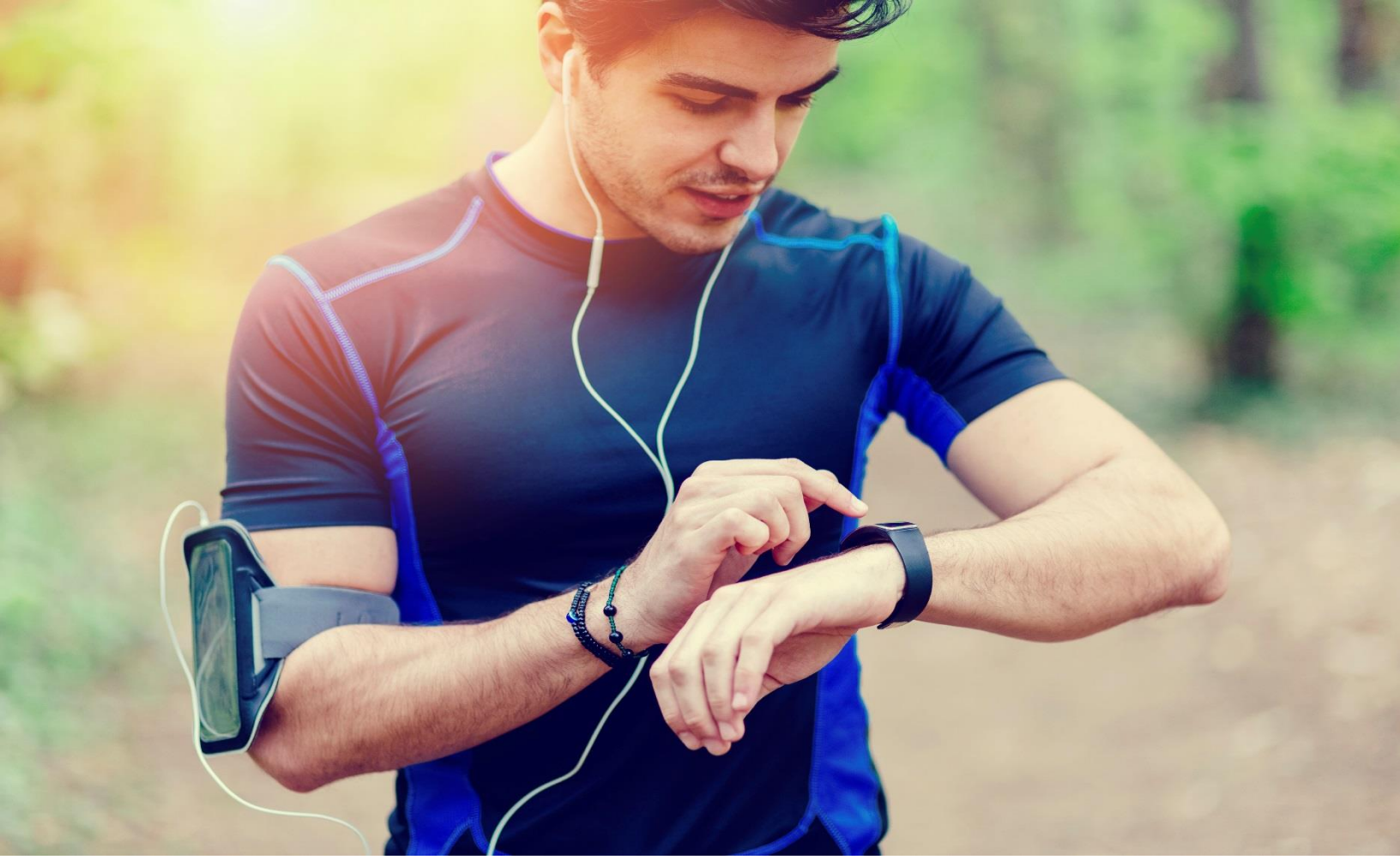


Wireless wearables: The role of Wi-Fi® in enabling digital health

May 2016

Executive summary

Enabling the promise and value of digital health as it relates to the Internet of Health (IoH) requires the use of wireless technology. With the proliferation and ubiquity of Wi-Fi® in the home, hospital, and everything in-between, Wi-Fi will play a dominant role in making the digital health vision a reality. The benefits of using wireless technology in wearable devices are numerous, ranging from reduced cable clutter, fewer accessories requiring infection control, increased patient comfort through smaller wearable devices, uninterrupted monitoring outside the hospital, and reduced recovery time by enabling patients to ambulate within the care area and still be monitored. Historically, these benefits only extended to the boundaries of the hospital, but with the digital health ecosystem, those boundaries will be broken down and extended into the patient home. In the ecosystem of digital health, users will be monitored in real-time, anytime and anywhere, through the use of wearable wireless devices.

This paper provides an overview of wireless technologies in the digital health ecosystem and focuses on the role of Wi-Fi and associated best practices in enabling the promise of wearable devices in digital health. The paper will define and outline wireless wearables within the digital health ecosystem, typical radio frequency (RF) environments and use cases for wireless wearables as well as associated challenges and best practices, and relevant and associated Wi-Fi certification programs to deliver the optimal user experience through Wi-Fi connectivity.

Introduction

The lines delineating which wireless technologies are most appropriate for which part of the data link between wearable devices and sensors, smart phones, data aggregators, gateways, and connectivity to data warehouses are increasingly blurry. Understanding where Wi-Fi fits into these different models, how to meet the variety of connectivity requirements, and which Wi-Fi implementation decisions are best practice is a challenge for all developers of wireless wearable devices.

This white paper addresses common questions of product developers, integrators, and end users of wireless wearable devices. Below are questions the reader should consider for their given role.

Product developers

- How does Wi-Fi deliver as the wireless technology in wearable wireless device, and what are the important design considerations and associated best practices?
- Where does Wi-Fi play a role in expected use models, and what are the capabilities and requirements at both the device and wireless local area network (WLAN) infrastructure levels associated with the successful implementation of Wi-Fi-based solutions?

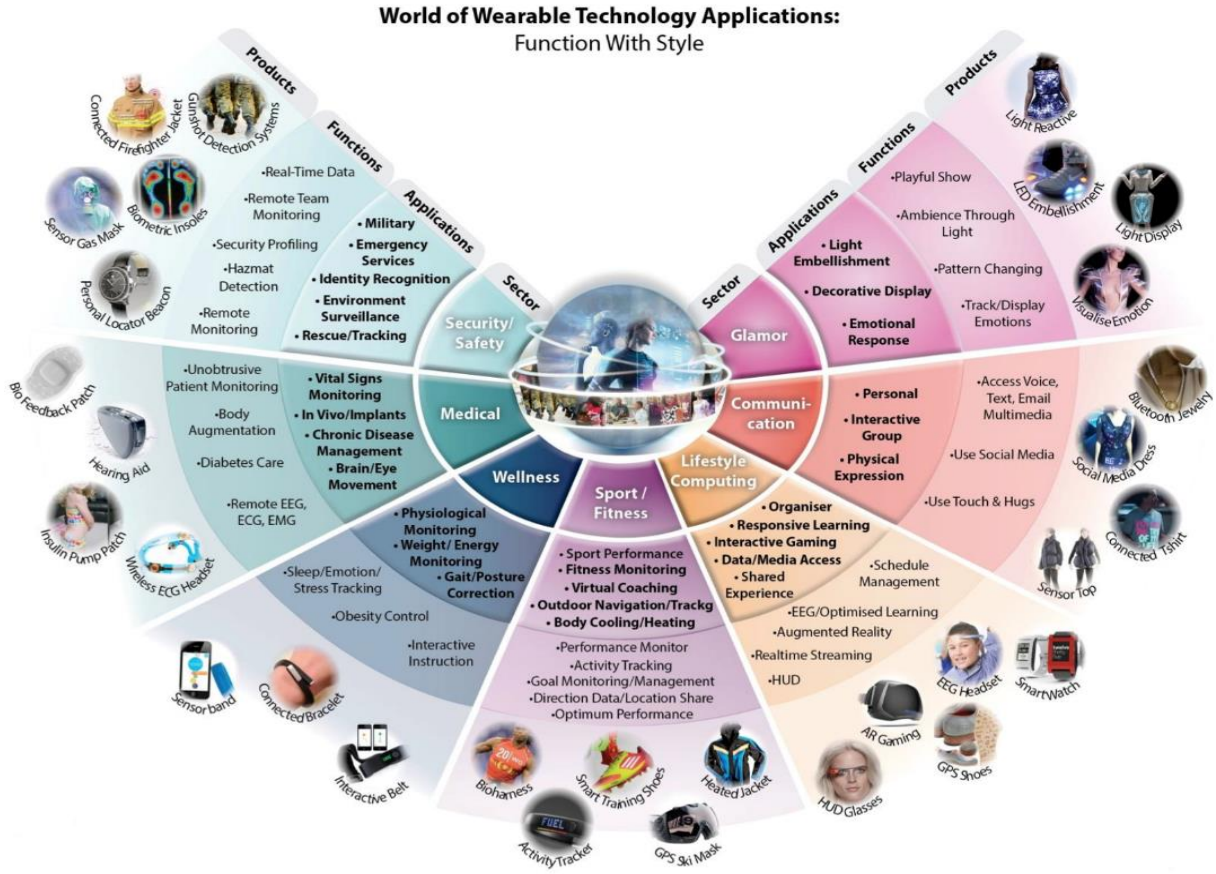
Infrastructure system integrators, healthcare delivery organizations, end users

- As a user of the digital health ecosystem and wireless wearable devices, what implementation and use considerations are important for wireless wearable devices?
- What Wi-Fi capabilities should factor into the selection of Wi-Fi devices (e.g. certifications), and what best practices are critical in successfully enabling Wi-Fi in expected environments (e.g. home, enterprise)?
- Who are the purchasing decision makers and users of wireless wearables? Have their inputs been adequately considered in the purchase, deployment, and use of devices?

Digital health wireless ecosystem

The healthcare industry is moving from a reactive model of providing care where sickness is managed post occurrence, to a preventive value-based model where patients and their families play a key role in proactively managing their own health. Digital health fits into the framework of the Internet of Things (IoT) as an ecosystem that captures vast amounts of data from many devices and sensors and enables big data in healthcare such as population health management and clinical decision support. The wireless connectivity of These

sensors can take advantage of the ubiquitous wireless connectivity of Wi-Fi and its inherent capabilities to enable secure, robust, mobile connectivity. Machine-to-machine (M2M) connections in the connected health consumer segment are forecasted to grow by more than eight-times (54 percent CAGR) from 2014 to 2019[1]. The consumerization of healthcare enables digital health by providing innovative hardware and software platforms for building wireless wearables and their connectivity into the healthcare ecosystem. To ensure that this data is available when and where needed requires subsystems to



Source: Beecham Research, Ltd. & Wearable Technologies AG

Figure 1. World of Wearable Technology

interoperate collectively without loss or degradation of connectivity. These connectivity requirements combined with other system-level requirements, such as cybersecurity and patient data confidentiality, place significant demands on supporting wireless communications. Whether it is high-bandwidth streaming data or aperiodic bursts of data, there is significant demand for secure, ubiquitous, and reliable wireless transport.

[1] http://finance.yahoo.com/news/cisco-visual-networking-index-predicts-120000213.html

Figure 2 shows common architectures of wireless wearable communications. In general, wireless wearables are sensors or other health data devices that connect either directly to a wireless network or through some other proxy device such as a gateway router or smart phone. The data sent by a wearable through the Internet typically makes its way into a data center or cloud-based service. Here, the data is stored, analyzed, and presented to patients, families, and physicians. This may happen through interfaces such as patient portals that tailor the information to the user's specific view. Moreover, the applications analyzing the received data may also trigger notifications urging specific actions. For example, readings from a glucose monitor might send an alert to a patient urging them to take insulin. Additionally, abnormal readings from a heart monitor could elicit an alarm to a patient's doctor warning of the need for further evaluation and action.

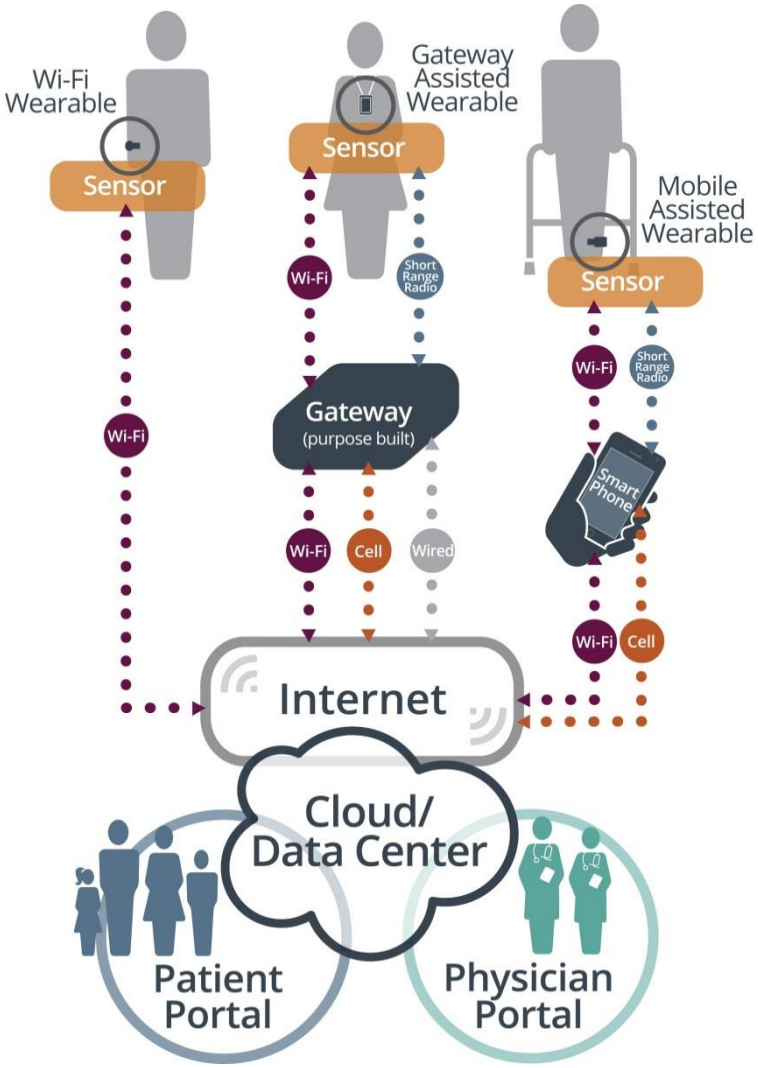


Figure 2. Architecture Overview

Figure 2 shows three typical paths of communication:

1. Wi-Fi wearable: a sensor or other body-worn health-monitoring device that supports Wi-Fi natively in the device and directly connects to the network via a Wi-Fi access point (AP).

2. Gateway-assisted wearable: a sensor or other body-worn health-monitoring device that uses wireless technology to connect to a middleware device that acts as a gateway and provides connectivity to the Internet.

3. Mobile-assisted wearable: a sensor or other body-worn health-monitoring device that connects wirelessly to a mobile phone (e.g. smart phone) for access to the network or internet as well as access to applications on the mobile phone.

Wireless wearable design & development considerations

Wireless wearable devices appear in a variety of healthcare ecosystems ranging from the home, the hospital, or anywhere in-between, such as coffee shops, fitness centers, and public and private transportation. Each of these environments may have a different wireless operational model with their own unique RF environments that require consideration in the design phase. With widespread use in all of these environments, Wi-Fi is the wireless technology of choice for enabling the digital health ecosystem.

Coverage & capacity

Two key factors related to the successful operation of Wi-Fi in these environments are RF coverage and data capacity. Coverage is the ability to have adequate access to wireless services in a specific physical area. Capacity is the amount of bandwidth available in the area of coverage. Together, these two key factors define the available bandwidth in a specified area. Coverage and capacity are interrelated when considering how to meet the data needs of anticipated wireless wearable devices. The links in the reference section provide more details regarding best practices in the WLAN design to meet coverage and capacity needs. From a device perspective, developers should specify and accommodate the operational needs in terms of coverage and capacity during the design phase and verify adequate coverage and capacity during development testing.

Antenna & radio design

A key, often overlooked consideration in meeting the operational needs of a device is the combined performance of the antenna and radio. Even when a radio that has antennas built into the module is used, the quality of the selected radio and the performance of antennas embedded inside the wearable device housing impact the overall performance of the wearable device.

With a well-designed infrastructure and a strong radio design, wireless medical devices are able to connect anywhere within a hospital and reliably deliver the vital patient data they collect to the viewing and data storage devices on the network. In the case of Wi-Fi, the IEEE 802.11 standard calls out several key radio requirements that any Wi-Fi-enabled product must meet in order to maintain performance. Any radio selected for a wearable wireless device should be thoroughly tested first, for compliance to the IEEE 802.11 standard, and second, for sufficient design margin to ensure the radio performs in the harshest of wireless environments.

Once confident in the radio design, the next area of focus is the antenna. In some cases, the wireless wearable device has embedded antennas. The surrounding material can

greatly affect the radiation pattern of the antenna when compared to the datasheet values obtained in free space or open air. Power supplies, displays, printed circuit boards, and even the device enclosure can cause constructive (increased signal) or deconstructive (decreased signal) interference with respect to the free-space antenna gain. Furthermore, if the clinical use case requires antennas in close proximity to a hand, head, or torso, additional signal degradation can occur.

Prior to product release, developers should conduct extensive testing to ensure the antenna is radiating the maximum amount of power appropriate for the anticipated clinical use cases. An industry standard test, Converged Wireless Group – Radio Frequency (CWG-RF), developed jointly by Wi-Fi Alliance® and CTIA, is commonly executed with smart phones and other handheld devices. Executing the CWG-RF test procedure provides valuable insight into antenna performance. Outputs of these tests include radiated power, radiated sensitivity, and 3D volumetric plots that show exactly how well the antenna performs across supported data rates and channels. Developers can use this data to optimize the device's Wi-Fi performance. Please review the link in the *Relevant Wi-Fi certification programs* section for more details regarding CWG-RF testing.

Wi-Fi and cellular coexistence

The wireless market is increasingly seeing converged wireless devices that incorporate both cellular and Wi-Fi functionality, and many wearable devices will likely utilize multiple wireless technologies (e.g. at the gateway device). For wearable devices or gateways that co-locate both Wi-Fi and cellular type communications, the need to test the wireless operation of the device in terms of supporting the localized coexistence of the radios is critical to meeting the end user experience needs. Wi-Fi Alliance has developed test requirements and certification processes for converged cellular and Wi-Fi devices with the aforementioned CWG-RF program.

Security

As the promise of the IoT continues to grow, bringing with it more devices with wireless connectivity, potential security vulnerabilities could surface if not properly mitigated in the design and implementation phase. During these phases, focused attention on authentication and encryption is critical. Fortunately, Wi-Fi includes strong measures to ensure a secure connection.

Privacy and security concerns are top-of-mind in the digital health ecosystem. Wi-Fi provides government-grade encryption capabilities with Wi-Fi Protected Access® 2 (WPA2™). In the home, WPA2-Personal is typically the highest level of security configured. The generally accepted best practice in the enterprise, such as in a hospital, is the use of

WPA2-Enterprise. Supporting WPA2 in a wearable device is the minimum recommended baseline and should be available in all chipsets. WPA2 is required of all Wi-Fi CERTIFIED devices, and obtaining WPA2 certification as guided in the certification section is highly recommended.

Device provisioning

The onboarding of a device onto a wireless network is a critical step in not only establishing a wireless connection but also in terms of authenticating both the user and network in order to establish a secure, encrypted connection. With today's sensitivities around cyber security, it is critical that the security protocols available for authentication and encryption are up-to-date and meet industry-agreed security requirements. Wi-Fi offers advanced, seamless, and secure mechanisms to meet these stringent security needs for onboarding the device types identified here. This section reviews the two main types of wireless wearables, and offers Wi-Fi capabilities that meet the onboarding requirements of these devices. This paper provides additional information regarding these capabilities in subsequent sections.

Wireless sensors and other types of wearables can come in many form factors, and the user interface is limited physically, ranging from an LCD type interface to a headless device that has no physical interface. The type of user interface will dictate the type of onboarding process available.

- **Device with a user interface:** A device that allows for user interaction can make security credentials (e.g. login and password) and other onboarding mechanisms available for entry on the device. For Wi-Fi devices, the use of Wi-Fi CERTIFIED Passpoint™ online sign-up provides the ability to provision a device with WPA2-Enterprise credentials, as well as the ability to access multiple networks with a single set of credentials. For example, the user could use the same credentials for home, hospital, and public hotspot access.
- **Device without a user interface:** A headless device either requires an external tool for configuration and management or comes pre-configured with no interaction necessary from the end user to enable or manage operation. A headless device often requires more effort from the developer or network administrator to automate onboarding as users will expect the device to "just connect" to the most appropriate network. A provisioning capability in-development for Wi-Fi will provide a secure and simple way to connect and configure devices that do not have a display or other input mechanisms. Multiple methods of provisioning are currently being explored, such as scanning a QR code, tapping a near field communications (NFC) tag, or leveraging an existing Bluetooth pairing.

System test

Typically, unit level testing during the development phase of a project requires the use of a wireless lab for testing that may require RF enclosures to isolate the device under test during radiated and conducted radio performance measurements. However, unit level testing does not include system level tests, which simulate a real world environment such as a hospital Wi-Fi enterprise deployment where hundreds or more APs are in operation. This environment can be drastically different from typical lab setups where testing is done in a more controlled manner. System testing allows product developers to identify the performance degradation issues they are likely to experience when they deploy their device within an actual hospital Wi-Fi network—issues they are unlikely to find through unit and integrated lab testing alone—and avoid the additional product development cycles necessary to resolve these issues. The two main reasons for this are:

1. The 802.11 access layer mechanisms (Carrier Sense Multiple Access (CSMA)) are intended to enable PHY-layer coexistence with many other devices. While these mechanisms are generally successful, they do require the cooperation of all devices in a shared RF space where congestion comes from not only RF interference but also the devices themselves.
2. The dynamic nature of the RF environment where signal strength can vary significantly, even for stationary devices, due to multipath and other factors. The advanced capabilities of Multiple Input Multiple Output (MIMO) and antenna diversity attempt to take advantage of these harsh RF environments, but how a client manages these operational characteristics still requires careful implementation at both the hardware design (e.g. antennas) and software (e.g. 802.11 driver).

It is highly recommended that product developers test their devices in real world trials, and end users and IT managers test devices on their networks as a pilot before live engagement with patients and clinicians.

Mobility considerations

Wireless wearable devices are inherently mobile and must operate in diverse RF environments. Device design considerations must take into account these varying environments to ensure that devices maintain reliable connectivity across the continuum of care. Wi-Fi Alliance is developing certification programs that will continue to improve the experience for users of Wi-Fi CERTIFIED™ devices that are streaming capable (e.g. streaming physiological parameters) and operate in mobile or managed environments. There are three main deployment models that should be taken into consideration: Personal WLAN, Enterprise WLAN, and Public hotspot.

Use cases and Wi-Fi environments

Each environment poses unique challenges in terms of RF, network access, and security measures. This section will explore each environment and define the unique characteristics and requirements.

Personal WLAN

A personal wireless LAN is a wireless network owned and managed by an individual for private use. Connecting wirelessly through an AP at home is a classic example of a personal WLAN. More recently, personal wireless networks have become mobile through the use of personal hotspots. For example, a user can link a PC or tablet using Wi-Fi to a cellular phone or a small cellular modem that bridges the connection onto the Internet.

The typical characteristics of a personal Wi-Fi network include:

- The network services a small coverage area typical of a home setting
- Anywhere from a few devices to 20 or more share the wireless network
- Coverage is typically mostly indoors
- One or more unmanaged APs provide connectivity
- One or two SSIDs typically serve all devices on the network
- Applications vary widely from users browsing through the Internet, to short communication bursts from environmental controls, to high-definition streaming of on-demand movies or video calls with friends and family
- Neighboring networks overlap and contend for access to the medium

Personal wireless LAN owners thus expect the following from their equipment to meet these demands:

- Wi-Fi networks should be easy to set up and use
- Securing the network is desirable but also needs to be a simple process
- The wireless network should be available across an entire dwelling
- Applications should perform as fast and seamlessly as possible
- All devices need to communicate with each other regardless of whether they are wired or wireless

To function well within a personal network and meet its demands, wearable devices need the following capabilities:

- Operate in both the 2.4 GHz and 5 GHz bands in order to support the broadest range of coverage, provide the greatest capacity, and avoid interference with neighbors

- Support 802.11ac at a minimum to perform at the best possible speeds available
- Provide an authenticated and encrypted connection through a pre-shared key (e.g. WPA2-Personal) in order to protect the device from malicious attacks and to secure its data transmissions
- Facilitate securing the wireless link with a minimal amount of effort from the end user
- Maximize a wearable's battery life when in use on the wireless network

Enterprise WLAN

An enterprise WLAN is a wireless network run by a business for the purposes of conducting daily operations. In the context of this paper, hospitals and clinics are the prominent examples of enterprise WLANs. The characteristics of an enterprise wireless network include:

- Actively managed by the enterprise
- Ubiquitous coverage throughout a facility
- Shared by many mobile users and systems
- Multiple applications running across the medium including voice, video, and business critical data
- Private and guest access

To support these characteristics, a medical facility's wireless infrastructure tends to have stricter controls but also richer features than a home or public Wi-Fi network. Enterprise WLAN configurations usually have:

- Multiple network segments (SSID and/or VLAN) to differentiate between applications and uses
- Strong authentication and encryption to secure access to the network
- Multi-band support for increased capacity and the broadest coverage of devices
- Quality of service (QoS) controls to ensure the best experience for each application
- Enhanced roaming parameters for fast, secure hand-offs between infrastructure APs as devices and users move throughout a facility
- Monitoring tools to assess, troubleshoot, and tune the wireless environment

To best function within an enterprise WLAN, wearable devices with embedded Wi-Fi or mobile end-points that bridge a wearable device onto a Wi-Fi network should support the following features:

- Multi-band operation in both the 2.4 GHz and 5 GHz bands for the broadest possible wireless coverage

- WPA2-Enterprise to provide strong user-based authentication for a wearable end-point, authorize it for use, and encrypt its communication to and from the network
- Wi-Fi Multimedia™ (WMM®) to enable QoS in order to enhance communication to and from a wearable device
- WMM-Admission Control so that a device may account for network load and RF conditions when participating on a Wi-Fi network
- WMM-Power Save to help conserve an end-point's battery life while connected to a Wi-Fi network
- Minimally 802.11n and optionally 802.11ac to promote the most efficient use of spectrum regardless of the bandwidth requirements of the device
- 802.11k neighbor reports to assist a wearable device in determining the best roaming options as it moves through a site
- 802.11r Fast Transition so that a wirelessly enabled wearable can swiftly and securely roam between APs without dropping traffic as it travels around a facility
- 802.11v BSS Transition management so that APs can steer clients to the best AP

Public hotspot

A public hotspot is physically located in neither the home nor the healthcare setting, but rather in-between the two. A public hotspot tends to have stronger built-in control mechanisms for supporting secure and seamless initial connectivity but does not have the complexity of an enterprise Wi-Fi network. Examples of public hotspots would be public venues, public transportation, stores, and coffee shops. The size of the WLAN can vary from small single-AP deployments to large venues (e.g. airport) that have many APs. In either case, the access capabilities are similar enough that we will combine them for the characteristics, configuration, and recommended capabilities. The characteristics of a public hotspot would be:

- Small to large coverage area served by one or many APs
- Owned by a business or service provider
- Not actively managed but serviced by a business owner or service provider
- Multiple connected devices operating varying applications (e.g. voice, video, gaming, file downloads)
- Many, especially smaller scale deployments, lack advanced enterprise capabilities such as:
    - Radio resource management capabilities
    - Strong security policies
    - Bandwidth allocation

To support these characteristics a public hotspot is usually configured with:

- Multiple security models:
    - Broadcast open network – no security on the SSID[2]
    - Broadcast open network with a captive portal
    - WPA2-Personal
    - WPA2-Enterprise, optionally with Passpoint
- Dual band (2.4 GHz & 5 GHz) operation

To best function within a public hotspot, wearable devices with embedded Wi-Fi should support the following features with minimal user interaction:

- Multi-band operation in both the 2.4 GHz and 5 GHz bands for the broadest possible wireless coverage
- WMM-Power Save to help conserve an end-point's battery life while connected to a Wi-Fi network
- Minimally 802.11n and preferably 802.11ac to promote the most efficient use of spectrum regardless of bandwidth requirements of a device
- Network access that provides a secure and robust connection
    - For devices with a user interface, preferably WPA2-Enterprise with Passpoint
    - Open access using a captive portal
    - Minimally use WPA2-Personal
    - Leverage Passpoint[3] for seamless network access and online sign-up
    - Support for a device provisioning capability when available

Relevant Wi-Fi CERTIFIED programs

A Wi-Fi CERTIFIED device offers a level of assurance that the device, regardless of the manufacturer, meets industry-agreed standards for interoperability, security, and a range of application specific protocols. Devices carrying the Wi-Fi CERTIFIED seal of approval deliver the best user experience. Certification programs are built around functionality that address unique business models or use cases. The following are some suggested certification programs that can address some of the challenges in developing and operating wireless wearable devices.

Connectivity (Wi-Fi CERTIFIED b/a/g/n/ac) and new frequency bands

Wi-Fi Alliance connectivity certification is the core of Wi-Fi Alliance. This certification offers baseline interoperability and backward compatibility for both client and AP devices. All

[2] When using Passpoint, this open configuration is sometimes deployed

device types, including devices in the wearables space, should have this certification as a baseline.

Wi-Fi access and authentication

Wi-Fi Protected Setup™: Wi-Fi Protected Setup is a technology designed to simplify the process of securing wireless networks at home or in small offices. Wi-Fi Protected Setup removes the complexity of understanding the various options to set up a WPA2-protected connection by replacing it with one of three simple actions: entering a PIN, pushing a button, or using NFC (i.e. bringing the device close enough to an AP in order to trigger the setup process). Devices with a user interface may choose to use Wi-Fi Protected Setup for their onboarding mechanism.

Wi-Fi CERTIFIED Passpoint: Passpoint allows a user or device easy and secure access to a Wi-Fi WLAN. Passpoint provides a solution to streamline network access in hotspots and eliminate the need for users to find and authenticate a network each time they connect. In Wi-Fi networks that do not support Passpoint, users typically search for and choose a network and in many cases must re-enter their authentication credentials. Passpoint automates that entire process, enabling a seamless connection between hotspot networks and mobile devices, all while delivering the highest WPA2 security. Passpoint enables a more cellular-like experience when connecting to managed Wi-Fi networks. Advanced devices with a user interface and operating on both Wi-Fi and carrier networks should consider this certification for their onboarding mechanism. Passpoint has important attributes for wireless wearable devices that provider a user interface, including seamless access using established credentials from a roaming hotspot partner, and automated provisioning credentials using Passpoint online sign-up.

Wi-Fi optimization

Wi-Fi Multimedia: WMM adds QoS to Wi-Fi networks. WMM classifies traffic into one of four priority categories: background, best effort, video, and voice. Data marked with a higher classification has a higher probability of delivery prior to traffic with a lower marking. By using WMM, administrators can tune their wireless network for the best possible user experience, especially when mixing sensitive traffic such as voice and video with other data types. Devices that may operate in an enterprise WLAN, such as a hospital, should consider the use of QoS and the WMM certification for optimal coexistence performance in a shared-spectrum WLAN.

WMM-Power Save: WMM-Power Save improves the battery life of mobile devices and increases the efficiency of transmission of real-time traffic over Wi-Fi networks. Most wireless wearable devices will have a low power requirement and should use WMM-Power Save.

Future Wi-Fi Alliance certification considerations

Application Services Platform (ASP 2.0)

Wi-Fi Alliance is exploring the potential requirements of a certification program extending the existing Wi-Fi Alliance Applications Services Platform (ASP) functionality used in Wi-Fi Direct® to perform Pre-Association Service Discovery of services available on Wi-Fi infrastructure networks using the IEEE 802.11aq (Pre-Association Discovery) amendment currently being developed within IEEE 802.11. This functionality would also serve as a mechanism for Wi-Fi wearable devices to assist in connection to the WLAN.

Device provisioning

A new method for device provisioning will enhance the user experience with a simple, secure, and consistent method for on- and off-boarding any type of device on a Wi-Fi network. The new mechanism will obtain a device's credentials in a secure manner and automatically provision it for use on a Wi-Fi network. In the case of wearables where no user interface may be available, having a seamless and secure method of establishing network connectivity without user interaction would be highly valuable.

Wi-Fi HaLow™: Wi-Fi HaLow extends Wi-Fi into the 900 MHz band, enabling the low-power connectivity necessary for applications including sensor and wearables. Wi-Fi HaLow's range is nearly twice that of today's Wi-Fi, and will be capable of not only transmitting signals further, but also providing a more robust connection in challenging environments where the ability to more easily penetrate walls or other barriers is an important consideration. Wi-Fi HaLow will include broadly-adopted Wi-Fi protocols and deliver many of the benefits that consumers have come to expect from Wi-Fi today, including multi-vendor interoperability, strong government-grade security, and easy setup.

Location

With the growing footprint of Wi-Fi CERTIFIED infrastructure available in enterprises and public environments, Wi-Fi Alliance members are developing a certification program addressing location. This technology and certification program will establish a common mechanism for determining location in the vicinity of Wi-Fi CERTIFIED APs, positioning Wi-

Fi-enabled location as the interoperable indoor location technology for users and healthcare administrators across products from a range of brands.

Mobile Multimedia

A Mobile Multimedia program will ensure that a device performs well for the types of multimedia data flows it supports. As an example, the certification will test devices providing interactive voice and video against latency, jitter, and throughput performance requirements under a variety of conditions.

Multiband Operation (MBO)

Wearable devices must operate seamlessly in the hospital and home, and in-between. To do this may require devices to transition from one wireless network to another. To address some of the challenges associated with transitioning between Wi-Fi and other networks, Wi-Fi Alliance is exploring technology and certification requirements to improve Wi-Fi network performance through the efficient use of available frequency bands, channels, and network infrastructure. Wi-Fi CERTIFIED infrastructure and client devices will exchange information to enable intelligent band selection decisions, including capability to steer clients to the cellular network when appropriate.

Multi-user (MU) MIMO

An update to Wi-Fi CERTIFIED™ ac will bring new features such as MU-MIMO to increase performance and network capacity, taking Wi-Fi beyond the gigabit Wi-Fi speeds already supported. This second wave of features will enable users to realize the full potential of Wi-Fi CERTIFIED ac and help meet the increase in capacity demands from IoH/IoT by supporting faster and more scalable operator networks.

Optimized Connectivity Experience (OCE)

For wearables to operate in fixed, mobile, and hotspot locations, network operators around the globe are deploying Wi-Fi as part of their managed network offering. Wi-Fi Alliance is working on delivering a better user experience in managed network environments that have a high-density of active or connected devices. Managed networks based on Wi-Fi CERTIFIED equipment will take advantage of systemic information to shorten connection setup, reduce airtime overhead, optimize transitions, and improve roaming performance.

Conclusion

The digital health ecosystem requires the use of robust, reliable, and secure wireless connectivity. Achieving this with an evolving wireless landscape and myriad use models is a challenging proposition for both the product developer and the end user. Wi-Fi devices can meet these requirements when properly designed and implemented. Following the guidance contained in this paper around system architectures, WLAN infrastructure design and deployment, as well as device-level feature support (e.g. device provisioning), appropriate Wi-Fi certifications, and radio/antenna integration, the digital health ecosystem can be fully realized from the hospital to home.

Consumers may be familiar with wireless issues exemplified by the "can you hear me now" campaign, but the age of digital health will bring a flood of IoH devices and an exponential increase in complexity to wireless ecosystems. For digital health to deliver the promise of lower cost, more convenience, and better care, wireless needs to "just work." Wi-Fi will bring that level of assurance.

References

1. Wi-Fi® in Healthcare: The solution for growing hospital communication needs (2011)
2. Wi-Fi® in Healthcare: Security Solutions for Hospital Wi-Fi Networks (2012)
3. Wi-Fi® in Healthcare: Improving the user experience for connected hospital applications and devices (2013)

These papers are available for download at: http://www.wi-fi.org/discover-wi-fi/healthcare.

About Wi-Fi Alliance

www.wi-fi.org

Wi-Fi Alliance® is a global non-profit industry association – our members are the worldwide network of companies that brings you Wi-Fi®. The members of our collaboration forum come from across the Wi-Fi ecosystem and share a common vision of connecting everyone and everything, everywhere. Since 2000, the Wi-Fi CERTIFIED™ seal of approval designates products with proven interoperability, industry-standard security protections, and the latest technology. Wi-Fi Alliance has certified more than 30,000 products, delivering the best user experience and encouraging the expanded use of Wi-Fi products and services in new and established markets. Today, billions of Wi-Fi products carry a significant portion of the world's data traffic in an ever-expanding variety of applications.

