energies

Review

Wireless Battery Management Systems: Innovations, Challenges, and Future Perspectives

Zhi Cao , Wei Gao, Yuhong Fu and Chris Mi *

Department of Electrical and Computer Engineering, San Diego State University, San Diego, CA 92182, USA; zcao2@sdsu.edu (Z.C.); wgao2@sdsu.edu (W.G.); yfu@sdsu.edu (Y.F.)
* Correspondence: cmi@sdsu.edu

Abstract: With the growing adoption of battery energy storage systems in renewable energy sources, electric vehicles (EVs), and portable electronic devices, the effective management of battery systems has become increasingly critical. The advent of wireless battery management systems (wBMSs) represents a significant innovation in battery management technology. Traditional wired battery management systems (BMSs) face challenges, including complexity, increased weight, maintenance difficulties, and a higher chance of connection failure. In contrast, wBMSs offer a robust solution, eliminating physical connections. wBMSs offer enhanced flexibility, reduced packaging complexity, and improved reliability. Given that wBMSs are still in a preliminary stage, this review paper explores their evolution, current state, and future directions. A comprehensive survey of state-of-the-art wBMS technologies, including academic and commercial solutions, is elaborated in this paper. We compare wireless communication technologies like Bluetooth Low Energy (BLE), Zigbee, Near-Field Communication (NFC), Wi-Fi, and cellular networks in the context of wBMSs. We discuss their performance in terms of efficiency, reliability, scalability, and security. Despite its promising outlook, wBMSs still face challenges such as data security, signal interference, regulatory and standardization issues, and competition from the continued advancement of wired BMS technologies, making the advantages of wBMSs less evident. This paper concludes with guidelines for future research and development of wBMSs, aiming to address these challenges and pave the way for a broad adoption of wBMSs across various applications. This paper aims to inspire further research and innovation in the field, contributing to developing an industry-ready wBMS.

Keywords: wireless battery management system (wBMS); Bluetooth Low Energy (BLE); Zigbee; Near-Field Communication (NFC); Wi-Fi; cellular network; energy storage systems; battery management systems

check for updates

Citation: Cao, Z.; Gao, W.; Fu, Y.; Mi, C. Wireless Battery Management Systems: Innovations, Challenges, and Future Perspectives. *Energies* **2024**, *17*, 3277. https://doi.org/10.3390/en17133277

Academic Editor: Fangming Jiang

Received: 14 May 2024
Revised: 30 June 2024
Accepted: 2 July 2024
Published: 4 July 2024

1. Introduction

A battery management system (BMS) is primarily designed to monitor and manage the operational parameters and states of a battery pack, including voltage, current, temperature, and State of Charge (SoC), to ensure optimal performance and prevent conditions leading to premature failure or safety hazards. The BMS is becoming increasingly critical in the era of renewable energy, electric vehicles (EVs), and portable electronic devices, where batteries are the lifeblood of technology [1–5]. Especially as the adoption of EVs and hybrid electric vehicles (HEVs) grows, the demand for advanced BMS technologies becomes increasingly important [6,7]. A well-designed BMS ensures the longevity, reliability, and performance of battery packs, which are essential for these vehicles' overall efficiency and safety [8].

Figure 1 illustrates the typical composition of a BMS, which includes hardware components such as sensors, battery measurement chips, microcontrollers, and embedded software that execute various functions. Common functions of a BMS include measuring operational parameters like voltage, current, and temperature [5]; estimating SoC and State of Health (SoH) [9,10]; cell balancing [11,12]; thermal management [13,14]; and fault diagnosis and handling [15]. In EVs and HEVs, the BMS plays a vital role by monitoring and controlling various aspects of the battery pack, including charge and discharge cycles, thermal management, and fault detection. An effective BMS can enhance the overall energy efficiency of EVs and HEVs by ensuring balanced and optimized battery usage, which can extend the driving range [16,17]. Additionally, the BMS maintains vehicle safety by preventing overcharging, overheating, and other conditions that could lead to battery damage or failure [18,19].

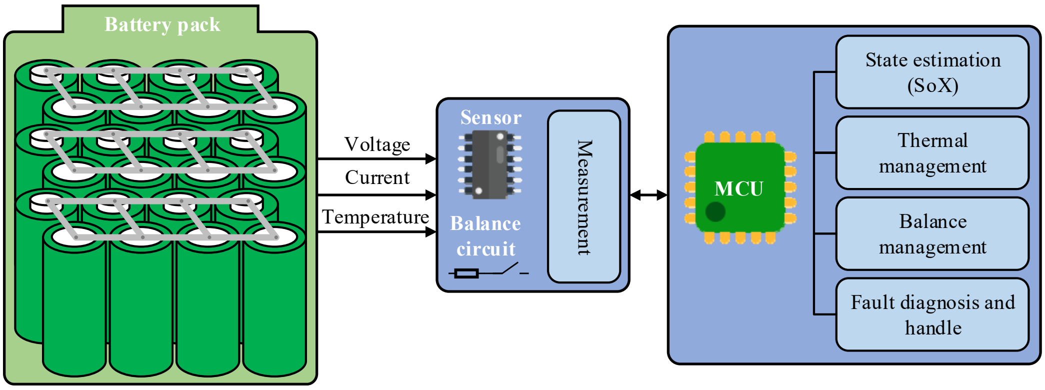


Figure 1. Function diagram of the BMS.

Over the years, BMS technology has evolved significantly, with the transition from traditional wired BMSs to wireless BMSs (wBMSs) being one of the most notable advancements in the past four years [20]. In a traditional wired BMS, each cell in a battery pack is linked by cable to a monitor, and the monitor data are transmitted via wired communication paths to the microcontroller. CAN (Controller Area Network), I2C (Inter-Integrated Circuit), and SPI (Serial Peripheral Interface) are common communication protocols adopted for the wired BMS [21,22].

As the need for higher capacity or voltage in battery packs grows, there is a corresponding increase in the number of cells, which consequently results in a greater number of wires and connectors. Although effective, wired systems add complexity, weight, and cost and reduce flexibility, particularly in configurations where space optimization and scalability are crucial [23]. According to [24], connectors take up 8% of the electrical component cost in an EV propulsion system. Additionally, they cause more physical failures, like wire breaks and poor connector contact, especially in vibratory environments [25]. These factors provide strong reasons to introduce robust wireless technology in new battery system platforms.

The general architectures of a wired BMS and a wBMS are presented in Figure 2. The wired BMS shown in Figure 2a typically includes multiple cell management units (CMUs), which are connected to a group of battery cells to monitor and control these cells; a central controller, often referred to as MCU, interfaces with CMUs via wired communication methods to manage the functionality of the system. In contrast, a wBMS, as shown in Figure 2b, eliminates physical connections and allows the CMU to interface with CMUs wirelessly.

A wBMS offers much greater flexibility in battery packaging, simplifies wiring, reduces battery package weight and volume, lowers service and maintenance costs, and enhances reliability by minimizing connection failure risks compared with wired systems [26]. For repurposing and recycling retired batteries, the simple connections and absence of a communications wiring harness simplify and accelerate the removal of battery modules compared with wired systems. The presence of a wBMS facilitates easier integration of these modules into second-life applications. Furthermore, integrating a wBMS into modern applications paves the way for intelligent, interconnected energy systems. In the context of the Internet of Things (IoT), a wBMS enables real-time monitoring and management of battery packs across various devices and platforms, thus enhancing operational efficiency and supporting predictive maintenance strategies. This seamless integration is crucial for the advancement of smart grids, autonomous vehicles, and other emerging technologies dependent on efficient and reliable energy storage solutions.

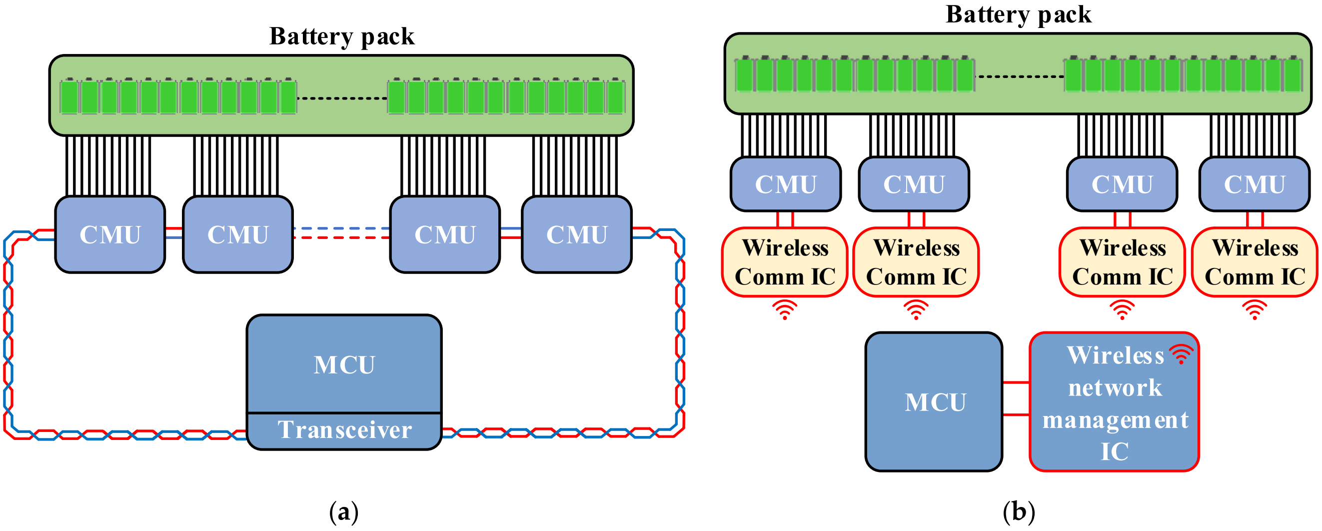


Figure 2. Architectures of wired and wireless BMS: (**a**) wired BMS architecture and (**b**) wireless BMS architecture.

Both the academic and industrial sectors recognize the potential of wBMSs, and they have already developed various wBMS solutions. In recent years, some have shown promising results. However, research into wBMSs is in its preliminary phase and is far from achieving large-scale implementation in real-world applications. Current research and development efforts have yet to address key issues fully, such as security, reliability, regulatory, and standardization challenges and competition from ongoing advancements in wired BMSs.

Only a few review papers on existing wBMS technologies have been published in recent years. Bansal et al. conducted a qualitative analysis of different wireless communication protocols for wBMSs, focusing on range, power consumption, performance, reliability, and simplicity [27], which gave valuable insights for selecting a protocol for wBMS design. Vishnu et al. explained and compared various types of wBMSs implemented at the time, discussing their operation and key findings [28]. The most recent survey presented by Samanta et al. [29] summarized existing developments and elaborated on future developments, emphasizing issues, emerging trends, and challenges. However, wireless technologies continue to evolve daily.

Therefore, this paper comprehensively reviews all state-of-the-art wBMS technologies, supplementing previous publications. In addition to emerging academic technologies, this paper also covers commercial wBMS solutions. This review elaborates on research trends and major challenges, offering guidelines for future developments and encouraging increased research efforts toward an industry-ready wBMS. As we delve further into this review, we explore the fundamental concepts, technological advancements, challenges, and future directions of wBMSs, highlighting its growing importance in powering modern applications.

2. wBMS Communication Technologies

The technological backbone of wBMSs rests on integrating advanced wireless communication techniques. Advances in wireless communication have opened new possibilities for battery monitoring without physical connections. Several successful academic attempts to design wBMSs exist. This section explains and compares these fundamental concepts and technologies.

In [28,29], the classification of wBMS communication technologies has a conceptual clarity issue: Bluetooth, Zigbee, and Wi-Fi are specific communication protocols, whereas the IoT is a broader framework that utilizes these and potentially other protocols to enable interconnectivity and intelligence across various devices and systems. IoT should not be categorized alongside specific communication technologies, as it is an overarching concept that integrates these technologies for advanced interactions and data exchange among interconnected devices. Additionally, cloud computing, referenced as CWBMS, primarily offers a model for delivering computing services—storage, processing, and analytics—over the internet and inherently relies on underlying communication technologies to connect devices and cloud infrastructure. It is not a communication technology per se but a platform that supports the scalability and accessibility of wBMS data and services.

Therefore, for more precise classification, this paper groups wireless communication technologies in terms of their communication range, and they are classified into short-range wireless communication, Wireless Local Area Network (WLAN), Metropolitan Area Network (MAN), and Wide Area Network (WAN). All these wireless communication technologies have been covered to a certain extent in the existing literature. Among them, the most popular protocols in wBMSs include Bluetooth Low Energy (BLE), Zigbee, Near-Field Communication (NFC), Wi-Fi, and cellular networks. In addition, there are other customized communication protocols for wBMSs. Figure 3 depicts the detailed classification of wBMS communication protocols.

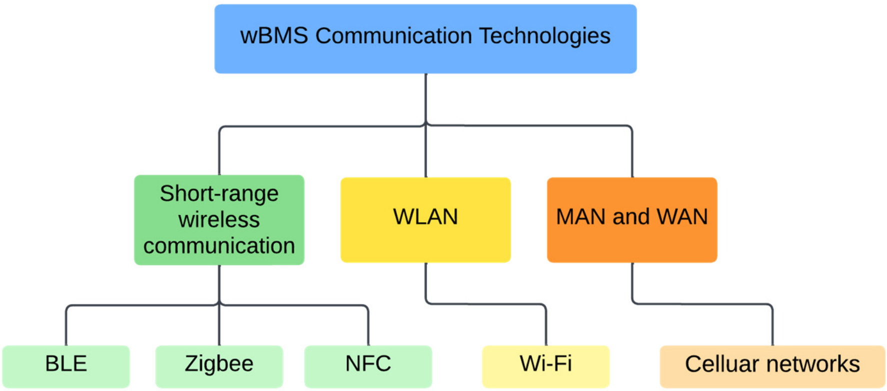


Figure 3. Classification of wireless communication technologies applied in wBMSs.

2.1. *Short-Range Wireless Communication Technologies*

These technologies are designed for short distances, typically ranging from centimeters to several tens of meters, enabling data transmission among closely situated devices.

2.1.1. Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE), introduced in the Bluetooth 4.0 core specification, is a lightweight version of traditional Bluetooth technology [30]. BLE is widely used in smartphones and is now gaining popularity in the automotive industry because of its good performance, low energy consumption, and widespread diffusion [31].

Basic Operation [32]—As shown in Figure 4, a BLE device begins by scanning for advertising signals to detect available devices and services. It can operate as either a peripheral or a central. As a peripheral, it advertises its presence and capabilities to nearby central devices, waiting for connection requests. If operating as a central, it listens for these advertisements and can initiate connections with peripherals. Upon connection, the central and peripheral devices can exchange data and utilize services like the Generic Attribute Profile (GATT) to manage their interactions. BLE supports advanced security features like encrypted communication through pairing and bonding processes to ensure secure data exchange. Devices can scan for additional connections to manage or optimize network links while connected. BLE devices also enter low-power modes during inactivity to conserve energy. Furthermore, connections are dynamically managed, allowing devices to adjust their visibility and operational status to optimize power usage and communication efficiency.

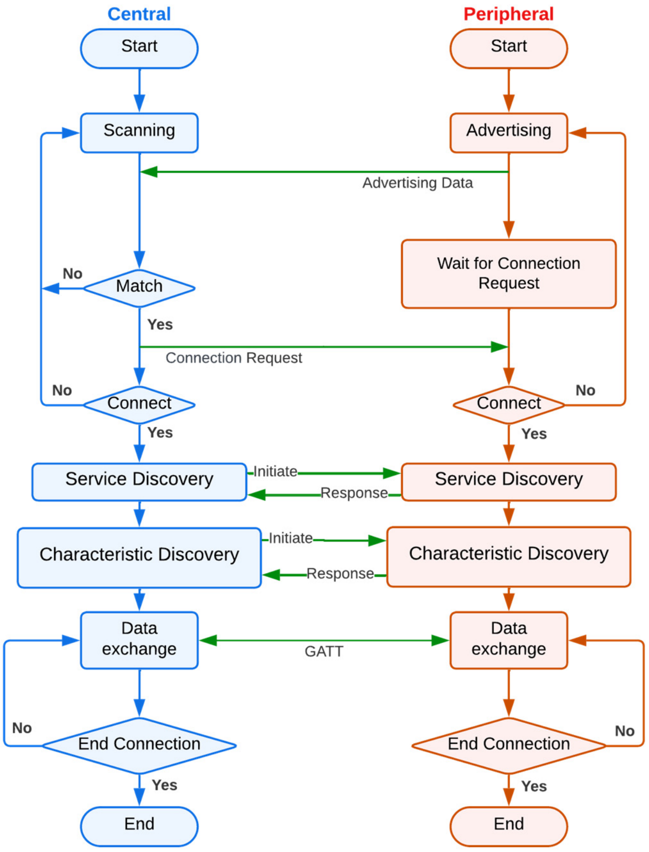


Figure 4. The flowchart of BLE basic operation.

Protocol stack [33]—The BLE protocol stack is presented in Figure 5, and it includes the following three levels: the controller, host, and application layers.

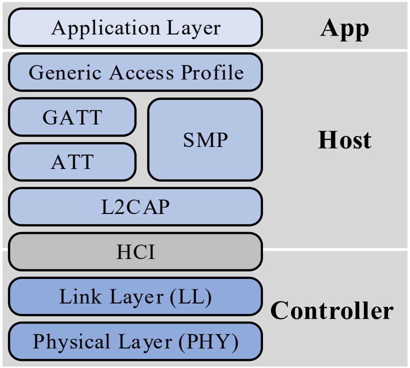


Figure 5. BLE protocol stack.

The controller is divided into two layers as follows:

- The physical layer (PHY) operates at low power and transmits data over 40 channels, each 2 MHz wide, within the 2.4 GHz unlicensed ISM (industrial, scientific, and medical) frequency band. To enhance transmission reliability in this crowded frequency range, BLE employs Frequency-Hopping Spread Spectrum (FHSS), which improves resistance to interference and multipath fading by rapidly switching the transmission frequency among the available channels. Furthermore, BLE uses Gaussian frequency-shift keying (GFSK) for modulation, which optimizes the trade-off between spectral

efficiency and power consumption. These features collectively contribute to BLE's robust performance in environments with high electromagnetic interference.
- The link layer (LL) directly interfaces with the PHY layer and manages activities including advertising, scanning, connection creation, and maintenance.

The Host Controller Interface (HCI) serves as the bridge between the controller and host, facilitating communication through various commands and actions.

The host of BLE comprises several stacked layers.

- The Logic Link Control and Adaptation Protocol (L2CAP) acts as the initial interface linking the upper layer protocols with the controller. It handles channel multiplexing, which ensures packets from the LL are directed to the appropriate upper-layer protocol during channel setup and helps differentiate among various upper-layer entities using the same protocol. From Bluetooth Core Specifications Version 5.2, L2CAP has taken on additional responsibilities like controlling the size of the Protocol Data Unit (PDU) to improve data interleaving and reduce latency. L2CAP also supports controllers with limited transmission capabilities by managing the fragmentation and reassembly of L2CAP PDUs. Furthermore, it oversees error control and meets Quality of Service (QoS) requirements.
- The Security Manager Protocol (SMP) establishes a framework that facilitates the generation and distribution of security keys among devices. It also specifies security requirements and capabilities using distinct PDU fields.
- The Attribute Protocol (ATT), used by the Generic ATT Profile (GATT) as a transport mechanism and data organizer, stores services, characteristics, and related data using a lookup table with 16-bit IDs for each entry.
- The Generic Access Profile (GAP) oversees the methods and procedures for device access, including tasks such as device discovery, establishing and terminating connections, initiating security measures, and configuring devices.
- The Generic Attribute Profile (GATT) manages data exchange over established connections by utilizing the Attribute Protocol (ATT). It comprises services, characteristics, and descriptors that are systematically arranged in the attribute table.

The application layer is the topmost interface in the BLE stack, including the interface, the application logic, and the structure within BLE devices.

Shell et al. [24] utilized a Bluegiga BLE112 Bluetooth System-on-a-Chip to transmit data between battery cell management units (CMUs) and the central controller based on the BLE 4.0 protocol. They added a memory buffer between communication channels to maintain data integrity, even in cases of temporary failures in the communication link. Upon implementation, their wBMS reliably collected data without interference or failure. However, the wBMS underwent testing with a very limited number of nodes, leaving its scalability unproven.

Rincon et al. [34,35] proposed a network architecture featuring high reliability and low power consumption, utilizing an enhanced version of the IEEE Std 802.15.4 [36] Time Slotted Channel Hopping (TSCH) Medium Access Control (MAC) mode over the BLE physical layer. They implemented the proposed wBMS network to a Renault Zoe battery, consisting of 12 modules with eight cells each. The wBMS included a master and 12 slave nodes. The test results showed that the proposed network achieved 100% reliability. Each slave node's average current consumption was below 1 mA. However, the performance in real EV driving scenarios was not verified.

Pannerselvam et al. [26] used BLE communication to replace wired communication for the BMS in a star topology. A SMART-A-BLE algorithm was developed to optimize the management of multi-peripheral BLE networks, facilitating efficient operation in both low-current and low-latency modes. It dynamically modified the connection parameters of the BLE link layer, adapting them according to the quality of the link. However, their tests of the wBMS were limited to a single master and five slave devices within a closed metallic container, simulating an automotive battery pack environment.

Ahamed et al. [37] adopted a wBMS with a BLE 5.0 architecture to enhance efficiency and safety. This low-power device supported the maintenance of ad hoc connections. Besides offering a 1 Mbps data rate, it employed three advertising channels to detect other devices in the 2.4 GHz band. It utilized an Adaptive Frequency Hopping algorithm to minimize interference, with an activation period ranging from 0.6 to 1.2 ms. The data rate of this technology was lower compared with standard Bluetooth, making it ideal for devices that transmit data intermittently.

BLE is characterized by its minimal power consumption, which is ideal for systems powered by batteries. Nonetheless, for the BMS of large-capacity battery packs, BLE communication falls short because of its limitations in handling the high volume and speed of data transfers necessary for safe and reliable battery management. Furthermore, BLE is sensitive to channel noise [38], which could hinder it from meeting the reliability rate required for safety and automotive standards when considering data throughput for BMSs.

2.1.2. Zigbee

Zigbee is a wireless communication technology that offers low-power, low-data rate, short-range communication. It operates on the IEEE 802.15.4 standard and is designed to facilitate reliable, cost-effective, and energy-efficient wireless communication over short distances.

Basic Operation [39]—As displayed in Figure 6, a Zigbee device begins by searching for a network to join or deciding to create a new one. The device follows different procedures based on its role as a coordinator, router, or end device.

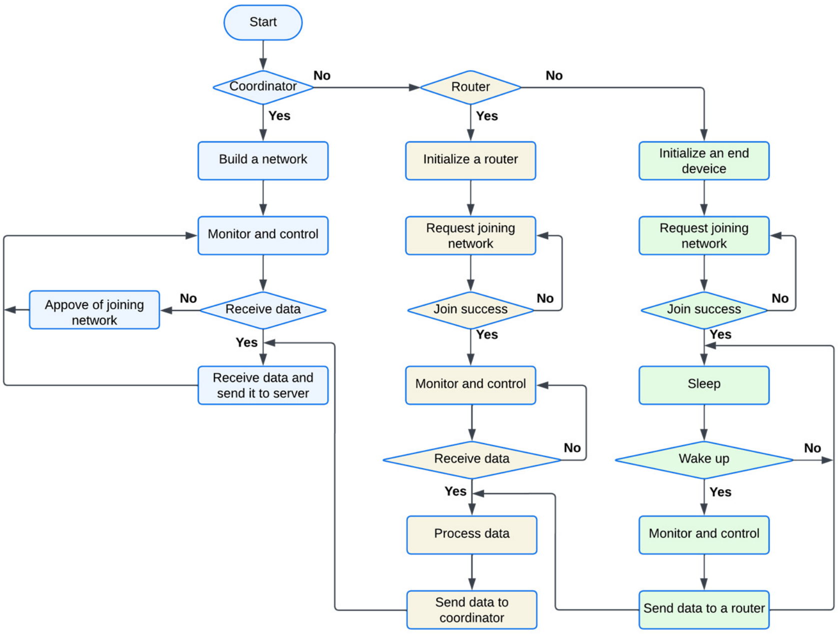


Figure 6. The flowchart of the Zigbee basic operation [39].

The device selects to join an existing network based on beacon signal strength and parameters such as network ID and channel. After choosing a network, it sends an association request to the network's coordinator or router.

If the device is set as a coordinator when no suitable network exists, it establishes a new network, assigns itself a network ID, selects an operating channel, and begins broadcasting beacons to allow other devices to join.

A router joins an existing network and extends the network's coverage area by acting as an intermediate transmitter, allowing end devices to connect indirectly to the coordinator through the router.

After successfully joining a network, the Zigbee device can participate in network communication, sending and receiving data as per the application's needs. It supports complex mesh networking, enabling devices to relay messages through intermediate nodes if direct communication is not feasible. Moreover, Zigbee implements robust security measures, including encryption and authentication, to ensure secure data exchanges within the network.

To conserve energy, Zigbee devices can enter sleep mode when inactive. They wake intermittently to check communications or transmit data. The device remains ready to exit sleep mode and rejoin active communication upon receiving specific signals or at pre-defined intervals, ensuring it remains synchronized with the network's activity while conserving energy.

Protocol stack—The Zigbee protocol stack is displayed in Figure 7, and it is composed of several layers that enable its functionality and flexibility. The most critical layers include [40]:

- Physical Layer (PHY): This layer operates on the 2.4 GHz frequency band globally, along with additional bands like 868 MHz in Europe and 915 MHz in North America. It uses direct sequence spread spectrum (DSSS) for modulation, which helps reduce interference and improve signal integrity across multiple channels in noisy environments.
- Media Access Control (MAC) Layer: The MAC layer ensures secure and organized communication across the physical radio, managing spectrum access, collision avoidance, and error detection and retransmission. The PHY layer and the MAC sub-layer are specified by the IEEE 802.15.4 standard as the foundational layers.
- Network (NWK) Layer: This layer is fundamental to Zigbee's effectiveness in creating large-scale mesh networks. It manages routing, maintaining, initiating the network, and ensuring data reaches its destination across multiple nodes. The network layer in Zigbee is highly optimized for low-power operation and is capable of self-healing and self-organizing, which enhances network reliability and stability.
- Application Layer: This layer is composed of three sub-layers—the Application Support Sub-layer (APS), the Zigbee Device Objects (ZDOs), and the application framework itself. The APS provides the interface between the network and application layers, handling data transmission tasks and managing binding tables that link devices together. The ZDO handles device management and security, covering aspects like device roles, addressing, and the discovery of other devices within the network. Finally, the application framework hosts user applications, providing standard profiles for specific device controls.

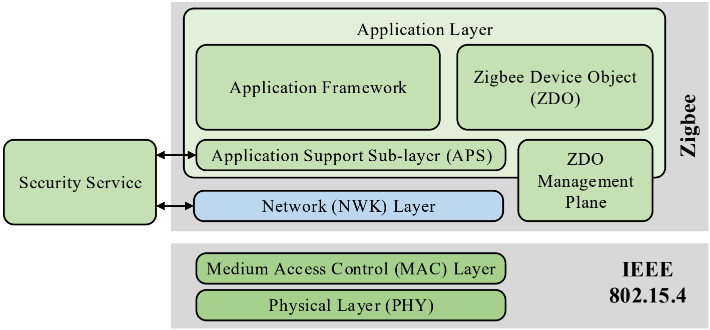


Figure 7. Zigbee protocol stack.

Vallo [41] investigated a wBMS using a ZigBee module to transmit data and commands between master and slave modules; however, the system faced limitations on the maximum number of batteries connectable.

Rahman et al. [42] designed a wBMS utilizing the ZigBee communication protocol and a point-to-point wireless topology. Microcontrollers and wireless modules collected data from multiple sensors and then transmitted this information to display devices. The wBMS effectively reduced massive wiring issues. However, the paper primarily addressed cell balancing and thermal management, offering limited analysis of the ZigBee-based wBMS.

Although Zigbee offers advantages such as low cost, low power consumption, and simplicity in implementation, its application in the wBMS remains limited because of its restricted data transfer capacity [29].

2.1.3. Near-Field Communication (NFC)

NFC is a short-range wireless communication technology that uses magnetic fields instead of electric fields for data transmission. It offers a simple way of wireless data transfer by bringing devices within a few centimeters of each other. An NFC device has very low power consumption as it does not require a power source and is activated only when near a powered NFC device. In addition, NFC has high security because it facilitates short-range communication, which is challenging to exploit from a distance.

Basic Operation [43]—As demonstrated in Figure 8, NFC devices can operate in three different modes including the following:

- Reader/Writer Mode: In this mode, self-powered active devices initiate communication by energizing passive devices through energy harvesting. They detect, initiate, and maintain power supply to passive devices during communication. Once connected, passive devices respond to active devices using "load modulation", a technique that modulates the existing electromagnetic field to transmit data. This mode is critical for applications like reading information from NFC tags embedded in products.
- Peer-to-Peer Mode: In this mode, both participating devices are active, each equipped with its power source. The initiator establishes the electromagnetic field and begins communication, while the second device is the target. Communication between the two devices uses Amplitude Shift Keying (ASK) modulation exclusively, facilitating a robust data exchange for transferring information like contacts, photos, or other media among smartphones or between a smartphone and another NFC-enabled device.
- Card Emulation Mode: Combining the principles of the previous modes, card emulation enables a passive device like a smartphone to function as a traditional NFC card. This is particularly useful in transactional applications where the smartphone emulates an NFC payment card or transit pass. In this mode, the passive device initiates communication without power, enabling interactions with powered readers like payment terminals or access control systems.

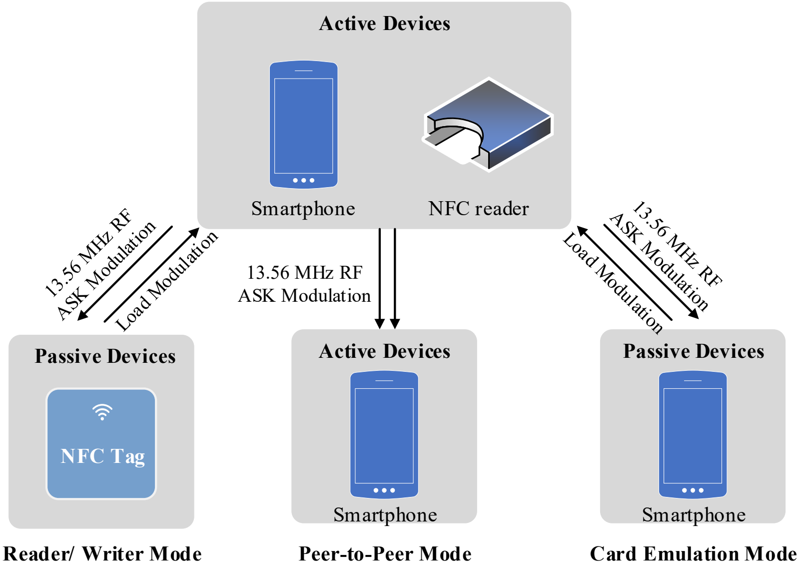


Figure 8. NFC operation modes [44].

Protocol stack—Each operating NFC mode has its communication interfaces and standards. The key layers of the NFC protocol stack include the following:

- Physical Layer (PHY) and Radio Frequency Interface (RFI): NFC operates within the 13.56 MHz frequency band. The PHY layer manages signal modulation and demodulation using Amplitude Shift Keying (ASK) to encode data. The RFI oversees the activation and deactivation of the radio frequency field, controlling the timing and ensuring accurate signal reception and processing between the initiator and target.
- Data Link Layer (DLL): Responsible for error detection and correction, the DLL ensures data transmission integrity, using protocols to detect and retransmit data if errors occur. This layer is crucial in environments prone to data corruption from interference.
- Protocol Layer: This layer manages the communication protocols that define how devices interact with each other in various NFC modes. It includes the NFC Data Exchange Format (NDEF), which standardizes the structure of messages exchanged among devices. The protocol layer ensures that NFC devices can interact seamlessly, regardless of the manufacturer.
- Transaction Layer: Critical for applications requiring secure communication, like payment systems, this layer manages secure transaction setup and execution, utilizing encryption and secure channel protocols to safeguard data and ensure communication privacy and integrity.
- Application Layer: The application layer includes the software applications that utilize NFC technology. These applications range from simple data exchange applications to complex payment and ticketing systems. The application layer interfaces with the underlying NFC technology to deliver a seamless user experience for various use cases.

Basic et al. [45] proposed a wBMS architecture using NFC technology for battery module cells' sensor readout. An active NFC reader was integrated into the standard battery cell controller. The battery sensors were connected to the designated passive NFC device, thereby avoiding extra connections or energy use. Security and data handling were managed by an extra microcontroller unit. These components, along with the battery cell controller, constituted a new overall control block. This setup allowed the BMS to perform security checks on recorded data efficiently, maintaining its fundamental functionality with minimal overhead. In [46], the authors expanded on this work by merging two distinct designs, where one focused on internal sensor readouts from battery packs, while the other dealt with external status and diagnostic outputs in the design of BMS systems. The feasibility of their approach was confirmed through comprehensive testing. The system achieved a throughput of 264 bytes/s for reading 8 bytes of measurement data, along with low power consumption. However, further optimization in both hardware and software is necessary for high sample rates, an increased number of devices, antenna design, and customized control at the link layer.

2.2. WLAN Technologies

This technology includes wireless communication within a local area network, covering distances from tens to hundreds of meters.

Wi-Fi operates under the IEEE 802.11 standards [47]. It can support high-throughput networking and is compatible with many types of encryption and network security protocols, making it ideal for both public and private network environments.

Basic Operation [48]—As depicted in Figure 9, a Wi-Fi station scans available channels to identify active network broadcasting beacons. It selects a network to connect to, operating either in ad hoc or infrastructure mode. In infrastructure mode, the station first verifies its identity with the access point (AP)—a process known as authentication—followed by establishing a connection, known as association. If Wi-Fi Protected Access (WPA) security protocols are active, an additional complex authentication step, such as a four-way handshake, is required before the station can fully participate in the network. Wi-Fi supports various levels of Quality of Service (QoS), ranging from "best effort" (basic service) to "prioritized" (higher priority for certain data) and, in some cases, even "guaranteed" services for critical data transmission. Once connected, stations may continue to monitor for new networks, and if a stronger signal is found, they may switch networks to maintain optimal connectivity. This roaming capability allows stations to transition among networks sharing a common distribution system seamlessly, enhancing user mobility. Also, stations can enter a sleep mode to conserve power when not transmitting data actively. After completing operations in infrastructure mode, a station will formally disconnect from the AP by de-authenticating and disassociating.

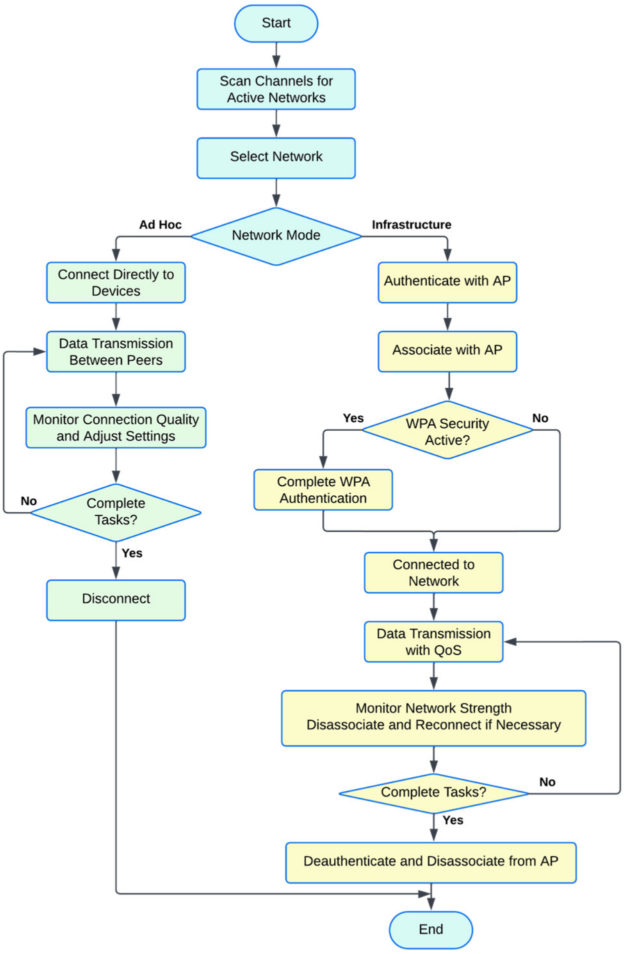


Figure 9. The flowchart of Wi-Fi basic operation.

Protocol stack—The Wi-Fi protocol stack is shown in Figure 10, which is comprised of several key layers [49] including the following:

- Physical Layer (PHY): Depending on the specific Wi-Fi version (e.g., 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac), the physical layer operates at different frequencies, primarily 2.4 GHz or 5 GHz. The choice of frequency band affects the balance between range and data rate. The PHY layer uses various modulation techniques, such as Quadrature Amplitude Modulation (QAM) or Orthogonal Frequency-Division Multiplexing (OFDM), to optimize data transfer rates and bandwidth efficiency.
- Data Link Layer: This layer includes the Media Access Control (MAC) and Logical Link Control (LLC). The MAC Layer manages access to the radio frequency channel, frame formatting, data encryption, and addressing using protocols like WPA and WPA2. It is crucial for securing the network and maintaining Quality of Service (QoS). The LLC Layer provides interface and flow control between the MAC sub-layer and the network layer.

- Network Layer: Wi-Fi does not define network layer functionalities, but it supports IP-based protocols such as IPv6, which enhance routing capabilities across complex networks with minimal power usage.
- Transport Layer: The transport layer offers end-to-end data transfer through lightweight protocols such as UDP, which is preferred for its simplicity and low overhead.
- Application Layer: The application layer includes user-end software that interfaces with Wi-Fi hardware, providing functionalities like network discovery, connection management, and user authentication. This layer enables the applications to utilize the network efficiently and securely.

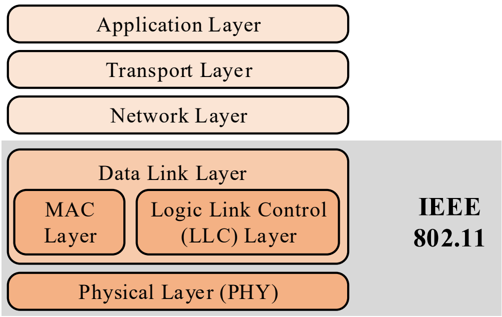


Figure 10. Wi-Fi protocol stack.

Ricco et al. [50] used Wi-Fi modules for their smart battery pack system. In their system, slave boards were connected to the terminal of battery cells, switches, and a CC3200MOD Wi-Fi module. The master board included a Snickerdoodle board equipped with a Xilinx ZYNQ system-on-chip and a Texas Instruments WiLink8 RF transceiver module for Wi-Fi communication. The WiLink8 transceiver managed the Wi-Fi communication stack's physical layer, interfacing with the ZYNQ via an SDIO interface. A pre-built Linux image running on the ZYNQ managed the upper layers of the Wi-Fi protocol Simultaneously, the Hostapd user space daemon handled the functionality of the access point (AP) and managed the Wi-Fi network that it created. Huang et al. [51] adopted a similar wBMS configuration for smart battery management. However, these papers primarily focused on cell balancing and fault tolerance and put minimal emphasis on wireless data transmission. Moreover, Zebrowski et al. claimed that Wi-Fi's message overhead is considered redundant in the context of wBMSs [52].

2.3. MAN and WAN Technologies

Cellular networks are wireless communication technologies designed for wide area coverage, supporting mobile voice and data services over large geographic areas. These networks consist of cells, each served by at least one fixed-location transceiver or cell site/base station. This cellular structure enables extensive coverage and capacity, accommodating numerous users across cities, countries, and continents.

Figure 11 presents a simplified diagram of cellular network architecture [53,54]. The mobile device accesses the Internet via base stations and a core network. Below the IP layer, the specialized protocol stack for cellular networks encompasses protocols for both the data plane and control plane. The data plane is primarily responsible for delivering user data and voice communications, whereas the control plane manages the exchange of signaling messages to enable content delivery. Physical and link-layer protocols define device communication with base stations for effective radio access. Above these, control-plane protocols defined by the cellular network include Radio Resource Control (RRC), which manages the allocation of radio resources and managing connections; Mobility Management (MM), which deals with updating locations and supporting mobility; and Session Management (SM), which establishes and sustains voice and data sessions. On most commercial phones, the operating system (OS) and applications have restricted access to detailed, cellular-specific information during runtime, as it is embedded within the hardware chipset. The OS accesses elementary cellular functions and states via the standard radio interface layer library, which offers only broad-level information. Additionally, the OS simplifies and relays a portion of these data to applications through the system APIs.

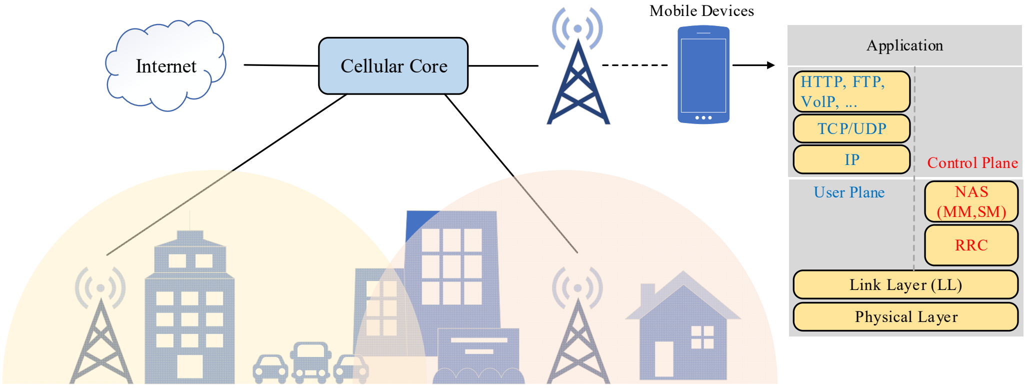


Figure 11. Cellular network architecture and protocol stack [53].

Adopting cellular networks facilitates the development of cloud-based wBMSs, which are ideal for distributing BMS modules across wider areas. Cloud server access can also enhance computational power and data storage for running sophisticated algorithms that would be unfeasible on the resource- and process-limited microcontrollers typically used in BMS field operations.

Lohar et al. [55] utilized a quad-band GSM/GPRS module to develop a wBMS, with sensors continuously monitoring voltage levels and wirelessly transmitting data to a central monitoring station. They efficiently tested the wBMS, achieving accurate SoC calculations.

Faika et al. [56] introduced a novel distributed wireless IoT network tailored for a decentralized wBMS. Their design featured a lightweight IoT protocol, a rapid and autonomous leader election algorithm for data aggregation, and external system communications, along with an IoT gateway to facilitate cloud support services. Cell data, temporarily stored in an IoT node's memory, was securely transmitted to the cloud database via 4G/5G LTE networks through an IoT gateway. To enhance the communication and data security of the wBMS from malicious cyber-attacks, they further integrated blockchain technology into their system [57]. The designed IoT network was intended to simplify battery systems, making them more distributed, scalable, reliable, and cost-efficient.

The rollout of 5G and upcoming 6G networks, featuring high speed and low latency, offers more reliable and responsive wireless communication, enabling real-time data transfer and control for the BMS [58]. However, these technologies come with relatively high power consumption and costs.

2.4. Other Technologies

Lee et al. proposed one of the pioneering works that combines BMS with wireless design, using custom chips and protocols [23]. Their study introduced the WiBaAN protocol, operating on the 900 MHz band with data rates up to 1 Mbit/s, enabling direct communication between numerous battery cells and the primary BMS controller. However, despite its novelty at the time of publishing, the absence of recent research updates on this technology might limit its application in contemporary BMS developments. Nevertheless, their work remains significant, laying the groundwork for future advancements in wBMS technology.

2.5. Summary of Wireless Communication Technologies

Table 1 provides a comprehensive comparison of the communication technologies discussed above [59–62]. The selection of wireless communication technology for a wBMS should consider several factors, such as efficiency, reliability, scalability, and security, as well as the specific environmental conditions and system architecture.

Table 1. Comparison of different wBMS communication protocols.

Technology	Frequency	Data Rate	Range	Latency	Power Consumption	Cost	Suitability
BLE	2.4 GHz	1 to 2 Mbps	Up to 100 m	Low	Low	Low	• Small- to medium-sized battery systems. • Supports mesh networking in the latest versions.
Zigbee	2.4 GHz	Up to 250 kbps	Up to 100 m	Low	Low	Low	• Small data packets. • Supports mesh networking, enabling robust and extendable communication networks.
NFC	13.56 MHz	Up to 424 kbps	Up to 10 cm	Low	Very Low	Low	• Instant pairing and data transfer. • Enhances security because of the short communication range.
Wi-Fi	2.4 GHz, 5 GHz	0.1 to 600 Mbps	Up to150 m	Low to Medium	Medium	Medium	• Applications requiring frequent data uploads to the cloud or central servers. • High data rate, supports direct internet connectivity.
Cellular networks	Cellular bands	Up to several hundred Mbps	Several kilometers	Medium	High	High	• Applications requiring uninterrupted connectivity across different regions. • Wide-area coverage.

2.5.1. Efficiency and Power Consumption

BLE is highly efficient in power consumption and suitable for small- to medium-sized networks. Zigbee offers low power consumption and is effective for devices that require long battery life. NFC has the highest power efficiency because of its passive nature in certain modes but is constrained to very short-range communications.

Wi-Fi and cellular networks consume more power but are necessary for applications that demand high data rates and longer ranges, such as cloud connectivity for data analysis and remote management.

2.5.2. Reliability

BLE and Zigbee both support mesh networking, which enhances the reliability of network communications through multiple paths among devices, which is essential in environments with potential physical and electromagnetic interference. Wi-Fi and cellular networks offer strong connections over longer distances. Cellular networks offer carrier-grade reliability in diverse environments, which is ideal for critical BMS applications needing consistent connectivity. NFC’s reliability is high in its specific use case of close-range communication, ensuring a stable connection at distances of just a few centimeters.

2.5.3. Scalability

Zigbee excels in scalability, supporting thousands of nodes in a single network, which is ideal for large-scale BMS applications. BLE is suitable for small to medium networks. Wi-Fi and cellular networks can scale well but may require more sophisticated network management and infrastructure to handle a large number of BMS devices efficiently. NFC is not suitable for scalable applications because of its inherent one-to-one communication model.

2.5.4. Security

BLE, Zigbee, Wi-Fi, and cellular networks provide advanced security features, including encryption and authentication mechanisms, essential for securing BMS communications. Selecting among these technologies requires consideration of the specific security needs and potential threats within the deployment environment. NFC ensures secure communication because of its short range, which naturally limits the potential for eavesdropping and other attacks.

2.5.5. Environmental Conditions and System Architecture

Zigbee and BLE, with their mesh networking capabilities, adapt well to environments with physical obstructions and interference, making them suitable for complex BMS architectures. Wi-Fi and cellular networks are better suited for environments where BMS components are spread out over larger areas, offering longer-range communications. NFC is used explicitly in environments requiring close device proximity.

According to the discussion above, Figure 12 shows the evaluation of the different wireless communication technologies in wBMSs in six dimensions.

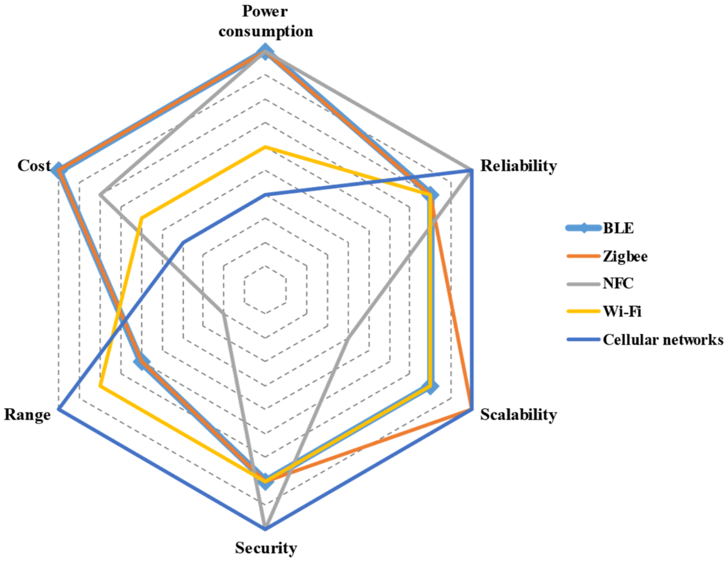


Figure 12. Comparison of different wireless communication technologies in different factors.

2.6. Comparison to Wired BMSs

The previous sections discuss various wireless communication technologies applied in wBMSs. To better understand the current state and potential of wBMSs, it is essential to compare them to the traditional wired BMS. This comparison highlights the technical, operational, and economic differences between wired and wireless BMSs, shedding light on the advancements and challenges that wBMSs currently face. Table 2 summarizes the advantages and disadvantages of wired and wireless BMSs from different aspects.

Wired BMSs are highly mature, widely used, and have well-established standards. In contrast, wireless BMSs are in an emerging stage, with lower adoption in commercial products and lacking universal standards, relying mainly on proprietary protocols from different companies.

Wireless BMSs have several advantages over wired BMSs. By eliminating physical connections, wireless BMSs simplify system connections, reduce weight, and offer higher flexibility and greater scalability compared to wired BMS, making it easier from installation to maintenance.

In terms of reliability, wired BMSs can suffer from connection failures but offer high data reliability due to direct physical connections [58]. Wireless BMSs improve reliability by reducing connection points, but data reliability can be affected by signal interference. In terms of security, wired BMSs provide a fully secure system, whereas wireless BMSs may be vulnerable if not properly secured. Wired BMSs generally have lower power consumption while wireless BMSs require more power for communication modules. In terms of cost, wired BMSs may have lower initial costs, whereas wireless BMSs require higher initial investment. However, repurposing and reusing batteries with wired BMSs can be challenging, whereas wireless BMSs make this process easier. As a result, the overall cost of wireless BMSs throughout their lifetime may be reduced.

Table 2. Comparison of wBMS and wired BMS.

Technology	Wired BMS	Wireless BMS
Technical maturity	+ Highly mature + Well-established standards	− Emerging − Lack of universal standards
Weight	− Increased due to cables and connectors	+ Reduced due to eliminating physical connections
Complexity	+ High due to extensive wiring	− Low with reduced wiring
Flexibility	− Limited	+ High adaptability
Scalability	− Limited scalability	+ Highly scalable
Reliability	− Prone to connection failures + High data reliability due to direct physical connection	+ Improved reliability with fewer connection points − Data reliability challenges due to signal interference
Security	+ Fully secure system communication	− Potentially vulnerable if not properly secured
Installation	− Complex and time-consuming	+ Fast and simple installation
Maintenance	− Complex	+ Easy
Power consumption	+ Lower	− Higher for communication modules
Cost	+ Potentially lower initial costs	− Higher initial investment
Repurpose and reuse	− Difficult	+ Easy

+ indicates a relative advantage in the specified criterion. − indicates a relative disadvantage in the specified criterion.

Overall, both wired and wireless BMSs have their respective strengths and weaknesses. Wired BMSs offer maturity, reliability, and lower power consumption, making them suitable for well-established applications. On the other hand, wireless BMSs provide flexibility, scalability, and easier maintenance, making them a promising option for future advancements and applications where these attributes are critical. Understanding these differences can help guide the advancement of wireless BMS technologies.

3. State-of-Art Commercial wBMS Solutions

3.1. Commercial wBMS Product Comparison

Some companies have introduced several wBMS solutions to the market, and their specifications are summarized in Table 3.

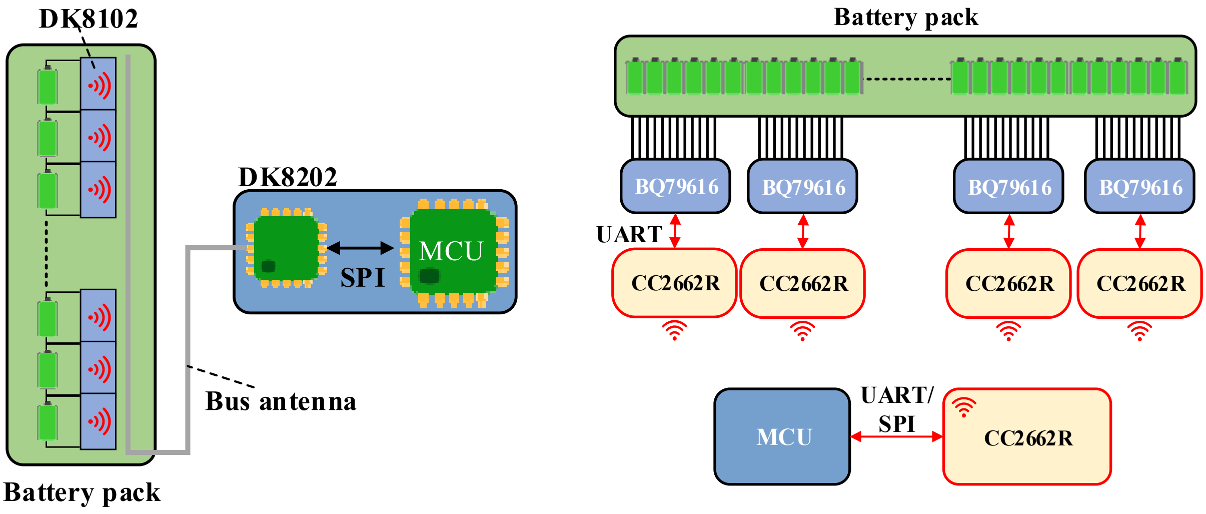
The technical schemes among these commercial products have several differences in terms of the following aspects:

- Configuration of the cell measurement unit (CMU).

TI, ADI, and NXP extend existing CMUs by connecting them with a dedicated wireless communication IC. Figure 13b shows that each CMU monitors multiple cells and links to one slave communication node. The slave nodes relay sensor data from the battery cell over the air to the master node, and the master node forwards these data to the BMS controller. Dedicated wireless communication ICs configure the network of nodes and manage the communications protocol. As displayed in Figure 13a, Dukosi integrates RF communication directly into each CMU, assigning one CMU per cell to enhance integration. However, this approach may limit scalability compared with others, as each CMU connects to only one cell.

Table 3. Comparison of different commercial wBMS technologies.

Company	Analog Devices (ADI)	Texas Instruments (TI)	NXP Semiconductors	Dukosi
ICs	Master node: ADRF8850 Slave node: ADRF8800	Master node: CC2662R Slave node: BQ79616+ CC2662R	Master node: 2 × KW38 + MPC5744P Slave node: MC33771 + KW37	Master node: DK8202 Slave node: DK8102
Protocol	SmartMesh	TI SimpleLink wBMS protocol	Optimized BLE 5.0	Dukosi C-SynQ
Network topology	Mesh	Star	Star and Mesh	Star
CMU configuration	Standalone	Standalone	Standalone	2-in-1
Max nodes	-	Up to 100	Up to 32	Up to 220
Operating frequency	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz
Range	Far	Far	Far	Near
Data rate	1 Mbps, 2 Mbps	Up to 1.2 Mbps	Up to 2 Mbps	2 Mbps
Security features	Hardware accelerator supporting AES-128, AES-256, ECC-256, and SHA-256 True random number generator (TRNG)	Hardware acceleration supporting AES-128/256, ECC, RSA-2048, SHA-2. TRNG	AES-128 TRNG LE Secure Connections	-



(**a**) (**b**)

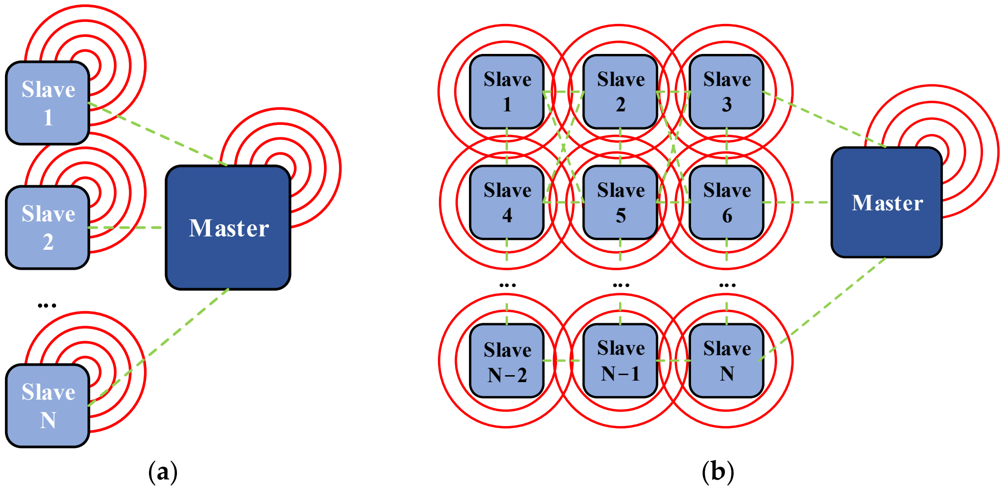
Figure 13. Architectures of two different commercial wBMSs: (**a**) Dukosi's wBMS architecture and (**b**) TI's wBMS architecture.

- Communication protocol.

Most of these commercial products utilize proprietary communication protocols tailored specifically for wBMSs. In TI, ADI, and NXP solutions, slave nodes are located within the battery pack, and the master node can be positioned at a distance, with data transmitted wirelessly, necessitating ongoing security investments to prevent unauthorized remote access. Conversely, Dukosi's protocol has a significantly shorter communication range, described as "Near-Field" Communication. Dukosi uses a single bus antenna originating from the master node to loop through each CMU inside the battery pack, enabling close yet contactless data exchange with slave nodes. Compared with other wBMS solutions, Dukosi's wired-like connection can effectively mitigate typically harsh automotive electromagnetic (EM) environments, and it is naturally immune to remote communication hacks because of its very short communication range coverage. Moreover, Dukosi's communication protocol ensures precise control over the RF channel at each point, eliminating the need for multiples and maintaining consistent latency between all nodes and CMUs.

- Network topology.

The network topologies of these products vary: ADI's wBMS uses a mesh network, TI and Dukosi opt for a star network, and NXP's wBMS can switch between star and mesh networks. Two network topology diagrams are shown in Figure 14. In a star network, all slave nodes are directly connected to a master node. The star connection simplifies management and enhances reliability, as the failure of a single slave node does not impact others. However, the master node forms a single point of failure and potential performance bottleneck.



(**a**) (**b**)

Figure 14. Different network topologies: (**a**) a star network and (**b**) a mesh network.

Conversely, a mesh network topology has nodes interconnected directly in a full or partial mesh, allowing data to transmit in multiple paths from one node to another. This increases reliability and flexibility, with data still reaching their destination even if some paths or nodes fail. While offering improved redundancy and self-healing capabilities, mesh networks are more complex to configure and manage.

- Power consumption.

Figure 15 presents the increase in power consumption of slave nodes as their number grows. NXP's system exhibits the lowest power consumption, while TI's has the highest. The difference becomes more evident as the number of cells increases. More ICs are required in Dukosi's system with the same number of cells being monitored because each CMU can only monitor one battery cell while other CMUs can simultaneously monitor multiple cells. Despite this, Dukosi's system displays moderate power consumption. It is important to note that the power consumption of ICs depends on their configurations, and this analysis considers only the typical power consumption in active mode. The power consumption of slave nodes for TI and NXP includes both communication ICs and CMUs; in their configurations, the communication ICs are standalone from CMUs.

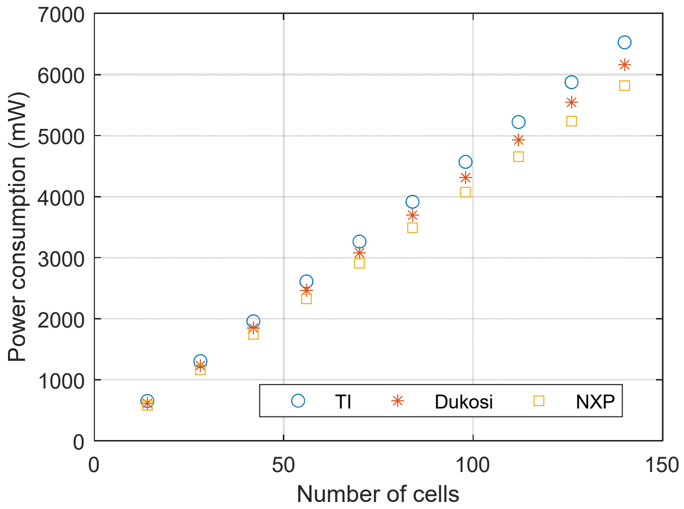


Figure 15. Power consumption of slave nodes with different commercial wBMSs.

3.2. Real-World Examples and Case Studies

These commercial wBMSs are currently in a tentative development stage and few successful real applications have been reported. General Motors (GM) pioneered the large-scale adoption of a wBMS for its Ultium EV platform [63]. GM developed its wBMS using a wireless communication system from ADI. In this wBMS, modules have the capability to interact with each other and with vehicle systems, facilitating real-time health monitoring and ongoing balancing. GM reported that its wBMS cut down the amount of wiring in Ultium battery packs by as much as 90%, which lightened the pack, enhanced the vehicle's energy efficiency, and extended the driving range achievable with the same battery capacity [63]. Also, the wBMS improved the scalability of battery packs across various vehicle types and sizes. Additionally, GM has prioritized security and resilience in its design from the outset, with a strong emphasis on cybersecurity measures extending to the wBMS.

4. Challenges and Potential Countermeasures

Currently, the implementation of wBMSs is still facing some barriers and challenges. This section outlines these major challenges and discusses corresponding solutions. An overview of various open challenges and their countermeasures is given in Figure 16.

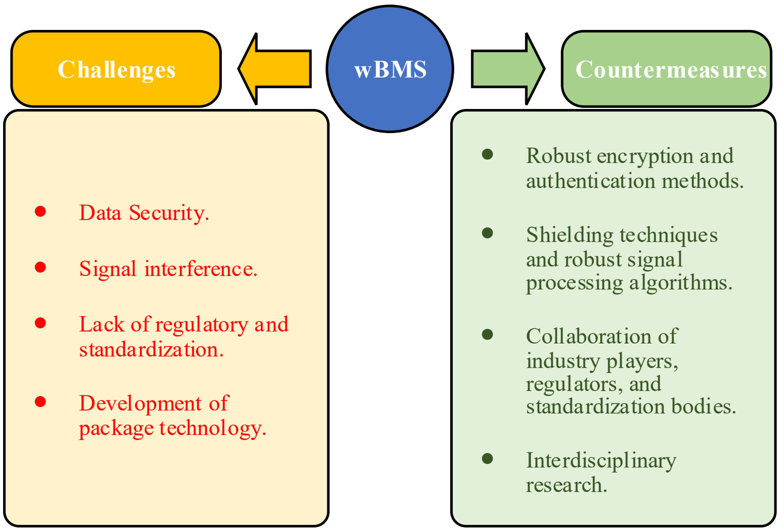


Figure 16. An overview of wBMS challenges and countermeasures.

4.1. Data Security

wBMSs are susceptible to cybersecurity threats such as eavesdropping, unauthorized access, data breaches, and cyber-attacks on the communication network [64–66]. Several papers have examined the security risks and underlying challenges posed by the fundamentally open nature of wireless communications [33,67–69].

More effort should be put into developing robust encryption and authentication methods to guarantee security. Furthermore, blockchain technology is promising for the cybersecurity enhancement of wBMSs, with some research already underway [57,70].

4.2. Signal Interference

Most wBMS communications operate at a 2.4 GHz frequency. Despite different wireless protocols, signal interference can still exist. Without proper management, wBMS wireless signals could interfere with other electronic devices or become vulnerable to external interference. Lee et al. [71] observed that RF jamming significantly compromised the performance of a wBMS, resulting in reduced throughput and heightened packet errors. Nevertheless, encasing the wBMS in metallic materials was shown to enhance system performance and diminish interference.

Therefore, countermeasures like improved shielding methods or advanced signal processing algorithms should be implemented to boost the resilience of wBMSs against signal interference.

4.3. Regulatory and Standardization Issues

Standardization can mitigate technical and financial constraints. Currently, companies use various communication protocols and architectures, leading to inconsistencies. To the authors' knowledge, there has yet to be a standardization for wBMS technology. The lack of universal standards for wBMSs limits interoperability among components from different manufacturers, constraining the flexibility and scalability advantages that wireless systems typically offer. Moreover, though wBMSs would bring many advantages for the lifetime management of batteries and echelon use of second-life batteries, the need for more regulation and standardization would pose barriers to this progress.

To address this challenge, industry players, regulators, and standardization bodies should collaborate to establish clear guidelines and standards. This collective effort is essential for ensuring the safe and efficient use of wBMSs and realizing their full potential.

4.4. Development of Package Technology

The packaging technology of battery packs has been evolving in recent years. The integration level within the battery pack has been improved, and the connection between the slave and master nodes has been reduced to less wire harness usage. Furthermore, as more integrated battery packages like CTP (Cell-to-Pack) [72], CTC (Cell-to-Chassis) [73], and CTB (Cell-to-Body) [74], become mainstream, the modular approach is gradually being replaced. Consequently, the distinct benefits of wBMSs for the echelon usage of retired battery packs at the module level are becoming less evident.

The ongoing evolution of battery technologies introduces uncertainties for wBMSs, necessitating comprehensive and interdisciplinary research in this area.

5. Conclusions

This paper presents a comprehensive up-to-date review of wBMSs from both academic and industry perspectives. The advent of wBMSs marks a major advancement in battery management technology. By offering enhanced flexibility, reduced complexity, and improved reliability, wBMSs are set to play a crucial role in the future of energy storage, electric mobility, and beyond.

5.1. Key Findings

- Technological evolution: wBMSs have evolved with the development of advanced wireless communication technologies like BLE, Zigbee, NFC, Wi-Fi, and cellular networks. Each technology offers unique benefits and challenges in terms of efficiency, reliability, scalability, and security.
- Academic and commercial developments: Both academic research and commercial solutions have demonstrated promising results. Academic efforts have focused on enhancing the efficiency and reliability of wBMSs, while commercial products are beginning to achieve practical implementation, as evidenced by General Motors' Ultium platform.
- Comparison with wired BMSs: Compared with traditional wired BMSs, wBMSs offer several advantages, including reduced weight, enhanced flexibility, and easier maintenance. However, challenges such as signal interference, data security, and regulatory issues must be addressed.

5.2. Future Directions

Despite the promising outlook, several challenges must be addressed to achieve broad adoption of wBMSs including the following:

- Data security: Robust encryption and authentication methods are essential to protect against cybersecurity threats. Blockchain technology holds the potential to enhance the security of wBMSs.
- Signal interference: Advanced signal processing algorithms and improved shielding techniques can mitigate the effects of signal interference, ensuring reliable communication.
- Standardization: Collaboration among industry players, regulators, and standardization bodies is crucial to establishing universal standards for wBMSs, ensuring interoperability and scalability.

5.3. Implications

In the context of EVs and HEVs, wBMSs have the potential to significantly improve the efficiency and reliability of battery systems, enabling better monitoring, easier maintenance, and more effective use of resources. Furthermore, integrating a wBMS into smart grids and IoT ecosystems paves the way for innovative applications in energy management and distribution. Real-time monitoring and predictive maintenance enabled by a wBMS can lead to smarter energy systems that are more responsive and adaptive to changing conditions.

In conclusion, wBMSs represent a transformative step forward in battery management technology. Continued research and development are essential to overcome existing challenges and fully realize the potential of wBMSs, revolutionizing battery management. This paper offers detailed guidelines, summarizing existing developments, current challenges, and countermeasures for researchers focusing on future advancements. This paper aims to encourage the research community to intensify efforts in wBMS research, advancing its progress and broad adoption across various applications.

Author Contributions: Conceptualization, Z.C. and C.M.; investigation, Z.C.; writing—original draft preparation, Z.C.; writing—review and editing, C.M. and W.G.; visualization, Z.C.; supervision, Y.F. and C.M.; project administration, C.M.; funding acquisition, C.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the California Energy Commission (CEC), grant number EPC-21-039.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Mishra, S.; Swain, S.C.; Samantaray, R.K. A Review on Battery Management System and Its Application in Electric Vehicle. In Proceedings of the 2021 International Conference on Advances in Computing and Communications (ICACC), Kakkanad, India, 21–23 October 2021; pp. 1–6.

2. Darwish, M.; Ioannou, S.; Janbey, A.; Amreiz, H.; Marouchos, C.C. Review of Battery Management Systems. In Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Piscataway, NJ, USA, 7 October 2021; pp. 1–6.
3. Gabbar, H.A.; Othman, A.M.; Abdussami, M.R. Review of Battery Management Systems (BMS) Development and Industrial Standards. *Technologies* **2021**, *9*, 28. [CrossRef]
4. Balasingam, B.; Ahmed, M.; Pattipati, K. Battery Management Systems—Challenges and Some Solutions. *Energies* **2020**, *13*, 2825. [CrossRef]
5. Lelie, M.; Braun, T.; Knips, M.; Nordmann, H.; Ringbeck, F.; Zappen, H.; Sauer, D.U. Battery Management System Hardware Concepts: An Overview. *Appl. Sci.* **2018**, *8*, 534. [CrossRef]
6. Yong, J.Y.; Ramachandaramurthy, V.K.; Tan, K.M.; Mithulananthan, N. A Review on the State-of-the-Art Technologies of Electric Vehicle, Its Impacts and Prospects. Renew. *Sustain. Energy Rev.* **2015**, *49*, 365–385. [CrossRef]
7. amkumar, M.S.; Reddy, C.S.R.; Ramakrishnan, A.; Raja, K.; Pushpa, S.; Jose, S.; Jayakumar, M. Review on Li-Ion Battery with Battery Management System in Electrical Vehicle. *Adv. Mater. Sci. Eng.* **2022**, *2022*, 3379574. [CrossRef]
8. annan, M.A.; Lipu, M.S.H.; Hussain, A.; Mohamed, A. A Review of Lithium-Ion Battery State of Charge Estimation and Management System in Electric Vehicle Applications: Challenges and Recommendations. *Renew. Sustain. Energy Rev.* **2017**, *78*, 834–854. [CrossRef]
9. Kassim, M.R.M.; Jamil, W.A.W.; Sabri, R.M. State-of-Charge (SOC) and State-of-Health (SOH) Estimation Methods in Battery Management Systems for Electric Vehicles. In Proceedings of the 2021 IEEE International Conference on Computing (ICOCO), Virtual, 17 November 2021; pp. 91–96.
10. Klee Barillas, J.; Li, J.; Günther, C.; Danzer, M.A. A Comparative Study and Validation of State Estimation Algorithms for Li-Ion Batteries in Battery Management Systems. *Appl. Energy* **2015**, *155*, 455–462. [CrossRef]
11. Lee, Y.-L.; Lin, C.-H.; Farooqui, S.A.; Liu, H.-D.; Ahmad, J. Validation of a Balancing Model Based on Master-Slave Battery Management System Architecture. *Electr. Power Syst. Res.* **2023**, *214*, 108835. [CrossRef]
12. Ren, H.; Zhao, Y.; Chen, S.; Wang, T. Design and Implementation of a Battery Management System with Active Charge Balance Based on the SOC and SOH Online Estimation. *Energy* **2019**, *166*, 908–917. [CrossRef]
13. Shet, V.V.; Ponangi, B.R.; Jacob, K. Design of a Thermal Management System for a Battery Pack in an Electric Vehicle Using Dymola. *Heat Transf.* **2020**, *49*, 2686–2705. [CrossRef]
14. Kim, E.; Shin, K.G.; Lee, J. Real-Time Battery Thermal Management for Electric Vehicles. In Proceedings of the 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), Berlin, Germany, 14–17 April 2014; pp. 72–83.
15. Tran, M.-K.; Fowler, M. A Review of Lithium-Ion Battery Fault Diagnostic Algorithms: Current Progress and Future Challenges. *Algorithms* **2020**, *13*, 62. [CrossRef]
16. Ma, Z.; Luan, Y.; Zhang, F.; Xie, S.; Coskun, S. A Data-Driven Energy Management Strategy for Plug-in Hybrid Electric Buses Considering Vehicle Mass Uncertainty. *J. Energy Storage* **2024**, *77*, 109963. [CrossRef]
17. Vatanparvar, K.; Faezi, S.; Burago, I.; Levorato, M.; Al Faruque, M.A. Extended Range Electric Vehicle With Driving Behavior Estimation in Energy Management. *IEEE Trans. Smart Grid.* **2019**, *10*, 2959–2968. [CrossRef]
18. John, P.C.; Kumar, B.P.N. Functional Safety Design and ISO26262 Compliance for BMS in EV and HEV. In *Intelligent Solutions for Smart Grids and Smart Cities*; Siano, P., Williamson, S., Beevi, S., Eds.; Springer Nature: Singapore, 2023; pp. 329–339.
19. Marcos, D.; Garmendia, M.; Crego, J.; Cortajarena, J.A. Functional Safety BMS Design Methodology for Automotive Lithium-Based Batteries. *Energies* **2021**, *14*, 6942. [CrossRef]
20. Krishna, G.; Singh, R.; Gehlot, A.; Akram, S.V.; Priyadarshi, N.; Twala, B. Digital Technology Implementation in Battery-Management Systems for Sustainable Energy Storage: Review, Challenges, and Recommendations. *Electronics* **2022**, *11*, 2695. [CrossRef]
21. Yang, S.; Liu, X.; Li, S.; Zhang, C. Key Technologies of BMS. In *Advanced Battery Management System for Electric Vehicles*; Yang, S., Liu, X., Li, S., Zhang, C., Eds.; Springer Nature: Singapore, 2023; pp. 33–51. ISBN 978-981-19349-0-2.
22. Krishnamoorthy, R.; Bharatiraja, C.; Krishnan, K. Review of Communication Network Interfaces and Battery Management for PHEV-ECU Materials and Components. *Mater. Today Proc.* **2021**, *45*, 3444–3448. [CrossRef]
23. Lee, M.; Lee, J.; Lee, I.; Lee, J.; Chon, A. Wireless Battery Management System. In Proceedings of the 2013 World Electric Vehicle Symposium and Exhibition (EVS27), Barcelona, Spain, 17–20 November 2013; pp. 1–5.
24. Shell, C.; Henderson, J.; Verra, H.; Dyer, J. Implementation of a Wireless Battery Management System (WBMS). In Proceedings of the 2015 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, Pisa, Italy, 11–14 May 2015; pp. 1954–1959.
25. Battery Management System Trends, Issues and Solutions | Renesas. Available online: https://www.renesas.com/us/en/blogs/battery-management-system-trends-issues-and-solutions (accessed on 19 March 2024).
26. Pannerselvam, S.; Narayanan, V.; Gireesh Kumar, T. Energy Efficient Machine Learning Based SMART-A-BLE Implemented Wireless Battery Management System for Both Hybrid Electric Vehicles and Battery Electric Vehicles. *Procedia Comput. Sci.* **2023**, *218*, 235–248. [CrossRef]
27. Bansal, P.; Nagaraj, P.R. Wireless Battery Management System for Electric Vehicles. In Proceedings of the 2019 IEEE Transportation Electrification Conference (ITEC-India), Bengaluru, India, 17–19 December 2019; pp. 1–5.

28. Vishnu, K.; Nema, R.K.; Ojha, A. Various Types of Wireless Battery Management System in Ev. In Proceedings of the 2020 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 19–20 February 2020; pp. 1–5.
29. Samanta, A.; Williamson, S.S. A Survey of Wireless Battery Management System: Topology, Emerging Trends, and Challenges. *Electronics* **2021**, *10*, 2193. [CrossRef]
30. Cristian, G.G.; Vicente, G.-D.; Pelayo, G.-B.; Cristina, B.; Cueva, L. *Juan Manuel Protocols and Applications for the Industrial Internet of Things*; IGI Global: Hershey, PA, USA, 2018; ISBN 978-1-5225-3806-6.
31. Tosi, J.; Taffoni, F.; Santacatterina, M.; Sannino, R.; Formica, D. Performance Evaluation of Bluetooth Low Energy: A Systematic Review. *Sensors* **2017**, *17*, 2898. [CrossRef]
32. Zhou, L.; Chen, X.; Li, Y.; Li, J. Bluetooth Low Energy 4.0-Based Communication Method for Implants. In Proceedings of the 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), Shanghai, China, 14 October 2017; IEEE: Shanghai, China, 2017; pp. 1–5.
33. Lacava, A.; Zottola, V.; Bonaldo, A.; Cuomo, F.; Basagni, S. Securing Bluetooth Low Energy Networking: An Overview of Security Procedures and Threats. *Comput. Netw.* **2022**, *211*, 108953. [CrossRef]
34. Rincon Vija, F.A.; Cregut, S.; Papadopoulos, G.Z.; Montavont, N. Enabling Robust Wireless Communication for BMS on Electric Vehicles. In Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 4 October 2021; IEEE: Edmonton, AB, Canada, 2021; pp. 423–426.
35. Rincon Vija, F.A.; Cregut, S.; Papadopoulos, G.Z.; Montavont, N. From Wired to Wireless BMS in Electric Vehicles. In Proceedings of the 2021 17th International Conference on Mobility, Sensing and Networking (MSN), Exeter, UK, 13–15 December 2021; IEEE: Exeter, UK, 2021; pp. 255–262.
36. *IEEE Std 802.15.4-2020 ; (Revision of IEEE Std 802.15.4-2015)*. IEEE Standard for Low-Rate Wireless Networks. IEEE: Piscataway, NJ, USA, 23 July 2020; pp. 1–800. [CrossRef]
37. Ahamed, M.M.I.; Mateen, S.; Savadi, A.; Haroon, P.S.A.L.; Naushad, S. of the Wireless Charging and BMS for Optimizing Electric Vehicle Charging and Battery Management. In Proceedings of the 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballar, India, 29 April 2023; IEEE: Ballar, India, 2023; pp. 1–7.
38. Spörk, M.; Boano, C.A.; Römer, K. Performance and Trade-Offs of the New PHY Modes of BLE 5. In Proceedings of the ACM MobiHoc Workshop on Pervasive Systems in the IoT Era, New York, NY, USA, 2 July 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 7–12.
39. Huan, J.; Liu, X.; Li, H.; Wang, H.; Zhu, X. A Monitoring and Control System for Aquaculture via Wireless Network and Android Platform. *Sens. Transducers* **2014**, *169*, 250–256.
40. Li, P.; Li, J.; Nie, L.; Wang, B. Research and Application of ZigBee Protocol Stack. In Proceedings of the 2010 International Conference on Measuring Technology and Mechatronics Automation, Changsha, China, 13–14 March 2010; Volume 2, pp. 1031–1034.
41. Vallo, N.J. *Design and Analysis of A Wireless Battery Management System for an Advanced Electrical Storage System*; University of Dayton: Dayton, OH, USA, 2016.
42. Rahman, A.; Rahman, M.; Rashid, M. Wireless Battery Management System of Electric Transport. *IOP Conf. Ser. Mater. Sci. Eng.* **2017**, *260*, 012029. [CrossRef]
43. Coskun, V.; Ozdenizci, B.; Ok, K. The Survey on Near Field Communication. *Sensors* **2015**, *15*, 13348–13405. [CrossRef] [PubMed]
44. Basic, F. *Enabling Secure and Wireless Battery Management Systems*; Graz University of Technology: Graz, Austria, 2023.
45. Basic, F.; Gaertner, M.; Steger, C. Secure and Trustworthy NFC-Based Sensor Readout for Battery Packs in Battery Management Systems. *IEEE J. Radio Freq. Identif.* **2022**, *6*, 637–648. [CrossRef]
46. Basic, F.; Laube, C.R.; Stratznig, P.; Steger, C.; Kofler, R. Wireless BMS Architecture for Secure Readout in Vehicle and Second Life Applications. In Proceedings of the 2023 8th International Conference on Smart and Sustainable Technologies (SpliTech), Bol, Hotel Elaphusa, 20 June 2023; pp. 1–6.
47. *IEEE Std 802.11-2020; (Revision of IEEE Std 802.11-2016)*. IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems—Local and Metropolitan area Networks–Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE: Piscataway, NJ, USA, 2021; pp. 1–4379. [CrossRef]
48. Ferro, E.; Potorti, F. Bluetooth and Wi-Fi Wireless Protocols: A Survey and a Comparison. *IEEE Wirel. Commun.* **2005**, *12*, 12–26. [CrossRef]
49. Froiz-Míguez, I.; Fernández-Caramés, T.; Fraga-Lamas, P.; Castedo, L. Design, Implementation and Practical Evaluation of an IoT Home Automation System for Fog Computing Applications Based on MQTT and ZigBee-WiFi Sensor Nodes. *Sensors* **2018**, *18*, 2660. [CrossRef] [PubMed]
50. Ricco, M.; Meng, J.; Gherman, T.; Grandi, G.; Teodorescu, R. Smart Battery Pack for Electric Vehicles Based on Active Balancing with Wireless Communication Feedback. *Energies* **2019**, *12*, 3862. [CrossRef]
51. Huang, X.; Acharya, A.B.; Meng, J.; Sui, X.; Stroe, D.-I.; Teodorescu, R. Wireless Smart Battery Management System for Electric Vehicles. In Proceedings of the 2020 IEEE Energy Conversion Congress and Exposition (ECCE), Virtual, 11 October 2020; pp. 5620–5625.
52. Zebrowski, D. *Development and Evaluation of Prototype Wireless Battery Management System*; KTH, School of Electrical Engineering and Computer Science: Stockholm, Sweden, 2022.

53. Li, Y.; Peng, C.; Yuan, Z.; Deng, H.; Li, J.; Wang, T. MobileInsight: Analyzing Cellular Network Information on Smartphones. *GetMobile Mob. Comput. Commun.* **2017**, *21*, 39–42. [CrossRef]
54. Li, Y.; Peng, C.; Yuan, Z.; Li, J.; Deng, H.; Wang, T. Mobileinsight: Extracting and Analyzing Cellular Network Information on Smartphones. In Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking, New York City, NY, USA, 3–7 October 2016; p. 215.
55. Lohar, G.V.; Kumar, M.S. Design and Implementation of IoT Based Wireless Battery Management System for Electric Vehicles. *Int. J. Intell. Syst. Appl. Eng.* **2023**, *11*, 360–369.
56. Faika, T.; Kim, T.; Khan, M. An Internet of Things (IoT)-Based Network for Dispersed and Decentralized Wireless Battery Management Systems. In Proceedings of the 2018 IEEE Transportation Electrification Conference and Expo (ITEC), Long Beach, CA, USA, 13–15 June 2018; pp. 1060–1064.
57. Faika, T.; Kim, T.; Ochoa, J.; Khan, M.; Park, S.-W.; Leung, C.S. A Blockchain-Based Internet of Things (IoT) Network for Security-Enhanced Wireless Battery Management Systems. In Proceedings of the 2019 IEEE Industry Applications Society Annual Meeting, Baltimore, MD, USA, 29 September 2019; pp. 1–6.
58. Liu, J. Wireless BMS vs. Wired BMS: Who Is the Key Battery Technology? MokoEnergy: Shenzhen, China, 2023.
59. Rahman, A.B.A.; Jain, R. Comparison of Internet of Things (IoT) Data Link Protocols. Available online: https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_dlc/ (accessed on 7 April 2024).
60. Ohwo, O.; Olujimi, A. A Comparative Review of Emerging Wireless Technology. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2020**, *7*, 163–175. [CrossRef]
61. Sikimic, M.; Amovic, M.; Vujovic, V.; Suknovic, B.; Manjak, D. An Overview of Wireless Technologies for IoT Network. In Proceedings of the 2020 19th International Symposium Infoteh-Jahorina (Infoteh), East Sarajevo, Bosnia and Herzegovina, 18–20 March 2020; IEEE: East Sarajevo, Bosnia and Herzegovina, 2020; pp. 1–6.
62. Alobaidy, H.A.H.; Mandeep, J.S.; Nordin, R.; Abdullah, N.F. A Review on ZigBee Based WSNs: Concepts, Infrastructure, Applications, and Challenges. *Int. J. Electr. Electron. Eng. Telecommun.* **2020**, *9*, 189–198. [CrossRef]
63. Abuelsamid, S. *GM to Use First Wireless Battery Management System in Ultium Battery Packs*; Forbes: Jersey City, NJ, USA, 2020.
64. Sripad, S.; Kulandaivel, S.; Pande, V.; Sekar, V.; Viswanathan, V. Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks. *arXiv* **2019**, arXiv:arXiv:1711, 4822.
65. Kumbhar, S.; Faika, T.; Makwana, D.; Kim, T.; Lee, Y. Cybersecurity for Battery Management Systems in Cyber-Physical Environments. In Proceedings of the 2018 IEEE Transportation Electrification Conference and Expo (ITEC), Long Beach, CA, USA, 13–15 June 2018; pp. 934–938.
66. Naseri, F.; Kazemi, Z.; Larsen, P.G.; Arefi, M.M.; Schaltz, E. Cyber-Physical Cloud Battery Management Systems: Review of Security Aspects. *Batteries* **2023**, *9*, 382. [CrossRef]
67. Sofi, M. Bluetooth Protocol in Internet of Things (IoT), Security Challenges and a Comparison with Wi-Fi Protocol: A Review. *Int. J. Eng. Res.* **2016**, *V5*, 42–56. [CrossRef]
68. Cäsar, M.; Pawelke, T.; Steffan, J.; Terhorst, G. A Survey on Bluetooth Low Energy Security and Privacy. *Comput. Netw.* **2022**, *205*, 108712. [CrossRef]
69. Zohourian, A.; Dadkhah, S.; Neto, E.C.P.; Mahdikhani, H.; Danso, P.K.; Molyneaux, H.; Ghorbani, A.A. IoT Zigbee Device Security: A Comprehensive Review. *Internet Things* **2023**, *22*, 100791. [CrossRef]
70. Bere, G.; Ochoa, J.J.; Kim, T.; Aenugu, I.R. Blockchain-Based Firmware Security Check and Recovery for Battery Management Systems. In Proceedings of the 2020 IEEE Transportation Electrification Conference & Expo (ITEC), Chicago, IL, USA, 23–26 June 2020; pp. 262–266.
71. Je Lee, S.; Lee, Y.H.; Park, J.; Park, N. Analyzing RF Interference on Wireless BMS in High-Congestion Environments. In Proceedings of the 2023 IEEE Green Energy and Smart Systems Conference (IGESSC), Long Beach, CA, USA, 13–14 November 2023; pp. 1–6.
72. Pampel, F.; Pischinger, S.; Teuber, M. A Systematic Comparison of the Packing Density of Battery Cell-to-Pack Concepts at Different Degrees of Implementation. *Results Eng.* **2022**, *13*, 100310. [CrossRef]
73. Jin, C.; Sun, Y.; Yao, J.; Feng, X.; Lai, X.; Shen, K.; Wang, H.; Rui, X.; Xu, C.; Zheng, Y.; et al. No Thermal Runaway Propagation Optimization Design of Battery Arrangement for Cell-to-Chassis Technology. *eTransportation* **2022**, *14*, 100199. [CrossRef]
74. Lian, Y.; Ling, H.; Jiang, L.; Yi, B.; Zhang, F.; Liu, J.; Song, G.; Tang, M. *Development of Cell to Body Technology towards High Levels of Integration, High Strength and High Stiffness*; SAE International: Warrendale, PA, USA, 2023.