# Study of Bluetooth protocol and applications

**Technical Report** · September 2021

DOI: 10.13140/RG.2.2.25521.71526



**1 author:**

Pooja Pandit

**28** PUBLICATIONS **0** CITATIONS

SEE PROFILE

# Study of Bluetooth protocol and applications

Pooja D. Pandit,
Mumbai University,
India

***Abstract*—Bluetooth is one of the popular technology standards for exchanging data over short distances. In this paper, a study of Bluetooth protocol and its applications is presented. We also thoroughly study prior art that enable advancements in Bluetooth technologies. Further, we also provide an overview of prior art in Wi-Fi which is one of the coexisting technologies with Bluetooth.**

## I. Introduction

Bluetooth is one of the key technologies that enables transmission of packets between two wireless enabled devices over a short distances. Bluetooth technology is popular for a number of applications such as streaming music, wireless mouse control, etc.

Due to its popularity and potential to create new applications in the future, it is important to understand the protocols involved in Bluetooth operation. Further, it is also important to understand the challenges involved in design of next generation Bluetooth technology.

In this paper, we first present an overview of Bluetooth related protocol and discuss its applications. Next we present an overview of prior art in Bluetooth as well as in Wi-Fi.

The organization of this paper is as follows. In Section II, we provide a discussion on Bluetooth Technology including the topologies and the Bluetooth architecture. Section III discusses the operation protocol of Bluetooth technology. Section IV provides a discussion on Bluetooth Enabling Technologies and Section V provides details of Wi-Fi Bluetooth Interference issues. We conclude in Section VI.

## II. Discussion on Bluetooth Technology

### A. Bluetooth History

Bluetooth is a wireless technology standard for exchanging data over short distances. This technology was created to solve a simple problem of replacing the cables used on mobile hand held devices with RF communication technologies. Consequently, one of the earliest applications of Bluetooth was in the context of mobile devices.

The technology encompasses a simple low-cost, low-power, global radio system for integration into mobile devices. Such devices can form a quick ad-hoc secure ”piconet” and communicate among the connected devices.

Bluetooth is a wireless technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on. A Bluetooth LAN is an adhoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet.

### B. Bluetooth Topology

Bluetooth defines two types of networks: Piconet and Scatternet. Details of these two types of networks are provided below.

*1) Piconets:* A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries. All the Secondary stations synchronize their clocks and hopping sequence with the primary. The communication between the primary and the secondary can be

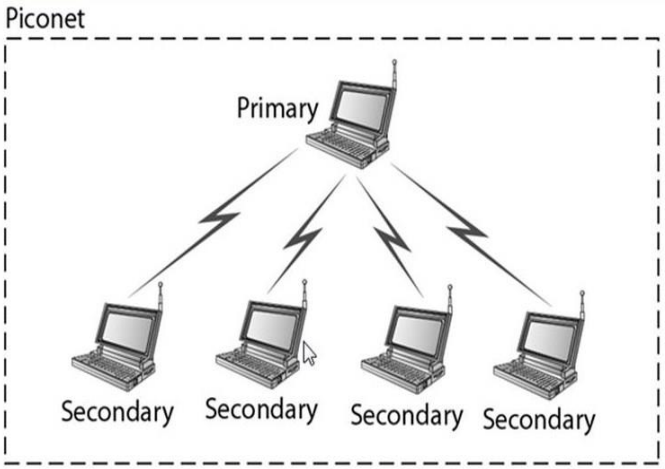


**Fig. 1:** An illustration to depict a Bluetooth Piconet

one-to-one or one-to-many. An illustration to depict a piconet is shown in Fig. 1.

Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the parked state. A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

*2) Scatternet:* Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets. An illustration to show a scatternet is depicted in Fig. 2.

### C. Bluetooth Node Architecture

A bluetooth node architecture is as shown in Fig. 3. An overview of each of the layers of the Bluetooth Architecture is as follows.

*1) Radio Layer:* The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.

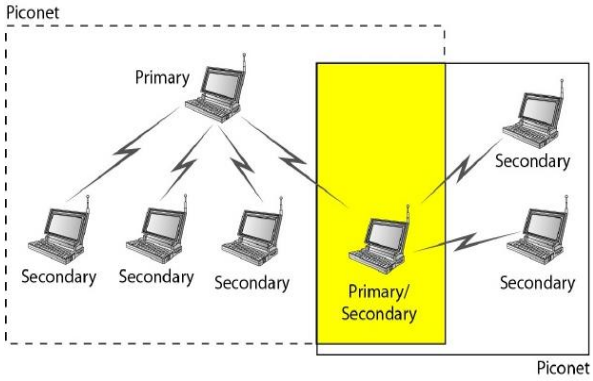


**Fig. 2:** An illustration to depict a Bluetooth Scatternet

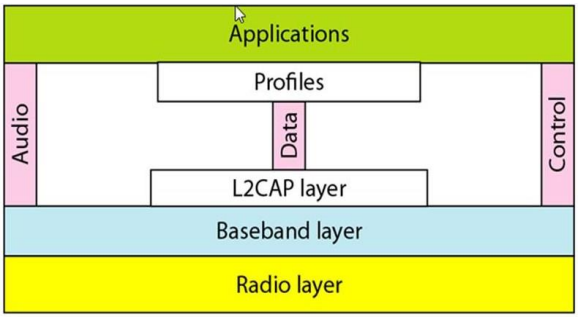


**Fig. 3:** Bluetooth Architecture

- Band: Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.
- FHSS: Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks. Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second. The dwell time is 625 microseconds.

*2) Baseband Layer:* The baseband layer is roughly equivalent to the MAC sub-layer in LANs. The access method is TDMA. The primary and secondary communicate with each other using time slots. The length of a time slot is exactly the same as the dwell time, 625 microseconds. Two types of links can be created between a primary and a secondary:

- SCQ Links: A synchronous connection-oriented (SQA) link is used when avoiding latency (delay in data delivery) is more

important than integrity (error-free delivery). In an SCQ link, a physical link is created between the primary and a secondary by reserving specific slots at regular intervals. The basic unit of connection is two slots, one for each direction. If a packet is damaged, it is never retransmitted.

- ACL Links: An asynchronous connectionless link (ACL) is used when data integrity is more important than avoiding latency. In this type of link, if a payload encapsulated in the frame is corrupted, it is retransmitted. A secondary returns an ACL frame in the available odd-numbered slot if and only if the previous slot has been addressed to it.

*3) L2CAP:* The Logical Link Control and Adaptation Protocol, or L2CAP is roughly equivalent to the LLC sub-layer in LANs. It is used for data exchange on an ACL link; SCQ channels do not use L2CAP.

*4) Other Upper Layers:* Bluetooth defines several protocols for the upper layers that use the services of L2CAP; these protocols are specific for each purpose.

## III. Bluetooth Operation

Bluetooth networking transmits data via low-power radio waves. It communicates on a frequency of 2.45 gigahertz (actually between 2.402 GHz and 2.480 GHz, to be exact). This frequency band has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM).

- Single-Secondary Communication: If the piconet has only one secondary, the TDMA operation is very simple. The time is divided into slots of 625 microseconds. The primary uses even-numbered slots (0, 2, 4, ...); the secondary uses odd-numbered slots (1, 3, 5, ...). In slot 0, the primary sends, and the secondary receives; in slot 1, the secondary sends, and the primary receives.
- Multiple-Secondary Communication: The process is a little more involved if there is more than one secondary in the piconet. Again, the primary uses the even-numbered slots, but a secondary sends in the next odd-numbered slot if the packet in the previous slot was addressed to it. All secondaries listen on even-numbered slots, but only one secondary sends in any odd-numbered slot.

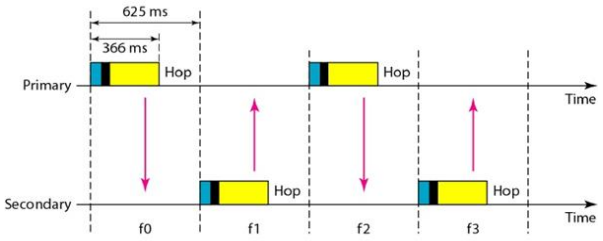


**Fig. 4:** Single Secondary Communication

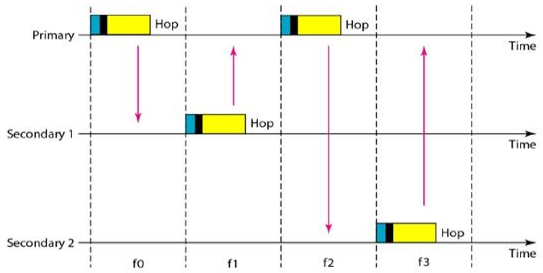


**Fig. 5:** Multiple Secondary Communication

## IV. Bluetooth Enabling Technologies

In this section, we present prior work related to Bluetooth. We focus on three key aspects which are Antenna Design, usage of Bluetooth in localization and Bluetooth Security.

### A. Antenna Design

Antenna design is one of the key aspects of a Bluetooth enabling hardware. As Bluetooth devices tend to have a size and cost constraint, design of a size and cost effective antenna structure is extremely for Bluetooth operation. To enable efficient Bluetooth communication, [1] presents a novel compact antenna design which leverages a two element design. A first element is used to generate on band of operation. Another element is placed compactly around the first element to generate a new

band of operation. The coupling creates a resonant frequency support that is suitable for Bluetooth applications. A similar approach is used in [2] and [3] to provide Bluetooth support. Other designs of antenna can also be potentially extended to support Bluetooth applications [4], [5].

### B. Positioning with Bluetooth

Bluetooth based positioning is one of the key applications of Bluetooth in recent times. Prior work has studied a number of approaches for achieving this goal. Some of the approaches involve leveraging existing positioning protocols for Bluetooth [6] or leveraging the RSSI together with the triangulation methods [7].

### C. Bluetooth Security

In order to become a key enabler of numerous applications, Bluetooth connection needs to be secure. Security of Bluetooth has been studied in a number of works such as [8], [9], etc.

## V. Co-existing technologies for Bluetooth

Wi-Fi is one of the main technologies that co-exist with Bluetooth. IEEE 802.11 networks operating in the sub-6GHz band and especially those operating in the 2.4GHz band tend to cause an interference to Bluetooth technologies. In the same way, an interference due to Bluetooth operation can also cause performance degradation for Wi-Fi. Wi-Fi works in a contention based manner to enable fairness amongst the contending nodes. Consequently, each node with a packet to send follows a backoff based contention procedure. Interference to Wi-Fi transmissions can cause a severe degradation in the user experience. Wi-Fi performance already has a lot of performance issues as shown in [10]–[13]. Consequently, additional degradation is undesirable.

The performance degradation of Wi-Fi can affect end user performance by lowering their achievable throughputs. To detect such performance issues, [14], [15] and [16] present two novel solutions. By leveraging the TCP handshakes, a passive estimation of the end-users TCP throughput can be made thereby enabling a remote reconfiguration of the network to reduce any potential interference due to co-existence issues.

## VI. Conclusion

In this paper, a study of Bluetooth Technology, its node architecture and protocols is presented. Further, some prior work on key Bluetooth enabling technologies has also been studied. Finally, we study Wi-Fi as a co-existing technology with Bluetooth.

## References


[1] P B Nayak et al. A novel compact tri-band antenna design for wimax, wlan and bluetooth applications. In *2014 Twentieth National Conference on Communications (NCC)*, pages 1–6. IEEE, 2014.

[2] P B Nayak et al. Compact dual-band antenna for wlan applications. In *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 1381–1385. IEEE, 2013.

[3] R Endluri et al. A low cost dual band antenna for bluetooth, 2.3 ghz wimax and 2.4/5.2/5.8 ghz wlan. *International Journal of Computer Applications*, 975:8887.

[4] P B Nayak et al. Ultrawideband (uwb) antenna design for cognitive radio. In *2012 5th International Conference on Computers and Devices for Communication (CODEC)*, pages 1–4. IEEE, 2012.

[5] P B Nayak et al. Multiband fractal antenna design for cognitive radio applications. In *2013 International Conference on Signal Processing and Communication (ICSC)*, pages 115–120. IEEE, 2013.

[6] Josef Hallberg, Marcus Nilsson, and Kare Synnes. Positioning with bluetooth. In *10th International Conference on Telecommunications, 2003. ICT 2003.*, volume 2, pages 954–958. IEEE, 2003.

[7] Yapeng Wang, Xu Yang, Yutian Zhao, Yue Liu, and Laurie Cuthbert. Bluetooth positioning using rssi and triangulation methods. In *2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, pages 837–842. IEEE, 2013.

[8] Markus Jakobsson and Susanne Wetzel. Security weaknesses in bluetooth. In *Cryptographers' Track at the RSA Conference*, pages 176–191. Springer, 2001.

[9] John Padgette, Karen Scarfone, and Lily Chen. Guide to bluetooth security. *NIST Special Publication*, 800(121):25, 2012.

[10] Shravan Rayanchu, Ashish Patro, and Suman Banerjee. Airshark: detecting non-wifi rf devices using commodity wifi hardware. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, pages 137–154, 2011.

[11] P Nayak et al. Multi-user downlink with single-user uplink can starve tcp. In *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*, pages 1–9. IEEE, 2017.

[12] P Nayak et al. Modeling multi-user wlans under closed-loop traffic. *IEEE/ACM Transactions on Networking*, 27(2):763–776, 2019.

[13] P Nayak. Performance evaluation of mu-mimo wlans under the impact of traffic dynamics. Master's thesis, 2016.

[14] P Nayak et al. uscope: a tool for network managers to validate delay-based slas. In *Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, pages 171–180, 2021.

[15] P Nayak. *AP-side WLAN Analytics*. PhD thesis, Rice University, 2019.

[16] P Nayak et al. Virtual speed test: an ap tool for passive analysis of wireless lans. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pages 2305–2313. IEEE, 2019.