The Wireless Protocols Tying Together the Internet of Things

With the number of devices for the connected home expected to skyrocket by the end of the decade, it's important to understand how all of these devices communicate with each other, both within the home and reaching out to the humans relying on them.

This is where wireless communication protocols come into play. In this whitepaper we take a look at the protocols available today and some of the characteristics of each.

Table of Contents:

Introduction

Right now, there are six primary wireless communication protocols for the connected home; sub-GHz, Wi-Fi, Bluetooth, zigbee, Z-Wave, and Thread. Each of these protocols has its place, and choosing the right mix for your designs is an important part of the development process, because no one protocol provides a universal one-size-fits-all solution. We examine the most commonly used wireless protocols and discuss which use cases are best for each one.

Sub-GHz Wireless

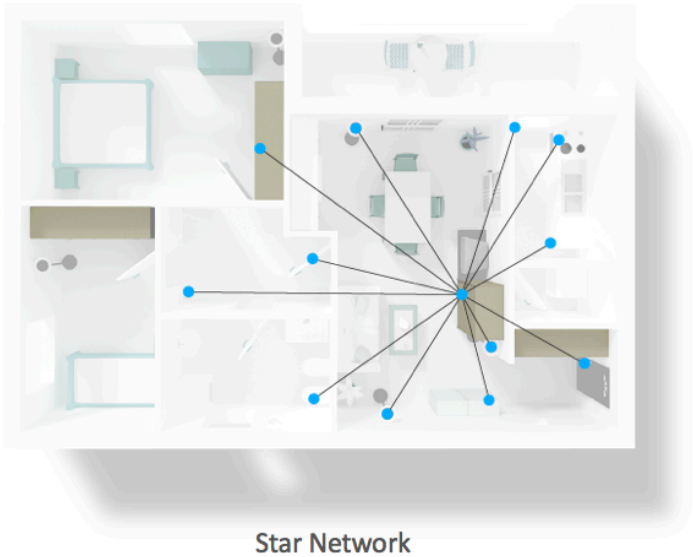
For low-data-rate applications like home security and automation, sub-GHz networks (operating at frequencies below 1 GHz) offer substantive benefits over the more powerful and feature-rich protocols such as Wi-Fi®, *Bluetooth*® and zigbee® operating in the 2.4 GHz band.

In star networks, traffic is directed through a centralized point, whereas a mesh network provides device-to-device connectivity.

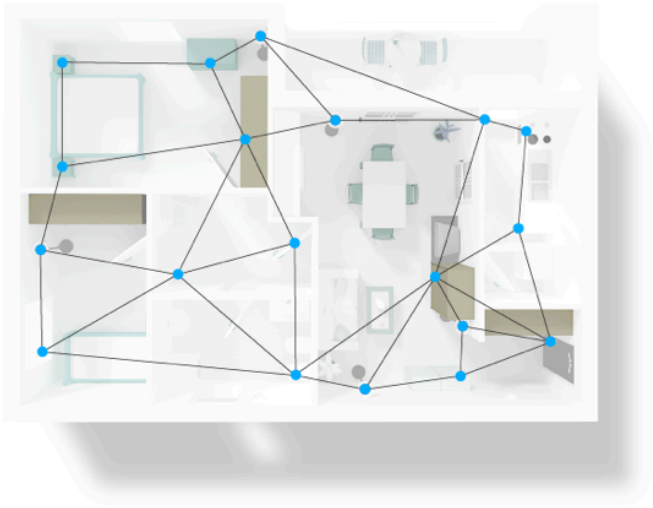
Range is one area where a sub-GHz network shines. Narrowband transmissions can operate uninterrupted for a kilometer or more. They transmit data to distant hubs without hopping from node to node. However, this longer range can also come with increased interference from adjacent devices. Lower interference can be a benefit, in regions where a wide range of sub-GHz frequencies, and these frequencies are less 'crowded' than the 2.4 GHz band. However, in some regions there are few available sub-GHz channels and they may have duty cycle restrictions limiting the time a device can be transmitting. Finally, sub-GHz wireless also uses very little power compared to 2.4 GHz protocols.

However, sub-GHz networks aren't a perfect fit for every aspect of the connected home. Many of the existing sub-GHz networks use proprietary protocols and are closed systems. Such systems often require application translation to communicate with other systems. Intra-home communication, and communication to a data services and controls that might reside in the cloud, can be more complex using sub-GHz wireless.

Note: Understanding the difference between 802.11 b/g/n-based devices and mesh networks is important when trying to get a feel for the wireless protocol landscape. The figure below shows a star network (typical of 802.11 deployments) versus a mesh network (typical of ZigBee and Thread). The first thing you're likely to notice is that in the star network, all traffic is directed through a centralized point, whereas a mesh network provides device-to-device connectivity.



Star Network



Mesh Network

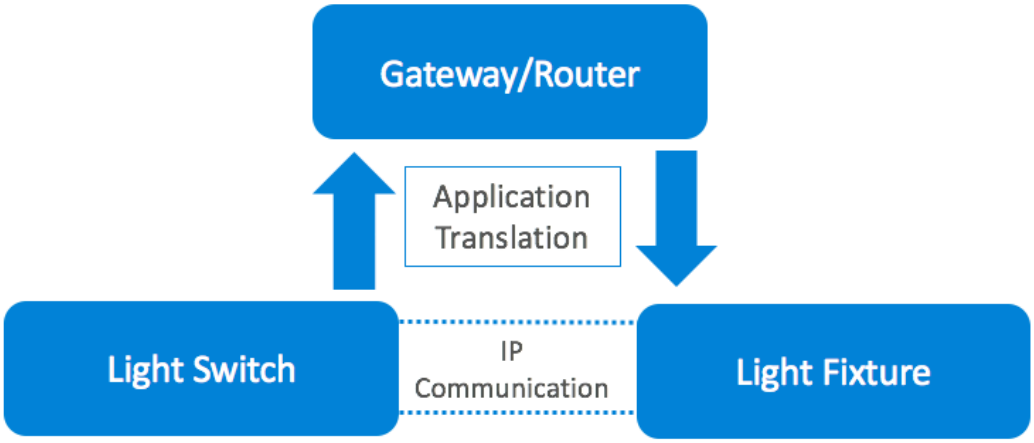
Wi-Fi (802.11)

Wi-Fi is the best known protocol by far, because most of us use it in our own homes every day, and have for more than a decade. This wide adoption has been fostered by the standards and upgrades The Institute of Electrical and Electronics Engineers (IEEE) provides through letter designations (g/n/ac), while the Wi-Fi Alliance manages certification and branding of devices.The chief advantage of Wi-Fi is its familiarity, the perception that it is “easy” compared to other protocols, and its ubiquity in existing homes. After all, the precursor to Wi-Fi was first developed in 1991. At this point most tech-savvy homeowners (the likely customer base for current connected home products) can reset a Wi-Fi router to troubleshoot basic issues. Wi-Fi defines a MAC layer protocol and security but it does not define application objects for devices and how they communicate.

This means each manufacturer can define their own application level protocol and device to device communication is complex or impossible unless two companies work closely together to define them. This limits Wi-Fi usage in the device to device market for the connected home. Wi-Fi also assumes a central access point model of a network which means if that access point is not operating the network stops functioning.Wi-Fi consumes a great deal of power relative to other protocols so while suitable for powered devices it does not do as well in applications where battery powered operation is critical.

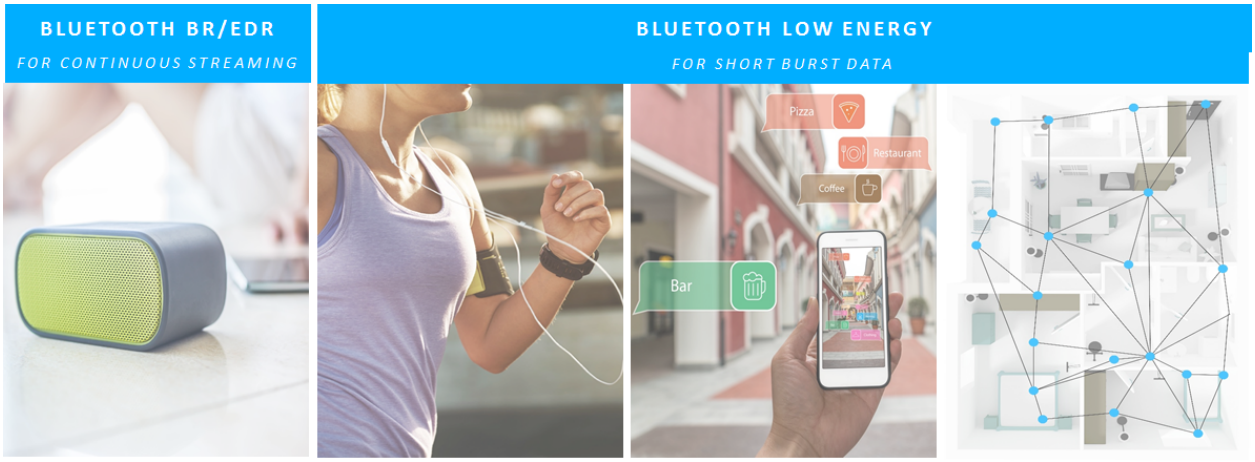
Wi-Fi has also shown issues around scalability. For example, some routers are configured to only support a maximum of 15 devices where the connected home is expected to have closer to 100 devices. Another issue is competition on the Wi-Fi network due to the variety of data sources. If you have streaming video competing with your thermostat, both data streams may not get the bandwidth they need. And if you thought having your streaming TV show competing with your kids’ videogame download was inconvenient, imagine having your thermostat trying to get in on the bandwidth, too.

Note: Reliance upon a single gateway to funnel traffic and translate among all the diverse devices on a network creates what’s known as a “single point of failure.” This means that if the gateway device becomes inoperable none of the devices on the network can communicate, causing the whole network to go down in turn. Single points of failure aren’t desirable in any context because of this increased vulnerability.



Bluetooth

Bluetooth is a wireless technology specification managed by the Bluetooth Special Interest Group (SIG). Designed for data transfer and exchange over short distances, Bluetooth makes use of the unlicensed ISM band at 2.4 GHz. Bluetooth includes a number of capabilities that span from point-to-point audio streaming to large-scale many-to-many (m:m) mesh networks.



Bluetooth BR/EDR

Bluetooth Basic Rate/Ehanced Data Rate (BR/EDR is a short-range communications protocol that is ubiquitous in smartphone applications. It doesn't require a special gateway to function because it already uses the smartphone or mobile device, but it does have some drawbacks. It only supports point-to-point networks, which limits range and reliability. If your smartphone is not within range of the end point, a connection for streaming cannot be established.

Bluetooth Low Engergy (LE)

The initial Bluetooth LE core specification was adopted in June 2010 and primarily focused on reduced power consumption. A standard for one-way communication was also introduced, which paved the way for Bluetooth beacons. The Bluetooth LE core specification has been updated a number of times by the Bluetooth SIG since 2010, with each release bringing functionality enhancements.

Bluetooth Beacons

A Bluetooth beacon is a small, battery-powered, wireless device that uses Bluetooth LE technology to advertise its presence and services. Beacons operate by repeatedly broadcasting or advertising a beacon identifier to compatible smartphones or tablets within its proximity. The smartphone or tablet can then use the beacon's information to determine its location and services, and act accordingly. Beacons are utilized for retail advertising, indoor positioning, and asset tracking applications.

Bluetooth 5

Bluetooth 5.0 was considered the most significant update to the Bluetooth specification since the introduction of Bluetooth low energy. The most notable features of Bluetooth 5 include twice the speed, four times range, and eight times the advertising capacity for long range, more robust connections, better user

experience, and smarter beacons. These enhancements focused on increasing the adoption of Bluetooth for the IoT.

Bluetooth Mesh

Bluetooth Mesh is a network topology available for Bluetooth LE devices that enables many-to-many (m:m) communications. It's optimized for creating large-scale node networks and is ideally suited for lighting, building automation, sensor networks, and asset tracking solutions. Key benefits of Bluetooth mesh networking include:

- **Extend the range -** of connections from gateways or mobile devices with multi-hop communication
- **Reduce power consumption -** in a system with shorter transmission distances between devices
- **Increase system scale -** by supporting 100's of devices in a single subnet
- **Improve system reliability -** with self-healing networks that overcome node failures
- **Deliver optimal responsiveness -** with device-to-device communication

zigbee

zigbee was first standardized in 2004, and features lower power consumption relative to Wi-Fi. It operates on the IEEE's 802.15.4 physical radio specification (as opposed to the more familiar 802.11 of Wi-Fi fame). zigbee is used heavily in home automation mesh networks currently, as well as in many industrial applications. zigbee has created a set of application protocols defining a wide range of devices and their communication patterns for device to device usage in home and businesses. These application protocols were developed within an Alliance of companies so there is a healthy ecosystem of products as well as competing silicon providers.

There are numerous advantages to the zigbee protocol, including its reliability, scalability and ability to self-heal its mesh network:

- **Reliability**: As we saw above and in the star versus mesh diagram in Figure 1, devices on a zigbee network can communicate with each other even if the gateway goes down or there is no gateway to begin with.
- **Scalability**: zigbee and other 802.15.4 protocols are not constrained by the number of devices they can have per router. You can add dozens, even hundreds, of devices without reaching an upper limit.
- **Self-Healing**: If the Personal Area Network (or PAN) coordinator for the mesh network is no longer available or is inoperable, the mesh seamlessly fails over and continues to function. Think of it like RAID for your computer—if one hard drive goes down, then the mirrored second hard drive takes over so that your work isn't interrupted. In the case of home automation, it means that your thermostat still works even if your gateway is down.

Right now, zigbee is contending with a compartmentalization of application standards and a perceived lack of easy interoperability, in addition to a need for direct IP addressability. zigbee devices require both address and application layer translation to communicate with devices on the internet, creating a potential failure point at the gateway.

Z-Wave

The Z-Wave protocol is primarily devoted to home control and monitoring, and is proprietary in nature. Home security companies use the Z-Wave wireless protocol to create networks of door/window sensors, fire detectors, thermostats and other home automation devices that are accessible through high-level applications or even over the Web. Z-Wave functions best in low-bandwidth, sub-GHz deployments.

Z-Wave has created an application protocol to standardize how devices communicate with each other to allow true device to device communication in the home. However, this standard is controlled by one company making growth and expansion difficult. The application layer protocol is not IP friendly and required translation into IP protocols for device to cloud or phone communications. Z-Wave is not an open standard and requires both address and

application translation to communicate with devices on the internet. Z-Wave requires a gateway to function creating a single point of failure in the networks. Additionally, the protocol assumes that devices are static, disallowing mobile devices (like remote controls) from joining the network.

Thread

Thread is an open standard that assigns an Internet Protocol (IP) address to every device on a network, and that IP address extends through the node. Thread provides device-to-device communication without the need for an application gateway. Remember the Side Notes above - eliminating the need for a gateway (or allowing for multiple gateways) also eliminates the single point of failure, which is highly desirable in a meshed network that needs to be always-on.Thread presents three major advantages:

- **Scalability**: The average connected home will host a hundred devices. If that sounds like a lot, just remember that every window and door will have a sensor, and every room will be monitored for temperature and humidity. At that rate, complexity and scale grows exponentially.
- **Interoperability**: With so many devices in play within a single mesh network, it's important that they all communicate with each other and with the home owner in an intelligent and effective manner.
- **Less expensive and simpler hardware**: It's not a new story that as a technology becomes more widely adopted the cost of devices tends to go down. (Look at what happened with flat-screen televisions over the last decade.) IP-based technology is well known and easy to implement.

Security and the Connected Home

Security is built into many of the existing mesh-network connected home protocols at a deep level in the software stack, for example, using AES encryption at the 802.15.4 MAC layer. Traffic is always encrypted, and with the addition of authentication technology, all nodes will have the capability to require authentication to communicate with each other and the network.Even devices using low level security in the software stacks are only as secure as the method used to install the keys in new devices. Weaknesses in this key installation or device bring up then require rekeying of the entire system.

IP Connectivity and the Connected Home

The existing protocols in the home are a mix of IP and not-IP stacks. Other markets and networks have converged onto IP because it offers a number of different addressing, routing and security mechanisms that can be selected for a given network or device and still allow end to end addressability and routing of messages without application layer translation.

The rapid expansion of the Internet into other industries and market segments is an indication of how this technology shift opens up innovation and rapid development of new services and devices over the appropriate IP infrastructure.The use of IP also allows a mix of underlying technologies with bridging devices between the different MAC/PHY so that an application running on your PC at home connected over Ethernet can also run wirelessly to your cell phone using Wi-Fi or a cellular connection. This type of seamless connectivity is important in many new application areas where consumers expect control while in their home but also from their phone when traveling.

The Connected Home is an area where large numbers of companies are innovating and creating new devices and services. Some of these services require high bandwidth and are more suitable for using Wi-Fi, while others are constrained battery operated sensors that would prefer using the 802.15.4 lower power radios and a ZigBee stack today, migrating to a Thread stack in the future.

Comparison of Wireless Protocols

Protocol	Supports 2.4 GHz	Standard Compliant Radio	IP-capable	Proprietary or Open Source	Suitable For	Not Suitable For
Sub-GHz	No	No	No	Proprietary	Narrowband transmitters Long-range	Mesh networking
Wi-Fi g/n/ac	Yes	Yes (802.11)	Yes	Open Source	High Bandwidth Home Internet networking (video cameras)	Networks with a large number of devices. Device to device communication without cloud or phone interaction
Bluetooth Mesh	Yes	Yes	No	Number of existing suppliers	Audio and voice streaming, device-to-device data transfer, beacons and advertising, and mesh device networks	Networks requiring IP capability
zigbee	Yes	Yes (802.15.4)	No	Number of existing suppliers	Mesh connected home networks with many devices. Device to device communication. Devices comunicating to a gateway. Critical devices that must have the ability to self-heal (medical/industrial applications)	Networks requiring IP capability
Z-Wave	Yes	No	No	Proprietary	Full Z-Wave ecosystems administered from central gateways	Networks requiring IP capabilities
Thread	Yes	Yes (802.15.4)	Yes	Number of suppliers of silicon and software	Complex mesh networks with a multitude of device that would benefit from individual IP addressability	Low-power, low-bandwidth devices

Conclusion

As the Internet of Things and the Connected Home continue to explode in popularity, it won't be uncommon to have several protocols running simultaneously in your home, just like you do in your smartphone. It isn't a case of one protocol "winning," but rather finding the right combinations of protocols to keep your IoT applications happily communicating with each other, the gateway, the cloud, and the consumer. What applications do you anticipate enabling your home? We may not be getting our flying cars anytime soon, but with the proliferation of devices and protocols available, we'll soon have connected homes that function seamlessly to make our environments more convenient, comfortable and energy-friendly.