Bluetooth

Related terms:

Wi-Fi, Bluetooth Device

View all Topics

Learn more about Bluetooth

Generic SoC Architecture Components

Sanjeeb Mishra, ... Vijayakrishnan Rousseau, in System on Chip Interfaces for Low Power Design, 2016

Bluetooth

Bluetooth is a short-range wireless communication technology standard. Bluetooth uses short-wavelength UHF radio waves of a frequency range between 2.4 and 2.485 GHz. Bluetooth enables one to create a personal area network wherein multiple devices talk to each other wirelessly via Bluetooth—a typical usage is home control automation systems. For example, the electronic devices in a home can be connected to a central control system via Bluetooth, and the central control system is controlled over the Internet. This usage scenario did not take off as anticipated; however, Bluetooth now is used to transfer data and control signal between two devices. These specific applications of Bluetooth are standardized as various profiles. There are many profiles defined, and two examples of these profiles are A2DP and hands-free profile (HFP). Advanced audio distribution profile (A2DP) is used for audio over Bluetooth, while HFP is used for hands-free operation of mobile phones. UART and USB are two of the leading interfaces for Bluetooth chips. UART is used when a Bluetooth chip is built into the system, such as in tablet devices. The USB interface is used when the Bluetooth module is connected as a separate dongle. We'll discuss the details in Chapter 6.

> Read full chapter

ZigBee Coexistence

Shahin Farahani, in ZigBee Wireless Networks and Transceivers, 2008

8.4 Coexistence with Bluetooth

Bluetooth systems operate in the 2.4 GHz ISM band and use the frequency hopping spread spectrum (FHSS) method instead of DSSS to spread their signals. Figure 8.3 shows the Bluetooth basic operation mechanism. The transmitted signal bandwidth is 1 MHz, but the frequency channel is changed using a pseudorandom sequence. The maximum number of hops in Bluetooth is 1600 hops per second in the connection state. There are 79 frequency channels in Bluetooth separated by 1 MHz:

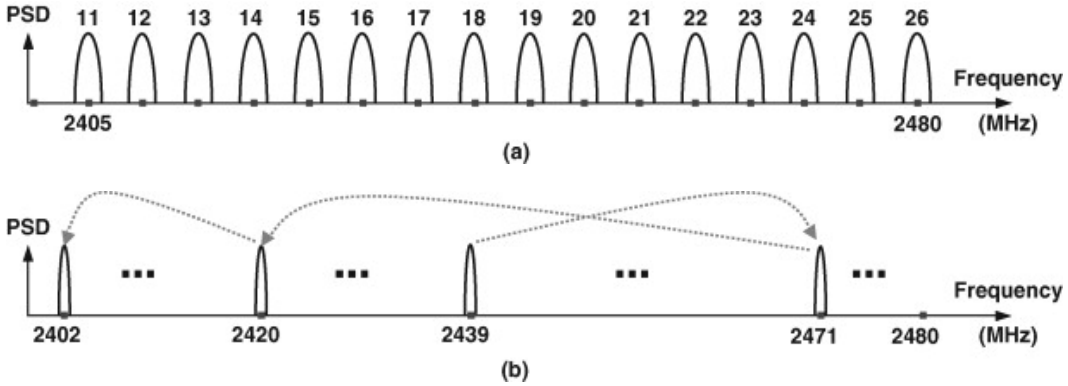

Figure 8.3. (a) IEEE 802.15.4 Channels and (b) Bluetooth Channels

(8.2)

where k is the channel number.

Bluetooth typical output power can be as high as 20 dBm. Bluetooth versions 1.1 and 1.2 were ratified as IEEE 802.15.1. But future versions of Bluetooth will not be ratified as any IEEE standard. The Bluetooth version 2.0 and higher can provide data rates of up to 3 Mbps. The device type in Bluetooth can be either master or slave. A master device can communicate with up to seven devices. The slaves periodically synchronize their clocks with the master.

FHSS, similarly to DSSS, provides processing gain, which improves the chance of successful packet delivery when interference is present. An IEEE 802.15.4 signal has 2 MHz bandwidth and may cause interference to three of the Bluetooth channels. Therefore, if the nearby Bluetooth device is using all 79 channels for frequency hopping, the maximum chance of interference between a single ZigBee node and a Bluetooth node is 3 out of 79 hops, which is approximately 4%.

However, a Bluetooth device can reduce the effect of presence of a ZigBee network (or any other network) by using adaptive frequency hopping (AFH). The AFH identi-

fies the channels where interferences are present and marks these channels as “bad channels.” Then the sequence of hops is modified such that the frequency channels with high-level interference are avoided. The bad channels in the frequency-hopping pattern are replaced with good channels via a lookup table. The Bluetooth master may periodically listen on a bad channel and if the interference has disappeared, the channel is marked as a good channel. Bluetooth slaves can also send a report regarding the channel quality to the master if necessary. The AFH method not only improves the performance of the Bluetooth network, it also reduces the effect of the Bluetooth network on other nearby networks that are not Bluetooth compliant.

The Bluetooth devices might not notice the presence of the ZigBee network due to the low duty cycle and low power of typical ZigBee nodes. If the frequency channel used by the ZigBee network is not marked as a bad channel, the Bluetooth network can cause interference to the ZigBee network, depending on the distance between the Bluetooth and ZigBee nodes.

> Read full chapter

New Technology

Matthew Neely, ... Chris Sanyk, in Wireless Reconnaissance in Penetration Testing, 2013

Bluetooth

Bluetooth is an extremely common technology, found in pretty much every cell-phone, most laptops, many desktop-class personal computers, and in ever-growing number of cars. Bluetooth uses frequency-hopping spread spectrum in the 2.4 GHz ISM band, the same band used by WiFi, microwave ovens, and most other 2.4 GHz consumer devices. Bluetooth devices form a piconet containing up to eight nodes—one master and seven slaves. Bluetooth is used for short-range communications between device peers, as well as device to peripheral. The number and variety of peripherals which communicate via Bluetooth is immense—wireless headsets for hands-free cell phone use, keyboards, mice, videogame controllers, audio speakers, you name it. Bluetooth is best known for transmitting audio, as in Bluetooth headsets. But it can also be used to connect HID devices such as keyboards and mice, and send data. Although not very popular, there are Bluetooth access points which function the same as WiFi access points to connect multiple devices to a network.

Attack tools against Bluetooth exist, such as Ubertooth (Figure 9.2), but still Bluetooth is not commonly targeted in penetration tests. Ubertooth is a custom made

radio dongle that can attack radio systems in the 2.4 GHz range. Originally it was created to attack only Bluetooth, hence the name, but has since been expanded. The project's home page is http://ubertooth.sourceforge.net/.

Figure 9.2. Ubertooth One Dongle. Reprinted with Permission from Meagan Call

Ubertooth can be used to monitor traffic, inject traffic, and do basic spectrum monitoring. It is very much a platform still in development, so new features are being added all the time. It is one of the cheaper, if not cheapest, ways to sniff Bluetooth, and the cheapest tool to inject custom packets. It has lowered the cost of entry to start attacking Bluetooth devices.

The key with Ubertooth is it is very difficult to take a consumer Bluetooth dongle and have it sniff and inject custom frames. With WiFi, this was very easy to do. Nearly any WiFi adaptor can be used to sniff traffic, and today most support injection as well. Once this was discovered, it became a lot cheaper to attack WiFi. To date, the only way we have seen to accomplish this on a Bluetooth dongle is to load a commercial firmware, which has probable EULA violation implications. Commercial tools to sniff a nd inject Bluetooth packets cost thousands of dollars. Ubertooth has lowered the cost for a device to attack Bluetooth to $120.

> Read full chapter

Mobile Malware Mitigation Measures

In Mobile Malware Attacks and Defense, 2009

Bluetooth

A Bluetooth firewall provides similar functionality for interactions over the Bluetooth interface. There have been various Bluetooth attacks demonstrated against common phones. While there is limited data measuring their frequency in the wild, there is at least some real exposure here today. In some cases, it's not viable to just turn off Bluetooth completely. Even making your phone "undiscoverable" isn't foolproof. A firewall or something similar that would be able to prevent unwanted connections and look for suspicious activity (like forged unpair requests) would be useful. Following the Bluetooth best practices will likely be sufficient for most people, but if you're extra-concerned, adding a little additional security wouldn't

hurt. Bluetooth security packages often add very little overhead since they only really operate when there is Bluetooth traffic.

> Read full chapter

Using the Palm OS for Bluetooth Applications

In Bluetooth Application Developer's Guide, 2002

The Future of Palm OS Bluetooth Support

Bluetooth is, of course, a very young technology, and will certainly see a fair amount of evolution over the next few years. Similarly, Palm OS's Bluetooth support will likely continue to evolve alongside the technology. In the near future, Bluetooth devices will address the issues of Layer 3 (Network level) support in the Bluetooth communication protocol stack. New specifications will define a network layer for communications between all the members of a piconet (not just master to slave), as well as inter-piconet communication issues. Roaming and scatternets will also be addressed. The eventual goal is the creation of true ad-hoc networks, self-configuring network groupings that grow and change as the user's environment changes. For Bluetooth technology to succeed in the long run, it will also need to address issues like discovery time (currently far too slow) and maximum throughput (to align with 3G technologies).

As much as possible, these changes will be integrated seamlessly into the Palm OS Bluetooth Library. New editions of the library will expand the Palm OS's Bluetooth capabilities, without compromising existing applications.

> Read full chapter

Linux Bluetooth Development

In Bluetooth Application Developer's Guide, 2002

Introduction

Bluetooth technology is an open standard while Linux is open source. There's some obvious synergy there: combine low cost devices with free software and you've got a communications technology anybody can afford.

Linux is proving to be the obvious system of choice for students and academics trying to get into Bluetooth technology on tight budgets. But don't think it's just for educational use: Linux is being deployed in real commercial products from local area network (LAN) access points to laptops, and more besides. To give it a real stamp of credibility, Linux Bluetooth development has backing from a Bluetooth Special Interest Group (SIG) promoter with IBM's BlueDrekar middleware, and, of course, a myriad of smaller companies and individuals are contributing to the development of open source, too.

This chapter takes a look at what Linux can do for your Bluetooth applications, and gives you some useful insight from inside the Linux developer's community.

> Read full chapter

Domain 4

Eric Conrad, ... Joshua Feldman, in Eleventh Hour CISSP® (Third Edition), 2017

Bluetooth

Bluetooth, described by IEEE standard 802.15, is a PAN wireless technology, operating in the same 2.4 GHz frequency as many types of 802.11 wireless devices. Small, low-power devices such as cell phones use Bluetooth to transmit data over short distances. Bluetooth versions 2.1 and older operate at 3 Mbps or less; Versions 3 and 4 offer far faster speeds.

Sensitive devices should disable automatic discovery by other Bluetooth devices. The “security” of discovery relies on the secrecy of the 48-bit MAC address of the Bluetooth adapter. Even when disabled, Bluetooth devices are easily discovered by guessing the MAC address. The first 24 bits are the OUI, which can be easy to guess, while the last 24 bits may be determined via brute-force attack.

> Read full chapter

System Security

Derrick Rountree, in Security for Microsoft Windows System Administrators, 2011

Bluetooth

Bluetooth uses radio waves to transmit data. Bluetooth is becoming ever more popular for communicating between devices. There are a large number of Bluetooth devices available today. There are Bluetooth-enabled computers, mice, keyboards, phones, and headsets. Bluetooth can provide a quick and easy method for sending short communications or transferring small amounts of data.

Bluejacking

Bluejacking is the practice of sending unsolicited messages to someone's Bluetooth connection on his or her phone, computer, and so on. Bluejacking is often used to send advertising messages out to people's phones.

Bluesnarfing

Bluesnarfing is hacking into someone's phone via the Bluetooth connection. You can use this connection to send e-mails and text messages or to view contacts and calendar information. Most of these require that the attacking device and hacked device be "paired." One way to combat Bluesnarfing is not to leave your device in "discoverable" mode. If your device is not in discoverable mode, it's harder for the attacking device to find it.

> Read full chapter

Layer 1: The Physical Layer

In Hack the Stack, 2006

Bluetooth

Bluetooth was developed as the standard for small, cheap, short–range wireless communication. It was envisioned to allow for the growth of wireless personal area networks (PANs), which allow a variety of personal and handheld electronic devices to communicate. Standard 802.15.1 is an Institute of Electrical & Electronics Engineers (IEEE) standard that deals with Bluetooth and PANs. Portions of the Bluetooth protocol suite reside at the physical layer of the OSI model, as seen in Figure 2.3.

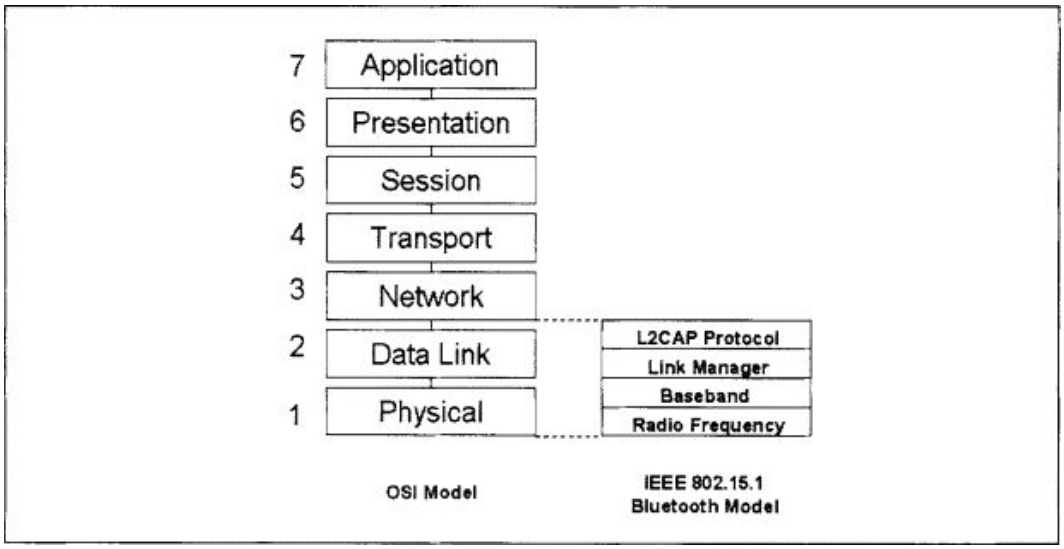

Figure 2.3. Relationship of Bluetooth to the OSI Model

There are three categories of Bluetooth devices:

- **Class 1** Allows for transmission of up to 100 meters and has lOOmW of power
- **Class 2** Allows for transmission of up to 20 meters and has 2.5 mW of power
- **Class 3** Allows for transmission of up to 10 meters and has lmW of power; also the widest deployment base

Bluetooth operates at a frequency of 2.45 GHz and divides the bandwidth into narrow channels to avoid interference with other devices utilizing the same frequency. To keep it secure, make sure Bluetooth–enabled devices are set to non–discoverable mode. Because Bluetooth can be monitored by third parties, use secure applications that limit the amount of cleartext transmissions. Practice a "deny all" methodology, meaning if you don't need Bluetooth functionality in a device, turn it off. This is important because Bluetooth–enabled devices can be configured to access shared directories without authentication, which would open it up to viruses, Trojans, and information theft.

Note

In 2005, AirDefense released BlueWatch, which was the first commercial security tool designed to monitor Bluetooth devices and identify insecure devices. More information can be found at www.airdefense.net/products/bluewatch/index.php.

> Read full chapter

Domain 4: Communication and Network Security (Designing and Protecting Network Security)

Eric Conrad, ... Joshua Feldman, in CISSP Study Guide (Third Edition), 2016

Bluetooth

Bluetooth, described by IEEE standard 802.15, is a Personal Area Network (PAN) wireless technology, operating in the same 2.4 GHz frequency as many types of 802.11 wireless devices. Bluetooth can be used by small low-power devices such as cell phones to transmit data over short distances. Bluetooth versions 2.1 and older operate at 3 Mbps or less; Versions 3 (announced in 2009) and higher offer far faster speeds.

Bluetooth has three classes of devices, summarized below. Although Bluetooth is designed for short-distance networking, it is worth noting that class 1 devices can transmit up to 100 meters.

- Class 3: under 10 meters
- Class 2: 10 meters
- Class 1: 100 meters

Bluetooth uses the 128-bit *E0* symmetric stream cipher. Cryptanalysis of E0 has proven it to be weak; practical attacks show the true strength to be 38 bits or less.

Sensitive devices should disable automatic discovery by other Bluetooth devices. The "security" of discovery relies on the secrecy of the 48-bit MAC address of the Bluetooth adapter. Even when disabled, Bluetooth devices may be discovered by guessing the MAC address. The first 24 bits are the OUI, which may be easily guessed; the last 24 bits may be determined via brute-force attack. For example, many Nokia phones use the OUI of 00:02:EE. If an attacker knows that a target device is a Nokia phone, the remaining challenge is guessing the last 24 bits of the MAC address.

> Read full chapter