

Demystifying Wireless for Real-World Measurement Applications

Kurt Veggeberg, Business, Development Manager (kurt.veggeberg@ni.com)
 National Instruments, 11500 N. Mopac C, Austin, TX 78759

ABSTRACT - Wireless technology extends the concept of PC based data acquisition beyond the limits of cables and wired infrastructure for new remote or distributed measurement application. Gain an understanding of wireless networking basics. Learn how to deploy reliable wireless measurement in a variety of outdoor or harsh environments for reliable and secure data acquisition systems. Examples of distributed outdoor noise and structural monitoring systems will illustrate networking layers and topologies for specific applications.

Introduction

Understanding technology capabilities and application requirements is important when selecting a wireless technology for your application. The reasons to choose wireless include reduced installation costs, installation and deployment flexibility, and the ability to address new applications. Before selecting wireless, you first need to ensure the bandwidth available with wireless meets your application requirements.

Choosing the Right Technology

Although the ability to eliminate cabling costs with wireless installations presents potential cost savings, wireless technology must address the application requirements. Two of the main reasons to select a wired protocol are bandwidth and reliability. Standard wired 100BASE-TX Ethernet is faster than both wireless IEEE 802.11g, or Wi-Fi, and IEEE 802.15.4, which provides the basis for Zigbee®. When gigabit Ethernet at 1 Gbit/s is included, the bandwidth advantage for Ethernet is clear. If you do not require a bandwidth above 100 Mbit/s, then the cost savings combined with installation flexibility make wireless an effective option.

	Ethernet, Copper (100BASE-TX)	Ethernet, Fiber (100BASE-FX)	Wireless (IEEE 802.11n)	Wireless (IEEE 802.15.4)
Physical Wire or RF	Copper	Fiber Optic	2.4 GHz	2.4 GHz
Frequency	Copper	Fiber Optic	2.4 GHz	2.4 GHz
Bandwidth (max bit rate)	100 Mbit/s	100 Mbit/s	100 Mbit/s	250 kbit/s
Range (without repeaters)	100 m	400 m	~100 m	~300 m
Power Requirements	High	High	Medium	Low
Typical Battery Lifetime	–	–	1–2 days	3–5 years

Table 1. Bandwidth, Range, and Power Comparison for Ethernet and Wireless Technology

Networks based on 2.4 GHz Spectrum – Bandwidth Range and Power Requirements

The frequency spectrum covers a broad range of signals. Today we will focus on the 2.4 GHz unlicensed section within the general frequency range of radio wave. Within this “radio spectrum” there are different frequencies used for different applications from long wave radio to satellite broadcasting. Wi-Fi in the 2.4 GHz range is a sweet spot for distance and bandwidth. (Figure 1)

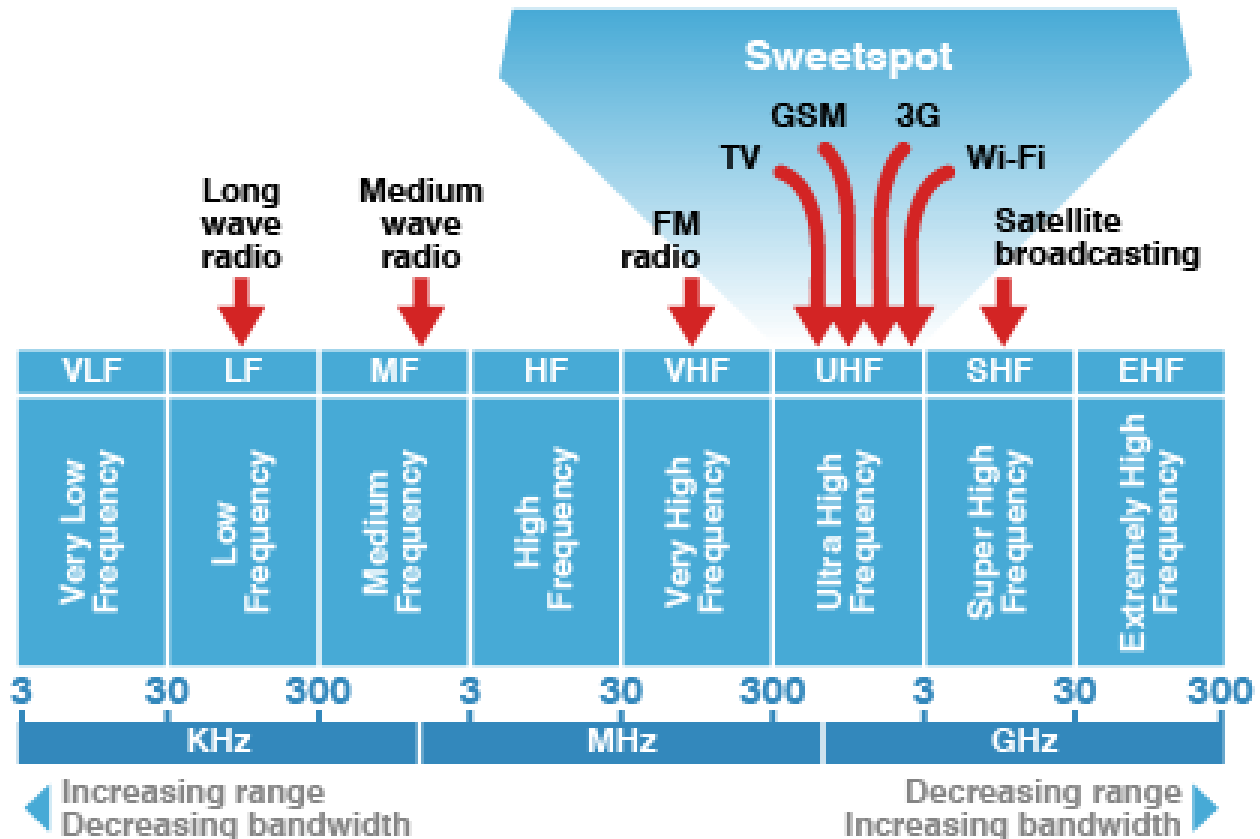


Figure 1. Radio Spectrum “Sweet Spot.”

There are three key factors to consider when evaluating wireless technologies: bandwidth, range, and power requirements. When you compare wireless protocols based on IEEE 802.11 and IEEE 802.15.4, Wi-Fi has the advantage in bandwidth with a maximum bit rate of 100 Mbit/s, while 802.15.4 has the advantage in distance and power requirements. This is a typical trade-off made in wireless protocols. Wi-Fi offers significantly higher data rates, which require additional encoding; extra data requires additional radio traffic resulting in increased power consumption by the radio. This bandwidth and power trade-off is obvious in systems such as laptops or smart phones with integrated Wi-Fi that typically operate for a matter of days between recharging and provide high-speed data transfer, compared to a wireless sensor network based on IEEE 802.15.4 technology that might operate for years on standard AA batteries and transfer reduced data between sleep states. (Figure 2)

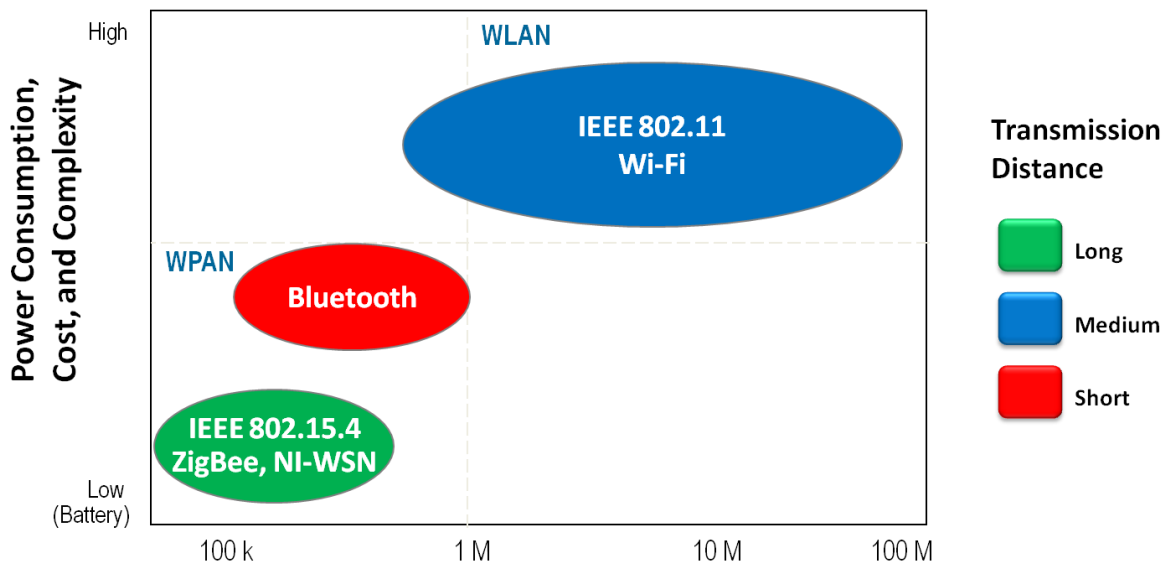


Figure 2. Tradeoffs in wireless technologies.

For technologies based on IEEE 802.15.4, this trade-off in bandwidth also results in up to a 10X improvement in distance. At a maximum distance of 300 m and a bandwidth trade-off from 54 Mbit/s to 250 kbit/s, protocols based on IEEE 802.15.4 are ideal for low-speed, long-distance remote monitoring applications, while Wi-Fi is ideal for shorter-distance, higher-power, and higher-bandwidth applications.

Significant time and money has been invested into researching the use of wireless technology for remote monitoring. Yet, significant wireless deployments are just beginning to materialize in industry such as construction site management and building acoustics where running wires can be difficult. There are many advantages to eliminating cables in remote monitoring applications, but there are also many challenges. As standards such as Wi-Fi (IEEE 802.11) continue to mature, those challenges are being addressed.

IEEE 802.11 has a variety of advantages for remote data acquisition and data streaming for dynamic signal acquisition as compared to other standards such as IEEE 802.15 (Zigbee[®]) including range and security. IEEE 802.11 typically operates on 2.4 GHz. It is typically specified with a range from 30 to 100 meters with data rates from 54 to 600 Mbps. The range depends on a variety of factors and can be extended significantly through a variety of network topologies and high gain antennas.

IEEE 802.11 divides the band from 2400 to 2483.5 GHz into channels, analogously to how radio and TV broadcast bands are carved up but with greater channel width and overlap. For example the 2.4000–2.4835 GHz band is divided into 13 channels each of width 22 MHz but spaced only 5 MHz apart, with channel 1 centered on 2.412 GHz and 13 on 2.472 GHz to which Japan adds a 14th channel 12 MHz above channel 13. (Figure 3)

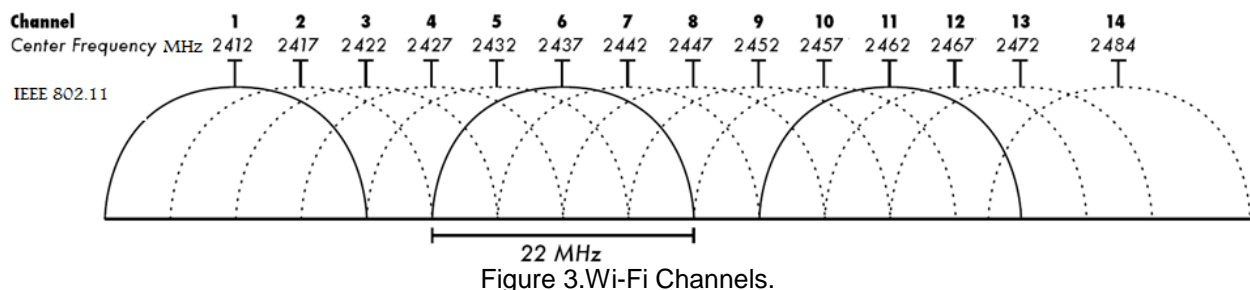


Figure 3. Wi-Fi Channels.

Availability of channels is regulated by country, constrained in part by how each country allocates the frequency to various services. Japan permits the use of all 14 channels (with the exclusion of 802.11g/n from channel 14), while Spain allowed only channels 10 and 11 and France allowed only 10, 11, 12 and 13 (now both countries follow the European model of allowing channels 1 through 13). Most other European countries are almost as liberal as Japan, disallowing only channel 14, while North America and some Central and South American countries further disallow 12 and 13.

IEEE 802.15.4-2006 specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANS). It is maintained by the IEEE 802.15 working group. In the 2.4 GHz band there are 16 Zigbee® channels, with each channel requiring 5 MHz of bandwidth. The center frequency for each channel can be calculated as, $F_c = (2405 + 5 * (ch - 11))$ MHz, where $ch = 11, 12, \dots, 26$.

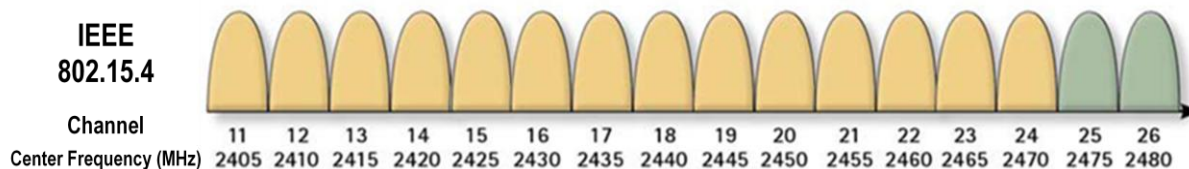


Figure 4. IEEE 802.15 channels.

In order to plan wireless networks it is important to remember the channels that are used by 802.11 and 802.15.4. These channels do overlap on the frequencies ranges between 2400 and 2480 MHz (2.4 GHz). With knowledge about these channels it is possible to plan and install systems that avoid channel overlap. It is also worth noting that two wireless devices, one based on 802.15.4 and the other based on 802.11 use much different data rates so even if they are transmitting on the same frequency they will function. In the case where either is trying to transmit at maximum data rate it is a good idea to architect systems to avoid channel overlap.

One way to ensure co-existence of Wi-Fi and WSN channels includes setting Wi-Fi Access Points and Zigbee® channels to avoid overlap. The other includes creating spatial distance between systems with same channel. (Figure 5)

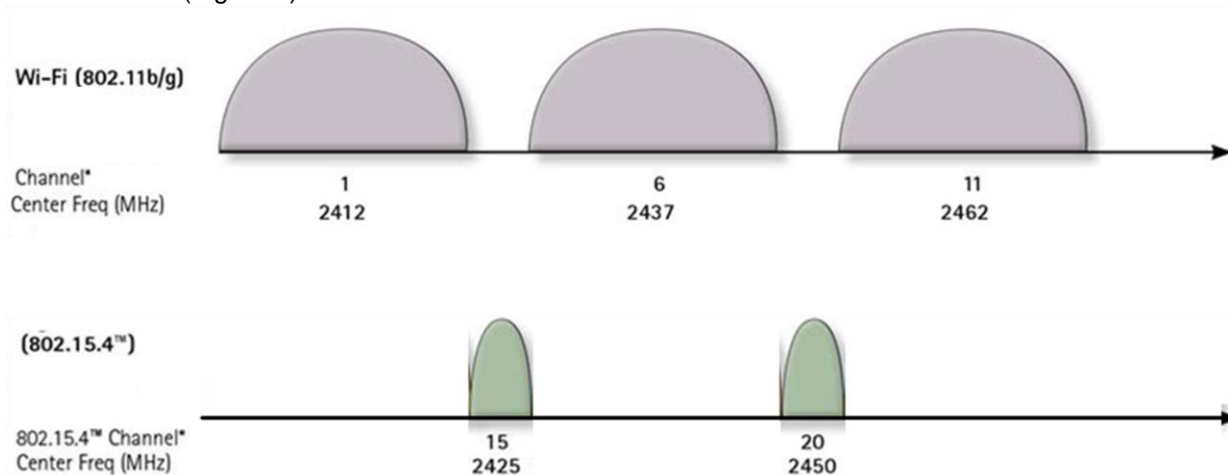


Figure 5. Setting Wi-Fi and Zigbee® channels to avoid overlap.

Figure 5 is an example of channels that are commonly used with Wi-Fi to avoid the overlap between different 22 MHz Wi-Fi channels, in this case channels 1, 6, and 11 are used on the wireless access point. These channels are actually very common channels in Wi-Fi systems

Another way to avoid channel overlap is to plan systems with enough distance between networks that the channels that are within range are different and then channels outside of network range can repeat. This is channel spacing. Typically this would be greater than 30 m for 802.11 and greater than 300 m. for 802.15.4 (Figure 6)

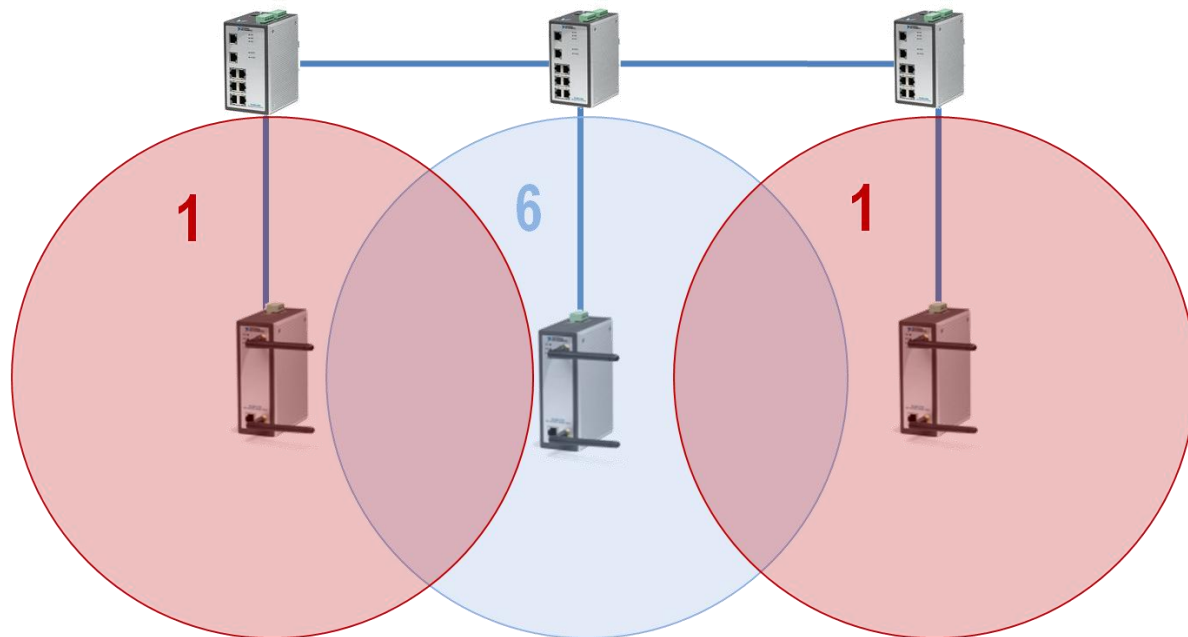


Figure 6.Channel Spacing

Security

Security is a top concern for many engineers and scientists considering wireless. The reasoning behind this is due in large part to the failings of early wireless standards such as wired equivalent privacy (WEP), which did not prevent unauthorized access well. There are two main components of network security that must be addressed before wireless is widely adopted: authentication and encryption.

A wireless network is inherently more accessible than a wired network (such as Ethernet) because it is not a closed system: data travels through the air. IEEE 802.11X has evolved to provide authentication on wireless networks based on the Extensible Authentication Protocol (EAP). Clients on the network must identify themselves before being granted access to the network. There are other less sophisticated strategies for preventing unauthorized network access as well. Good security practice for wireless networks includes MAC and/or Internet Protocol (IP) address filtering and service set identifier (SSID) suppression.

Even if data is accessible to an unauthorized user, it is not necessarily intelligible. Data encryption on wireless networks has evolved significantly over the last decade from clear-text broadcasts to 128-bit cryptography. The Advanced Encryption Standard (AES) is now a NIST standard and a requirement for all U.S. government installations. (Figure 7)

Key size (bits)	Number of alternative keys	Time required at 1 decryption/us	Time required at 10 ⁶ decryptions/us
32	$2^{32} = 4.3 \times 10^9$	35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	1,142 years	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{24} years	5.4×10^{18} years

Figure 7. Time required for exhaustive key search (brute force attack)

Network Topology

In addition to total distance, protocols based on IEEE 802.15.4 offer a couple of options for network topologies. A Wi-Fi system is typically configured in a star topology with a center access point and clients up to 30 m from the access point. If you need additional distance, a tree topology for which you can use either Wi-Fi repeaters or IEEE 802.15.4 routers helps extend your distance. While standard Wi-Fi installations support repeaters or routers to extend distance and can be configured in a cluster or tree, they do not support meshing, which is the ability for a node or device to route packets back to the gateway. If network reliability is important, then with an IEEE 802.15.4 mesh network an end node can route packets through multiple routers to a gateway. This provides network reliability in case a router fails. Many 802.15.4-based wireless sensor networks (WSNs) support star, cluster tree, and mesh networking topologies. (Figure 8).

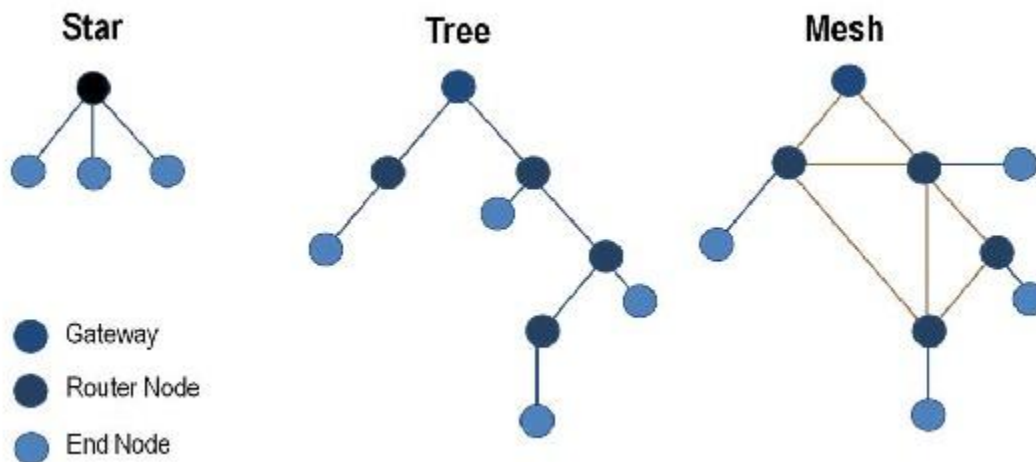


Figure 8. A Star, cluster tree, and mesh networking topologies.

Measurement Speeds and Wireless Throughput

Wi-Fi offers higher bandwidth and as the IEEE 802.11 wireless protocol can support much higher sample rates than IEEE 802.15.4 based protocols. Measurement type, number of measurement channels, and measurement speed will determine the throughput requirements.

For high-speed measurements such as dynamic signal acquisition, Wi-Fi offers additional bandwidth. For instance, 24-bit high-speed sound and vibration data is sent in 32-bit packets and for 4 channels at 51.2 kS/s the required throughput is 6.6 Mbit/s. There is some additional overhead for Wi-Fi packets, but clearly the sample rate of 51.2 kS/s requires the bandwidth of Wi-Fi.

$$4 \text{ channels} \times \frac{51.2 \text{ kSamples}}{\text{second}} \times \frac{32 \text{ bits}}{\text{sample}} = 6.6 \text{ Mbit/s}$$

IEEE 802.15.4 based protocols are well suited for higher channel count applications. As an example an NI WSN application with 8 nodes and 4 analog and 4 digital channels per node at 1 second sample interval requires 5.2 kbit/s. The 82 Bytes per sample packet includes packet header information, 4 analog input channels, 4 DIO channels, and channel information such as link quality and battery voltage.

$$8 \text{ nodes} \times \frac{1 \text{ sample}}{\text{second}} \times \frac{82 \text{ Bytes}}{\text{Sample Packet}} \times \frac{8 \text{ bits}}{\text{Byte}} = 5.2 \text{ kbit/s}$$

For larger topologies such as a network with four routers and 32 end nodes the total throughput is 44.6 kbit/s. An important note is that in this topology the 32 end nodes communicate through one of the four routers so the network traffic is doubled from these end nodes. To calculate throughput in this extended topology multiply the number of nodes in this case, connected directly to the gateway by 1 hop and the number of end nodes connected to a router and then gateway by two hops and add the results.

$$4 \text{ nodes} \times 1 \text{ hop} \times \frac{1 \text{ sample}}{\text{second}} \times \frac{82 \text{ Bytes}}{\text{Sample Packet}} \times \frac{8 \text{ bits}}{\text{Byte}} = 2.6 \text{ kbit/s}$$

$$32 \text{ nodes} \times 2 \text{ hops} \times \frac{1 \text{ sample}}{\text{second}} \times \frac{82 \text{ Bytes}}{\text{Sample Packet}} \times \frac{8 \text{ bits}}{\text{Byte}} = 42 \text{ kbit/s}$$

Distance Requirements

An important consideration is the distance from your measurement to your network access. If the distance is greater than 30 meters line of sight, then you may need repeaters for Wi-Fi. Even if distances are less than 100 m, RF interference sources including trees or buildings can reduce the achievable distance. To ensure a reliable system, a site survey is recommended for all wireless installations. If required distances exceed 100 m, then IEEE 802.15.4 offers an option with a maximum distance of 300 m line of sight, and with routers the total distances can be extended.

Power Availability

The final consideration when deciding between wireless technologies is power availability. For two- to three-year battery deployments at lower bandwidths, IEEE 802.15.4 is ideal. The central gateway and embedded PC require either 9 to 30 VDC power or solar power; however, end nodes function for several years on standard AA batteries. In Wi-Fi, an access point generally requires power while the end devices are typically powered by DC or solar power for extended operation.

After considering the issues of throughput, range and power, you can more easily select the wireless technology that is right for your application. Addressing your application requirements is the first step. For any wireless installation, you should analyze the RF performance at the deployment site. Site surveys conducted by professionals ensure adequate coverage, network performance, and the ability to scale as you add more sensors.

Applications for Wi-Fi-based Wireless Data Acquisition

The higher bandwidth of Wi-Fi at up to 100 Mbit/s enables wireless data acquisition systems to address high speed waveform measurements such as strain and acceleration. The trade-off for higher bandwidth is power. An example wireless data acquisition application is short term load and strain tests. UT Ferguson Structural Engineering Lab is researching economical methods for inspection and monitoring of steel-girder highway bridges (temperature, strain, and acceleration). In the example below, a load cell was attached to the crane load line above the lift bucket to obtain accurate weight measurements of road fill being used to collapse a bridge segment being tested. A Wi-Fi transmitter was connected to the load cell so that the load data could be easily read and recorded from across the work-site. (Figures 9,10,11)



Figure 9. Bridge collapse test crane load measurements.



Figure 10. Remote load cell monitoring.

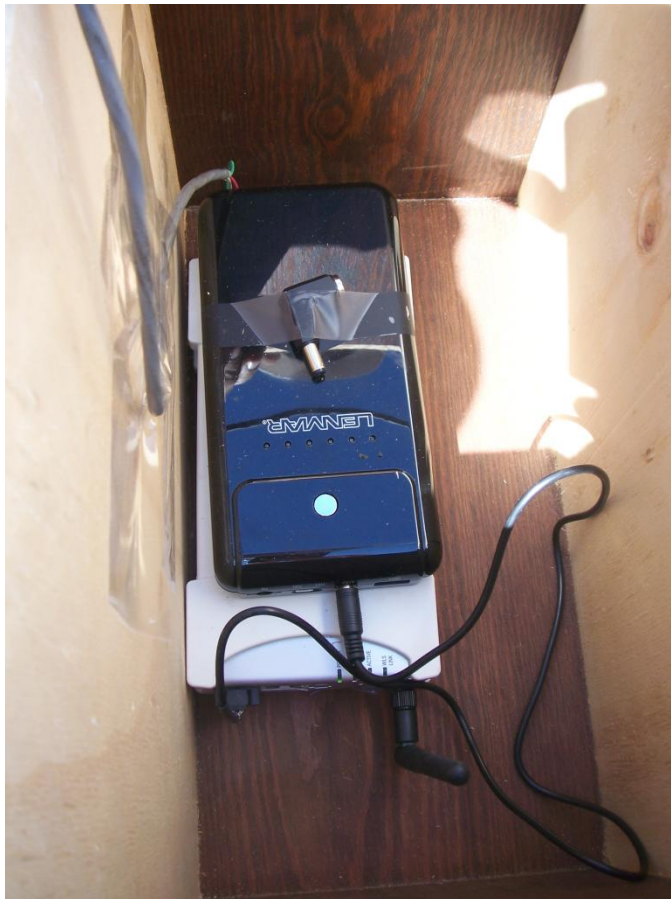


Figure 11. Wi-Fi DAQ module with battery in housing box for instrumenting load cell.

Applications for IEEE-802.15.4 based WSNs

The low power and longer distance available with IEEE 802.15.4-based networks fits well for longer-term remote measurement applications. One example is structural health monitoring. The ability to easily distribute several nodes up to 300 m from a gateway and further extend this distance through mesh routers, makes WSN ideal for monitoring large structures like bridges or buildings. The system can easily measure strain. The battery operated end nodes are easily installed close to critical areas of the bridge without the requirement of local power or communication wiring. Then data is sent wireless to a gateway with a real-time PC for storage and connectivity to IT infrastructure. (Figures 11 & 12)



Figure 11. Wireless Sensor Modules being tested on a bridge on I-35 in Austin, Texas

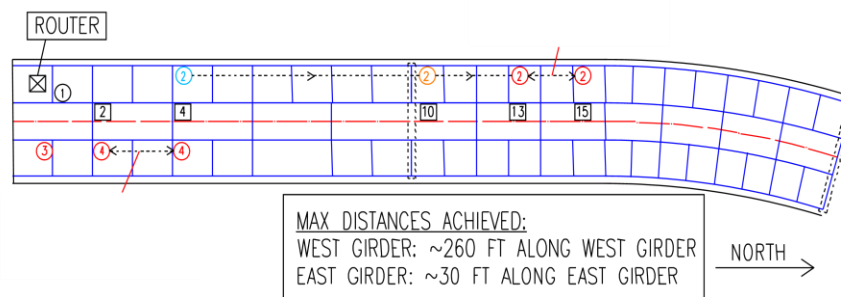


Figure 12. Wireless range testing on bridge girders.

Wireless DAQ and Wireless Sensor Networks

If wireless meets your application requirements, you then need to decide between two wireless technologies: Wi-Fi or IEEE 802.15.4-based networks. The trade-off between wireless protocols typically comes down to bandwidth, distance, and power. Wi-Fi has the bandwidth advantage while IEEE 802.15.4 based networks perform better in applications that require longer-distance coverage and lower power. IEEE 802.15.4-based protocols often deliver additional network flexibility with a mesh network topology, which routes packets from end nodes to the gateway through the shortest path available.