar Choudhari, Department Computer Science & Engineering, Rajiv Gandhi Prodhoyogiki Vishwavidhyalaya, Bhopal, Madhya Pradesh India.

Prof Akhilesh A. Waoo, Department Computer Science & Engineering, Rajiv Gandhi Prodhoyogiki Vishwavidhyalaya, Bhopal, Madhya Pradesh India.

Dr. P S Patheja, Department Computer Science & Engineering, Rajiv Gandhi Prodhoyogiki Vishwavidhyalaya, Bhopal, Madhya Pradesh India.

Dr. Sanjay Sharma, Department Computer Science & Engineering, Bhopal,Madhya Pradesh, India.

The above standards cover LAN and MAN carrying variably sized packets. They find the no. of channels that devices can use in the 2.4GHz band and together they appear to coexist happily. ZigBee devices can use up to 16 separate 5MHz channels (nos. 11-26) in the 2.4 GHz band, almost all the channels do not overlap with channels occupied by 802.11 and Wi-Fi network. What's more, as considered above, ZigBee automatically retransmits data end-to-end in the event of interference. And even then, very little data is retransmitted. With its exclusive focus on sensors and controls, ZigBee should not be affected by similar wireless technologies with different purposes.[7]

Yet concerns have been voiced that despite efforts made by standardisation bodies to ensure smooth coexistence, communication technologies transmitting at very different power levels could interfere with each other. Questions have in particular been raised over how Wi-Fi might affect ZigBee when both are transmitting in the same channel with Wi-Fi transmissions taking place at a much higher power rating.

C. Cheaper:

Low cost for users is not only about lower power consumption. Other factors are low retail cost and low maintenance and installation costs. The 802.15.4 PHY layer was designed precisely to ensure low cost and high levels of integration. Although ZigBee's radio design principally uses digital circuitry it does include analog stages. However, the use of direct sequence CDMA results in very simple analog circuitry that lends itself to low-cost implementation.

As observed above, 802.15.4's MAC enables multiple topologies that are not complex and have only two basic modes of operations. The result is low or no maintenance (particularly in residential fit-and-forget applications), while networks' self-healing capability and node redundancy further dispenses with maintenance. The extensive use of RFDs – cheap to manufacture and maintain thanks to their inherent low functionality, low ROM and RAM – helps keeps cost down. Further controlling cost is the ZigBee application layer. It was designed to let networks grow physically without the need for more powerful power transmitters, even when networks have very large numbers of nodes with low latency requirements.

In addition to low power consumption, the key factor in ZigBee's low cost is, perhaps, its simplicity. By way of comparison, the number of layers in ZigBee's protocol stack is four times less than in Bluetooth's. Indeed, further comparison with Bluetooth can be a convenient way of highlighting some other ZigBee strong points.

D. Major Parts of the IEEE 802.15.4 WPAN:

A system meeting the requirements to this standard consists of several components. The most basic is the device. Two or more devices communicating on the same physical channel constitute a WPAN. However, this WPAN includes at least one FFD, which operates as the PAN coordinator.[1]

II. LR-WPAN ARCHITECTURE

The IEEE 802.15.4 is defined in terms of a number of blocks in order to simplify the standard. These blocks are called layers. Each layer is responsible for one part of the standard and offers services to the higher layers.

The interfaces between the layers serve to define the logical links that are described in this standard. An LR-WPAN device comprises at least one PHY, which consists of the radio frequency (RF) transceiver along with its low-level control mechanism, and a MAC sub layer that provides access to the physical channel for all types of transfer.

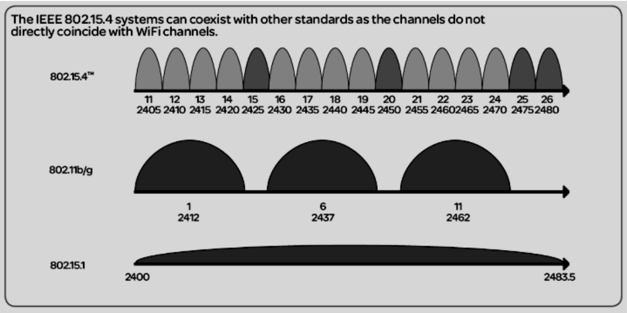


Figure 1: IEEE 802.X Wi-Fi standard comparison

Figure 1 show these blocks in a graphical representation, which are described in more detail in next paragraphs.

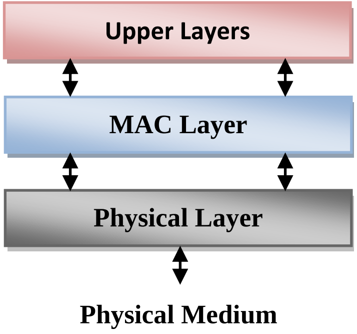


Figure 2: LR-WPAN device architecture

The upper layers, shown in Figure 3, consist of a network layer, which provides network configuration, manipulation, and message routing, and an application layer, which provides the intended function of the device. The definition of these upper layers is outside the scope of this standard [1].

A. Physical layer (PHY):

The PHY provides two services: the PHY data service and the PHY management service. The PHY data service enables the transmission and reception of PHY protocol data units (PPDUs) across the physical radio channel. The features of the PHY are activation and deactivation of the radio transceiver, ED, LQI, channel selection, clear channel assessment (CCA), and transmitting as well as receiving packets across the physical medium. The UWB PHY also has the feature of precision ranging.[1][2][6]

B. MAC sub layer:

The MAC sub layer provides two services: the MAC data service and the MAC management service interfacing to the MAC sub layer management entity (MLME) service access point (SAP) (known as MLMESAP). The MAC data service enables the transmission and reception of MAC protocol data units (MPDUs) across the PHY data service. The features of the MAC sub layer are beacon management, channel access, GTS management, frame validation, acknowledged frame delivery, association, and disassociation. In addition, the MAC sub layer provides hooks for implementing application-appropriate security mechanisms.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

C. Security Architecture:

ZigBee uses 128-bit keys to implement its security mechanisms. A key can be associated either to a network, being usable by both ZigBee layers and the MAC sub layer, or to a link, acquired through pre-installation, agreement or transport. Establishment of link keys is based on a master key which controls link key correspondence. Ultimately, at least the initial master key must be obtained through a secure medium (transport or pre-installation), as the security of the whole network depends on it. Link and master keys are only visible to the application layer. Different services use different one-way variations of the link key in order to avoid leaks and security risks.

Key distribution is one of the most important security functions of the network. A secure network will designate one special device which other devices trust for the distribution of security keys: the trust canter. Ideally, devices will have the trust canter address and initial master key preloaded; if a momentary vulnerability is allowed, it will be sent as described above. Typical applications without special security needs will use a network key provided by the trust canter (through the initially insecure channel) to communicate.

Thus, the trust centres maintains both the network key and provides point-to-point security. Devices will only accept communications originating from a key provided by the trust centre, except for the initial master key. The security architecture is distributed among the network layers as follows:

- The MAC sub layer is capable of single-hop reliable communications. As a rule, the security level it is to use is specified by the upper layers.
- The network layer manages routing, processing received messages and being capable of broadcasting requests. Outgoing frames will use the adequate link key according to the routing, if it is available; otherwise, the network key will be used to protect the payload from external devices.
- The application layer offers key establishment and transport services to both ZDO and applications. It is also responsible for the propagation across the network of changes in devices within it, which may originate in the devices themselves (for instance, a simple status change) or in the trust manager (which may inform the network that a certain device is to be eliminated from it). It also routes requests from devices to the trust center and network key renewals from the trust center to all devices. Besides this, the ZDO maintains the security policies of the device. The security levels infrastructure is based on CCM, which adds encryption- and integrity-only features to CCM.

D.Security Method Review:

In the recent years many experiment for a wireless network has been done to use ECC 160 based encryption that shows that ECC 160 is more powerful & low power consumption instead AES & higher key length RSA. To confirm this the comparison chart is just for analyzing so that AES will be replaced to get the low power benefit as our approach of multi transmitter scheme is a little bit high power consumption to existing system. Hence battery life will down in the years. This impact has to be reduced.

In addition to flexible key exchange and peer authentication, public-key cryptography can be the enabling technology for numerous other WSN applications, including securely connecting pervasive devices to the Internet and distributing signed software patches.[9]

Table 1.0 Comparison among AES, RSA and ECC 160

Parameter	AES	RSA	ECC 160
Time Complexity	Medium	Very High	Less
Space	Medium	Very High	Less
Power Consumption	High	High	Very Less
Key Size	128 bit	1024 bit	160 bit
Security Strength	Good	Weak	More Enough
Steps	Series of Steps	3 Steps	Less to AES
Type	Symmetric Key	Asymmetric Key	Symmetric Key
For Wireless	Good	Complex	Best
MISO System	Good	Not Good	Best
Speed of Encryption	10 Times Faster to RSA	Slow Encryption	15 Times Faster to RSA

The above comparison shows that ECC can be effectively use in the ZigBee Based Wireless Sensor network. Its proved that we may apply the ECC 160 algorithm for encryption and decryption cause it is more beneficial since it having low power consumption, faster , small time complexity , small space complexity.[14] Here we are giving a table for another review in aspect of how much strength ECC 160 has to protect ZigBee based wireless network.[10]

Table 1.1 Key Comparisons [10]

Sr Num	ECC	DSA	RSA	Ratio	Comment
1	160	512	1024	1:6	Short Time
2	256	2048	3072	1:12	Medium Period
3	384	3072	7680	1:20	Long Period

E. ECC in Wireless Sensor Network

Wireless sensor networks (WSNs) are rapidly growing in their importance and relevant to both the research community and the public at large. Security is critical for a variety of sensor network applications. There exist a large number of security vulnerabilities in WSNs, which cause many kinds of attacks.

Wireless sensor networks (WSN) are representative networks using these tiny and low-power sensor devices. Two types of Communications occur in sensor networks: one is between end nodes, and the other is between end node and base station (BS). Since not only the resource restriction in conventional wireless networks but security critical applications, security functions are very important issues in WSN.

A study of software implementations of ECC over binary and prime fields in WSNs is presented. An analytical study of the underlying finite field, representation basis, and performance of these implementations is conducted. The study shows that the fastest prime field implementation, among all reported ones that uses 160-bit on 8-bit, took 0.57 s. As for the implementations over binary field, the study demonstrates that the majority of these implementations are carried out using polynomial basis representation, expect for one implementation that uses normal basis representation. Where the fastest binary field implementation, among all reported ones that uses 163-bit on 8-bit, took 0.67 s.[12]

Multiplication, squaring and reduction operations in ECC point multiplication cost around 2.2 sec, which is roughly 73% of the total time (3.1 s) tested in the experiment. Based on the above analysis, the performance of ECC operations can be further improved by more refined and careful programming.[11][13]

And this, in the end, is the reason ECC is an appropriate choice to achieve security in Wireless sensor networks (WSN). ECC is an excellent choice for asymmetric cryptography in portable constrained devices. 1024-bit RSA key provides the same level of security as a160-bit elliptic curve key. The advantages can be achieved from smaller key sizes including storage, speed and efficient use of power and bandwidth. The use of shorter keys means lower space requirements for key storage and quicker arithmetic operations. These advantages are essential when public-key cryptography is applied in constrained devices, such as in mobile devices or RFID. In brief, ECC based algorithms can be easily included into existing protocols to get the same backward compatibility and security with smaller resources.[10]

F. Power Consumption Considerations:

In many applications that use these standard, devices will be battery powered, and battery replacement or recharging in relatively short intervals is impractical. Therefore, the power consumption is of significant concern. Battery-powered devices will require duty-cycling to reduce power consumption. These devices will spend most of their operational life in a sleep state; however, each device periodically listens to the RF channel in order to determine whether a message is pending. This mechanism allows the application designer to decide on the balance between battery consumption and message latency. Higher powered devices have the option of listening to the RF channel continuously.

In addition to the power saving features of the LR-WPAN system, the UWB PHY also provides a hybrid modulation that enables very simple, non coherent receiver architectures to further minimize power consumption and implementation complexity. [2]

With a given amount of energy, we were able to perform 4.2 times the number of key exchange operations (including mutual authentication) with ECC-160 compared to RSA-1024. While such absolute numbers are platform-specific, we expect the computational cost to fall faster than the cost to transmit and receive. For example, ultra-low-power microcontrollers such as the 16-bit Texas Instruments MSP430 [17] can execute the same number of instructions at less than half the power required by the 8-bit ATmega128L. A similar analysis conducted on such platforms is likely to show communication costs representing a larger fraction of the overall energy spent on authentication and key exchange protocols. The benefits of transmitting smaller ECC keys and certificates will in turn be more significant.[9]

III. ZIGBEE FRAME STRUCTURE

The superframe is defined between two beacon frames and has an active period and an inactive period. Figure 8 depicts the IEEE 802.15.4 superframe structure.

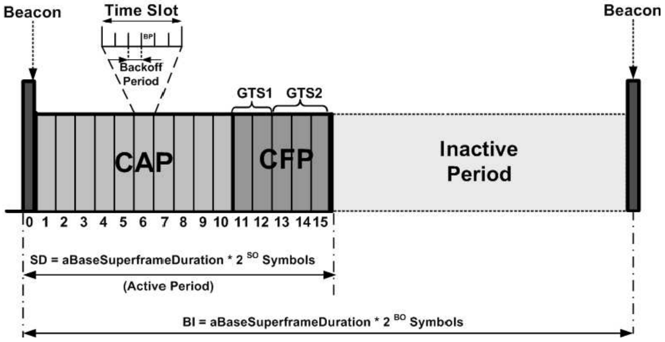


Figure 3 - IEEE 802.15.4 Super frame Structure

The active portion of the super frame structure is composed of three parts, the *Beacon*, the *Contention Access Period* (CAP) and the *Contention Free Period* (CFP):

Beacon: the beacon frame is transmitted at the start of slot 0. It contains the information on the addressing fields, the super frame specification, the GTS fields, the pending address fields and other PAN related.

Contention Access Period (CAP): the CAP starts immediately after the beacon frame and ends before the beginning of the CFP, if it exists. Otherwise, the CAP ends at the end of the active part of the super frame. The minimum length of the CAP is fixed at *aMinCAPLength = 440 symbols*. This minimum length ensures that MAC commands can still be transmitted when GTSs are being used. A temporary violation of this minimum may be allowed if additional space is needed to temporarily accommodate an increase in the beacon frame length, needed to perform GTS management. All transmissions during the CAP are made using the Slotted CSMA/CA mechanism. However, the acknowledgement frames and any data that immediately follows the acknowledgement of a data request command are transmitted without contention. If a transmission cannot be completed before the end of the CAP, it must be deferred until the next superframe.

Contention Free Period (CFP): The CFP starts immediately after the end of the CAP and must complete before the start of the next beacon frame (if *BO* equals *SO*) or the end of the superframe. Transmissions are contention-free since they use reserved time slots (GTS) that must be previously allocated by the ZC or ZR of each cluster.

All the GTSs that may be allocated by the Coordinator are located in the CFP and must occupy contiguous slots. The CFP may therefore grow or shrink depending on the total length of all GTSs. In beacon-enabled mode, each Coordinator defines a superframe structure Figure 3 which is constructed based on:

The *Beacon Interval* (*BI*), which defines the time between two consecutive beacon frames.

The *Superframe Duration* (*SD*), which defines the active portion in the *BI*, and is divided into 16 equally-sized time slots, during which frame transmissions are allowed.

Optionally, an inactive period is defined if *BI* > *SD*. During the inactive period (if it exists), all nodes may enter in a sleep mode (to save energy). *BI* and *SD* are determined by two parameters, the Beacon Order (*BO*) and the Superframe Order (*SO*), respectively, as follows:

$$\left.\begin{array}{l} BI = aBaseSuperframeDuration \times 2^{BO} \\ SD = aBaseSuperframeDuration \times 2^{SO} \end{array}\right\} for\ 0 \leq SO \leq BO \leq 14$$

aBase Superframe Duration = 15.36 ms (assuming 250 kbps in the 2.4 GHz frequency band) denotes the minimum duration of the superframe, corresponding to *SO=0*. As depicted in Figure 3, low duty cycles can be configured by setting small values of the *SO* as compared to *BO*, resulting in greater sleep (inactive) periods. In ZigBee Cluster-Tree networks, each cluster can have different and dynamically adaptable dutycycles. This feature is particularly interesting for WSN applications, where energy consumption and network lifetime are main concerns. Additionally, the Guaranteed Time Slot (GTS) mechanism is quite attractive for time-sensitive WSNs, since it is possible to guarantee end-to-end message delay bounds both in Star and Cluster-Tree topologies.

IV.RELATED WORK

A physical layer simulation of an IEEE 802.15.4 transceiver is developed in accordance with the specifications detailed in the IEEE standard. The simulator is validated by comparing the bit-error-ratio (BER) versus signal-to-noise-ratio (SNR) curve found from simulation with that expected from theory.[6] A broadband non-Gaussian impulsive noise model described by a symmetric α-stable (SαS) distribution is designed and used to assess robustness of the IEEE 802.15.4 receiver to impulsive noise. In ZigBee channels below 1 GHz use BPSK modulation (Binary PSK), while the 2400 MHz band employs O-QPSK (Offset Quadrature PSK). QPSK is spectrally efficient, but requires a linear transmitter due to the state transitions through zero. So, the developers chose O-QPSK which avoids the zero state and thus allows for a constant envelope transmitter, significantly decreasing transmitter complexity and inefficiency.

Algorithm:

The Execution of the simulation is described in following steps:

Step-1: First of all we will defined the parameters necessary to create Zigbee
(IEEE 802.15.4 standard) architecture. In which we are defining sapling frequency range of signal to Noise Ratio for which we are calculating error rate then No of Bytes per symbol, Data rate, chip rate no. of transmitters, No. of frame repetitions etc.

Step-2: Start simulation for first transmitting frame.

Step-3: Now generate random data (Bit Sequence) called as PSDU (Public Service Data Unit). Defined Preamble after that set SFD (Start Frame Delimiter) Defined frame length and Reserved bit. These all parameters produce one frame. ECC 160 Encryption applied.

Step-4: One Single frame in IEEE 802.15.4 standard known as (PPDU Presentation Protocol Data Unit)

Step-5: Now in this step we are performing DSSS (Direct Sequence Spread Spectrum) Which is a kind of digital modulation technique in where we spread the digital data by multiplying it with a chip sequence know as PN sequence.

Step-6: In this step the resulting bit stream from previous step divided in two parts Even & Odd that is the starting of OQPSK Modulation. After OQPSK Modulation the signal is ready to transmit.

Step-7: Now this point is the changing point where we can improve the performance of existing system by using multiple transmitters instead of one transmitter.

Step-8: After transmission signal travels through wireless channel which introduce some noise in signal which distort or create errors here the characteristics of wireless channel is considered as AWGN channel. AWGN channel is the prototype of wireless channel considering all the possible noises in the media.

Step-9: Now continue simulation for first value of SNR that is -20 dB.

Step-10: Now receive signal that is combination of transmitted signal and noise signal.

Step-11: Demodulate received signal.

Step-12: Perform dispreading of the sequence (Inverse Direct Sequence Spread Spectrum)

Step-13: Now calculate Bit error rate form received data and go to step 9 and keep repeating for all the values of SNR.ECC 160 Decryption This is complete simulation of one frame.

Step-14: To get the precise result repeat above steps for your convenience. Here we have simulated above proposed methodology for 25, 50, 75, 100, 125,150,175and 200frame repetition with one, two and three transmitter.

V.PROPOSED METHODOLOGY

In this work we are working on the physical layer of network architecture in which we are trying to increase the error rate performance of the system by implementing multiple transmitters instead of single transmitter in existing system. We are replacing the AES Encryption method from ECC 160 as of recent research has done. The system design and simulation has been done on MATLAB 2011b environment. The algorithm of simulation procedure is given.

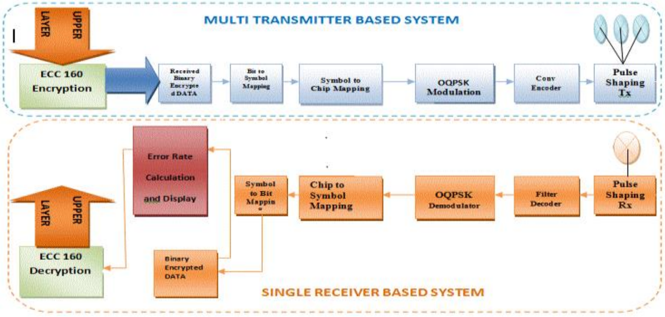


Figure 4 MISO & ECC 160 Encryption Based ZigBee Block Diagram for Proposed Model

VI. SIMULATION RESULTS

The simulation has been done with the MATLAB R2011b environment. During simulation we are calculating the Bit Error Rate for multiple transmitters using different iterations. The below graphs show how system efficiently works with more than single antenna. We have also done analysis on five factors of PHY layer to support our research to enhance the performance of ZigBee based Wireless Sensor Network.The Simulation results are shown from figure 4.1 to figure 4.12. Figure 4.1 & 4.2 are shown for Bit Error Rate over Signal to Noise Ratio.

As above paragraph described, the vital role of MISO system in various applications and we implement the efficient MISO approach in MATLAB for ZigBee wireless technology also got the resourceful improvement in various parameters which are given below:

1. Reduced Bit Error Rate against Signal to Noise Ratio.
2. Capacity of ZigBee MISO System.
3. Battery Life Compression.
4. Performance of Probability of Error with various digital modulation techniques.
5. Data Rate
6. Power spectrum Density.

Figure 4.3 to 4.12 are shown for the supporting factors of our work to enhance to performance of the ZigBee based Wireless Sensor Network.

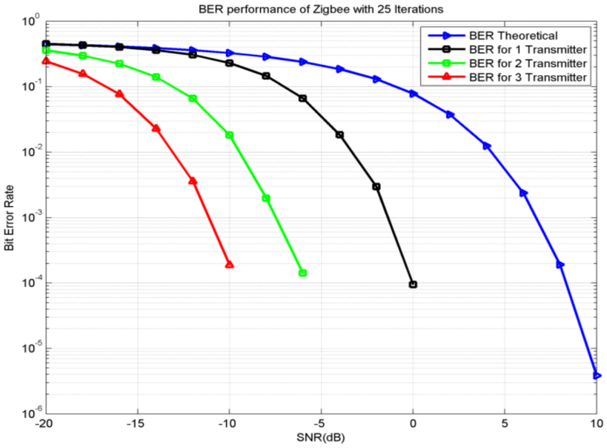


Figure 4.1 BER Vs SNR Performance of the System with Multiple Antennas and 25 iterations.

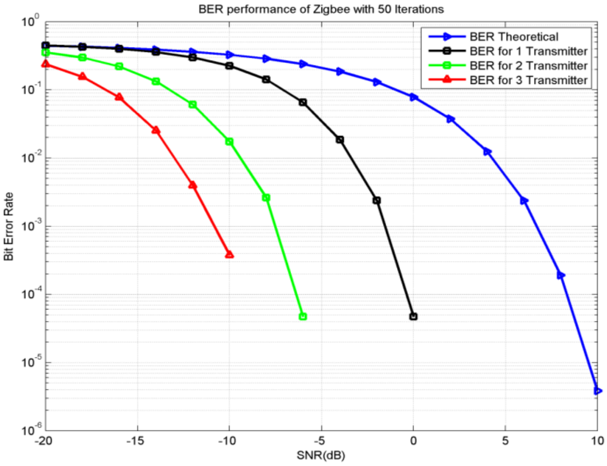


Figure 4.2 BER Vs SNR Performances of the System with Multiple Antennas and 50 Iterations

From above all the experiments it is clear that the "Green" & "Red" characteristics are showing better results of Bit Error Rate for lower values of SNR, which are for two and three transmitters respectively. Now if we use more than one transmitter instead of one (existing system) then the performance of Zigbee (IEEE 802.15.4) system will improve. These results are based on simulation experiments and may vary during practical implementations in the actual conditions.

From the above results in figures from 4.1 to 4.2 it is clear that if we increase the transmitters and the transmitter size of the system the Bit Error Rate reduced significantly, and the signal power requirements also reduces which is the great thing about our proposed approach. And also shows that then if we increase the no. of repetitions of the frame our results precisely improved.

A. Capacity of ZigBee MISO System.

The channel capacity is given by Shannon Capacity Theorem:

$$C = B\, log_2\left(1 + \frac{S}{N}\right)$$

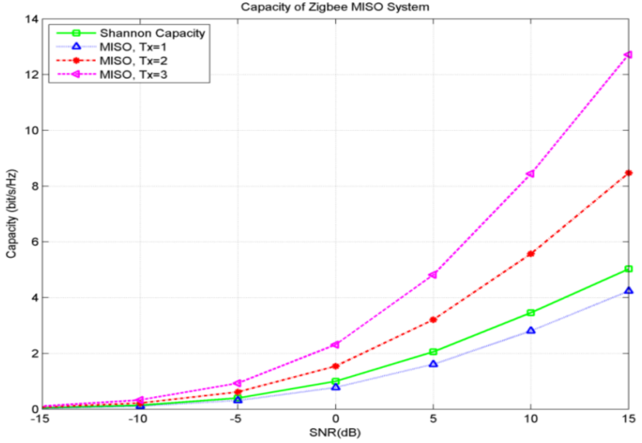


Figure 4.3 Capacity of ZigBee MISO System Vs SNR Characteristics.

As per the result we can see that on increment of the transmitter in the ZigBee Based Wireless Network the channel capacity is going up according to follow with Shannon channel capacity theorem. The purple line of 3 transmitters is showing maximum capacity for the MISO system. Hence this factor support to our work that to increase the transmitter is beneficial to get higher capacity (bits/Hz).

B. Battery Life Compression

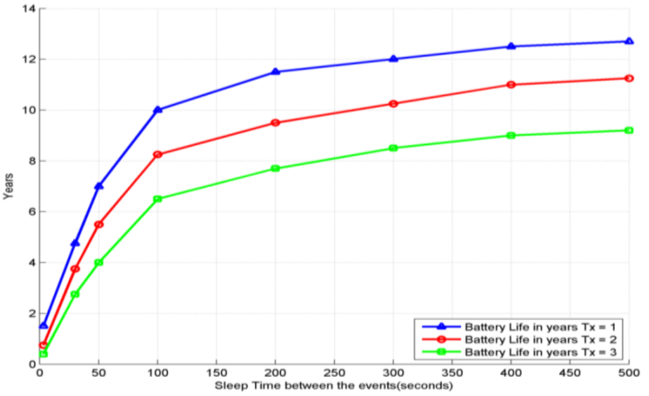


Figure 4.4 Battery Life vs Sleep Time for Zigbee System

As per Zigbee specifications the battery life for the system in years which includes the sleep time of the system i.e. idle condition, figure 6.4 is given below. Figure 6.5 shows Energy Usage Breakdown (Battery Usage per month). This has characteristics Active Energy usage and Total Energy Usage. This characteristics helps us to analyze the battery performance in various conditions. Battery Life can vary according to the duration of data transmission and interval between active mode and sleep mode. The switching from sleep mode to active mode or active mode to sleep mode also causes battery power consumption.

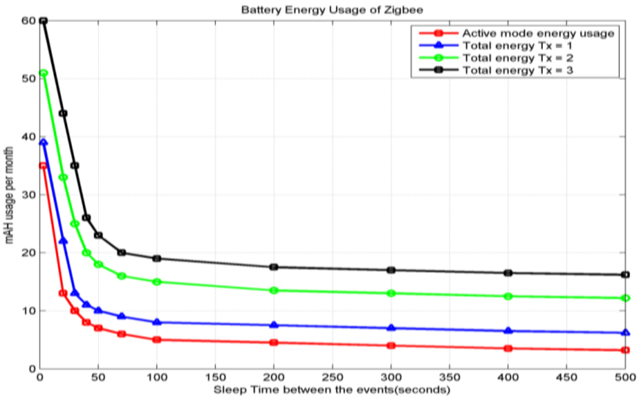


Figure 4.5 Battery mAH usage of Zigbee System.

C. *Performance of Probability of Error with Various Digital Modulation Techniques.*

The Error Probability of Zigbee System shown in figure 4.6 for various digital modulation techniques.Digital modulationtechniques are gives different performance with ZigBee.Speed (or data rate) and distance (or range) are inversely proportional. That is, other things being equal, a higher data rate system will not transmit as far as a lower data rate system.Radio frequency (RF) signals of a given carrier frequency, such as 2.4 gigahertz (GHz), lose power as they propagate. Called path loss, this is similar to the way a sound is softer the farther it is from the source. Path loss in decibels (dB) increases with the square of the distance and is relatively easy to estimate when the path is unobstructed. The free space loss equation at 2.4 GHz is simply this:path loss in dB = 40 dB + 20 log (distance in meters).

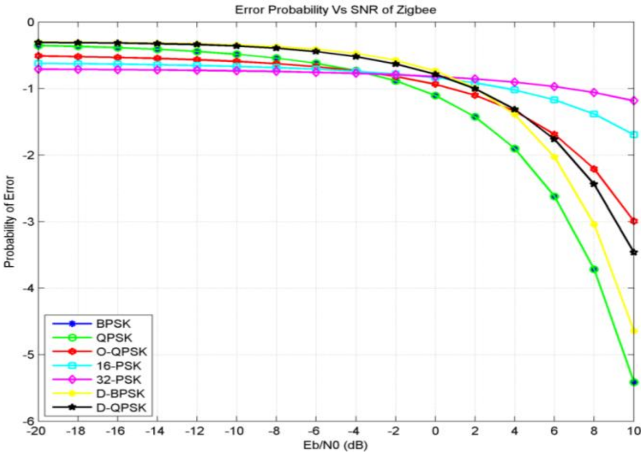


Figure 4.6 Performance of Probability of Error with Various Digital Modulation Techniques of ZigBee System with 1 Tx

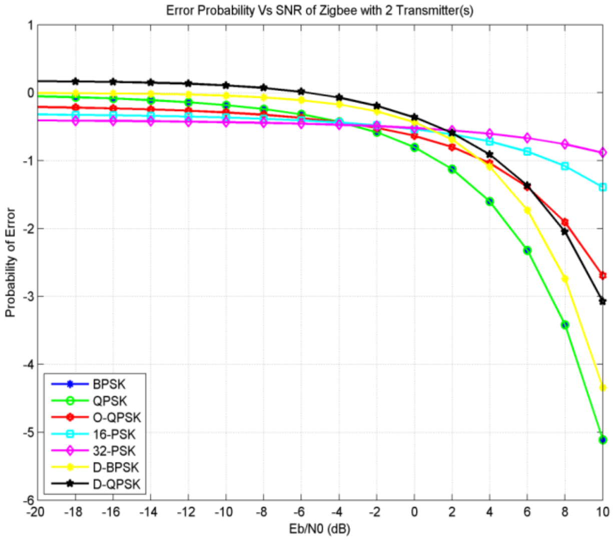


Figure 4.6 Performance of Probability of Error with Various digital Modulation Techniques of ZigBee System with 2 Tx

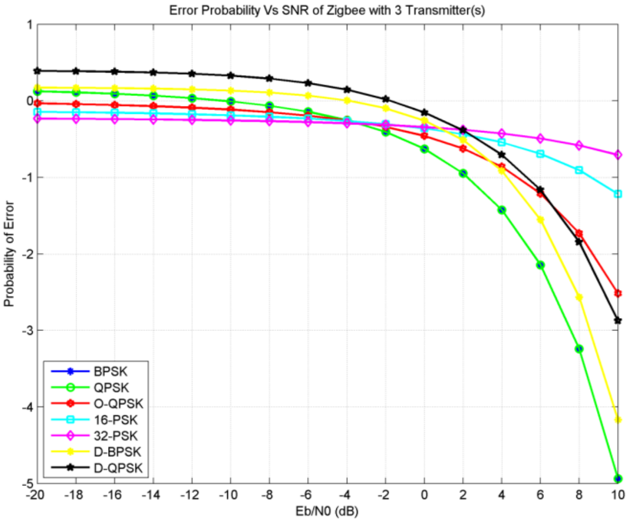
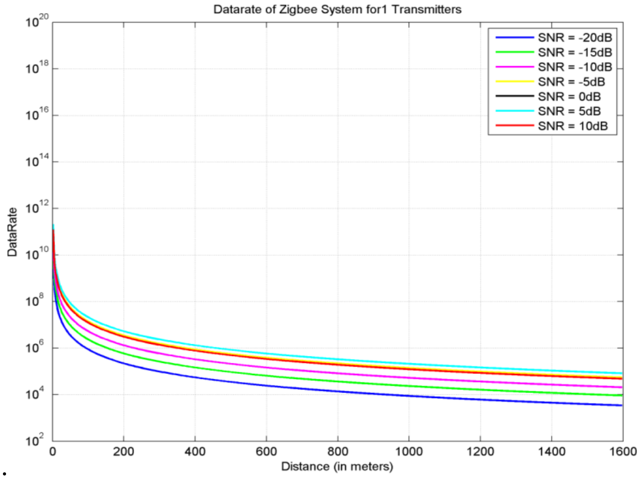


Figure 4.6 Performance of Probability of Error with Various Digital Modulation Techniques of ZigBee System with 3 Tx

D. *Data Rate*



.

Figure 4.7 Variation in Data Rate with Distance and Performance for Values of SNR for 1 Transmitter.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

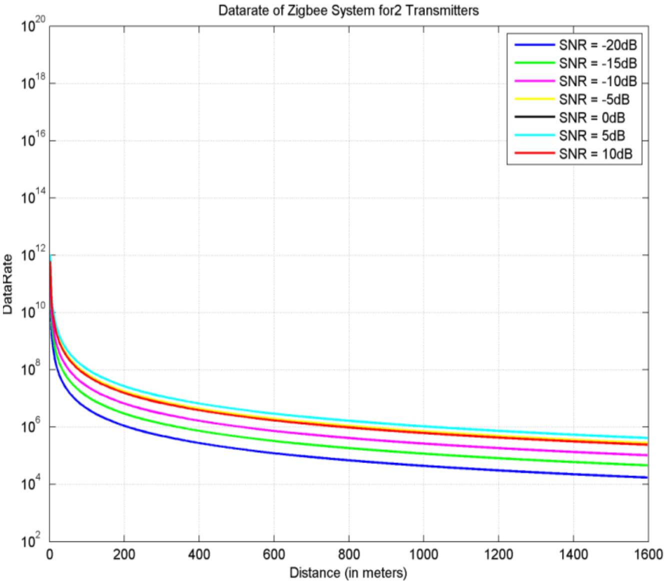


Figure 4.8 Variation in Data Rate with Distance and Performance for values of SNR for 2 Transmitter.

Figure showing the data rate of Zigbee for distance and for various values of Signal to Noise ratio. The data rate performance increases with the increase in number of transmitters. Here we have shown data rate performance for 1 transmitter (Existing System), 2 transmitters and 3 transmitters (Proposed Method).

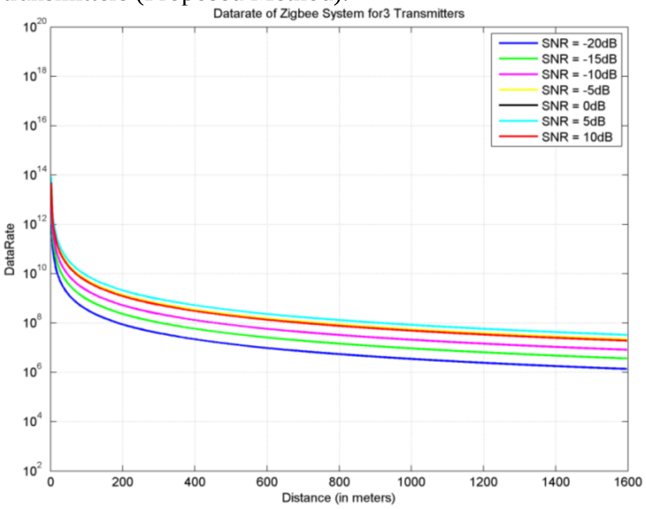


Figure 4.9 Variation in Data Rate with Distance and Performance for Values of SNR for 3 Transmitter.

E. Power Spectrum Density

Power spectral density (PSD) refers to the amount of power per unit (density) of frequency (spectral) as a function of the frequency. The power spectral density, PSD, describes how the power (or variance) of a time series is distributed with frequency. By knowing the power spectral density and system bandwidth, the total power can be calculated. Power spectral density (PSD) shows the strength of the variations (energy) as a function of frequency. In other words, it shows at which frequencies variations are strong and at which frequencies variations are weak. The unit of PSD is energy per frequency (width) and you can obtain energy within a specific frequency range by integrating PSD within that frequency range. Computation of PSD is done directly by the method called FFT or computing autocorrelation function and then transforming it.The power spectral density for existing system of Zigbee (1 Transmitter), and Proposed Approach (i.e. multiple transmitters) are calculated and shown in the figure 4.10, 4.11 and 4.12 respectively.

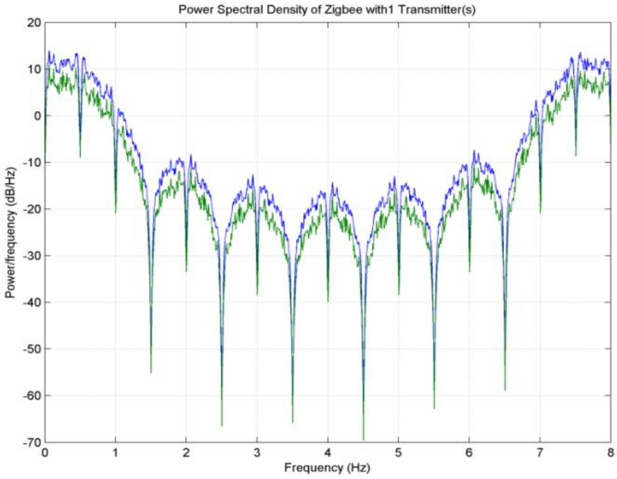


Figure 4.10 Power Spectral Density of ZigBee System with 1 Transmitter

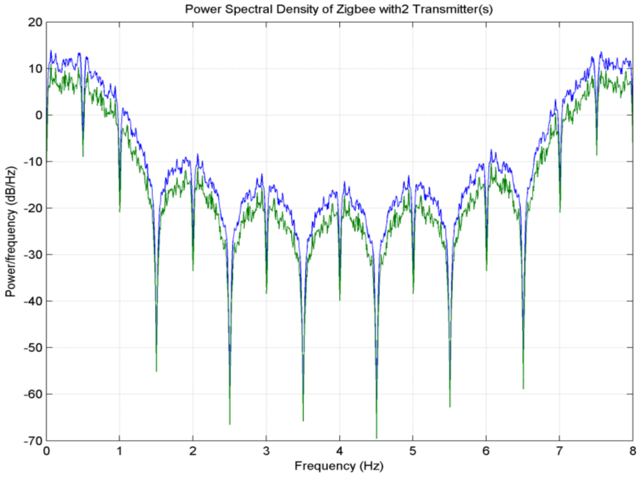


Figure 4.11 Power Spectral Density of Zigbee System with 2 Transmitters

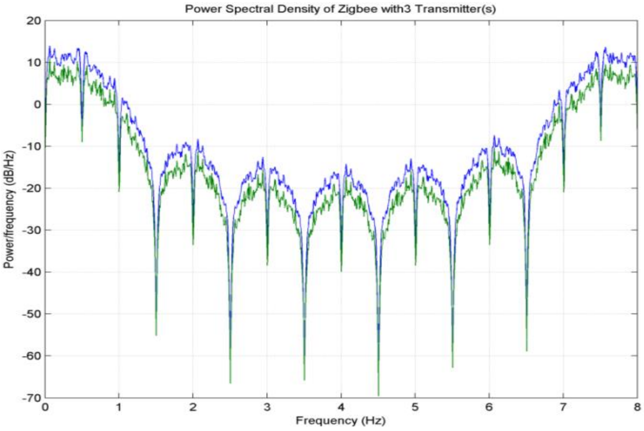


Figure 4.12 Power Spectral Density of Zigbee System with 3 Transmitters

From the result it is clear that the PSD for multiple Transmitters is slightly more than that of existing system. And it is not doubled as number of transmitters goes double. That's why the proposed approach gives better result than existing system.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

VII. CONCLUSIONS AND FUTURE WORK

From the Simulation results, the existing ZigBee system with 2.4 GHz band and with O-QPSK modulation works significantly with low power operations but there is always a need some improvement in the system, so here we have tried to reduce the Bit Error Rate and taken an analysis on five factors of ZigBee system and tried to reduce the power consumption using ECC 160 security algorithm also the Power of the system which will be the revolution in the field of 802.15.4. Here we have increased the number of transmitters which greatly reduces the error rate of the existing system. Here we simulate system up to three transmitters but in future with the developments in the antenna technology we can increase more transmitters as our ease. The future of our proposed work will be the lowest power consumption Personal Area Network (PAN) for information sharing and network access.

REFERENCES

1. J. Stankovic, I. Lee, A. Mok, R. Rajkumar, “Opportunities and Obligations for Physical Computing Systems”, in IEEE Computer, Volume 38, Nov, 2005.
2. The Economist, “When everything connects”, April 28th – May 4th, 2007.
3. N. Aakvaag, M. Mathiesen, and G. Thonet, “Timing and power issues in wireless sensor networks, an industrial test case”, In Proceedings of the 2005 International Conference on Parallel Processing Workshops (ICPPW). IEEE, 2005.
4. S A Bhatti (Student), I A Glover, “Performance Evaluation of IEEE 802.15.4 Receiver in the Presence of Broadband Impulsive Noise” IEEE Student Application Paper 2011.
5. Minakshmi Roy, H.S. Jamadagni, “Cancellation of Zigbee interference in OFDM based WLAN for multipath channel”, ACEEE Int. J. on Network Security, Vol. 02, No. 01, Jan 2011.
6. Nilesh Shirvoikar, Hassanali Virani, Dr. R.B. Lohani, “Performance Evaluation of Zigbee Using Matlab Simulation”, in IJIIT, vol. 1 issue 3 2012-13.
7. IEEE Std. 802.15.4, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), IEEE, New York, N.Y., 2006.
8. Alnuaimi, Mariam work on “Performance Evaluation of IEEE 802.15.4 Physical Layer Using MatLab/Simulink” Innovations in Information Technology, 2006, in Coll. of Inf. Technol., UAE Univ., Al-Ain , page 1 – 5.
9. Arvinderpal S. Wander†, Nils Gura‡, Hans Eberle‡, Vipul Gupta‡, Sheueling Chang Shantz‡†University of California, Santa Cruz ‡Sun Microsystems Laboratories “Energy Analysis of ECC for Wireless Sensor Network”.
10. International Journal of EngineeringResearch & Technology (IJERT) ISSN: 2278-0181 Vol. 1 Issue 3, May – 2012” Elliptic Curve Cryptography (ECC) for Security in Wireless Sensor Network.”.
11. *Int. J. Security and Networks, Vol. 1, Nos. 3/4, 2006 “*Elliptic Curve Cryptography-Based Access Control in Sensor Networks”
12. Journal of Communication and Computer 9 (2012) 712-720 Hilal Houssain1, Mohamad Badra2 and Turki F. Al-Somani1 “Software Implementations of Elliptic CurveCryptography in Wireless Sensor Networks”
13. 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops “Analytical study of implementation of Elliptical Curve Cryptography for Wireless Sensor Networks” Pritam Gajkumar Shah, Xu Huang, Dharmendra Sharma,Faculty of Information Sciences and Engineering,University of Canberra, Act 2601-Australia
14. Research Paper IEEE Wireless Technology and Applications (ISWTA), 2012 IEEE Symposium on Date of Conference: 23-26 Sept. 2012 **Author(s):** Rosli, R. Fac. of Electr. Eng., Univ. Teknol. MARA, Shah Alam, Malaysia Yusoff, Y.M.; Hashim, H.**Page(s):** 187 - 191 **Product Type:** Conference Publications.
15. ZigBee Alliance “ www.zigbee.org “