F3 Wireless

White Paper

# Wi-Fi vs. Cellular
for IoT Device Connectivity

Introduction

Connectivity is the lifeblood of any IoT device. It is literally the “I” in “Internet of Things” – so if it does not reliably connect, your device ceases to be useful.

When thinking through the development of a new IoT device, be it for industrial, medical, municipal, energy or basically any use-case, it can be tempting to look at “ambient Wi-Fi” as a solution for internet connectivity. Typically, the most compelling reasons for using “existing Wi-Fi” or “the customer’s Wi-Fi” vs. using cellular are the recurring communication and device costs. There are implications in using infrastructure you don’t control, however, that are not immediately obvious.

It is vital to make informed decisions on the best connectivity method for your device in the case where you can’t apply local infrastructure: Wi-Fi or cellular. Below we outline the pros and cons of each option.

Wi-Fi devices communicate using a Wif-Fi radio. Cellular technology connects IoT devices to the Internet through a cellular radio.

Using Wi-Fi for IoT

With Wi-Fi technology, devices can communicate using multiple bands at frequencies of 2.4 GHz and 5.8 GHz. Some devices only support 2.4GHz and some support both. A device must have a Wi-Fi radio to communicate on the network and the radio comes in a few different forms.

For devices with a big processor running Linux, the radio can be a low-cost, high-performance part from Qualcomm, Marvell, RealTek or others. In this case, most of the software to implement Wi-Fi and TCP/IP runs on the host CPU and the interface to the host is usually USB, SDIO or PCIe. It normally isn’t SPI or UART because those interfaces aren’t fast enough.

For smaller, lower cost devices it’s more common to have a Wi-Fi radio module that includes the Wi-Fi and TCP/IP networking software processing. This allows for a much simpler software interface to a simple microcontroller running an RTOS or C on bare metal, typically over a UART or SPI interface.

Using cellular for IoT

Cellular technology connects IoT devices to the Internet through the same networks used by smartphones and other mobile devices. A device must have a cellular radio and supporting circuitry, and all cellular radios include both the cellular network and TCP/IP processing needed for communications. Your host microcontroller controls the radio with UART or USB. Some cellular modules can also appear as a network interface card via USB and allow for the TCP/IP processing to be done by the host CPU.

Comparison by feature

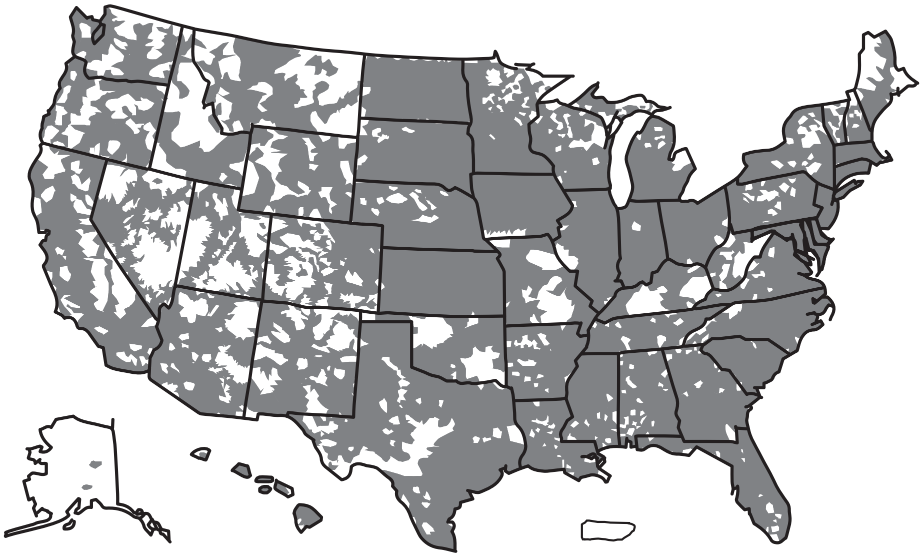
While there are a wide range of specific technical details that can be compared, such as power consumption based on use-case, interference susceptibility, bandwidth, and latency guarantees, we’ll focus on the fundamental nature of the radio systems and the implications on your system design.

COVERAGE

Wi-Fi coverage is typically limited to what you can cover with a single access point (AP). Some AP systems allow you to have multiple APs that use the same network name (SSID), but residential and even many commercial users seldom have more than a single AP with a given SSID. This can be a particular problem when deploying products further away from a typical AP location. For instance, Wi-Fi devices may be located in basements, garages or other locations with greater distance and/or obstacles between the AP and device. This can create situations where the only viable solution is to add another AP specifically to support the new device.

While all radio signals are affected by obstacles, cellular networks are designed to cover a much wider area, using much more elaborate and expensive equipment and techniques than any single AP deployment could justify. This leads to a much better typical signal strength across a wider range of use-cases.

The signal levels in the basement or in the garage are similar to the home office. From a system planning standpoint, cellular coverage is much more consistent and reliable than Wi-Fi coverage. This isn't to say there aren't coverage issues with cellular, but generally it's not an issue you have to solve for every device you sell like it tends to be for Wi-Fi.



EXAMPLE OF US CARRIER CELLULAR COVERAGE MAP

This issue becomes most important when you consider who's responsible for creating or repairing that coverage. When you rely on the end user themselves to create or repair coverage, you're pretty much asking for tech support calls. While some products can push back and basically say "that's the customer's responsibility," there are plenty of products where that's not an acceptable situation.

It would be easy to assume that Wi-Fi is free.

SECURITY & PRIVACY

The equipment required to intercept cellular radio messages is fairly exotic compared to Wi-Fi, giving cellular an advantage. While this wouldn't deter an intentional attack, it does cut down on the occurrence of casual mischief. The bigger security issue with Wi-Fi is actually after the radio link. That wire coming out of the Wi-Fi AP has no encryption on it at the network layer, so whatever messages are going over that link are visible to anyone along the way.

The cellular network and its connections within the phone company are encrypted and generally only accessible to the phone company itself. This makes it much harder for anyone without access inside the phone company or an internet service provider to get access to the data channel.

Security updates are another factor to consider. With cellular, updates are typically made by dedicated cybersecurity professionals. Cellular carriers have more incentive to ensure security updates are made as soon as possible and in a seamless, transparent way. With Wi-Fi, it falls to individual network owners to make these updates, making it easy to overlook or delay making vital changes.

Properly designed IoT devices implement end-to-end encryption with no reliance on channel encryption. This ensures that regardless of the channel, your data is secure – and that holds true for both Wi-Fi and cellular.

COST

It would be easy to assume that Wi-Fi is free, since someone else is usually paying for the internet access, equipment, and infrastructure installation time. While it is true that, versus cellular, the per-byte cost for Wi-Fi is cheaper if everything works according to plan, nothing is completely free. For example, will some part of your customer base need to install Wi-Fi just to use your device when they want to use it? Forcing customers to create an infrastructure could definitely be a disincentive to using your product – and therefore may not be preferable over cellular.

Let's take a closer look at the cost of two major factors:

- **Installation costs** – It can be easy to assume that Wi-Fi would be cheaper. Since the end user is doing the installation, it doesn't have to be factored into the up-front costs shown in a cost/benefit spreadsheet. In reality, installation costs can actually end up being higher once you factor in returns, shipping, and complaints from customers that can't set up your product to use their Wi-Fi. In many cases it's not a problem with documentation or ease of use. It's simply that Wi-Fi is fairly complicated to set up even when handled well and often setup requires working with

It all boils down to this: Who owns the network and who owns the device?

multiple devices such as the DSL/Cable modem, a separate Wi-Fi AP, and range extenders in addition to your new device. Most consumers are not networking experts.

- **Support costs** – With Wi-Fi, the end user is doing any troubleshooting, so the assumption is support costs are lower with less need of a professional support team. In reality, like with installation, you may well see higher support costs once you factor in equipment exchanges, customer frustration, and customer down time.

INSTALLATION & SUPPORT

It's not just installation and support costs that need to be considered. You also have to factor in who is responsible for these things when something goes awry.

With Wi-Fi, the end user is doing the installation, so responsibility falls to them to place the device in the best location for optimal performance. This also means you have little control of when the user performs the install, how prepared they are, and if they have proper training.

The end user would also be doing any troubleshooting to the device post installation. Since the user is responsible however, they may or may not fix something when it breaks. They may not even notice if something is wrong for quite a while. Once they do notice, users often blame the device rather than changes to their infrastructure.

Conclusion

There is no one-size-fits-all solution to IoT connectivity. This means that taking the time to make educated decisions based on what will work best for your particular device is crucial.

In many ways, it all boils down to this: Who owns the network and who owns the device. Wi-Fi works best if the network and device are owned and managed by the same entity with an interest in the device being functional. That could be a residential user installing a network camera for their own use for instance.

When selecting the best option for IoT connectivity, your best bet is to work with the experts. At F3 Wireless, we specialize in making the "thing" in the Internet of Things. Our professionals can help you explore your business case needs and help you understand the trade-offs so you can choose what works best for your needs. F3 has options for Wi-Fi-enabled products and works with all of the major cellular module vendors as well. Whichever route is best for your device, F3 can take care of making it wireless.

About F3 Wireless
F3 Wireless is a custom wireless electronics device organization based in Minneapolis that offers consulting, engineering, design, certification, and manufacturing for the "things" in the IoT. F3's core competency is wireless in all of its variations, and providing best in class device cost and time to volume.

For more information, visit www.f3wireless.com.