**1.1 Wireless Communication**

When it comes to wireless communication, there are many developments that have been made to the field in the past 20 years. Some of these developments include Wi-Fi (developed by the Wi-Fi Alliance, introduced in 1998), Bluetooth (introduced by Ericsson in 1994, developed by the Bluetooth Special Interest Group), and ZigBee (developed by ZigBee Alliance, introduced in 1998).

* + 1. **Why use wireless communication?**

Wireless communication allows multiple different devises to be connected over a wireless network. This allows devises to be self-contained without the inconvenience of communication wires. Moreover, if wires are required for communication, the system is very static. Wireless communication allows for a dynamic system that can grow and change as system requirements change.

The S.M.A.R.T Alarm system will rely heavily on wireless communication, transmitting sensor data to the central processing and direction data back to the alarms. S.M.A.R.T. Alarm is a dynamic system, have different configurations and alarm needs deepening on the building. Wireless communication is a core component of the S.M.A.R.T. Alarm system. The following section will provide information on the aforementioned wireless communication options and will discuss the feasibility of their inclusion in the S.M.A.R.T Alarm system.

**1.1.2 Wireless Fidelity (Wi-Fi)**

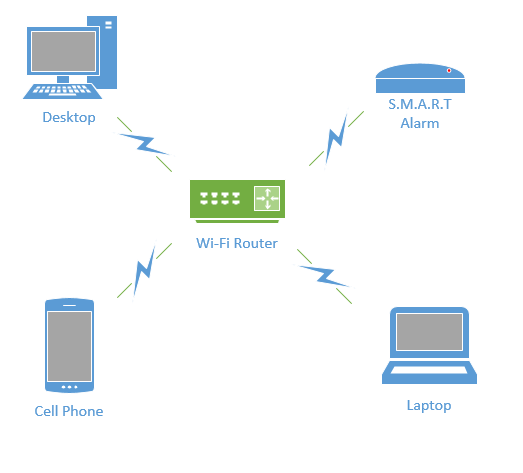
As the most commonly used form of wireless communication, Wi-Fi is used in nearly every household in the world. A Wi-Fi router covers an area, such as a household or business, with a blanket of Wi-Fi signal which allows any smart device to connect to the internet.

Introduced for commercial use in 1998, Wi-Fi is a Wireless Local Area Network (WLAN) that is based on the IEEE 802.11 standards. IEEE 802.11 is the radio frequency needed to transmit packets over radio links. These data packets are known as Ethernet frames, which have built-in error checking. This means that if a data packet is altered or destroyed before it reaches its destination, the packet will be resent until it is confirmed that it was received by its target. IEEE 802.11b and 802.11g use the 2.4 GHz industrial, scientific and medical (ISM) radio bands. Due to the choice of this frequency band, Wi-Fi devices occasionally experience interference by other RF devices and devices such as microwave ovens, cell phones, Bluetooth and ZigBee devices.

Spectrum assignments for the 2.4GHz band are not the same worldwide. For example, the U.S. only permits 11 channels for the 2.4GHz band to be operated without a license, whereas Australia and Europe allow two additional channels (12 and 13).  A Wi-Fi signal occupies five channels in the 2.4 GHz band, therefore it is only possible to have a group of three non-overlapping channels (Channels 1, 6 and 11) in the U.S.

All Wi-Fi certified devices will work with any Wi-Fi access point anywhere in the world, proved they can make it through the security checkpoints such as Wired Equivalent Privacy or WEP (which has been phased out due to weakness of security) or the more popular Wi-Fi Protected Acces[s](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) (WPA and WPA2) which requires a passcode for access to the network.

Wi-Fi range is dependent on the frequency band, radio power output, antenna type and gain as well as the technique used in modulation. A Wi-Fi access point that complies with either the 802.11b or 802.11g protocols, using a stock antenna, can get a range of about 100 meters (330ft). However, using multiple access points such as multiple routers, allow for network redundancy and higher ranges.



Overall, Wi-Fi would be an excellent form of wireless communication for the S.M.A.R.T Alarms, if not for the power consumption of transmitting and receiving Wi-Fi signals. Because the S.M.A.R.T Alarms will be powered by batteries as a backup power source, a more power efficient communication system may be desired.

**1.1.3 Bluetooth**

Bluetooth is a wireless communication technology used to transmit and receive data over short distances using short-wavelength UHF radio waves in the industrial, scientific and medical (ISM) bands (2.4 - 2.485 GHz). Most Bluetooth networks have a range of only about 10 meters (30 ft.) depending on signal strength and obstructions, classifying their networks as Personal Area Networks (PANs). The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard.

Bluetooth has a master-slave structure and is a packet based protocol. One master may communicate with up to 7 slaves, all the slaves sharing the master's clock. Bluetooth uses a frequency-hopping spread spectrum radio technology to transmit the data packets over one of 79 designated Bluetooth channels. Each one of these channels have a bandwidth of 1 MHz, and it usually transmits at 800 hops per second. Security in a Bluetooth system is very weak compared to other wireless communication systems, only relying on a four-digit encryption, compared to the twelve-digit encryption you get from Wi-Fi securities. Due to the limited range (about 30 ft.) and lack of proper encryption, associated with Bluetooth transmission, it is not feasible to use Bluetooth in the S.M.A.R.T. Alarm systems.

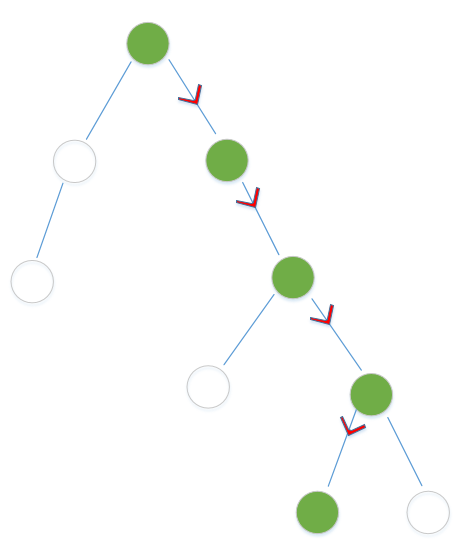
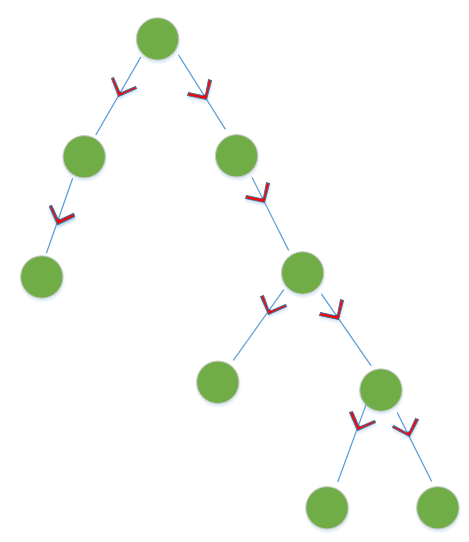
**1.1.4 Radio Frequency**

Radio Frequency or RF is a very common form of wireless communication around the world. RF can be integrated into a system with relative ease due to the versatility of RF systems. RF signals can travel very long distances (at low frequencies) and can travel through many different mediums with relative ease (i.e. Water, Air, Solids, Space). Radio Frequency communication is widely use throughout the United States as well as the rest of the world and since RF can be transmitted at such a wide variety of frequencies, it is very strongly regulated. There is only a small range of frequencies that can be transmitted without needing a license or permission from the federal government.

Communication protocols like WIFI, Bluetooth and ZigBee all operate in the 2.4 GHz frequency range, an approved (unlicensed) ranged for transmission signals. If the S.M.A.R.T. Alarm were to use RF communications to transfer data packets, it would require the design of a proprietary protocol to modulate and demodulate the signal to work. Communication systems like WIFI and ZigBee already have these established protocols, making using them a for feasible form of wireless communication than RF.

**1.1.5 ZigBee**

ZigBee is an IEEE 802.15.4 based high level wireless communication system. ZigBee creates Personal Area Networks (PANs) with relatively small low power radios. Used mostly in home automation and other low-power low-bandwidth application, ZigBee communication is great for small scale projects that need wireless communication. ZigBee was designed to be more simple and less expensive than other wireless PANs, like Wi-Fi or Bluetooth. ZigBee is described as “a low power, inexpensive, wireless mesh network standard that is employed throughout many applications that utilize wireless sensor networking and control” [E].

Due to ZigBee’s low power consumption, it limits transmission ranges to about 10-100 meters line-of-sight depending on power output and environment. However, using a mesh network, data can be transferred from one device to another, allowing for an expansive range. A mesh network is a type of network that relies on relaying data from node to node. A mesh network can transfer this data by using either a flooding method or a routing method. The routing method propagates a message from one router node to the next, until it reaches its destination. Algorithms are used to ensure that the shortest transmission paths are used, continuously checking for path availability. If a node is damaged or unusable, the system will “self-heal” and adjust its data path to reach its end goal. Due to this dynamic routing, these types of systems are very reliable, prone to very few errors. The flooding method is a process in which a data packet is sent out from a coordinator and sent through every outgoing node in the network. There are two types of flooding, uncontrolled and controlled flooding. Uncontrolled flooding is not a preferred method of networking because the neighboring nodes will send packets indefinitely, causing a broadcast storm. A broadcast storm consumes up a great deal of network resources, which can cause a system to be unable to further transfer data. However, controlled flooding utilizes two algorithms to make it a reliable networking solution. Each data packet in a controlled flood is labeled with an address and sequence number. Router nodes in the network keep track of the senders and sequence numbers it has received and only forwards packets that they have never seen before. Therefore, each of these router nodes may receive a packet more than once, but will only forward the packet one time. The network then utilizes Reverse Path Forwarding to notify the coordinator that the packet has been successfully sent to all routers in the network so it can stop transmission of that data packet [C].

Flooding Network Method

Routing Network Method

The S.M.A.R.T. Alarm will utilize both routing and flooding transmission methods. It will use a routing method to send Smoke Alarm sensor data to the coordinator, using the fastest transmission path possible. Once the coordinator receives this data, it will do the necessary calculations and exit route mapping and send the alarm and direction packets out to all the alarms in the system using the controlled flooding technique. The combination of these two routing methods will ensure the S.M.A.R.T. Alarm works properly and efficiently in alerting the inhabitance of a building of a potential fire.

ZigBee operates in the ISM radio bands (2.4 GHz) with data transmission rates varying from 20 kbit/s for the 868 MHz band to 200 kbits/s at the 2.4 GHz band. ZigBee can support both star and tree networks, as well as generic mesh networking. Every ZigBee network must have one coordinating device which essentially creates the network environment, control over the network parameters and basic maintenance of the system. In a star network, the coordinating device must be the central node, in contact with all other devices. However, tree and mesh networks both allow use of ZigBee routers to extend communication at a network level.

ZigBee builds on IEEE 802.15.4 standards of physical layer and media access control for low rate PANs. There are four key components in addition to the set standards. Those additions are a network layer, application layer, manufacturer defined applications, and ZigBee device objects. These additions allow for customization and total integration of a system. ZigBee device objects or ZDOs are responsible for keeping track of device roles, managing network join requests as well as device discovery and security.

There are three kinds of ZigBee devices:

* ZigBee Coordinator - Described Above
* ZigBee Router - Runs applications as well as acting as intermediate router in a mesh or tree network. Requires less memory than Coordinator but more than End Device. Power consumption higher than that of End Device.
* ZigBee End Device - Has just enough functionality to communicate with parent node (Coordinator or Router). Cannot relay data from other devices. Gives the best battery life due to lack of need for communication and ability to enter sleep mode.

Software for ZigBee is designed to be easy to develop on small, inexpensive microprocessors, which will cut down on costs as well as time needed to set up the network. This is important when it comes to budgeting, as well as creating a product that is cost efficient and reasonably priced for a consumer.  Since ZigBee has very low power usage and low data rate (250 kbit/s), it is a great communication tool for battery powered devices. ZigBee also has a great security system (128-bit symmetric encryption keys). These factors make it best suited for occasional data transfers from sensors or input devices [B].

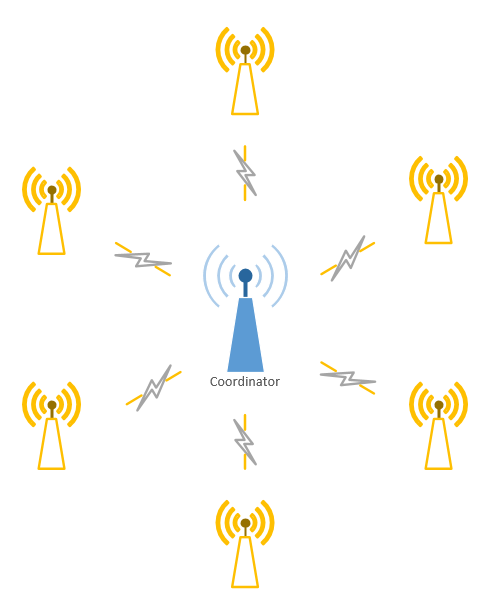
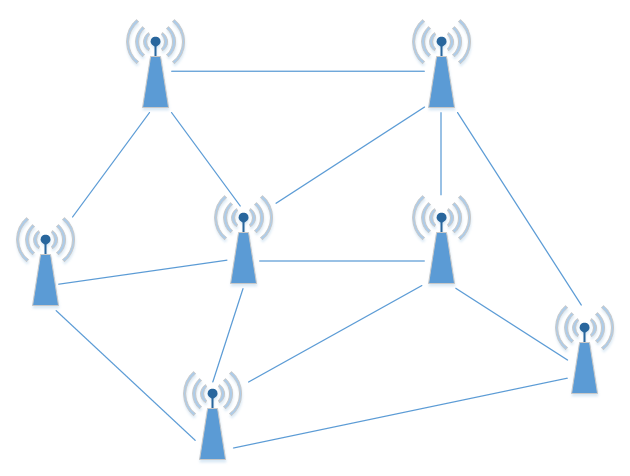
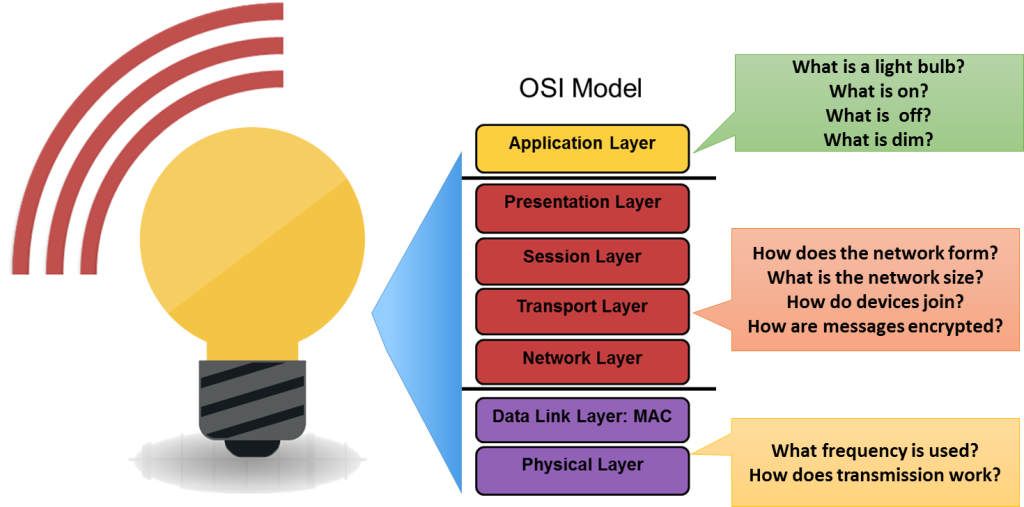
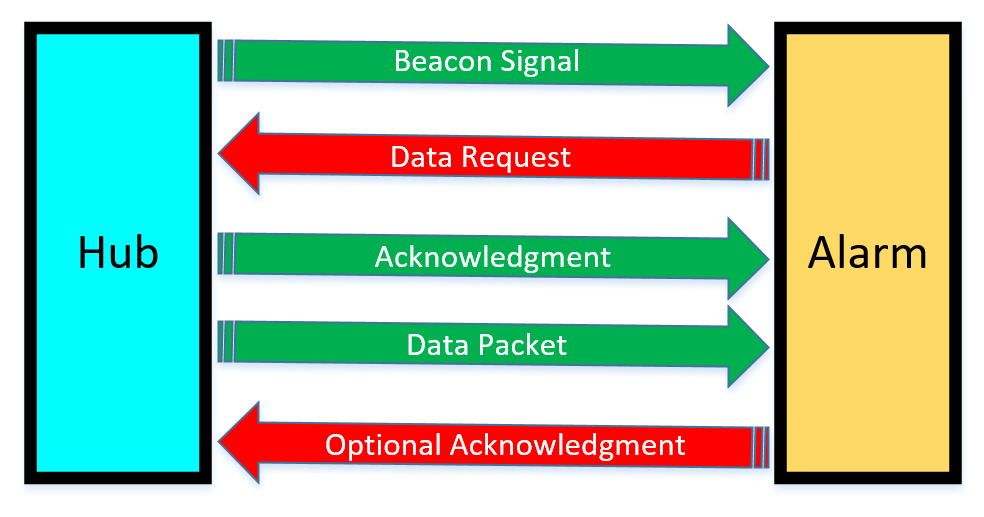
 

Figure 1.1.5-1 ZigBee Star Network Figure 1.1.5-2 ZigBee Mesh Network

**ZigBee Protocol**

As previously mentioned, ZigBee communication uses the IEEE 802.15.4 protocol. IEEE 802.15.4 is one of the largest standards for low power, low data rate WPANs. IEEE 802.15.4 defines the Physical Layer (frequency, modulation, power and other wireless conditions) and Media Access Control Layer (format of data handling and data linking) of the Open System Interconnection (OSI). The 802.15.4 also uses two additional sublayers, Logical Link Control and Service Specific Convergence Sub-Layer, to allow communication with all upper OSI layers. These upper layers come from the ZigBee enhancement to the IEEE 802.15.4. ZigBee uses layers 3 and above to define additional communication features, such as encryption, data routing, authentication with valid nodes and forwarding capabilities (which allows for mesh networking). Due to this, ZigBee is the most popular wireless sensor for mesh networks [A]. These processes are done in either the Network, Transport, Session, Presentation or Application level of the ZigBee system.

Data is transferred in either a beacon or non-beacon network. In a beacon network, if the coordinator needs to transmit data to a device or group of devices, it first sends out a beacon signal that tells the devices that there is data ready to be transferred. The coordinator then waits for the device or devices to send a data request message meaning that it is ready to receive data. The coordinator acknowledges this message and begins to send the data to the device, the device can then send an optional acknowledgement message back to the coordinator to confirm the data was received. In a non-beacon network, the coordinator must wait for the reception of a data request from a device to send data. Once the data request is received by the coordinator, the process is the same as the beacon network. [D]



Error detection is a very important part of the ZigBee protocol. An error can occur in a ZigBee system when one or are received differently from the way they were sent [C]. There are two types of errors, bit and burst errors. A bit error occurs when the probability of error is the same for each bit, and a burst error occurs when the error probability is greater for bits near another error. In either case, and error is when for whatever reason, and bit or bits in a data packet are corrupt and flipping from 0 to 1 or 1 to 0. To detect and fix these types of errors, the ZigBee system makes use of three different techniques; Parity, Check-sums, and Cyclic Redundancy Checks (CRCs).

Parity is used to find a single bit error. A bit is added at the end of each frame such that the total number of bits an even parity or odd parity. These parities are checked again when data transfer is completed to see if a bit has been corrupted. This technique works in multiple detentions and is very useful for detecting single bit error as a simple form of Forward Error Correction (FEC).

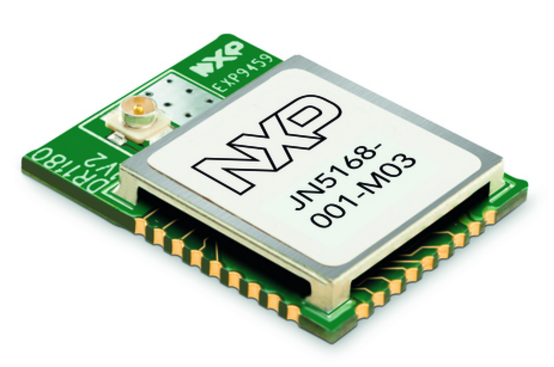
Check-sums make use of 1’s complement sums of 16-bit words in a message (padded with a 0 byte if odd it has an odd length) [C]. This detection method can detect up to 16 bit errors, however it is not a guarantee that it will detect more than 1 error. In the event of a two-bit error, there is a 1/16th chance that the error will not be detected.

Cyclic Redundancy Checks utilized both shift registers and XOR gates to check if an error has occurred in data transmission. A CRC calculates a short binary sequence (check value) for each data packet being sent and adds it to the end of the sequence known as a “code word”. When the code word is read by the receiving device, the device compares the check value to a newly calculated one at the device. If the new check value does not match that of the one sent, the data packet contains an error. The device will then take corrective measures, like rereading the data packet or requesting the data to be resent. If the check values do match, the data is assumed to contain no errors.

**ZigBee Modules**

We looked at three different ZigBee modules, the Digi International’s Legacy XBee S1, Telegesis ETRX351, and NXP JN5168-001-M003 modules. The following section will dive into the specifications of these three modules.

**NXP JN5168-001-M003**

The NXP JN5168-001-M003 is in the family of NXP’s ultra-low power, high performance surface mount ZigBee modules [F]. The modules use NXP’s JN5168 wireless microcontroller to provide large memory, as well as high CPU and radio performance with all RF components included. The module operated at 2.4 GHz with either PCB or external antenna options. Transmission power for the JN5168-001-M003 is +2.5 dBm with receiver sensitivity up to -95 dBm. The module operates at a voltage range of 2.0 – 3.6V, transmission current of 14.3 mA and receiving current of 17 mA.

The JN5168 microcontroller is a 32-bit RISC CPU, with up to 32 MIPs with low power. It supports RF4CE, JenNet-IP and ZigBee stacks with a JTAG debug interface. The microcontroller has a 4-input, 10-bit ADC with one comparator, as well as 2 UART ports, one SPI Master-Slave port with three selects, a 2-wire serial interface, battery and temperature sensor and up to 20 Digital I/Os. The modules itself is 30mm x 16mm for the PCB antenna module and 16mm x 21mm for the external antenna mount module. The JN5168-001-M003 has an operating temperature of between -40o – 85o C.

If we were to use the JN5168-001-M002 in the S.M.A.R.T. Alarm system, we would be limited to using only the JN5168 of microcontroller. Moreover, the programmer is required to code only on the embedded microcontroller as well, making this device not a good choice for the application since it would limit the team to one architecture and implementation.

**Telegesis ETRX351**

The Telegesis ETRX351 is a low power, 2.4 GHz ZigBee module based on the latest Ember EM351 single chip ZigBee solutions [G]. This is a 3rd generation ZigBee module developed by Telegesis, who have been recently acquired by Silicon Labs. These modules have been designed to be easily integrated into any device with minimal RF knowledge required. The module uses the EmberZNet ZigBee stack (a proprietary stack), enabling the ETRX351 to add powerful wireless networking capabilities to existing products in a timely manner. The module makes use of an AT-style command line interface which allows users to integrate ZigBee networking quickly into systems without the need for complex software.

The ETRX351 is a relatively small surface mount module (25mm x 19mm). There are two antenna option, either a PCB or U. FL coaxial connector antenna can be used with this device. This module uses JTAG programming for debugging via the Ember InSight port. The chip has 128kB of flash memory and 12kB of RAM and has the option to add a 32.768 kHz watch crystal externally. The ETRX351 can be used as either a coordinator, router or end device. This module offers up to 24 general-purpose I/O lines including analogue inputs. Hardware supported encryption is available and the ETRX351 is CE, FCC and IC compliant as well as FCC modular approved.

The ETRX351 has a supply voltage range between 2.1 – 3.6V with an operating temperate range between -40o – 85o C. The transmission current for the ETRX351 is about 31 mA and a receiving current of about 26.5 mA. This module also has the option to go into a “Boost Mode” which boost the output power, extending the transmission range of the module. While in boost mode, the receiving current is about 27 mA but the transmission current jumps up to 42 mA, which is about a 35% increase in current consumption. The ETRX351 operates in the 2.4 GHz ISM band with an over air data transfer rate of 250 kbit/s.

Although the ETRX351 could be a great a solid choice for the S.M.A.R.T. Alarm system, it falls under the same category as the NXP JN5168-001-M003 when it comes to integrated microcontroller. Moreover, like the JN5168-001-M003, the ETRX351 is a surface mount module, which makes it much harder to prototype/breadboard with, making it a less viable option than the Digi International Xbee module.

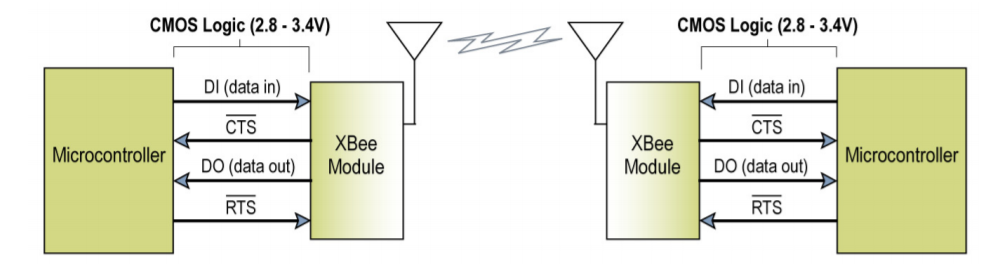
**Digi International Legacy XBee S1**

The XBee RF Modules are engineered to meet IEEE 802.15.4 standards and support the need of a low-cost, low-power wireless sensor network. The modules require minimal power and provide reliable data delivery between XBee devices. The XBee modules operate within the 2.4 GHz ISM frequency band and are pin-for-pin compatible with each other [H]. XBee modules are ideal for applications that require predictable and low latency communication timing that provide quick, strong, communication in point-to-point, peer-to-peer, multipoint, star, or mesh network configurations [I]. The modules come with a free X-CTU Software for testing and configuration as well as AT and API command modes for configuring module parameters. These modules also offer analog-to-digital conversion, digital input/output and I/O line passing.

The Legacy XBee S1 has a 250 kbit/s data rate with a range of approximately 30 m (range can be extended with external antenna). The module has an transmit power of 1 mW (+0 dBm) and a receiver sensitivity of -92 dBm. The transceiver chipset used in the Xbee module is the Freescale MC13212. This XBee module has a 3.3V CMOS UART serial data interface and a DSSS (Direct Sequence Spread Spectrum) interface immunity. The module has eight digital I/O ports and antenna option that include, PCB, Wire, Whip, U.FL and RPSMA. Encryption for the XBee is a 128-bit AES (Advanced Encryption Standard).

The Legacy XBee S1 is 24.38 mm x 27.62 mm, has a supply voltage range of 2.8 – 3.4 VDC and an operation temperature range of -40o – 80o C. The module has a transmission current of about 45 mA at 3.3 VDC and a receive current of about 50 mA at 3.3 VDC. The XBee’s power down current is less than 10 µA at 25o C, which is great for a low power consumption system.

The XBee RF module interfaces to a host device through a logic-level asynchronous serial port. With this serial port, the module can communicate with any logic and voltage compatible UART, or through a level translator to any serial device [H]. Any device that has a UART interface can connect to the pins of the XBee RF module as follows:

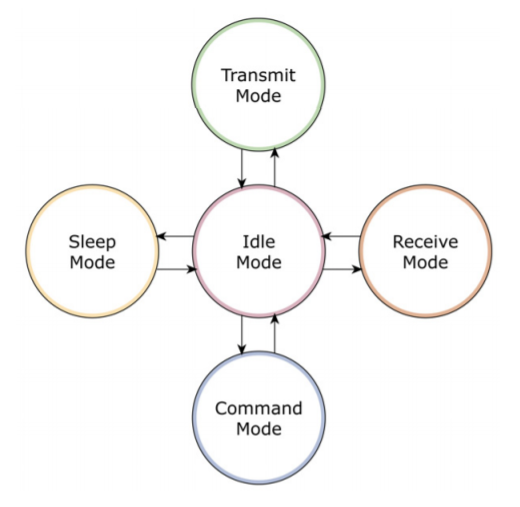


Data enters the modules UART through the DI pin as an asynchronous signal (signal idles high when no data is being transmitted). Each data byte contains a start bit (logic low), 8 data bits with the least significant bit first and a stop bit (logic high). For the RF module and the microcontroller’s UARTs to communicate correctly, the setting for each module must be set to be compatible, such as baud rate, parity, start bits and data bits. In order to configure the baud rate and parity settings on the XBee module, the BD and SB commands must be used.

Data is buffered in the DI buffer until one of three cases occurs in the system, causing the data to be made into a packet and transmitted. One case is if no serial characters are received for the amount of time determined by the RO parameter. If RO is made equal to zero, the packetization of the data begins when a character is received. Another case is when the maximum number of characters that will fir in a data packet is reached, which is 100 characters. The final case is when the Command Mode Sequence (CMS) is received, causing any character buffering in the DI buffer to be put into a packet and transmitted. The CMS for the XBee module is “GT + CC + GT”. Since a module cannot transmit can receive at the same time, storing data in the DI buffer allows for transmission of data possible once the module is done receiving data. In the case that the DI buffer becomes full, hardware or software flow control must be used to ensure that data will not be lost and to prevent data overflow.

The XBee modules have the ability to use Application Programming Interface (API) operations to extend the level of which a host application can interact with the networking capabilities of the module. The API allows alternative means of configuring the module as well as routing data at the application level. Using the API has many advantages including transmitting data to multiple destinations without entering command mode, receiving success/failure status of each transmitted packet and identifying the source address of each received packet. These features are very useful to the S.M.A.R.T. Alarm system, especially the latter, due to the need to know which Alarm module has detected the fire so the main hub plan an appropriate route to exit a building and broadcast that data to the alarms. All I/O data is sent out the UART using an API frame in the XBee module.

The user can select a sampling rate for the XBee modules. This means instead of constantly checking ADC and DIO data, the module will check periodically these periodically on modules that are not configured to operate in sleep mode (TX) . If a module is configured in sleep mode and the sampling rate (IR) is set, the module will stay awake until the IT (Samples before TX) has been reached. Once a certain pin is enabled for IR, the sample rate must be chosen for that pin. The maximum sampling rate is one sample per millisecond or 1 KHz.

I/O line passing in the XBee modules allows for received RF data packets that contain I/O data to update any enabled outputs (PWN and DIO) based on the data it receives. I/O lines are mapped in pair, therefore, AD1 can only update PWM1 or DI3 can only update DO3. The XBee’s default setup is that no outputs are to be updated, which mean I/O data is forced to be sent out through the UART. To allow updating outputs, the I/O Input Address (IA) must be setup with the address of the module that has the appropriate updates enabled, which basically shields the outputs of a module from the input. The IA can also be setup to accept I/O data for output changes from any module by setting the IA parameter to 0xFFFF. This feature may be used in the S.M.A.R.T. Alarm system as way to have a manual alarm trigger such as a pull lever in common alarm systems. Data will bypass the hub and the whole alarm system will begin to sound. This will be a temporary alert until a S.M.A.R.T. Alarm unit detects smoke, in which case path planning and broadcasting will commence.

The XBee RF modules operate in five different modes; Idle, Sleep, Command, Transmit and Receive Mode. Idle mode occurs when the module is not receiving or transmitting data, and will only shift out of idle if ont of the following conditions are met; Serial data is received in the DI buffer (Transmit Mode), RF data is received through the antenna (Receive Mode), Sleep condition is met (Sleep Mode) or a CMS is issued (Command Mode).

Ease of use is a very important factor when it comes to choosing the correct ZigBee module for the S.M.A.R.T Alarm system. The module needs to be able to programmed easily and have the ability to work seamlessly when integrated into a mesh network. We found that Digi International’s Legacy XBee S1 modules have all the networking capabilities necessary for the S.M.A.R.T. Alarm system to communicate seamlessly in a ZigBee network. Moreover, these modules are very highly recommended over any other ZigBee module, a fact that we did not take lightly when deciding our device. We will be powering our system off facility power, so the higher power consumption of the XBee modules compared to the competition did not come up as an issue when making our decision. That being said, if the Alarm needs to rely on its battery backup, the power consumption of the XBee’s are very small, allowing it to run on battery for quite some time, more than enough time to restore power to the facility. Moreover, The XBee modules are through hole, a plus when it comes to bread boarding our system, making the process much easier and less time consuming.

The following is a tabulated view of the specification for each of the three ZigBee modules:

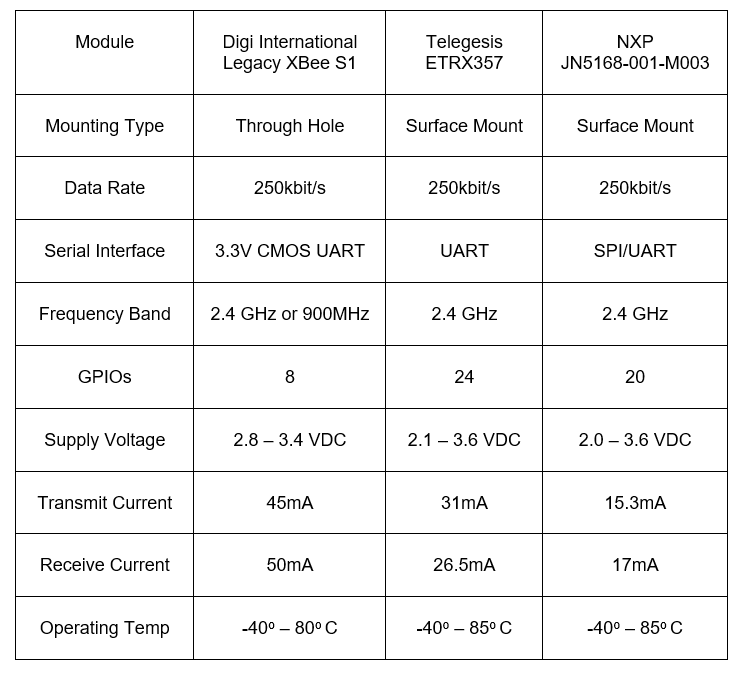


Table 1.1.5-1: ZigBee Module Comparison

A]<http://electronicdesign.com/what-s-difference-between/what-s-difference-between-ieee-802154-and-zigbee-wireless>

[B] <https://www.controlanything.com/Relay/Device/A3001-1>

[E] Gislason, D. (2008). ZigBee wireless networking. Oxford: Elsevier, Newnes.

[C] <https://www2.hawaii.edu/~esb/2009spring.ics451/apr16.html>

[D] Farahani, Shahin. Designing ZigBee Networks and Transceivers: The Complete Guide for RF/wireless Engineers. Oxford: Newnes, 2008. Print.

[F] <http://www.nxp.com/documents/other/JN-DS-JN5168MO-1v2.pdf>

[G] <http://www.mouser.com/ds/2/368/tg-pm-0516-etrx35x-957725.pdf>

[H] <https://www.sparkfun.com/datasheets/Wireless/Zigbee/XBee-Datasheet.pdf>

[I] http://www.mouser.com/ds/2/111/ds\_xbeemultipointmodules-19140.pdf