Supplemental Reading for Mobile Device Networks

Wireless Network Protocols for IoT

In this reading, you will learn how Internet of Things (IoT) devices connect to wireless networks. As an IT Support specialist, you may need to support wireless IoT devices in a networked environment. For example, you may have a client who needs to install a smart, wireless security system for their home or office. The client might need assistance with connecting the security system to a private network for onsite monitoring and/or to the internet for remote monitoring. Understanding the properties of wireless IoT networks will help you select appropriate network protocols for various IoT applications.

IoT wireless network protocols at the physical layer

IoT devices can use both wired and wireless methods to connect to the Internet. For wireless connections, there are multiple network protocols that manufacturers configure IoT devices to use. Some of these network protocols support global internet connectivity, while others are intended for short-distance Personal Area Networks (PANs). Network protocols connect at the OSI physical layer.

Most IoT devices can use at least one of the following network protocols:

- **Wireless-Fidelity (Wi-Fi):** Wi-Fi is the more familiar brand name for the IEEE 802.11 standard for wireless networks. Wi-Fi is the most common wireless protocol across the world, with billions of devices capable of using Wi-Fi, including many IoT devices. Wi-Fi is a great option when needing to integrate IoT devices into an existing IP network that is connected to the internet. Wi-Fi 6 can support up to 500 Mbps data transfer speeds, for fast performance with large amounts of data. IoT networks often include a hub or a control system that uses Wi-Fi to facilitate wireless networking.

  As you have learned previously, Wi-Fi networks communicate on radio frequencies 2.4 GHz and 5 GHz. The 2.4 GHz frequency extends to 150 feet (45 meters) indoors and 300 feet (92 meters) outdoors. However, the 2.4 GHz frequency can experience congestion due to a limited number of channels. Plus, 2.4 GHz is more likely to experience interference from other nearby devices that use the same frequency, like microwaves. The 5 GHz frequency provides a stronger signal than 2.4 GHz and has more channels to handle more traffic. The 5 GHz drawback is that its range is limited to 50 feet (12 meters) indoors and 100 feet (30.6 meters) outdoors.
- **IEEE 802.15.4:** An inexpensive, low-power wireless access technology intended for IoT devices that operate on battery power. IEEE 802.15.4 uses the 2.4 GHz or lower radio band frequencies. IEEE 802.15.4 is normally used for low-rate wireless personal area networks (LR-WPANs) and uses a 128-bit encryption. Examples of IoT technologies that use IEEE 802.15.4 network connections include:
  - **ZigBee:** An LR-WPAN intended for smart home use. However, ZigBee has also been adopted globally for commercial IoT products. ZigBee includes a universal language that facilitates the interoperability of smart objects through a self-healing mesh network. ZigBee LR-WPAN networks can be accessed through Wi-Fi or Bluetooth.
- **Thread:** A low-latency wireless mesh networking protocol based on IPv6 addressing and existing open standards and technologies. These characteristics make thread networks compatible with a broad spectrum of IoT ecosystems. Thread devices do not use proprietary gateways or translators, making them inexpensive and easier to implement and maintain than other wireless technologies. Thread is used by the Google Nest Hub Max.
- **Z-Wave:** An interoperable, wireless mesh protocol (described below) that is based on low powered radio frequency (RF) communications. The Z-Wave protocol uses an RF signal on the 908.2MHz frequency band and extends 330 feet. Z-Wave allows users to control and monitor IoT smart devices. Z-Wave is inexpensive, reliable, and simple to use. The Z-wave protocol supports a closed network for security purposes. Over 3300 types and models of home and business IoT devices are certified to use Z-Wave technology, with more than 100 million devices in use worldwide.
- **Wireless mesh network (WMN):** Mesh networks are used by many popular wireless IoT network protocols, like Zigbee and Z-Wave, for device communication. Wireless mesh networks use less power than other wireless connectivity options. Wireless mesh is a decentralized network of connected wireless access points (WAP), also called nodes. Each WAP node forwards data to the next node in the network until the data reaches its destination. This network design is “self-healing,” meaning the network can recover on its own when a node fails. The other nodes will reroute data to exclude the failed node. Wireless mesh is a good option for high reliability and low power consumption, which is better for battery powered IoT devices. Wireless mesh networks can be configured to be full or partial mesh:
  - **Full mesh network:** Every node can communicate with all of the other nodes in the network.
  - **Partial mesh network:** Nodes can only communicate with nearby nodes.
- **Bluetooth:** Bluetooth is a widely used wireless network that operates at a 2.45 GHz frequency band and facilitates up to 3 Mbps connections among computing and IoT devices. Bluetooth has a range of up to 100 feet (30.6 meters) and can accommodate multiple paired connections. It is a good choice for creating a short distance wireless connection between Bluetooth enabled devices. Bluetooth is often used by computing devices to manage, configure, control, and/or collect small amounts of data from one or more close range IoT devices. For example, Bluetooth may be used to control smart home lighting or thermostat IoT devices from a smartphone.
- **Near-Field Communication (NFC):** NFC is a short-range, low data, wireless communication protocol that operates on the 13.56 MHz radio frequency. NFC technology requires a physical chip (or tag) to be embedded in the IoT device. NFC chips can be found in credit and debit cards, ID badges, passports, wallet apps on smartphones (like Google Pay), and more. A contactless NFC scanner, like a Point-of-Sale (PoS) device, is used to read the chip. This scanner communication connection often requires the IoT device to be within 2 inches (6 cm) of the scanner, but some NFC chips have an 8 inch (20 cm) range. This short-distance range helps to limit wireless network security threats. However, criminals can carry a portable NFC scanner into a crowded area to pick up NFC chip data from items like credit cards stored inside purses and wallets. To protect against this type of data theft, the cards should be placed inside special NFC/RFID sleeves that make the chips unreadable until they are removed from the sleeves. NFC technology may also be used in the pairing process for Bluetooth connections.
- **Long Range Wide Area Network (LoRaWan):** LoRaWan is an open source networking protocol designed to connect battery powered, wireless IoT devices to the Internet for widely dispersed networks.