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).

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. 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.

1.1.1 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.

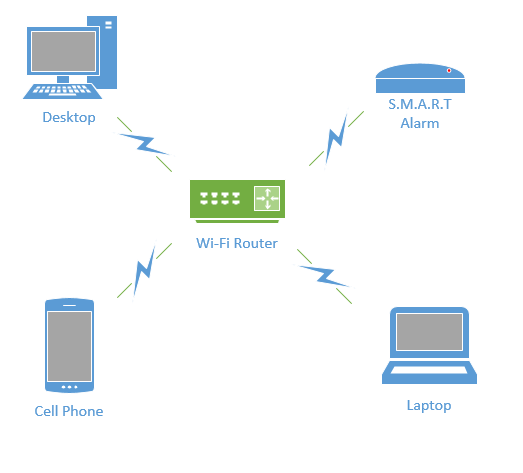


Figure 1.1.1-1 Wi-Fi Network

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 final 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, a more power efficient communication system must be used.

1.1.2 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.

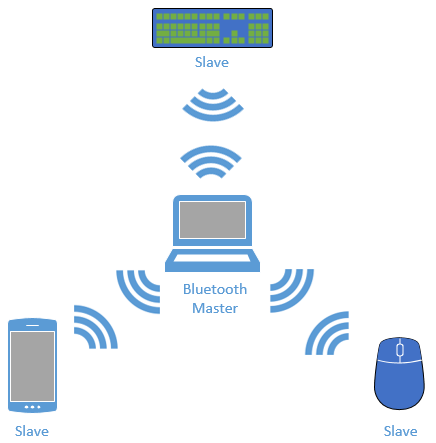


Figure 1.1.2-1 Bluetooth Network

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.

1.1.3 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.

Due to ZigBee’s low power consumption, it limits transmission ranges to about 10-100 meters depending on power output and environment. However, through the use of a mesh network, data can be transferred from one device to another, allowing for an expansive range.

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 essentialyl 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.

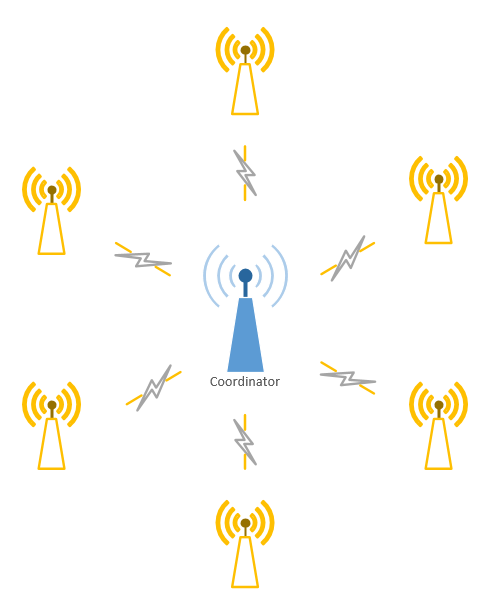


Figure 1.1.3-1 ZigBee Star Network