WHITE PAPER

Expert Tips for Optimizing Industrial Wireless Networks

Wen-Hsuan Chen
Moxa Product Manager

MOXA®

Abstract

Compared with its popularity in everyday commercial environments, Wi-Fi has been slow to gain a foothold in industrial M2M applications. One of the main reasons that industrial customers are reluctant to move from wired to wireless is the problems associated with stability. Wireless transmission is NOT as reliable as wired transmission. However, by following certain best practices it is possible to set up a wireless network that will provide the level of reliability needed for M2M communication applications. In this whitepaper, we present eight expert tips that you can follow to optimize your wireless networks for industrial application environments.

Overview

The 802.11 wireless technology standards, more commonly referred to as Wi-Fi, were introduced in 1992. Since then, 802.11 technology has grown rapidly from 802.11b to today's 802.11ac, with wireless transmission rates improving from 11 Mbps to more than 1.3 Gbps. In addition, with the widespread use of smart phones, tablet PCs, and other handheld devices, Wi-Fi technology is now deployed in most offices, commercial enterprises like restaurants and coffee shops, as well as in many private residences, providing a relatively transparent medium for much of our day-to-day communication.

One might assume that factories, warehouses, harbors, and even mines also utilize wireless technology to improve mobility and flexibility and reduce deployment costs for M2M communication. However, although the Wi-Fi trend has made inroads into industrial applications, it is much less common than you might think. One of the main reasons that industrial customers are reluctant to move from wired to wireless is the problems associated with stability. Wireless transmission is NOT as reliable as wired transmission. However, by following certain best practices it is possible to set up a wireless network that will provide the level of reliability needed for M2M communication applications. In this whitepaper, we present eight expert tips that you can follow to optimize your wireless networks for industrial application environments.

Improving the Quality of Wireless Connections

The first issue to consider when deploying wireless technology in industrial applications is stability. Unstable wireless connections are often caused by a "high wireless packet loss rate," which is caused by **channel saturation**, **insufficient signal reach**, and **hidden nodes and lack of redundancy**.

Released on July 18, 2016

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

Tip 1: Overcome Channel Saturation by Using 5-GHz Channels

A key aspect of wireless technology is that standard Wi-Fi connections are based on "carrier sense multiple access with collision avoidance" (CSMA/CA). This means that all Wi-Fi radios that are operating in the same area and have the same channel settings share the same transmission medium. For this reason, when considering channel utilization, you need to take into account all radio devices operating in that area. For example, if you are transmitting over 2.4-GHz channel 6, when checking if this channel is saturated or not, you not only need to look at all access points operating in that area, but also any non-802.11 devices (including microwave, ZigBee, and Bluetooth) that are using the same channel.

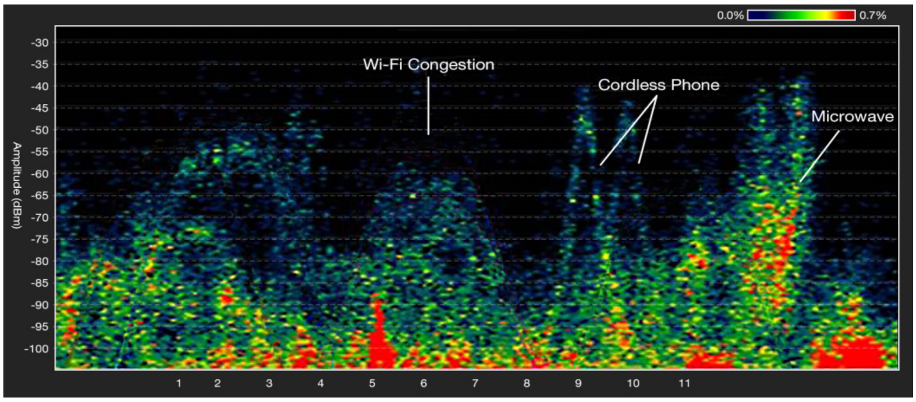


Fig. 1: 2.4-GHz channel utilization graph created with the Fluke frequency analyzer.

The easiest way to look at channel utilization is to use a frequency analyzer, such as Fluke or Wi-Spy (Fig. 1). You may find that the only way to avoid over-saturating the channel is to use a different channel. In fact, 2.4 GHz channels are not recommended for industrial applications due to their narrow bandwidth and the fact that they are already being used in many different environments for other applications. 5 GHz provides a wider frequency range with more non-overlapping channels (Fig. 2).

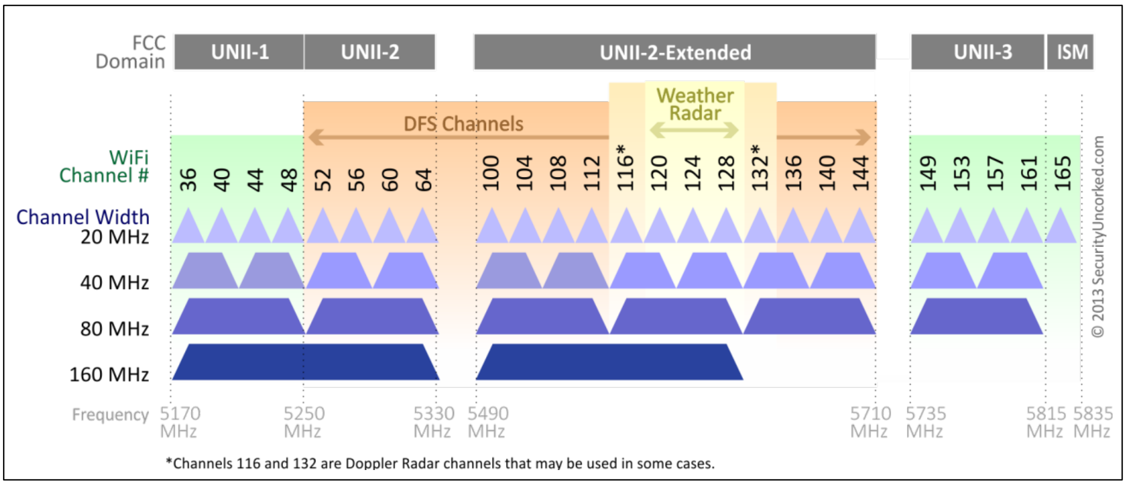


Fig. 2: 802.11ac 5-GHz Wi-Fi channels for North America (reproduced with permission from SecurityUncorked.com).

Note, however, that to legally operate on many 5-GHz channels, APs are required to support dynamic frequency selection (DFS) to avoid interfering with radar signals.

Tip 2: Achieve Maximum Signal Reach in a Long-Distance Connection through Scientific Distance Calculation

Achieving a higher 802.11 wireless transmission rate requires a stronger radio signal to avoid insufficient radio signal reach, which can result in low throughput, or even disconnection. There are several ways to improve signal reach. For example, installing higher gain antennas or switching to a lower frequency (900 MHz, for example) can reduce free-space path loss (FSPL). In order to accurately estimate realistic Wi-Fi transmission distances and bandwidths, a wireless distance calculator can be used to generate theoretical values, and an actual site survey can be conducted to give users even more control over their wireless bandwidth and capacity.

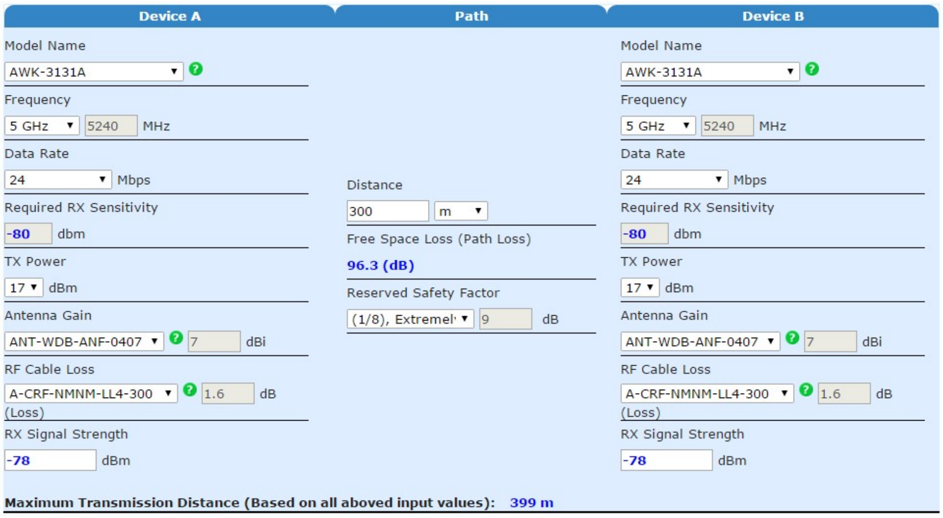
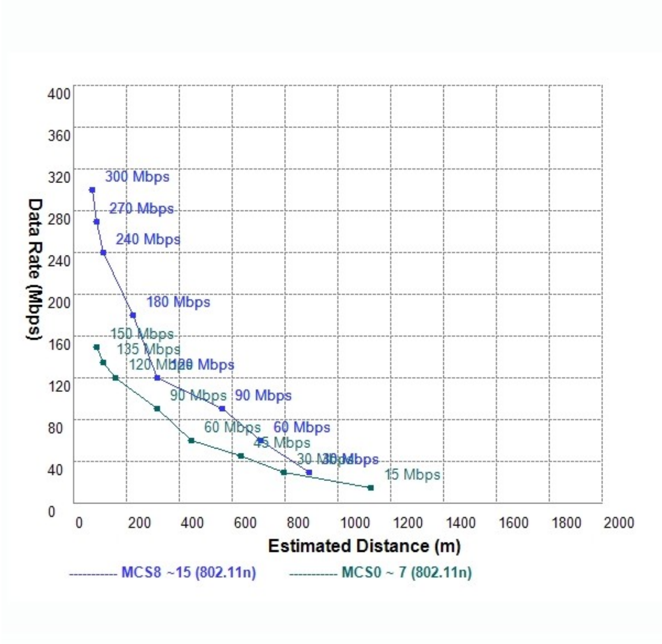


Fig. 3: The Moxa WLAN Calculator can be used to estimate signal reach values.

For example, an online distance calculator (Fig. 3) allows users to gather useful information about their radio system. A theoretical calculation is done to generate a distance vs. wireless "data rate" table (Fig. 4); you can expect the available throughput to correspond roughly with the mapped "data rate."



Estimated Distance (m)	Data Rate (Mbps)
1124	MCS0 (15 Mbps), 802.11n
796	MCS1 (30 Mbps), 802.11n
632	MCS2 (45 Mbps), 802.11n
447	MCS3 (60 Mbps), 802.11n
317	MCS4 (90 Mbps), 802.11n
159	MCS5 (120 Mbps), 802.11n
112	MCS6 (135 Mbps), 802.11n
89	MCS7 (150 Mbps), 802.11n
893	MCS8 (30 Mbps), 802.11n
709	MCS9 (60 Mbps), 802.11n
563	MCS10 (90 Mbps), 802.11n
317	MCS11 (120 Mbps), 802.11n
224	MCS12 (180 Mbps), 802.11n
112	MCS13 (240 Mbps), 802.11n
89	MCS14 (270 Mbps), 802.11n
71	MCS15 (300 Mbps), 802.11n

Fig. 4: Distance vs. data rate table created by the Moxa WLAN Calculator.

Tip 3: Maximize Link Uptime Using Wireless Redundancy Technology

Even after setting up a clean wireless transmission environment and sufficient signal reach, other factors could affect the stability of a wireless network. Hidden nodes[1], for example, which affect the ability of Wi-Fi clients to roam between different APs, are often encountered when setting up a wireless network. Another problem you may need to overcome, depending on where your wireless network is deployed, is the undesirable effects of an unpredictable environment. For mission-critical applications, wireless redundancy technologies such as dual RF redundancy or Moxa's AeroLink Protection[2] should be used to ensure quick recovery from unexpected failures.

Optimizing Mobile Communication

For M2M applications in which the machines need to communicate while on the move, such as factory floor vehicles, bus-to-depot communication, or harbor-crane control, ensuring reliable wireless transmission between the moving objects is a big challenge. Some advanced users are able to set up a reliable static wireless connection, but find that once the vehicles start moving, the connection becomes unstable. Other than ensuring that the wireless solution supports an advanced roaming technology, such as Turbo Roaming, other factors, such as 1) insufficient AP coverage, 2) incorrect roaming threshold setup, and 3) inappropriate antenna installation, can also contribute to an unstable mobile connection.

Tip 4: Achieve Sufficient AP Coverage on Your Network for Mobile Equipment

Wireless APs provide coverage over relatively small areas. For example, commercial APs deployed with their default antennas provide coverage over a circular region with radius of about 50 meters. In order to allow wireless clients to roam smoothly when moving from one AP region to another, coverage overlap is needed. Site planning software, such as Ekahau or AirMagnet, can provide a simulated wireless coverage heat map to visualize the AP distribution (Fig. 5).

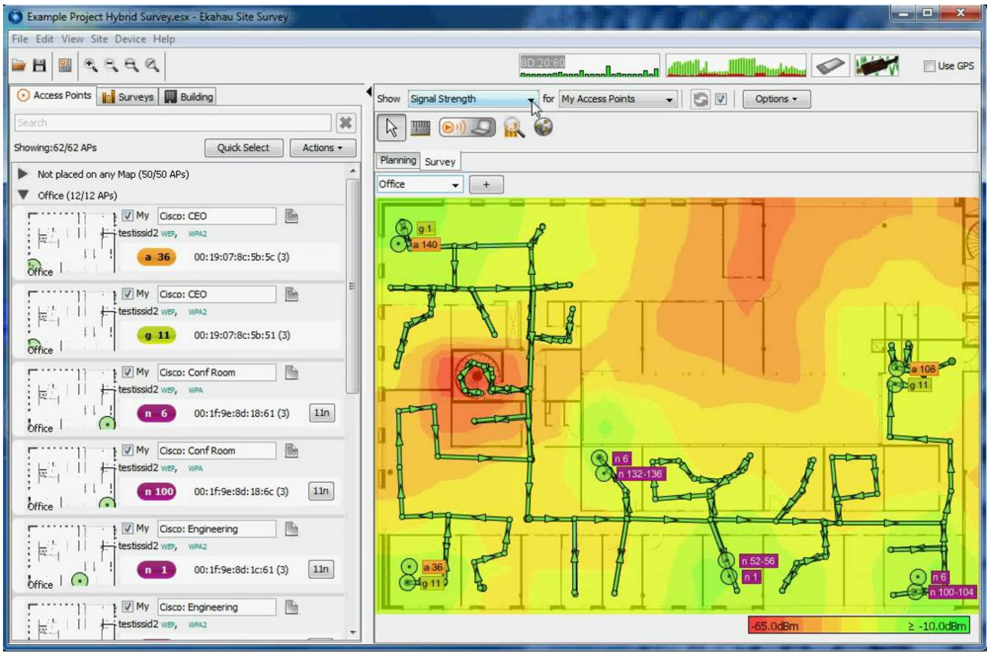


Fig. 5: Site survey created using the Ekahav Site Survey tool.

In addition, even though wireless coverage can be extended through adjacent antennas, users tend to overlook the antennas' vertical coverage. Most 802.11 antennas are passive components, which means they cannot amplify the signal's energy, but their reach can be extended by compressing the radiation pattern. For example, an omnidirectional antenna has a 360-degree horizontal radiation angle; in order to improve its horizontal coverage, the vertical angle needs to be reduced. For this reason, if you change to a high-gain antenna, don't place the antenna higher than 3 or 4 meters above the AP antennas installed on the moving vehicles.

Tip 5: Enhance Mobile Operation Using MIMO Client Antennas

2.4-GHz and 5-GHz wireless transmission requires maintaining Line of Sight (LoS) between the AP and the client. Even though the wireless connection might still get through due to signal penetration and obstacle reflection, the reduction in signal strength can affect the stability and overall throughput. There are two things you can do to prevent the connection from being weakened by obstacles: increasing the AP's distribution, and using a better antenna for the client radio. If the wireless client supports MIMO antennas, installing antennas on both ends of the vehicle (Fig. 6) will ensure better signal reception to avoid LoS problems caused by merchandise loaded on the vehicle.

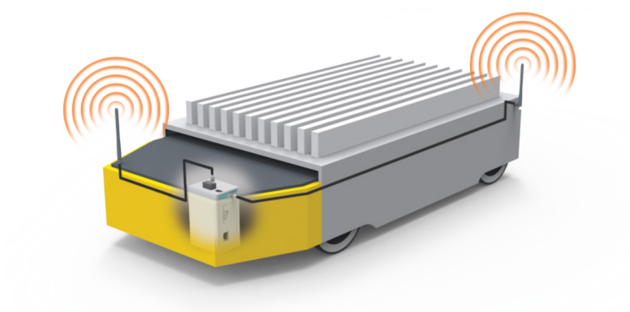


Fig. 6: Installing MIMO antennas on both ends of a moving vehicle can improve the quality of your wireless communication.

Tip 6: Optimize Roaming Performance for Mobile Operations

Advanced roaming technology should be used to keep the AP-handover time at the millisecond level. Even though standards such as 802.11r support advanced roaming technology, most wireless M2M vendors provide products that support their own proprietary roaming technologies. To optimize roaming performance, it is important that you understand how to configure the roaming technology supported by your product.

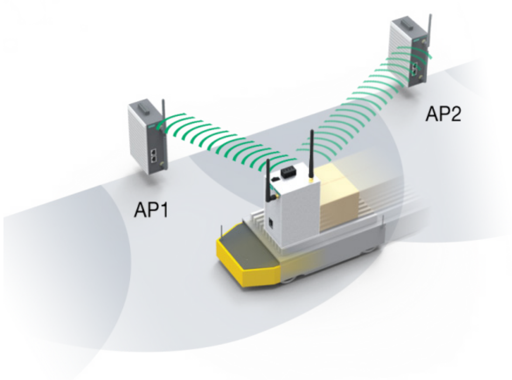


Fig. 7: Understand how to configure the roaming technology supported by your product.

Moxa's Turbo Roaming technology, for example, requires configuring the **roaming threshold** and **roaming difference** parameters.

Roaming threshold: The roaming threshold defines what conditions will prompt the wireless client to start looking for new roaming candidates. Setting this parameter to a higher absolute value, 40 dB or -35 dBm for example, allows wireless clients to start looking for new APs even though the current link is still strong enough. The drawback of this strategy is that the wireless connection will tend to switch back and forth between different APs.

Roaming difference: The roaming difference triggers the roaming event. Setting this number at a lower value makes the roaming more sensitive, and hence helps to reduce the handover time.

Ensuring Protocol Compatibility and Device Interoperability

With the Industry 4.0 and IIoT (Industrial Internet of Things) trends in full swing, a variety of automation protocols and devices are now required to operate over both wired and wireless OSI-based[3] networks. The goal is to make factories more accessible, easier to manage, and smarter. As far as industrial wireless networks are concerned, a key requirement is ensuring protocol compatibility and device interoperability.

Tip 7: Overcome Issues Related to Protocol Compatibility

Factory-based automation engineering, which has a long and distinguished history, has traditionally made use of special-purpose protocols like PROFINET and Modbus operating over very localized wire serial networks. On the other hand, IT engineering is a newer discipline that operates primarily over shared wire and wireless Ethernet networks. Whereas automation engineers have always needed to transmit data (sensor readings and control signals, for example) in essentially real time, IT engineers did not have this limitation, but instead concentrated more on providing many users with access to large amounts of centralized data.

Now that factory automation engineers have bought into the advantages of IT-type networks, that is, having ready access to all of their devices from a central location and being able to expand their operation by simply connecting devices to the network, making IT-type networks operate in real time has become a primary concern. As far as wire networks are concerned, this problem has essentially been solved. However, certain characteristics of the 802.11 protocol prevent transparent communication from a wired Ethernet connection to a wireless link. Even though most TCP/IP-based automation protocols will be transmitted successfully, there are still cases where the 802.11 configuration needs to be tweaked to ensure compatibility with the automation protocols.

The 802.11 AP/Client communication address protocol was designed with the assumption that wireless clients, such as smart phones, are the endpoints of the network. This is why only a limited number of addresses are reserved in a wireless packet for this purpose. When the wireless client is not the actual endpoint, but a device that is used to connect to additional Ethernet-based endpoints (for example, a PLC and the field devices connected to it), the standard 802.11 protocol will not be able to forward data packets correctly using just the MAC address of the endpoint device. Moxa solves this layer 2 Ethernet communication limitation with Moxa MAC Clone technology. The MAC Clone technology allows the MAC address for the additional endpoint devices to be transparent across the wireless links, enabling wireless communication for layer-2 based automation protocols such as PROFINET.

Tip 8: Handheld Device Interoperability Ensured by the Wi-Fi Alliance Logo

The widespread use of smart phones and tablet PCs for everyday applications has fueled the move to using smart handheld devices for industrial operations, and although different smart device vendors (e.g., Apple, HTC, Samsung, and Sony) use different operating systems (e.g., iOS, Android, and Windows), one thing the devices and operating systems have in common is that they all adhere to the 802.11 standard when communicating with your factory's APs. The "Wi-Fi Alliance" non-profit organization, which owns the Wi-Fi trademark, promotes Wi-Fi technology and certifies Wi-Fi products that conform to certain standards of interoperability. Not having a Wi-Fi logo does not necessarily imply that a device is incompatible with other Wi-Fi devices. However, products that have been certified and display the Wi-Fi logo provide users with greater confidence that the requisite Wi-Fi interoperability specifications are supported.

Summary

In this white paper, we have shared eight tips, divided into three main categories, on how to best use Wi-Fi in industrial applications:

Improving the Quality of Wireless Connections

1. Overcome Channel Saturation by using 5-GHz Channels
2. Achieve Maximum Signal Reach in a Long-Distance Connection through Scientific Distance Calculation
3. Maximize Link Uptime Using Wireless Redundancy Technology

Optimizing Mobile Communication

4. Achieve Sufficient AP Coverage on Your Network for Mobile Equipment
5. Enhance Mobile Operation Using MIMO Client Antennas
6. Optimize Roaming Performance for Mobile Operations

Ensuring Protocol Compatibility and Device Interoperability

7. Overcome Issues Related to Protocol Compatibility
8. Handheld Device Interoperability Ensured by the Wi-Fi Alliance Logo

Moxa has many years of experience helping customers build reliable wireless networks. Click here to download our success story brochure to learn more about Moxa's wireless solutions.

References

[1] **Hidden Nodes Issue:**
http://www.moxa.com/support/request_catalog_detail.aspx?id=1447

[2] **Wireless Redundancy Technologies:**
http://www.moxa.com/support/request_catalog_detail.aspx?id=1439

[3] **OSI 7 Layer:**
https://en.wikipedia.org/wiki/OSI_model