technologies

MDPI

Review

Real-Time Synchronisation in Low-Power Wireless Sensor Networks: From Industry to Healthcare

Reshman Jabeen, Manoochehr Rasekh * and Wamadeva Balachandran *

College of Engineering, Design and Physical Sciences, Brunel University of London, Uxbridge UB8 3PH, UK
* Correspondence: manoochehr.rasekh@brunel.ac.uk (M.R.); wamadeva.balachandran@brunel.ac.uk (W.B.)

Abstract

The growing demand for real-time data synchronisation has increased the importance of supervisory control systems in industrial automation, smart grids, healthcare monitoring, and environmental applications. Low-power wireless sensor networks (LPWSNs) have emerged as key enablers of scalable and energy-efficient monitoring. However, achieving reliable synchronisation remains challenging due to latency, energy constraints, scalability limitations, security vulnerabilities, and data integrity concerns. This review examines the role of time synchronisation in supervisory control systems and evaluates how LPWSNs support real-time monitoring and decision-making. Established synchronisation protocols, including Reference Broadcast Synchronisation (RBS), the Flooding Time Synchronisation Protocol (FTSP), and the Timing-Sync Protocol for Sensor Network (TPSN), are analysed in terms of accuracy, energy efficiency, and scalability. Key optimisation strategies, such as clock drift compensation, data aggregation and compression, and edge computing, are also discussed. Recent advances, including artificial intelligence and machine learning (AI/ML)-based predictive synchronisation, blockchain, software-defined networking (SDN), and 5G-enabled LPWSNs, are reviewed across industrial, energy, healthcare, and agricultural applications. The review critically evaluates their benefits and trade-offs and identifies remaining challenges related to cybersecurity, energy efficiency, and large-scale deployment. Finally, future research directions are outlined to support robust, scalable, and efficient real-time synchronisation in LPWSNs.

Keywords: real-time synchronisation; supervisory control systems; low-power wireless sensor networks (LPWSNs); Internet of Things (IoT); industrial automation; smart healthcare; energy efficiency; scalability

Academic Editor: Zhipeng Wu

Received: 13 May 2026
Revised: 25 June 2026
Accepted: 26 June 2026
Published: 28 June 2026

1. Introduction

Sensor nodes with basic processors, low-power antennas, and a variety of detectors make up a wireless sensor network (WSN). Sensor networks can be established quickly, cost-effectively, and with minimal environmental impact because they do not require extensive wired communication infrastructure [1]. The hardware and software architecture of sensor nodes allows them to store and process data locally. Their ability to communicate with one another enables collaborative operation, allowing them to complete complex tasks and share information. The long lifespan of sensor nodes is supported by the low-power communication mechanisms [2]. Greater benefits are also offered by the nodes' ability to be reprogrammed after deployment.

Wireless sensor nodes are widely used in diverse industrial, environmental, and supervisory control applications due to their affordability and adaptability. They are capable of measuring physical parameters such as temperature, pressure, humidity, and other environmental variables. These nodes function as both sensing and actuation tools with response-generating capabilities [3]. Sensors acquire physical information from the environment that requires monitoring and control.

The analogue-to-digital converters (ADCs) digitise the continuous analogue signals recorded by the sensors before transmitting them to controllers for further processing. Sensor nodes are typically characterised by small size, low power consumption, the ability to operate under harsh conditions, autonomy, unattended operation, and environmental adaptability [4]. Due to energy constraints, wireless sensor nodes rely on low-capacity sources, typically batteries (e.g., 0.5 Ah and 1.2 V). The microcontroller serves as the central functional unit, responsible for task execution, data processing, and the coordination of other sensor node components.

Various processing units such as digital signal processors (DSPs), field-programmable gate arrays (FPGAs), application-specific integrated circuits, and general-purpose microprocessors can be used as controllers. However, low-power microcontrollers and microprocessors remain the most practical choice for WSN nodes [5]. Their programmability, flexibility in interfacing, ability to enter low-power sleep modes, and energy-efficient operation make them well-suited for embedded systems [6].

Wireless communication in WSNs enables data transmission over wide areas using different technologies, including radio frequency (RF) and optical (laser) communication. Although laser communication is energy-efficient, it is sensitive to atmospheric conditions and requires a line of sight. Similarly, infrared communication has a limited range but does not require an antenna [7]. In contrast, RF-based communication is the most widely adopted method due to its robustness and flexibility. Typical WSNs communication frequencies range from 433 MHz to 2.4 GHz. Applications of WSNs include environmental monitoring, remote tracking, industrial automation, smart grids, healthcare monitoring, and even customer behaviour analysis [8–12].

1.1. Motivation, Research Gap and Scope of Review

Rapid development in industrial automation and the growing dependence on data-driven decision-making have highlighted the importance of supervisory control and data acquisition (SCADA) systems and other supervisory control frameworks in the modern industry [13]. The rise of Industry 4.0, predictive maintenance, and smart manufacturing has significantly increased the demand for real-time data synchronisation [14]. This synchronisation ensures that distributed components of supervisory control systems operate cohesively, minimising delays and inefficiencies that could otherwise affect system performance. With the advancement of automation, low-power wireless sensor networks (LPWSNs) have emerged as a key enabling technology for industrial monitoring and control [15]. However, integrating LPWSNs with SCADA systems remains a significant challenge for researchers and practitioners, particularly when attempting to achieve seamless data synchronisation while minimising energy consumption and reducing dependence on communication infrastructure [16].

In the field of supervisory systems and energy-efficient WSNs, a substantial body of research has examined synchronisation protocols, energy management strategies, and communication architectures. These studies have provided valuable insights into the operation and optimisation of LPWSNs across a range of application domains. However, a clear research gap remains in understanding how real-time data synchronisation can be achieved in energy-constrained LPWSNs while simultaneously satisfying the require-

ments of scalability, reliability, security, and low latency within supervisory control environments. Also, existing surveys often focus on specific synchronisation protocols, general WSN architectures, or individual application domains, with limited attention given to the broader integration of synchronisation techniques, emerging technologies, and practical deployment challenges across multiple sectors.

The current review seeks to address this gap by analysing time-sensitive data synchronisation in supervisory control systems through the use of LPWSNs. The paper provides a focused analysis of key areas, including SCADA systems, smart manufacturing, predictive maintenance, power optimisation strategies, and data transfer mechanisms in LPWSNs, together with the challenges associated with achieving seamless real-time synchronisation. Also, the practical applications of these technologies in domains such as smart grids, healthcare, and environmental monitoring are discussed.

The novelty of this review lies in its integrated and cross-disciplinary perspective on real-time synchronisation in LPWSNs. Unlike existing surveys that typically examine synchronisation methods or application domains in isolation, this review brings together conventional synchronisation techniques, clock drift compensation methods, data aggregation strategies, edge and fog computing frameworks, and emerging developments such as artificial intelligence (AI)/machine learning (ML)-based predictive synchronisation, blockchain-enabled security, software-defined networking (SDN), and fifth generation (5G) / LPWAN integration. In addition, the review provides comparative analyses of synchronisation approaches, deployment challenges, mitigation strategies, and representative studies, highlighting the trade-offs between synchronisation accuracy, energy efficiency, scalability, and security. By synthesising developments across industrial automation, smart grids, environmental monitoring, and healthcare systems, the review offers a comprehensive assessment of current capabilities, identifies unresolved research challenges, and outlines future directions for next-generation LPWSNs.

The study is grounded in a critical review of existing literature, identifying key limitations, emerging trends, and future research opportunities. It aims to provide researchers and practitioners with valuable insight and practical recommendations for developing more energy-effective, secure, scalable, and robust real-time synchronisation frameworks for supervisory control systems and related LPWSN applications.

1.2. Importance of Real-Time Data Synchronisation and Role of LPWSNs in Modern Industry

Data synchronisation ensures consistent, accurate, and reliable data across distributed systems, supporting effective operations and improved user experience [17]. It maintains consistency between multiple data sources and endpoints, ensuring that systems operate with up-to-date information. Before utilisation, newly acquired data is typically processed and validated to address errors, duplication, and inconsistencies [17]. The core of systems such as SCADA systems is data acquisition (DAQ), which involves collecting, monitoring, and analysing data from multiple sources to provide a comprehensive understanding of system behaviour. Any lack of synchronisation can result in outdated or inconsistent data, leading to reduced operational efficiency or even critical system failures [16,17]. Therefore, data records must remain consistent across systems, and any updates must be propagated in real time to minimise errors, ensure data integrity, and maintain accessibility of current information [18]. Similarly, in smart manufacturing, data synchronisation enables precise monitoring and control of production processes, improving product quality while reducing resource wastage [19]. LPWSNs enable data collection from multiple distributed sensing points, supporting flexible, scalable, and real-time monitoring and control in industrial environments [19]. These networks connect critical assets to control systems and operators, allowing timely analysis and informed decision-making.

As a result, operational teams can reduce data collection costs, prevent unplanned downtime, and enhance overall system efficiency through improved visibility of system performance [20]. Collectively, these capabilities provide a significant competitive advantage in modern industry.

Integrating LPWSNs with SCADA systems offers several advantages. Their low power consumption extends sensor lifespan and enables long-term deployment using battery-powered devices. This facilitates a wide range of applications, including cost-sensitive and large-scale deployments. Wireless sensors and actuators can be used for leak detection, factory automation, and inventory management [21]. They are also suitable for monitoring parameters such as temperature, vibration, and pressure in remote or hard-to-access environments, including pipelines, turbine systems, and storage facilities [22]. In smart grid applications, LPWSNs support real-time monitoring and management of energy generation, distribution, and consumption [23]. They enable sensing of environmental and operational parameters such as pressure, humidity, wind conditions, and radiation, while supporting remote control of infrastructure components such as turbines and transmission systems, as well as efficient household energy management [24].

Despite these advantages, LPWSNs face several challenges, including limited energy resources, communication delays, and dependence on reliable network connectivity. Addressing these issues requires advanced network design, energy-efficient protocols, and robust data management strategies to ensure reliable and scalable real-time synchronisation.

1.3. Review Methodology

This review was conducted to examine recent developments in real-time synchronisation techniques for LPWSNs, with particular emphasis on industrial automation, supervisory control systems, smart manufacturing, healthcare monitoring, and emerging Internet of Things (IoT) applications. The literature survey primarily focused on publications from 2020 to 2026 to ensure coverage of the most recent advances, emerging technologies, and current research trends in the field.

Relevant literature was identified through searches conducted across major scientific databases, including Google Scholar, Web of Science, PubMed, IEEE Xplore, and ScienceDirect. The search process employed combinations of keywords and related terms, including “real-time synchronisation”, “supervisory control systems”, “LPWSNs”, “IoT”, “industrial automation”, “smart healthcare”, “energy efficiency”, and “scalability”. Additional relevant studies were identified through reference tracking of selected articles.

The inclusion criteria focused on peer-reviewed journal articles, conference papers, and review studies addressing synchronisation protocols, clock drift compensation, energy-efficient communication, edge and fog computing, artificial intelligence and machine learning applications, blockchain-enabled synchronisation, and LPWSN-based industrial or healthcare systems. Studies not directly related to LPWSNs, real-time synchronisation, or practical IoT-based applications were excluded from the review. The selected literature was screened based on relevance, technical contribution, recency, and alignment with the objectives of this review. The collected studies were subsequently analysed and synthesised to identify key technological developments, existing challenges, research gaps, and future directions for real-time synchronisation in LPWSNs. To ensure a structured and consistent comparison across the reviewed studies, this paper adopts a multi-criteria evaluation framework for analysing real-time synchronisation techniques in LPWSNs. Each technique is assessed based on key performance dimensions, including synchronisation accuracy, communication latency, energy consumption, scalability, security robustness, and suitability for domain-specific applications such as industrial automation and healthcare monitoring. These criteria are used to interpret and compare classical protocols,

optimisation strategies, and emerging intelligent approaches in a unified manner. Rather than focusing solely on qualitative descriptions, this framework enables a more systematic synthesis of trade-offs between competing solutions, highlighting their relative strengths and limitations under resource-constrained and real-time operating conditions.

2. SCADA System Network and LPWSNs

The SCADA architecture comprises both software and hardware components. The software includes the human–machine interface (HMI), central database, and other application software, while the hardware layer consists of remote terminal units (RTUs), master terminal units (MTUs), sensors, and actuators. These components enable communication and interaction between the physical process and supervisory control systems. Sensors and actuators interface directly with the physical environment, while RTUs acquire and process field data and transmit telemetry information to the MTUs. This enables effective monitoring and control of the overall SCADA system [25,26].

The SCADA control centre is responsible for supervising and managing operational data, system monitoring, and communication between multiple RTUs and the MTUs. Information is presented in the form of status data, measurements, events, and alarms to support operational decision-making. Data, events, and alerts generated through bidirectional communication between field devices and SCADA control centre are stored in a historian, which provides time-series data for analysis, trending, and reporting. The SCADA system can be implemented as a centralised server or distributed across multiple nodes, depending on system scale and architecture [25,26].

Operators interact with the system through HMI stations, which provide graphical visualisations, real-time monitoring, and trend displays for process control.

The SCADA communication network enables reliable data exchange between field devices, control systems, programmable logic controllers (PLCs)/(RTUs), and the control centre using industrial communication protocols. This layered architecture, illustrated in Figure 1, ensures structured data flow, operational visibility, and system control across the network. Communication within SCADA systems can be implemented using either wired or wireless media. In recent years, wireless technologies have become increasingly prevalent due to their flexibility, particularly for geographically distributed assets and hard-to-access locations [8,27,28]. The evolution of SCADA communication paradigms can be broadly categorised into four stages: monolithic, distributed, networked, and IoT—enabled architectures. In modern systems, interoperability between industrial hardware and software applications is commonly achieved through standardised interfaces such as open platform communication (OPC) servers, which facilitate reliable and vendor-neutral exchange [29]. LPWSNs are increasingly integrated into SCADA systems to enable flexible and scalable monitoring of geographically distributed assets. These networks play a critical role in modern critical infrastructures by improving operational efficiency and reliability while supporting real-time data acquisition. However, LPWSNs introduce challenges related to limited energy resources, latency constraints, and security vulnerabilities. With the evolution toward IoT-enabled SCADA architectures, wireless communication technologies are becoming fundamental to applications such as smart grids and industrial automation, where secure and efficient data exchange is essential [27,30–33].

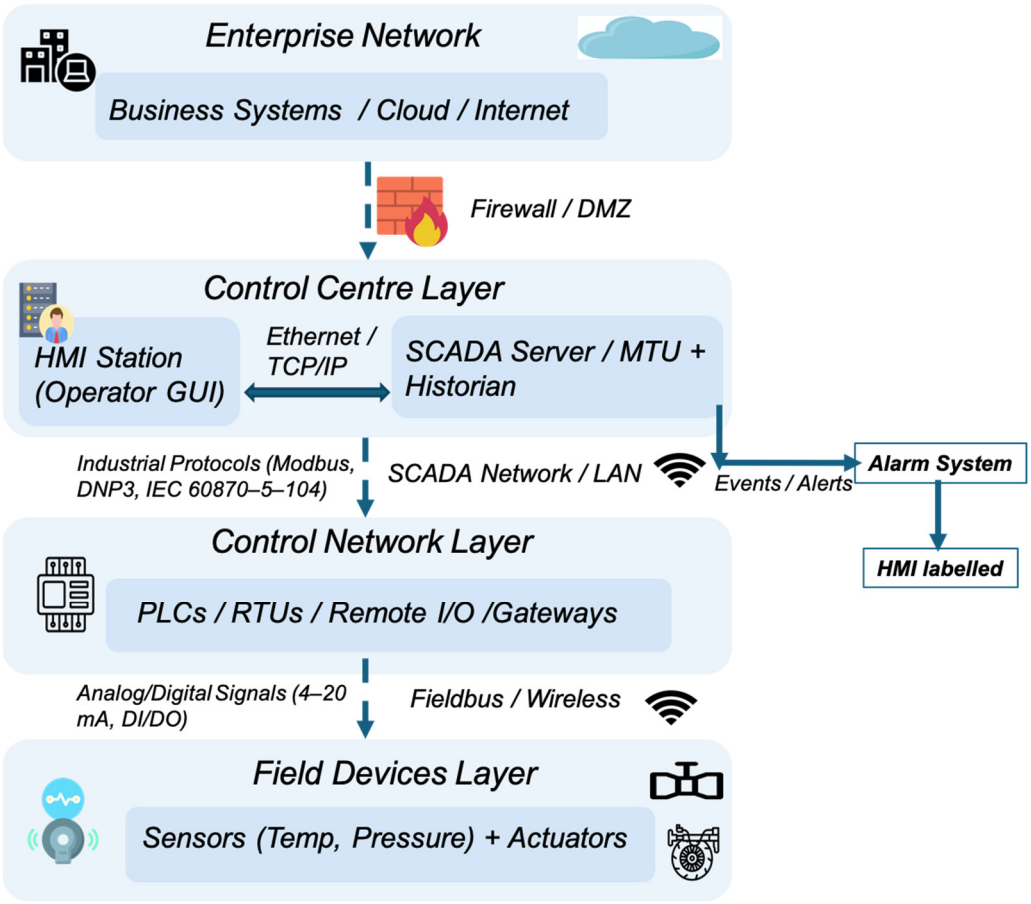


Figure 1. Layered SCADA system architecture showing data flow and communication between enterprise systems, control centre components (SCADA/MTU, HMI, historian), control network devices (PLCs/RTUs), and field instruments, along with security boundaries and communication technologies (the figure was designed by the authors). DMZ: Demilitarised Zone; GUI: Graphical User Interface; TCP: Transmission Control Protocol; IP: Internet Protocol; DNP3: Distributed Network Protocol 3; IEC: International Electro-Technical Commission (e.g., IEC 60870); DI/DO: Digital Input/Digital Output; Fieldbus: Industrial communication protocol for real-time distributed control; HMI: Human–Machine Interface.

Integrating SCADA systems with WSNs requires careful trade-offs between energy efficiency, communication latency, and system security. In this context, emerging communication technologies such as 5G ultra-reliable low-latency communication (URLLC) enable mission-critical industrial applications by providing ultra-low latency (on the order of 1 ms), very high reliability (up to 99.9999%), and deterministic quality of service (QoS).

Such capabilities support advanced use cases including smart grid automation, industrial process control, autonomous systems, and remote healthcare operations. In parallel, technologies such as OPC unified architecture (OPC UA) and AI-driven edge computing are facilitating seamless interoperability and localised intelligence, thereby enhancing the scalability, resilience, and real-time performance of modern industrial IoT-enabled SCADA systems [29]. Similar communication and reliability requirements are also emerging in healthcare cyber-physical systems, where SCADA-like architectures support applications such as remote patient monitoring and tele-surgery, requiring ultra-low latency, high reliability, and secure data exchange [34,35].

Smart Manufacturing with LPWSNs

Manufacturing processes, factories, and industrial warehouses are rapidly transitioning toward a highly digitalised and interconnected environment. The factories of the future (FoF) paradigm integrates advanced technologies such as AI, the IoT, and big data analytics, forming the foundation of the Industry 4.0 vision [16]. The success of FoF is strongly dependent on a reliable and scalable communication infrastructure due to the increasing volume and velocity of data generated across industrial processes [18]. Traditionally, industrial communication has relied on wired networks installed during plant deployment. While these provide reliability, they limit flexibility and incur significant time and cost when maintenance or reconfiguration is required [19,20]. In contrast, wireless communication technologies enable greater adaptability, supporting dynamic manufacturing environments, rapid production line reconfiguration, and reduced infrastructure cost.

LPWSNs have emerged as a key enabler of smart manufacturing by facilitating real-time sensing, monitoring, and data exchange across distributed industrial assets [24]. These networks support improved operational efficiency and machine performance by enabling reliable communication even in harsh industrial environments [36]. LPWSNs are particularly attractive due to their low energy consumption, scalability, and cost-effective deployment, making them suitable for large-scale industrial systems. The architecture of LPWANs in smart manufacturing typically consists of multiple layers. At the sensing layer, sensor nodes collect environmental and operational data. This data is transmitted through lower-power wireless technologies such as Bluetooth low energy (BLE), ZigBee, and long range (LoRa) to higher layers for processing and analysis, as illustrated in Figure 2 [37].

Such layered architectures enable efficient data aggregation and system-wide visibility. Recent development also highlights the integration of LPWSNs with green networking principles and emerging communication paradigms, including sixth-generation (6G) systems. Energy-efficient communication protocols, low-power devices, and the adoption of renewable energy sources contribute to reducing the environmental impact of industrial networks while enhancing system sustainability and resilience [38].

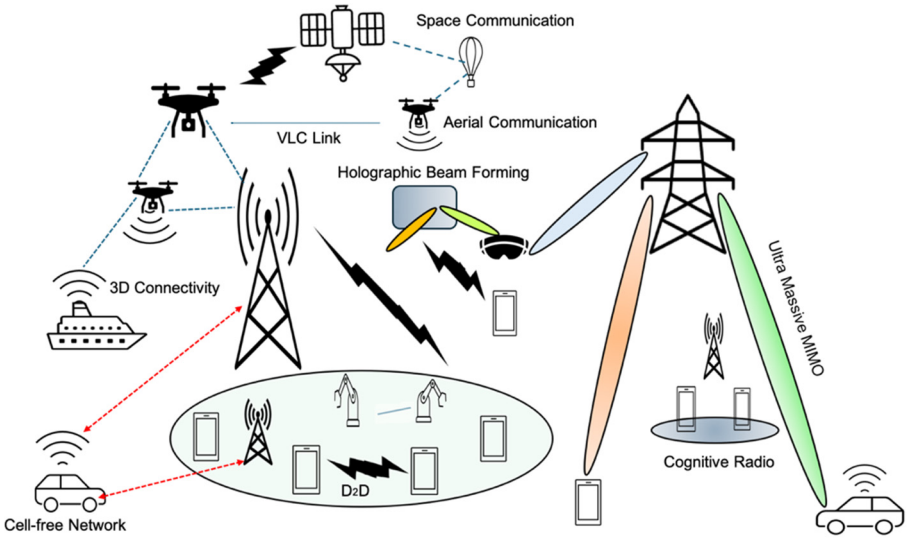


Figure 2. Smart manufacturing architecture with 6G communication (adapted with permission from Ref. [38]. Copyright 2023, © IEEE).

To address the increasing data demands of industrial applications, modern LPWSNs are often integrated with edge computing technologies. This allows data processing to occur close to the source, reducing latency, improving response times, and alleviating bandwidth constraints. However, several challenges remain. Energy efficiency continues to be a critical concern due to battery limitations in long-term deployments. Additionally, security vulnerabilities expose LPWSNs to cyber threats such as data breaches and network disruption, necessitating robust protection mechanisms, including lightweight cryptographic techniques such as elliptic curve cryptography [39]. Scalability is another key challenge, particularly in large-scale deployments, where efficient routing protocols and cluster-based network management are required to maintain performance. Practical implementations demonstrate the effectiveness of LPWSNs in industrial environments. For example, in pharmaceutical manufacturing, LPWSNs have been deployed to monitor environmental conditions, ensuring compliance with strict regulatory standards while improving operational reliability [40]. Looking forward, the integration of LPWSNs with AI, 5G/6G communication technologies, and blockchain is expected to further enhance smart manufacturing systems. AI enables predictive maintenance and anomaly detection, while advanced communication technologies provide ultra-reliable, low-latency connectivity. Blockchain can additionally support secure and transparent data management. Together, these technologies contribute to the development of autonomous, intelligent, and self-optimising manufacturing systems [41,42].

3. Real-Time Data Synchronisation Techniques and Challenges in LPWSNs

3.1. Timing Synchronisation Protocols

Wireless sensor networks (WSNs) used in supervisory control systems require accurate time synchronisation to ensure that data collected from distributed sensors remains consistent and reliable [43]. Accurate synchronisation is particularly important in latency-sensitive applications such as industrial monitoring, process automation, smart manufacturing, and healthcare systems, where even minor timing mismatches can affect decision-making, fault detection, and control operations. However, achieving precise synchronisation in LPWSNs remains challenging due to constrained energy resources, limited computational capabilities, packet delays, and dynamic network conditions. Consequently, several synchronisation protocols have been developed to balance accuracy, scalability, energy efficiency, and communication overhead.

One of the earliest and widely recognised approaches is Reference Broadcast Synchronisation (RBS). Instead of synchronising directly with the sender nodes to compare their local clock, a common broadcast reference message is used. This approach significantly reduces uncertainties associated with sender-side transmission delays and medium access latency, thereby improving synchronisation accuracy [44]. Because the reference packet does not contain a timestamp generated by the sender, the protocol minimises non-deterministic delays that commonly affect traditional sender–receiver synchronisation schemes. However, RBS requires multiple message exchanges among neighbouring nodes to compare timestamps, which increases communication overhead and energy consumption. As network density and scale increase, the number of reference exchanges grows substantially, limiting the practicality of RBS in large-scale or energy-constrained LPWSNs. Also, the protocol performs less effectively in highly dynamic environments where node mobility and unstable connectivity introduce additional synchronisation complexity.

Another prominent synchronisation method is the flooding time synchronisation protocol (FTSP), which was specifically designed to provide high synchronisation accuracy in multi-hop WSN environments. FTSP employs a hierarchical flooding mechanism in which a root node periodically disseminates timestamped synchronisation packets throughout the network. Nodes then apply linear regression-based clock correction techniques to estimate and compensate for clock drift over time, improving long-term synchronisation stability [45]. Compared with RBS, FTSP demonstrates better scalability and robustness in multi-hop topologies because synchronisation information propagates efficiently across the network hierarchy. In addition, FTSP is more resilient to local clock fluctuations and temporary communication disruptions due to its drift compensation mechanism. Nevertheless, the protocol can experience increased latency and communication overhead in large-scale deployments because synchronisation messages must propagate hop-by-hop through multiple intermediate nodes. Frequent flooding also contributes to higher energy consumption, which may reduce network lifetime in battery-powered LPWSNs. Moreover, maintaining a stable root node introduces a potential single point of failure, particularly in industrial environments with harsh operating conditions or intermittent connectivity.

The Timing-Sync Protocol for Sensor Network (TPSN), originally proposed by Ganeriwal et al. [46], is another widely adopted solution for network-wide synchronisation in WSNs. TPSN operates in two main phases: a level discovery phase and a synchronisation phase. During the discovery phase, nodes are organised into a hierarchical tree structure, where each node is assigned a level according to its distance from a root node. This hierarchical organisation enables structured communication and reduces unnecessary synchronisation exchanges between unrelated nodes. In the synchronisation phase, TPSN follows a sender–receiver mechanism in which a receiver synchronises its clock with that of a sender through a two-way message exchange process, as illustrated in Figure 3A [47,48].

For example, when Node A sends a timestamped message at time T_1, Node B receives it at T_2 and sends a response at time T_3 that is received by Node A at T_4; the relationship between the transmitted and received timestamps can be expressed as follows [47,48]:

$$T_2 = T_1 + D + d \quad (1)$$

where D represents the relative clock offset between Node A and Node B, while d denotes the propagation delay between the two nodes. Node B then transmits an acknowledgement containing timestamps T_1, T_2, and T_3, together with its level information. Upon receiving this response at time T_4, Node A calculates the clock offset and propagation delay using the standard TPSN equations [48,49]:

$$D = [(T_2 - T_1) - (T_4 - T_3)]/2 \quad (2)$$

$$\text{Offset} = [(T_2 - T_1) + (T_3 - T_4)]/2 \quad (3)$$

During the discovery phase, nodes are assigned hierarchical levels that form a tree-based structure rooted at a reference node (Level 0), as shown in Figure 3B [50]. This layered architecture enables synchronisation to propagate systematically throughout the network while reducing redundant communication overhead. In the synchronisation phase, each node performs a two-way handshake with its parent node in the hierarchy, similar to the mechanism employed in the Network Time Protocol (NTP) [47,49]. Through this process, synchronisation propagates from the root node to all other nodes, enabling network-wide temporal alignment [48].

The hierarchical structure of TPSN provides good scalability; nodes synchronise locally with their parent nodes while maintaining overall network consistency [48,51]. Compared with RBS, TPSN generally achieves lower communication overhead and improved synchronisation precision because of its structured sender–receiver approach. However, unlike FTSP, TPSN is less tolerant to topology changes and node mobility due to its dependence on a stable hierarchical structure. Although TPSN can achieve high synchronisation accuracy in relatively static deployments, maintaining the hierarchy can increase energy consumption and management overhead in dynamic environments where nodes frequently join, leave, or move within the network. Since each node depends on its parent for synchronisation, topology changes require repeated reconfiguration of the network hierarchy, introducing additional communication costs and latency [49,50]. This dependency also increases vulnerability to node failures, link instability, and potential security attacks targeting parent or root nodes. Consequently, TPSN is generally more suitable for stable industrial monitoring systems than highly dynamic or mobility-driven LPWSN applications [49,51–54].

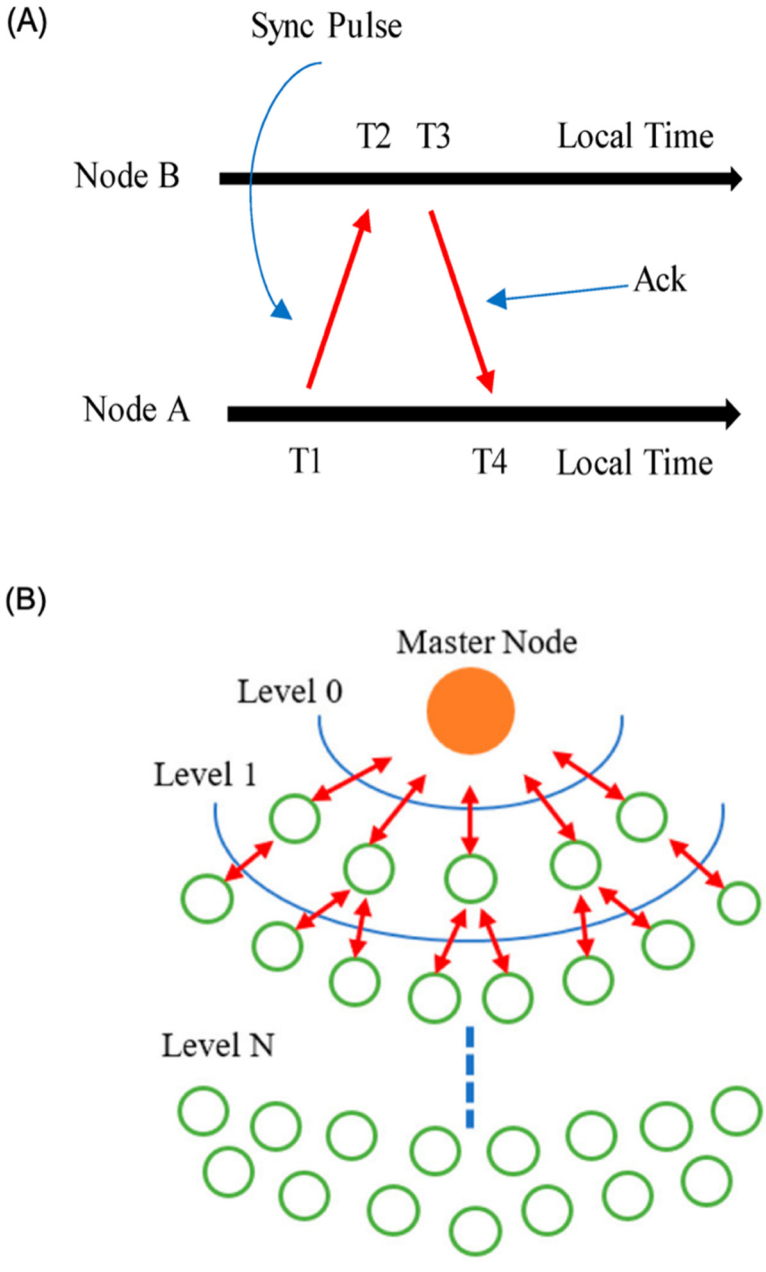


Figure 3. (**A**) Synchronisation between two nodes and (**B**) hierarchical topology used in TPSN. Adapted from [53].

Recent advancements in WSN time synchronisation have increasingly focused on protocols designed for industrial-grade reliability, ultra-low latency, and deterministic communication. One notable example is Glossy (a synchronous flooding protocol), which exploits constructive interference and synchronous transmissions to achieve sub-microsecond synchronisation accuracy across multiple nodes. Unlike traditional flooding approaches, Glossy enables highly efficient network-wide dissemination with extremely low latency, making it particularly attractive for mission-critical industrial automation and cyber-physical systems. However, its effectiveness depends heavily on precise radio timing and strict hardware synchronisation requirements, which may complicate deployment in heterogeneous LPWSN environments.

Similarly, the time-slotted channel hopping (TSCH) protocol, introduced as part of the IEEE 802.15.4e standard, combines time synchronisation with channel hopping to improve both reliability and energy efficiency [55]. TSCH organises communication into repeating slot frames in which nodes transmit and receive data within tightly synchronised time slots while dynamically hopping across different frequency channels to minimise interference. Compared with conventional contention-based communication schemes, TSCH offers improved determinism, lower packet collision rates, and enhanced robustness in noisy industrial environments. This capability is particularly beneficial in smart manufacturing and SCADA-based systems where predictable communication latency is essential. However, TSCH scheduling and network management can become increasingly complex as network size and traffic heterogeneity grow. In addition, maintaining strict synchronisation across dense LPWSN deployments may introduce additional computational and coordination overhead, particularly in resource-constrained sensor nodes [56].

Overall, no single synchronisation protocol fully satisfies the competing requirements of accuracy, scalability, energy efficiency, robustness, and security in LPWSNs. RBS offers high precision but suffers from communication overhead, FTSP provides strong scalability and drift compensation at the cost of increased flooding traffic, while TPSN achieves accurate hierarchical synchronisation but lacks flexibility in dynamic environments. Emerging approaches such as Glossy flooding and TSCH demonstrate significant improvements for industrial and real-time applications; however, challenges related to interoperability, deployment complexity, security resilience, and energy-aware adaptation remain active research problems in next-generation LPWSNs.

Collectively, RBS, FTSP, TPSN, Glossy, and TSCH exhibit distinct trade-offs. RBS achieves high accuracy by eliminating sender-side uncertainty but incurs additional message exchanges. FTSP provides robust multi-hop synchronisation but may experience increased latency in large-scale deployments. TPSN offers good accuracy and scalability through its hierarchical structure, although maintaining the hierarchy can increase overhead in dynamic networks. Glossy achieves sub-microsecond synchronisation accuracy but requires tight coordination and may be less energy-efficient in some deployment scenarios. TSCH provides enhanced reliability and energy efficiency through scheduled communication and channel hopping, making it particularly attractive for industrial IoT environments. Consequently, protocol selection depends on application requirements, network scale, mobility, latency constraints, and energy availability.

3.2. Clock Drift Compensation Techniques

Clock drift is an inherent challenge in WSNs, arising from variations in the oscillator frequencies of individual sensor nodes, which gradually lead to inconsistencies in time

measurement over extended operating periods [57]. In LPWSNs, even small timing deviations can accumulate over time and significantly affect synchronisation accuracy, particularly in real-time supervisory control, industrial automation, and healthcare monitoring applications where precise temporal coordination is essential. Consequently, effective drift compensation mechanisms are required to minimise cumulative timing errors while maintaining low energy consumption.

One common approach for mitigating clock drift involves software-based compensation techniques, where sensor nodes periodically estimate and adjust their local clocks using synchronisation updates. Techniques such as linear regression are widely employed to model drift behaviour by analysing historical timestamp information and predicting future clock deviations [58,59]. Compared with hardware-based methods, software-driven compensation offers greater flexibility and lower implementation cost, making it particularly attractive for resource-constrained LPWSNs. However, low-cost oscillators commonly used in sensor nodes typically exhibit limited stability and are highly sensitive to environmental conditions such as temperature variation, humidity, voltage fluctuation, and hardware ageing. As a result, software-only approaches may struggle to maintain long-term synchronisation accuracy in harsh or highly dynamic operating environments. In contrast, hardware-based solutions utilise high-stability oscillators or temperature-compensated crystal oscillators (TCXOs) to minimise drift directly at the hardware level. These components significantly improve timing precision and long-term stability by reducing the influence of environmental fluctuations on oscillator frequency. Although hardware-assisted compensation can achieve superior synchronisation accuracy, the associated increase in cost, energy consumption, and hardware complexity limits its suitability for large-scale and low-power LPWSN deployments. Consequently, purely hardware-based synchronisation approaches are less commonly adopted in practical WSN applications, particularly in cost-sensitive or battery-powered systems [60].

To balance synchronisation accuracy and energy efficiency, many modern LPWSN synchronisation frameworks employ adaptive drift compensation strategies. In these approaches, synchronisation intervals are dynamically adjusted according to observed drift behaviour, application requirements, and network conditions. Rather than relying on fixed periodic updates, sensor nodes initiate synchronisation only when estimated clock drift exceeds a predefined threshold. This adaptive mechanism reduces unnecessary communication overhead while preserving acceptable timing accuracy, thereby improving overall energy efficiency and network lifetime. Such approaches are particularly effective in dynamic environments where traffic patterns, interference levels, and node activity fluctuate over time.

Recent research has increasingly explored hybrid compensation approaches that combine software estimation techniques with environmental awareness and intelligent prediction models. For example, temperature-aware drift compensation frameworks incorporate sensor-derived environmental measurements to predict oscillator behaviour more accurately, thereby improving long-term synchronisation stability without requiring expensive hardware upgrades. Compared with conventional linear estimation methods, these context-aware approaches provide better adaptability under varying environmental and operational conditions. In addition, machine learning-based compensation techniques have emerged as a promising direction for modelling nonlinear drift behaviour and improving prediction accuracy in complex LPWSN environments. By learning temporal drift patterns from historical synchronisation data, ML models can proactively estimate clock deviations and reduce the frequency of synchronisation exchanges [61].

These approaches are particularly attractive for industrial IoT and smart healthcare systems, where network conditions and environmental factors may change continuously. However, implementing ML-driven drift compensation on resource-constrained sensor

nodes introduces additional computational and energy challenges that remain insufficiently addressed in current research. Furthermore, the reliability and explainability of AI-based predictions under safety-critical operating conditions require further investigation before widespread deployment can be achieved.

On balance, existing drift compensation techniques involve important trade-offs between synchronisation accuracy, hardware complexity, energy efficiency, and scalability. Software-based methods provide flexibility and low cost but may suffer from long-term instability, whereas hardware-assisted approaches improve precision at the expense of increased power consumption and deployment cost. Emerging adaptive and AI-assisted compensation techniques offer improved intelligence and context awareness; however, their practical implementation in large-scale LPWSNs still requires further optimisation in terms of computational efficiency, robustness, and security resilience.

In addition to clock drift, an important challenge in distributed sensing systems is sampling-rate mismatch among heterogeneous sensors and multiple inertial measurement units (IMUs). Even when devices are time-synchronised, small differences in sampling frequencies can accumulate over time, leading to temporal misalignment of data streams, reduced fusion accuracy, and degraded system performance. This issue is particularly relevant in LPWSN-based applications such as motion tracking, healthcare monitoring, and human activity recognition, where accurate coordination between IMUs, biosensors, and other sensing devices is required. Recent studies have highlighted the importance of jointly addressing clock synchronisation and sampling-rate consistency through techniques such as resampling, interpolation-based alignment, and timestamp correction to harmonise multi-rate sensor data before fusion. These approaches extend traditional clock drift compensation by improving both timing accuracy and data consistency across distributed sensing platforms and represent an important direction for future research in real-time LPWSN deployments [58–61].

3.3. Data Aggregation and Compression for Energy Efficiency

In WSNs used for supervisory control and industrial monitoring applications, efficient data management is essential to reduce energy consumption and extend the operational lifetime of battery-powered sensor nodes. Since wireless communication represents the most energy-intensive operation in WSNs, techniques such as data aggregation and compression are widely employed to minimise redundant transmissions and improve overall network efficiency [62]. These techniques are particularly important in LPWSNs, where communication overhead directly affects synchronisation performance, latency, and long-term network sustainability.

Data compression plays a critical role in reducing network traffic by decreasing the volume of sensed data transmitted across the network. In general, compression techniques can be categorised into lossless and lossy methods depending on whether the original data can be perfectly reconstructed after decompression. As illustrated in Figure 4A, lossless compression enables exact data recovery with high fidelity but typically achieves lower compression ratios, whereas lossy compression achieves greater compression efficiency at the expense of some information loss. This trade-off between data accuracy and compression efficiency is a key consideration in LPWSN design, particularly in applications where real-time decision-making depends on reliable sensor information.

Lossless compression methods preserve the original data exactly after decompression, making them suitable for applications requiring high data fidelity, such as SCADA systems, industrial automation, and healthcare monitoring. Common approaches include Huffman coding and Lempel–Ziv–Welch (LZW), which reduce redundancy by exploiting statistical patterns within the sensed data [63]. In contrast, lossy compression techniques

achieve higher compression ratios by selectively discarding less critical information, making them more appropriate for applications where approximate measurements are acceptable.

A wide range of compression techniques has been developed specifically for WSN environments, as shown in Figure 4B [64,65]. These approaches include: (1) string-based methods, which adapt traditional text compression techniques for sensor data processing; (2) image-based approaches, which apply image compression after hierarchical organisation of sensor nodes; (3) distributed source coding, based on the Slepian–Wolf theorem, which enables correlated sensor data to be encoded separately while preserving reconstruction efficiency; (4) compressed sensing, which exploits signal sparsity to reduce both sampling and transmission requirements; and (5) data aggregation techniques, where intermediate nodes combine multiple sensor readings through operations such as averaging, filtering, or summation to minimise communication overhead. Among these methods, compressed sensing and aggregation-based strategies are generally considered the most energy-efficient because they directly reduce transmission frequency, which is the dominant source of power consumption in LPWSNs [66–68].

Hybrid approaches that combine data aggregation with compression techniques have demonstrated further improvements in energy efficiency and network performance. For example, compressed sensing enables sensor nodes to transmit only a subset of measurements while still allowing accurate signal reconstruction at the receiver. Such strategies maintain a balance between energy savings and acceptable data fidelity, thereby improving the efficiency of WSN-based supervisory control systems [69]. However, aggressive compression or excessive aggregation may introduce reconstruction errors, information loss, or increased processing delays, which can negatively affect synchronisation accuracy and real-time responsiveness in latency-sensitive applications.

Beyond data compression, routing strategies also play a critical role in optimising energy efficiency by determining how sensed data is transmitted through the network toward the base station. Clustering-based routing protocols such as low-energy adaptive clustering hierarchy (LEACH) reduce communication costs by organising sensor nodes into clusters and assigning cluster heads responsible for data aggregation and forwarding [70]. Although clustering significantly improves scalability and reduces redundant transmissions, cluster-head selection and maintenance may create uneven energy consumption across the network, potentially leading to premature node depletion and reduced network stability.

To further improve performance, hybrid optimisation frameworks have been proposed that integrate adaptive compression techniques with intelligent routing strategies. For example, adaptive lossless data compression (ALDC) and fast efficient lossless adaptive compression scheme (FELACS) can be combined with optimisation-based routing methods such as ant colony optimisation (ACO) and cuckoo search (CS) to enhance overall network efficiency.

ALDC dynamically adjusts compression parameters according to the statistical properties of sensed data by exploiting temporal correlations between consecutive measurements. Typically, predictive encoding techniques estimate the predicted value $\hat{x}\imath$ from previous samples, while only the prediction error $e_i = x_i - \hat{x}\imath$ is encoded, thereby reducing transmission redundancy. Similarly, FELACS improves compression performance through lightweight adaptive encoding, variable-length coding, and run-length encoding techniques that minimise computational overhead while preserving lossless reconstruction.

On the routing side, ACO is inspired by the foraging behaviour of ants, where routing paths are probabilistically selected according to pheromone intensity and path desirability. The probability of selecting a path from node *i* to node *j* is defined as:

$$P_{ij} = [(\tau_{ij})^{\alpha} (\eta_{ij})^{\beta}]/\sum_{k} (\tau_{ik})^{\alpha} (\eta_{ik})^{\beta} \quad (4)$$

where τ_{ij} represents pheromone intensity, η_{ij} denotes the routing cost metric (e.g., inverse distance or energy cost), and α and β control their relative influence. This mechanism enables the network to gradually converge towards energy-efficient routing paths.

In contrast, CS employs Levy flight-based search optimisation to explore the routing search space efficiently and identify optimal routing paths. In this approach, inefficient routes are iteratively replaced by more suitable alternatives, improving network performance and balancing energy consumption. The Levy flights step length is defined as:

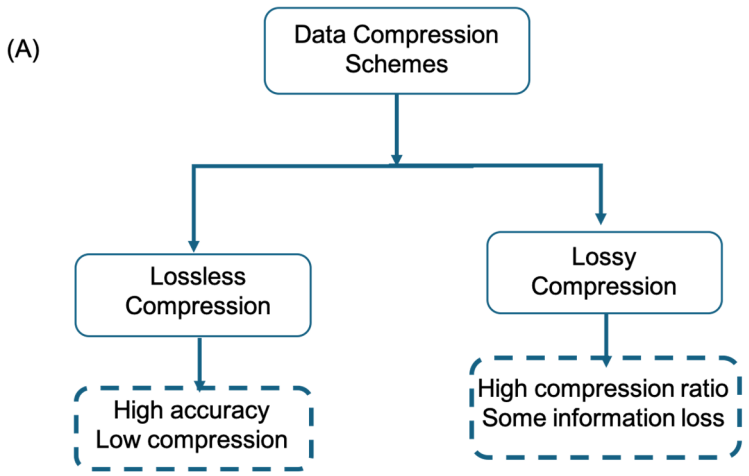
$$L(s) = \mu/(|s|^{1+\beta}) \quad (5)$$

where μ is a scaling constant, s represents the step size, and β controls the step distribution.

In these hybrid optimisation frameworks, sensed data are first compressed at the sensor node using ALDC or FELACS before being routed through optimised communication paths generated by ACO or CS algorithms, as illustrated in Figure 4C. This integrated optimisation of compression and routing reduces transmission overhead, balances energy consumption across nodes, and extends overall network lifetime while maintaining reliable data delivery [71].

Despite these advances, achieving an optimal balance between compression efficiency, computational complexity, routing overhead, latency, and data fidelity remains a major research challenge. Many advanced optimisation algorithms improve energy efficiency but increase processing requirements, making them difficult to deploy on highly resource-constrained sensor nodes. Furthermore, maintaining synchronisation accuracy while aggressively reducing communication traffic remains an unresolved issue in large-scale LPWSNs. Consequently, future research should focus on lightweight adaptive optimisation frameworks capable of jointly managing energy efficiency, real-time communication, and synchronisation reliability under dynamic operating conditions.

It is also noted that routing-focused protocols such as LEACH-based approaches may rely on simplified energy models that do not fully capture idle listening and hardware-specific consumption characteristics, which can lead to optimistic energy estimates in some simulation scenarios. In addition, routing protocols such as RPL, which are widely used in low-power and lossy networks, share structural similarities with hierarchical coordination mechanisms and may offer relevant performance advantages in integrated routing and synchronisation frameworks. However, they are outside the primary scope of this review, which focuses on time synchronisation and energy-efficient data handling in LPWSNs [72].



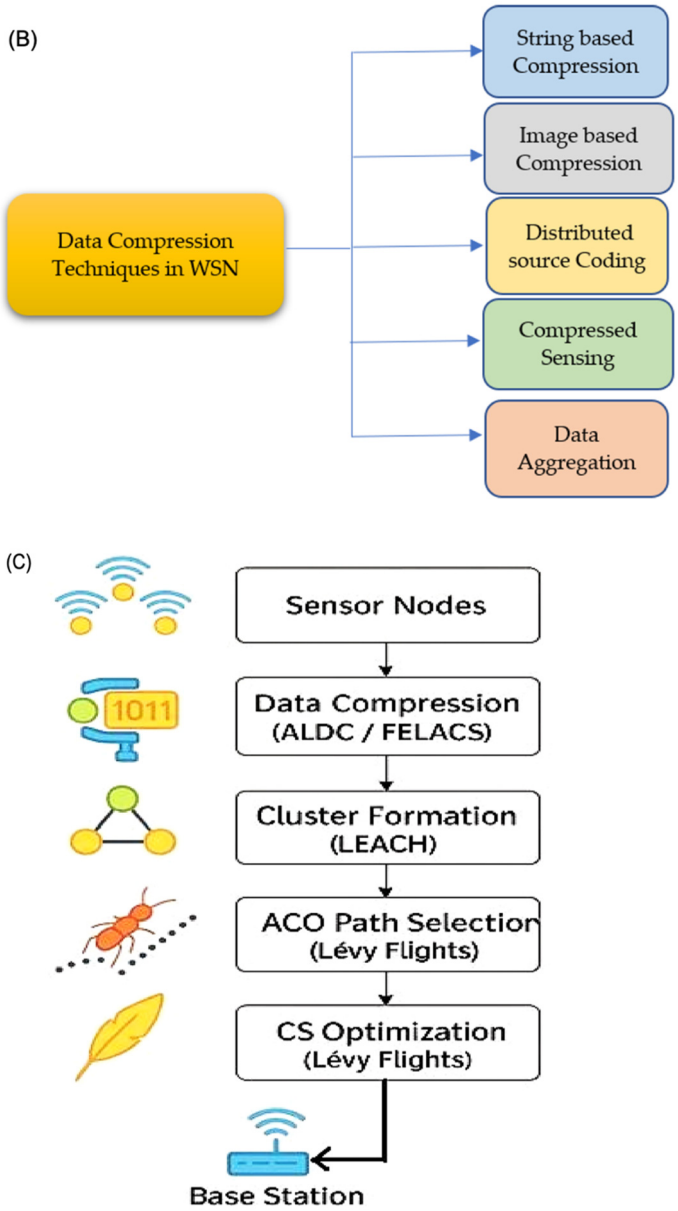


Figure 4. Overview of data compression and energy-efficient optimisation in wireless sensor networks: (**A**) classification of compression schemes (designed by the authors); (**B**) categorisation of compression techniques (adapted from [64]); and (**C**) hybrid framework combining data compression with routing optimisation (adapted from [71]).

3.4. Edge and Fog Computing for Localised Processing

With the growing demand for real-time data processing in supervisory control and industrial automation systems, edge and fog computing paradigms are increasingly being integrated into WSN architectures [73]. These distributed computing approaches reduce latency and improve resource utilisation by moving computational tasks closer to the data source rather than relying exclusively on centralised cloud infrastructures. This shift is particularly important in LPWSNs, where transmitting large volumes of data to remote cloud platforms can introduce communication delays, increase bandwidth consumption, and accelerate energy depletion.

Edge computing enables data processing at or near the sensor nodes, gateways, or local edge devices, allowing preliminary operations such as data filtering, aggregation, and anomaly detection, and local decision-making to be performed before transmission

to higher-level systems. This localised processing reduces communication overhead, conserves bandwidth, and lowers energy consumption, while simultaneously enabling faster response times for latency-sensitive applications [74]. Compared with cloud-centric architectures, edge computing offers improved responsiveness and operational continuity, particularly in environments where real-time decision-making is critical, such as industrial automation, healthcare monitoring, and smart manufacturing systems.

Fog computing extends this concept by introducing distributed processing capabilities across intermediate network layers positioned between the edge and the cloud. This paradigm is especially beneficial in large-scale industrial environments where multiple WSNs support complex supervisory control operations [75]. By distributing computational workloads across fog nodes, the network can reduce congestion, improve scalability, and enhance fault tolerance. Fog architectures also support more efficient coordination between heterogeneous LPWSNs by enabling localised synchronisation management, traffic optimisation, and adaptive resource allocation across different network segments.

In SCADA-enabled supervisory control applications, the integration of edge and fog computing supports efficient data synchronisation, real-time monitoring, and responsive decision-making. These capabilities are essential for maintaining operational stability in latency-sensitive and data-intensive industrial environments. For example, edge-assisted synchronisation can reduce dependency on remote cloud servers by processing timing corrections locally, thereby improving synchronisation responsiveness during communication disruptions or network congestion. Similarly, fog-based coordination can improve scalability by distributing synchronisation tasks across multiple regional processing nodes rather than relying on a single central controller.

Despite these advantages, edge and fog computing also introduce several important challenges that remain active research issues in LPWSNs. Managing distributed computation across heterogeneous devices increases system complexity and may create interoperability problems between different hardware platforms, communication protocols, and software frameworks. In addition, deploying edge and fog infrastructures introduces new security vulnerabilities, including distributed attack surfaces, unauthorised access points, and data privacy concerns.

Another important challenge involves resource orchestration and workload balancing. Although edge processing reduces communication overhead, excessive local computation may increase energy consumption at edge devices and sensor gateways. Similarly, maintaining synchronisation consistency across distributed edge–fog–cloud layers remains difficult in highly dynamic or large-scale deployments. Consequently, future LPWSN architectures will require intelligent orchestration frameworks capable of dynamically balancing latency, energy consumption, computational load, and synchronisation accuracy across distributed processing environments. Overall, edge and fog computing provide important opportunities for improving scalability, responsiveness, and real-time synchronisation in LPWSNs. However, practical deployment still requires addressing challenges related to interoperability, security, distributed management, and energy-aware coordination [73–75]. A Comparative analysis of real-time data synchronisation techniques in LPWSNs is presented in Table 1.

Table 1. Comparative analysis table for real-time data synchronisation techniques in LPWSNs.

Technique	Description	Advantages	Limitations	Applications	Ref
Time Synchronisation Protocols (RBS, FTSP, TPSN)	Clock synchronisation protocols ensuring accurate and consistent	RBS: high precision; mitigates delay effects. FTSP: robust multi-hop accuracy.	RBS: high overhead; poor scalability. FTSP: high energy use; latency in large networks.	RBS: Small-scale, energy-constrained networks. FTSP: environmental monitoring;	[44,53,54]

	time alignment in sensor networks	TPSN: low overhead; precise offset estimation	TPSN: limited flexibility; no drift compensation	healthcare. TPSN: general WSN synchronisation	
Clock Drift Compensation Techniques (RTT, NTP, PTP)	Methods that estimate delay and clock offset to reduce drift and maintain synchronisation accuracy	RTT: simple delay estimation; periodic recalibration. NTP: continuous adjustment; widely deployable. PTP: sub-microsecond accuracy; precise offset correction	RTT: sensitive to network delays; limited precision. NTP: lower accuracy in constrained networks; higher overhead. PTP: requires specialised hardware; higher cost and complexity	RTT: delay-sensitive applications. NTP: large-scale general WSNs. PTP: industrial automation; telecom systems	[45,54]
Data Aggregation and Compression	Reduces transmitted data through aggregation and compression to improve energy efficiency	Fewer transmissions; lower communication overhead; preserves data integrity (lossless methods)	Processing overhead; compression latency; reconstruction complexity (compressed sensing)	Industrial monitoring; smart cities; smart agriculture; environmental monitoring	[63,65]
Edge and Fog Computing	Localised data processing to reduce latency, bandwidth use, and cloud dependence	Reduced congestion; lower energy use; real-time response.	Higher processing demands; architectural complexity; limited scalability for constrained devices	Industrial automation; smart grids; IoT-based supervisory control	[73,74]

RBS: Reference Broadcast Synchronisation; FTSP: Flooding Time Synchronisation Protocol; TPSN: Timing-Sync Protocol for Sensor Network; RTT: Round-Trip Time; NTP: Network Time Protocol; PTP: Precision Time Protocol.

3.5. Challenges in Real-Time Data Synchronisation

3.5.1. Latency Due to Network Congestion

WSNs consist of multiple sensor nodes that collect and transmit data to a central controller. As the number of nodes increases, network congestion leads to excessive data transmissions, resulting in increased latency and degraded synchronisation performance. This is particularly critical for time-sensitive applications such as industrial automation, environmental monitoring, and healthcare systems, where delays can lead to outdated or incorrect decision-making [76].

Contention-based medium access control (MAC) protocols are a primary source of latency. Carrier-sense multiple access with collision avoidance (CSMA/CA), widely used in WSNs, reduces collisions but introduces delays as nodes must wait for a free communication channel before transmitting [77]. These delays become more pronounced in dense networks. Additionally, multi-hop communication further contributes to latency, as data packets traverse multiple intermediate nodes, incurring transmission, processing, queuing, and retransmission delays [78]. Under heavy network load, increased queuing delays at intermediate nodes further degrade synchronisation performance.

3.5.2. Energy Constraints and Battery Limitations

Energy efficiency remains a critical challenge in LPWSNs, as sensor nodes are typically battery-powered and often deployed in inaccessible locations. Continuous data collection and transmission required for supervisory control applications significantly reduces battery life [79]. Energy constraints can disrupt synchronisation, as nodes may enter low-power or sleep states, causing delays and inconsistencies in time-critical data exchange.

Radio communication is the primary source of energy consumption, with both transmission and reception requiring significant power. Frequent synchronisation updates further accelerate energy depletion. To mitigate this, many WSNs employ duty cycling, where nodes alternate between active and sleep states to conserve energy [80]. However, this introduces synchronisation challenges, as nodes may not be active simultaneously. Additional energy is consumed in maintaining synchronisation, particularly for clock drift compensation. Frequent synchronisation improves accuracy but increases energy usage [81]. Techniques such as energy harvesting (e.g., solar or vibration sources) and adaptive sleep scheduling can extend network lifetime by ensuring only essential nodes remain active during critical synchronisation periods.

3.5.3. Packet Loss and Synchronisation Errors in Large-Scale Deployments

In large-scale WSNs, synchronisation accuracy is often degraded due to packet loss and accumulated timing error. Packet loss occurs when transmitted data fails to reach its destination due to interference, weak signal strength, or network congestion. High packet loss disrupts synchronisation processes, leading to delays and inconsistencies in supervisory control applications [82]. Industrial environments further exacerbate this issue due to electromagnetic interference, physical obstruction (e.g., metal structures), and harsh environmental conditions. Synchronisation errors may also arise from node failures caused by battery depletion, hardware faults, or software malfunctions, which are common in large-scale deployments. To mitigate these issues, error control techniques such as forward error correction (FEC) or automatic repeat reQuest (ARQ) can be employed to recover lost data. Additionally, redundancy in synchronisation mechanisms, such as multiple reference nodes, improves robustness. Adaptive synchronisation algorithms that adjust synchronisation frequency based on network conditions can further enhance accuracy and reliability [83,84].

3.5.4. Security and Data Integrity Concerns

Ensuring secure and reliable real-time data synchronisation in WSN-based supervisory control systems is a critical challenge, particularly in safety-critical domains such as industrial automation, energy systems, and healthcare monitoring. Due to their wireless, distributed, and resource-constrained nature, WSNs and LPWSNs are inherently exposed to a wide range of security vulnerabilities that can directly impact accuracy, data integrity, and overall system stability. Spoofing attacks represent one of the most serious threats in synchronisation-sensitive environments, where adversaries inject false timing or synchronisation messages to manipulate sensor clocks. This can lead to cascading inconsistencies in distributed time references, ultimately affecting coordinated control operations in SCADA systems. Similarly, denial-of-service (DoS) attacks can disrupt synchronisation protocols by overwhelming nodes with excessive requests or malicious traffic, resulting in rapid energy depletion and communication breakdown. Also, passive attacks such as eavesdropping and active manipulation attacks such as data tampering can compromise both the confidentiality and integrity of synchronisation data, leading to incorrect system states (i.e., incorrect operating conditions) and unreliable decision-making [85,86]. In industrial SCADA environments, these attacks are particularly critical because compromised synchronisation can disrupt closed-loop control processes, de-stabilise automation workflows, and potentially cause operational hazards in physical systems. Unlike general IoT networks, SCADA systems require deterministic timing guarantees, meaning that even small synchronisation errors introduced by malicious interference can have severe consequences.

To address these challenges, lightweight security mechanisms have traditionally been employed due to the limited computational and energy resources of LPWSNs. Encryption

protocols such as TinySec and MiniSec provide basic confidentiality and integrity protection for synchronisation messages, while authentication techniques such as message authentication codes (MACs) and lightweight digital signatures ensure that messages originate from legitimate nodes and have not been modified in transit. Intrusion detection systems (IDS) can also monitor network behaviour to identify abnormal synchronisation patterns and detect potential attacks, enabling administrators to respond to threats in a timely manner [30]. However, conventional security mechanisms are increasingly insufficient to address modern threat landscapes in large-scale LPWSNs, particularly as these networks become more interconnected and integrated with cloud, edge, and AI-driven systems. This has led to growing interest in more adaptive and layered security frameworks.

One emerging approach is the adoption of zero-trust architecture (ZTA), which assumes that no device, node, or communication request should be inherently trusted, even within the same network boundary. In LPWSNs, ZTA-based designs enforce continuous authentication, fine-grained access control, and real-time verification of synchronisation messages. This is particularly relevant for distributed SCADA and industrial IoT environments, where compromised nodes may otherwise be exploited to inject false timing information or disrupt coordination across control layers. Another critical and increasingly relevant issue is the rise of adversarial AI threats, particularly in systems that integrate machine learning for predictive synchronisation or anomaly detection. In such scenarios, attackers may manipulate training data, inject adversarial inputs, or exploit model vulnerabilities to distort synchronisation predictions or trigger incorrect clock adjustments. This creates a new class of security risks where the synchronisation mechanism itself becomes a target of intelligent attacks, rather than just the communication infrastructure. As a result, the integration of AI into LPWSNs introduces a dual challenge: improving performance while simultaneously ensuring robustness against adversarial manipulation.

In addition, the convergence of LPWSNs with SCADA systems introduces specific cyberattack risks targeting industrial control environments. SCADA cyberattacks may include false data injection, command manipulation, replay attacks, and time-shift attacks, where adversaries deliberately distort temporal consistency between sensing and control layers. Such attacks can be particularly damaging in real-time control systems because they exploit the dependency of control logic on accurate and synchronised timestamps, potentially leading to incorrect actuation or delayed response in critical processes. To mitigate these evolving threats, hybrid security frameworks combining lightweight cryptography, behavioural anomaly detection, and AI-assisted intrusion detection are being explored. In particular, AI-based security systems can enhance the detection of synchronisation anomalies by identifying deviations from expected timing behaviour patterns. However, these approaches must be carefully designed to avoid introducing additional computational overhead or latency, which could negatively affect synchronisation performance in LPWSNs [30,86].

Overall, securing real-time synchronisation in LPWSNs requires a shift from isolated cryptographic protections toward multi-layered, adaptive, and intelligence-driven security architectures. Future systems must jointly address communication security, synchronisation integrity, adversarial AI resilience, and SCADA-specific threat models to ensure robust and trustworthy operation in critical infrastructure environments. Table 2 provides a detailed overview of the challenges in real-time data synchronisation, including their causes, impacts, and corresponding mitigation strategies.

Table 2. Challenges, impacts, and mitigation strategies for real-time data synchronisation in WSNs.

Challenge	Root Causes	Impact	Mitigation Strategies	Ref
Latency Due to Network Congestion	Dense traffic; CSMA/CA contention; multi-hop delays	Reduced synchronisation accuracy; degraded real-time performance; increased retransmissions	Priority scheduling; adaptive aggregation; QoS-based bandwidth allocation	[76,78]
Energy Constraints and Battery Life Limitations	Limited battery capacity; energy-intensive communication; duty cycling	Node failures; data inconsistency; reduced synchronisation accuracy due to infrequent updates	Energy-aware MAC protocols (e.g., TDMA); energy harvesting; adaptive sleep scheduling	[80,81]
Packet Loss and Synchronisation Errors in Large-Scale Deployments	Wireless interference; signal degradation; harsh environments; node failures	Synchronisation errors; data inconsistency; network desynchronisation	FEC and ARQ error recovery; redundant reference nodes; adaptive synchronisation	[82–84]
Security and Data Integrity Concerns	Wireless vulnerability; spoofing; DoS attacks	False synchronisation; compromised data integrity; system failures	Lightweight encryption (e.g., TinySec, MiniSec); authentication (MACs, digital signatures); IDS	[86–89]

ARQ: automatic repeat reQuest; CSMA/CA: carrier-sense multiple access with collision avoidance; EMI: electromagnetic interference; FEC: forward error correction; MACs: message authentication codes (for security context); MiniSec: Miniature Security Protocol for Wireless Sensor Networks; TDMA: time division multiple access; TinySec: Tiny Security Architecture for Wireless Sensor Networks; IDS: intrusion detection systems.

4. Recent Advances in Real-Time Data Synchronisation for LPWSNs

4.1. AI/ML-Based Predictive Synchronisation

Recent advances in AI and ML have enabled the development of predictive synchronisation techniques for LPWSNs. Traditional synchronisation methods typically rely on periodic message exchange, which can introduce latency, increase energy consumption, and remain vulnerable to network disturbances and packet losses [90]. Although conventional protocols such as TPSN and FTSP provide reliable synchronisation under relatively stable conditions, their dependence on frequent communication updates can significantly reduce energy efficiency in large-scale or highly dynamic LPWSNs. In contrast, predictive synchronisation approaches leverage historical timing data and learned clock behaviour patterns to estimate and correct synchronisation errors proactively, thereby reducing the need for continuous communication overhead.

A key application of ML in this context is adaptive clock drift compensation. ML models analyse historical synchronisation errors, reference node updates, and environmental factors such as temperature fluctuations, hardware instability, and node mobility to predict future clock drift behaviour. These predictions enable sensor nodes to adjust their clocks locally, significantly reducing synchronisation errors without requiring message exchange [51]. Compared with traditional drift estimation methods, AI-driven prediction models can better adapt to nonlinear clock variations and changing environmental conditions, particularly in industrial and healthcare LPWSNs where operating conditions fluctuate continuously. As a result, communication overhead is reduced, improving both energy efficiency and network lifetime.

In dynamic LPWSN environments, where traffic congestion, interference levels, and node activity vary over time, fixed synchronisation intervals are often inefficient. Deep reinforcement learning (DRL)-based approaches address this limitation by dynamically

adapting synchronisation frequency according to real-time network conditions. Rather than applying uniform synchronisation intervals across the network, DRL agents continuously optimise timing updates based on latency requirements, energy availability, and communication quality. This enables the system to maintain timing accuracy while minimising unnecessary synchronisation traffic and power consumption [91]. For example, in smart grid applications, sensor nodes may increase synchronisation frequency during peak energy demand periods while reducing updates during low-activity intervals, thereby balancing timing precision and energy efficiency.

AI techniques also improve synchronisation robustness through an intelligent anomaly detection mechanism. By analysing real-time sensor behaviour and network traffic patterns, AI models can identify irregularities caused by fault nodes, network congestion, clock instability, or cyberattacks. This enables proactive responses such as adaptive synchronisation reconfiguration, fault isolation, or dynamic rerouting of communication paths, thereby improving network resilience and operational reliability. In addition, AI-assisted synchronisation frameworks can support scalability by dynamically adjusting synchronisation policies across heterogeneous and large-scale LPWSNs, making them suitable for complex industrial IoT deployments [92].

Despite these advantages, AI/ML-based synchronisation approaches introduce several practical and technical challenges that remain insufficiently addressed in current research. Many predictive models require extensive training datasets and computational resources, which may exceed the processing and memory capabilities of low-power sensor nodes. Moreover, continuous model training and inference operations can increase energy consumption, partially offsetting the communication savings achieved through predictive synchronisation. In resource-constrained LPWSNs, balancing model complexity with real-time responsiveness therefore remains a major challenge.

Another important concern involves the explainability and reliability of AI-driven decision-making. In mission-critical applications such as healthcare monitoring and industrial automation, inaccurate predictions or unstable learning behaviour may compromise synchronisation precision and affect system safety. Also, AI-based synchronisation systems are increasingly vulnerable to adversarial machine learning attacks, including poisoned training data, malicious timing manipulation, and false anomaly injection. Such attacks may intentionally disrupt synchronisation accuracy or trigger incorrect adaptive responses, potentially leading to cascading failures in distributed LPWSNs. Consequently, although AI/ML-based predictive synchronisation demonstrates significant potential for improving adaptability, scalability, and energy efficiency, further research is required to develop lightweight, secure, and explainable AI frameworks that can operate reliably under strict resource and real-time constraints. Future work should particularly focus on federated learning, edge AI integration, adversarial resilience, and energy-aware adaptive learning models for next-generation LPWSNs.

4.2. Blockchain-Enabled Secure Data Synchronisation

Blockchain technology has emerged as a promising approach for enhancing the security, integrity, and traceability of data synchronisation in LPWSNs. By maintaining a decentralised and tamper-resistant ledger of synchronisation events and timestamps, blockchain reduces reliance on centralised control entities, which are often vulnerable to cyber-attacks, insider threats, and single points of failure. [93]. This decentralised architecture is particularly attractive for industrial IoT, SCADA, and healthcare systems, where synchronisation, reliability and data authenticity are essential for safe and coordinated operation. One of the primary advantages of blockchain-based synchronisation is trustless verification, in which synchronisation updates are validated collectively by participating

nodes rather than a single authority. Once recorded on the blockchain ledger, synchronisation transactions become effectively immutable, preventing unauthorised modification and improving the integrity of timing information. Compared with conventional centralised synchronisation management, blockchain frameworks provide improved transparency, auditability, and resistance against data tampering or replay attacks. This capability is particularly important in applications where accurate timing directly affects operational safety, distributed coordination, and real-time decision-making.

In addition, smart contracts, which are self-executing programmes embedded within the blockchain framework, can automate synchronisation management processes. These contracts can enforce authentication policies, regulate synchronisation requests, dynamically allocate communications slots, and identify inconsistencies in timing information. For example, in industrial IoT environments, smart contracts can ensure that only authenticated and authorised sensor nodes participate in synchronisation activities, thereby strengthening network security and operational reliability [94]. Such mechanisms are increasingly aligned with zero-trust security architectures, where every device and communication request must be continuously verified rather than implicitly trusted based on network location.

To address the resource constraints of LPWSNs, lightweight blockchain consensus mechanisms such as proof of authority (PoA) and lightweight proof of stake (PoS) have been proposed as alternatives to computationally intensive approaches such as proof of work (PoW). These lightweight consensus strategies significantly reduce computational complexity, communication overhead, and energy consumption while still maintaining secure synchronisation validation. Compared with traditional blockchain implementations, lightweight consensus models are more suitable for low-power sensor environments where battery life and processing capacity are constrained. Blockchain technology also provides valuable support for fault diagnosis, event tracing, and forensic analysis. By maintaining a complete historical record of synchronisation activities, network administrators can identify anomalies, trace the root causes of failures, and implement corrective measures more effectively. This capability is particularly beneficial in critical infrastructure applications, including smart cities, industrial automation systems, and healthcare networks, where traceability and accountability are essential for regulatory compliance and operational safety [95,96].

In healthcare applications, for example, blockchain can enhance the protection of sensitive medical data transmitted through wearable IoT devices and LPWSN-enabled monitoring systems. Its decentralised and verifiable structure helps preserve the authenticity, confidentiality, and integrity of patient information, even in untrusted communication environments. By supporting secure data provenance and controlled information sharing, blockchain offers a robust framework for healthcare data management in distributed LPWSNs [97,98].

Despite these advantages, blockchain-enabled synchronisation still faces several major deployment challenges in practical LPWSN environments. One of the most significant limitations is the additional latency introduced by transaction validation and consensus operations, which may conflict with the ultra-low-latency requirements of real-time industrial and healthcare systems. Even lightweight blockchain mechanisms can generate non-negligible communication and processing overhead, particularly in dense or large-scale sensor deployments.

Scalability also remains a critical concern. As the number of synchronisation events and participating nodes increases, blockchain ledgers may grow rapidly, creating storage and bandwidth burdens for resource-constrained devices. Also, maintaining consensus across heterogeneous LPWSNs can become increasingly complex in environments characterised by intermittent connectivity, node mobility, and fluctuating traffic conditions.

Another emerging concern involves the interaction between blockchain systems and AI-driven synchronisation frameworks. While blockchain can improve trust and traceability, malicious nodes may still attempt adversarial attacks such as false timestamp injection, smart contract exploitation, or consensus manipulation. In industrial SCADA environments, compromised synchronisation records may disrupt coordinated control processes and potentially affect system safety. Therefore, future blockchain-enabled LPWSN architectures must integrate lightweight cryptography, zero-trust verification, AI-assisted threat detection, and energy-aware consensus optimisation to achieve secure and scalable real-time synchronisation. Collectively, blockchain-based synchronisation provides important advantages in terms of decentralisation, security, and traceability. However, challenges related to latency, scalability, computational overhead, and interoperability remain significant barriers to widespread deployment in next-generation LPWSNs.

4.3. Software-Defined Networking (SDN) in LPWSNs

SDN introduces a new paradigm for the management and optimisation of LPWSNs by decoupling the control plane from the data plane. In traditional WSNs, synchronisation is handled locally at individual nodes, which can limit network-wide coordination and adaptability. In contrast, SDN enables centralised control of synchronisation, allowing network-wide timing updates to be managed dynamically based on global network conditions [99]. One of the key advantages of SDN is centralised time management. An SDN controller maintains a global view of the network and coordinates the distribution of synchronisation updates, reducing redundant transmissions and improving timing accuracy. This is particularly beneficial in mission-critical applications, for example, aerospace systems and industrial automations, where precise and reliable synchronisation is essential [99].

Another important capability is dynamic synchronisation path optimisation. SDN controllers can analyse real-time network conditions, including congestion, interference, and node failures, and select optimal paths for propagating synchronisation messages. Unlike static routing approaches, SDN enables adaptive dissemination of timing information, minimising latency and improving overall synchronisation performance. For instance, in smart transportation systems, SDN can prioritise synchronisation updates for traffic control sensors, ensuring accurate and coordinated signal timing. SDN also enhances energy efficiency through intelligent resource allocation. By monitoring node energy levels, the controller can schedule synchronisation tasks in a way that avoids overburdening low-energy nodes, thereby prolonging network lifetime [100,101].

In addition, SDN provides a robust framework for addressing security and privacy challenges in LPWSNs. Its centralised architecture facilitates the enforcement of network-wide security policies, including authentication, access control, and encryption mechanisms. This enables consistent protection of synchronisation data across the network while simplifying management in large-scale deployments. Overall, the integration of SDN with LPWSNs offers a flexible, scalable, and secure approach to real-time data synchronisation, particularly in dynamic and heterogeneous IoT environments [102].

4.4. 5G and LPWAN Integration for High-Speed Synchronisation

The integration of 5G networks with LPWANs represents a significant advancement in achieving high-speed, low-latency, and energy-efficient synchronisation in large-scale sensor networks. 5G technology offers ultra-low latency, high bandwidth, and massive device connectivity, making it well-suited for real-time synchronisation in data-intensive and time-critical applications [103].

One of the most promising features of 5G in this context is network slicing, which enables the creation of dedicated virtual network segments tailored for specific tasks. For

synchronisation, this allows time-sensitive data to be prioritised, ensuring minimal delay and reduced jitter. For example, in autonomous vehicle systems, network slicing can support rapid and reliable synchronisation between vehicles and roadside infrastructure, improving safety and traffic efficiency [104].

However, while 5G provides high performance, it is relatively energy-intensive and may not be suitable for battery-powered LPWSNs. To address this limitation, it is often integrated with LPWAN technologies such as LoRa-WAN and Narrowband IoT (NB-IoT), which offer long-range communication with low power consumption. In such hybrid architectures, LPWAN can handle routine or background synchronisation tasks, while 5G is utilised for high-priority or latency-sensitive updates. This complementary approach enables efficient resource utilisation while maintaining real-time synchronisation capabilities [105]. Also, edge computing in 5G networks enhances synchronisation performance by processing time-sensitive data closer to the source. This reduces end-to-end latency and supports faster decision-making, which is critical in applications such as industrial automation, smart grids, and intelligent transportation systems. Overall, the integration of 5G and LPWAN technologies provides a balanced solution that combines high-speed communication with energy efficiency, making it a promising approach for next-generation LPWSNs requiring reliable and real-time synchronisation [104,105]. Table 3 summarises recent advances in real-time data synchronisation techniques for LPWSNs, highlighting their key characteristics, energy impact, and scalability.

Table 3. Recent advances in real-time data synchronisation for LPWSNs.

Technique	Key Concept	Synchronisation Role	Advantages	Limitations	Energy Impact	Scalability	Example Applications	Ref
AI/ML (Predictive)	Learning-based drift prediction	Adaptive synchronisation, anomaly detection	Lower communication overhead, improved accuracy	Training and model complexity	Low-Moderate	High	Smart grids, IoT monitoring	[106]
Blockchain	Decentralised ledger	Secure timestamp validation	Tamper-resistant, high data integrity	Computational and storage overhead	Moderate-High	Moderate	Healthcare, smart cities	[107]
SDN	Centralised control	Network-wide synchronisation management	Global optimisation, flexibility, coordination	Controller dependency, single point of failure	Low-Moderate	High	Industrial IoT, aerospace systems	[108]
5G + LPWAN	Hybrid communication framework	High-speed, energy synchronisation	Low latency, wide coverage, reliable connectivity	Integration complexity, infrastructure cost	Low (LPWAN)-High (5G)	Very High	Autonomous systems, smart transportation	[103]

5. Applications of Real-Time Data Synchronisation in LPWSNs

5.1. Industrial Automation and Smart Manufacturing

Real-time data synchronisation plays a critical role in enabling predictive maintenance in industrial automation. Modern manufacturing systems rely on distributed sensor networks to continuously monitor equipment health and detect early signs of failure. Accurate time alignment of sensor data is essential; without precise synchronisation, anomalies may be misinterpreted or detected too late, leading to unplanned downtime and increased maintenance costs. LPWSNs support predictive maintenance by providing precisely timestamped data, enabling maintenance teams to identify degradation trends and intervene proactively, thereby extending equipment lifetime and reducing operational costs [109].

Another key application is robotic coordination in smart manufacturing environments. Industrial processes increasingly depend on autonomous robotic arms and collaborative robots (COBOTS) that must operate in a tightly coordinated manner. Even minor timing inconsistencies can lead to misalignment, defective products, or safety risks. Real-

time synchronisation ensures that robotic systems execute tasks in a coordinated sequence, maintaining production efficiency and operational safety. In addition, synchronised LPWSNs enable real-time quality monitoring and control. Distributed sensors continuously track production parameters such as temperature, pressure, and vibration. When integrated with machine vision systems, synchronised data allows for immediate defect detection and rapid corrective actions, improving product quality and manufacturing yield. Overall, real-time synchronisation enhances reliability, efficiency, and safety in modern industrial systems [110].

5.2. Smart Grids and Energy Management Systems

Real-time synchronisation is a fundamental enabler of smart grids, which represent a transition from traditional, centrally controlled power systems to more dynamic and distributed energy networks. Unlike conventional grids, smart grids must accommodate fluctuating demand and integrate diverse energy sources, requiring precise coordination across generation, transmission, and consumption [14].

One of the most critical functions supported by synchronisation is load balancing and demand response management. Accurate timing allows utilities to align electricity generation with consumption patterns, reducing the risk of overloads, blackouts, and energy waste. By leveraging LPWSNs, grid operators can dynamically adjust power distribution in response to real-time demand conditions, improving overall system stability and efficiency [15].

Real-time synchronisation is also essential for renewable energy integration. Sources such as solar and wind are inherently intermittent and depend on environmental conditions. LPWSNs enable continuous communication between distributed energy resources and grid operators, facilitating real-time adjustments in energy generation, storage, and distribution. This coordination supports efficient load shifting, energy storage management, and grid stability [111,112]. Solar energy systems convert solar radiation into electrical power through interconnected components that capture, store, and distribute energy as needed. Similarly, wind energy systems harness the kinetic energy of moving air using turbines to generate electricity. The variability of these sources makes synchronisation with the grid particularly important [112].

To address this variability, energy storage systems (ESS) including mechanical (e.g., pumped hydro, compressed air), thermal, and electrochemical storage play a vital role. Synchronised communication between storage units and the grid ensures that excess energy is stored and redistributed efficiently when demand increases. Furthermore, LPWSNs support fault detection and outage management by enabling real-time monitoring of grid conditions. Synchronised data allows rapid identification of faults and localisation of failures, reducing response times and improving service reliability [113].

In addition, synchronisation contributes to energy efficiency in smart buildings. Devices such as smart thermostats, lighting systems, and appliances coordinate their operation based on occupancy and environmental conditions. This real-time coordination minimises unnecessary energy consumption, enhances system efficiency, and reduces carbon emissions. This coordination is supported by an underlying communication infrastructure, often enhanced by SDN-based frameworks to enable efficient data exchange and network-wide control [111,114]. Figure 5A,B illustrate the overall smart grid architecture and the interactions among key system components within LPWSN-enabled environments.

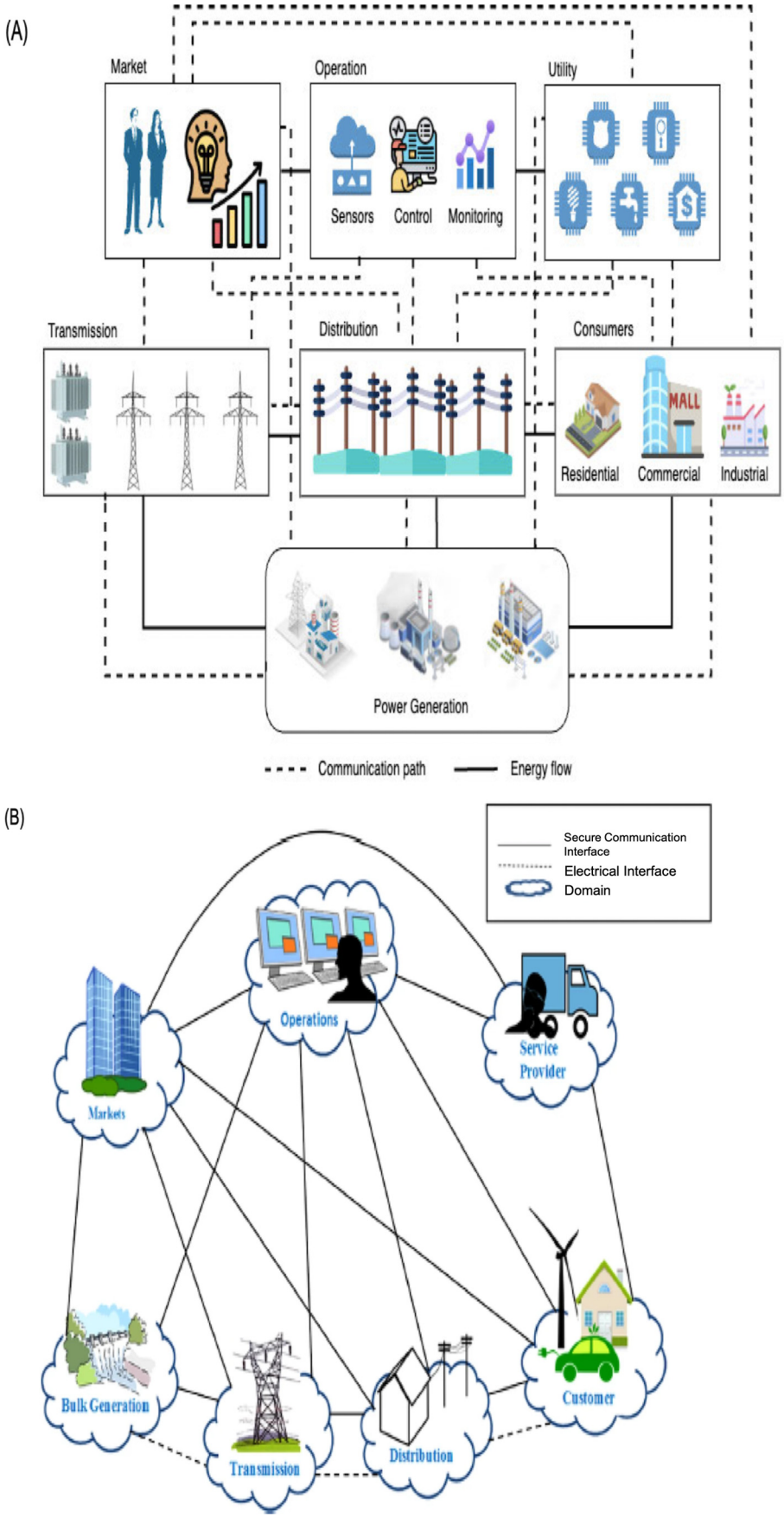


Figure 5. Overview of smart grid systems enabled by LPWSNs, illustrating both system-level interactions and underlying communication architecture. (**A**) Interaction of key actors in a smart grid ecosystem, showing real-time coordination between energy generation sources, storage systems, grid operators, and end users for efficient energy management [114]. (**B**) Smart grid communication

architecture highlighting the integration of network infrastructure and control layers, including SDN-enabled frameworks for efficient data exchange and system coordination [111].

5.3. Environmental and Agricultural Monitoring

LPWSNs are widely used in environmental monitoring and precision agriculture, where real-time data synchronisation is essential for accurate sensing, analysis, and decision-making. By enabling coordinated data collection from distributed sensors, LPWSNs support efficient resource management, environmental protection, and sustainable agricultural practices. In environmental monitoring, synchronised sensor networks measure parameters such as temperature, humidity, carbon dioxide levels, and air pollutants. These time-aligned data streams allow governments and environmental agencies to track environmental changes and support early warning systems for events such as wildfires, air pollution, and natural disasters. Accurate synchronisation ensures that data from multiple locations can be reliably compared and analysed in real time [115].

In precision agriculture, LPWSNs enable smart irrigation and crop management through continuous monitoring of soil, weather, and plant conditions. Typical systems follow a multi-layer architecture consisting of sensing (perception), communication (network), and application layers. Sensors collect data on soil moisture, pH, salinity, and nutrient levels, as well as environmental factors such as temperature, rainfall, solar radiation, and wind conditions. This information is synchronised and processed to optimise irrigation scheduling, fertiliser application, and pest control strategies. However, the diversity of agricultural environments, such as variations in soil type, climate, and farm size, makes the design of optimal system architectures challenging. In addition, the large volume of data generated by distributed sensors introduces challenges in real-time data processing, storage, and communication [116]. LPWSNs can be further enhanced through integration with drones and AI-based analytics, enabling real-time monitoring of crop health, soil conditions, and weather patterns. This allows farmers to make informed decisions that maximise yield while minimising environmental impact [41]. Another important application is wildlife and biodiversity monitoring. Sensors and GPS-enabled tracking devices can synchronise data on animal movement, enabling researchers to study migration patterns, monitor endangered species, and prevent illegal activities such as poaching. Similarly, LPWSNs are used to monitor forests, water bodies, and ecosystems, supporting data-driven conservation efforts [117]. The implementation of LPWSN-based monitoring systems in environmental and agricultural applications typically follows a layered architecture, integrating sensing, communication, and data processing components. These systems enable continuous, synchronised data collection from distributed sensors, supporting real-time analysis and decision-making [118,119]. Figure 6A,B illustrate representative architectures and deployment scenarios for such systems in precision agriculture and environmental monitoring contexts.

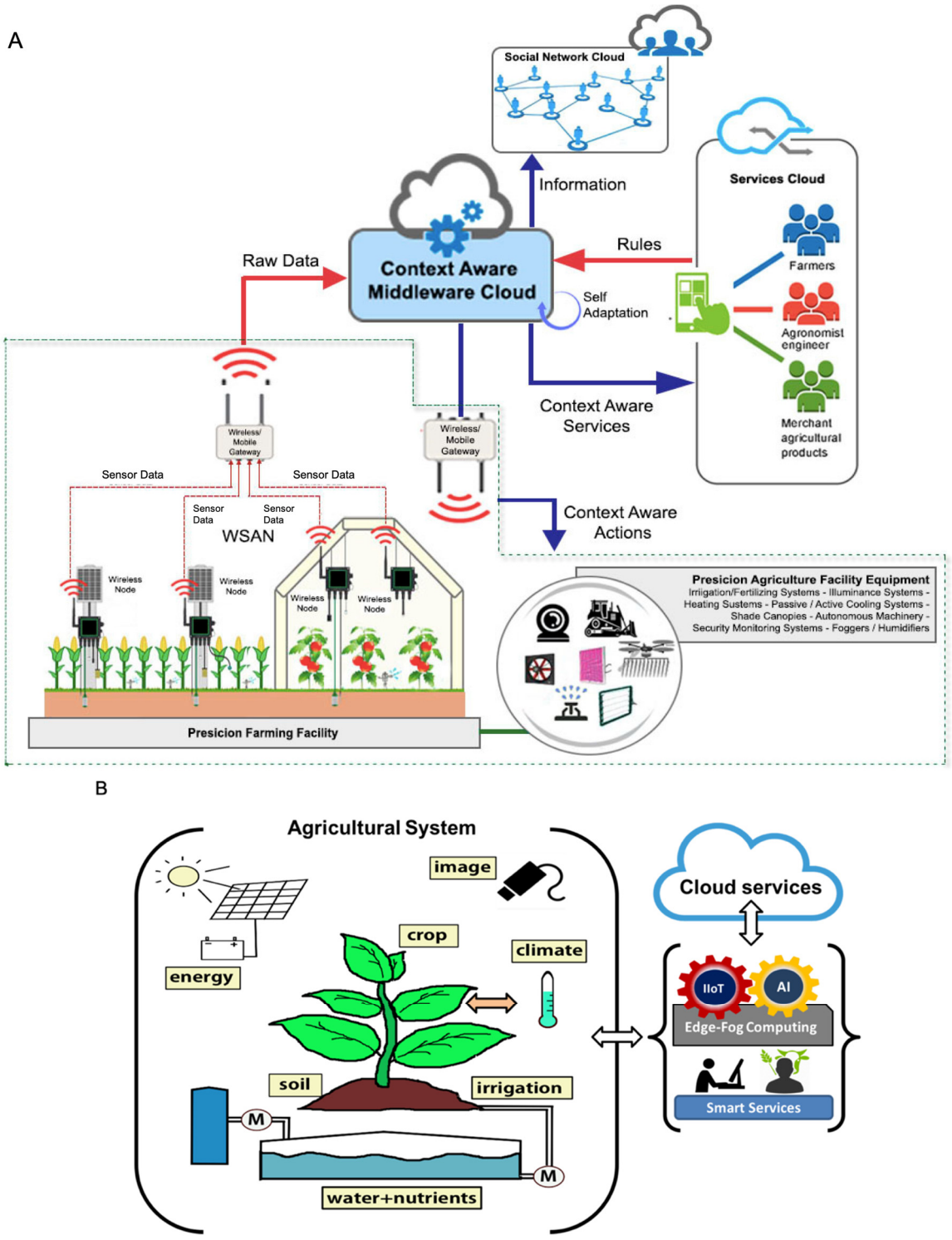


Figure 6. LPWSN-enabled environmental and agricultural monitoring systems. (**A**) Generic IoT-based architecture and data workflow for precision agriculture, illustrating sensor data acquisition, communication, and cloud-based processing [118]. (**B**) Agricultural IoT system showing field-level sensor deployment and communication with control and decision systems [119].

5.4. Healthcare Monitoring with Wearable IoT Devices

Real-time data synchronisation plays a vital role in healthcare applications based on wearable IoT devices. Modern wearables such as smartwatches, fitness trackers, electrocardiogram (ECG) monitors, and continuous glucose monitoring systems rely on synchro-

nised data exchange to provide accurate health insights and enable timely medical interventions. By ensuring consistent and time-aligned data streams, LPWSNs support reliable monitoring of physiological parameters in both clinical and home environments. One of the most significant applications is remote patient monitoring (RPM). Patients with chronic conditions, including diabetes, hypertension, and cardiovascular diseases, can be continuously monitored using wearable sensors that track vital signs such as heart rate, blood glucose levels, and blood pressure. These devices synchronise data with cloud platforms and healthcare providers in real time, allowing clinicians to detect abnormalities early and intervene proactively. This reduces hospital visits while improving patient outcomes and quality of care [11].

Synchronisation is also critical in telemedicine and emergency response systems. Wearable devices can detect critical health events such as arrhythmias or sudden drops in vital signs and generate immediate alerts to healthcare providers or emergency services. This rapid, synchronised communication enables timely medical assistance, which is crucial in life-threatening situations such as cardiac arrest or stroke. In addition, synchronised LPWSNs support rehabilitation and activity monitoring. Wearable motion sensors track patient movements during recovery from surgery or injury, providing real-time feedback to clinicians and enabling personalised rehabilitation plans. This facilitates continuous assessment of patient progress and improves the effectiveness of therapy.

LPWSNs also play an important role in elderly care and fall detection systems. Wearable devices equipped with accelerometers and gyroscopes can detect falls and automatically notify caregivers or emergency responders. This ensures rapid assistance and reduces the risk of severe complications. More broadly, synchronised wearable systems are advancing personalised and data-driven healthcare. Emerging technologies, such as flexible and wearable electronics, enable continuous health monitoring in a non-intrusive manner. When combined with AI-based analytics, synchronised health data can be used to identify disease patterns, predict health risks, and support preventive care strategies, paving the way for decentralised and intelligent healthcare systems [120,121].

Beyond healthcare applications, achieving reliable time synchronisation in wireless body area networks (WBANs) presents several unique challenges. Unlike many industrial LPWSN deployments, wearable healthcare systems operate in highly dynamic environments characterised by user mobility, heterogeneous sensor platforms, variable sampling rates, and intermittent wireless connectivity. Accurate temporal alignment is particularly important when integrating data from multiple sensors, such as ECG monitors, inertial measurement units (IMUs), pulse oximeters, and glucose monitoring devices, where even small timing mismatches can affect data fusion and clinical interpretation. To address these challenges, specialised synchronisation approaches have been developed for WBANs, including lightweight clock synchronisation schemes, adaptive synchronisation strategies, and fractional time-synchronisation methods designed to improve timing accuracy while minimising energy consumption. These approaches recognise the stringent power constraints of wearable devices while maintaining the temporal consistency required for reliable health monitoring and decision support [120–122]. Alongside conventional LPWSN synchronisation protocols, healthcare-oriented WBANs have motivated the development of specialised synchronisation approaches tailored to wearable and implantable devices. For example, fractional-based synchronisation methods have been proposed to improve timing accuracy while minimising energy consumption and communication overhead in body-centric sensor networks. Such approaches are particularly relevant for continuous physiological monitoring applications, where reliable temporal alignment of sensor data is essential for accurate diagnosis and real-time healthcare decision-making [123].

Healthcare monitoring systems can be broadly categorised into decentralised wearable-based approaches and traditional centralised architectures. In wearable systems, data is continuously collected from body-mounted sensors and synchronised with remote healthcare platforms, enabling real-time monitoring and timely interventions. In contrast, centralised healthcare systems rely on aggregated data processing through cloud or hospital-based infrastructures, where multiple data sources are integrated for clinical analysis and decision-making. Understanding the differences between these architectures is essential for evaluating the role of LPWSNs in enabling scalable, energy-efficient, and real-time healthcare solutions [122,124]. Figure 7A,B illustrate these two approaches.

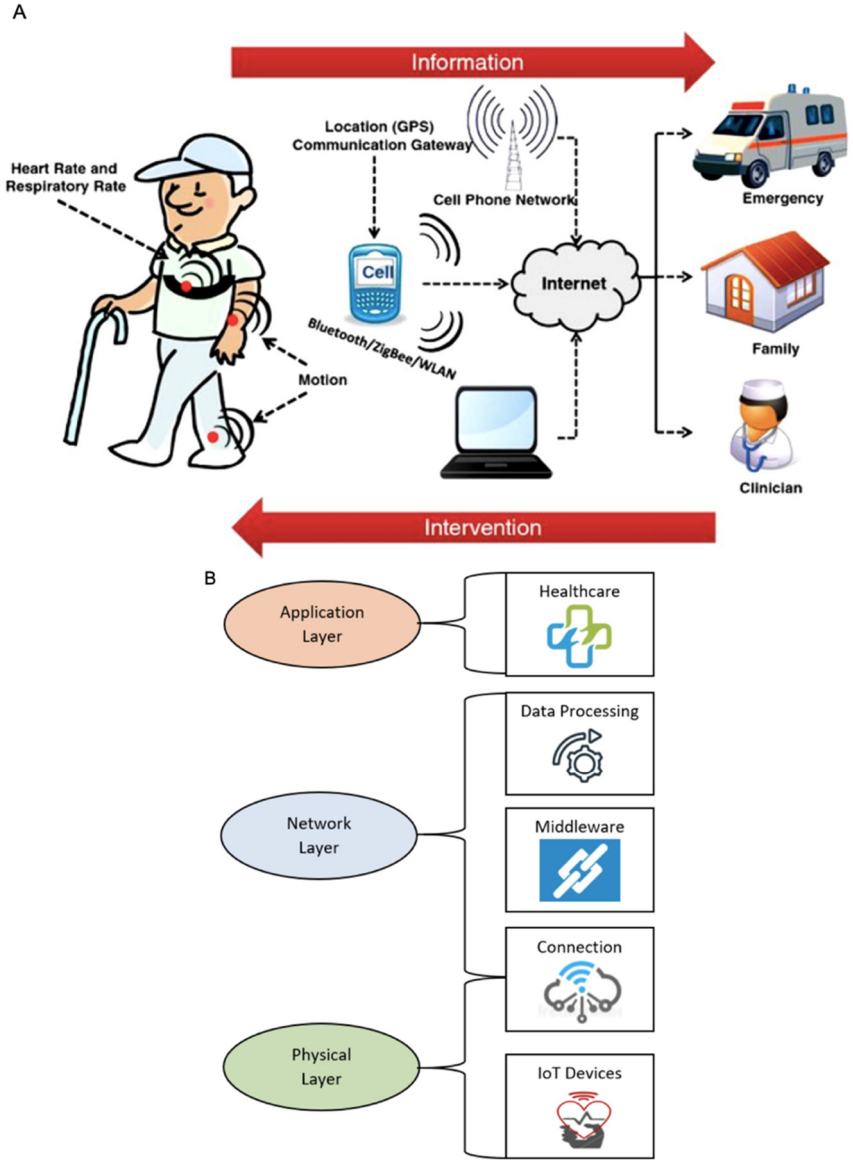


Figure 7. Comparison of healthcare monitoring architectures, highlighting decentralised wearable-based systems and centralised healthcare infrastructures. (**A**) Wearable health monitoring system illustrating real-time data collection and transmission from body sensors to remote healthcare providers [122]. (**B**) Centralised IoT-based healthcare architecture showing layered data acquisition, communication, and cloud-based processing for clinical decision-making [124].

5.4.1. Time Synchronisation Protocols in Wearable and WBAN Healthcare Systems

In addition to application-level wearable IoT systems, real-time healthcare monitoring increasingly relies on specialised time synchronisation protocols designed for

WBANs, where strict constraints on energy consumption, latency, and mobility are critical. Protocols such as energy-efficient WBAN synchronisation schemes and fractional synchronisation approaches have been proposed to address challenges arising from body movement, heterogeneous sensor sampling rates, and intermittent connectivity. These methods aim to maintain temporal consistency across physiological signals such as ECG, IMU, and blood pressure measurements, which is essential for accurate multi-modal health data fusion. Compared to conventional WSN synchronisation protocols, WBAN-specific approaches prioritise ultra-low-power operation and robustness under frequent topology changes caused by human motion. However, trade-offs remain between synchronisation accuracy, computational overhead, and battery lifetime, particularly in continuous long-term monitoring scenarios. These developments further reinforce the role of LPWSN synchronisation research as a foundational enabler for next-generation healthcare systems [11,120,125].

5.4.2. Challenges and Future Directions for Healthcare Synchronisation

Healthcare monitoring applications impose some of the most stringent requirements on real-time data synchronisation in LPWSNs. Wearable and body area sensor networks often integrate multiple sensing modalities, including ECG, motion, temperature, blood pressure, and glucose monitoring devices, which must operate in a coordinated and time-aligned manner to ensure accurate clinical interpretation. However, maintaining synchronisation across heterogeneous sensors remains challenging due to differences in sampling rates, clock drift, communication delays, and intermittent connectivity caused by patient mobility. These issues can affect the quality of multi-sensor data fusion and reduce the reliability of health assessment and decision-support systems.

In addition to synchronisation accuracy, healthcare deployments must address energy constraints, data privacy, and cybersecurity requirements. Wearable devices are typically battery-powered and expected to operate continuously for extended periods, requiring energy-efficient synchronisation mechanisms that minimise communication overhead while preserving timing precision. Emerging research is increasingly exploring AI-assisted synchronisation, edge computing, and adaptive resource management to improve reliability and responsiveness in real-time healthcare environments. Future work should focus on developing lightweight, secure, and scalable synchronisation frameworks capable of supporting continuous patient monitoring while maintaining high levels of accuracy, privacy, and energy efficiency in both clinical and home-based healthcare settings [11,120,125].

6. Future Directions and Research Gaps

Current limitations in LPWSNs continue to constrain the achievement of reliable, scalable, and energy-efficient real-time synchronisation. As LPWSNs become increasingly integrated into industrial automation, smart manufacturing, healthcare monitoring, smart grids, and large-scale IoT infrastructures, synchronisation requirements are becoming more stringent and application-dependent. Although substantial progress has been made in synchronisation protocols, predictive modelling, edge computing, and secure communication frameworks, several unresolved challenges remain that limit large-scale real-world deployment.

Improving energy-efficient real-time synchronisation remains one of the most important research priorities for future LPWSNs. Since most LPWSNs rely on battery-powered sensor nodes operating under strict resource constraints, maintaining accurate synchronisation without excessive communication overhead remains difficult. Existing approaches, including duty cycling, adaptive synchronisation intervals, and lightweight synchronisation protocols, provide partial improvements. However, they often struggle

to maintain long-term accuracy in highly dynamic or dense network environments. Also, many current solutions achieve energy savings at the expense of synchronisation precision, latency, or network reliability, highlighting the need for more balanced and adaptive synchronisation strategies.

Future research should therefore investigate hybrid energy-aware synchronisation frameworks capable of dynamically adjusting synchronisation behaviour according to network conditions, node activity, and application requirements. Integrating renewable energy harvesting techniques, such as solar, kinetic, thermal, and radio-frequency energy harvesting, may help extend network lifetime while supporting continuous synchronisation operations in remote or difficult-to-access environments. In parallel, AI-driven predictive synchronisation models offer promising opportunities to minimise unnecessary communication by forecasting clock drift and synchronisation requirements in advance. Machine learning algorithms may also support intelligent load balancing and adaptive resource allocation, reducing uneven energy depletion across sensor nodes and improving network stability. However, further investigation is needed to develop lightweight and explainable AI models that can operate reliably within the computational and energy limitations of LPWSNs.

Security remains another major research challenge, particularly as LPWSNs are increasingly deployed in safety-critical applications such as healthcare systems, industrial control networks, and smart infrastructure. Distributed LPWSNs are vulnerable to multiple threats, including spoofing attacks, jamming, replay attacks, false timestamp injection, and unauthorised network access. In industrial SCADA environments, synchronisation failures caused by malicious attacks may disrupt coordinated control processes and compromise operational safety. Similarly, in healthcare monitoring systems, inaccurate or delayed synchronisation can directly affect patient monitoring accuracy and emergency response reliability. Ensuring secure real-time synchronisation therefore requires lightweight yet robust security mechanisms suitable for resource-constrained devices. Although blockchain-based synchronisation frameworks improve data integrity and traceability, their computational complexity, communication overhead, and latency remain significant barriers for practical LPWSN deployment. As a result, lightweight cryptographic approaches, including elliptic curve cryptography (ECC), lightweight authentication protocols, and homomorphic encryption, are attracting increasing research interest due to their lower computational requirements. At the same time, zero-trust security architectures are emerging as a promising direction for LPWSNs by enabling continuous device authentication, access verification, and communication monitoring rather than relying on static trust assumptions.

AI-driven intrusion detection systems may further improve network resilience by identifying anomalous behaviour and mitigating cyber threats in real time. However, the growing integration of AI into synchronisation frameworks also introduces new security concerns related to adversarial machine learning attacks, poisoned training datasets, and manipulated synchronisation predictions. Consequently, future research should focus not only on improving synchronisation accuracy but also on ensuring robustness, explainability, and adversarial resilience in intelligent LPWSN environments. In addition, emerging areas such as quantum-resistant cryptography and post-quantum lightweight security protocols warrant further investigation to ensure long-term protection against evolving cyber threats.

Scalability continues to represent another critical challenge as LPWSNs expand toward ultra-dense and geographically distributed deployments involving thousands of interconnected sensor nodes. Traditional synchronisation approaches often become less effective in large-scale deployments due to accumulated timing errors, increased communication latency, packet collisions, and network congestion. Hierarchical and cluster-

based synchronisation architectures can partially alleviate these issues by distributing synchronisation tasks more efficiently across the network. Nevertheless, maintaining consistent timing accuracy across heterogeneous and mobile LPWSN environments remains difficult, particularly when network topology changes dynamically or communication quality fluctuates.

AI-driven adaptive frequency allocation, interference management, and traffic prediction techniques may help improve synchronisation stability in dense deployments. In addition, SDN offers promising capabilities for centralised and programmable synchronisation management by enabling dynamic control of routing, timing updates, and network resources according to real-time operating conditions. Despite these advantages, SDN-based LPWSNs still face important challenges related to controller scalability, fault tolerance, interoperability, and security. Furthermore, integrating SDN frameworks into legacy industrial systems may require significant architectural modifications and standardisation efforts. The integration of LPWSNs with next-generation communication technologies also represents an important research direction. The convergence of LPWSNs with 5G-enabled LPWAN technologies can support ultra-low-latency communication, improved reliability, and enhanced synchronisation precision while maintaining energy efficiency. Looking further ahead, 6G networks are expected to provide even greater synchronisation accuracy, intelligent resource orchestration, and native AI support for mission-critical applications. However, practical deployment of 5G- and 6G-enabled LPWSNs will require overcoming several challenges related to infrastructure cost, interoperability, spectrum management, backward compatibility, and real-time coordination across heterogeneous communication platforms.

Edge and fog computing paradigms are also expected to play an increasingly important role in future LPWSN architectures by processing time-sensitive data closer to the network edge, thereby reducing latency and minimising cloud communication overhead. Although edge-assisted synchronisation can improve responsiveness and scalability, efficient coordination between edge, fog, and cloud layers remains an open research problem, particularly in highly distributed industrial and healthcare systems. Seamless integration with broader IoT ecosystems, digital twins, and smart city infrastructures will therefore be essential to ensure the long-term adaptability and interoperability of LPWSNs.

This review has identified several key research gaps, including energy-efficient synchronisation, secure and trustworthy data exchange, large-scale scalability, intelligent synchronisation management, and integration with emerging communication technologies. These challenges are particularly significant in healthcare applications, where reliable real-time synchronisation directly affects patient monitoring, clinical decision-making, and emergency response systems. Table 4 summarises representative studies in the literature, highlighting their primary contributions, technological focus areas, and remaining limitations. The comparative analysis further demonstrates that no existing synchronisation framework simultaneously satisfies the competing requirements of ultra-low latency, high scalability, energy efficiency, security, adaptability, and deployment simplicity. Future research should therefore prioritise the development of intelligent, adaptive, secure, and interoperable synchronisation frameworks capable of operating efficiently across diverse and large-scale LPWSN environments. Particular attention should be given to lightweight AI integration, zero-trust security models, edge-assisted synchronisation, quantum-resistant protection mechanisms, and standardised architectures that support real-world deployment in industrial, healthcare, and smart infrastructure systems.

Table 4. Comparison of representative studies on real-time synchronisation in LPWSNs.

Paper/Study	Application/Focus Area	Key Contributions	Limitations / Research Gaps	Ref
Wireless Fieldbus Networking with Precision Time Synchronisation	Industrial WSNs/WSANs	Low-power fieldbus architecture with high-precision synchronisation for industrial control	Limited scalability and increased complexity in large or dynamic networks	[1]
Long-Range Low-Power Multi-Hop WSN for Monitoring Vibration Response	Multi-hop LPWSNs; structural health monitoring	Long-range synchronised data acquisition for vibration monitoring	Increased energy use and latency in multi-hop networks, limiting scalability	[2]
Integration of SCADA and Industrial IoT	SCADA-LPWSN integration; Industrial IoT	Improved data acquisition and system-level synchronisation for industrial monitoring	Limited real-time adaptability and insufficient focus on energy-efficient synchronisation	[14]
Secure and Energy-Efficient Data Transmission Model for WSN	Security and energy-efficient LPWSNs	Encryption-based framework for secure, energy-efficient data transmission	Computational overhead may limit real-time synchronisation	[23]
An Efficient Wireless Sensor Network for Industrial Monitoring and Control	WSN-based industrial automation	Adaptive synchronisation with ML-enhanced optimisation for improved efficiency	Limited support for predictive, low-overhead synchronisation in large-scale real-time systems	[43,126]
Monitoring of Renewable Energy Systems by IoT-Aided SCADA	Smart grid; IoT-enabled SCADA	IoT-enabled SCADA framework for real-time monitoring and synchronisation of renewable energy systems	Limited cybersecurity resilience and secure synchronisation mechanisms	[39]
AI-based Wearable Sensors for Digital Health Monitoring	Healthcare monitoring; wearable IoT (LPWSNs)	AI-enabled wearable sensors for real-time, synchronised health monitoring	Challenges in privacy, energy efficiency, and reliable real-time synchronisation	[120]

7. Conclusions

Real-time data synchronisation is a fundamental requirement for modern supervisory systems, ensuring accurate and timely alignment of sensor data with decision-making processes. LPWSNs have emerged as a powerful solution for enabling real-time monitoring across a wide range of applications, including industrial automation, smart grids, environmental systems, and healthcare. However, these networks continue to face challenges related to energy constraints, network scalability, synchronisation accuracy, and cybersecurity.

This review has presented a comprehensive analysis of key synchronisation protocols in LPWSNs, highlighting their strengths and limitations in terms of accuracy, energy efficiency, and scalability. It has also examined recent advancements, including AI-driven synchronisation, blockchain-based security mechanisms, and SDN-based network management, which offer promising pathways toward more efficient and reliable synchronisation. This review also applies a structured evaluation perspective to compare synchronisation approaches across multiple performance dimensions, including accuracy, latency, energy efficiency, scalability, and security. This enables a more critical synthesis of existing solutions and supports clearer identification of trade-offs across different application domains. The analysis further reinforces the importance of balancing performance with resource constraints in the design of future LPWSN-based synchronisation systems. Despite these advancements, several challenges remain unresolved. Future LPWSNs must evolve toward more adaptive, energy-aware, and secure architectures capable of support-

ing large-scale and heterogeneous deployments. Continuous progress in artificial intelligence, next-generation wireless networks (5G/6G), edge computing, and advanced cryptographic techniques will play a crucial role in addressing these challenges.

Ultimately, the development of resilient, scalable, and intelligent synchronisation frameworks will be essential for unlocking the full potential of LPWSNs in next-generation supervisory control systems. As industries increasingly rely on data-driven decision-making, robust real-time synchronisation will remain a cornerstone for enabling efficient, autonomous, and sustainable networked systems**.** To provide a more critical perspective on the surveyed approaches, this review identifies several techniques as particularly promising for real-time synchronisation in LPWSNs. Protocols such as FTSP and TSCH demonstrate strong performance in terms of accuracy and robustness in multi-hop industrial environments, while PTP-based approaches offer superior precision where hardware support is available. In parallel, AI-driven synchronisation and edge-assisted optimisation frameworks appear most promising for next-generation systems due to their adaptability, scalability, and ability to handle dynamic network conditions. However, these approaches also introduce additional computational overhead, which must be carefully managed in resource-constrained deployments. In summary, hybrid solutions that combine lightweight synchronisation protocols with intelligent optimisation at the edge are considered the most viable direction for future industrial and healthcare applications.

Author Contributions: Conceptualization, R.J. and M.R.; Literature survey and writing—original draft preparation, M.R. and R.J.; Preparation of figures and tables, M.R. and R.J.; Critical review and editing, M.R. and W.B.; Supervision, M.R. and W.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work received no external funding.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: No new data were created or analysed in this study. Data sharing is not applicable to this article.

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

Abbreviations

The following abbreviations are used in this manuscript:

5G	Fifth Generation
6G	Sixth Generation
AI	Artificial Intelligence
ACO	Ant Colony Optimisation
ADCs	Analogue-to-Digital Converters
ALDC	Adaptive Lossless Data Compression
ARQ	Automatic Repeat reQuest
BLE	Bluetooth Low Energy
COBOTS	Collaborative Robots
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CS	Cuckoo Search
DAQ	Data Acquisition
DI/DO	Digital Input/Digital Output
DMZ	Demilitarised Zone
DNP3	Distributed Network Protocol 3
DoS	Denial of Service
DRL	Deep Reinforcement Learning
DSP	Digital Signal Processing
ECG	Electrocardiogram

ECC	Elliptic Curve Cryptography
ESS	Energy Storage Systems
FEC	Forward Error Correction
FoF	Factories of the Future
FELACS	Fast Efficient Lossless Adaptive Compression Scheme
Fieldbus	Industrial Communication Protocol for Real-Time Distributed Control
FPGA	Field Programmable Gate Array
FTSP	Flooding Time Synchronisation Protocol
GHz	Giga Hertz
GPS	Global Positioning Tracker
GUI	Graphical User Interface
HMI	Human–Machine Interface
IDS	Intrusion Detection Systems
IEC	International Electro-Technical Commission
IMUs	Inertial Measurement Units
IoT	Internet of Things
IP	Internet Protocol
LZW	Lempel–Ziv–Welch
LoRa	Long-Range Wireless Connection
LPWSN	Low-Power Wireless Sensor Networks
LEACH	Low-Energy Adaptive Clustering Hierarchy
MAC	Medium Access Control
MACs	Message Authentication Codes
MHz	Mega Hetrz
ML	Machine Learning
MTU	Master Terminal Units
NB-IoT	Narrowband Internet of Things
NTP	Network Time Protocol
OCXO	Oven Controlled Crystal Oscillator
ONOS	Open Network Operating System
OPC	Open Platform Communication
PLCs	Programmable Logic Controllers
PoA	Proof of Authority
PoS	Proof of Stake
POW	Proof of Work
PTP	Precision Time Protocol
QoS	Quality of Service
RF	Radio Frequency
RBS	Reference Broadcast Synchronisation
RPM	Remote Patient Monitoring
RTUs	Remote Terminal Units
RTT	Round-Trip Time
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Network
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TinySec	Tiny Security Architecture for Wireless Sensor Networks
TPSN	Timing-Sync Protocol for Sensor Network
TSCXO	Temperature-Compensated Crystal Oscillator
TSCH	Time-Slotted Channel Hopping
URLLC	Ultra-Reliable Low-Latency Communication
WBANs	Wireless Body Area Networks
WSN	Wireless Sensor Network
ZTA	Zero-Trust Architecture

References

1. Chen, C.-H.; Lin, M.-Y.; Tew, W.-P. Wireless Fieldbus Networking with Precision Time Synchronisation for a Low-Power WSAN. *Microprocess. Microsyst.* **2022**, *90*, 104509.

2. Tronci, E.M.; Nagabuko, S.; Hieda, H.; Feng, M.Q. Long-Range Low-Power Multi-Hop Wireless Multi Sensor Network for Monitoring the Vibration Response of Long-Span Bridges. *Sensors* **2022**, *22*, 3916.
3. Chi, C.; Liu, G.-P.; Hu, W. Design and Implementation of a Mobile Terminal Cloud Supervisory Control Platform for Networked Control Systems. *Trans. Inst. Meas. Control* **2021**, *44*, 1070–1080.
4. Teixeira, M.A.; Zolanvari, M.; Khan, K.M.; Jain, R.; Meskin, N. Flow-Based Intrusion Detection Algorithm for Supervisory Control and Data Acquisition Systems: A Real-Time Approach. *IET Cyber-Phys. Syst. Theory Appl.* **2021**, *6*, 178–191.
5. Wajgi, D.W.; Tembhurne, J.V. Localisation in Wireless Sensor Networks and Wireless Multimedia Sensor Networks Using Clustering Techniques. *Multimed. Tools Appl.* **2023**, *83*, 6829–6879.
6. Jabeen, T.; Jabeen, I.; Ashraf, H.; Jhanjhi, N.Z.; Yassine, A.; Hossain, M.S. An Intelligent Healthcare System Using IoT in Wireless Sensor Network. *Sensors* **2023**, *23*, 5055.
7. Khriji, S.; Chéour, R.; Kanoun, O. Dynamic Voltage and Frequency Scaling and Duty-Cycling for Ultra Low-Power Wireless Sensor Nodes. *Electronics* **2022**, *11*, 4071.
8. Yadav, G.; Paul, K. Architecture and security of SCADA systems: A review. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100433.
9. Dash, L.; Pattanayak, B.K.; Mishra, S.K.; Sahoo, K.S.; Jhanjhi, N.Z.; Baz, M.; Masud, M. A Data Aggregation Approach Exploiting Spatial and Temporal Correlation among Sensor Data in Wireless Sensor Networks. *Electronics* **2022**, *11*, 989.
10. Ortega-Gonzalez, L.; Acosta-Coll, M.; Pineres-Espitia, G.; Butt, S.A. Communication protocols evaluation for a wireless rainfall monitoring network in an urban area. *Heliyon* **2021**, *7* (6).
11. Regterschot, G.R.H.; Ribbers, G.M.; Bussmann, J.B. Wearable movement sensors for rehabilitation: From technology to clinical practice. *Sensors* **2021**, *21*, 4744.
12. Wei, S.; Wu, Z. The Application of Wearable Sensors and Machine Learning Algorithms in Rehabilitation Training: A Systematic Review. *Sensors* **2023**, *23*, 7667.
13. Larkin, R.D.; Lopez, J., Jr.; Butts, J.W.; Grimaila, M.R. Evaluation of Security Solutions in the SCADA Environment. *ACM SIGMIS Database* **2014**, *45*, 38–53.
14. Nechibvute, A.; Mafukidze, H.D. Integration of SCADA and Industrial IoT: Opportunities and Challenges. *IETE Tech. Rev.* **2024**, *41*, 312–325.
15. Babayigit, A.; Abubaker, M. Industrial Internet of Things: A Review of Improvements over Traditional SCADA Systems for Industrial Automation. *IEEE Syst. J.* **2023**, *18*, 120–133.
16. Sverko, M.; Grbac, T.G.; Mikuc, M. SCADA Systems with Focus on Continuous Manufacturing and Steel Industry: A Survey on Architectures, Standards, Challenges and Industry 5.0. *IEEE Access* **2022**, *10*, 109395–109430.
17. Enemosah, A.; Ifeanyi, O.G. SCADA in the Era of IoT: Automation, Cloud-Driven Security, and Machine Learning Applications. *Int. J. Sci. Res. Arch.* **2024**, *13*, 3417–3435.
18. Younis, J.A.; Raouf, M.; Abdallah, M.A. The Influence of SCADA Information Technology System Application on Improving Performance Efficiency (Field Study on the Ministry of Electricity and Oil of the Kurdistan Region of Iraq). *J. Posit. Psychol. Wellbeing* **2022**, *6*, 1040–1061.
19. Tükez, E.T.; Kaya, K.A. SCADA System for Next-Generation Smart Factory Environments. *ICONTECH Int. J.* **2022**, *6*, 48–52.
20. Basholli, F.; Mema, B.; Hyka, D.; Basholli, A.; Daberdini, A. Analysis of Security Challenges in SCADA Systems, a Technical Review on Automated Real-Time Systems. *Adv. Eng. Days* **2023**, *8*, 18–22.
21. Zagrouba, R.; Kardi, A. Comparative Study of Energy-Efficient Routing Techniques in Wireless Sensor Networks. *Information* **2021**, *12*, 42.
22. Uthayakumar, G.S.; Jackson, B.; Durai, C.R.B.; Kalaimani, A.; Sargunavathi, S.; Kamatchi, S. Systematically Efficiency Enabled Energy Usage Method for an IoT-Based WSN Environment. *Meas. Sens.* **2023**, *25*, 100615.
23. Singh, A.K.; Alshehri, M.; Bhushan, S.; Kumar, M.; Alfarraj, O.; Pardarshani, K.R. Secure and Energy-Efficient Data Transmission Model for WSN. *Intell. Autom. Soft Comput.* **2021**, *27*, 761–769.
24. Kim, J.; Lee, D.; Hwang, J.; Hong, S.; Shin, D.; Shin, D. Wireless Sensor Network (WSN) Configuration Method to Increase Node Energy Efficiency through Clustering and Location Information. *Symmetry* **2021**, *13*, 390.
25. Bhamare, D.; Zolanvari, M.; Erbad, A.; Jain, R.; Khan, K.; Meskin, N. Cybersecurity for industrial control systems: A survey. *Comput. Secur.* **2020**, *89*, 101677.
26. Radvanovsky, R.; Brodsky, J. *Handbook of SCADA/Control Systems Security*, 2nd ed.; CRC Press: Boca Raton, FL, USA, 2020. Available online: https://www.routledge.com/Handbook-of-SCADA-Control-Systems-Security/Radvanovsky-Brodsky/p/book/9780367596668 (accessed on 20 April 2026).

27. Daousis, S.; Peladarinos, N.; Cheimaras, V.; Papageorgas, P.; Piromalis, D.D.; Munteanu, R.A. Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures. *Future Internet* **2024**, *16*, 33.
28. Jain, K.; Kumar, A.; Singh, A. Data Transmission Reduction Techniques for Improving Network Lifetime in Wireless Sensor Networks: An Up-to-Date Survey from 2017 to 2022. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4674.
29. Lee, C.; Kim, N.; Hong, S. Toward industrial IoT: Integrated architecture of an OPC UA synergy platform. *IEEE Access* **2021**, *9*, 164720–164731.
30. Faris, M.; Mahmud, M.N.; Salleh, M.F.; Alnoor, A. Wireless Sensor Network Security: A Recent Review Based on State-of-the-Art Works. *Int. J. Eng. Bus. Manag.* **2023**, *15*, 18479790231157220.
31. Nuruzzaman, M.; Rana, S. IoT-Enabled Condition Monitoring in Power Distribution Systems: A Review of SCADA-Based Automation, Real-Time Data Analytics, and Cyber-Physical Security Challenges. *J. Sustain. Dev. Policy* **2025**, *1 (01)*, 25–43.
32. Gulati, K.; Boddu, R.S.; Kapila, D.; Bangare, S.L.; Chandnani, N.; Saravanan, G.J. A Review Paper on Wireless Sensor Network Techniques in Internet of Things (IoT). *Mater. Today Proc.* **2022**, *51*, 161–165.
33. Yilmaz, S.; Dener, M. Security with Wireless Sensor Networks in Smart Grids: A Review. *Symmetry* **2024**, *16*, 1295.
34. Goyal, S.; Sharma, N.; Bhushan, B.; Shankar, A.; Sagayam, M. IoT Enabled Technology in Secured Healthcare: Applications, Challenges and Future Directions. In *Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications*; Springer International Publishing: Cham, Switzerland, 2020; pp. 25–48.
35. Kumar, M.; Kumar, A.; Verma, S.; Bhattacharya, P.; Ghimire, D.; Kim, S.H.; Hosen, A.S. Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues. *Electronics* **2023**, *12*, 2050.
36. Merabtine, N.; Djenouri, D.; Zegour, D.E. Towards Energy-Efficient Clustering in Wireless Sensor Networks: A Comprehensive Review. *IEEE Access* **2021**, *9*, 92688–92705.
37. Chéour, R.; Jmal, M.W.; Khriji, S.; El Houssaini, D.; Trigona, C.; Abid, M.; Kanoun, O. Towards hybrid energy-efficient power management in wireless sensor networks. *Sensors* **2021**, *22*, 301.
38. Salama, R.; Al-Turjman, F.; Bordoloi, D.; Yadav, S.P. Wireless Sensor Networks and Green Networking for 6G Communication—An Overview. In *2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)*; IEEE: Ghaziabad, India, 2023; pp. 830–834.
39. Qays, M.O.; Ahmed, M.M.; Parvez Mahmud, M.A.; Abu-Siada, A.; Muyeen, S.M.; Hossain, M.L.; Yasmin, F.; Rahman, M.M. Monitoring of Renewable Energy Systems by IoT-Aided SCADA System. *Energy Sci. Eng.* **2022**, *10*, 1874–1885.
40. Bravo-Arrabal, J.; Zambrana, P.; Fernandez-Lozano, J.J.; Gomez-Ruis, J.A.; Barba, J.S.; Garcia-Cerezo, A. Realistic Deployment of Hybrid Wireless Sensor Networks Based on ZigBee and LoRa for Search and Rescue Applications. *IEEE Access* **2022**, *10*, 64618–64637.
41. Ghanimi, H.M.; Suguna, R.; Jeyaraj, J.P.; Sreekanth, K.; Rangasamy, R.; Sengan, S. Smart Fertilizing Using IoT Multi-Sensor and Variable Rate Sprayer Integrated UAV. *Scalable Comput. Pract. Exp.* **2024**, *25*, 3766–3777.
42. Kaur, M.; Khan, M.Z.; Gupta, S.; Alsaeedi, A. Adoption of blockchain with 5G networks for industrial IoT: Recent advances, challenges, and potential solutions. *IEEE Access* **2021**, *10*, 981–997.
43. De Beelde, B.; Plets, D.; Joseph, W. Wireless sensor networks for enabling smart production lines in Industry 4.0. *Appl. Sci.* **2021**, *11*, 11248.
44. Al Imran, M.A.; Dalveren, Y.; Tavli, B.; Kara, A. Optimal operation mode selection for energy-efficient light-weight multi-hop time synchronisation in linear wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020 (1)*, 109.
45. Prasetya, M.F.; Budi, A.S.; Akbar, S.R. Time Synchronisation on ESP-NOW Based Wireless Sensor Network Using Flooding Time Synchronisation Protocol. In *Proceedings of the 8th International Conference on Sustainable Information Engineering and Technology*; Association for Computing Machinery: New York, NY, USA, 2023; pp. 608–611.
46. Ganeriwal, S.; Kumar, R.; Srivastava, M.B. Timing-Sync Protocol for Sensor Networks. In *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems* **2003**; pp. 138–149.
47. Wang, H.; Yu, F.; Li, M.; Zhong, Y. Clock skew estimation for timestamp-free synchronisation in industrial wireless sensor networks. *IEEE Trans. Ind. Inform.* **2020**, *17*, 90–99.
48. Malhotra, S.; Jain, S. Survey of Time Synchronisation in Wireless Sensor Networks. *J. Act. Passiv. Electron. Devices* **2020**, *15*.
49. Zervopoulos, A.; Tsipis, A.; Alvanou, A.G.; Bezas, K.; Papamichail, A.; Vergis, S.; Stylidou, A.; Tsoumanis, G.; Komianos, V.; Koufoudakis, G.; et al. Wireless sensor network synchronisation for precision agriculture applications. *Agriculture* **2020**, *10*, 89.
50. Huan, X.; Kim, K.S. Per-hop delay compensation in time synchronisation for multi-hop wireless sensor networks based on packet-relaying gateways. *IEEE Commun. Lett.* **2020**, *24*, 2300–2304.

51. Balakrishnan, K.; Dhanalakshmi, R.; Gopalakrishnan, R. Clock Synchronisation in Industrial Internet of Things and Potential Works in Precision Time Protocol: Review, Challenges and Future Directions. *Int. J. Cogn. Comput. Eng.* **2023**, *4*, 205–219.
52. Yiğitler, H.; Badihi, B.; Jäntti, R. Overview of Time Synchronisation for IoT Deployments: Clock Discipline Algorithms and Protocols. *Sensors* **2020**, *20*, 5928.
53. Weng, Y.; Zhang, Y. A Survey of Secure Time Synchronisation. *Appl. Sci.* **2023**, *13*, 3923.
54. Geetha, S.; Latha, P.; Suganya, R.; Nidhya, MS. Clock Synchronisation Protocols and Models for Wireless Sensor Networks. In *Proceedings of the 2024 IEEE 16th International Conference on Computational Intelligence and Communication Networks (CICN)*; IEEE: Piscataway, NJ, USA, 2024; pp. 36–39.
55. *IEEE Std 802.15.4-2020*; IEEE Standard for Low-Rate Wireless Networks (LR-WPAN). Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2020. Available online: https://standards.ieee.org/standard/802_15_4-2020.html (accessed on 25 April 2026).
56. Vera-Pérez, J.; Silvestre-Blanes, J.; Sempere-Payá, V. TSCH and RPL joining time model for industrial wireless sensor networks. *Sensors* **2021**, *21*, 3904.
57. Seijo, O.; Val, I.; Luvisotto, M.; Pang, Z. Clock synchronisation for wireless time-sensitive networking: A march from microsecond to nanosecond. *IEEE Ind. Electron. Mag.* **2021**, *16*, 35–43.
58. Coviello, G.; Avitabile, G.; Florio, A. A synchronized multi-unit wireless platform for long-term activity monitoring. *Electronics* **2020**, *9*, 1118.
59. Cappelle, J.; Goossens, S.; De Strycker, L.; Van der Perre, L. Low-power synchronization for multi-IMU WSNs. *IEEE Embed. Syst. Lett.* **2023**, *16*, 210–213.
60. Santos, G.; Wanderley, M.; Tavares, T.; Rocha, A. A multi-sensor human gait dataset captured through an optical system and inertial measurement units. *Sci. Data* **2022**, *9*, 545.
61. Shi, F.; Yang, S.X.; Tuo, X.; Ran, L.; Huang, Y. A novel rapid-flooding approach with real-time delay compensation for wireless-sensor network time synchronisation. *IEEE Trans. Cybern.* **2020**, *52*, 1415–1428.
62. Zhang, M.; Zhang, H.; Fang, Y.; Yuan, D. Learning-Based Data Transmissions for Future 6G Enabled Industrial IoT: A Data Compression Perspective. *IEEE Netw.* **2022**, *36*, 180–187.
63. Alshanbari, H.S. Medical image watermarking for ownership & tamper detection. *Multimed. Tools Appl.* **2021**, *80*, 16549–16564.
64. Mishra, M.; Sen Gupta, G.; Gui, X. Investigation of Energy Cost of Data Compression Algorithms in WSN for IoT Applications. *Sensors* **2022**, *22*, 7685.
65. Jayasankar, U.; Thirumal, V.; Ponnurangam, D. A Survey on Data Compression Techniques: From the Perspective of Data Quality, Coding Schemes, Data Type and Applications. *J. King Saud Univ.-Comput. Inf. Sci.* **2021**, *33*, 119–140.
66. Ketshabetswe, K.L.; Zungeru, A.M.; Mtengi, B.; Lebekwe, C.K.; Prabaharan, S.R.S. Data compression algorithms for wireless sensor networks: A review and comparison. *IEEE Access* **2021**, *9*, 136872–136891.
67. Al-Kadhim, H.M.; Al-Raweshidy, H.S. Energy efficient data compression in cloud based IoT. *IEEE Sens. J.* **2021**, *21*, 12212–12219.
68. Ghaderi, M.R.; Tabataba Vakili, V.; Sheikhan, M. Compressive sensing-based energy consumption model for data gathering techniques in wireless sensor networks. *Telecommun. Syst.* **2021**, *77*, 83–108.
69. Gandhimathi, L.; Murugaboopathi, G. Mobile malicious node detection using mobile agent in cluster-based wireless sensor networks. *Wirel. Pers. Commun.* **2021**, *117*, 1209–1222.
70. Khan, A.; Marriwala, N. A literature survey on leach protocol and its descendants for homogeneous and heterogeneous wireless sensor networks. In *Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences: PCCDS 2020*; Springer: Singapore, 2021; pp. 631–643.
71. Maurya, S.; S, K.; K, P.; Karthik, P.C.; Saranya, V.G. Hybrid Compression-Based Routing Strategies for Enhanced Energy Efficiency in Wireless Sensor Networks. *J. Cloud Comput.* **2025**, *14 (1)*, 71.
72. Fazeli, M.; Raji, M.; Fazeli, M.M. DTranIDS: A Two-Tiered Intrusion Detection System for RPL-based IoT Networks based on Decision Tree and Transformer Models. In *2025 15th International Conference on Computer and Knowledge Engineering (ICCKE)*; IEEE: Mashhad, Iran, 2025; pp. 1–7.
73. Chinamanagonda, S. Edge Computing: Extending the Cloud to the Edge-Growth in IoT and Real-Time Data Processing Needs. *Int. J. Sci. Res.* **2020**, *9*, 1941–1949.
74. Stanford, C.; Tanner, A. K-Means Clustering for Large Data: Anomaly Detection in Supervisory Control and Data Acquisition Systems. In *Proceedings of the 2023 Congress in Computer Science, Computer Engineering, and Applied Computing (CSCE)*; IEEE: Las Vegas, NV, USA, 2023; pp. 1624–1627.

75. Abdali, T.A.N.; Hassan, R.; Aman, A.H.M.; Nguyen, Q.N. Fog computing advancement: Concept, architecture, applications, advantages, and open issues. *IEEE Access* **2021**, *9*, 75961–75980.
76. Shmelova, T.; Smolanka, V.; Sikirda, Y.; Sechko, O. Real-time monitoring and diagnostics of the person's emotional state and decision-making in extreme situations for healthcare. *Decis. Mak. Anal.* **2024**, *2 (1)*, 11–32.
77. Cicioğlu, M.; Calhan, A. Internet of Things-based firefighters for disaster case management. *IEEE Sens. J.* **2020**, *21*, 612–619.
78. Bishoyi, P.K.; Misra, S.; Kumar, N. Collaborative and efficient body-to-body networks for IoT-based healthcare systems. *IEEE Internet Things J.* **2021**, *9*, 12147–12154.
79. Huang, X.; Cao, X.; Ma, Y. Sampled-Data Exponential Synchronisation of Complex Dynamical Networks with Time-Varying Delays and T–S Fuzzy Nodes. *Comput. Appl. Math.* **2022**, *41*, 2.
80. Lumbantoruan, H.; Adachi, K. Array antenna equipped UAV-BS for efficient low power WSN and its theoretical analysis. *IET Commun.* **2021**, *15*, 2054–2067.
81. Ouadou, M.; Mafamane, R.; Minaoui, K. A Hybrid Anti-Collision Protocol Based on Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA) for Radio Frequency Identification (RFID) Readers. *Network* **2024**, *4*, 217–236.
82. Yang, D.-H.; Kim, D.; Chang, J.-H. Masked Frequency Modeling for Improving Packet Loss Concealment in Speech Transmission Systems. In *Proceedings of the 2023 IEEE Workshop on Applications of Signal Processing to Audio and Acoustics (WASPAA)*; IEEE: Piscataway, NJ, USA, 2023; pp. 1–5.
83. Jiang, L.; Tan, R.; Easwaran, A. Resilience bounds of network clock synchronisation with fault correction. *ACM Trans. Sens. Netw. (TOSN)* **2020**, *16*, 1–30.
84. Emara, S.; Fong, S.L.; Li, B.; Khisti, A.; Tan, W.T.; Zhu, X.; Apostolopoulos, J. Low-Latency Network-Adaptive Error Control for Interactive Streaming. *IEEE Trans. Multimed.* **2021**, *24*, 1691–1706.
85. Irshad, A.; Aljaedi, A.; Bassfar, Z.; Jamal, S.S.; Daud, A.; Chaudhry, S.A.; Das, A.K. SAWPS: Secure Access Control for Wearable Plant Sensors-Reinforcing Agriculture 4.0. *IEEE Sens. J.* **2024**, *24*, 29293–29304.
86. Park, J.; Mohaisen, M.; Nyang, D.; Mohaisen, A. Assessing the Effectiveness of Pulsing Denial of Service Attacks under Realistic Network Synchronisation Assumptions. *Comput. Netw.* **2020**, *173*, 107146.
87. Elsadig, M.A. Detection of denial-of-service attack in wireless sensor networks: A lightweight machine learning approach. *IEEE Access* **2023**, *11*, 83537–83552.
88. Kim, Y.W.; Kim, W. Clustering-Based Adaptive Query Generation for Semantic Segmentation. *IEEE Signal Process. Lett.* **2025**, *32*, 1580–1584.
89. Zhao, Z. Design and Implementation of Artificial Intelligence-Driven Network Intrusion Detection System. In *Proceedings of the 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)*; IEEE: Bidar, India, 2025; pp. 1–5.
90. Vosughi, A.; Tamimi, A.; King, A.B.; Majumder, S.; Srivastava, A.K. Cyber–Physical Vulnerability and Resiliency Analysis for DER Integration: A Review, Challenges and Research Needs. *Renew. Sustain. Energy Rev.* **2022**, *168*, 112794.
91. Zhao, W.; Cheng, Y.; Liu, Z.; Wu, X.; Kato, N. Asynchronous DRL-Based Multi-Hop Task Offloading in RSU-Assisted IoV Networks. *IEEE Trans. Cogn. Commun. Netw.* **2025**, *11*, 546–555.
92. Asharf, J.; Moustafa, N.; Khurshid, H.; Debie, E.; Haider, W.; Wahab, A. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. *Electronics* **2020**, *9*, 1177.
93. Dong, S.; Abbas, K.; Li, M.; Kamruzzaman, J. Blockchain Technology and Application: An Overview. *PeerJ Comput. Sci.* **2023**, *9*, e1705.
94. Anthony, B. Deployment of Distributed Ledger and Decentralised Technology for Transition to Smart Industries. *Environ. Syst. Decis.* **2023**, *43*, 298–319.
95. Alrubei, S.M.; Ball, E.; Rigelsford, J.M. The Use of Blockchain to Support Distributed AI Implementation in IoT Systems. *IEEE Internet Things J.* **2021**, *9*, 14790–14802.
96. Haque, E.U.; Shah, A.; Iqbal, J.; Ullah, S.S.; Alroobaea, R.; Hussain, S.A. Scalable Blockchain Based Framework for Efficient IoT Data Management Using Lightweight Consensus. *Sci. Rep.* **2024**, *14 (1)*, 7841.
97. Panwar, S.V.; Boukabous, H. A review on routing protocols in mobile IoT networks based on SDN. In *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*; IEEE: Salem, India, 2024; pp. 1561–1566.
98. Akter, S.; Sanam, T.F. A blockchain framework for secure healthcare data management using role-based access control and smart contracts. In *2025 International Conference on Electrical, Computer and Communication Engineering (ECCE)*; IEEE: Chittagong, Bangladesh 2025; pp. 1–6.

99. Veisi, F.; Montavont, J.; Théoleyre, F. Enabling Centralised Scheduling Using Software Defined Networking in Industrial Wireless Sensor Networks. *IEEE Internet Things J.* **2023**, *10*, 20675–20685.
100. Hussein, N.H.; Koh, J.S.; Yaw, C.T.; Tiong, S.K.; Benedict, F.; Yusaf, T.; Kadirgama, K.; Hong, T.C. SDN-based VANET routing: A comprehensive survey on architectures, protocols, analysis, and future challenges. *IEEE Access.* **2024**, *13*, 126801–126861.
101. Jurado-Lasso, F.F.; Marchegiani, L.; Jurado, J.F.; Abu-Mahfouz, A.M.; Fafoutis, X. A Survey on Machine Learning Software-Defined Wireless Sensor Networks (ML-SDWSNs): Current Status and Major Challenges. *IEEE Access* **2022**, *10*, 23560–23592.
102. Hussain, M.; Shah, N.; Amin, R.; Alshamrani, S.S.; Alotaibi, A.; Raza, S.M. Software-defined networking: Categories, analysis, and future directions. *Sensors* **2022**, *22*, 5551.
103. Chen, Y.; Sambo, Y.A.; Onireti, O.; Imran, M.A. A Survey on LPWAN-5G Integration: Main Challenges and Potential Solutions. *IEEE Access* **2022**, *10*, 32132–32149.
104. Zoghlami, C.; Kacimi, R.; Dhaou, R. 5G-Enabled V2X Communications for Vulnerable Road Users Safety Applications: A Review. *Wirel. Netw.* **2023**, *29*, 1237–1267.
105. Kumar, V.; Yadav, P.; Soares Indrusiak, L. Resilient Edge: Building an Adaptive and Resilient Multi-Communication Network for IoT Edge Using LPWAN and WiFi. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 3055–3071.
106. Sanjalawe, Y.; Fraihat, S.; Al-E'mari, S.; Makhadmeh, S.N. Bridging the Gap: A Comprehensive Survey on AI-Driven Digital Twin Networks for Future Wireless Systems. *J. King Saud Univ. Comput. Inf. Sci.* **2026**, *38*, 113.
107. Ismail, S.; Dawoud, D.W.; Reza, H. Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review. *Future Internet* **2023**, *15*, 200.
108. Hudda, S.; Haribabu, K. A Review on WSN Based Resource Constrained Smart IoT Systems. *Discov. Internet Things* **2025**, *5*, 56.
109. Jamwal, A.; Agrawal, R.; Manupati, V.K.; Sharma, M.; Varela, L.; Machado, J. Development of cyber physical system based manufacturing system design for process optimization. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *997*, 012048.
110. Liu, Y.; Yu, W.; Dillon, T.; Rahayu, W.; Li, M. Empowering IoT predictive maintenance solutions with AI: A distributed system for manufacturing plant-wide monitoring. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1345–1354.
111. Adebiyi, A.A.; Zulu, M.L.; Mazibuko, T.F. Smart Grid Model for Efficient Sustainable Energy Management. *Discov. Sustain.* **2026**, *7 (1)*, 219.
112. Moreno Escobar, J.J.; Morales Matamoros, O.; Tejeida Padilla, R.; Lina Reyes, I.; Quintana Espinosa, H. A comprehensive review on smart grids: Challenges and opportunities. *Sensors* **2021**, *21*, 6978.
113. Jha, A.V.; Appasani, B.; Ghazali, A.N.; Pattanayak, P.; Gurjar, D.S.; Kabalci, E.; Mohanta, D.K. Smart grid cyber-physical systems: Communication technologies, standards and challenges. *Wirel. Netw.* **2021**, *27*, 2595–2613.
114. Velasquez, W.; Moreira-Moreira, G.Z.; Alvarez-Alvarado, M.S. Smart Grids Empowered by Software-Defined Network: A Comprehensive Review of Advancements and Challenges. *IEEE Access* **2024**, *12*, 63400–63416.
115. Okafor, N.U.; Alghorani, Y.; Delaney, D.T. Improving data quality of low-cost IoT sensors in environmental monitoring networks using data fusion and machine learning approach. *ICT Express* **2020**, *6*, 220–228.
116. Ali, A.; Hussain, T.; Zahid, A. Smart irrigation technologies and prospects for enhancing water use efficiency for sustainable agriculture. *AgriEngineering* **2025**, *7*, 106.
117. Quy, V.K.; Hau, N.V.; Anh, D.V.; Quy, N.M.; Ban, N.T.; Lanza, S.; Randazzo, G.; Muzirafuti, A. IoT-enabled smart agriculture: Architecture, applications, and challenges. *Appl. Sci.* **2022**, *12*, 3396.
118. Symeonaki, E.; Arvanitis, K.; Piromalis, D. A Context-Aware Middleware Cloud Approach for Integrating Precision Farming Facilities into the IoT toward Agriculture 4.0. *Appl. Sci.* **2020**, *10*, 813.
119. Ferrández-Pastor, F.J.; García-Chamizo, J.M.; Nieto-Hidalgo, M.; Mora-Martínez, J. Precision Agriculture Design Method Using a Distributed Computing Architecture on Internet of Things Context. *Sensors* **2018**, *18*, 1731. https://doi.org/10.3390/s18061731.
120. Shajari, S.; Kuruvinashetti, K.; Komeili, A.; Sundararaj, U. The Emergence of AI-Based Wearable Sensors for Digital Health Technology: A Review. *Sensors* **2023**, *23*, 9498.
121. Deng, Z.; Guo, L.; Chen, X.; Wu, W. Smart wearable systems for health monitoring. *Sensors* **2023**, *23*, 2479.
122. Smith, A.A.; Li, R.; Tse, Z.T. Reshaping Healthcare with Wearable Biosensors. *Sci. Rep.* **2023**, *13*, 4998.
123. Coviello, G.; Avitabile, G.; Florio, A.; Talarico, C.; Wang-Roveda, J.M. A novel low-power time synchronization algorithm based on a fractional approach for wireless body area networks. *IEEE Access* **2021**, *9*, 134916–134928.
124. Aivaliotis, V.; Tsantikidou, K.; Sklavos, N. IoT-Based Multi-Sensor Healthcare Architectures and a Lightweight-Based Privacy Scheme. *Sensors* **2022**, *22*, 4269.
125. Zheng, Y.; Tang, N.; Omar, R.; Hu, Z.; Duong, T.; Wang, J.; Wu, W.; Haick, H. Smart materials enabled with artificial intelligence for healthcare wearables. *Adv. Funct. Mater.* **2021**, *31*, 2105482.

126. Phan, L.A.; Kim, T. Enabling rapid time synchronisation with slow-flooding in wireless sensor networks. *IEEE Commun. Lett.* **2022**, *26*, 947–951.