



Advancements and Architectural Paradigms in Bluetooth Low Energy (BLE): A Comprehensive Analysis of Ultra-Low Power Wireless Communication

*Aswin T D^a, Prof. Riya K Prakash^b, Dr. L C Manikandan^c **

^aB.Tech Student, Department of CSE, Universal Engineering College, Thrissur, Kerala, India. E-mail: aswinachuz268@gmail.com

^bAssistant Professor, Department of CSE, Universal Engineering College, Thrissur, Kerala, India. E-mail: riyajothish13@gmail.com

^cProfessor, Department of CSE, Universal Engineering College, Thrissur, Kerala, India. E-mail: lcmanikandan@gmail.com

ABSTRACT :

The expansion of the Internet of Things (IoT) has reshaped wireless network requirements by prioritizing extreme power efficiency, scalable topologies, and dependable short-to-medium-range data links. Bluetooth Low Energy (BLE)—introduced in the Bluetooth 4.0 specification—has established itself as the standard solution for these demands. This paper analyzes the architectural foundations, physical-layer mechanisms, and protocol stack operations that define BLE. Particular attention is given to features introduced across the Bluetooth 5.0 through 5.4 specifications, including long-range transmission via Coded PHY, submeter indoor positioning through Angle of Arrival (AoA) and Angle of Departure (AoD), and low-latency streaming via LE Audio with the LC3 codec. Additionally, the introduction of Periodic Advertising with Responses (PAWR) in Bluetooth 5.4 resolves long-standing bidirectional bottleneck issues in large-scale star networks, enabling standardized deployments such as Electronic Shelf Labels (ESL) and ambient sensor systems. By examining the Generic Attribute Profile (GATT), cryptographic frameworks, and duty-cycled state machines, this report illustrates how BLE maintains reliable performance on microampere energy budgets and projects its development trajectory over the coming decade.

Keywords: Bluetooth Low Energy (BLE), Internet of Things (IoT), LE Audio, Direction Finding (AoA/AoD), Periodic Advertising with Responses (PAWR), Generic Attribute Profile (GATT), Ultra-Low Power Communication, Wireless Sensor Networks (WSN).

Introduction

Early Wireless Personal Area Networks (WPANs) relied heavily on Classic Bluetooth (Basic Rate/Enhanced Data Rate, or BR/EDR), which targeted high-throughput continuous streams like voice audio and file transfers. However, Classic Bluetooth proved poorly suited for battery-constrained sensor networks. Its synchronized link requirements forced radios to wake frequently, exhausting coin-cell batteries in days. Furthermore, establishing a connection in BR/EDR often took several seconds—a delay unacceptable for event-driven sensor nodes transmitting tiny packets [3].

To bridge this gap, Nokia initiated project "Wibree" in 2001. The goal was to build an asymmetric protocol allowing field sensors to run for years on a single CR2032 button cell by offloading processing to central hubs like smartphones. Wibree optimized energy usage by prioritizing ultra-short radio bursts, small payload sizes, and extended sleep periods. In 2006, Wibree was publicly introduced, leading the Bluetooth Special Interest Group (SIG) to integrate it into the core standard. It was formally adopted as Bluetooth Low Energy under the Bluetooth 4.0 specification in 2010 [8].

BLE filled a distinct niche: connecting embedded systems without the high power consumption of Wi-Fi or the complex network management of Zigbee. Existing alternatives either drained batteries quickly, required expensive silicon, or suffered from fragmented device support. BLE bypassed these adoption barriers by integrating directly into existing mobile phone chipsets, creating an immediate global gateway network. Modern BLE extends beyond simple sensor reading into mesh networks, synchronized audio streams, and precise spatial tracking—operating on the 2.4 GHz ISM band while retaining little architectural overlap with Classic Bluetooth [13], [15].

Architectural Framework of BLE

The BLE stack optimizes power efficiency and execution speed by dividing operations across three main layers: Controller, Host, and Application [1].

1.1. The Controller Layer

Implemented directly on the radio frequency (RF) integrated circuit, the Controller manages lower-level hardware tasks via the Physical Layer (PHY) and Link Layer (LL).

Physical Layer (PHY): Operating within the 2.4 GHz ISM spectrum (2402 MHz to 2480 MHz), BLE divides its bandwidth into 40 channels spaced 2 MHz apart. This design relaxes oscillator tolerances compared to Classic Bluetooth's 79 1-MHz channels, lowering silicon manufacturing costs and suppressing adjacent-channel interference. Channels 37, 38, and 39 serve as Primary Advertising Channels, positioned between standard Wi-Fi channels (1, 6, and 11) to avoid co-channel overlap. The remaining 37 channels handle active data transfers using Adaptive Frequency Hopping (AFH) to steer clear of congested frequencies [1].

Link Layer (LL): The LL runs the protocol state machine (Standby, Advertising, Scanning, Initiating, and Connection). It controls inter-frame spacing ($T_{IFS} = 150 \mu s$), manages packet construction, executes Cyclic Redundancy Checks (CRC), and processes hardware-accelerated AES-128 encryption [2].

1.2. The Host Layer

Positioned above the Controller and communicating through the Host Controller Interface (HCI), the Host handles upper-tier protocol processing:

- **Logical Link Control and Adaptation Protocol (L2CAP):** Serves as a multiplexer that breaks down upper-layer payload data into formats matching lower-layer limits, reassembling them at the destination node.
- **Security Manager (SM):** Controls pairing protocol exchanges and key generation. It executes cryptographic handshakes—such as Passkey Entry, Numeric Comparison, and Out-of-Band pairing—using Elliptic Curve Cryptography (ECC) to maintain confidentiality and node authenticity.
- **Attribute Protocol (ATT) & Generic Attribute Profile (GATT):** ATT defines low-level read/write commands for hardware attributes, while GATT organizes these attributes into structured Services and Characteristics [1].
- **Generic Access Profile (GAP):** Establishes operational roles (Broadcaster, Observer, Peripheral, Central) and manages discovery, connection setup, and advertising routines.

Recent Technological Breakthroughs: The BLE 5.x Specifications

The release of specifications 5.0 through 5.4 transformed BLE from a simple point-to-point link into a scalable network architecture.

1.3. Bluetooth 5.0: Speed, Range, and Extended Advertising

Bluetooth 5.0 introduced the 2M PHY, doubling the physical layer symbol rate to 2 Ms/s to shorten radio transmission windows and lower overall energy draw during bulk transfers. For long-range applications, it introduced the LE Coded PHY, which applies Forward Error Correction (FEC) at rates of S=2 or S=8. This coding allows receivers to decode signals below the noise floor, extending line-of-sight range beyond one kilometer without increasing transmission power. Additionally, Extended Advertising raised maximum payload limits from 31 bytes to 255 bytes, expanding connectionless broadcast capacity [5].

1.4. Bluetooth 5.1: Angle of Arrival and Angle of Departure Location Tracking

Replacing traditional Received Signal Strength Indication (RSSI) methods, Bluetooth 5.1 added directional spatial tracking using Constant Tone Extension (CTE) signals—unmodulated fields appended to standard packets. Multi-antenna arrays calculate spatial trajectories via microsecond phase shifts:

- **Angle of Arrival (AoA):** A multi-antenna receiver measures incoming signals from a single-antenna transmitter, making it ideal for tracking tags.
- **Angle of Departure (AoD):** A single-antenna receiver calculates its relative position from a multi-antenna beacon array, targeted at indoor navigation.

These mechanics enable submeter location accuracy [7].

1.5. Bluetooth 5.2: Isochronous Channels and LE Audio

Bluetooth 5.2 introduced Isochronous Channels, providing time-synchronized data delivery to multiple receivers. Paired with the Low Complexity Communications Codec (LC3), LE Audio delivers higher acoustic fidelity at half the bitrate of the older SBC codec. This foundation enables Auracast for unlimited public audio broadcasts while supporting independent left and right audio streams for wireless earbuds [4].

1.6. Bluetooth 5.3 and 5.4: Connection Subrating and PAwR

Bluetooth 5.3 added Connection Subrating, enabling devices to switch between low and high duty cycles without renegotiating the link connection state. Bluetooth 5.4 introduced Periodic Advertising with Responses (PAwR), establishing synchronized time slots for bidirectional communication between a central hub and thousands of peripheral nodes. This capability supports scalable systems such as Electronic Shelf Labels (ESL), allowing a single point to update and audit thousands of low-power digital displays [1], [10].

Data Representation: Deep Dive into GATT

Active connection state exchanges use the Generic Attribute Profile (GATT). Devices act as GATT Servers (hosting data) or GATT Clients (requesting data), independent of their GAP network roles [1]. Data is organized using three primary abstractions shown in Table 1.

Table 1 - GATT data abstractions

Construct	Description	Identifiers
Characteristic	The fundamental data unit, containing a single value, permission declarations (Read, Write, Notify, Indicate), and metadata descriptors.	16-bit or 128-bit UUIDs
Service	A logical grouping of related Characteristics that define a specific feature set (e.g., Health Thermometer).	SIG Standard (16-bit) or Custom Vendor (128-bit)
Profile	A high-level collection of predefined Services designed for specific device implementations.	Standardized by Bluetooth SIG

To lower power consumption, GATT emphasizes event-driven notifications. Rather than requiring clients to poll servers periodically, the client enables the Client Characteristic Configuration Descriptor (CCCD). The server then pushes state changes automatically via unacknowledged Notifications or acknowledged Indications, keeping radio activity to a minimum.

Cryptographic Security and Privacy Mechanisms

Security is managed through the Security Manager Protocol (SMP) [12] in three sequential phases:

- **Pairing Feature Exchange:** Devices negotiate their Input/Output capabilities (e.g., DisplayOnly, KeyboardOnly, NoInputNoOutput) to select an appropriate pairing protocol.
- **Key Generation (LE Secure Connections):** Elliptic Curve Diffie-Hellman (ECDH) key exchange derives a shared secret over an unencrypted channel. Depending on hardware capabilities, authentication uses Just Works (unauthenticated), Numeric Comparison (MITM protection via a 6-digit confirmation code), or Out-of-Band (data exchange via NFC).
- **Key Distribution:** Devices exchange long-term keys (LTK) to enable Link Layer AES-128 payload encryption.

To prevent physical location tracking, devices use Resolvable Private Addresses (RPAs). The device regularly rotates its public advertising MAC address (typically every 15 minutes). Only bonded devices holding the corresponding Identity Resolving Key (IRK) can resolve the randomized address to the true hardware identity.

Comparative Analysis: BLE vs. Alternative Topologies

Selecting a short-range wireless protocol involves trade-offs across throughput, power draw, and network structure:

- **BLE vs. Classic Bluetooth:** Classic Bluetooth maintains continuous synchronous links drawing 20–30 mA, making it suited for high-bandwidth streaming. BLE relies on brief micro-burst transmissions with long sleep cycles, maintaining average current draws in the low microampere range [9].
- **BLE vs. Wi-Fi (IEEE 802.11):** Wi-Fi offers high throughput (hundreds of Mbps) and direct IP routing, but its power demands (>100 mA) require frequent battery recharging or dedicated power sources. BLE sacrifices raw bandwidth for multi-year battery lifespans on standard coin cells [13].
- **BLE vs. Zigbee (IEEE 802.15.4):** Zigbee traditionally dominated low-power mesh applications using explicit routing paths. Bluetooth Mesh addresses this space using a managed flood network model that eliminates reliance on central routing nodes. A key operational advantage of BLE is native support across consumer smartphones, removing the need for proprietary hardware gateways [6], [14].

Conclusion

Bluetooth Low Energy has established itself across the short-range wireless domain by balancing strict energy budgets with adaptable protocol features. Its evolution from simple sensor monitoring in Bluetooth 4.0 to the complex architectures of Bluetooth 5.4 demonstrates continuous adjustment to growing IoT requirements. Coded PHY expands physical operational range, phase-based direction finding (AoA/AoD) provides high-accuracy indoor location tracking, and LE Audio replaces legacy Classic Bluetooth voice channels.

Over the next decade, innovations like Periodic Advertising with Responses (PAwR) will help support batteryless, energy-harvesting tags in large-scale retail and logistics networks. As edge computing expands, BLE stacks will increasingly incorporate dynamic channel mapping to limit interference within crowded 2.4 GHz spectrums. Standardized integration of IPv6 over BLE (6LoWPAN) will further unify local sensor networks with global IP infrastructure, maintaining BLE's role as a core physical layer for embedded wireless communication [1], [11].

REFERENCES

- [1] Bluetooth Special Interest Group, "Bluetooth Core Specification Version 5.4," Kirkland, WA, USA, Tech. Rep., Jan. 2023.
- [2] M. Spörk, C. Boano, and K. Römer, "Improving the Reliability of Bluetooth Low Energy Connections," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 605–616, Jan. 2020.
- [3] K. Townsend, C. Cufi, A. Davidson, and R. Davidson, *Getting Started with Bluetooth Low Energy: Tools and Techniques for Low-Power Networking*. Sebastopol, CA: O'Reilly Media, 2014.
- [4] J. Decuir, "Introducing Bluetooth LE Audio: The next generation of wireless audio," *IEEE Consumer Electronics Magazine*, vol. 10, no. 4, pp. 60–64, July 2021.
- [5] A. M. H. Abbas, M. S. A. Mutalib, and R. Hassan, "Performance evaluation of Bluetooth Low Energy (BLE) 5.0 coded PHY in long-range IoT networks," 2022 IEEE International Conference on Telecommunications and Photonics (ICTP), 2022.
- [6] S. M. Darroudi and C. Gomez, "Bluetooth Low Energy Mesh Networks: A Survey," *Sensors*, vol. 17, no. 7, p. 1467, 2017.
- [7] H. Zhai et al., "Centimeter-Level Indoor Localization using Bluetooth Low Energy 5.1 Angle-of-Arrival (AoA)," in *Proc. IEEE International Conference on Communications (ICC)*, 2021.
- [8] R. Heydon, *Bluetooth 1.2 to 5.2 and Beyond: The Inside Story*. Artech House, 2021.
- [9] T. Chang, et al., "Energy Consumption Models for Bluetooth Low Energy 5.0," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3855–3868, 2021.
- [10] Bluetooth SIG, "Electronic Shelf Label Profile (ESLP) Specification Version 1.0," Kirkland, WA, USA, 2023.
- [11] M. Collotta and G. Pau, "A novel energy management approach for smart homes using Bluetooth Low Energy," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 12, pp. 2788–2798, 2015.
- [12] J. Liu, C. Chen, and Y. Ma, "Security and Privacy Vulnerabilities in Bluetooth Low Energy: A Comprehensive Review," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2680–2712, 2020.
- [13] Nordic Semiconductor, "The ultimate guide to Bluetooth Low Energy (BLE)," Whitepaper, 2023.
- [14] M. Siekkinen, M. Hienkari, J. K. Nurminen, and J. Nieminen, "How low energy is bluetooth low energy? Comparative measurements with ZigBee/802.15.4," in *Proc. 2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2012, pp. 232–237.
- [15] C. Gomez, J. Oller, and J. Paradells, "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology," *Sensors*, vol. 12, no. 9, pp. 11734–11753, 2012.