Ad Hoc Networks 192 (2026) 104335

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Survey paper

Comparative analysis of BLE SIG mesh and Wirepas mesh for Ad Hoc IoT deployments: Features, security, efficiency and application suitability

Muhammad Zeeshan Waheed [a,b,*], Fahad Sohrab [b], Waleed Bin Qaim [b], Matti Vakkuri [c], Jyrki Okkonen [c], Mikko Valkama [b], Moncef Gabbouj [b]

[a] Nokia, Finland
[b] Faculty of Information Technology and Communication Sciences, Tampere University, Finland
[c] Haltian, Finland

ARTICLE INFO

Keywords:
BLE mesh
Bluetooth mesh
Wirepas mesh
IoT mesh networking
Bluetooth low energy
BLE mesh performance

ABSTRACT

The rapid increase in the number of Internet of Things (IoT) devices has led to the development of advanced networking technologies such as bluetooth low energy (BLE) standardized by special interest group (SIG) mesh and Wirepas mesh networks. Each of these technologies offers unique features and capabilities. BLE is a widely used short-range technology that has made a significant impact on the IoT paradigm development thanks to its simplicity, low power consumption, robustness, and low cost. In contrast, Wirepas mesh is a decentralized wireless communication protocol, meaning that each node in the network selects its own role while maintaining and optimizing the connection automatically based on its environment. This paper provides a comparative analysis of BLE SIG mesh and Wirepas mesh, focusing on their security, scalability, power, and memory efficiency, as well as application suitability in diverse ad hoc IoT environments. The study highlights that while BLE SIG mesh benefits from easy adoption, low power consumption, and ease of integration into the consumer IoT ecosystem, Wirepas mesh excels in high-density, large-scale industrial applications due to its robust management and decentralized control. Security is realized in BLE SIG mesh with standard authentication and encryption, whereas Wirepas mesh utilizes deployment-configurable security mechanisms to handle diverse network topologies. This comparative review enables IoT industrialists and researchers to select appropriate mesh technologies based on their specific requirements and deployment constraints.

1. Introduction

Driven by the demand for emerging services and applications, the rapid evolution of wireless communication technologies has drawn significant attention to mesh networking protocols, particularly BLE mesh and Wirepas mesh. These protocols have become foundational for building robust, scalable, and energy-efficient wireless networks across diverse domains, including industrial IoT, building automation, and smart homes [1–3]. BLE mesh, a standardized protocol maintained by the bluetooth special interest group (SIG), supports managed and interoperable deployments [4]. In contrast, Wirepas mesh offers a proprietary decentralized alternative developed and maintained by Wirepas, focusing on flexibility, scalability, and ease of deployment [5]. Bluetooth technology, originally introduced in 2000 as a cable replacement solution, quickly gained popularity in the wireless domain, particularly in computer peripheral devices such as keyboards and mice [6–8]. A major leap occurred in 2010 with the advent of bluetooth low energy (BLE), which significantly expanded the relevance of Bluetooth in many other devices such as smartphones, tablets, headsets, health and fitness gadgets, and various wearable technologies [9, 10]. In parallel, wireless mesh communication systems have emerged as an effective approach for covering large areas such as industries, hospitals, and residential environments. However, many early implementations mainly relied on proprietary or niche technologies, raising concerns over interoperability and global compatibility across devices such as smartphones, computers, and home automation devices, including smart locks, temperature sensors, light bulbs, etc., to name a few [11]. In response, BLE SIG introduced the BLE mesh in 2017, extending BLE to support large-scale device-to-device communication. Its core specification focuses on re-meshing capabilities, energy conservation, and efficient device management, ensuring reliable data transmission even in dynamic network conditions. Recent updates have

* Corresponding author at: Faculty of Information Technology and Communication Sciences, Tampere University, Finland.
E-mail addresses: muhammad.waheed@nokia.com (M.Z. Waheed), fahad.sohrab@tuni.fi (F. Sohrab), waleed.binqaim@tuni.fi (W.B. Qaim), matti.vakkuri@haltian.com (M. Vakkuri), jyrki.okkonen@gmail.com (J. Okkonen), mikko.valkama@tuni.fi (M. Valkama), moncef.gabbouj@tuni.fi (M. Gabbouj).

https://doi.org/10.1016/j.adhoc.2026.104335
Received 17 December 2025; Received in revised form 15 May 2026; Accepted 22 June 2026
Available online 29 June 2026
1570-8705/© 2026 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

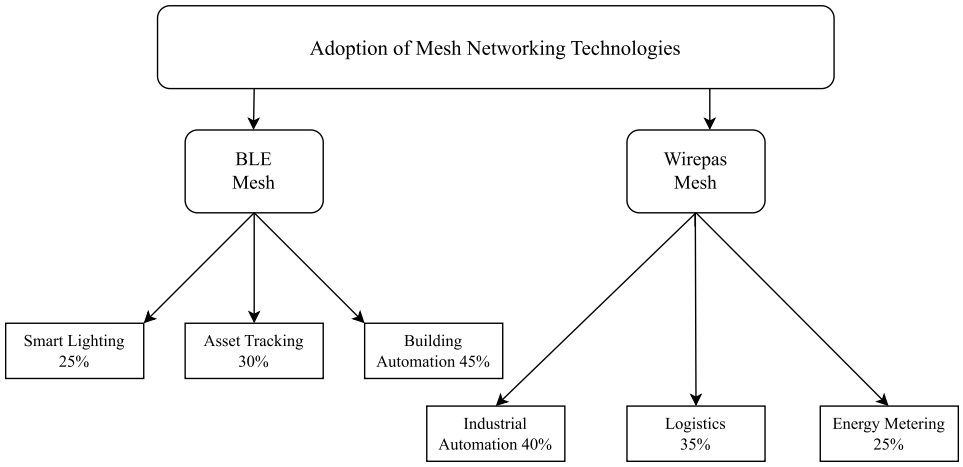

Fig. 1. An overview of the adoption rate of BLE mesh and Wirepas mesh across various industries.

Table 1
Summarizing the adoption of BLE mesh and Wirepas mesh across industries.

Category	Protocol	Adoption Insight	Source
Adoption Rate	BLE mesh	65 qualified products within a year of launch	[15,16]
–	Wirepas mesh	7 million connected devices and 160 partners (2023)	[17]
Market Growth	BLE mesh	Market size expected to grow from €3.67 billion (2024) to €7.56 billion (2030) at a CAGR of 14.5%	[16,18]
–	Wirepas mesh	Wirepas generated approximately €6 million in revenue (2023), with deployments exceeding 1 million smart electricity meters in Norway and about 500,000 new meters added monthly.	[19]
Key Use Cases	BLE mesh	Smart lighting, asset tracking, building automation	[16]
–	Wirepas mesh	Industrial automation, logistics, energy metering	[20]

further enhanced its support for large networks, improved provisioning mechanisms, direct forwarding, and private beacons [6,12–14].

In contrast, Wirepas mesh is an independently developed protocol that diverges from the BLE standard to emphasize scalability, decentralized control, and node flexibility. Unlike traditional mesh implementations, where routing is centrally managed, Wirepas mesh employs a fully decentralized architecture in which each node autonomously selects its role and configures connections based on local conditions. This results in highly optimized, self-organizing networks that offer reliability, scalability, and low operational complexity. The ability of Wirepas mesh to maintain robust communication in dense, interference-prone environments maybe beneficial for industrial automation, logistics, and energy metering applications depending on the deployment conditions [21–23]. The general adoption rate of BLE mesh and Wirepas mesh networking technologies across different industries is given in Fig. 1. In addition, Table 1 presents a detailed breakdown of how each technology is utilized within these industries. Recent research has addressed diverse perspectives on the applicability, performance, and limitations of mesh networking technologies within the IoT domain. For example, the work in [10] highlights challenges related to configuration, parameter tuning, and chipset constraints, all of which directly influence the reliability and efficiency of BLE mesh networks. At the same time, these studies emphasize the robustness and simplicity of BLE mesh, particularly noting the effectiveness of managed flooding as a mechanism for urgent, small-scale, or highly dynamic network scenarios. Building on this, the survey in [24] provides a broader examination of BLE mesh networking, analyzing critical design trade-offs such as flooding versus routing, addressing models, and mesh-specific features including relay, proxy, and low-power friendship mechanisms. While valuable, this survey is limited to BLE mesh and does not provide comparative performance insights with other proprietary mesh solutions, such as Wirepas mesh. Other surveys have examined wireless mesh networking more generally. For instance, [25] present a comprehensive overview of wireless mesh network architectures, applications, and open research issues, but their focus predates the emergence of IoT-specific mesh standards such as BLE mesh and Wirepas. More recently, surveys such as [26,27] explore low-power wireless mesh standards (e.g., 6LoWPAN, ZigBee, Thread), but omit an in-depth analysis of BLE mesh and Wirepas mesh, which are increasingly relevant in industrial and consumer IoT deployments. Complementary comparative evaluations of BLE mesh and Wirepas mesh have further revealed distinct performance characteristics. Empirical results show that Wirepas achieves substantially lower median latency in low-latency mode and reduced power consumption in low-energy mode, whereas BLE mesh, while exhibiting higher latency, demonstrates stable current consumption. These findings underscore the importance of considering both energy efficiency and delay sensitivity when evaluating mesh protocols for IoT applications [5].

Taken together, these prior works establish the foundation for this survey while revealing clear gaps. Existing surveys either: focus exclusively on BLE mesh without comparison to alternative industrial solutions, emphasize traditional mesh networking without addressing modern IoT-centric performance trade-offs, or, overlook proprietary solutions such as Wirepas. Consequently, to the best of our knowledge, this is the first survey to provide a comprehensive comparative study of BLE mesh and Wirepas mesh, analyzing their distinctive characteristics, performance capabilities, energy efficiency, security features, and practical applications.

The aim of this paper is to explore the distinctive characteristics, performance capabilities, energy efficiency, security features, and practical applications of BLE mesh and Wirepas mesh. To this end, the following key research questions are addressed:

- What are the fundamental technical differences between BLE mesh and Wirepas mesh?
- How do these two protocols support essential mesh functionalities such as re-meshing, security, energy consumption, device management, and network resilience?
- What trade-offs arise when deploying either protocol in specific use cases?

Understanding these factors is crucial for determining the most suitable mesh network implementation, particularly as the IoT ecosystem continues to expand and grow in complexity. The comparative analysis presented in this paper seeks to clarify the technological distinctions between BLE mesh and Wirepas mesh while also highlighting their respective strengths, limitations, and suitability for diverse application domains.

In the context of this paper, "ad hoc IoT deployments" refer to infrastructure-less, self-organizing networks where nodes can dynamically join, leave, and communicate without centralized co-ordination. Key features include decentralized operation, dynamic topology, and minimal reliance on already existing infrastructure. This definition is particularly relevant when evaluating mesh networking technologies, as their ability to support self-configuration and scalability directly impacts their suitability for such deployments.

In this context, BLE mesh supports ad hoc communication through its managed flooding mechanism, which enables devices to relay messages without requiring fixed routing paths. This can enhance robustness in dynamic environments; however, it may introduce communication overhead and scalability challenges in dense networks. In contrast, Wirepas mesh employs a decentralized routing approach in which nodes dynamically select communication paths based on local conditions. This design can support adaptive behavior in infrastructure-less environments, although its performance depends on configuration and deployment conditions. Therefore, both technologies support ad hoc networking principles to varying degrees, with different trade-offs in terms of scalability, overhead, and adaptability.

The remainder of this paper is organized as follows. Section 2 discusses the methodology used in this survey Section 3 introduces the technical background of BLE SIG mesh and Wirepas mesh, focusing on their architectures and key features. Section 4 examines re-meshing and network self-healing capabilities. Section 5 analyzes the security mechanisms employed by both protocols. Section 6 addresses considerations of energy efficiency, scalability, and memory usage. Section 7 discusses hardware requirements and licensing costs. Section 8 reviews algorithmic flexibility and customization opportunities. Section 9 surveys application domains where BLE SIG mesh and Wirepas mesh are deployed. Section 10 compares alternative mesh networking technologies. Finally, Section 11 concludes by summarizing the findings and recommending the more suitable protocol based on the criteria examined throughout the paper.

2. Survey methodology

This survey is based on a structured literature review of BLE mesh and Wirepas mesh. The initial step was to identify appropriate keywords and associated synonyms to construct an effective search expression. After a initial review of the literature, the following search expressions were developed:

("BLE mesh" OR "Bluetooth mesh" OR "BLE mesh performance") AND ("Wirepas mesh" OR "Wirepas") AND ("energy efficien*" OR " Bluetooth low power" OR "scalability" OR "latency" OR "IoT mesh networking")

A systematic search was then conducted for the 2005–2025 period using the selected keywords across widely recognized academic databases in the Information and Communications Technology (ICT) domain, including platforms such as Web of Science. In addition, AI-assisted search tools such as Scopus AI were used to complement the literature discovery process by refining and expanding search results based on the defined keywords.

The search process resulted in a broad set of potentially relevant publications. Subsequently, titles, abstracts, and keywords were analyzed to identify studies specifically addressing BLE mesh and Wirepas mesh technologies. Publications were included based on the following criteria: peer-reviewed journal and conference papers that present experimental, simulation, or analytical evaluations of BLE mesh and Wirepas mesh technologies, including their development and evolution.

Exclusion criteria included non-technical articles, purely promotional materials, and sources lacking sufficient empirical evidence. However, selected industry white papers and technical reports are referenced where necessary to reflect real-world deployment insights and practical utilization of the considered mesh networks.

The comparisons provided in this paper are based on reported metrics such as latency, scalability, energy consumption, deployment scenarios, and security mechanisms. It is important to note that results across different studies are not always directly comparable due to variations in experimental setups, network configurations, and traffic conditions. Therefore, the findings in this paper should be interpreted as indicative trends rather than absolute performance benchmarks.

3. Technical background

In this section, we discuss the fundamental terms and concepts necessary to understand mesh networking topologies. The basic principles of mesh networks are similar for both BLE mesh and Wirepas mesh, with the primary differences lying in their architectures and operational methods.

Most BLE devices communicate using a single point-to-point network topology, which enables one-on-one device communication. In the Bluetooth core specifications, this topology is referred to as a "piconet". A simple example is a smartphone connected to a headset. The same smartphone can also connect to other devices, such as an activity tracker or a car stereo. However, these devices communicate only with the smartphone and not with each other because each has a separate point-to-point connection with the smartphone [4,28].

In contrast, a mesh network uses a many-to-many topology, allowing devices to communicate directly with one another, as illustrated in Fig. 2. Each device in a mesh network is called a node, and a node can consist of multiple components known as elements. Every node and element in the network is assigned a unique address. Communication occurs through messages sent to these addresses, and nodes can relay messages to other nodes. This relaying capability extends the overall communication range beyond the individual radio range of each node [29]. Devices that are not part of the mesh network are referred to as "unprovisioned devices". The process that transforms an unprovisioned device into a node is called "provisioning". In the following subsections, we provide more details on some of these fundamental concepts.

3.1. The provisioning process

Provisioning is a secure process that involves several stages and is accomplished using an application on a device such as a smartphone or a tablet [4]. The provisioning process progresses through four steps, which are described as follows:

3.1.1. Beaconing

In beaconing, an unprovisioned device indicates its availability to be provisioned by using the mesh beacon. In BLE mesh new generic access profile (GAP) access data (AD) types, such as the "mesh Beacon", were introduced to support Bluetooth mesh features like provisioning [4]. The user usually starts this advertising by holding a combination of buttons or a particular button for a certain length of time.

3.1.2. Invitation

In invitation the Provisioner sends an invite to the device to be provisioned in the form of a provisioning invite protocol data unit (PDU). The beaconing device responds with information about itself in a provisioning capabilities PDU exchange public keys, where the provisioner and the device to be provisioned exchange information about their public keys, either directly or by using an out-of-band (OOB) method.

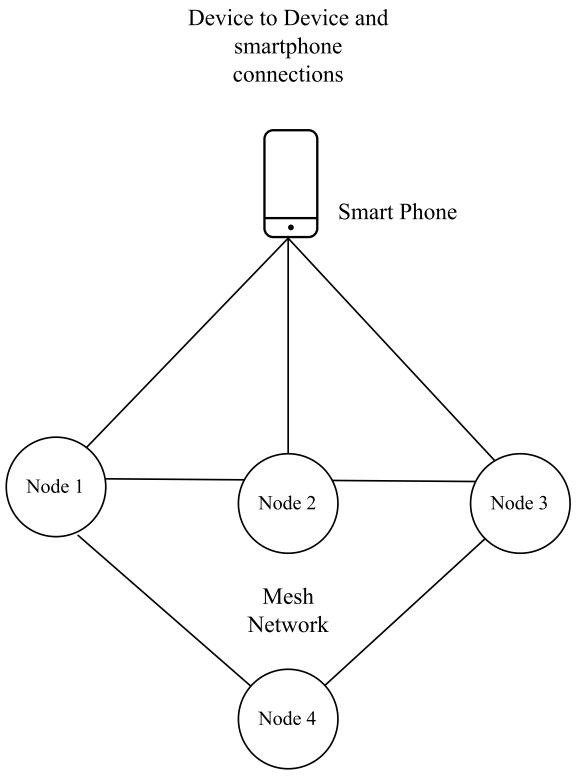

Fig. 2. mesh network showing a smartphone and several nodes communicating with each other.

3.1.3. Authentication

In authentication, the device to be provisioned outputs some sort of signal, such as a light-emitting diode (LED) flashing or some numbers displayed, which then the user enters into the provisioner for authentication.

3.1.4. Distribution

In distribution, the network key (NetKey) used as a security key is distributed among the provisioned devices. This NetKey is basically a mesh security parameter known as a Unicast Address, allocated by the provisioner. It is known as a node.

Fig. 3 shows the Bluetooth mesh architecture layers. In the following subsections, we will explore each layer of the mesh architecture, working our way from bottom to top [4,30].

3.2. Bluetooth mesh networking architecture

As discussed, the Bluetooth mesh networking architecture utilizes a layered architecture built upon BLE to enable many-to-many communication between devices in large networks [30]. Each layer is assigned a dedicated role which is further elaborated as follows:

3.2.1. Bearer layer

mesh messages require a predefined communication system to handle the transmission and reception. The bearer layer defines how the given communication system will handle the mesh PDUs. This is achieved via two bearers called the "advertising bearer" and the "generic attribute profile (GATT) bearer". The advertising bearer uses the BLE's advertising and scanning feature to convey and receive PDUs, while the GATT bearer is used in devices that do not support the advertising bearer.

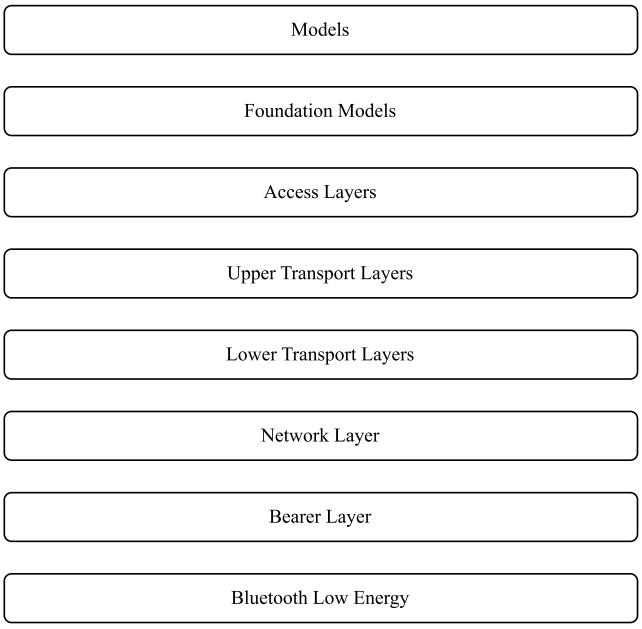

Fig. 3. Bluetooth mesh Networking Architecture.

3.2.2. Network layer

The network layer defines various message address types and formats, which allow the transport layer PDUs to be transported over the bearer layers. This layer also defines which network interfaces to utilize for output messages. An input filter is also applied to the incoming messages from the bearer layer to determine whether or not they should be delivered to the network layer for further processing.

3.2.3. Lower transport layer

The lower transport layer takes PDUs from the upper transport layer and sends them to the lower transport layers on peer devices. It also performs segmentation and reassembly of the PDUs where needed, especially for longer packets that do not fit into single-transport PDUs.

3.2.4. Upper transport layer

The upper transport layer is responsible for the encryption, decryption, and authentication of application data passing to and from the access layer. The upper transport layer also handles the transport messages responsible for actions within the transport layers of different peer nodes.

3.2.5. Access layer

The access layer is responsible for determining how applications can make use of the upper transport layer. This includes defining the format of the application data and controlling the encryption and decryption process, which is performed in the upper transport layer.

3.2.6. Foundation models layer

The foundation model layer is typically responsible for the configuration and management of a mesh network. The implemented models typically include configuration servers and client models, which manage network settings such as device keys, subscriptions, addresses, and relay functionality. Additionally, these models support fault procedures and network diagnostics.

3.2.7. Models layer

The models layer specifies the behavior of mesh nodes by defining models, which represent a collection of states, state transition and messages. These models ensure interoperability between devices by standardizing how features such as switching, dimming, sensing or configurations are implemented. Models also define state bindings, where changes in one state automatically affect others, for example, turning on a light bulb implicitly sets its brightness level. Communication is achieved through standardized client "Get" and "Set" messages. By encapsulating both functionality and messaging rules, the model layer acts as a key application-level abstraction of Bluetooth mesh. All the messages and behavioral requirements are governed by the Bluetooth mesh model specifications as described in, [4]

3.3. Wirepas mesh networking architecture

In Contrast to BLE SIG mesh, which is heavily layered with well-defined abstractions such as transport network and application layers, Wirepas mesh takes a fundamentally different approach. Instead of relying on such traditional layers, Wirepas mesh relies on a decentralized mesh networking mechanism. Fig. 4 shows some of the key features of the Wirepas mesh architecture [31], and they are elaborated as follows:

3.3.1. Decentralized operation

In this mode, every node independently selects its function, maintaining and optimizing connections without centralized oversight. Nodes handle tasks such as channel selection, timing, and message forwarding autonomously, maintaining and optimizing connections without any centralized controller. This self-organizing approach enhances scalability and fault tolerance, as the network can adapt to node failures or topology changes without manual intervention.

3.3.2. Multi-hop routing

In a Wirepas mesh network, the devices route traffic through multiple hops, enhancing network coverage and reliability. This multi-hop approach extends network coverage beyond the radio range of a single device, improving reliability as data can dynamically take alternative paths if a node or link becomes unavailable. It is particularly useful in dense or obstructed environments where line-of-sight communication is limited.

3.3.3. Scalability and density

The network supports large-scale deployments and high-density environments by utilizing up to 40 different channels. In the Wirepas mesh network, the nodes automatically select the least crowded channels, and communication is organized into time slots to optimize channel usage and minimize power consumption.

3.3.4. Reliability and resilience

Since there is no single point of failure, the mesh network is able to recover itself if a particular node fails, ensuring continuous operation. Battery-operated devices can act as a router node if needed, and the network supports multiple gateways for enhanced reliability. This architecture enables the creation of large-scale, self-healing networks suitable for various applications, including industrial IoT solutions. Table 2 summarizes the key differences between the BLE mesh architecture and the Wirepas mesh architecture. From the comparison, it can be observed that Wirepas mesh offers a flexible and dynamic deployment approach due to its decentralized routing mechanism, which can be advantageous in large and evolving network environments.

In contrast, BLE mesh follows a more structured architecture based on managed flooding, which supports interoperability and standardized operation. This approach can be advantageous in applications where compatibility and ecosystem support are important, particularly in small- to medium-scale deployments. However, it may introduce communication overhead in dense or large-scale networks, which can affect scalability under certain conditions.

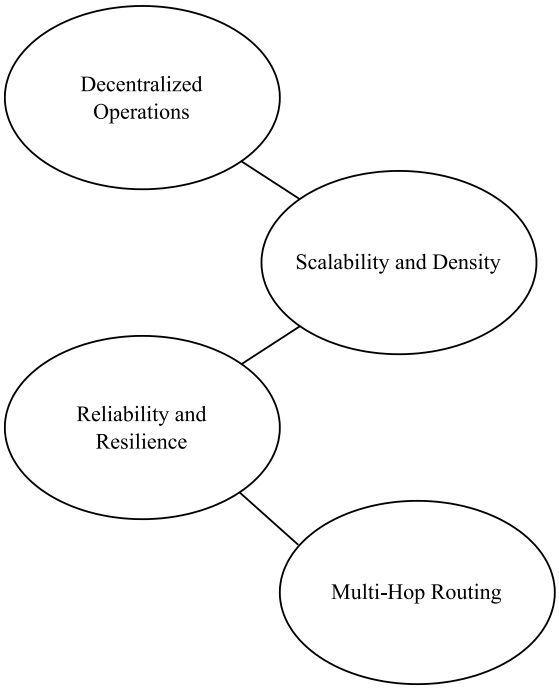

Fig. 4. Wirepas mesh architecture key features.

Table 2
Key differences between BLE mesh and Wirepas mesh.

Feature	BLE mesh	Wirepas mesh
Architecture Type	Layered, hierarchical architecture	Fully decentralized and autonomous operation
Control Mechanism	Centralized control with predefined node roles	No centralized controller; each node operates independently
Communication Layers	Clearly defined protocol layers (transport, network, physical)	Integrated communication stack without strict layering
Routing Approach	Preconfigured relay and managed routing paths	Adaptive multi-hop routing established in real time
Channel Management	Static channel assignment with periodic frequency hopping	Dynamic channel selection based on real-time interference and environment
Scalability Design	Optimized for moderate or small-sized networks	Designed for large-scale deployments with self-organizing adjustments

4. Re-meshing and network healing

Both Wirepas mesh and Bluetooth mesh are designed to support re-meshing and self-healing capabilities. This ensures continuous operation even if an individual node fails or becomes unavailable [32,33]. An overview of re-meshing and network healing capabilities of the Wirepas mesh network and the BLE mesh network is given in the following subsections.

4.1. Wirepas mesh network healing

Wirepas mesh features built-in network healing capabilities, allowing the network to automatically recover from node or link failure. When a node becomes unavailable or when the connection is disrupted, the nearby nodes quickly rearrange and find alternative routes for communication [31]. The following subsections discuss two commonly used network healing operations.

4.1.1. Decentralized self-healing

Wirepas mesh operates without any central controller. Each node automatically determines its role in the network and optimizes connections based on its environment. If a node fails, it can identify new connection paths, ensuring there is no single point of failure.

4.1.2. Dynamic routing adjustments

Nodes continuously monitor the network topology and make adjustments in real-time to find alternative routing paths. This dynamic adjustment allows the network to adjust quickly to changes, maintaining high reliability and availability [17]. However, the effectiveness of dynamic routing depends on network configuration and may introduce variability in performance under different deployment conditions.

4.2. Bluetooth mesh network healing

Bluetooth mesh network also supports self-healing to ensure network reliability. When a node becomes unavailable, Bluetooth uses its "managed-flooding" mechanism to recover, ensuring data can still reach the destination without interruption [34]. In Bluetooth mesh networks, network healing is achieved through a managed flooding mechanism combined with message caching, as discussed in the following subsections.

4.2.1. Managed flooding mechanism

Bluetooth mesh adopts a managed flooding technique for message broadcasting. In this technique, messages are broadcast to all nodes within range, and each node decides whether to relay the message based on specific criteria. This enables self-healing as messages can reach their destination through multiple paths, hence reducing redundancy.

4.2.2. Relay nodes and message caching

Dedicated relay nodes are responsible for forwarding messages to extend the network range. These nodes maintain a message cache to prevent retransmission of already relayed messages, to reduce traffic, and prevent collisions of the messages. While this setup offers resilience against node failure, it becomes vulnerable to failures if multiple nodes fail simultaneously [4].

From the above discussion, it is evident that both Wirepas mesh and Bluetooth mesh provide mechanisms for network healing, however, through different design approaches. Wirepas mesh employs a decentralized architecture that enables nodes to dynamically adjust routing paths, which can offer flexibility and rapid adaptation in changing network conditions.

In contrast, Bluetooth mesh utilizes a managed flooding mechanism combined with relay nodes and message caching, which enhances reliability through multiple transmission paths and provides robustness in the presence of node failures. However, this approach may introduce additional communication overhead in dense or highly dynamic environments.

While Wirepas mesh may offer advantages in scenarios requiring dynamic routing and large-scale adaptability, its performance depends on deployment configuration and proprietary implementation aspects. Similarly, Bluetooth mesh benefits from a standardized and interoperable framework, although it may face scalability challenges under certain high-density conditions due to message flooding.

Overall, both approaches present trade-offs between reliability, scalability, and adaptability, and their effectiveness depends on the specific requirements of the deployment scenario.

5. Security analysis

Mesh security is a fundamental requirement in both Bluetooth mesh and Wirepas mesh, ensuring that communications, applications, and devices are protected against unauthorized access and attacks. Bluetooth mesh employs a multi-layered security architecture that includes network, application, and device-level protection. At the network layer, the network key (NetKey) authenticates and encrypts all network messages, preventing unauthorized devices from joining or eavesdropping. Application security is enforced through application keys (AppKeys), ensuring that only authorized nodes can access specific functionalities. Devices are authenticated during the provisioning process, which securely adds them to the network and prevents rogue device inclusion [35].

Additionally, messages are encrypted and protected using sequence numbers and replay protection mechanisms, ensuring confidentiality, integrity, and resistance to replay attacks. While this layered approach provides strong security guarantees, it also introduces complexity in key management, particularly in large-scale deployments. Device manufacturers are responsible for conducting threat analyses to define appropriate security configurations, which can influence the overall robustness of the system [36–38].

In Wirepas mesh networks, both data transmission and network signaling are secured at the link layer using national institute of standards and technology (NIST)-recommended cryptographic algorithms, including advanced encryption standard (AES-128) and one-key message authentication code (OMAC1) for integrity verification. These mechanisms enable data protection and the generation of message integrity codes (MICs), which can be applied across the network. Key management can be configured from the application side, allowing flexibility in deployment, although this may introduce variability depending on implementation practices.

Furthermore, end-to-end security can be implemented at the application layer by encrypting the payload when required. While this flexible approach allows adaptation to different deployment scenarios, it may rely more heavily on proper configuration to ensure consistent security levels across the network.

When evaluating the security features of BLE SIG mesh and Wirepas mesh, several aspects must be considered, including encryption methods, authentication processes, network integrity mechanisms, and resistance to common threats. Table 3 summarizes key differences between the security approaches of both technologies [5,6,39–41].

5.1. Security threat model comparison

BLE mesh and Wirepas mesh both incorporate robust security mechanisms, however, their effectiveness depends on the assumed threat model and deployment context. BLE mesh employs a hierarchical key structure, including network, applications and device keys, enabling fine-grained access control and limits the impact of node compromise. However, this structure introduces additional complexity in large scale deployments particularly when it comes to distribution and management.

Wirepas mesh uses a flexible security model with configurable encryption and authentication mechanisms. This allows adaptation to different deployment scenarios but may rely more heavily on implementation-specific configurations, which can introduce variability in security robustness.

In scenarios, such as replay attack [42], BLE mesh mitigates risks through sequence numbers and message authentication, while Wirepas mesh employs message integrity checks and counters. In terms of scalability, centralized provisioning in BLE mesh may become a bottleneck, whereas decentralized approaches in Wirepas may improve flexibility but require very careful configuration to maintain security consistency.

From a practical perspective, the security trade-offs between BLE mesh and Wirepas mesh become particularly relevant under different

Table 3
Key Security Aspects of BLE mesh and Wirepas mesh Across Industries.

Security aspect	BLE SIG mesh	Wirepas mesh
Encryption	Utilizes AES-CCM (Counter with CBC-MAC) for authenticated encryption, ensuring confidentiality and integrity of all transmitted messages.	Employs AES-128 encryption in counter mode for all communication, with each message protected by a unique encryption key.
Authentication	Implements device authentication during provisioning using device keys (DevKey), allowing only authorized devices to join the network.	Uses OMAC1-based message integrity checks (MICs) appended to each packet, preventing replay and man-in-the-middle attacks while ensuring key-pair verification.
Network Integrity	Enforces multi-level key hierarchy, including network and application keys, to isolate communication layers and prevent cross-layer compromise.	Secures both data transmission and signaling at the link layer, maintaining network integrity and preventing unauthorized access.
Resistance to Threats	Designed with industrial-grade security to defend against replay attacks using sequence numbers and privacy keys that obscure metadata.	Incorporates built-in integrity and ownership validation, offering resilience against unauthorized access and data tampering in large-scale deployments.
Over-the-Air (OTA) Security	Supports secure OTA updates with encryption and authentication to prevent unauthorized firmware delivery, ensuring device integrity during updates.	Provides secure OTA update mechanisms using AES-128 authenticated bootloaders that verify and decrypt OTAP scratchpads before installation.

deployment conditions. In BLE mesh, the reliance on a hierarchical key management system as discussed in Section 5 can introduce challenges in large-scale or highly dynamic networks, where frequent node additions or removals increase the complexity of key distribution and updates. Improper key management may lead to increased attack surfaces, such as unauthorized access due to delayed key revocation or misconfiguration. Additionally, the managed flooding mechanism, while enhancing reliability, may expose the network to increased traffic analysis risks, as repeated message propagation can reveal communication patterns [43].

In contrast, Wirepas mesh's decentralized and configurable security approach allows greater flexibility, which can be advantageous in infrastructure-less deployments. However, this flexibility places greater responsibility on implementers to ensure consistent and secure configurations across devices. Inconsistent key management or misconfigured security parameters may lead to vulnerabilities such as weakened authentication or reduced protection against replay and spoofing attacks [39,44]. Therefore, while Wirepas mesh can adapt to diverse deployment scenarios, its security effectiveness depends strongly on correct implementation and configuration practices.

These considerations highlight that security performance in both technologies is not solely determined by protocol design, but also by deployment scale, network dynamics, and operational management practices.

Overall, both approaches present trade-offs between standardization, scalability, and flexibility, and their effectiveness depends on the specific requirements and threat assumptions of the deployment environment.

6. Energy, scalability and performance

In the area of mesh networks and IoT applications, energy, scalability and memory efficiency are key factors influencing overall system performance. This section analyzes these aspects for both BLE mesh and Wirepas mesh, highlighting their respective design trade-offs under different deployment conditions.

6.1. Energy efficiency

Energy efficiency is a critical aspect of mesh networking as many devices are battery-powered and require long-term, maintenance-free operation [45,46]. Both BLE mesh and Wirepas mesh incorporate mechanisms to reduce energy consumption. For instance, BLE mesh minimizes energy consumption by spending extended periods in sleep mode, using low-power nodes (LPNs) that awaken only periodically to synchronize with "Friend" nodes. This mechanism allows the nodes to conserve energy while maintaining network connectivity [47–49].

Studies on energy consumption modeling have shown the feasibility of such approaches. For example, [50] present a Q-learning-based routing strategy that optimizes duty-cycle scanning in BLE mesh networks, enabling battery-powered IoT devices to maintain long operational lifetimes. Similarly, [51] propose an energy-balanced flooding algorithm that ensures reliable data delivery without draining node batteries prematurely, making it suitable for energy-limited sensor networks. Extending this line of research, [52] investigate energy-efficient designs for wireless mesh networks using IEEE 802.11ba, highlighting how low-power operation can support dense, resource-constrained IoT deployments.

In contrast, Wirepas mesh provides configurable operating modes, including low energy (LE) and low latency (LL) modes, allowing adaptation to different deployment requirements. LE mode supports battery-operated devices, while LL mode is intended for scenarios requiring faster data transmission, typically in mains-powered systems. Additionally, Wirepas allows battery-powered nodes to participate in routing, which can improve network flexibility.

However, the energy efficiency of Wirepas mesh depends on configuration choices, traffic patterns, and network density. While optimized routing can reduce redundant transmissions, maintaining routing functionality on battery-powered nodes may introduce additional energy overhead under certain conditions. Reported examples, such as long device lifetimes in specific deployments, are highly scenario-dependent and may not generalize across all use cases [5].

6.2. Memory efficiency

Memory efficiency is also quite an important factor in mesh networking as many devices run on limited resources and have very limited memory storage and random access memory (RAM). Efficient memory utilization enables devices to preserve routing information, participate in multi-hop communication, and maintain security keys without the need for large hardware to support, and hence reduces the overall running cost. The BLE mesh network protocol is designed to operate within the limitations of a typical embedded system. However, features such as device authentication, encryption, and support for multiple roles can increase memory requirements. Furthermore, BLE mesh devices that are assigned multiple roles when needed may require additional memory resources to handle the associated data structures and state information.

In contrast, Wirepas mesh utilizes a relatively lightweight protocol stack, which can enable efficient operation on resource-constrained devices. This approach may support scalability in large deployments with limited hardware resources. However, actual memory usage depends on implementation details, network configuration, and the level of routing and security functionality required [53,54].

6.3. Scalability and performance

Scalability and performance are also critical factors when it comes to evaluating the performance of mesh networking protocols, especially for large-scale Internet of Things (IoT) deployments. To assess the performance of BLE mesh, studies such as [15] report that BLE mesh can achieve average delays of approximately 250 ms (ms) over more than 10 hops under challenging network conditions. While these results demonstrate the feasibility of multi-hop communication, performance is influenced by network scale, node density, and traffic patterns. As the network size increases, latency may rise and reliability may be affected due to increased interference and network congestion, particularly in dense deployments [55,56]. However, in moderately sized or well-configured networks, BLE mesh can maintain acceptable performance levels, especially when optimized through relay configuration and traffic control mechanisms.

Scalability is one of the key features of a mesh network. In recent mid-to-long IoT applications, the number of devices in a network can vary from hundreds to thousands, and massive deployments are becoming very popular. BLE mesh supports large-scale networks with the capability of handling thousands of nodes. However, the use of the controlled-flooding broadcast scheme can represent a challenge for the expansion and scalability of a Bluetooth mesh network. Alternative possible paths for a PDU to be successfully transmitted through a network are provided by increasing the number of relay devices. The availability of these routes contributes to improving the performance; however, in networks using the flooding mechanism, one of the major issues that can be problematic is the broadcast storm. Broadcast storms in flooding-based networks arise due to redundant retransmissions, which increase channel contention and packet collisions. Prior studies have shown that this effect becomes more pronounced in dense deployments, leading to reduced network efficiency and increased energy consumption [43,51,57–62].

Wirepas mesh, on the other hand, has been reported to achieve latency values as low as 2.83 ms per hop in controlled experimental setups consisting of a 10-node chain topology, where transmission power, routing paths, and inter-node interference were carefully managed to minimize cross-talk and ensure predictable communication behavior. In these experiments, nodes communicated only with neighboring devices under tightly controlled radio conditions and fixed traffic patterns. More typical latency values are reported to be around 20 ms per hop depending on factors such as network topology, synchronization, traffic load, and deployment configuration [5]. While these results indicate the potential for low-latency communication, such performance is highly dependent on factors such as network topology, traffic load, synchronization accuracy, and environmental conditions. Consequently, these figures should be interpreted as indicative of best-case or optimized scenarios rather than representative of all real-world deployments.

Theoretical scalability estimates suggest support for extremely large networks, potentially reaching billions of devices. However, such figures are based on idealized assumptions and are constrained in practice by hardware limitations, synchronization requirements, and network management complexity. Furthermore, Wirepas' decentralized architecture and cost-based routing enable efficient operation in both extensive and dense networks without performance degradation [63].

From the above discussion, it is evident that both BLE mesh and Wirepas mesh are designed to support large-scale IoT networks, although they adopt different approaches. BLE mesh relies on managed flooding, which enhances reliability through redundant message propagation but may introduce communication overhead in dense deployments. In contrast, Wirepas mesh employs decentralized routing and scheduling mechanisms, which can improve scalability and reduce redundant transmissions under certain conditions.

Both protocols incorporate strategies to improve energy and memory efficiency. BLE mesh leverages low power nodes and standardized mechanisms to extend battery life, while Wirepas mesh provides configurable operating modes that allow adaptation to different energy and performance requirements. However, the effectiveness of these approaches depends on deployment configuration, traffic patterns, and device capabilities.

In terms of memory usage, BLE mesh includes additional features such as multi-role support and layered security, which may increase memory requirements but provide flexibility and interoperability. Wirepas mesh, on the other hand, may achieve lower memory usage through a more streamlined protocol design, although this depends on implementation and routing complexity.

Overall, neither approach universally outperforms the other. BLE mesh offers advantages in standardization and interoperability, while Wirepas mesh may provide benefits in scalability and routing efficiency in certain large-scale scenarios. The choice between the two depends on application requirements, network size, energy constraints, and deployment conditions.

Table 4
Licensing and hardware cost aspects of BLE mesh and Wirepas mesh.

Factor	BLE SIG mesh	Wirepas mesh
Licensing	Free to use. Requires only Bluetooth SIG membership for product qualification and certification.	Commercially licensed software; requires a deployment or device-based license from Wirepas.
Certification	Based on open Bluetooth SIG specifications, with standard interoperability certification.	License fee varies with deployment scale and device count; proprietary certification managed by Wirepas.
Scalability Cost	Performance may degrade in very large networks due to managed relay structure and limited control flexibility.	Optimized for large-scale networks, although performance depends on deployment conditions and configuration.
Hardware Cost	Utilizes standard off-the-shelf BLE chipsets widely available from multiple vendors, minimizing hardware cost.	Requires BLE-compatible hardware preloaded with Wirepas firmware, leading to slightly higher per-device cost.

7. Hardware and licensing costs

Hardware requirements and associated costs are critical considerations when evaluating mesh networking protocols, as they directly influence both implementation feasibility and total project cost.

BLE mesh is compatible with devices supporting Bluetooth 4.0 and above, though Bluetooth 5.0 is generally recommended for its extended range and improved throughput. A typical BLE mesh node consists of a system-on-chip (SoC) with flash memory ranging from 256 kilobytes (KB) to 1024 KB and random-access memory (RAM) between 32 KB and 256 KB. Development kits from vendors such as Nordic Semiconductor provide accessible platforms for BLE mesh application development. The total cost of a BLE mesh deployment depends on device complexity, production volume, and network size. For very large-scale projects exceeding approximately 250,000 units, custom chip designs may offer improved economies of scale [64].

In addition to hardware, licensing and certification costs play a significant role in BLE mesh deployments. While the "Adopter Membership" in the Bluetooth SIG is free of charge, product qualification requires certification, with fees that may increase depending on product scope and deployment scale. Organizations seeking broader privileges may opt for "Associate Membership", which involves higher costs but includes additional benefits. Furthermore, beyond qualification expenses, implementers must also account for development and software costs. Although open-source protocol stacks such as the Nordic

software development kit (SDK) and Zephyr real-time operating system (RTOS) help reduce software-related expenditures, integration and maintenance efforts may still contribute to overall system cost.

Wirepas mesh operates on commonly available radio hardware, including off-the-shelf SoCs such as Nordic's nRF52 series, and can run on relatively resource-constrained devices. This hardware compatibility may provide flexibility in sourcing components and designing deployments. Additionally, the protocol is designed to operate efficiently in terms of memory and processing requirements, which can support cost-effective implementations in certain scenarios [64]. However, actual hardware costs depend on the chosen platform, network configuration, and required performance characteristics. In some cases, additional optimization or configuration effort may be necessary to achieve the desired performance, which can influence overall system cost.

Unlike BLE mesh, Wirepas mesh is a proprietary solution and requires a commercial software license. The cost of this license depends on the size and nature of the deployment. While this model may provide access to vendor-supported features and optimized network functionality, it also introduces dependency on a specific ecosystem and may impact long-term flexibility and cost predictability.

Certification requirements differ from BLE mesh, as Bluetooth SIG qualification is not required. However, validation within the Wirepas ecosystem may still be necessary to ensure compatibility and performance consistency.

Ultimately, the choice between BLE mesh and Wirepas mesh in terms of hardware and licensing costs depends on the intended deployment and system requirements. BLE mesh benefits from an open standard, broad ecosystem support, and widely available hardware, which can simplify integration and reduce vendor dependency. However, certification and compliance processes may introduce additional costs.

In contrast, Wirepas mesh offers a proprietary solution that may provide flexibility in certain deployment scenarios and optimized performance through vendor-specific features. However, this comes with licensing costs and potential dependency on a single vendor ecosystem.

Therefore, the selection between the two approaches should consider not only initial hardware costs but also long-term factors such as scalability requirements, vendor dependency, maintenance, and total cost of ownership. A summary of the licensing and hardware cost considerations is presented in Table 4.

8. Algorithm and customization

In mesh networking, the underlying communication algorithm and the degree of customization are critical factors influencing scalability, flexibility, and overall network performance. Customization enables developers to fine-tune mesh behavior for specific operational goals such as latency reduction, energy efficiency, reliability, and throughput optimization [65].

BLE mesh uses a flooding-based message relaying mechanism known as managed flooding, in which nodes retransmit messages to ensure delivery. While this approach improves reliability in smaller networks, it can lead to network congestion and unnecessary energy consumption in larger deployments. BLE mesh allows limited customization at the host stack level, but the core protocol stacks are often locked by vendors. Since BLE mesh strictly follows Bluetooth SIG standards, devices from different vendors can interoperate, but this standardization also restricts deep, protocol-level customization [66].

In contrast, Wirepas mesh employs a time-synchronized channel hopping (TSCH) communication approach combined with a self-forming and self-healing routing mechanism. Nodes dynamically select communication paths based on factors such as link quality, network load, and energy usage, which can improve efficiency and adaptability under certain conditions.

Wirepas mesh also supports customization at the application level, allowing developers to tailor network behavior to specific deployment requirements while utilizing vendor-provided routing mechanisms. This flexibility can be advantageous in specialized use cases. However, the extent of customization depends on proprietary implementations, and deeper modifications to the underlying protocol may be constrained by the platform. Additionally, achieving optimal performance may require careful configuration and tuning [5,63].

9. Application areas

Wirepas mesh and BLE mesh offer different capabilities that make them suitable for a range of application domains. Their applicability depends on factors such as network scale, device capabilities, interoperability requirements, and deployment conditions [77]. Some of the key application areas for both of these technologies are discussed in the following subsections. Both BLE mesh and Wirepas mesh are applicable across multiple domains; however, their suitability depends on deployment scale, infrastructure constraints, and application requirements. The following discussion highlights representative use cases for each technology.

9.1. Wirepas mesh

Wirepas mesh is a decentralized mesh network that is designed for large IoT deployments. Some of the key application areas are:

9.1.1. Health care and smart hospitals

In a healthcare environment, Wirepas mesh provides features such as asset tracking, e.g., wheelchairs, medical equipment tracking in a hospital, improving patient experience, and overall healthcare experience. One example case study is at a children's hospital in Utrecht, Netherlands, where Wirepas mesh demonstrated its effectiveness in such applications [67]. In comparison, BLE mesh offers advantage in terms of smartphone integration and interoperability, its performance in large-scale deployments may depend on network configuration. In contrast, Wirepas mesh may provide advantages in large hospital environments due to its decentralized routing approach, although this depends on deployment conditions.

9.1.2. Smart metering and utilities

Smart metering refers to the remote collection of energy, water, or gas usage data across millions of households. The main requirements are long-range communication, low-latency data aggregation and the ability to scale to millions of devices. Wirepas mesh, with support for sub-GHz bands and decentralized operation, is well-suited for large-scale metering deployments under certain conditions. A notable example is Hafslund in Norway, where about 700,000 smart meters were installed using Wirepas mesh [68–70]. BLE mesh, while efficient for small-scale deployments, may face challenges in achieving the same coverage and scalability required for nationwide metering infrastructures. In contrast, Wirepas mesh is designed to support large-scale, distributed networks, although their effectiveness again depends on deployment conditions and configuration.

9.1.3. Industrial asset tracking and smart buildings

Factories and smart buildings require continuous monitoring of workforce safety, temperature, humidity and asset utilization. These applications demand low-latency communication, autonomous operation and the ability to adapt to dynamic environments. Wirepas mesh has actively been used in industries, especially factories, to monitor workforce, humidity, equipment, temperature, and lighting conditions to ensure a good and safe environment and efficient resource utilization [5]. Wirepas mesh's self-organizing and resilient routing capabilities make it effective in industrial deployments where downtime is costly. These features can be advantageous in industrial deployments where reliability and adaptability are required, although BLE mesh may still be suitable for smaller-scale or interoperability-focused scenarios.

Table 5
Comparative summary of application areas for BLE mesh and Wirepas mesh.

Application Area	Key Aspects	Suitable Protocol(s)	Pros	Cons	Source
Healthcare and Smart Hospitals	Scalability, self-healing battery tags	Both (depends on scale and integration)	Wirepas: decentralized routing, supports dense deployments; BLE: interoperability, smartphone integration	Wirepas: proprietary ecosystem; BLE: scalability depends on network size and configuration	[67]
Smart Metering and Utilities	Large-scale deployment, wide coverage	Both (depends on coverage and scale)	Wirepas: sub-GHz support, scalable infrastructure; BLE: standardized ecosystem, low-power operation	Wirepas: licensing cost; BLE: may face scalability limitations in wide-area deployments	[68–70]
Smart Agriculture and Environment	Outdoor coverage, low-power sensors	Both (depends on environment)	Wirepas: wide-area coverage, distributed routing; BLE: suitable for localized or indoor farming	Wirepas: proprietary ecosystem; BLE: limited range in open environments	[5]
Industrial Asset Tracking and Monitoring	Density, latency, autonomy	Both (depends on density and latency requirements)	Wirepas: adaptive routing, scalable tracking; BLE: interoperability, integration with existing devices	Wirepas: ecosystem dependence; BLE: may require careful planning in dense deployments	[5]
Smart Buildings and Environmental Sensors	Easy installation, energy efficiency	Both (depends on infrastructure and interoperability)	Wirepas: minimal RF planning, autonomous operation; BLE: standardized models, vendor interoperability	Wirepas: custom integration required; BLE: may require relay infrastructure	[5]
Vehicular IoT and Transportation	Mobility, low-latency communication	Both (depends on use case)	Wirepas: suitable for fleet monitoring; BLE: effective for passenger services and mobile interaction	Wirepas: limited smartphone integration; BLE: scalability depends on deployment density	[5]
Smart Lighting and Home Automation	Interoperability, standardized control	BLE mesh	Standardized models, strong ecosystem, cross-vendor compatibility	May require powered relays; scalability depends on network size	[6]
Indoor Positioning	Smartphone integration, context awareness	BLE mesh	Beacon support, proxy features, mobile integration	Limited range; performance may degrade in dense environments	[71]
Smart Cities, Proximity Services	User interaction, urban deployment	Both (depends on service type)	BLE: proximity services, smartphone interaction; Wirepas: scalable infrastructure support	BLE: limited large-scale coverage; Wirepas: less suited for direct user interaction	[72–76]
Wearables and Mobile Sensors	Low power, embedded devices	BLE mesh	Broad hardware support, energy-efficient operation	Limited scalability in dense multi-hop environments	[67]

9.1.4. Logistics and supply chain management

Supply chain management involves tracking goods in warehouses, ports, and transport vehicles. The challenges are high mobility, real-time location visibility, and large-scale deployments. Wirepas mesh may be suitable for such scenarios due to its decentralized routing and support for large-scale deployments, while BLE mesh can be applied in smaller or interoperability-focused deployments, depending on system requirements [17]. Wirepas mesh may be suitable for large-scale infrastructure deployments, while BLE mesh can complement such systems through smartphone-based interaction in last-mile scenarios.

9.1.5. Vehicular and transportation IoT

Transportation IoT spans fleet management, public transportation monitoring, and in-vehicle sensor networks. Requirements include low-latency, mobility support, and integration with passenger devices. Wirepas mesh is suitable for fleet-level monitoring because of its mobility support and scalability in dynamic networks. However, BLE mesh is more effective for passenger services, such as smartphone-based ticketing or infotainment, due to its widespread device compatibility. Thus, the choice depends on whether the focus is infrastructure monitoring (Wirepas) or passenger interaction (BLE) [78].

9.1.6. Smart agriculture and environmental monitoring

Smart agriculture requires deployment of soil sensors, irrigation controllers, and livestock trackers across large outdoor fields. The requirements include long-range communication, low power for solar/battery devices and support for thousands of nodes. Wirepas mesh, with its sub-GHz support and distributed architecture, provides reliable connectivity across wide rural areas [5]. BLE mesh, being limited to 2.4 GHz, is more suitable for greenhouses or indoor farming but less effective for open-field applications where Wirepas mesh may support wide-area deployments under certain conditions.

9.2. BLE mesh

In contrast to Wirepas mesh, BLE mesh also offers unique features and extends the BLE capabilities to support many-to-many device communication, enabling many application areas.

9.2.1. Smart lighting and home automation

Smart lighting and home automation require interoperability, low latency control and standardized models. BLE mesh is widely adopted in smart lighting and home automation due to its standardized models and strong interoperability across vendors [6]. While Wirepas could be applied, BLE mesh's standardized ecosystem makes it far more convenient.

9.2.2. Indoor positioning and smart museums

Indoor positioning requires context awareness and smartphone integration. BLE mesh supports proxy functionality and beacon models, enabling smartphone-based navigation and guidance. In museums, BLE beacons are used for localization. For example, the museum visitors can benefit from contextual information based on their location provided by BLE localization beacons [71].

9.2.3. Security and access control

Access control system demand secure authentication and integration with user devices. BLE mesh provides secure access control in many settings, such as offices, hospitals, and data centers, to ensure safe access and real-time monitoring of access points to enhance security protocols [39]. Wirepas could technically provide secure communication but BLE mesh offers advantages in access control scenarios due to its integration with personal devices and standardized security framework.

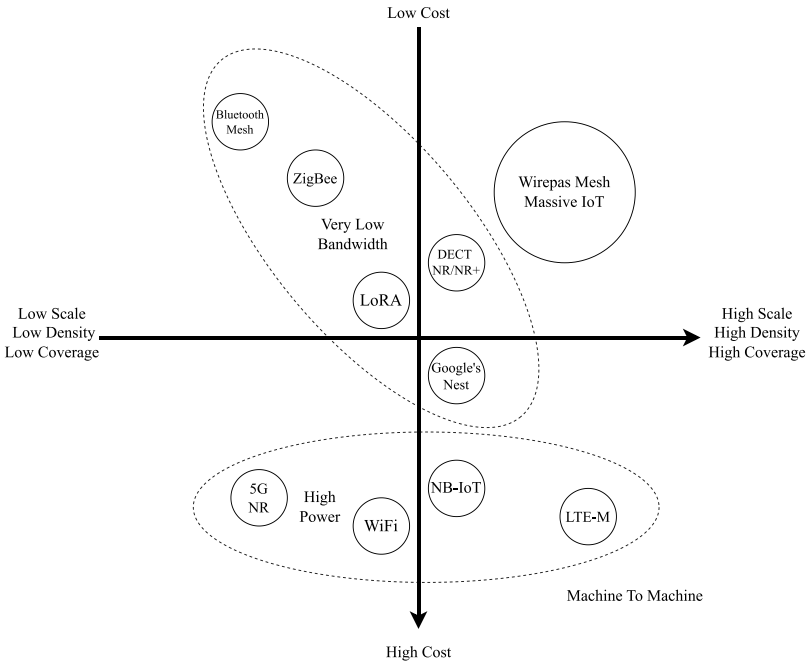

Fig. 5. Positioning of major mesh and IoT networking technologies based on cost, power, coverage, and scalability characteristics.

9.2.4. Smart cities

Smart city applications include context-aware services, location-based marketing and urban infrastructure monitoring. In smart cities, applications of BLE provide proximity marketing and indoor positioning. BLE low power consumption makes it suitable for large deployments in urban infrastructure projects [72–76]. However, for dense sensor deployments requiring massive scalability, Wirepas may offer advantages due to its decentralized routing approach, which can reduce communication overhead compared to flooding-based mechanisms.

9.2.5. Emergency and disaster recovery networks

BLE mesh, leveraging smartphone ubiquity and no reliance on infrastructure, can facilitate ad-hoc device-to-device communication networks in disaster situations, enabling large-scale peer connectivity when normal infrastructure fails [79]. Table 5 gives a comparative summary table about different application areas of Wirepas and BLE mesh with their respective pros and cons.

Overall, the suitability of BLE mesh and Wirepas mesh varies across application domains. BLE mesh is often preferred in scenarios requiring interoperability, smartphone integration, and standardized solutions, while Wirepas mesh may be advantageous in large-scale, infrastructure-oriented deployments requiring adaptive routing. Rather than a one-size-fits-all solution, both technologies address different segments of the IoT landscape depending on application requirements.

10. Alternative mesh networking technologies

In addition to BLE mesh and Wirepas mesh, several other mesh networking technologies have been developed to address diverse IoT communication requirements [80]. These technologies differ in terms of architecture, scalability, latency, and deployment models. The following subsections provide a comparative overview of selected alternatives, highlighting their characteristics and typical application domains.

10.1. Zigbee mesh

Zigbee is a low-power wireless communication protocol operating in the 2.4 GHz, 900 MHz, and 868 MHz bands. It utilizes routing mechanisms such as Ad hoc On-Demand Distance Vector (AODV) to support multi-hop communication. Zigbee is widely used in home automation and industrial monitoring applications due to its mature ecosystem and standardized profiles.

However, Zigbee networks may require dedicated coordinators and can exhibit higher latency in certain multi-hop scenarios, depending on network configuration. While it provides reliable communication for moderate-scale deployments, its flexibility and scalability may vary compared to other mesh networking approaches [81–83].

10.2. Thread mesh

Google's Nest develops thread mesh and is an IPv6-based mesh networking protocol that runs on IEEE 802.15.4 radios. It uses low-latency, self-healing mesh routing with border routers to connect to the internet. While Thread offers strong integration with IP-based systems and modern IoT frameworks, its adoption has been more prominent in specific application domains such as home automation. Deployment typically requires Thread-certified hardware and infrastructure components [84].

10.3. LoRaWAN mesh

LoRaWAN typically relies on a star topology; however, recently, efforts have been made to explore mesh-like topologies for extending coverage. LoRaWAN traditionally relies on star-based long-range communication, with some research on multi-hop mesh routing, which also makes it ideal for rural IoT deployments. Despite its benefits, high latency and low data rate make it less appealing as it is not suitable for real-time applications [85–87].

10.4. DECTNR/NR+ (Next-generation mesh technology)

DECT-2020 NR – also referred to as DECT-NR/NR+ – is an emerging 5G-aligned wireless technology standardized by european telecommunications standards institute ETSI to support massive IoT deployments. Unlike traditional DECT, DECT-2020 NR introduces a fully decentralized, self-organizing mesh architecture capable of supporting: ultra-reliable communication, large-scale device densities, long-range

sub-GHz operation, and scalable peer-to-peer routing without a central controller.

Recent studies indicate its potential for massive machine-type communication (mMTC) scenarios, offering high reliability and efficient spectrum utilization [21,88]. However, as an emerging technology, its adoption is still in early stages, and practical deployment considerations are evolving.

11. Conclusions

This survey presented a comprehensive comparison of BLE mesh and Wirepas mesh networks, evaluating their characteristics across key aspects such as network healing, energy efficiency, scalability, cost, and security, as summarized in Fig. 5. The analysis highlights that both technologies adopt fundamentally different design approaches, which influence their performance under varying deployment conditions.

Wirepas mesh utilizes a decentralized routing architecture that enables dynamic path selection and adaptability, supporting efficient operation in large and evolving network environments under appropriate conditions. In contrast, BLE mesh relies on a managed flooding mechanism, which enhances reliability through redundant message propagation and benefits from a standardized and interoperable framework. However, these approaches introduce trade-offs in terms of communication overhead, latency, and scalability.

In terms of energy efficiency, BLE mesh incorporates mechanisms such as LPNs to reduce energy consumption, while Wirepas mesh employs configurable communication modes and scheduling techniques to optimize power usage. The effectiveness of these approaches depends on network configuration, traffic patterns, and device capabilities.

Similarly, scalability and memory efficiency are influenced by architectural design choices. BLE mesh supports large-scale deployments through standardized mechanisms but may experience increased overhead in dense networks. Wirepas mesh, through decentralized routing and scheduling, may offer advantages in certain large-scale scenarios, although performance depends on implementation and deployment conditions.

Overall, neither technology universally outperforms the other. BLE mesh offers advantages in interoperability, standardization, and ecosystem support, making it suitable for applications requiring cross-vendor compatibility and integration with existing devices. Wirepas mesh provides flexibility in routing and configuration, which can be beneficial in large-scale or dynamic deployments. Therefore, the selection between the two should be guided by specific application requirements, including network size, energy constraints, infrastructure availability, and long-term system considerations.

Future work should focus on standardized benchmarking frameworks to enable more direct and fair comparisons between mesh networking technologies under consistent and reproducible conditions.

CRediT authorship contribution statement

Muhammad Zeeshan Waheed: Writing – review & editing, Writing – original draft, Validation, Methodology, Investigation, Formal analysis, Conceptualization. **Fahad Sohrab:** Writing – review & editing, Supervision, Formal analysis. **Waleed Bin Qaim:** Writing – review & editing, Validation, Investigation. **Matti Vakkuri:** Validation, Supervision. **Jyrki Okkonen:** Supervision, Methodology, Conceptualization. **Mikko Valkama:** Supervision, Formal analysis. **Moncef Gabbouj:** Supervision.

Declaration of generative AI and AI-assisted technologies in the manuscript preparation process

During the preparation of this work, the authors used Scopus AI to assist in narrowing and identifying relevant references based on the keywords and topics addressed in this paper. All retrieved material was subsequently reviewed, verified, and selected by the authors, who take full responsibility for the content of the published article. Additionally, generative AI tools such as “ChatGPT” were used to a limited extent for minor grammar and language refinement in selected sections of the manuscript.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] S.M. Darroudi, C. Gomez, J. Crowcroft, Bluetooth low energy mesh networks: A standards perspective, IEEE Commun. Mag. 58 (4) (2020) 95–101.
[2] A. Čolaković, M. Hadžialić, Internet of things (IoT): A review of enabling technologies, challenges, and open research issues, Comput. Netw. 144 (2018) 17–39.
[3] N. Todtenberg, R. Kraemer, A survey on bluetooth multi-hop networks, Ad Hoc Netw. 93 (2019) 101922.
[4] M. Baert, J. Rossey, A. Shahid, J. Hoebeke, The bluetooth mesh standard: An overview and experimental evaluation, Sensors 18 (8) (2018) 2409.
[5] S. Cortesi, C. Vogt, E. Reinschmidt, M. Magno, Latency and power consumption in 2.4 GHz IoT wireless mesh nodes: An experimental evaluation of bluetooth mesh and wirepas mesh, in: 19th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob, IEEE, 2023, pp. 200–205.
[6] I. Natgunanathan, N. Fernando, S.W. Loke, C. Weerasuriya, Bluetooth low energy mesh: Applications, considerations and current state-of-the-art, Sensors 23 (4) (2023) 1826.
[7] O.A. Amodu, M. Othman, Machine-to-machine communication: An overview of opportunities, Comput. Netw. 145 (2018) 255–276.
[8] H. Alemdar, C. Ersoy, Wireless sensor networks for healthcare: A survey, Comput. Netw. 54 (15) (2010) 2688–2710.
[9] A. Aijaz, A. Stanoev, D. London, V. Marot, Demystifying the performance of bluetooth mesh: Experimental evaluation and optimization, in: Wireless Days, WD, IEEE, 2021, pp. 1–6.
[10] D. Pérez-Díaz-De-Cerio, M. García-Lozano, A.V. Bardají, J.-L. Valenzuela, et al., Bluetooth mesh analysis, issues, and challenges, IEEE Access 8 (2020) 53784–53800.
[11] A. Nikoukar, S. Raza, A. Poole, M. Güneş, B. Dezfouli, Low-power wireless for the internet of things: Standards and applications, IEEE Access 6 (2018) 67893–67926.
[12] G. Koulouras, S. Katsoulis, F. Zantalis, Evolution of bluetooth technology: BLE in the IoT ecosystem, Sensors 25 (4) (2025) 996.
[13] M. Ghaemifar, S. Motie, S.M. Moosaviun, Y. Nemati, S. Ebadollahi, Bluetooth low energy for indoor positioning: Challenges, algorithms and datasets, Autom. Constr. 177 (2025) 106316.
[14] K. Szyc, M. Nikodem, M. Zdunek, Bluetooth low energy indoor localization for large industrial areas and limited infrastructure, Ad Hoc Netw. 139 (2023) 103024.
[15] R. Rondón, A. Mahmood, S. Grimaldi, M. Gidlund, Understanding the performance of bluetooth mesh: Reliability, delay, and scalability analysis, IEEE Internet Things J. 7 (3) (2019) 2089–2101.
[16] C. Bisdikian, An overview of the bluetooth wireless technology, IEEE Commun. Mag. 39 (12) (2002) 86–94.
[17] I. Wroe, How wirepas’ low-power mesh technology provides a reliable, affordable, and highly scalable way to track your assets, 2023, 2026, [Online] Available: https://www.oxspring.com/blog/wirepas-low-power-mesh-technology. (Accessed 15 May 2026).
[18] Z. Hosseinkhani, C. Gomez, M. Nabi, Mobile bluetooth mesh networks: Performance evaluation of a novel concept, IEEE Sens. J. 25 (8) (2025) 14124–14136.

[19] Wirepas ltd, wirepas mesh expansion world wide, 2022, 2026, [Online] Available: https://wirepas.com/news/wirepas-mesh-expands-rapidly-in-smart-energy/. (Accessed 15 May 2026).

[20] Wirepas ltd, wirepas mesh technology, 2025, 2026, [Online] Available: https://wirepas.com/wirepas-mesh/. (Accessed 15 May 2026).

[21] R. Kovalchukov, D. Moltchanov, J. Pirskanen, J. Säe, J. Numminen, Y. Koucheryavy, M. Valkama, DECT-2020 new radio: The next step toward 5G massive machine-type communications, IEEE Commun. Mag. 60 (6) (2022) 58–64.

[22] K. Roohi, A.R. Fekr, A comparative analysis of indoor localization technologies, Comput. Netw. 270 (2025) 111527.

[23] S.M. Asaad, H.S. Maghdid, A comprehensive review of indoor/outdoor localization solutions in IoT era: Research challenges and future perspectives, Comput. Netw. 212 (2022) 109041.

[24] S.M. Darroudi, C. Gomez, Bluetooth low energy mesh networks: A survey, Sensors 17 (7) (2017) 1467.

[25] I.F. Akyildiz, X. Wang, W. Wang, Wireless mesh networks: a survey, Comput. Netw. 47 (4) (2005) 445–487.

[26] M.R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the internet of (important) things, IEEE Commun. Surv. Tutor. 15 (3) (2012) 1389–1406.

[27] A. Rashid, T. Pecorella, Is 6LoWPAN-ND necessary?(spoiler alert: Yes), Comput. Netw. 250 (2024) 110535.

[28] M. Garg, G. Kaur, G. Singh, G. Sandhu, S. Gupta, S.R. Nayak, M.F. Ijaz, A review on internet of things: communication protocols, wireless technologies, and applications, in: Advances in Communication, Devices and Networking: Proceedings of ICCDN 2021, Springer, 2022, pp. 265–278.

[29] L. Lei, A. Tang, X. Wang, Analysis on the scalability issues of wireless mesh networks: Key factors and potential solutions, in: IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems, MASS, IEEE, 2022, pp. 586–591.

[30] Y.-H. Kao, C.-S. Wu, H.-K. Su, Design and analysis of a large-scale BLE mesh network, in: IEEE International Symposium on Measurements & Networking (M&N), IEEE, 2024, pp. 1–6.

[31] Wirepas, Wirepas mesh concepts and overview, https://developer.wirepas.com/support/solutions/articles/77000484367-wirepas-mesh-conceptsWirepas-mesh-Introduction/.

[32] A. Samuylov, D. Moltchanov, M. Alam, J. Pirskanen, J. Numminen, Y. Koucheryavy, M. Valkama, Performance of MAC layer mechanisms in DECT-2020 NR mMTC technology, in: IEEE Vehicular Technology Conference (VTC.2024-Spring), 2024.

[33] R.S. Shende, K.P. Patil, Re-organizable wireless mesh network using ARS, in: 2014 International Conference on Reliability Optimization and Information Technology, ICROIT, IEEE, 2014, pp. 240–244.

[34] P. Zhou, X. Fang, Y. Fang, R. He, Y. Long, G. Huang, Beam management and self-healing for mmwave UAV mesh networks, IEEE Trans. Veh. Technol. 68 (2) (2018) 1718–1732.

[35] D. Hortelano, T. Olivares, M.C. Ruiz, Providing interoperability in bluetooth mesh with an improved provisioning protocol, Wirel. Netw. 27 (2) (2021) 1011–1033.

[36] A. Adomnicai, J.J. Fournier, L. Masson, Hardware security threats against bluetooth mesh networks, in: IEEE Conference on Communications and Network Security, CNS, IEEE, 2018, pp. 1–9.

[37] A. Lacava, V. Zottola, A. Bonaldo, S. Basagni, Securing bluetooth low energy networking: An overview of security procedures and threats, Comput. Netw. 211 (2022) 108953.

[38] M. Cäsar, T. Pawelke, J. Steffan, G. Terhorst, A survey on bluetooth low energy security and privacy, Comput. Netw. 205 (2022) 108712.

[39] M.R. Ghori, T.-C. Wan, M. Anbar, G.C. Sodhy, A. Rizwan, Review on security in bluetooth low energy mesh network in correlation with wireless mesh network security, in: 2019 IEEE Student Conference on Research and Development, SCOReD, IEEE, 2019, pp. 219–224.

[40] K. Bansal, Bluetooth® mesh device authentication & secure network commissioning, in: 4th International Conference on Innovative Practices in Technology and Management, ICIPTM, 2024, pp. 1–6.

[41] H. Alamleh, A. Cantelli-Forti, Defending against BLE-based covert channels in crowdsourced location networks, Comput. Secur. (2026) 104835.

[42] Z. Feng, J. Ning, I. Broustis, K. Pelechrinis, S.V. Krishnamurthy, M. Faloutsos, Coping with packet replay attacks in wireless networks, in: 2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, IEEE, 2011, pp. 368–376.

[43] L. Wang, J. Li, M. Li, A rapid flooding approach based on adaptive delay and low-power sleep for BLE mesh networks, IEEE Access 12 (2024) 65323–65332.

[44] M.R. Ghori, T.-C. Wan, G.C. Sodhy, Bluetooth low energy mesh networks: Survey of communication and security protocols, Sensors 20 (12) (2020) 3590.

[45] D. Hortelano, T. Olivares, M.C. Ruiz, Reducing the energy consumption of the friendship mechanism in bluetooth mesh, Comput. Netw. 195 (2021) 108172.

[46] I. Lahsen-Cherif, L. Zitoune, V. Vèque, Energy efficient routing for wireless mesh networks with directional antennas: When Q-learning meets ant systems, Ad Hoc Netw. 121 (2021) 102589.

[47] A.K. Sultania, C. Delgado, C. Blondia, J. Famaey, Downlink performance modeling and evaluation of batteryless low power BLE node, Sensors 22 (8) (2022) 2841.

[48] Q. Xiao, Z. Chang, W. Wang, Y. Luo, B. Zhao, A bidirectional passive BLE chip for battery-free IoT mesh network, IEEE Trans. Circuits Syst. I. Regul. Pap. (2026).

[49] M. Malhotra, A. Sharma, S. Sharma, R. Khanna, Design and experimental evaluation of an nRF52832-based bluetooth mesh network for efficient sensor data collection and cloud-based visualization, in: International Conference on Next-Generation Networks and Deployable Artificial Intelligence, Springer, 2025, pp. 127–136.

[50] L. Jiang, J. Liu, L. Wang, A Q-learning approach to energy-efficient routing in BLE mesh network based on duty cycle scanning, in: International Conference on Internet of Things As a Service, Springer, 2023, pp. 358–370.

[51] A.S. Brandão, M.C. Lima, C.J.B. Abbas, L.J.G. Villalba, An energy balanced flooding algorithm for a BLE mesh network, IEEE Access 8 (2020) 97946–97958.

[52] R. Sanchez-Vital, C. Gomez, E. Garcia-Villegas, Exploring the boundaries of energy-efficient Wireless mesh Networks with IEEE 802.11 ba, Internet Things 28 (2024) 101366.

[53] J.D. Gotz, O.K. Rayel, G.L. Moritz, Improving bluetooth mesh energy efficiency using clustering, J. Commun. Inf. Syst. 36 (1) (2021) 156–165.

[54] X. Jiang, H. Zhang, E.A.B. Yi, N. Raghunathan, C. Mousoulis, S. Chaterji, D. Peroulis, A. Shakouri, S. Bagchi, Hybrid low-power wide-area mesh network for IoT applications, IEEE Internet Things J. 8 (2) (2020) 901–915.

[55] X. Jiang, H. Shokri-Ghadikolaei, G. Fodor, E. Modiano, Z. Pang, M. Zorzi, C. Fischione, Low-latency networking: Where latency lurks and how to tame it, Proc. IEEE 107 (2) (2018) 280–306.

[56] A. Belli, M. Esposito, S. Raggiunto, L. Palma, P. Pierleoni, Relaying mechanisms in BLE mesh networks: A method for improving latency and reliability, IEEE Internet Things J. 12 (12) (2025) 22282–22297.

[57] L. Jinying, Y. Yanping, Y. Yan, Y. Zhengqing, Broadcasting algorithm based on successful broadcasting ratio of neighbor nodes in mobile ad hoc networks, in: IEEE 17th International Conference on Communication Technology, ICCT, IEEE, 2017, pp. 965–969.

[58] P. Zenker, S. Krug, M. Binhack, J. Seitz, Evaluation of BLE mesh capabilities: A case study based on CSRmesh, in: Eighth International Conference on Ubiquitous and Future Networks, ICUFN, IEEE, 2016, pp. 790–795.

[59] C. Dandelski, B.-L. Wenning, M. Kuhn, D. Pesch, Broadcast storm problem in dense wireless lighting control networks, in: 2015 International Symposium on Wireless Communication Systems, ISWCS, IEEE, 2015, pp. 91–95.

[60] S. Pathak, A. Mani, A. Chatterjee, M. Sharma, Broadcast storm problem in software defined vehicular network, in: 2019 International Conference on Intelligent Computing and Control Systems, ICCS, IEEE, 2019, pp. 1537–1542.

[61] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, J.-P. Sheu, The broadcast storm problem in a mobile ad hoc network, in: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, 1999, pp. 151–162.

[62] B. Lin, H. Su, Experimental evaluation and performance improvement of bluetooth mesh network with broadcast storm, IEEE Access 11 (2023) 137810–137820.

[63] R. Biswas, J. Säe, J. Pirskanen, J. Lempiäinen, Reliable and low-latency communications for critical infrastructures utilizing wireless mesh networks, in: International Conference on Computing, Networking and Communications, IEEE, 2024.

[64] S.M. Darroudi, R. Caldera-Sànchez, C. Gomez, Bluetooth mesh energy consumption: A model, Sensors 19 (5) (2019) 1238.

[65] E. Giacomini, F. D'Alterio, A. Lacava, F. Cuomo, BLUES: A self-organizing BLE mesh-network paradigm for IoT environments, in: IEEE 21st International Symposium on" a World of Wireless, Mobile and Multimedia Networks"(WoWMoM), IEEE, 2020, pp. 409–414.

[66] Y.-D. Lin, S.-L. Chang, S.-H. Tao, J.-H. Yeh, Realizing and benchmarking broadcast algorithms in wireless mesh networks, Comput. Commun. 34 (10) (2011) 1169–1181.

[67] F. Gül, H. Eroğlu, Low-cost IoT mesh network for real-time indoor air quality monitoring, in: 9th International Conference on Communication and Electronics Systems, ICCES, IEEE, 2024, pp. 01–06.

[68] A. Oy, 700,000 meters in two years – Hafslund's roll-out in its final stage, 2026, [Online] Available: https://aidon.com/. (Accessed 15 May 2026).

[69] W.B. Qaim, A. Ometov, A. Molinaro, I. Lener, C. Campolo, E.S. Lohan, J. Nurmi, Towards energy efficiency in the internet of wearable things: A systematic review, IEEE Access 8 (2020) 175412–175435.

[70] J.P.A. Leon, C.L.D. Santos, A.M. Mezher, J.C. Barrera, J. Meng, E.C. Guerra, Exploring the potential, limitations, and future directions of wireless technologies in smart grid networks: A comparative analysis, Comput. Netw. 235 (2023) 109956.

[71] D. Villa, C.-K. Lin, A. Kuenzi, M. Lang, Bluetooth low energy mesh network for power-limited, robust and reliable IoT services, 2022, arXiv preprint arXiv:2208.04050.

[72] V.F. Onotu, Bluetooth low energy: A comprehensive technology analysis and role in internet of things applications, Int. J. Nat. Sci. Adv. Res. 2 (1) (2023).

[73] K.E. Law, Enhanced reliable mesh communication platforms for smart patient wristbands, in: IEEE International Conference on E-Health Networking, Application & Services (HealthCom), IEEE, 2024, pp. 1–4.

[74] Y. Zhao, L. Wang, Z. Liu, Y. Xu, F. Dang, X. Wang, H. Zhao, X. Miao, A comprehensive evaluation of bluetooth low energy mesh, in: IEEE 30th International Conference on Parallel and Distributed Systems, ICPADS, IEEE, 2024, pp. 544–551.
[75] L. Davoli, G. Ferrari, et al., Wireless Mesh Networks for IoT and Smart Cities: Technologies and Applications, The Institution of Engineering and Technology (IET), 2022.
[76] H. Habibzadeh, T. Soyata, B. Kantarci, A. Boukerche, C. Kaptan, Sensing, communication and security planes: A new challenge for a smart city system design, Comput. Netw. 144 (2018) 163–200.
[77] M.M. Martín-Lopo, J. Boal, Á. Sánchez-Miralles, A literature review of IoT energy platforms aimed at end users, Comput. Netw. 171 (2020) 107101.
[78] U. Lee, M. Gerla, A survey of urban vehicular sensing platforms, Comput. Netw. 54 (4) (2010) 527–544.
[79] F. Álvarez, L. Almon, H. Radtki, M. Hollick, Bluemergency: Mediating post-disaster communication systems using the internet of things and bluetooth mesh, in: IEEE Global Humanitarian Technology Conference, GHTC, IEEE, 2019, pp. 1–8.
[80] P. Narendra, S. Duquennoy, T. Voigt, BLE and IEEE 802.15. 4 in the IoT: Evaluation and interoperability considerations, in: International Internet of Things Summit, Springer, 2015, pp. 427–438.
[81] A. Ghobakhlou, D.Z. Al-Hamid, S. Zandi, J. Cato, A comprehensive analysis of security challenges in ZigBee 3.0 networks, Sensors 25 (15) (2025) 4606.
[82] A. Jatti, S. Deokar, J. Sayyad, A. Vibhute, L. Chaudhari, Structural health monitoring system: Vibration analysis using a ZigBee module, in: Smart Sens., CRC Press, 2025, pp. 165–179.
[83] R. Das, J.N. Bera, Self-reconfigurable partial mesh using ZigBee control board towards fail-proof and reliable home area networking, Ad Hoc Netw. 152 (2024) 103327.
[84] I. Unwala, Z. Taqvi, J. Lu, Thread: An iot protocol, in: IEEE Green Technologies Conference (GreenTech), IEEE, 2018, pp. 161–167.
[85] M. Slabicki, G. Premsankar, M. Di Francesco, Adaptive configuration of LoRa networks for dense IoT deployments, in: NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2018, pp. 1–9.
[86] X. Wang, W. Zhao, X. Niu, Low voltage user power internet of things monitoring system based on LoRa wireless technology, Energy Inform. 8 (1) (2025) 12.
[87] L. Sciullo, A. Trotta, M. Di Felice, Design and performance evaluation of a lora-based mobile emergency management system (LOCATE), Ad Hoc Netw. 96 (2020) 101993.
[88] A. Samuylov, D. Moltchanov, A. Gaydamaka, E. Lyczkowski, A. Frotzscher, F. von Schoettler, J. Pirskanen, J. Numminen, J. Salokannel, E. Llaguno, et al., Empowering near-URLLC IoT with 5G DECT-2020 NR: Current state and the road ahead, IEEE Commun. Mag. 63 (4) (2025) 130–136.