Low-Latency Group Communication in BLE Networks via Whisper-Inspired L2CAP Relaying

Nikheel Vishwas Savant, Reality Labs, Meta

Abstract: Reliable and low-latency group communication remains a critical challenge in Bluetooth Low Energy (BLE) networks, especially in mobile and resource-constrained environments. Existing solutions such as GATT notifications and BLE Mesh suffer from limited scalability, high energy overhead, and congestion under load. This paper introduces a theoretical system architecture that leverages the Whisper Protocol—a lightweight, peer-assisted data dissemination strategy—adapted for BLE through the use of L2CAP Connection-Oriented Channels (CoC). The proposed design enables decentralized, flow-controlled broadcasting among bonded peer devices using randomized backoff, relay suppression, and credit-based transmission gating. Unlike BLE Mesh, this framework operates over secure ACL links, reducing message collisions and improving energy efficiency without requiring complex routing infrastructure. While the system is not experimentally implemented, we define detailed evaluation metrics—packet delivery ratio, end-to-end latency, credit exhaustion rate, and memory footprint—to guide future benchmarking. The architecture is particularly suitable for applications in wearable synchronization, industrial safety systems, and smart home automation. This work contributes a standards-compliant and deployment-oriented design for efficient peer-to-peer group messaging in embedded BLE systems.

***Index Terms*— Bluetooth Low Energy (BLE), L2CAP Connection-Oriented Channels (CoC), Whisper Protocol, peer-to-peer communication, wireless broadcasting, flow control, low-latency networking, embedded systems, group messaging, smart wearables, industrial IoT, energy-efficient networking.**

I. Introduction

Bluetooth Low Energy (BLE) has become a ubiquitous protocol for short-range wireless communication across wearables, smart home devices, and embedded systems [1]. Its energy-efficient design and growing support across consumer and industrial platforms make it a compelling choice for distributed, low-power communication. However, BLE's native support for group messaging remains limited. Traditional methods such as GATT notifications and advertisements are inherently unicast or connectionless and lack flow control or broadcast scalability [2], [3]. As a result, developers often resort to sequential updates across individual links, leading to increased latency, packet collisions, and wasted energy—especially in multi-device environments.

To address these limitations, the Bluetooth SIG introduced the Mesh Profile Specification, which enables many-to-many communication over advertisement channels [4]. While suitable for fixed, infrastructure-like deployments, BLE Mesh incurs significant overhead from managed flooding, mesh routing, and advertising congestion. It also lacks robustness in mobile or interference-prone environments, where frequent topology changes and noisy channels degrade performance [5], [6].

This paper presents an alternative design paradigm for BLE group communication: peer-assisted broadcasting using L2CAP Connection-Oriented Channels (CoC), inspired by the Whisper Protocol—a low-overhead, slot-coordinated flooding mechanism developed for wireless sensor networks [7]. Instead of relying on GATT or Mesh, the proposed system operates over secure ACL connections, leveraging CoC's flow-controlled, bidirectional communication capabilities. Each node forms L2CAP CoC links with a small subset of trusted peers and relays messages using randomized backoff, suppression of overheard transmissions, and credit-aware flow gating.

The primary goal is not to introduce a new routing layer but to repurpose existing BLE capabilities—bonded peer trust, credit-based flow control, and message caching—for efficient group data dissemination. Unlike BLE Mesh, which requires device provisioning and relies on broadcast advertisements, this architecture supports structured group communication with lower congestion and better compatibility for mobile, wearable, and resource-constrained platforms [8].

While the protocol has not yet been implemented, this paper offers a deployment-oriented architecture, complete with:

- System design and relay logic adapted for embedded BLE stacks,
- Energy-aware and congestion-aware optimizations,
- Use-case-driven application scenarios, and
- A rigorous set of simulation-based evaluation metrics.

The proposed architecture aligns with current BLE standards and is designed to be realizable using existing platforms such as Nordic nRF SDK, Zephyr RTOS, or Android's BLE APIs [9], [10]. Application domains include wearable device synchronization, industrial safety alerts, and smart home event propagation—where reliable and low-latency group communication is essential.

The remainder of this paper is organized as follows: Section II provides technical background on BLE L2CAP CoC, the Whisper Protocol, and peer-to-peer dissemination methods. Section III describes the proposed system architecture and broadcast workflow. Section IV introduces protocol-level optimizations. Section V defines key evaluation metrics. Section VI highlights real-world applications. Section VII discusses deployment challenges and open questions, followed by related work in Section VIII and concluding remarks in Section IX.

II. Background

This section introduces the key technologies that underpin the proposed peer-assisted broadcast framework: Bluetooth L2CAP Connection-Oriented Channels (CoC), the Whisper Protocol for low-power flooding, and prior work in peer-to-peer dissemination models. These components provide the basis for scalable and energy-aware group communication over BLE.

A. Bluetooth L2CAP Connection-Oriented Channels

The Logical Link Control and Adaptation Protocol (L2CAP) is a transport layer in the Bluetooth protocol stack responsible for multiplexing, segmentation and reassembly, and logical channel management. For Bluetooth Low Energy (BLE), the Bluetooth Core Specification defines two operating modes: the default LE L2CAP channel for Attribute Protocol (ATT) traffic, and the LE Credit-Based Flow Control Mode, introduced in Bluetooth 4.1 and enhanced in later versions [1].

L2CAP Connection-Oriented Channels (CoC) allow two BLE devices to establish logical data streams over Asynchronous Connection-Less (ACL) links. CoC provides several key advantages:

- Segmented data transfer with larger Maximum Transmission Units (MTUs)
- Bidirectional communication
- Flow control via a credit-based mechanism, which ensures receiver-side buffer safety and prevents channel congestion [2]

In conventional applications, L2CAP CoC is used for use cases such as audio streaming, file transfer, or OTA firmware updates [3], where higher throughput is required. However, it remains underutilized for group communication due to its point-to-point nature. This paper proposes repurposing CoC for multi-hop dissemination by leveraging existing ACL connections and applying peer-assisted relaying logic.

B. Whisper Protocol

The Whisper Protocol, first introduced for low-power wireless sensor networks (WSNs), is a fast-flooding mechanism designed to minimize latency and packet redundancy [4]. Unlike conventional probabilistic flooding, which leads to collisions and energy waste, Whisper uses precise time synchronization and coordinated slot-based transmission to achieve constructive interference.

In Whisper, only a subset of nodes relay a packet during each synchronized slot, using deterministic backoff and message suppression to reduce contention. The result is a flooding protocol with:

- Low end-to-end latency (e.g., <50 ms over 4 hops)
- High reliability with minimal retransmissions
- Minimal energy usage by suppressing redundant broadcasts

While Whisper was originally implemented on IEEE 802.15.4 radios and real-time OSes such as Contiki, its core principles—relay suppression, time-aware forwarding, and energy-aware broadcast minimization—can be adapted for asynchronous BLE systems using randomized backoff instead of slot synchronization [4], [5].

C. Peer-to-Peer Dissemination in Embedded Systems

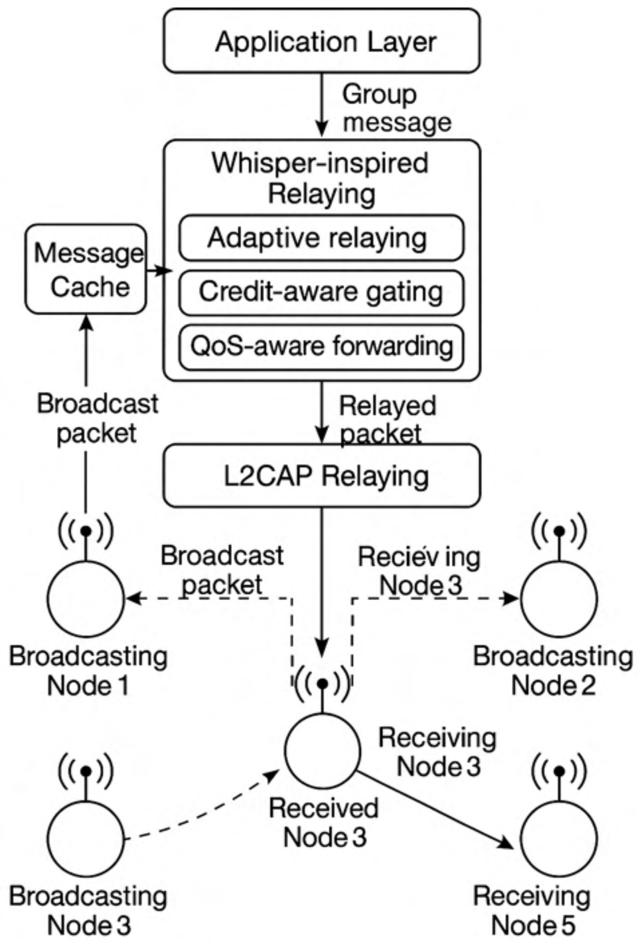
Peer-assisted broadcast techniques have long been used in distributed systems, including epidemic algorithms [6], gossip protocols [7], and collection tree routing [8]. These methods focus on decentralized message dissemination using:

- Hop-limited or TTL-constrained flooding
- Message caching and replay suppression
- Probabilistic relaying and redundancy reduction

In wireless embedded networks, protocols such as the Collection Tree Protocol (CTP) and Directed Diffusion introduced the idea of topology-aware flooding with local optimization [8], [9]. While these techniques are traditionally implemented at the network layer, the proposed system differs by implementing transport-layer dissemination using BLE L2CAP channels and bonding-based trust models.

This design avoids the need for a full-fledged routing protocol, instead relying on bonded peer clusters and low-level channel management. By integrating flow control (from L2CAP), suppression (from Whisper), and probabilistic relay control (from epidemic-style forwarding), the framework aims to deliver a scalable and implementation-ready solution for group messaging over BLE.

III. System design



This section presents the design of a peer-assisted broadcast framework that adapts the Whisper Protocol's low-redundancy flooding principles to the Bluetooth Low Energy (BLE) stack. The system uses L2CAP Connection-Oriented Channels (CoC) for structured, flow-controlled communication and enables scalable, low-latency group broadcasting through partial mesh topologies and probabilistic peer relaying.

A. Group Formation and Trust Establishment

The first step in the system is establishing a group of trusted peers capable of participating in secure and efficient data relaying. Trust is established via Bluetooth LE Secure Connections (LESC) pairing, which provides authenticated, encrypted links and protection against man-in-the-middle (MITM) attacks [1]. Only bonded peers are allowed to join the relay group, and device addresses are stored in a whitelist.

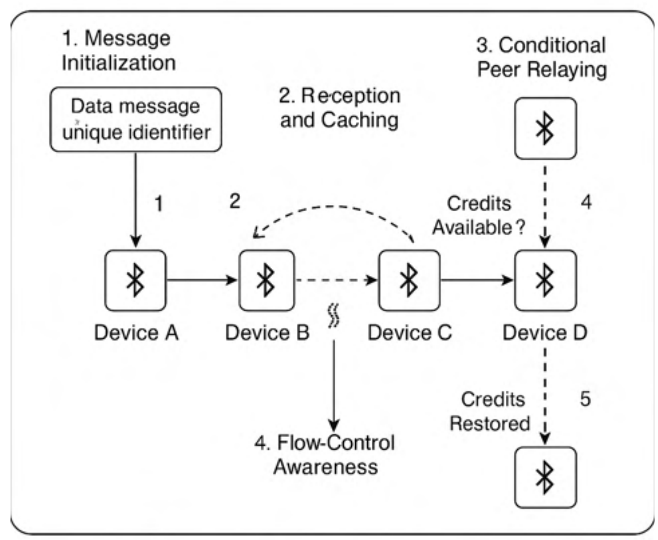
Each device maintains CoC connections with a small number of bonded neighbors (typically 2–4), forming a partial mesh or clustered ring topology. Full mesh formation is avoided to reduce traffic redundancy and channel congestion. Peer selection is informed by:

- Recent RSSI values
- Mobility history or proximity trends
- Hop distance balancing to reduce overlap

Initial configuration may be assisted by a central controller (e.g., a smartphone) during provisioning, but normal broadcast operation is decentralized. ACL links and CoC channels are maintained autonomously among the peers.

B. Whisper-Style Broadcast Workflow

The core innovation lies in adapting Whisper's deterministic flooding principles for the asynchronous, connection-oriented BLE environment. To accomplish this, each message follows a five-stage workflow:



1. Message Initialization

A source device (e.g., a smartwatch) generates a message payload, appends a UUID or hash-based identifier, and transmits it to all currently connected peers over CoC channels.

2. Reception and Caching

Receiving devices check the message ID against a replay cache of recently seen messages. If the message is new, the node caches it, sets a randomized delay timer (2–20 ms), and schedules it for potential rebroadcast.

3. Conditional Peer Relaying

During the delay window, if a device overhears the same message from another peer (via a local CoC buffer monitor), it suppresses its own transmission to avoid redundancy—mirroring Whisper's slot suppression logic [4], [5].

4. Flow-Control-Aware Transmission

Each CoC transmission is governed by the receiver's available credits. Credits are decremented per packet and restored upon acknowledgment. If insufficient credits are available, the node defers transmission using exponential backoff and queues the packet [2].

5. TTL and Expiry

Messages carry a Time-To-Live (TTL) value (e.g., hop count or max age of 300 ms). Once expired, they are discarded to limit flooding radius and preserve bandwidth.

This relaying model allows the system to emulate Whisper's low-collision, rapid flooding—without requiring precise slot synchronization or special PHY features—while leveraging BLE's native flow control mechanisms.

C. Implementation Considerations

The system is designed for integration with real BLE stacks used in embedded platforms such as Zephyr RTOS, Android, or Nordic SDK. Key considerations include:

1. L2CAP CoC Setup

CoC channels must be initialized post-pairing using standard BLE APIs such as bt_l2cap_connect() or BluetoothDevice.createL2capChannel() [9], [10].

2. Message Replay Cache

Each node maintains a FIFO replay cache (e.g., 64–128 entries) with time-based expiration to prevent re-broadcasting seen messages and limit memory usage.

3. Send Budget Management

Devices calculate a "send budget" based on battery level, connection reliability, and channel utilization, allowing energy-constrained nodes to reduce participation while maintaining message reception.

4. Fail-Safe Modes

In case of failed relays due to persistent credit exhaustion or dropped peers, nodes fall back to broadcasting over a GATT notification or initiating a temporary advertising burst.

IV. Protocol Optimizations

While the core design enables functional peer-assisted broadcasting over BLE L2CAP CoC, further optimizations are necessary to scale the system in real-world deployments. This section presents a set of protocol-level enhancements that improve reliability, reduce collisions, manage energy usage, and prioritize critical messages under constrained conditions.

A. Adaptive Rebroadcast Probability

In dense environments, naïve flooding can lead to excessive retransmissions and channel congestion. To address this, each node applies adaptive relay suppression based on local network conditions. Nodes estimate neighbor density using:

- Number of active CoC links
- RSSI variation from recent peers
- Historical relay success or collision detection rates

Nodes with high peer density (e.g., ≥4 neighbors) probabilistically reduce their rebroadcast rate to as low as 25%, while isolated or edge devices maintain near-100% relaying. This dynamic behavior mimics epidemic dissemination models used in distributed databases [6], [7], while leveraging BLE's low-level connectivity awareness.

B. Credit-Aware Congestion Throttling

L2CAP CoC enforces flow control using a credit-based mechanism that prevents sender overflow at the receiver buffer [2]. This system enhances that behavior by using credit availability not just for packet gating but as a signal for network-level congestion control.

When a node detects sustained credit exhaustion (e.g., over multiple message intervals), it:

- Drops or delays low-priority messages
- Applies exponential backoff for non-urgent packets
- Flags saturated peers to avoid redundant forwarding

This prevents "relay collapse" in constrained receivers and improves resilience in bursty or mobile traffic scenarios [5].

C. Energy-Aware Forwarding Policy

BLE devices often operate under strict energy budgets. To balance participation with power availability, nodes evaluate a local energy-aware relay policy, factoring:

- Remaining battery percentage
- Role (central vs. peripheral)
- User or application-specified QoS profiles

For example, a device below 10% battery may opt out of forwarding while still receiving broadcasts. Such behavior parallels routing-aware energy adaptation in wireless sensor networks (WSNs) [8], [9].

D. Priority Tagging and QoS Policies

Not all group messages carry equal urgency. To accommodate a range of scenarios—from firmware synchronization to emergency alerts—each message includes a Quality-of-Service (QoS) tag:

- 0 – Background Sync (non-urgent)
- 1 – Interactive Update (moderate latency)
- 2 – Critical Alert (latency-sensitive)

Nodes enforce differentiated forwarding policies:

- High-priority messages bypass randomized delay and are transmitted immediately
- CoC channels are preemptively cleared of lower-priority

packets
- Battery-aware nodes prioritize critical packets even if non-forwarding for others

This approach aligns with differentiated services frameworks used in network QoS scheduling [10].

E. Replay Suppression and Cache Management

To prevent uncontrolled flooding loops or replay attacks, each node maintains a fixed-size replay cache storing recently seen message IDs. A typical configuration may include:
- FIFO structure with 64–128 entries
- 5–10 second expiration window
- Message hash or UUID indexing

Messages are dropped if:
- The ID exists in cache
- TTL is exceeded
- Flow control remains inactive beyond a threshold (e.g., 1s)

This lightweight mechanism ensures flooding bounds remain controlled and avoids the complexity of network-layer routing tables.

V. Evaluation metrics

Although this work is theoretical and does not include hardware or software implementation, it proposes a complete set of evaluation metrics to guide future validation efforts. These metrics aim to assess scalability, reliability, energy efficiency, and resource consumption—all critical factors for BLE-based embedded systems operating under real-world constraints.

The following key performance indicators (KPIs) are recommended for emulation, simulation (e.g., with ns-3), or prototype-based measurement using platforms like Zephyr RTOS or Nordic SDK.

A. Packet Delivery Ratio (PDR)

1. Definition: The percentage of participating group members that successfully receive a broadcasted message within its TTL window.

2. Significance: PDR is a fundamental indicator of reliability in any flooding or peer-assisted broadcast protocol. It reflects message reachability in the presence of mobility, interference, and congestion.

3. Test Conditions:
- Varying network sizes (e.g., 5 to 50 nodes)
- Presence of channel interference (simulated or real)
- Dynamic peer churn (e.g., 10–30% nodes joining/leaving)

4. Target Outcome: >95% PDR in static or lightly mobile topologies, consistent with prior BLE Mesh benchmarks [5], [6].

B. End-to-End Latency

1. Definition: The time elapsed from the message transmission at the source device to successful reception at the final peer node.

2. Significance: Latency is especially critical in emergency scenarios (e.g., industrial safety alerts or fall detection) where rapid group notification is required.

3. Evaluation Factors:
- Message QoS levels (0–2)
- Adaptive vs. fixed backoff configurations
- Different CoC MTU settings and credit grants

4. Target Outcome: <300 ms latency over 3–4 hops for high-priority messages, similar to optimized BLE Mesh latency under low congestion [6].

C. Channel Congestion Indicators

1. Definition: Indicators of buffer saturation and flow control inefficiency, including:
- CoC credit exhaustion frequency
- Number of deferred or dropped packets
- CoC channel queue length over time

2. Significance: Helps assess how the system reacts under load and how quickly it recovers from temporary congestion.

3. Expected Observations:
- Congestion should correlate with peer density and message frequency
- Adaptive suppression and backoff should smooth out spikes in usage

D. Energy Consumption

1. Definition: The energy cost per message received and relayed, measured in mJ or normalized to battery percentage over time.

2. Significance: In embedded or wearable systems, energy consumption determines deployment viability, especially for battery-powered peripherals.

3. Measurement Method:

- Compare relaying vs. non-relaying nodes
- Simulate different message frequencies (e.g., 1 Hz, 5 Hz)
- Include idle, active, and transmission states in total energy profile

4. Target Savings: ≥40% reduction in forwarding energy vs. uncontrolled flooding, aligned with prior WSN flooding energy benchmarks [4], [8].

E. Scalability and Network Resilience

1. Definition: The protocol's ability to maintain reliability and latency as network size increases or topology changes.

2. Measurement Dimensions:

- Max nodes supported before PDR drops below 90%
- Performance degradation under 20–50% node mobility
- Recovery behavior under temporary partitioning

3. Tools: ns-3, Zephyr test harnesses, or testbed emulators (e.g., Nordic nRF5340 DK cluster)

F. Memory and Processing Overhead

1. Definition: RAM and flash usage for maintaining replay caches, CoC connection states, and per-peer relay queues.

2. Significance: Embedded systems often have limited resources (e.g., 64–128 KB RAM), so memory usage must be predictable and bounded.

3. Measurement Targets:

- <8 KB RAM usage for replay cache and forwarding logic
- Optional compile-time configuration to reduce memory footprint

4. Target Platforms: ARM Cortex-M4/M33-based BLE SoCs (e.g., nRF52840, STM32WB, Dialog DA14531)

VI. Applications

The proposed broadcast architecture offers a robust and energy-efficient mechanism for real-time group communication over BLE, particularly well-suited to embedded, battery-operated, and mobile environments. This section presents several application domains where the protocol's low latency, peer-assisted relaying, and secure group bonding can deliver significant performance advantages over traditional BLE Mesh or GATT-based systems.

A. Wearable Synchronization and Multi-Device Coordination

In ecosystems involving smartwatches, fitness trackers, smartglasses, and other wearable devices, synchronized events—such as alerts, posture reminders, or shared audio cues—must often be propagated across devices within tight latency and energy budgets. Conventional BLE approaches require sequential GATT notifications from a smartphone or hub, incurring cumulative delays and excessive transmission energy.

With Whisper-style CoC broadcasting:

- A smartwatch can notify multiple co-worn devices (e.g., glasses, rings) simultaneously.
- Peer devices can compensate for temporary hub unavailability by relaying messages locally.
- Credit-based CoC communication avoids write congestion and improves battery performance.

This model supports emerging distributed user experiences, such as ambient context sharing and coordinated feedback loops in Google and Apple wearable ecosystems [1], [9].

B. Smart Home Event Propagation

Smart home networks increasingly rely on BLE-capable devices for automation triggers, security alerts, and inter-device coordination. BLE Mesh provides one option but suffers from advertising congestion and complexity in dynamic environments such as apartments or mobile home devices.

The proposed system offers:

- Fast propagation of events like door unlocks, motion detection, or alarm triggers across a trusted peer set (e.g., bulbs, locks, speakers).
- Lower packet loss due to connection-oriented CoC relays.
- Group-wide acknowledgments and state syncing via bonded trust.

Example: A BLE door sensor broadcasts an "open" alert to a set of bonded nodes (e.g., interior camera, lights, security panel) that respond in under 200 ms.

C. Industrial Safety and Condition Monitoring

In industrial and factory settings, BLE-equipped worker vests, helmets, and sensors may need to receive high-priority alerts—such as gas leak warnings or proximity alarms.

Whispered CoC broadcasting ensures:

- Resilient propagation under RF interference from heavy machinery or metal walls.
- Multi-hop delivery even if some workers move out of range from the source.
- Prioritization of critical alerts over periodic telemetry.

Integration into existing safety systems allows for low-infrastructure safety compliance, improving both worker protection and regulatory reporting.

D. Healthcare Monitoring and Triage Alerting

BLE-enabled health sensors—such as pulse oximeters, fall detectors, and location tags—are increasingly used in hospitals and eldercare environments. These devices must often share critical events across a cluster of local responders (e.g., nurse stations, wearables).

The protocol supports:

- Ultra-low-latency fall alerts or vitals anomalies broadcasted to multiple caregivers.
- Secure group bonding ensuring only authenticated devices receive medical events.
- Operation without dependency on cloud or Wi-Fi infrastructure.

This allows localized alert propagation in triage zones, rural clinics, or temporary care units—bridging infrastructure gaps while ensuring patient safety [10].

E. Classroom and Education Synchronization

BLE networks in education environments power use cases such as quiz delivery, AR-based exploration, and real-time activity synchronization across student devices.

Example scenarios include:

- Teacher broadcasts "start test" command to tablets and clickers.
- AR headset content updates propagated via peer devices when the central router is overloaded.
- Low-QoS messages like classroom presence beacons are deprioritized during live exams.

Whisper-style relaying ensures fairness, latency compliance, and infrastructure resilience in classrooms with limited Wi-Fi or constrained AP bandwidth.

VII. Challenges and Open Questions

While the proposed architecture provides a compelling blueprint for peer-assisted group broadcasting over BLE, several technical and operational challenges must be addressed for robust deployment. This section outlines the key open issues that warrant further research, prototyping, and refinement.

A. Topology Volatility and Peer Mobility

In wearable and mobile IoT environments, network topology is inherently dynamic. Devices frequently move in and out of range, causing:

- Peer link breakage and reformation
- Asymmetric CoC availability
- Temporary isolation of nodes

These disruptions can impair message propagation reliability and increase overhead from frequent CoC teardown and setup. Potential mitigations include:

- Opportunistic re-pairing with nearby bonded devices
- Heartbeat-based link status tracking
- Proximity-based rebonding using RSSI and motion sensors [3], [5]

A hybrid design with fallback to advertisement-based alerts may also improve resilience under high churn.

B. Group Membership and Trust Management

The framework assumes that all participating devices are pre-bonded using Bluetooth LE Secure Connections (LESC). However, managing large or dynamic groups (e.g., factory workers or hospital staff) introduces complexity:

- How are credentials issued, rotated, or revoked?
- Can devices delegate bonding (e.g., bootstrap new members)?
- What governance exists for temporary device access?

Solutions may draw from Matter, FIDO Device Onboarding (FDO), or decentralized trust delegation schemes [11], [12]. Future work should explore scalable bonding orchestration with limited overhead and strong authentication.

C. Data Integrity and Message Authentication

Whisper-style broadcasting assumes cooperative behavior among relaying nodes. However, without lightweight cryptographic checks, a malicious or compromised device could:

- Inject fake messages (e.g., false alerts)
- Replay stale packets to manipulate system state
- Exfiltrate relayed payloads

Suggested countermeasures include:

- Per-packet HMACs using a shared session key
- Timestamp-based UUIDs to prevent replay
- Optional ECDSA signatures or pre-shared public keys for authenticated relays [10]

A tradeoff must be evaluated between cryptographic robustness and the computational overhead on constrained embedded devices.

D. Congestion and Broadcast Storm Mitigation

Although flow control at the L2CAP level prevents buffer overflows, coordinated broadcast storms may still occur when:

- Multiple sources simultaneously trigger messages
- Backoff timers expire in close succession
- Receiver queues are saturated

To mitigate this:

- Time-slot-based relaying may be used in dense networks
- Flood window coordination (token passing or delay staggering) can help isolate critical traffic
- Future revisions could integrate TSCH-style time coordination or GATT-initiated sync anchors [8], [13]

E. Memory and Resource Constraints

Most BLE SoCs offer between 64–256 KB flash and 16–64 KB RAM. Supporting:

- Replay cache (64–128 UUIDs)
- Per-peer relay queues

- CoC connection management
- QoS prioritization logic

…may stress available memory, especially in real-time OS environments.

Strategies to address this include:

- Static memory provisioning using compile-time flags
- Relay mode configuration (listener-only vs. relay-capable)
- Hybrid fallback to GATT or Mesh for memory-constrained peripherals

F. Prioritization and Message Scheduling

The current design supports simple QoS tiers but lacks formal scheduling models for overlapping floods. Open questions include:

- Should high-priority messages preempt lower-priority packets in CoC queues?
- How are multi-source broadcasts coordinated to avoid cross-flood contention?
- Can differentiated traffic classes (like IEEE 802.1Q or DSCP) be adapted for BLE relaying?

Answering these questions will require both simulation and empirical testing on heterogeneous device clusters.

VIII. RELATED WORK

This section reviews foundational technologies and recent research that relate to peer-assisted communication in BLE networks and low-power wireless systems. The proposed design is positioned as a synthesis of these efforts—retaining compatibility with BLE standards while addressing limitations in scalability, reliability, and energy efficiency.

A. BLE Mesh Networking

The Bluetooth Mesh Profile [4] enables many-to-many communication over BLE by using managed flooding on the advertising channels. It supports publish-subscribe models, friend nodes for power optimization, and message relaying across intermediate devices.

However, BLE Mesh has several drawbacks:

- Relies on non-connectable advertisements, which are susceptible to collisions and interference.
- Uses multi-layer packet headers and fragmentation/reassembly, increasing complexity and overhead.
- Not optimized for mobile or resource-constrained devices, particularly wearables or intermittently connected peripherals [5].

Studies such as [6] show that BLE Mesh suffers from latency degradation and delivery failures under high node mobility and RF noise. In contrast, the proposed system uses connection-oriented ACL links and L2CAP CoC, providing reliable transport, secure peer bonding, and built-in flow control without introducing a new routing layer.

B. GATT Notifications and BLE CoC

GATT notifications remain the most common BLE data dissemination method but are inherently unicast, requiring repeated transmissions to multiple peers. This approach increases energy use and degrades responsiveness in group contexts [2].

L2CAP Connection-Oriented Channels, introduced in Bluetooth 4.1, provide a flow-controlled alternative with larger MTUs and bidirectional support [1]. While primarily used for audio and data transfer, prior work has explored CoC for secure file transfer and streaming [10]. However, few efforts have adapted CoC for decentralized multi-peer broadcast relaying, as proposed in this architecture.

C. Whisper Protocol and WSN Flooding

The Whisper Protocol [7] was originally developed for IEEE 802.15.4-based WSNs. It uses synchronized time slots and constructive interference to minimize flooding delay and redundancy. Whisper has been shown to outperform probabilistic flooding in terms of energy and latency but depends on strict PHY-layer timing.

This work borrows Whisper's principles—relay suppression, flood minimization, and fast convergence—but adapts them for asynchronous, BLE-based systems using randomized backoff and credit-based gating instead of synchronization.

Related WSN protocols such as Glossy, CTP, and Directed Diffusion [8], [9] offer additional insights into energy-aware routing and topology-aware dissemination. However, they operate at the network layer and are unsuitable for direct deployment on BLE stacks.

D. Epidemic and Gossip Protocols

Epidemic algorithms and gossip protocols have been widely applied in distributed databases, peer-to-peer overlays, and blockchain networks. These methods spread information probabilistically using peer contact patterns, TTL limits, and suppression of duplicates [6], [7].

This paper incorporates epidemic principles into the BLE transport layer:

- Peer-level suppression of overheard packets
- Probabilistic relaying based on peer density
- Use of TTLs and message ID caching

Unlike traditional gossip, however, the design leverages BLE's flow-controlled CoC links and secure bonding, resulting in better delivery guarantees under embedded system constraints.

E. Secure Onboarding and Trust Models

The proposed architecture relies on bonded peer groups formed via LE Secure Connections (LESC). Emerging frameworks such as Matter, Wi-Fi Easy Connect, and FIDO Device Onboarding (FDO) [11], [12] introduce scalable, cryptographically robust device provisioning models that could enhance group management in future versions of the system.

While not implemented in this work, the architecture is designed to support such enhancements, offering a standards-aligned foundation for secure and dynamic trust formation in embedded BLE ecosystems.

IX. Conclusion

This paper presents a theoretical but deployment-oriented system architecture that enables low-latency, energy-efficient group communication over Bluetooth Low Energy (BLE) by adapting the Whisper Protocol's broadcast efficiency principles to the L2CAP Connection-Oriented Channel (CoC) transport layer. The proposed design addresses key shortcomings of existing BLE group messaging techniques, such as the unicast nature of GATT and the congestion-prone, high-overhead structure of BLE Mesh.

Key innovations include:

- A peer-assisted relaying workflow using randomized backoff, replay suppression, and message caching.
- Use of credit-based flow control from BLE CoC to prevent overflow and manage congestion.
- Adaptive policies for energy-aware relaying, QoS-based prioritization, and congestion throttling.
- A secure group model based on LE Secure Connections (LESC) bonding and whitelist enforcement.

While the system is conceptual and lacks an implementation, it is grounded in BLE specification capabilities and designed to be portable across embedded platforms such as Zephyr RTOS, Nordic SDK, and Android. The paper contributes a comprehensive evaluation framework, recommending practical metrics—packet delivery ratio, latency, energy usage, congestion indicators, and memory overhead—to guide simulation and prototyping.

Future work will focus on:

- Implementing the protocol on a real BLE testbed (e.g., using Nordic nRF5340 boards or Android-based smartglasses).
- Benchmarking performance under mobility, interference, and varying network sizes.
- Exploring hybrid GATT-CoC models for fallback compatibility.
- Integrating trust delegation frameworks such as FIDO Device Onboarding to support scalable provisioning.

Overall, this system offers a standards-compliant approach to secure, reliable, and efficient peer-to-peer broadcasting in BLE networks—bridging the gap between theoretical wireless dissemination strategies and real-world embedded system constraints.

References

[1] Bluetooth SIG, Bluetooth Core Specification Version 5.4, 2024. [Online]. Available: https://www.bluetooth.com/specifications

[2] K. Townsend, B. C. Fenner, and R. Cuno, Getting Started with Bluetooth Low Energy, O'Reilly Media, 2014.

[3] 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.

[4] Bluetooth SIG, Bluetooth Mesh Profile Specification, 2017. [Online]. Available: https://www.bluetooth.com/specifications/mesh

[5] Y. Yang, T. Lv, S. Dai, and J. Liu, "On the Performance of BLE Mesh Networks: Experimental Evaluation and Theoretical Modeling," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9833–9845, Jun. 2021.

[6] M. Keshavarz, M. Portoles-Comeras, S. Duquennoy, and A. Dunkels, "Mesh Under Interference: Performance and Robustness of the Bluetooth Mesh Protocol," in Proc. ACM IPSN, 2020.

[7] S. Duquennoy, B. Al Nahas, and O. Landsiedel, "Whisper: Fast Flooding for Low-Power Wireless Networks," in Proc. ACM/IEEE IPSN, pp. 1–12, Apr. 2017.

[8] R. Fonseca, O. Gnawali, K. Jamieson, and P. Levis, "The Collection Tree Protocol," in Proc. ACM SenSys, 2009.

[9] T. Voigt, A. Dunkels, J. Alonso, and H. Ritter, "Smartdust Protocols for Wireless Sensor Networks," in Proc. IEEE WCNC, 2004, pp. 2268–2273.

[10] C. Perkins, Ad Hoc Networking, Addison-Wesley, 2001.

[11] FIDO Alliance, FIDO Device Onboard (FDO) Protocol Specification, Version 1.1, 2022. [Online]. Available: https://fidoalliance.org/specs/fido-device-onboard

[12] Connectivity Standards Alliance, Matter Specification v1.2, Oct. 2023. [Online]. Available: https://csa-iot.org/all-solutions/matter

[13] M. Siekkinen, M. Hiienkari, J. K. Nurminen, and J. Nieminen, "How Low Energy is Bluetooth Low Energy? Comparative Measurements with ZigBee/802.15.4," in Proc. IEEE WCNC, 2012.

[14] A. Demers et al., "Epidemic Algorithms for Replicated Database Maintenance," in Proc. ACM PODC, 1987.

[15] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," in Proc. ACM MobiCom, 2000.

Nikheel V. Savant (Senior Member, IEEE) received the B.E. degree in Electronics and Communication Engineering from B.V. Bhoomaraddi College of Engineering and Technology, Hubli, India, in 2013, and the M.S.E. degree in Embedded Systems from the University of Pennsylvania, Philadelphia, PA, USA, in 2016.
He has held engineering roles at Apple as a Wi-Fi Systems Software Engineer and at Tesla as a Vehicle Connectivity Intern, where he focused on wireless communication protocols and automotive telemetry. He is currently a Senior Software Engineer at Meta, where he leads the development and optimization of Bluetooth protocols for next-generation wearable and embedded platforms.
His research interests include Bluetooth protocol stacks, embedded wireless systems, AI-driven connectivity diagnostics, and low-power communication architectures. He received the Gold Medal for academic excellence during his undergraduate studies. Mr. Savant is a Senior Member of the IEEE and actively contributes to standardization efforts within the Bluetooth Special Interest Group (SIG).