

An Architecture and Programming of The Zigbee

2.1 Introduction:

Present research work emphasizes the development of Wireless Sensor Network (WSN) to realize the Site Specific Crop Management (SSCM). It is an innovative field comprising typically designed sensor nodes, WSNodes [1, 2]. As per architecture of the WSN, described in topic 1, the WSNodes must be networked, wirelessly, depicting specific networking topology. Indeed, to establish wireless communication, the deployment of RF modules is essential. During early days, the nodes of WSN are linked with GPS technology [3], wherein satellite communication is employed. Such WSN reveals wide coverage area [4], but featured with tremendously high infrastructural cost. Moreover, to ensure an innovative technique of Precision Agriculture (PA), the precision agriculturists are attracting towards polyhouse agriculture, which is constrained in the limited areas. To play with spatial as well as temporal variability of the site specific data and to achieve sustainable growth of the plants of the polyhouse, a WSN with short range of communication is most suitable [5]. To ensure short range RF communication, following IEEE standards, within the capture area of WSN, each WSNode must be equipped with highly sophisticated RF module [6, 7]. It is found that, the Zigbee technology, in association with IEEE and Digi Corporation, is pervasively emerging. They launched RF module called “Zigbee module”, which is highly suitable to establish the dedicated Wireless Sensor Network (WSN) [8]. Therefore, the Zigbee devices are extensively studied and details regarding the same are presented in this topic. It is to be noted that the Zigbee is the technology and the device which ensures this technology is named by the Digi as “Xbee”. Therefore, Xbee and Zigbee can be synonymously used.

In fact, the device Zigbee (may be Xbee) realizes the present day VLSI technologies, wherein reconfiguration of on-chip resources is primarily focused. The WSN is featured with reconfigurability and therefore, it needs the device with

programming capabilities. It known that, the Zigbee is a programmable RF module. Therefore, it is essential to explore the programming techniques. For programming of the Zigbee device, the Digi Corporation has provided very smart IDE called “X-CTU”. Therefore, the details of X-CTU are studied and deployed for programming of Zigbee device in desired mode. The details regarding X-CTU and programming of the Zigbee are discussed in subsequent article. Thus the topic is devoted for architecture of the Zigbee and its programming.

On survey, it is found that, to collect data and disseminate the same to monitoring station following means are available [Table 2.1]. The table 2.1 summarizes the features of different wireless technologies.

On comparative study, it is found that, a novel technology known as “Zigbee technology” is most suitable for establishment of Wireless Sensor Network. To ensure

TABLE 2.1: Features of Wireless Technologies

Sr. No.	Parameters	Zigbee Technology	802.11 (Wi-fi)	Bluetooth	UWB (Ultra Wide Band)	IR Wireless
1.	Data Rate	20, 40 and 250 Kbits/s	11 & 54 Mbits/s	1 Mbits/s	100 – 500 Mbits/s	20 – 40 Kbits/s 115 Kbits/s 4 & 6 Mbits/s
2.	Range (meters)	10 – 100	50 – 100	10	< 10	< 10
3.	Networking Topology	Ad-hoc, peer to peer, star, mesh	Point to Hub	Ad-hoc, very small Networks	Point to point	Point to point
4.	Operating Frequency	868 MHz (Europe) 900-928 MHz(NA), 2.4 GHz (Global)	2.4 and 5 GHz	2.4 GHz	3.1 – 10.6 GHz	800 – 900 nm
5.	Complexity	Low	High	High	Medium	Low
6.	Power Consumption (Battery option and life)	Very low (low power is a design goal)	High	Medium	Low	Low
7.	Security	128 AES plus application layer security		64 and 128 bit encryption		

wide portability, one of the groups of IEEE is working and they had launched a typical standard, called Zigbee standard. This Zigbee standard is released in 2004 [9, 10]. This technology focuses on the low cost, low power consumption and ability to connect in mesh network. Therefore, it becomes more optimum solution for various applications. The term Zigbee is originated from the domestic honeybees, which avail a Zigzag path for messaging among them. In fact, it realizes basic principles of hopping techniques.

On combination of above two words the word Zigbee is composed. It is to be noted that, the Zigbee device, follows IEEE 802.15.4 standards to establish the communication. As discussed in the topic 1, it uses MAC and PHY layers along with its own stack of upper layers. This topic devotes the discussion on architecture and programming of the Zigbee.

2.2 Architecture of the Zigbee:

According to architecture, the Zigbee devices are classified into following two types.

- **Zigbee Series 1**

These radios use a Microchip made by Freescale that provide simple, standards-based point-to-point communications, as well as a proprietary implementation of mesh networking.

- **Zigbee Series 2**

It uses a microchip from Ember Networks that enables several different flavors of standards.

Both the Series 1 and Series 2 Zigbee devices are available in two different versions, such as regular and PRO. The Zigbee devices are as depicted in Figure 2.1. The regular version is called simply an Xbee but The XBee-PRO device has more power consumption and it is rather expensive [11].

The Zigbee comes with variety of antenna styles providing differing

amounts of gain. The devices such as CC2xxx ensure Wi-Fi communication through the antenna fabricated on PCB itself [12, 13]. Two of the most popular versions are the chip antenna and whip antenna styles. These use a chip with the actual antenna structure embedded in the chip. Many of these devices have a whip (external) antenna via connector. A whip is often a coiled piece of wire matched to the circuit.

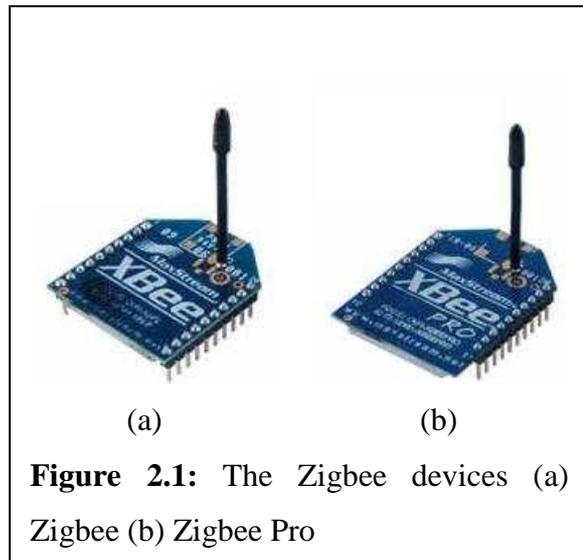


Figure 2.1: The Zigbee devices (a) Zigbee (b) Zigbee Pro

2.2.1: The Salient features of Zigbee devices:

The salient features of both devices are presented in table 2.2. On investigation of structural details, it is found that Zigbee module of series 2(S2) is most suitable for establishment of Wireless Sensor Network. Therefore, for present research work series 2 Zigbee pro is employed and Wireless Sensor Network is established.

TABLE 2.2: Salient features of S1 and S2 Zigbee devices

Sr. No.	Parameter Name	Series 1	Series 2
1.	Typical (indoor/urban) range	30 meters	40 meters
2.	Best (line of sight) range	100 meters	200 meters
3.	Transmit/Receive current	45/50 mA	40/40 mA
4.	Firmware (typical)	802.15.4 point-to-point	ZB Zigbee mesh
5.	Digital input/output pins	8 (plus 1 input-only)	11
6.	Analog input pins	7	4
7.	Analog (PWM) output pins	2	None
8.	Low power, low bandwidth, low cost, standardized, small, popular	Yes	Yes
9.	Interoperable mesh routing, ad hoc network creation, self healing networks	No	Yes
10.	Point-to-point, star topologies	Yes	Yes
11.	Mesh, cluster tree topologies	No	Yes
12.	Single firmware for all modes	Yes	No
13.	Requires Coordinator node	No	Yes
14.	Point-to-point configuration	Simple	More involved
15.	Standards-based networking	Yes	Yes
16.	Standards-based applications	No	Yes
17.	Underlying chipset	Free scale	Ember
18.	Firmware available	802.15.4 (IEEE standard), Digi Mesh (proprietary)	ZB (Zigbee 2007), Znet 2.5 (obsolete)
19.	Up-to-date and actively supported	Yes	Yes

2.2.2: Pin Description of the Zigbee :

The WSNodes are designed, wherein the Zigbee devices are employed to ensure RF communication. To design hardware of the WSNode, the structural details of Zigbee devices are explored. The pin-out of the device is depicted in figure 2.2. As shown in figure 2.2, the Zigbee is a 20-pin DIP module with pin spacing of 2 mm (0.079in) as opposed to typical pin spacing of 2.54 mm (0.1in). Moreover, table 2.3 depicts the pin assignments.

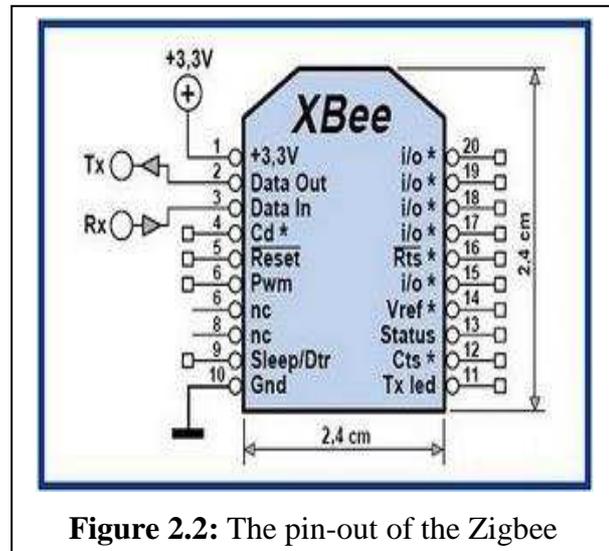
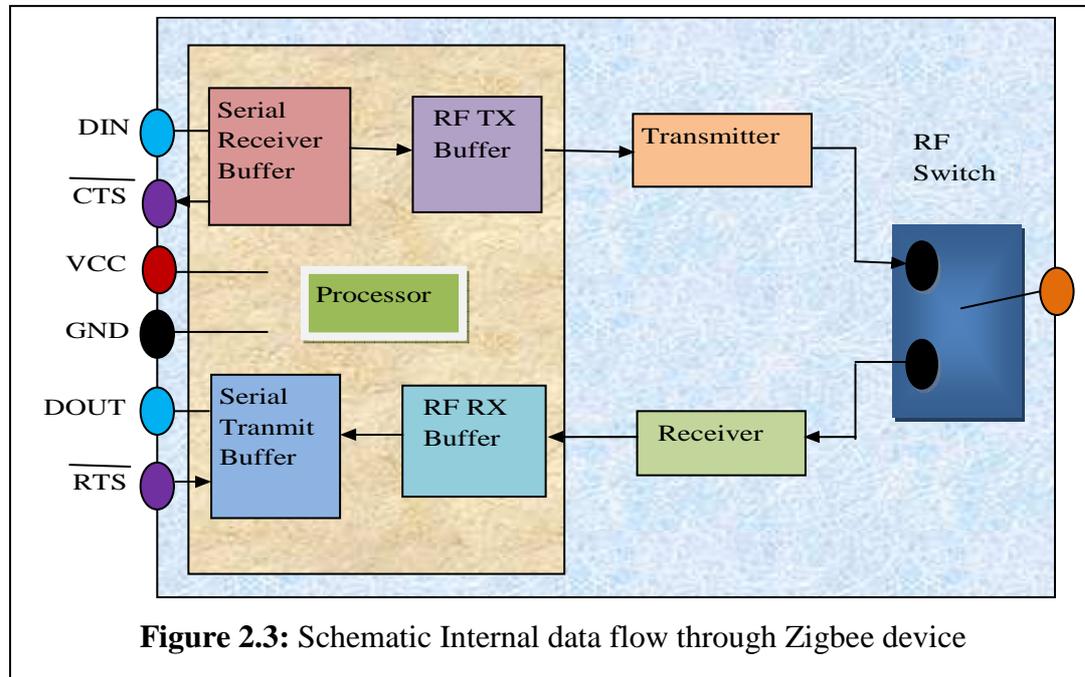


Figure 2.2: The pin-out of the Zigbee

TABLE 2.3: Pin description of the Zigbee

Pin No.	Name	Direction	Default State	Description
1.	V _{CC}	-	-	Power Supply
2.	D _{OUT}	Output	Output	UART Data Out
3.	D _{IN} / CONFIG	Input	Input	UART Data In
4.	DIO12	Both	Disabled	Digital I/O 12
5.	Reset	Both	Open Collector With Pull Up	Module Reset(Reset Pulse Must Be At least 200 Ns)
6.	RSSI PWM/DIO 10	Both	Output	Rx Signal Strength Indicator/Digital I/O 10
7.	DIO11	Both	Input	Digital I/O 11
8.	Reserved	-	Disabled	Do Not Connect
9.	DTR/SLEEP_RQ/DIO8	Both	Input	Pin Sleep Control Line Or Digital I/O
10.	Gnd	-	-	Ground
11.	DIO4	Both	Disabled	Digital I/O 4
12.	CTS/DIO7	Both	Output	Clear To Send-Low Control Or Digital I/O 7. CTS, If Enabled Is An Output
13.	ON/SLEEP/ DIO9	Output	Output	Module Status Indicator Or Digital I/O 9
14.	V _{REF}	Input	-	This Pin Voltage Reference. If Analog Sampling is Desired. Otherwise, Connect To GND.
15.	Associate/DIO5	Both	Output	Associated Indicator, Digital I/O 5
16.	RTS/DIO6	Both	Input	Request To Send Flow Control, Digital I/O 6. RTS, If Enabled, Is An Input
17.	AD3/DIO3	Both	Disabled	Analog Input 3 Or Digital I/O 3
18.	AD2/DIO2	Both	Disabled	Analog Input 2 Or Digital I/O 2
19.	AD1/DIO1	Both	Disabled	Analog Input 1 Or Digital I/O 1
20.	AD0/DIO0/ Commissioning Button	Both	Disabled	Analog Input 0,Digital I/O 0 Or Commissioning Buffer

On investigation of structural details, it is found that, the Zigbee should be powered with highly regulated 3.3V supply. Therefore, one has to derive the same from the 5V, which is already availed for microcontroller based circuits. It is also suggested to use +5V power supply available on USB port of the PC. As described in the table 2.3



each pin is assigned for specific task. Zigbee adapter board has two 10 pin headers with two buffered inputs to the Zigbee [Fig 2.2]: DIN (Data into Zigbee for transmission) and RTS (Request to send flow control) and two outputs to the Zigbee [Fig 2.2] DOUT (Data out) and CTS (Clear to send flow control). The Zigbee RESET pin is connected through a diode to allow the controller to bring it low but not high. The schematic of internal data flow is presented in figure 2.3.

A typical System on Chip device for Zigbee consists of an 802.15.4 RF front-end, the associated baseband circuitry, a microprocessor, flash, RAM, and a complement of general purpose I/O. Since much of the appeal of Wireless Sensor Networks is their ability to make various sensing and control applications more cost effective and low-cost System-on-Chip devices are important in moving applications from research into commercialized products. Multiple silicon vendors, including Ember, ST Microelectronics, TI, Free scale, Jennic, Integration, and others, now provide System-on-Chip devices for the 2.4GHz 802.15.4 standard, with associated microcontrollers ranging from 8-bit to 32-bit cores. The internal block diagram of Zigbee RF module is as shown in figure 2.4 [14].

2.2.3 Organization of the Zigbee:

The internal architecture of the Zigbee device is depicted in figure 2.4. On inspection of figure 2.4, the block diagram of Zigbee, it is found that the Zigbee consist of two major sub systems, the analog subsystems and digital subsystem.

The digital subsystem comprises, processing core along with huge memory blocks, communication interfaces, data converter block and the block for configuration of physical and MAC layer etc. The memory block has flash of 128K, SRAM of 5K bytes. The Zigbee also consists of hardcore for UART, SPI and I²C communications. It has two 16-bit timers with PWM/CCP/CCM cores. It also consists of 4 channels ADC of delta-sigma type [14, 15], the UART in Zigbee module has buffers to communicate to the external controller. The serial data given by the controller at DIN input is

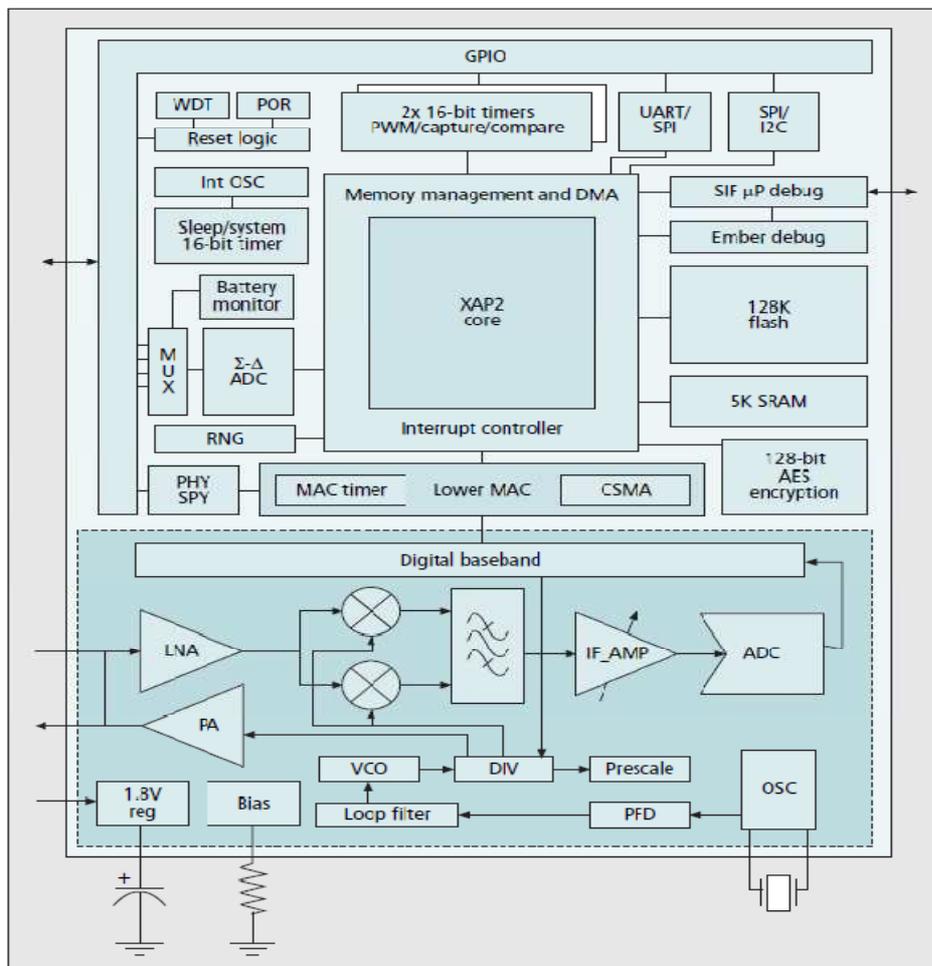


Figure 2.4: Internal architecture of Zigbee device [14]

collected in the buffer and then by framing into specific format, it is given to the transmitter for wireless transmission. The nodes are configured with their ID. The data received from the antenna section is hold into respective buffer and then send out to

read it in microcontroller. The details regarding frequency bands other standards are discussed in topic 1.

2.3 Types of the WSNodes:

According to wireless networking technology and the functionality of devices, the Wireless Sensor Nodes can be classified into two groups. As noted earlier, to clearly signify the meaning WSN is used for Wireless Sensor Network. However, the Wireless Sensor Nodes are referred as WSNode. In short, the Node and WSNode are same and are used interchangeably. Following is the classification of the WSNode.

- Full Function Devices (FFD)
- Reduced Function Devices (RFD).

An IEEE 802.15.4 network requires at least one FFD to act as a network Coordinator. A RFD needs only a minimum of resources to send or receive data for itself. Zigbee RFDs are generally battery powered. RFDs can talk only to FFD, a device with sufficient system resources for network routing. The FFD can be configured as a network Coordinator. Any FFD can talk to both FFD, in cluster based WSN and RFDs. Basically, in WSN philosophy the WSNodes are of following types.

- The Coordinator
- The Router
- End Device

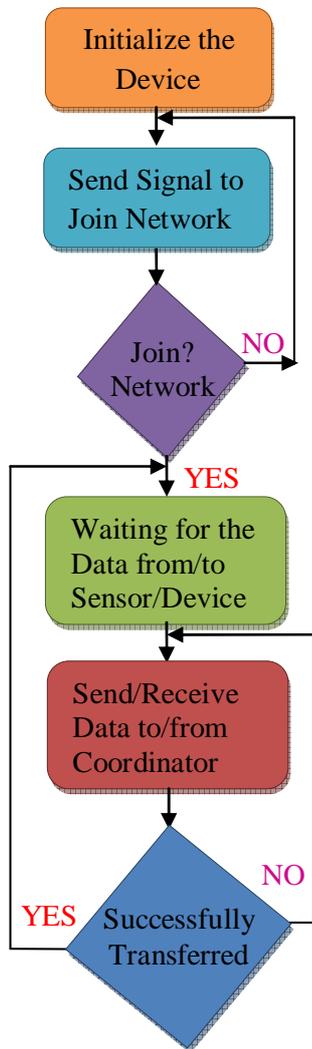
Tables 2.4 illustrate definition and functionalities of these nodes as well.

TABLE 2.4: WSNodes and their functionality

Type of Wireless Sensor Nodes	Coordinator	Router	End Device
Function	Network establishment and control	Supports routing functionality; can talk to other routers, Coordinator, and end devices	Can only talk to routers and the Coordinator
Full Function Device (FFD): Requires resources to handle all designated tasks.	Yes	Yes	Yes
Reduced Function Device (RFD): Requires modest resources compared to FFD.	No	No	Yes

The operation of above WSNodes, within WSN is presented in figure 2.5

Flow chart of working of zigbee End Device



Flow chart of working of zigbee coordinator

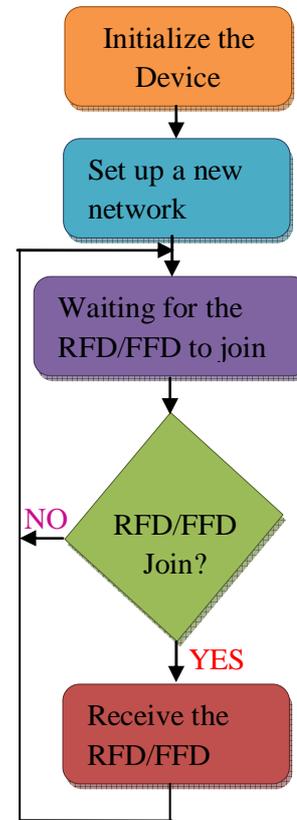


Figure 2.5: Operations of the WSNodes: Coordinator and End Device

2.4: Realization of Wireless Communication using Zigbee:

The WSNodes are designed for present WSN, wherein wireless communication is ensured through Zigbee devices. The mechanism of internal data flow during transmission and reception of the data is presented in figure 2.3. The details regarding availing of the resources during wireless communication are discussed.

i) Serial Communications:

The Zigbee RF module can be interfaced to a host device through a logic-level asynchronous serial port. Through its serial port, the module can communicate with typical logic and voltage compatible UART. It is also recommended to deploy level translator such as RS-232.

ii) UART Data Flow:

As discussed previously, the UART interfaces can be connected directly to the pins of the RF module. It is schematically represented in figure 2.6.

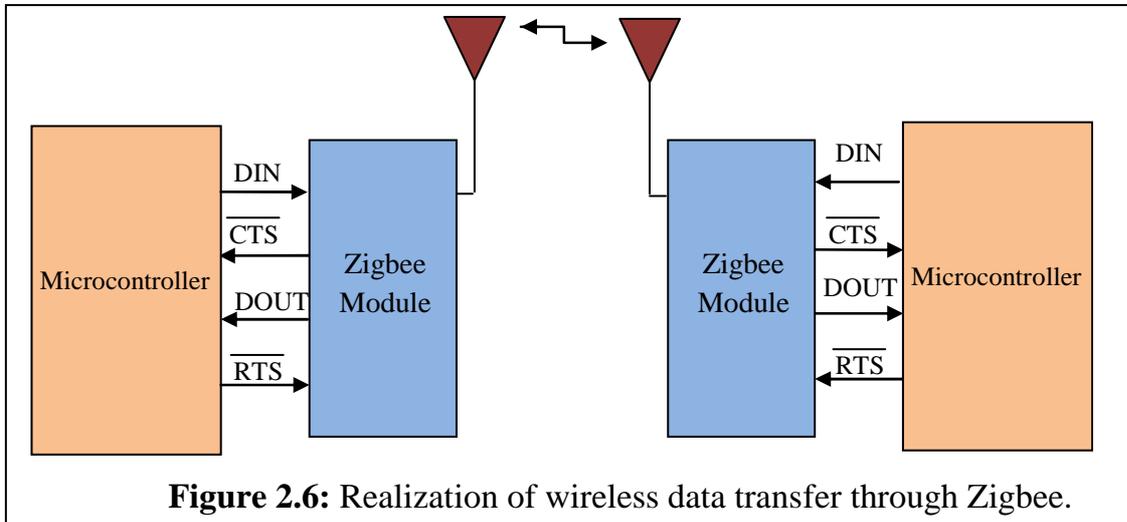


Figure 2.6: Realization of wireless data transfer through Zigbee.

The frame of Data enters into the device through the DIN (pin 3) as an asynchronous serial signal. The signal should idle high when no data is being transmitted. Each data byte is packetized into frame of one start bit (low) and two stop

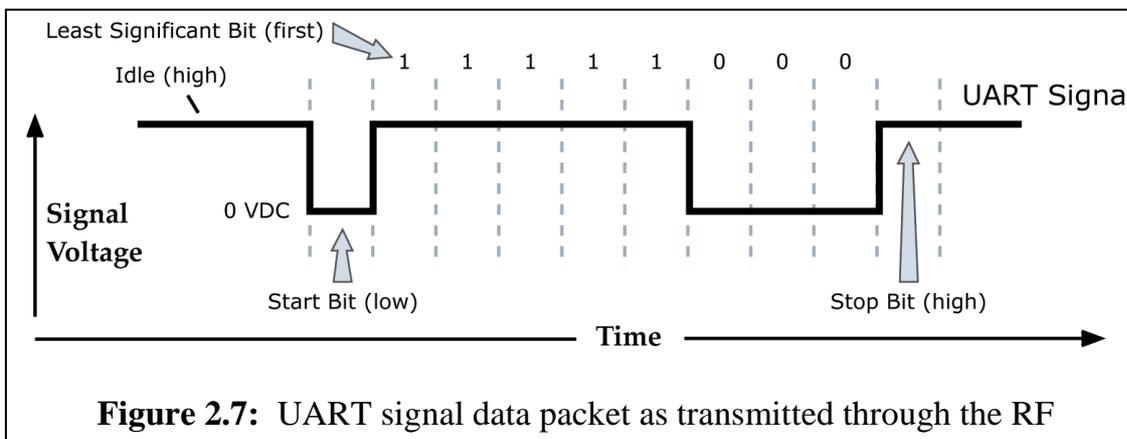


Figure 2.7: UART signal data packet as transmitted through the RF

bits (high). The LSB is communicated first. Frame of data packet is depicted in figure 2.7.

The module UART performs tasks, such as timing and parity checking, that are needed for data communications. For Serial communications, the parameters such as baud rate, parity, start bits, stop bits, data bits etc are configured. The communication link layer performs this task.

iii) Serial Buffers:

The modules maintain buffers to collect received serial and RF data, which is illustrated in the figure 2.3. The serial receive buffer collects incoming serial characters and holds them until they can be processed. The serial transmit buffer collects data that is received via the RF link that will be transmitted out the UART.

- **Serial Receive Buffer:**

When serial data enters the RF module through the DIN Pin (pin 3), the data is stored in the serial receive buffer until it can be processed. Under certain conditions, the module may not be able to process data in the serial receive buffer immediately. If large amounts of serial data are sent to the module, CTS flow control may be required to avoid overflowing the serial receive buffer. This also helps to minimize flooding of the data. If the module is receiving a continuous stream of RF data, the data in the serial receive buffer will not be transmitted until the module is no longer receiving RF data.

If the module is transmitting an RF data packet, the module may need to discover the destination address by routing. The module can also be configured in broadcast mode. On realization of hopping techniques, line of sight could be enhanced.

- **Serial Transmit Buffer:**

When RF data is received, the data is moved into the serial transmit buffer and is sent out the serial port. If the serial transmit buffer becomes full enough such that all data in a received RF packet won't fit in the serial transmit buffer, the entire RF data packet is dropped. If the RF data rate is set higher than the interface data rate of the module, the module could receive data faster than it can send the data to the host.

iv) Serial Flow Control:

The RTS and CTS module pins can be used to provide RTS and CTS flow control. These control signals play a vital role in synchronization of serial communication.

CTS Flow Control:

If CTS flow control is enabled (D7 command), when the serial receive buffer is filled with FT bytes, the module de-asserts CTS (sets it high) to signal

to the host device to stop sending serial data. CTS is re-asserted when less than FT - 16 bytes are in the UART receive buffer.

RTS Flow Control:

If flow RTS control is enabled (D6 command), data in the serial transmit buffer will not be sent out the DOUT pin as long as RTS is de-asserted (set high). The host device should not de-assert RTS for long periods of time to avoid filling the serial transmit buffer. If an RF data packet is received, and the serial transmit buffer does not have enough space for all of the data bytes, the entire RF data packet will be discarded. The Zigbee modules support both transparent and API (Application Programming Interface) serial interfaces.

2.5 Types of Operation:

On extensive study of structural and programming details, it is found that the Zigbee should be programmed into typical operation. There are following two types of operations that Zigbee can be programmed.

- a) Transparent Operation
- b) API Operation

a) Transparent Operation:

When Zigbee is programmed into transparent mode, the modules act as a serial line replacement. All UART data received through the DIN pin is queued up for RF transmission. Whereas the RF data when received, is sent out through the DOUT pin towards microcontroller for further processing. The module configuration parameters are configured by using the AT command mode interface. The dedicated IDE is provided by Digi Corporation [16, 17] to program the Zigbee in desired operation. The IDE provided by Digi Corporation is “Zigbee Configuration and Testing Utilities (X-CTU)”. The details regarding features of X-CTU and programming techniques are discussed in next article.

b) API Operation:

For configuration of WSN to ensure different protocols the API operation is recommended by the Digi Corporation. API operation is an alternative to transparent operation. The frame-based API extends the level to which a host application can interact with the networking capabilities of the module. When in API mode, all data

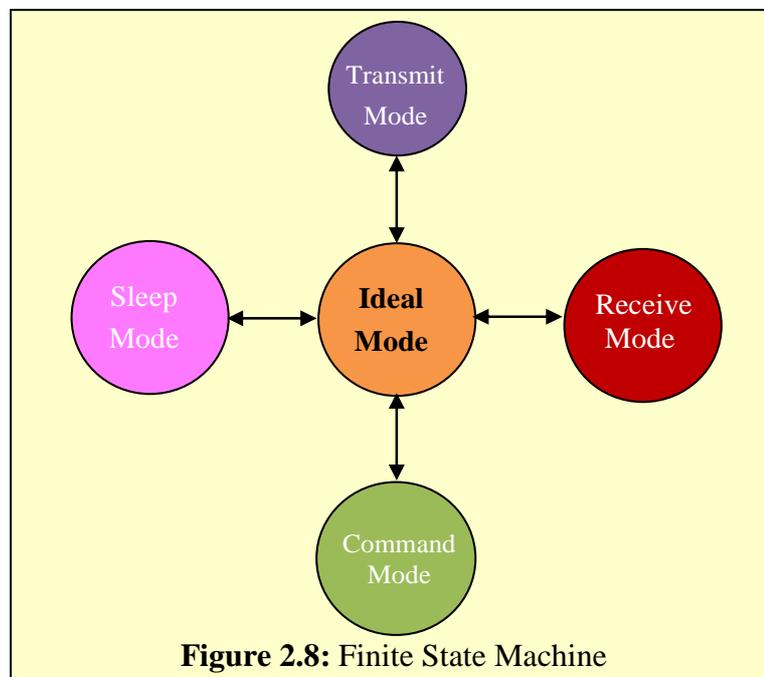
entering and leaving the module is packetized into frames that define operations or events within the module.

The API provides alternative means of configuring modules and routing data at the host application layer. A host application can send data frames to the module that contain address and payload information instead of using command mode to modify addresses. The module will send data frames to the application containing status packets as well as source and payload information from received data packets.

2.6 Modes of operation:

It is known that the WSN is establishment of WSNodes, who plays vital job of RF communication at 2.4 GHz. To ensure this communication, the Zigbee devices installed onto each WSNode should be programmed to operate in the following modes (Figure 2.8).

- Transmit Mode
- Receive Mode
- Idle Mode
- Sleep Mode
- Command Mode



The WSNodes, those are configured as an End Devices operates in transmit mode. However, in cluster based WSN the WSNodes should play in both transmit as

well as receive mode. The Coordinator is also playing the role of transmission as well as reception of the data.

i) Transmit Mode:

When serial data is received and is ready for packetization, the RF module will exit Idle Mode and attempt to transmit the data. The destination address determines which node(s) will receive the data. To communicate, modules must be configured to operate on the same channel and network ID. If a route is not known, route discovery will take place for the purpose of establishing a route to the destination node. If a module with a matching network address is not discovered, the packet is discarded. The data will be transmitted once a route is established. If route discovery fails to establish a route, the packet will be discarded. When data is transmitted from one node to another, a network-level acknowledgement is transmitted back across the established route to the source node. This acknowledgement packet indicates to the source node that the data packet was received by the destination node. If a network acknowledgement is not received, the source node will re-transmit the data.

ii) Receive Mode

In receive mode of operation, the Zigbee on interaction with source node receive the packet of data and then it transfers the same to the serial transmit buffer.

iii) Ideal Mode:

When not receiving or transmitting data, the RF module is in Idle Mode. During Idle Mode, the RF module is also checking for valid RF data. The module shifts into the other modes of operation under the following conditions:

- Transmit Mode (Serial data in the serial receive buffer is ready to be packetized)
- Receive Mode (Valid RF data is received through the antenna)
- Command Mode (Command Mode Sequence is issued)
- Sleep Mode (Sleep-enabled devices only)

iv) Sleep Mode:

Sleep mode allows the RF module to enter a low power state. The XBee Digi Mesh modules support a network synchronized sleep to conserve power.

v) Command Mode:

In this state, incoming characters are interpreted as commands. The commands are used to modify or read RF module parameters. To enter AT Command Mode, we will send the 3-character command sequence ”+++” and observe guard times before and

after the command characters. When a command is sent to the module, the module will parse and execute the command. Upon successful execution of a command, the module returns an “OK” message. If execution of a command results in an error, the module returns an “ERROR” message.

2.7 The Architecture of Zigbee Stack:

The present work emphasizes networking of the WSNodes. As discussed in 1.5.6 the philosophy of networking, the standard networking protocols reveal layered architecture. The specifications of each layer are governed by IEEE standards. For networking protocols the standard OSI model is usually deployed. This model is having typical layered architecture. In fact, the Zigbee does follow OSI model as it is. It employs IEEE standard only up to two basic layers; PHY and MAC layers. Rest of the part of the stack is dedicatedly designed for Zigbee operation. Figure 2.9 depicts the layered architecture of Zigbee stack. As indicated in Figure 2.9, Zigbee sits on top of the IEEE 802.15.4 PHY and MAC layers. However, the network layers and application layers are its own layer.

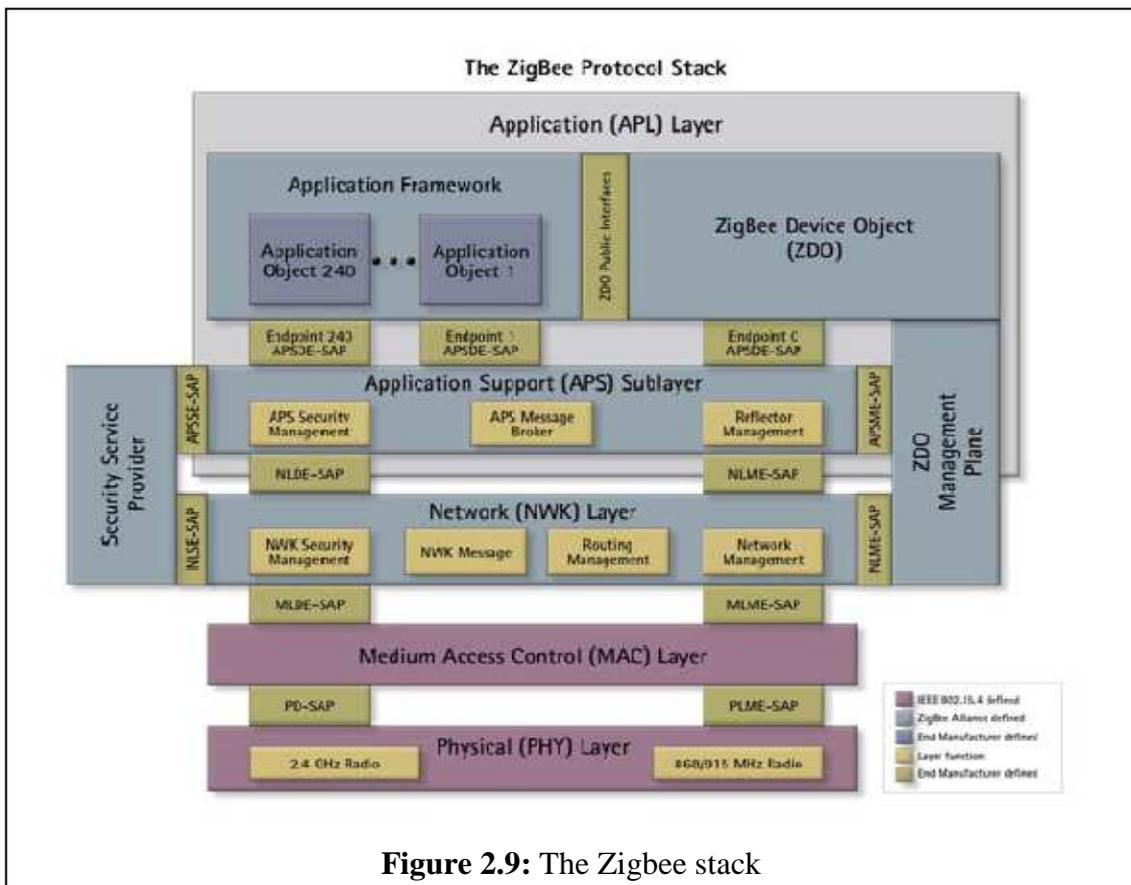


Figure 2.9: The Zigbee stack

Following are the layers of the Zigbee stack, which are devoted for Zigbee applications.

- **Zigbee Application (APL) Layer:**

The top layer in the Zigbee protocol stack consists of the Application Framework, Zigbee Device Object (ZDO), and Application Support (APS) Sub-layer.
- **Application Framework:**

It provides a description of how to build a profile onto the Zigbee stack. It also specifies a range of standard data types for profiles, descriptors to assist in service discovery, frame formats for transporting data, and a key value pair constructs to rapidly develop simple attribute-based profiles.
- **Application Objects**

It is a part of the layer that controls the Zigbee device. A single Zigbee node supports up to 240 application objects. Each application object supports endpoints numbered between 1 and 240 (with endpoint 0 reserved for the Zigbee Device Object (ZDO)).
- **Zigbee Device Object (ZDO)**

Defines the role of a device within the network (Coordinator, router or end device), initiates and responds to binding and discovery requests, and establishes a secure relationship between network devices. It also provides a rich set of management commands defined in the Zigbee Device Profile.
- **ZDO Management Plane**

Facilitates communication between the APS and NWK layers with the ZDO. It Allows the ZDO to deal with requests from applications for network access and security using ZDP (Zigbee Device Profile) messages.
- **Application Support (APS) Sublayer**

Responsible for providing a data service to the application and Zigbee device profiles. It also provides a management service to maintain binding links and the storage of the binding table itself.
- **Security Service Provider (SSP)**

It provides security mechanisms for layers that use encryption (NWK and APS). Initialized and configured through the ZDO.
- **Network (NWK) Layer**

Handles network address and routing by invoking actions in the MAC layer. Its tasks include starting the network (Coordinator), assigning network

addresses, adding and removing network devices, routing messages, applying security, and implementing route discovery.

- **Zigbee Security**

Zigbee security, which is based on a 128-bit AES algorithm, adds to the security model provided by IEEE 802.15.4. Zigbee's security services include methods for key establishment and transport, device management, and frame protection.

2.8 Programming of the Zigbee Devices: The X-CTU:

As discussed earlier, the Zigbee device, can be called as Xbee, should be configured before deploying the same into respective WSNode. The architecture of the device reveals that it has two sections, microcontroller based section and communication based section. Both parts are configurable and can be configured as per need. Present work is based on development of WSN to ensure Precision Agriculture. It comprises WSNode, wherein Zigbee are deployed. Therefore, to configure the devices the Digi Corporation has provided an Integrated Development Environment (IDE) called "Xbee Configuration and Test Utility (X-CTU)". Therefore, employing this IDE the Zigbee devices are programmed and then deployed for present WSN.

The X-CTU is open source window based software. The window of X-CTU is presented in figure 2.10. As shown in figure 2.10, it has four menus employing sequentially, the device can be not only programmed but also tested. Following are the four menus.

a) PC Settings: Allows a programmer to select the desired COM port and configure that port to fit the radios settings.

The PC Settings tab is broken down into three basic areas: The COM port setup, the Host Setup, and the User Com ports.

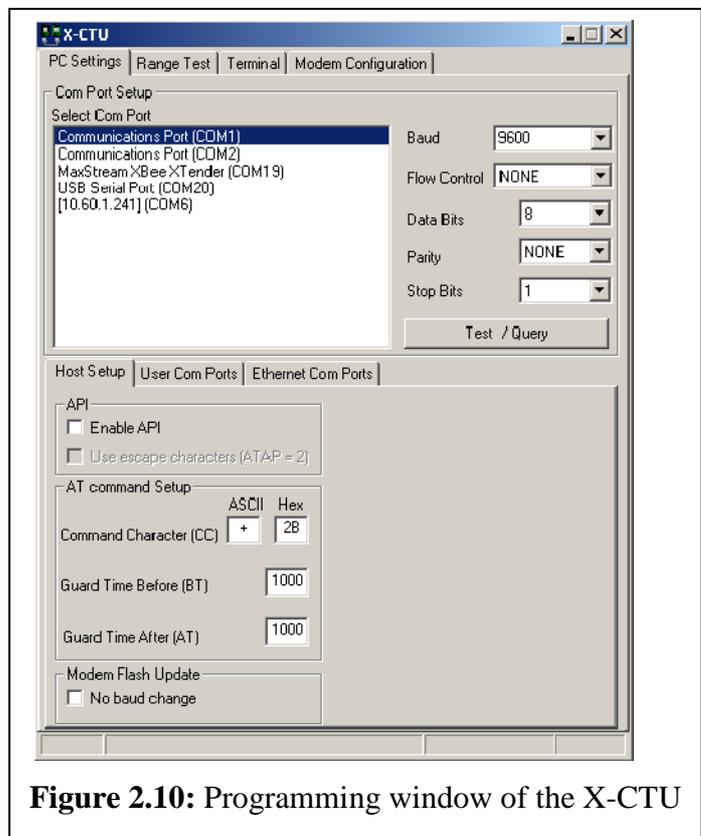


Figure 2.10: Programming window of the X-CTU

i) **COM port setup:**

The PC settings tab allows the user to select a COM port and configure the selected COM port settings when accessing the port. Some of these settings include:

- ✓ **Baud Rate:** Both standard and non-standard
- ✓ **Flow Control:** Hardware, Software (Xon/Xoff),
- ✓ **None Data bits:** 4, 5, 6, 7, and 8 data bits
- ✓ **Parity:** None, Odd, Even, Mark and Space
- ✓ **Stop bit:** 1, 1.5, and 2

To change any of the above settings, select the pull down menu on the left of the value and select the desired setting. To enter a non-standard baud rate, type the baud rate into the baud rate box to the left. The Test / Query button is used to test the selected COM port and PC settings. If the settings and COM port are correct, you will receive a response similar to the one depicted in Figure 4 below.

ii) **Host Setup:**

The Host Setup tab allows the user to configure how the X-CTU program is to interface with a radio's firmware. This includes determining whether API or AT command mode will be used to access the module's firmware as well as the proper command mode character and sequence. By default, the Host Settings are as follows: API mode: not enabled (Not checked) Command mode Character: + (ASCII) 2B (Hex). Before Guard Time: 1000 (1 Sec) After Guard Time: 1000 (1 Sec)

iii) **User COM ports:**

The user COM port option allows the user to "Add" or "Delete" a user-created COM port. This is only for temporary use. Once the program has closed, the user-created COM port will disappear and is no longer accessible to the program.

b) **Range Test:** Allows a programmer to perform a range test between two radios.

The range test tab is designed to verify the range of the radio link by sending a user-specified data packet and verifying the response packet is the same, within the time specified. By default, the size of the data packet sent is 32 bytes. This data packet specified can be adjusted in either size or the text sent.

Figure 2.11 depicts the details of this range test menu. To modify the size of the packet sent, change the value next to the “Create Data” box and click on the “Create Data” button. If programmer want to change the data sent, delete the text in the transmit window and place in your desired text. By modifying the text, data packet size, packet delay and the data receive timeout; the user is able to simulate a wide range of scenarios. **RSSI:** The RSSI option of the X-CTU allows the user to see the RSSI (Received Signal Strength Indicator) of a received packet when performing a range test.

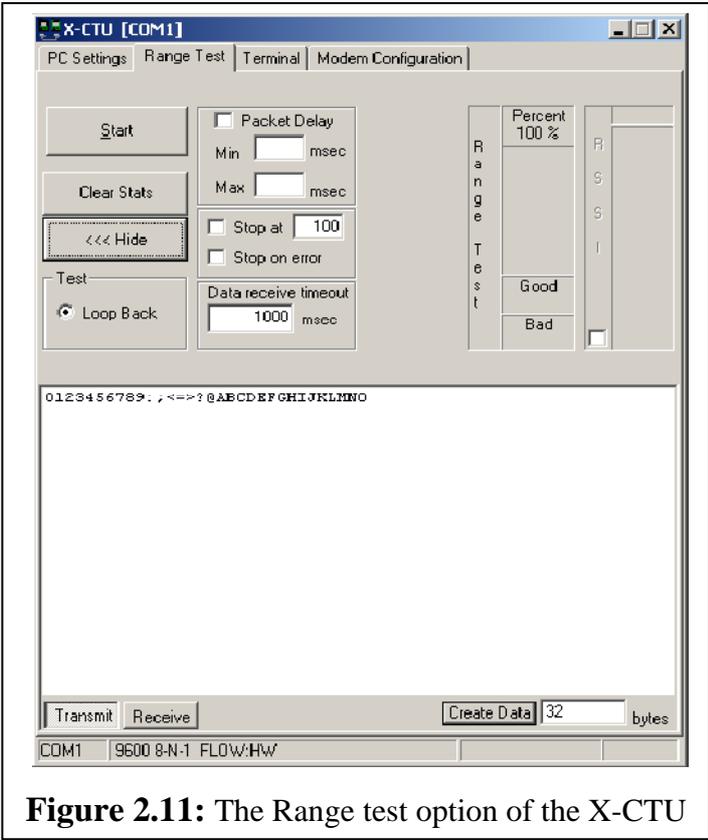


Figure 2.11: The Range test option of the X-CTU

API Function:

The X-CTU also allows the user to test the API function of a radio during a range test. To perform a range test with the API function of the radio, follow the steps outlined below:

1. Configure the Base with API enabled and a unique 16 bit or 64 bit source address.
2. Configure the remote radio with a unique source address and set the Destination address to equal the Base radio’s source address.
3. Enable the API option of the X-CTU on the PC Settings tab and connect the base radio to the PC (See Figure 3).
4. Connect the red loopback adapter to the remote radio and place them a distance apart.
5. Enter either the 16 bit or 64 bit destination address of the remote radio into the Destination Address box on the Range Test tab.
6. Create a data packet of your choosing by typing in the data in the Transmit box

7. To start a Range test, click on Start. You will notice the TX failures, Purge, CCA, and ACK messages will increment accordingly while the range test is performed. To stop a range test, click on the Stop button

c) Terminal: Allows access to the computers COM port with a terminal emulation program. This menu also helps to ensure hardware emulation. This tab allows the ability to access the radios firmware using AT commands.

The Terminal tab has three basic functions: Terminal emulator Ability to send and receive predefined data packs (Assemble packet) Ability to send and receive data in Hex and ASCII formats (Show/Hide hex)

i)The main terminal window

The main white portion of this tab is where most of the communications information will occur while using X-CTU as a terminal emulator. The text in

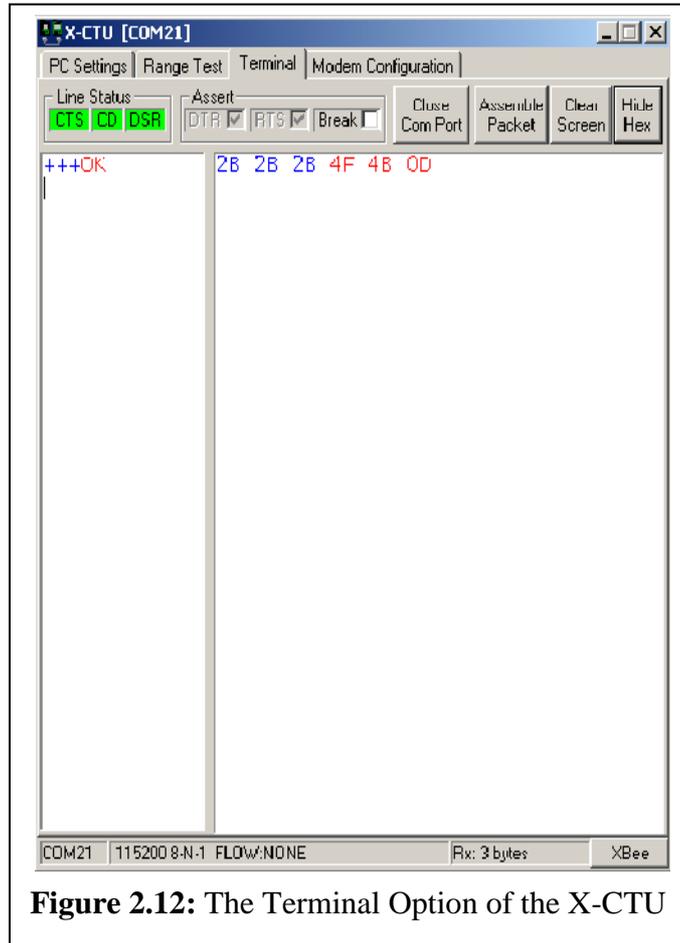


Figure 2.12: The Terminal Option of the X-CTU

blue is what has been typed in and directed out to the radio’s serial port while the red text is the incoming data from the radio’s serial port (Figure 2.12).

ii)Assemble Packet

The Assemble Packet option on the Terminal tab is designed to allow the user to assemble a data packet in either ASCII or Hex characters. This is accomplished by selecting the Assemble packet window and choosing either ASCII (default) or Hex. Once selected, the data packet is assembled by typing in the desired characters.

d) Modem Configuration: Allows the ability to program the radios’ firmware settings via a Graphical User Interface. Architecture of the modem configuration menu of the X-CTU is depicted in figure 2.12. As presented in figure 2.12, the Modem configuration tab has four basic functions:

1. Provide a Graphical User Interface with a radio's firmware
2. Read and Write firmware to the Zigbee.
3. Download updated firmware files from either the web or from a compressed file
4. Saving or loading a modem profile

i) Reading a Zigbee firmware:

To read a radio's firmware, follow the steps outlined below:

1. Connect the Zigbee module to the interface board and connect this assembly to the PC's corresponding port
2. Set the PC Settings tab to the Zigbee default settings.
3. On the Modem Configuration tab, select "Read" from the Modem Parameters and Firmware section (Figure 2.13).

ii) Modification in the Zigbee firmware setting:

Once the Zigbee firmware has been read, the configuration settings are displayed in three colors (Figure 2.13).

Black : Not configurable
Green: Set to Default value
Blue : Programmable as per the need of present WSN. To modify any of the use settable parameters, click on the associated command and type in the new value for that parameter. For ease of understanding a specific command, once the command is selected, a quick description along with its limits is also

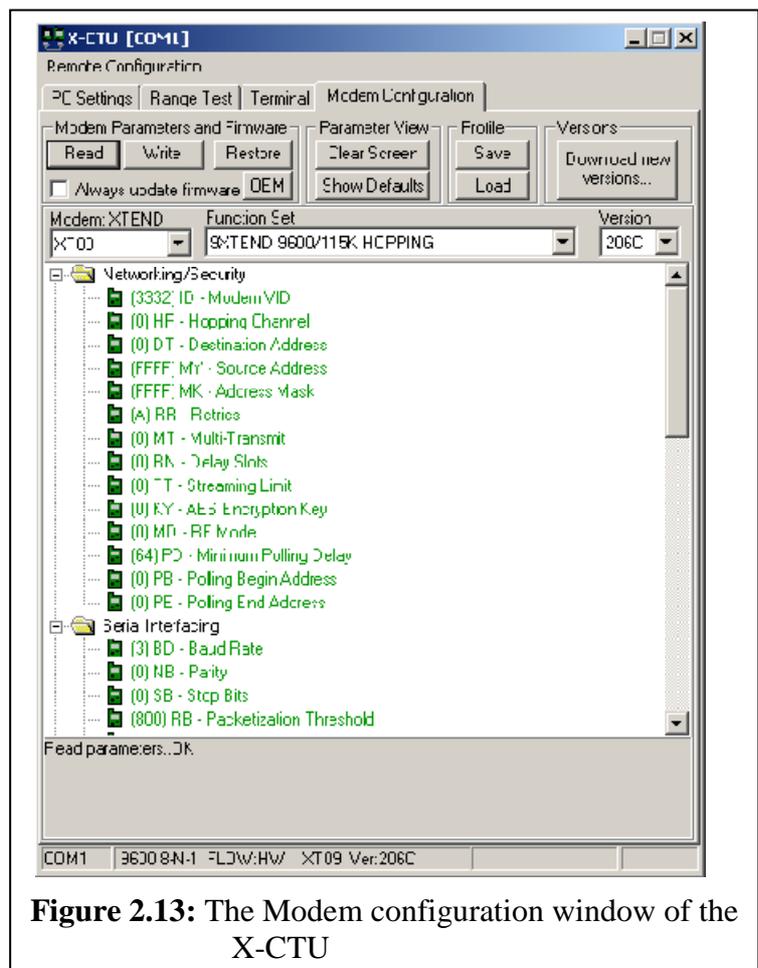


Figure 2.13: The Modem configuration window of the X-CTU

provided at the bottom of the screen. Once all of the new values have been entered, the new values are ready to be saved to the Zigbee's non-volatile memory. List of programmable fields and values to be entered are presented in table 2.5.

ii) Writing firmware to the Radio

To write the parameter changes to the Zigbee non-volatile memory, click on the Write button located in the Modem Parameters and Firmware section (Figure 2.13). Downloading Updated Firmware Files. Click on OK and Done when prompted. Following these steps the device can be programmed.

2.9 Programming of the Zigbee for present WSN:

The WSN designed to ensure Site Specific Crop Management (SSCM), consists of total 10 WSNodes. Out of these 10 devices 9 WSNodes are configured as End devices and one is configured as Coordinator. As shown in figure 2.13, the modem configuration window should be selected for programming the Zigbee. While programming, as stated above, the default setting of the device should read. Before beginning of the configuration, the device must be selected. Here, the device, XB24-B is selected. Then, the function for which the device to be programmed is selected. The devices are configured as End Devices. In table 2.5, fields to be reconfigured are presented. The Table 2.5 also represents the by default values and values of the parameters used for present WSN. Table 2.5(a) is for Parameters for configuration of Zigbee device as End Device, whereas, Table 2.5(b) is for Parameters for configuration of Zigbee device as Coordinator.

Out of above few field are configurable and rest will be set their default values. The details regarding parameters and its configuration are illustrated through following points.

- a) **Addressing:** During networking the addresses of the contributing devices plays vital role. Each device, End Device, Router and Coordinator, should be associated with their own addresses. Address of the device defines its place on the network. For addressing the End devices and Routers, the address fields are essential.

TABLE 2.5(a) Parameters for configuration of Zigbee device as End Device

Sr. No.	Parameter Symbol	Parameters Name	Values used for present configuration
1.	ID	PAN ID	1
2.	DH	Destination Address High	0
3.	DL	Destination Address Low	0
4.	BH	Broadcast Radius	0
5.	SC	Scan Channels	1FFE
6.	SD	Scan Duration	3
7.	JN	Join Notification	1
8.	NJ	Node Join Time	FF
9.	NI	Node Identifier	Node 1 to Node 9
10.	DD	Device Type Identifier	0
11.	NT	Node Discovery Timeout	3C
12.	AR	Aggregation Route Broadcast Time	FF
13.	PL	Power Level	4
14.	PM	Power Mode	1
15.	BD	Baud Rate	3
16.	NB	Parity	0
17.	R0	Packetization Timeout	3
18.	D7	DIO7 Configuration	1
19.	D6	DIO6 Configuration	0
20.	CT	AT Command Mode Timeout	64

TABLE 2.5 (b): Parameters for configuration of Zigbee device as a Coordinator

Sr. No.	Parameter Symbol	Parameters Name	Values used for present configuration
1.	ID	PAN ID	1
2.	DH	Destination Address High	0
3.	DL	Destination Address Low	0
4.	BH	Broadcast Radius	0
5.	SC	Scan Channels	1FFE
6.	SD	Scan Duration	3
7.	JN	Join Notification	1
8.	NJ	Node Join Time	FF
9.	NI	Node Identifier	-
10.	DD	Device Type Identifier	0
11.	NT	Node Discovery Timeout	3C
12.	AR	Aggregation Route Broadcast Time	FF
13.	PL	Power Level	4
14.	PM	Power Mode	1
15.	BD	Baud Rate	3
16.	NB	Parity	0
17.	R0	Packetization Timeout	3
18.	D7	DIO7 Configuration	1
19.	D6	DIO6 Configuration	0
20.	CT	AT Command Mode Timeout	64

- **Destination Address (DH & DL):** There are two fields, DH and DL, which configures the destination address to which the data is to be transmitted. This sets the lower 32 bits of destination address. In addition to this, each node is having default address, MY address as 0. As presented in table 2.5, it is configured for 0. However, to configure in broadcast mode the address should

be set to FFFF. Also, by employing different addresses, more than one WSN can be established in desired area.

b) Networking: The XBee devices are configured to ensure WSN. Basically, this field is used to configure the device for proper address and frequency. Following parameters are configured.

- **Channel (CH) Setting:** This is employed to set operating frequency of Xbee device within 2.4 GHz band. As discussed in topic 1, the Zigbee operates with IEEE 802.15. 4 standards with two bands. Out of total 27 channels, the 915 MHz band is having 11 channels, whereas 2.4 GHz is having remaining 16 channels. Therefore, the channels allocated for XBee devices (2.4GHz band) are 16. The address starts from 0C to 1A. This full range is available for non pro XBee devices. However, for XBee –Pro, it is constrained within the range C to 17 [18]. For present WSN pro devices are employed. Therefore, channels of the devices (XBee Series 2) are set to default value C [Table 2.5]. On configuration of channel number, it also possible to deploy more than one networks to ensure preciseness in the SSCM.
- **PAN ID (ID) setting:** Essentially, the network ID, the unique ID of the Personal Area Network. The devices with matching PAN-ID will establish communication only. For present WSN the devices of series 2 are deployed. Therefore, for programming this device, the modem type XB24-B is assigned. These Zigbee devices are having extended PAN ID with the valid range from 0 to 3FFF. However, at present the devices are configured at its default address by setting this field to 0 [Table 2.5].
- **Broadcast Radius (BH):** The Broadcast radius (BH) is set to 0 to use optimum broadcasting range.
- **Serial Number (SH & SL):** The two fields, such as Serial number High (SH) and Serial number Low (SL) are the serial number of the Zigbee devices and these are popped up during reading of the device.
- **Scan Channel (SC) and Scan Duration (DS):** Now Scan Channel (SC) and Scan Duration (DS) are the two parameters. The SC indicates number of channels to be scanned before joining the network. Moreover, the SD depicts the

time required to scan the channels. The SD, scan time can be obtained from the expression

$$\text{Scan Time (ms)} = \text{SC} \times (2^{\text{SD}}) \times 15.36 \text{ ms} \quad \dots 1$$

Setting of the SD and SC is given in table 2.5.

- **Join Notification (JN):** When device joins the network, this value determines to whom the joining notification message is to be sent. For present case, each nodes have to join to the Coordinator node. Therefore, this field is set to 1. It is to be noted that this field of configuration is available only for configuration of the End devices and not for that of Coordinator.
 - **Node Join Time (NJ):** The value of NJ determines the time (s) that the device will allowed other device to join. It is set to FF, so that the router will be allowed to join the network.
 - **Node Identifier (NI):** This field plays vital role during debugging and simulation of the network as well. The node identifier allows us to assign a noun to the Zigbee node to be seen when a node discovery is performed. For present WSN, the names Node 1 to Node 9 are assigned. This field is availed to assign the names for each WSNode and not to the Coordinator node.
 - **Device Type Identifier (DD):** This field is used to configure the device type. It can be used to differentiate multiple XB based products. As shown in table 2.5, it is set to 0.
 - **Node Discovery Timeout (NT):** This is used to configure the time out for discovery of the nodes. It can be 1 to FC. However, it is programmed to 3C, so that the node discovery time out would be (3C x 100 ms) 6000ms.
 - **Aggregation Route Broadcast Time (AR):** This should be configured for no more than one in the network to establish route the network to the node. Setting this to FF disables the aggregation of the route broadcasting. This ensures to avoid the aggregation of the data at the Coordinator.
- c) **RF Interfacing:** For realization of wireless communication the Zigbee devices are employed in each WSNode. For RF communication the power is essential parameter to be considered. There are two parameters for configuration, the power levels (PL) and power mode (PM).

- **Power Level (PL):** It determines the transmitter output power. There are 5 power levels to be configured. The table 2.6 presents power levels to which the device can be configured.

TABLE 2.6: Power levels of the devices

Number to be used	Power level	Amount of power dBm
0	Lowest	-7
1	Low	-3
2	Medium	-1
3	High	1
4	Highest	3

For present case, the power level of the devices is configured to 4 (3dBm)

- **Power Mode (PM):** It is used to enable or disable the boost mode. If enabled, if enabled the boost mode improves the sensitivity by 1dB and increases out power by 2dB. It also helps to improve the link margin and range as a well. For present WSN, it is enabled by setting the parameter to 1.
- d) Serial Interfacing:** The Zigbee devices are interfaced to the microcontroller in each WSNode and Coordinator to the PC through serial port. In fact, the devices are serial devices. The two pins DIN and DOUT ensure the serial communication for which required interfacings must be used and configured. While establishing serial communication, the parameters such as Baud rate, Packetization time out etc play vital role. In this field, three parameters are essentially set. The Baud rate is configured for 9600 and parity bit to No Parity. The D6 and D7 bits are assigned for configuration of CTS flow control.

Following fields are also programmable. But present case these field are used as their default setting values.

- e) Security.
- f) Sleep mode
- g) IO setting
- h) AT command option
- i) Diagnostic options

2.10 Conclusion:

With the view to deploy Zigbee technology for present investigation, the details regarding this innovative Zigbee technology are explored. Basically, the wireless communication is governed according to the standards laid down by the respective IEEE working group, IEEE 802.15.4. In association with Digi Corporation, this technology is emerged as Zigbee technology. The architectural details of Zigbee devices are intensively studied. The Zigbee devices incorporate a separate hardware block, on-chip, to ensure the wireless communication and the individual stack which comprises the PHY and MAC layers of IEEE 802.15.4 standards. The salient features of Zigbee devices make it suitable to deploy for design of Wireless Sensor Node that ensure serial communication with data rate 250 kbps.

A highly sophisticated programming environment 'X-CTU' is employed for programming of the Zigbee devices, either in Coordinator mode or end device mode. The X-CTU also provides smart terminal to ensure the process of debugging. Employing this IDE the Zigbee devices are programmed with the device ID as node1 to node 9 in broadcast mode. The Coordinator is also configured. All devices are configured for low power mode. The Zigbee devices are successfully wired into the WSNodes and they are operating with great reliability.

References:

1. J. K. Hart and K. Martinez' "Environmental Sensor Networks: A Revolution In The Earth System Science", *Earth-Science Reviews*, 78 3–4 (2006) 177–191.
2. J. Tang, B. Hao and A. Sen, "Relay Node Placement In Large Scale Wireless Sensor Networks", *Computer Communications*, 29 4 (2006) 490–501.
3. J. Elson, L. Girod, and D. Estrin, "Fine-Grained Network Time Synchronization Using Reference Broadcasts", *Proceedings of the Fifth Symposium on Operating Systems Design and Implementation*, (2002) 141–163.
4. P. A. M. Abusali, B. D. Tapley, and B. E. Schutz. "Autonomous Navigation of Global Positioning System Satellites Using Cross-Link Measurements", *Journal of Guidance, Control, and Dynamics*, 21 2 (1998) 321-327.
5. A.M. Pawar, S. N. Patil, A. S. Powar and B. P. Ladgaonkar, "Wireless Sensor Network To Monitor Spatio-Temporal Thermal Comfort Of Polyhouse Environment", *International Journal of Innovative Research in Science, Engineering and Technology*, 2 10 (2013) 4866-4875.
6. J. H. Moon and T. K. Ha, "A Car Parking Monitoring System Using Wireless Sensor Networks", *International Journal of Electrical, Robotics, Electronics and Communications Engineering*, 7 10 (2013) 843-846.
7. A. R. Priyadarshini and K. Sabarinathan, "Reducing Energy Consumption On Design of Sensor Node in WSN", *Proceedings of 2nd International Conference on Science, Engineering and Management*, Srinivasan Engineering College, Tamil Nadu, India, (2014) 248-253.
8. E. K. Lee, M. Gerla and S.Y. Oh, "Physical Layer Security In Wireless Smart Grid", *IEEE Communications Magazine*, 50 8 (2012) 46 – 52.
9. K. Selvarajah, A. Tully and P.T. Blythe, "ZigBee for Intelligent Transport System Applications", *Road Transport Information and Control - RTIC 2008 and ITS United Kingdom Members' Conference*, Manchester, (2008) 1 – 7.
10. S. Farahani, "ZigBee Wireless Networks and Transceivers", Elsevier Publication, USA.
11. <http://en.wikipedia.org/wiki/XBee>
12. Texas Instruments, Transceiver CC2520, last modified: January 2010 <http://www.ti.com/product/cc2520>

13. Texas Instruments, Transceiver CC2420, last modified: (2008)
<http://www.ti.com/product/cc2420>
14. A. Wheeler and E. Corporation, “Commercial Applications of Wireless Sensor Networks Using Zigbee”, IEEE Communication Magazine (2007) 70-77.
15. <http://www.adafruit.com/datasheets/XBee%20ZB%20User%20Manual.pdf>
16. R. Piyare and S. Lee, “Performance Analysis Of Xbee ZB Module Based Wireless Sensor Network”, International Journal of Scientific & Engineering Research, 4 4 (2013) 1615-1621.
17. A.A. Khan, A.I.E Yakzan and M. Ali, “Radio Frequency Identification (RFID) Based Toll Collection System”, IEEE Third International Conference on Computational Intelligence, Communication Systems and Networks, (2011) 103 – 107.
18. http://www.parallax.com/sites/default/files/downloads/32316-Propeller-MGH-Ch5-XBee_0.pdf