Wireless Sensor Network Technologies in Smart Homes: A Review of Key Technologies, Applications and Challenges

Zhihan Zhao

Southwest Petroleum University, Chengdu
3217549081@qq.com

Abstract Wireless Sensor Networks (WSNs) are used in smart home systems to provide the basic infrastructure for environmental monitoring, data collection and transmission in a smart home environment, and their performance directly affects the reliability, energy consumption, security and cross-device coordination of the entire system. Given the focus on smart home applications, this paper will systematically review the core WSN technologies in communication and networking, positioning, time synchronization, data fusion and interoperability, and analyze typical applications in existing research such as environmental control, elderly care, home security and energy management. Based on this analysis, it can be seen that current research has gradually shifted from whole-system architecture verification to low-power routing, security mechanisms and scenario-specific applications. Nevertheless, most existing achievements are still limited to simulations or laboratory prototypes. The problem of extending the lifespan of a real-life residential environment for resource-constrained nodes is still a trade-off among low-power consumption, reliability, cross-brand interoperability and security protection. Generally speaking, this research shifts from feasibility verification to low-power consumption, security improvement and scenario-based applications. However, real house long-term verifications still remain inadequate.

Keywords Wireless Sensor Networks; Smart Home; Low Power Consumption; Interoperability; Network Security

1. Introduction

The reason why Wireless Sensor Networks(WSNs) in smart home are worth studying singly is that there are various complex home-based scenario,which have many limitations including too many nodes,energy limitations,wall blockage,notable interference,heterogeneous devices as well as privacy sensitivity.Each of the limitations need corresponding solutions.With the development of the Internet of Things (IoT), edge computing and smart terminals have been introduced to increase the number of sensing nodes in residential areas steadily. Many micro-nodes work together to conduct environmental sensing, lightweight data processing and wireless transmission in WSNs to provide a basic infrastructure for connecting the physical environment with upper-layer decision-making systems in smart homes [1-3].

At the same time, the home environment has also created demand for such networks, such as low power consumption, stable communication, privacy protection and cross-brand interoperability. As a result, the application problems of a single protocol or algorithm cannot be fully understood by studying them in isolation. Based on the method of narrative review, this paper will systematically organise related research in the three areas of key technologies, typical applications and major problems, and focus on analyzing the gap between technical performance and real residential environments.

2. Key Technologies of Wireless Sensor Networks

2.1 Communication and Networking

Communication and Networking determine how nodes use channels to transmit data and build network connections. Home WSNs generally use a low-power MAC mechanism and routing protocols and multi-hop self-organisation schemes to reduce collisions, idle listening and redundant transmissions. At the MAC layer, it must balance channel utilization with node sleep scheduling. At the same time, other ways to reduce power consumption in MAC layer

are adaptive duty cycle, carrier sense and backoff. At the Routing Layer,it will choose a relatively stable route from the available options in the network.

When it comes to the currant situation of the Communication and Networking in smart home,with the addition of mobile nodes such as robot vacuums and wearable devices, the fixed-topology assumption is no longer valid, and adaptive MAC and mobile ad-hoc networking mechanisms have gradually gained attention [15]. Meanwhile,at the physical and link layers, security authentication, key generation and encrypted transmission are also closely related to the computing power and energy consumption constraints of nodes [13-14]. Therefore, optimisation of communication for smart homes should not only consider throughput but also address energy consumption, mobility and security overhead.

2.2 Localisation, Time Synchronization and Data Fusion

Localisation techniques aim at addressing the acquisition of position information.The two types of localisation techniques are range-based and range-free. Time of Arrival (TOA), Time Difference of Arrival (TDOA), Angle of Arrival (AOA) and Received Signal Strength Indicator (RSSI) have different accuracy levels, hardware costs, energy consumption and multipath resistance; TOA requires high-precision time measurement; AOA generally needs antenna array hardware; RSSI has a relatively low cost but is easily affected by obstructions and environmental changes. Range-free methods, such as Centroid, APIT, and DV-Hop, have even lower costs but generally have coarser localisation granularity [7].

Time synchronization aims at keeping the collected data from the distributed nodes in sync. Reference Broadcast Synchronization (RBS), Timing-sync Protocol for Sensor Networks (TPSN) and Flooding Time Synchronization Protocol (FTSP) are mechanisms that provide a unified time reference for event detection and multi-sensor cooperation [11].

Data fusion aims at solving how to fuse multi-source information.it reduces the number of data sources, and then, by weighted averaging of Kalman filtering, evidence reasoning and learning-based methods, minimizes redundant transmission. For the residential scenario, a simple fusion task can be carried out at the end node or gateway, and a complex model can be deployed on an edge server or in the cloud; however, a trade-off among real-time performance, computing power and communication delay needs to be made.

Overall, a basic trade-off in smart home exists among accuracy, energy and latency. Higher positioning accuracy usually cost greater energy consumption. Communication latency is also closely related to energy consumption, as frequent data exchange and high-precision sampling may increase communication load, contention and latency. In real-life smart home applications such as detection of human presence, anomaly localisation and device linkage in a smart home system do not always require the highest level of accuracy; therefore, schemes that consider cost, power consumption and deployment difficulty should be chosen.

2.3 Protocol Interoperability and Communication Methods

Communication technologies in home networks cannot be divided solely by transmission distance. ZigBee, Wi-Fi, 6LoWPAN and Matter are at different levels of the protocol stack and have different functions. For large-scale low-power sensing nodes, the requirements are low-power access and stable networking; for gateways and upper-layer control systems, IP interconnection, application-layer device models and cross-brand control are needed. Therefore, engineering design generally needs to cooperate with multiple-layer protocols and cannot meet all the requirements through a single wireless technology.

With the proliferation of various smart home devices from different companies, ensuring the interoperability of WSNs in practice has become a problem. A clear distinction must be drawn between these technologies in terms of their protocol stack layers. IEEE 802.15.4 constitutes the physical and medium access control (PHY/MAC) layer foundation for low-power wireless networks such as ZigBee and 6LoWPAN. Matter operates at the application layer to offers cross-brand device cooperation through a unified standard, which enables to run top of transport carriers such as Thread and Wi-Fi [12]. Short-distance, low-power technologies are suitable for indoor multi-node networks; however, LoRa is a low-power wide-area technology better suited to large-scale, low-rate applications. However, they are not the main choices for general residential buildings. According to the required coverage area, bandwidth, power consumption, device compatibility and maintenance cost, select a suitable protocol.

2.4 technical link summary

Generally speaking, Communication/networking, localisation/time synchronization/data fusion and interoperability are mapped to transmission, positioning and collaboration, and cross-device interconnection, respectively; these are a progressive relationship of functions in a smart home. Communication and Networking provide the basic connectivity and transmission support for the smart home system. In a real-life home environment, it supports wireless data transmission between the home gateway and sensor nodes distributed in various rooms, such as the living room, kitchen, bedroom and entrance. Localisation/time synchronization/data fusion offer multi-node sensing collaboration in a smart home system based on the basic transmission. Elderly fall detection, intrusion detection and all-encompassing home environment monitoring require sensing collaboration. The role of Interoperability

ISSN 3106-7018 (Print) ISSN 3106-5791 (Online)

in smart homes is system-level integration and intercommunication to address interoperation barriers among sensor nodes, smart appliances and security devices from different vendors and with heterogeneous communication protocols.

3. Typical Applications of WSNs in Smart Homes

3.1 Environmental Monitoring and Device Control

Early studies mainly verified the feasibility of wireless sensor networks (WSNs) for whole-house environmental monitoring and device control. Jiang Chengyan and others proposed an architecture of self-organisation, multi-hop relaying and a sink node. Modular sensor nodes are used in this way to collect data on temperature, humidity, gas concentration and intrusion events. Ji Qing and others used low-power ZigBee end devices to achieve environmental monitoring, security alarms and home appliance control [20, 21].

These studies have confirmed that the basic feasibility of WSNs in domestic sensing and control has been achieved, and low cost, low power consumption and scalability have been the focus of early research. However, most of its validation has been limited to theoretical design or laboratory prototype. Differences in the environment of the rooms, such as wall attenuation, cooking fumes and high humidity, have not been addressed. Therefore, the long-term stability of WSN deployment in real residential scenarios cannot be guaranteed.Furthermore,what environmental monitoring lays strong emphasis on is low power consumption and operational stability.

3.2 Elderly Care and Home Security

Ransing et al. designed an in-home monitoring system based on ZigBee, GSM and LabVIEW for older adults living alone. Gas, temperature and contact sensors were deployed in the kitchen and entrance areas, respectively, to trigger local and remote alarms in response to gas leakage, fire hazards and abnormal door status [23]. This scheme proposes the idea of differentiated sensor node deployment according to home functional zones.It also proposes a prototype architecture for the smart home monitoring system,but there’s no field validation conducted in actual residential spaces. Pirbhulal et al. have proposed a secure Internet of Things (IoT) scheme and key management mechanism for wireless sensor networks (WSNs) in smart homes in terms of network security [17]. These studies show that WSNs can be used for elderly care and home security. Further experiments are needed to determine the increase in the false alarm rate, network recovery after a disruption, link stability and privacy protection in a real residential environment. Furthermore, elderly care focuses more on real-time performance and false alarms, while security pays more attention to reliability and safety.

3.3 Energy Management / Energy-Efficient Operation

Most of the home sensor nodes are battery-powered; thus, their energy consumption directly affects maintenance costs and network lifespan. To elaborate on the above, we can distinguish between energy saving for WSN nodes and smart home energy management. For WSNs node, it improves mainly two aspects including software-algorithm level and hardware level to save energy, whereas for smart home energy-management, based on the data collected by wireless sensor networks, household appliances can be controlled by smart home system to reduce overall electricity consumption of the whole house. Pau and Salerno proposed a fuzzy logic adjustment scheme for MAC duty cycling based on the node load and remaining battery energy to dynamically adjust the sleep duration [18]. Yeh and others employed multi-objective routing to find a trade-off between energy consumption and transmission reliability [19]. Such studies show that energy saving should not only aim for a low-power state. Due to the overly long sleep, it may have reduced real-time performance. Data compression and fusion may lead to some loss of the original data, and complex routing adds to the computation. Energy management of a smart home system can be formulated as a multi-objective optimisation problem in many practical settings, and therefore, node life, data reliability, latency and maintenance convenience all need to be optimized simultaneously.

The application studies above show that the research development of WSNs in smart homes generally follows the path of "overall architecture proposal - laboratory prototype validation - optimisation of specific issues". The first studies focused on verifying the functions of the system aiming at solving how to performance in the smart home environment, and later research with the aim of solving how to feature lower power consumption, higher security and better reliability has also explored energy consumption, security and other applications. The next step aims to verify its long-term stable operation in real home.However, there are many differences in the studies in terms of hardware platforms, data scale and test environments; thus, direct comparison of the studies is not feasible. Therefore, in the future, review papers and experiments should provide more specific information, such as network scale, operating time, residential conditions and hardware platforms, to improve the comparability of research results.

4. Current Main Problems and Research Directions

4.1 Trade-off Between Reliability and Low Power Consumption

The reliability of residential WSNs is also highly scenario-dependent. The same network may have different lev-

els of obstruction, temperature-humidity conditions and electromagnetic interference in the living room, kitchen, bathroom, staircase, etc. The results of packet loss rate and energy consumption in a single laboratory environment cannot reflect the actual performance of an entire house. Therefore, future studies should be zone-based and extended for a longer time to observe node failure, disconnection and recovery in detail.

Wall occlusion, multipath effects, node mobility and channel contention are all causes of link fluctuations. To increase the reliability of the system, one may need to add retransmission or redundancy; otherwise, it will be less reliable. The present multi-objective routing and sleep scheduling schemes have provided feasible solutions, but many related results have not yet been validated beyond simulation environments [18-19]. In the future, report the packet loss rate, latency, node lifetime and maintenance cost under different house layouts and extended-operation conditions simultaneously, rather than optimising only a single performance indicator.

4.2 Security and Privacy Protection

When it comes to Security and Privacy Protection,it is necessary to distinguish Security and Privacy Protection. Security focuses mainly on attacks, unauthorized access and communication safeguards, while privacy includes minimizing the collection of sensitive data, defining where data is processed and clarifying boundaries for data usage.Security problems are also end-to-end issues. Sensor nodes are susceptible to physical tampering; wireless links are vulnerable to eavesdropping or jamming; and gateways and cloud platforms are also at risk of problems such as user accounts, interfaces and data storage. Only increasing the encryption strength of a single protocol layer will not solve the security problems in residential WSNs. Layered Protection is necessary in a resource-constrained environment. Based on the sensitivity of the data, authentication, encryption and local processing strategies will be employed to avoid increasing the power consumption of security mechanisms and impacting node battery life or real-time communication.

WSN nodes have relatively weak computing and memory capabilities. Therefore, they may be involved in physical modification, snooping, jamming and routing attacks. To enhance security by adding encryption and authentication, there is a corresponding cost in computation and communication. Therefore, at present, the popular research directions include lightweight identity authentication, key agreement and anomaly detection [16, 22]. Smart home research should also focus on reducing the collection of sensitive data, performing edge processing and access control for this data, and derive security not only from network attack prevention but also from other sources.

4.3 Cross-Ecosystem Interoperability and Real-Scenario Validation

There are four main problems in cross-ecosystem interoperability,including Functional Interoperability,Protocol and Version Compatibility,Long-term Upgrading ability ,Fault Recovery and Long-term Operational Stability.In the aspect of Fuctional Interoperability,diverse devices from various brands have diverse protocols and different original function.naturally,cross-brand devices cannot achieve cross-ecosystem performance.In terms of upgrading ability and protocol and version compatibility,-Sensors, gateways and home appliances in a smart home have different update cycles. After the launching of new protocols, old devices may not be upgradable, which may eventually result in partially compatible hybrid networks. when it comes to fault recovery and long-term operational stability,those are also significant aspects.Devices from different brands have different systems to handle recovery damage and maintain long-term stability.(if cross-brand devices still use entirely different system to solve these problems,it will consumption more energy and be more complex to operate in real home environment.Therefore, in the evaluation of interoperability, verification should also confirm that the devices are connected. Instead, function mapping, long-term upgradeability, fault recovery as well as the stability of concurrent operation among devices from different manufacturers should also be examined.

Diverse protocols and functional differences in devices from various brands which hinder the cross-ecosystem coordination. The unified standard of Matter will improve the interoperability of applications, but it is not guaranteed that all device functions will work correctly. Retrofitting of old devices, version compatibility and operational stability still need engineering verification [12]. Meanwhile, most existing studies lack long-term testing in real residential environments. In the future, the direction of research will move from "algorithm feasibility" to "system usability", and network performance tests will be conducted in environments such as kitchen fumes, high humidity, wall occlusion, and large-scale heterogeneous node deployment.

5. Conclusion and Outlook

Wireless Sensor Networks (WSNs) can provide smart homes with environmental awareness, data transmission and device control. Based on related studies, the reason for the lack of further application is that there is an overall trade-off among reliability, energy consumption, security and interoperability, rather than the performance of a single algorithm.

Future research should reduce the validation method of only using simulations and laboratory prototypes, and increase long-term tests in real residential areas. In addition, edge computing and lightweight intelligent methods can

ISSN 3106-7018 (Print) ISSN 3106-5791 (Online)

be used to enhance the data processing and anomaly detection capabilities of sensor nodes without adding a large extra cost.

References

[1] Yang M X, Fang K, Wang X D, and others. A Method for Searching and Repairing Sensing Coverage Holes in Wireless Sensor Networks [J]. Chinese Journal of Sensors and Actuators, 2020, 33(5): 750-756.

[2] Li J Z, Gao H. Research progress on wireless sensor networks [J]. Journal of Computer Research and Development, 2008, (1): 1-15.

[3] Shi W Z, Wang P, Huang X. Application of Wireless Sensor Networks in Smart Home Systems [J]. *Journal of Fujian Normal University (Natural Science Edition)*, 2010, 26(6): 59-63.

[4] Lü G M, Chen H B. UAV Formation-assisted Node Localization Scheme for Wireless Sensor Networks [J]. Computer Applications and Software, 2026, 43(6): 67-77, 139.

[5] Guo Z P, Li J, Zhao Y G, et al. Review of Wireless Sensor Network Technologies in the Internet of Things[J]. Computers and Applied Chemistry, 2019, 36(1): 72-83. DOI: 10.16866/j.com.app.chem201901009.

[6] Fu M, Yang S H. Wireless Sensor Network Scheduling Based on Node State Transition Probability and Energy Optimization [J]. Chinese Journal of Sensors and Actuators, 2026, 39(5): 1153-1158.

[7] Pu J Q, Chen D W. TOA localisation algorithm based on least squares method and BP neural network [J]. Computer Technology and Development, 2018, 28(5): 5-8.

[8] Nong J, Miao Y Q, Qin Z S, et al. Discrete Encryption Algorithm for Sensitive Information Transmission in Large-Area Wireless Sensor Networks [J]. Chinese Journal of Sensors and Actuators, 2026, 39(2): 415-421.

[9] Liu Q, Liang X Y. An Energy-efficient WSN Model Based on Passive Clustering Algorithm [J]. Computer Engineering and Applications, 2007, (16): 142-145.

[10] Wang T, Li G, Mei YX, and others. Review of Sensing Cloud and Edge Computing (Invited) [J]. Computer Engineering, 2026, 52(5): 3-42. DOI: 10.19678/j.issn.1000-3428.0260004.

[11] Hu B, Sun Z X. Research on Time Synchronization Mechanism in Wireless Sensor Networks [J]. Computer Science, 2015, 42(7): 1-4, 11.

[12] Mota A, Serôdio C, Valente A. Matter Protocol Integration Using Espressif's Solutions to Achieve Smart Home Interoperability[J]. Electronics, 2024, 13(11): 2217. https://doi.org/10.3390/electronics13112217

[13] Xu Y J, Li J, Luo D X, et al. Review of physical layer security technologies for near field communication[J]. *Journal of Electronics & Information Technology*, 2025, 47(11): 4129-4143.

[14] Liu K X, Huang K Z, Pei X L, and others. Physical Layer Key Generation Method for Integrated Communication and Sensing Systems [J]. Journal of Electronics & Information Technology, 2026, 48(4): 1659-1667.

[15] Yan T, Zhao Y F, Gao M H, et al. Review of Adaptive MAC Protocols in Mobile Ad Hoc Networks [J]. Computer Engineering and Applications, 2023, 59(11): 46-56.

[16] Shin S, Kwon T. A Lightweight Three-Factor Authentication and Key Agreement Scheme in Wireless Sensor Networks for Smart Homes [J]. Sensors, 2019, 19(9): 2012. DOI: 10.3390/s19092012

[17] Pirbhulal S, Zhang H, Alahi M E E, and others. A New Secure IoT-based Smart Home Automation System Using a Wireless Sensor Network [J]. Sensors, 2017, 17(1): 69. DOI: 10.3390/s17010069

[18] Salerno V M. Wireless Sensor Networks for Smart Homes: A Fuzzy-based Solution for Energy-efficient Duty Cycle [J]. Electronics, 2019, 8(2): 131. DOI: 10.3390/electronics8020131

[19] Yeh W C, Jiang Y Z, Huang C L, and others. Improving Energy Consumption and Signal Transmission Quality of Routing Protocols in Wireless Sensor Networks [J]. IEEE Access, 2020, 8: 198254-198264. DOI: 10.1109/ACCESS.2020.2968311

[20] Jiang C Y, Wu S Y, Chen W. Smart Home System Based on Wireless Sensor Networks [J]. Microcomputer Information, 2007, (13): 199-201.

[21] Ji Q, Duan P Y, Li L F, and others. Smart Home System Based on ZigBee Wireless Sensor Network [J]. Computer Engineering and Design, 2008, (12): 3064-3067. DOI: 10.16208/j.issn1000-7024.2008.12.071

[22] Oztoprak A, Hassanpour R, Ozkan A, and others. Security Challenges, Mitigation Strategies and Future Trends in Wireless Sensor Networks: A Review [J]. ACM Computing Surveys, 2024, 57(4): 1-29. DOI: 10.1145/3706583

[23] Ransing R S, Rajput M. Smart home for elderly care based on wireless sensor network[C]//2015 International Conference on Nascent Technologies in the Engineering Field (ICNTE). IEEE, 2015: 1-5. DOI: 10.1109/ICNTE.2015.7048015