Mixing Multiple Wireless Technologies

White Paper

Joel K. Young
Senior Vice President & CTO, Digi International Inc.

Abstract

This paper explores how to mix different wireless technologies, including cellular, Wi-Fi®/802.11, WiMAX™/802.16, Bluetooth®, ZigBee®/802.15.4 and proprietary wireless to form a successful commercial or industrial deployment.

1. The Quandary

More and more we find ourselves living in a wireless world. From the consumer market perspective, most of us have a cell phone – even our children; most of us have Wi-Fi in our house; and when we do use a landline telephone – often enough it's a wireless handset. As a part of this, as consumers, our behavior has adapted as well. We know to look at our phone and notebook computer to see "how many bars we have". We have learned to deal with moving around to improve the signal, how long our battery will last and the pitfalls of not putting our device back on the charger. Fortunately or unfortunately for consumers, mission criticality in the instant tends not to be as important and necessary human intervention is an accepted outcome. Finally, as consumers, we have also begun to expect that the cost of wireless will continue to approach the cost of the corresponding wired counterpart.

So what does this all mean for us in the world of industrial and commercial things? As advancements in wireless technology have caused the wired paradigm to fade and as pervasive wireless in consumer markets has driven our belief in easy, low cost solutions, we need to remember that commercial needs are different. We can't always rely on the human presence to adjust for the "number of bars" or to initiate a "new call." We also need to account for the relatively small number of devices in a consumer application environment compared to the thousands of units in a commercial or industrial environment. Sure, there are millions of consumer devices, but each of us still only has a handful to manage. Finally, we need to acknowledge that reliability and mission criticality needs have an impact and a cost. As such, we are forced to ask if a wireless solution in the commercial and industrial world can be cost effective.

Given both these consumer perceptions and commercial realities, this paper will explore how to mix different wireless technologies to form a successful commercial deployment.

2. Wireless Technologies

Figure 1 illustrates the different wireless technologies found in deployments today. For this article, we will be focusing on the interactions between all of them except Bluetooth, as we haven't seen a preponderance of usage outside of the consumer space.

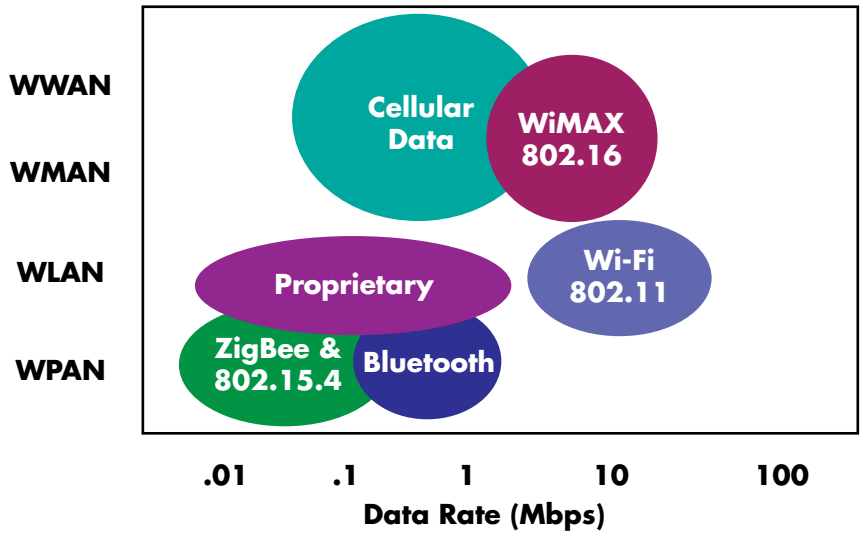


Figure 1 – Wireless Technologies

2.1 W-WAN: Cellular & Wi-Max

We start with wireless wide area networks or W-WANs. Figure 2 illustrates a view of both the history and expected future of these technologies. For those purists – please don't get too caught up in the dates as they are intended to represent a sort of worldwide average. The colors indicate the technology evolution and the throughput numbers are meant to illustrate best case. For comparison, Wi-Fi has also been added – even though it is really a LAN not WAN technology.

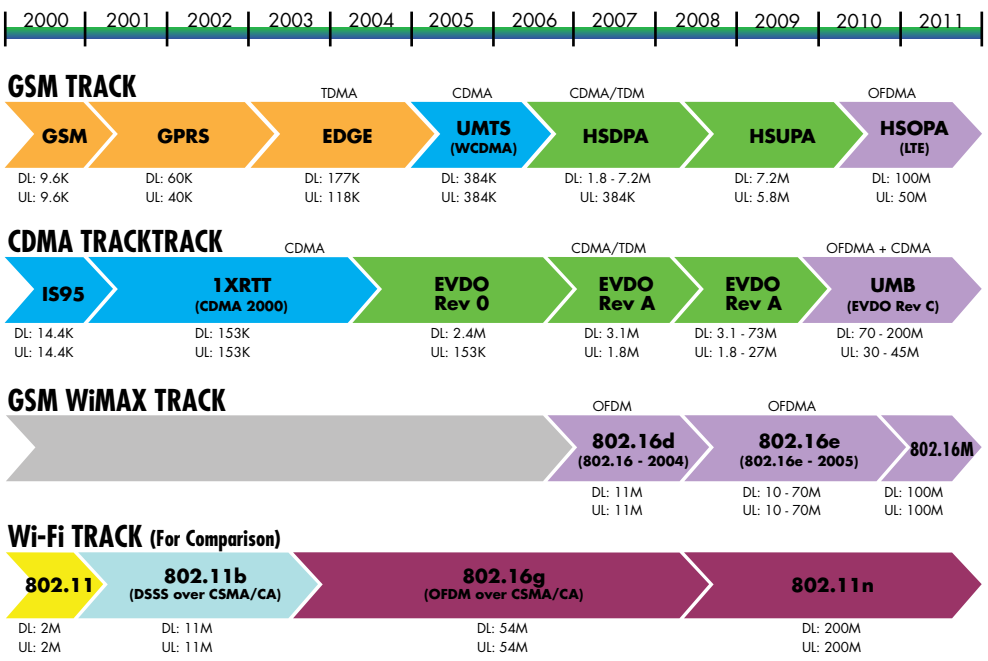


Figure 2 – Wireless WAN Technology Paths

While this paper is not intended to be a W-WAN tutorial, it is difficult to discuss the trade-offs without providing some brief definitions of the technology at hand.

TDMA (Time Division Multiple Access) – This is the technology used in the original GSM and the original digital cellular networks. With TDMA, a single frequency band (or channel) is shared by splitting it into time slots. Effectively, it provides equal time for all, as long as there are time slots available. It is simple and easy to manage; however, it doesn't tend to scale well for bursty, high throughput data applications. 2G and 2.5G cellular GSM systems use TDMA for GPRS and EDGE data services.

CDMA (Code Division Multiple Access) – By virtue of the same name, this is the technology used in the "CDMA" style networks. With CDMA, the signal is spread across multiple frequencies using a pseudo random code. If you don't know the code, the signal looks like noise. The amount of spread is related to the amount of data to be sent, so it scales to bandwidth demands. For this reason, high speed data on GSM networks (UMTS) uses CDMA technology. 2.5G cellular CDMA systems use a scheme called 1XRTT. With the advent of 3G systems, GSM based systems follow the UMTS/HSDPA track, while CDMA carriers follow the EV-DO track.

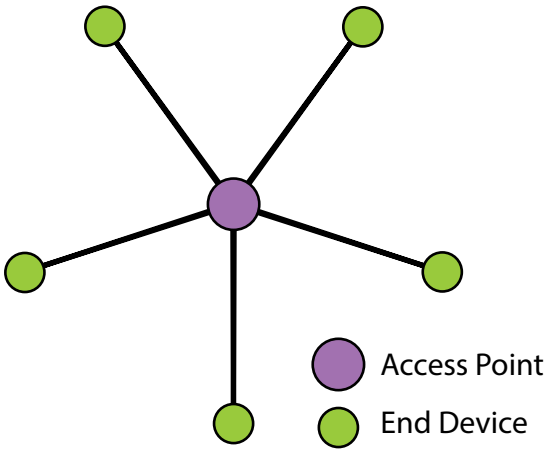
OFDMA (Orthogonal Frequency Division Multiple Access) – This is the technology used for Wi-MAX and the other fourth generation cellular data systems. OFDMA's cousin, OFDM, is used in higher speed Wi-Fi. With OFDMA, the signal is split to several narrow channels at different frequencies. Subcarriers are then assigned to individual users. It has the ability to offer bandwidth on demand and also offers immunity to multipath issues, enabling much higher data rates. OFDMA systems like Wi-MAX (802.16 family of standards) are completely optimized for data, which means they don't carry any of the voice infrastructure overhead. In theory this should make them more cost effective to deploy, more cost effective to certify and more open.

Key Issues – Depending on the needs of the application, there are a number of key issues that must be looked at when choosing a W-WAN system. The first of which is to assess what kind of data throughput, latency and quality of service that is needed. No matter what the technology, the higher the performance, the more you are going to pay. In addition, there are four other points worth remembering:

(1) IP Addresses & Routing are a big deal. Depending on the plan, IP Addresses are often private & dynamic and destination routing usually doesn't work. Hence make sure that you use device initiated connections or have a way of simulating an extended network using something like a VPN. Note – device initiated connections are critical.
(2) Data plans are complicated. This remains one of the immutable laws for telecom. There are very few unlimited data plans for the non-human tethered device. However, you can get a very low telemetry data plan as long as you know how much you are going to use. Hence it is important to know your data needs and select a plan which allows pooling of data.
(3) Carrier cooperation is critical. Whoever your carrier might be, make sure that the device you are using is supported and certified by their network. If it isn't, you may find yourself without service. Just because a SIM card works doesn't mean that you are allowed to connect your device into the network.
(4) There is no ubiquitous coverage. Even the carriers with the best coverage can't cover everywhere and the networks most often have capacity where humans are present. So if you are deploying to a remote site, you may need to employ extraordinary measures to get coverage.

2.2 Wi-Fi

Wi-Fi most often refers to the 802.11 family of standards. For those of you that like letters, the range of standards stretches from 802.11 and 802.11a all the way past 802.11s. Most of us have become familiar with the letters b, g, a, and n, with the more security savvy of you also knowing the letter i. Wi-Fi is used mostly as a WLAN (Wireless LAN), but also is used for some WAN-type access. Note that the "WAN" environments are really LANs masquerading as a WAN, without any of the



channel access quality of service attributes that you get from the aforementioned W-WAN technology. This is because, at its heart, Wi-Fi is a shared bandwidth system where access is handled using a collision avoidance system (CSMA-CA) akin to an intersection without traffic lights or stop signs – it works well when there isn't much traffic.

The typical architecture for a Wi-Fi system is a star topology where users associate with things called Access Points. Mobility is allowed between two Access Points – but often becomes problematic if the Access Points are on two different subnets. Probably the most important thing to note about Wi-Fi is manufacturers tend to cater to the mass of consumers carrying notebook computers and PDAs. Hence chipsets vendors turn over quickly looking for the lowest cost solution – which may not be appropriate for a long term commercial or industrial deployment. In addition, the other important points to note about Wi-Fi are that the system is not intended or well suited for low-power consumption and that you must be prepared to match the security policy of your environment.

Key Issues – Given the items mentioned above, the following are key issues that should be considered when choosing Wi-Fi for commercial and industrial applications.

(1) Plan to fit into the existing infrastructure – whatever it might be. One of the key benefits of Wi-Fi networks is that there are so many already deployed. This is one of the most common reasons why Wi-Fi is chosen as a technology. Nonetheless, remember that the network was probably deployed with humans in mind, so coverage might not exist where your device needs it. Hence, it is a good idea to perform a site survey to understand the range of the system.

(2) Interoperability starts and ends with SECURITY. Since the network you are using is most likely already deployed, it also already has a security policy. The family of Wi-Fi related standards has a myriad of different encryption and authentication methods – and as the new device on the network, it is your responsibility to conform to that policy. This means choosing an embedded Wi-Fi supplier that has implemented the full range of security options.
(3) Choose embedded partners wisely. While this relates to security, it also means that you want to make sure that the radio design will be available for the long term. Be wary of consumer radios that will trigger embedded driver upgrades. The cheap radio may not actually be low cost in the end.

2.3 ZigBee & Related PANs

Personal Area Networks or PANs originally were designed to mean a very small area around a person. Over time, this definition, like many others, has morphed and expanded to the point where I tend to define a PAN as any wireless network that is not Wi-Fi (WLAN). I've heard others describe it as any that doesn't support IP, but for me that seems too limiting. Nonetheless, when talking about PANs, we usually also start talking about mesh networks (even though a mesh network architecture can be wide area as well). Further, discussion of mesh networks often leads to ZigBee. The other key attributes commonly associated with PANs are low power (meaning the potential to power by battery for a long time) and low cost (meaning that it is cost effective to deploy a large number in a small location). I recognize that bringing complete order and understanding to this topic is easily a paper on its own. Nevertheless, to adequately discuss keys to deployment, it is necessary to have a mini-tutorial.

To begin, we must first separate two concepts: (a) a mesh network and (b) a point-to-multipoint network. Some purists will no doubt point out that I've left out a peer-to-peer network. However, I see a peer-to-peer network as the simplest form of point-to-multipoint, where the "multi" = 1. A point-to-multipoint network is a star topology (like Wi-Fi) where there is a central point that maintains a relationship with each end device. The central point may or may not provide routing to other end points. A mesh network dynamically forms routes between any two points via any other routing capable points that it sees, leading to the statement that all routers may be end points, but not all end points are necessarily routers. Point-to-multipoint networks are simple to manage, but require that every end point has a view of the central point, or hub. A common standard used in point-to-multipoint PAN implementations is 802.15.4. A mesh network doesn't care, thereby enabling an ad hoc type of deployment. Mesh networks then are easy to deploy, but may be difficult to trouble shoot if there is a problem. A popular mesh networking PAN standard is ZigBee, the latest version being ZigBee 2007. Finally, it is important to note that there are also many proprietary implementations of point-to-multipoint and mesh networks.

So the question becomes, how do you choose what type of wireless PAN technology is right for the application? For this I offer four words to remember: Power, Range, Environment and Data Flow.

Power – Are nodes and routers going to be battery powered or is there access to continuous mains power? Keep in mind that extreme low power solutions usually have restricted range and duty cycles. For example, if there is plenty of power, duty cycle and transmit power are non issues.

Range – How far do you need to go between RF points? This ends up being a direct trade-off with power consumption. If you need to a long distance, but don't have a big power budget then 900 MHz might be best. Or, if you have plenty of power and are uncertain about the location of end points, then a mesh network might be best.

Environment – Is it noisy or quiet from an RF perspective. Does the environment change based on time of day or other characteristics. In addition, are there multiple vendors of equipment? For example, if the 900 MHz spectrum is crowded, then a 2.4 GHz solution may be more suitable. If you want to talk in a multivendor environment, then you need ZigBee 2007.

Data Flow – How is the data meant to flow? Does it always flow to a centralized point? Are there any latency restrictions? What are the throughput requirements? How often does data flow? For example, if your data always flows to a reasonably close, centralized point, then a point-to-multipoint network may be best.

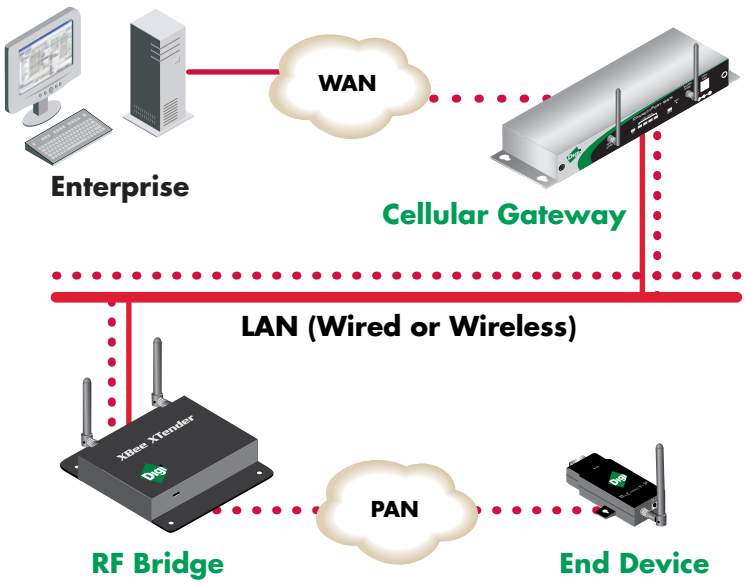
Key Issues – Given the items mentioned above, the following are key issues that should be considered when a PAN for commercial and industrial applications.

(1) Assess the environment. Generally you want to use a PAN when no other infrastructure present or when you have low power consumption requirements. Then ask what does the spectrum look like? If it is noisy, a frequency hopping or frequency agile solution is probably necessary. Do you have power?
(2) Test before you deploy. Even though you might be deploying an ad hoc network on the fly, you still need to identify the RF weak spots and single points of failure. This includes assessing the environment at different times of day.
(3) Practical interoperability over the air. What level of interoperability among different devices is required? Interoperability

means more than just conforming to the standard. For example, two 802.15.4 or two ZigBee based applications may not be able to talk to each other, even if they comply with the standard. A standard only goes so far and almost never guarantees application compatibility – rather, they are meant to define the level of interoperability that can be expected. Application context and provisioning really important for a practical sensor system

3. Putting the Pieces Together

A practical wireless system may involve wireless components at the WAN, LAN or PAN level. The critical components in architecting a well designed system must be selected with understanding and awareness regarding the flow of data and the type of service required.



Hence, in closing out this paper, I leave you with both a selection of critical questions and decisions and a set of guiding principles which should help ensure success.

3.1 Critical Decisions

Looking at the four areas can best help define the ideal solution which mixes multiple environments.

(1) Define how you want the application to work. In this context, it is important to assess the end to end the functionality, level of service, location of intelligence, and level of security. The question of functionality usually relates to whether the application is for logging, control, alarming or potentially all of them. Level of service involves whether the data is mission critical or best attempt. This is then helps drive where intelligence should be placed. As a general rule intelligence can be placed at the device, at an intermediate point or at the enterprise – and it is generally unwise to put intelligence every where and mission critical communication almost always requires intelligence at the end device. Security then should be overlayed on top by evaluating what happens if the system is compromised from both an access and eaves dropping perspective.

(2) Infrastructure – What's already in place? Evaluate the environment for what already exists. This includes whether there are any opportunities to use existing cabled communications and local power as well as the availability of wireless infrastructure like Wi-Fi and cellular signal strength.

(3) Fill in the Gaps. With the application needs determined and the available infrastructure evaluated, it is time to complete the puzzle. This now involves doing an environmental assessment, site survey and cost trade-offs for different deployment options.

(4) Look beyond the pilot. Deploying a mixed wireless system can be complex on the environment, but also on the deployment. As such, it is important to answer the final questions of how will the system be deployed over many sites? Is it scalable? Is it maintainable? Often times it is easy to get an initial system in place through brute force, but fall down when duplicating it or maintaining it.

3.2 Guiding Principles

With this in mind, the following are guiding principles that should help with the system design and deployment. As a general rule, in addition to the other technology specific hints offered earlier, following these will provide for the highest probability of success. We say highest probability, because with wireless, there always seems to be some magic.

(1) Focus energy on high payback things first. Don't try to solve world hunger from the start or you will have an unwieldy system to trouble-shoot. Nonetheless, you must do this with an eye for potential future expansion.

(2) Focus intelligence at a common level. Sometimes there is a natural tendency to build intelligence into the system at every level under the belief that it makes a more robust system. Unfortunately, custom logic and filtering at too many places makes trouble shooting difficult – especially when using multiple wireless technologies. Place decision making where it is most efficient.

(3) Minimize the number of vendors and/or different technologies. We all dream of a beautiful, efficient, multi-vendor environment. This is often quoted as the true benefit of standards. It is important to remember that standards give you multiple sources – but standards don't mean you must mix and match. Too much mixing and matching obviates your suppliers from responsibility – because they can always point to the other supplier.

(4) Match the network to the criticality of communications. Don't try to over engineer the system. If your system communications aren't mission critical, don't try to make it that way. It will add cost and complexity in the end.

(5) If you have a cable, use it! Wireless technologies are wonderful things, but a short cable always works better.

91001448
B1/1115

DIGI INTERNATIONAL WORLDWIDE HQ
877-912-3444 / 952-912-3444 / www.digi.com

DIGI INTERNATIONAL FRANCE
+33-1-55-61-98-98 / www.digi.fr

DIGI INTERNATIONAL JAPAN
+81-3-5428-0261 / www.digi-intl.co.jp

DIGI INTERNATIONAL SINGAPORE
+65-6213-5380

DIGI INTERNATIONAL CHINA
+86-21-50492199 / www.digi.com.cn