Wi-Fi in Sensor Applications

Abstract

Sensors are used for measurements and for acquisition of data; but they require an effective data transfer mechanism to enable full-fledged applications that utilize the data they collect. A popular method of data transfer is through wireless means. Among the wireless mechanisms, 802.11 Wi-Fi stands out for a number of reasons. Redpine's informative paper on the use of Wi-Fi in sensor applications describes these advantages; and also covers the implementation of such application scenarios.

A Wireless Sensor Network Architecture

A set of sensors monitored at a central facility is commonly referred to as a 'sensor network' as shown in Figure 1 – arising from them being organized as a mesh of interconnected nodes. Sensors are deployed in a variety of environments and for a number of purposes – including building automation, facility management, environmental monitoring, industrial automation, military zones, asset management, and many others. Legacy sensor networks have used proprietary wireless transport mechanisms, and lately standards based wireless transport like Zigbee or Bluetooth.

These wireless mechanisms are characterized by low operational power, low cost, low range, and largely proprietary network and data transfer protocols, including mesh networking. Sensors can potentially act as relays and be capable of adapting to changing scenarios.

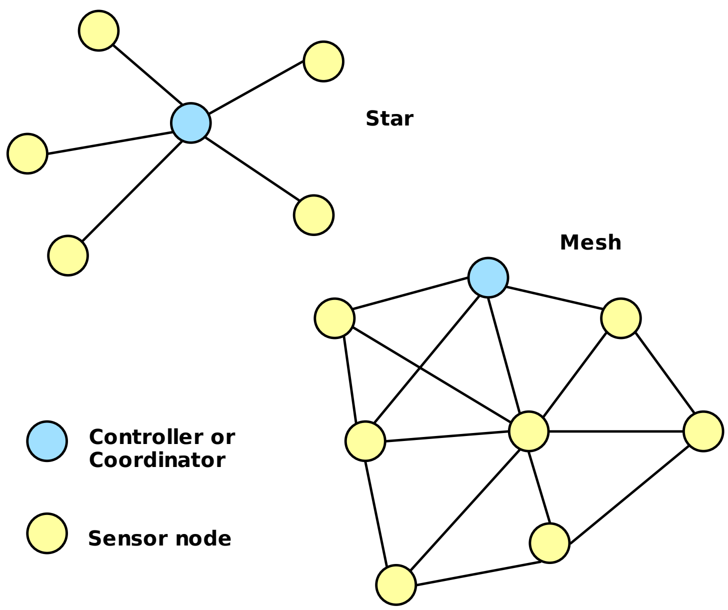

Figure 1: A Wireless Sensor Network

Recently, however, wireless networks based on 802.11 'Wi-Fi' have become pervasive in enterprise and industrial environments, among others, where sensors are often deployed. The presence of a well established and standardized wireless network has brought about a new possibility in the deployment of sensors – the use of Wi-Fi as the transport mechanism. 802.11 was, of course, not designed with sensor applications in mind, but innovations in implementations have enabled the use of 802.11 while satisfying all sensor requirements and more.

A typical Wi-Fi deployment would have a set of access points positioned so as to provide coverage over the operational area – which might be a large factory floor, multiple offices, a hospital, a campus, and many more. In almost all cases, the network is a star configuration, with the possible provision of client roaming or hand-off. The Access Points are connected to the enterprise's network through wired connections, or in part through a wireless distribution system. One of the advantages in this scenario is the location of a central controller or coordinator – this can be anywhere on the network, and with internet connectivity, potentially anywhere in the world. With standardized IP based transport, no additional network infrastructure needs to be added to transfer sensor information to any part of the network.

Wi-Fi may also be used to determine and provide the location of a client device. Typically the device's transmissions are received by several access points or receivers, or the device receives beacons from several access points. The relative signal strengths seen, or the relative times of arrival measured, provide the means to locate the client device. Access points in these scenarios are carefully located so as to provide the best ranging measurements, and a thorough measurement is carried out in advance of the signal propagation nuances of the deployment landscape.

Sensor Node Requirements

A 'sensor' itself is, of course, the device that gathers data – the transducer used for measurement of temperature, humidity, pressure, proximity, position, flow, sound, presence of liquids or gases, etc. A wireless communication facility now enables the sensor to be deployed at any location with ease. The resultant 'sensor node' is a self-contained device that gathers data, processes it, and communicates it to a control unit wirelessly. Successful deployment of a cost-effective wireless sensor network benefits from the availability of the following characteristics of the sensor node:

- Extremely low power consumption, with years of battery life
- Standardized wireless transport
- Good wireless range for ease of deployment
- Ability to coexist with other wireless devices in the vicinity
- Easy configuration

- Low cost

We will now see how all of these requirements are provided for in a Wi-Fi based sensor solution.

A Wi-Fi Sensor Node

Figure 2 depicts the typical configuration of a sensor node. The microcontroller is the main programming element in the design. It configures the sensors and the wireless subsystem; and it handles the battery or power management and the conditioning of sensor data as required. It may also be the device or functional block that provides the ultra-low power timed sleep mode. The Wi-Fi subsystem may be partitioned in various ways, based on the chipset used, but in general consists of a MAC, baseband processor, RF transceiver, and RF front-end.

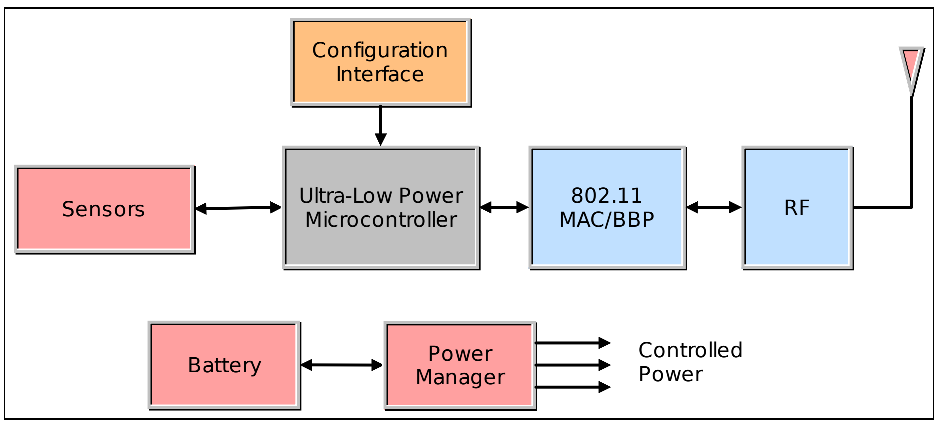

Figure 2: A Sensor Node

The battery drain of the system depends on several factors. They include the power consumption of the sensors, the active mode power consumption of the microcontroller and wireless subsystems, and the power consumed in the sleep mode. With typical duty cycles of operation of a few milliseconds ON and several minutes OFF, overall energy drain could be dominated by the sleep mode power, with other influencing factors being the time taken to reach an operating point upon being woken up, and of course, the peak active mode consumption. Sensors used for critical monitoring are also often kept active at all times, and in these cases the sensor's power consumption becomes important. A fundamental advantage with Wi-Fi based sensor networks is that no sensor node is burdened with the need to relay data from other nodes. The ON or active time therefore becomes highly regulated and predictable.

Transmission of data over the wireless channel can be in one of two modes. In the first mode, the node wakes up and associates to an access point or BSS before transmitting its data, with full compliance to the Wi-Fi network's protocol. In the second mode, the sensor node wakes up and transmits data without going through the association procedure with the BSS. In this case, the infrastructure systems or controller would need to be customized to receive this data. Normal or off-the-shelf Access Points would not handle or respond to packets sent by unassociated clients unless they are a special class of packets like probe requests. The advantage with this mode, however, is that the sensor node is awake for a shorter duration, thereby extending battery life. A significant advantage in either mode is that all transmissions can fully adhere to the collision avoidance mechanisms of the 802.11 protocol. And in the crowded ISM bands, it is advantageous for all transmitting devices to follow the same protocol, ensuring that overall avoidance of collisions is maximized.

The power advantage of 802.11 arises from the use of high transmit data rates in order to minimize active time. With modulation schemes up to 64-QAM, Wi-Fi's spectral efficiency is also higher than most other protocols. For example, sensor information amounting to 1k bytes can be transmitted in 802.11g or 802.11n format in as little as 160 microseconds, or a more usual 100 bytes of data can be sent in just about 30 us. Often, thus, the time taken to prepare the wireless subsystem to transmit the data is a significant energy drain. The subsystems therefore are optimized for these applications in enabling as quick a turn-on as possible.

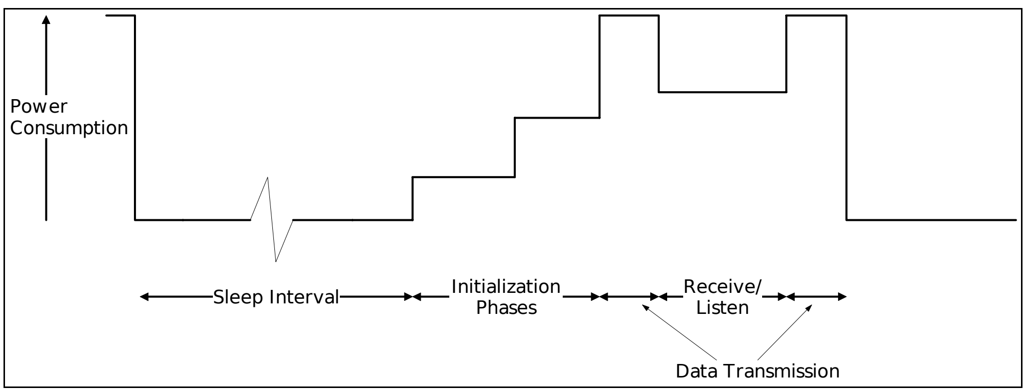

Figure 3: Operational Profile for Power Consumption

Ease of configuration before deployment, as well as after deployment in some cases, is an important requirement. Factory configuration of devices normally covers RF calibration, MAC address, and some configuration specific information. Other parameters like wireless network configuration, IP address, reporting intervals, and other operational parameters are commonly configured through a serial interface. In some cases they are also configured through the wireless interface itself, through a special mode. These configuration interfaces may also be used to deliver firmware upgrades.

The 802.11n Advantage

The IEEE 802.11n standard primarily provides for high throughput, high-efficiency, and long range data connectivity, and includes the use of multiple antennas and transmit-receive chains. However, the standard also includes a single-stream mode that is intended to provide the benefits of 11n to low-power small form-factor devices including sensor nodes. The use of single-stream 802.11n WLAN in these client devices provides the following benefits:

- Higher throughput and lower transmit times – achieved through better efficiency in PHY and MAC.
- Longer range – through use of multiple antennas at the access point
- Preservation of 802.11n network capacity – the presence of legacy 802.11a/b/g clients forces the 11n nodes to use protection mechanisms and results in overall drop in network capacity. 802.11n helps avoid this.

RS9110-N-11-31 in a Sensor Node

Redpine's RS9110-N-11-31 is the industry's first single-stream 802.11n module designed specially for Wireless Sensor Networks, offering an ideal solution satisfying all the requirements of sensor nodes. It has an ultra-low power microcontroller which interfaces with various sensors and Redpine's WLAN subsystem. The system-level and profile driven fine-grained power control offers a battery life of over 3 years over the IPv6 framework. It offers a higher range through STBC and also higher throughputs which result in lesser "awake" periods, thus reducing power consumption substantially. The RS9110-N-11-31 supports TCP/UDP over IPv6/IPv4, making it extremely easy to integrate into an already existing WLAN. It supports configuration over UART as well as Wi-Fi and offers digital and analog interfaces to work with a variety of sensors.