

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/371671907>

Wireless sensor networks in the internet of things: review, techniques, challenges, and future directions

Article in Indonesian Journal of Electrical Engineering and Computer Science · August 2023

DOI: 10.11591/ijeecs.v3i1.i2.pp1190-1200

CITATIONS

19

READS

7,163

5 authors, including:



Zijie Fu

University of Science Malaysia

1 PUBLICATION 19 CITATIONS

SEE PROFILE



Mahmood A. Al-Shareeda

Southern Technical University

215 PUBLICATIONS 2,515 CITATIONS

SEE PROFILE



Murtaja Ali

University of Basrah

43 PUBLICATIONS 482 CITATIONS

SEE PROFILE



Selvakumar Manickam

Universiti Sains Malaysia

371 PUBLICATIONS 4,850 CITATIONS

SEE PROFILE

Wireless sensor networks in the internet of things: review, techniques, challenges, and future directions

Fu Zijie¹, Mahmood A. Al-Shareeda², Murtaja Ali Saare³,
Selvakumar Manickam², Shankar Karuppayah²

¹School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia

²National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia

³Department of Computer Technology Engineering, Shatt Al-Arab University College, Basrah, Iraq

Article Info

Article history:

Received Jan 11, 2023

Revised Feb 24, 2023

Accepted Mar 12, 2023

Keywords:

Internet of things

Wireless sensor networks

WSN reviews

WSN-IoT

WSN-IoT approaches

WSN-IoT future direction

ABSTRACT

Wireless sensor networks (WSN) are an emerging multidisciplinary intersection of cutting-edge research fields, and their advantages in terms of freedom of formation, high signal-to-noise ratio, high strength, and unattended, which makes WSN have good prospects for application in the field of internet of things (IoT). Considering all the benefits that WSN offer, this paper reviews the development history of wireless sensor networks internet of things (WSN-IoT), analyses the technologies used by sensors in the IoT, and illustrates the future developing patterns and remaining challenges, in conjunction with the main technologies in the perception layer of the current network of things industry.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Selvakumar Manickam

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia

11800 USM, Penang, Malaysia

Email: selva@usm.my

1. INTRODUCTION

Information acquisition is an important area of research. All real-world things, states [1], [2], processes can be described in terms of physical quantities, and sensors can be used to obtain information about these physical quantities. Sensor information acquisition technology has evolved from its initial singularity to integration and networking, becoming an important means of information acquisition [3]. A wireless sensor network (WSN) system composed of spatially dispersed numerous sensors collaborating with each other provides stable and efficient communication between many sensors distributed in different places [4].

The internet of things (IoT) connects various forms of wired and wireless networks to the internet, thus linking objects to each other and forming a huge network for easy monitoring, analysis and control. Wireless sensing technology is widely used in many fields [5], such as battlefield surveillance, environmental and traffic detection, industrial and agricultural production. In essence, IoT technology is a technology that enables the interconnection of things through modern information networks [6], enabling the effective exchange and flow of information between items. However, the network environment itself has a certain openness, making it extremely easy for people to incur certain economic losses due to network risks in the application of IoT technology [7], [8]. Therefore, the improvement of the security of the network environment is also a major issue facing the wireless sensor network while improving its own technology level. The following is how the rest of this paper is arranged. The ideas of WSN and IoT are discussed in section 2. Section 3 describes the WSN-IoT's composition and application. Section 4 examines WSN-IoT research. Section 5 addresses the paper's issues and future directions. Section 6 finally brings the paper to a close.

2. WIRELESS SENSOR NETWORKS AND INTERNET OF THINGS

2.1. Wireless sensor networks

2.1.1. Overview

WNS, or wireless sensor networks, originated during the cold war, initially used in the military, it was used to monitor the activities of the enemy [9]-[12], and achieved better results, and later promoted to be more widely used, sensor technology is used in wireless sensor networks, network technologies wireless, embedded chip engineering [13], using a lot of tiny sensors to gather data and communicate with one another, so that it can real-time monitoring WSN technology is valued by many countries and has several potential variations [14], [15]. It is expected to play a greater role in industrial and agricultural production, urban planning and management, environmental monitoring, and battlefield surveillance in the future [16].

2.1.2. Architecture of WSN

WSN generally consist of three parts: sensor cells, managing nodes and aggregation nodes, the structure is displayed in Figure 1; i) sensor nodes: these are large nodes that can be thrown freely into the air and fall freely to the point of data collection for the entire WSN. These nodes are connected in series to form a whole sensor network; ii) convergence nodes: to provide a summary of all the details, the data acquired by the sensor nodes will be collected in the aggregate node using the routing mechanism; and iii) management node: the information filtered by the pooling node is transmitted via the network and communication equipment to a terminal platform, where the relevant staff can effectively analyze the data recorded.

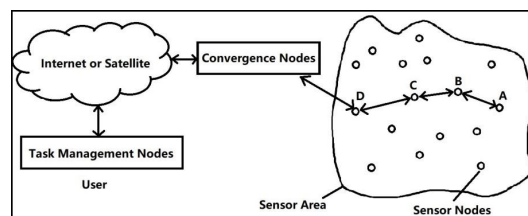


Figure 1. Architecture of WSN schematic

2.1.3. WSN Features

Networks of wireless sensors have the following features i) large scale: compared to other networks, networks of wireless sensors cover greater variety of information and acquire a greater amount of information [17]. These advantages are based on a profusion of sensor nodes. However, when the number of sensor nodes is high, this can make maintenance difficult [18]. In addition, the particular application area of the sensor nodes can make it challenging to replace them, especially in environments with high temperatures and pressures or high radiation levels [19]; ii) limited battery capacity: the stability of the working state of an infinite sensor network has a huge relationship with the battery capacity [20]. Typically, batteries are not renewable and need to be replaced in a timely manner in the event of damage or low power [21], but the relatively complex geographical location of sensor nodes makes timely replacement difficult and the relatively wide range of sensors used increases the difficulty of replacement [22]. Likewise, in order to ensure the correctness of the data obtained by the sensors, the battery life needs to be increased [23]; iii) Compensating for weak communication capabilities with the help of multi-hop network technology generally speaking, sensors are poorly equipped in terms of communication and must be routed with the help of multi-hop network technology when communicating with each other and other nodes [24]. Multi-hop network transmission technology can pass information to the aggregation node corresponding to the node and can forward information sent by other sensor nodes. Even if individual sensor nodes fail, they can be interconnected with other nodes [25]; and iv) the sensor node is the location of the free fall point after the sensor has been randomly thrown, and the corresponding network structure has to be built after finding the right fall point. During specific use, they are prone to a variety of faults, such as power failure or damage. Therefore, the entire sensor network needs to have a strong dynamic coordination capability.

2.2. Internet of things

2.2.1. Overview

The IoT can be connected to objects because of the sensors, processors and communication modules that are installed on them. On this level, the IoT has a wider range of applications than the internet. The main core functions of the IoT are sensing information, transferring information and controlling information [26], [27]. Through the IoT, people can quickly access, transfer and process information [28].

2.2.2. Architecture of IoT

As shown the Figure 2, any or all of these components plays an important role in the IoT's overall structure. i) perceptual layer: in an IoT system, temperature, operating status and other relevant parameters need to be collected through the sensing layer. When certain parameters reach a preset range, the IoT remote control is activated [29]. For example, in an IoT-based warehouse management system, the site environment is detected by an infrared temperature measuring device [30], but an alarm is issued when a fire is detected and a water spray is activated [8]; ii) network layer: the IoT system's skeleton is made up of the network transport layer. All types of networks, such as the internet [31], [32], ethernet and mobile networks, can be used as network transport layers. The information obtained from the sensing layer and the control commands communicated to the actuators need to be transmitted through the network layer of transmission; and iii) applying layer: the applying layer consists of two parts: a software system for processing information and a web page or mobile app for human control. The application layer integrates intelligent information processing technologies such as distributed computing and cloud computing. The data and information transmitted from the network transmission layer is concentrated in the application layer system for processing, and the system is equipped with functions such as addressing, command issuance, security control and data storage. In addition, the application layer has an extension interface to enable the expansion of new functions.

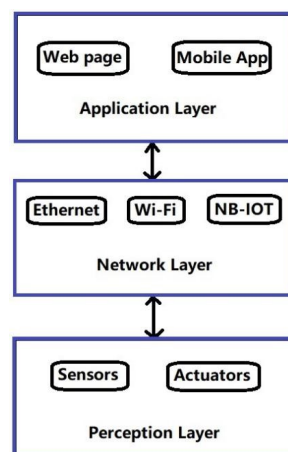


Figure 2. Architecture of IoT

3. WIRELESS SENSOR NETWORKS IN THE INTERNET OF THINGS

3.1. Architecture of WSN-IoT

As shown the Figure 3, these are three tiers to the WSN-IoT as flowers: i) the perception layer: the underlying perception layer is used to sense data. Before data arrives by the gateway, the perception layer is composed data gathering apparatuses like sensors and sensor networks. The foundation for the creation and use of the IoT is the perception layer [33]. The primary technologies utilized in the perception layer are radio frequency identification (RFID), short-range wireless communication, and control and sensing, which in turn includes chip development, communication protocol research, RFID materials, intelligent power saving and other subdivision technologies [34], [35]; ii) the transmission layer: the second layer contains the transmission layer for data transfer. The essential technology for implementing a data-centric IoT is the technology for managing and analysing sensor data in the transmission layer [36], which covers theories and methods for decision-making and behavior based on sensing data, as well as the understanding, analysis, storage, query,

and mining of sensor network data [37]. The cloud computing platform will be a crucial component of the IoT as a platform for the storing and analysis of enormous amounts of sensory data [38]; iii) the application layer: the application layer is the top layer. The application layer of the IoT offers users a variety of specialised services based on the analysed and processed sensory data [39]. These services can be categorised as monitoring (logistics monitoring, pollution monitoring), querying (intelligent retrieval, remote metre reading), controlling (intelligent traffic, intelligent homes, street light control), scanning (mobile phone wallet, highway non-stop toll). IoT application layer development aims to give consumers with vibrant IoT apps through software development and intelligent control technologies [28]; and iv) human sense organs, such as the eyes and ears, which can gather visual information, the nose, which can gather odour information, taste information, and the mouth, which can gather sound information, are the IoT's perception layer [40], if we use the human neural network as an example. Neurons are used to transport information to the brain's processing centre, and the neural channels generated by these neurons are analogous to the IoT's transmission layer, which has the same function. It can combine the information it gets from the eyes, nose, mouth, and ears to make certain helpful deductions [41], such as determining whether there is immediate danger, having the ability to read a book and watch a movie [42]. In other words, it creates value by using the knowledge from the perception layer [43].

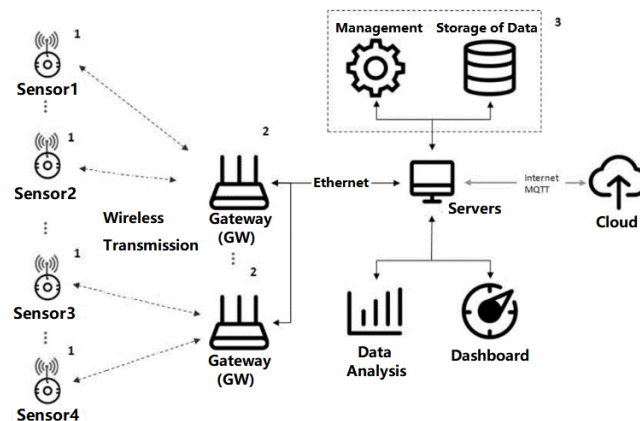


Figure 3. Architecture of WSN-IoT

3.2. Main technologies

Some of the main technologies of wireless sensor networks in IoT systems are discussed. In addition, the application of these technologies are provided in IoT systems. Figure 4 explains the following steps in detail.

- Network protocols: at this stage, media access control (MAC) protocols and routing protocols are the key technical items in the research of network protocols in intelligent wireless sensing networks. MAC protocols directly determine the way in which intelligent wireless sensing networks use wireless signal channels, and currently the more typical MAC protocols are TDMA, IEEE802, S-MAC, T-MAC protocols routing protocols can be divided into reliable routing protocols according to their functions. The following routing protocols are used: location-geographic routing, query routing, energy-aware routing.
- Node positioning: node placement is the process of locating a sensor node's exact location and locating it in relation to other nodes. Range-based node placement, which needs accurate measurement of angles and distances between nodes (distance-based positioning) [44]. Techniques that do not require actual measurements for node positioning are called range-free (distance-independent positioning) range-based techniques are energy-intensive and costly, and range-free positioning mechanisms are basically used in wireless smart sensor networks today [2].
- Routing security: network of wireless sensors once some of the nodes are malicious intrusion, it can be carried out through its destruction of the network, such as ordering it to stop collecting or sending information, send the wrong data or even attack the network environment. This requires the wireless sensor network in the design must take into account the security and stability of the protocol [45], through encryption, regular antivirus, system repair and other measures to ensure that the network can be normal operation, not easy to be infringed [46].

- Data fusion: data fusion technology has a specific application-oriented and always data-centric features, the use of data fusion technology can be omitted in the traditional network of addressing links, so that the nodes of information is directly and quickly organized [47], the use of fusion processing, the effective information quickly extracted and sent to the user to complete the reception can be, the commonly used data fusion methods include neural network method, Bayesian method, D-S evidence The common methods of data fusion include neural networks, Bayesian methods, D-S evidence theory.
- Topology control: the use of topology control technology allows the network topology to be generated automatically and well, making MAC protocols and routing protocols more efficient, while also providing a basis for synchronising time, fusing data, locating targets and other operations. This not only contributes to energy savings, but also to a degree that extends the useful life of the network. Currently, commonly used topology control techniques include power control, node heuristic wake-up, topology hierarchies and hibernation mechanisms [48].

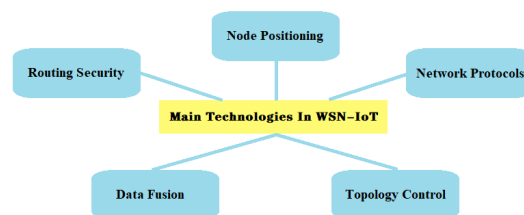


Figure 4. Main technologies of WSN-IoT

3.3. Model of WSN-IoT

Various architectures of WSN-IoT and their benefits, drawbacks, and applications are discussed here.

- Flat network structure: a flat network structure where all nodes are peer-to-peer and have identical functional characteristics, i.e., each node contains the same MAC, routing, management and security protocols. Advantages: Planar network structure is relatively simple, it is also referred to as a peer-to-peer structure since every node has an equal status; there are generally multiple pathways connecting the origin and destination nodes, the network load is shared by these paths, in general there is no bottleneck, the network is more robust [49]. Disadvantages: The flat network structure has problems in the organization of nodes, route establishment, control and maintenance of message overhead, which can take up a lot of bandwidth and affect the transmission rate of network data; in addition, the whole system will lose a lot of energy on a macro level; and poor scalability.
- Hierarchical network structure: the network is divided into two parts: the upper layer is a sub-network structure created by connecting the primary backbone nodes, the bottom layer is a sub-network structure created by connecting generic sensor nodes [50]. Advantages: in the hierarchical structure, the sensor network is divided into multiple clusters, each cluster is made up of a cluster head and several cluster members; the cluster heads comprise the network's upper level; It is the responsibility of cluster head nodes to transmit data across clusters, cluster members are only responsible for the collection of data, this significantly decreases the network's amount of control information, with good scalability [50]. Disadvantages: problematic is the cluster head's high energy consumption, as the frequency of sending and receiving messages is several times or more than ten times higher than that of a normal node, thus requiring that the cluster head can be replaced by running a cluster head selection procedure within the cluster.
- Hybrid network structure: a flat network structure is used between the network backbone nodes and between the general sensor nodes, while a hierarchical network structure is used between the network backbone nodes and the general sensor nodes. Advantages: fault diagnosis and isolation is easier, once the network fails, just diagnose which network device has a fault, and then disconnect that network device from the rest of the network. It is simple to add additional network devices, and some spare ports may be left in each network device [51]. The primary network link simply connects to the aggregation layer device, while the branch link links to the aggregation layer device and the access layer device. Disadvantages: intelligent network equipment is required to achieve automatic diagnosis of network faults and isolation of faulty nodes, moreover, the cost of network development is quite high; relying on the central node, if the equipment linked

to the centre fails, the entire network is paralysed, so the central equipment's reliability and redundancy requirements are high.

- Mesh network structure: mesh network structure is a fresh type of framework for a wireless sensor network. The greatest advantage of the mesh network structure is that all nodes are on a peer-to-peer basis and have the same computational and communication functions, a node can be designated as cluster head and can perform additional functions [52]. In the event of a cluster head node failing, another node can immediately replenish and take over those additional functions performed by the original cluster head. Benefits: fast deployment, easy installation of mesh wireless networking, ready to use on power. Non-line-of-sight transmission: direct line-of-sight nodes can forward signals to non-direct line-of-sight nodes, which can be easily configured using wireless mesh technology [53]. Stability: typically, using numerous routers to transport data is the best strategy to ensure network stability. Structural flexibility: since each device has several transmission lines available and the network may dynamically allocate communication routes based on each node's communication load, communication congestion can be successfully avoided [54], [55]. Disadvantages: each forwarding requires a certain delay, and the delay will be higher after multiple forwardings; the bandwidth capacity is limited, and the rate will decrease after each forwarding, so there cannot be too many nodes.

3.4. Application areas of WSN-IoT

The various application areas of WSNs in IoT and the contribution of WSNs in the field are described in detail. These applications are military, agricultural field, medical care, and transportation. The explanation of these application is provided as follows.

- Military: WSN technology is stealthy, self-organisable and highly fault-tolerant, which helps sensors to function in dangerous battlefield environments. In the military field, the artillery target area is covered by a huge number of sensor nodes that are deployed using wireless sensor network technology, aircraft and other launchers. Firstly, the magnetic field, humidity, sound, and temperature and other details about the environment around node of the sensor is collected; second, the sensor self-organizes the network and transmits the data to the information centre through satellite, the internet, and other communication channels, which in turn provides real-time monitoring of the tools of the adversary and strength, assessment of the front lines and continuous observation of the enemy's attacks, increasing efficiency in an effective manner of the army's operational success [56].
- Agricultural field: WSN has the advantages of dense distribution, simple deployment, and easy communication, can be in the agricultural sector in real-time monitoring of soil environmental conditions, livestock environmental conditions, crop growth, large and cumulative surface characteristics. In addition, wireless sensor network technology combined with mature global positioning system (GPS) technology, internet technology, can establish a dynamic real-time management platform, through wireless sensors to monitor the crop growth environment, analysis of crop quality and the relationship between the growth environment, and thus achieve precision agriculture, intelligent farming purposes.
- Medical care: with the ageing of the population, medical care for patients is now an issue that must be addressed. Wireless sensor network technology is playing an important role in the medical care sector [57]. Doctors can place various sensors on patients to detect and collect physiological information such as blood pressure, respiration and temperature in real time, so that they can understand the development of the patient's condition in real time and use the physiological information collected as a reference for drug development. In addition, multiple sensor nodes can be installed in the patient's living environment to monitor the patient's activities remotely in real time, so that the patient can be assisted in the event of a problem.
- Transportation: with the improvement of people's quality of life, the increasing number of private cars and the rapid development of the logistics industry, traditional traffic systems have become obsolete and intelligent transportation has come into being. WSN enable real-time monitoring of traffic conditions [58]. By placing sensors on the road to monitor vehicles and centrally analyzing the road conditions, the flow of traffic on each route segment can be measured, thus providing the best route for the traveler to take in order to increase the effectiveness of traffic management and lessen traffic congestion.

4. RESEARCH STUDIES IN WSN-IOT

Currently, WSN-IoT is applied in numerous fields, typically in transport, healthcare, agriculture and military, and the WSN technologies used in different fields differ. This section reviews the history of WSN-IoT and the implementation of WSN-IoT solutions in various studies. Information acquisition is an important research area in the information society. The development of sensor networks has undergone a long development process and can be roughly divided into four stages.

The beginning was in the 1970s when, as an emerging technology, multiple sensors were connected using sensing controllers to form the beginnings of sensor networks [59], which used rudimentary sensors with simple information signal acquisition capabilities and used transmission methods such as point-to-point connections to sensing controllers to form sensor networks. With the development of related disciplines, the second phase of the sensor network has the ability to acquire multiple information signals, and the interface with the sensing controller has been updated with a serial/parallel interface (e.g. RS-232, RS-485 interface), constituting a sensor network with information synthesis and processing capabilities.

The third stage appeared in the late 1990s and early 21st century, this period of sensors can be intelligent access to a variety of information, a new type of sensing of signals, connected to the sensing controller using field bus control, according to the application constitutes a number of local area networks, which can be called sophisticated sensor networks [60]. Sensor networks' fourth stage is being researched and developed, combined with the current research hotspot: a lot of sensors are used in wireless sensor networks with multiple types of signal acquisition capabilities organized into self-organizing wireless access networks, the biggest change is the wireless way to connect with the sensor network controller, thus forming a WSN.

The coverage of sensor nodes and energy consumption are important performance indicators of a WSN. The convergence speed of the traditional computer science algorithm is not high and the global monitoring capability is not strong. The step size of the algorithm is optimized with the momentum gradient descent method and the root mean square method to increase the algorithm's rate of convergence, then the global detection capability of the algorithm is improved with the Corsi-Gaussian variation factor to make finding the most advantageous global solution is preferable. To address the shortcomings of the EEUC algorithm that the cluster head nodes are not uniformly distributed and the competition radius remains unchanged [61], it is shown that selecting the cluster head nodes from two factors, namely the nodes' remaining energy and their physical placement, to make their distribution more uniform, and then the calculation formula of the competition radius is optimized from these two factors, so that it can make reasonable changes with the operation of the network and balance the energy consumption of the nodes. energy consumption of the nodes.

The number and variety of sensors in the network environment has increased, and with different sensors having different functions [62], the storage and transmission of data in the network environment has grown exponentially. Often set up in unattended environments, factors such as humidity and temperature in the environment can cause further increases in the probability of abnormal data changes in the network. Current researchers in the field are addressing the problem in two ways: reducing the burden of sensors on data collection and data transmission to lower the network operation's energy usage, and improving the network's resilience to abnormal data and promoting the overall robustness of the network operation. The most important issue in WSNs is data privacy protection. The current solutions proposed by researchers for data privacy protection in WSN-IoT are: slice-based data aggregation privacy protection algorithm (S-DAPP), authentication technology combined with WSN, cluster privacy data aggregation approach (CPDA), and slice mixing and aggregation mechanism (SMART).

5. CHALLENGES AND FUTURE DIRECTIONS

The technology underlying wireless sensor networks is far from perfect at the moment. that require more study and development, and whose innovative work will substantially ease the progress of the IoT.

- Multi-hosted network transmission method: the IoT relies on wireless sensor network technology to function. Attempts can be made to leverage multi-homed network transmission in an effort to boost the IoT's resiliency. It allows for many links to transfer commands from the top down, as well as the collecting of data from several sensors to be relayed to the upper network. This method has the potential to speed up data transfer via networks and make them more reliable.
- Designing low power systems: due to the non-linear nature of wireless sensor networks, it is not possible to link individual sensor nodes to the energy network, so in order to extend the lifetime of WS, the low-power

design of the system must be explored. Currently, studies rely on the low power requirements of individual sensors rather than connecting them. The low-power design of the system can attempt to collaborate individual sensors with software and hardware in an IoT environment, where wireless sensor networks rely on the IoT's data processing and analysis capabilities.

6. CONCLUSION

The development and deployment of IoT technologies is heavily influenced by WSN. The range of applications of WSN-IoT is constantly expanding and people are relying more and more on them. In practical applications, people can only improve the network performance of wireless sensors and encourage the advancement of cutting-edge information network technologies if they fully understand the connection between the IoT and WSN and optimize the specific technical forms. Based on the current power consumption and security of wireless sensor networks the following improvements are proposed.

Wireless sensors are limited by their size and carry a limited battery capacity, so it is important to reduce their power consumption while achieving information transfer. In traditional wireless sensor networks, communication between nodes requires wake-up to communicate. Wireless sensor networks can use a timed wake-up asynchronous communication mechanism to transfer information, i.e. The transmitting node has the ability to transmit data to the receiving node when it is asleep, and then send data to other nodes after the receiving node wakes up. The timing here is the node wake-up interval set by the wireless sensor network system, and the system can set the timing wake-up interval according to the real-time requirements. When real-time requirements are high, the node wake-up time interval is short, and vice versa, a longer wake-up time interval can be set. This can effectively improve the operational lifetime of the net and the throughput of the net.

In order to improve the security of the sensor net protocol, a cluster head election method can be added to the LEACH routing protocol, a one-way hash function and a shared key can be added to the communication between base station and sensor nodes, so that the communication key between the two can be changed periodically, and an authentication mechanism can be added so that only the internal members of the system have permission to access, thus increasing the confidentiality of the information in the communication and improving the security of the information transmission.

At present, the research and development of WSN technology still has many imperfections, its breakthrough research will certainly have a huge impact on the IoT, to further promote the construction and development of information technology, with the fast advancement of knowledge and technology, it is foreseeable that the future application of WSN-IoT will provide more convenience for people's production life.

REFERENCES

- [1] N. Prakash, M. Rajalakshmi, and R. Nedunchezian, "Analysis of QoS for conveying authorisation based on internet of things (IoT) in wireless sensor networks (WSN)," in *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, Jul. 2020, pp. 1–9, doi: 10.1109/ICSSS49621.2020.9202338.
- [2] M. A. Al-Shareeda and S. Manickam, "MSR-DoS: modular square root-based scheme to resist denial of service (DoS) attacks in 5G-enabled vehicular networks," *IEEE Access*, vol. 10, pp. 120606–120615, 2022, doi: 10.1109/ACCESS.2022.3222488.
- [3] M. Henschke, X. Wei, and X. Zhang, "Data visualization for wireless sensor networks using thingsboard," in *2020 29th Wireless and Optical Communications Conference (WOCC)*, May 2020, pp. 1–6, doi: 10.1109/WOCC48579.2020.9114929.
- [4] F. Ertam, I. F. Kilincer, O. Yaman, and A. Sengur, "A new IoT application for dynamic WiFi based wireless sensor network," in *2020 International Conference on Electrical Engineering (ICEE)*, Sep. 2020, pp. 1–4, doi: 10.1109/ICEE49691.2020.9249771.
- [5] M. Meli, E. Gatt, O. Casha, I. Grech, and J. Micallef, "A novel modular low power and low cost IoT wireless sensor node for air quality monitoring," in *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, Dec. 2021, pp. 1476–1481, doi: 10.1109/CSCI54926.2021.00019.
- [6] A. A. Gotsinas, K. Kalovrektis, A. Xenakis, and G. Stamoulis, "A ZigBee – based lightweight Wireless sensor system for measuring action potential bio signals in agriculture IoT applications," in *2020 11th International Conference on Information, Intelligence, Systems and Applications (IISA)*, Jul. 2020, pp. 1–7, doi: 10.1109/IISA50023.2020.9284340.
- [7] A. Mukherjee, J. J. P. C. Rodrigues, P. Goswami, L. Manman, R. Hazra, and L. Yang, "Green cooperative communication based cognitive radio sensor networks for IoT applications," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICCWorkshops49005.2020.9145290.
- [8] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 12, no. 2, pp. 930–939, Apr. 2023, doi: 10.11591/eei.v12i2.4466.
- [9] S. M. Rabeek and M. K. Raja, "Design of an autonomous IoT wireless sensor node for industrial environments," in *2020 IEEE Asia-Pacific Microwave Conference (APMC)*, Dec. 2020, pp. 715–717, doi: 10.1109/APMC47863.2020.9331650.

- [10] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and M. A. Saare, "Enhancement of NTSA secure communication with one-time pad (OTP) in IoT," *Informatica*, vol. 47, no. 1, Feb. 2023, doi: 10.31449/inf.v47i1.4463.
- [11] P. C. Menon, "IoT enabled aquaponics with wireless sensor smart monitoring," in *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Oct. 2020, pp. 171–176, doi: 10.1109/I-SMAC49090.2020.9243368.
- [12] U. Draz, S. Yasin, A. Ali, M. A. Khan, and A. Nawaz, "Traffic agents-based analysis of hotspot effect in IoT-enabled wireless sensor network," in *2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST)*, Jan. 2021, pp. 1029–1034, doi: 10.1109/IBCAST51254.2021.9393202.
- [13] J. Falcao, P. Menezes, and R. P. Rocha, "Automatic identification of wireless sensor network topology in a IoT domestic setup and discovery of user routines," in *2020 International Conference on Omni-layer Intelligent Systems (COINS)*, Aug. 2020, pp. 1–7, doi: 10.1109/COINS49042.2020.9191423.
- [14] T. M. Bandara, W. Mudiyanse, and M. Raza, "Smart farm and monitoring system for measuring the environmental condition using wireless sensor network - IOT Technology in farming," in *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)*, Nov. 2020, pp. 1–7, doi: 10.1109/CITISIA50690.2020.9371830.
- [15] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. Bin Omar, "SADetection: security mechanisms to detect SLAAC attack in IPv6 link-local network," *Informatica*, vol. 46, no. 9, Jan. 2023, doi: 10.31449/inf.v46i9.4441.
- [16] D. Kraus, K. Diwold, and E. Leitgeb, "Getting on track – simulation-aided design of wireless IoT sensor systems," in *2020 International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom)*, Jul. 2020, pp. 1–6, doi: 10.1109/CoBCom49975.2020.9174177.
- [17] S. K. Sarma, "Energy aware cluster based routing for wireless sensor network in IoT: impact of bio-inspired algorithm," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Aug. 2020, pp. 198–206, doi: 10.1109/ICSSIT48917.2020.9214156.
- [18] S. A. Yadav, S. Sharma, L. Das, S. Gupta, and S. Vashisht, "An effective IoT empowered real-time gas detection system for wireless sensor networks," in *2021 International Conference on Innovative Practices in Technology and Management (ICIPTM)*, Feb. 2021, pp. 44–49, doi: 10.1109/ICIPTM52218.2021.9388365.
- [19] M. A. Al-Shareeda, S. Manickam, M. A. Saare, S. Karuppayah, and M. A. Alazzawi, "A brief review of advanced monitoring mechanisms in peer-to-peer (P2P) Botnets," in *2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, Aug. 2022, pp. 312–317, doi: 10.1109/ICCITM56309.2022.10031721.
- [20] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communications in IoT systems: hiding information in interference," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 46–52, Dec. 2018, doi: 10.1109/MWC.2017.1800070.
- [21] J. Wang, C. Jiang, K. Zhang, T. Q. S. Quek, Y. Ren, and L. Hanzo, "Vehicular sensing networks in a smart city: principles, technologies and applications," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 122–132, Feb. 2018, doi: 10.1109/MWC.2017.1600275.
- [22] K. W. Choi *et al.*, "Toward realization of long-range wireless-powered sensor networks," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 184–192, Aug. 2019, doi: 10.1109/MWC.2019.1800475.
- [23] M. A. Al-Shareeda, S. Manickam, M. A. Saare, S. Karuppayah, and M. A. Alazzawi, "Detection mechanisms for peer-to-peer Botnets: a comparative study," in *2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, Aug. 2022, pp. 267–272, doi: 10.1109/ICCITM56309.2022.10031860.
- [24] X. Lin, M. Guizani, X. Du, C.-K. Chu, and Y. Yu, "Advances of security and privacy techniques in emerging wireless networks," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 8–9, Jun. 2020, doi: 10.1109/MWC.2020.9116080.
- [25] C. M. Costa and P. Baltus, "Design methodology for industrial internet-of-things wireless systems," *IEEE Sensors Journal*, vol. 21, no. 4, pp. 5529–5542, Feb. 2021, doi: 10.1109/JSEN.2020.3031659.
- [26] K. G. Omeke *et al.*, "DEKCS: a dynamic clustering protocol to prolong underwater sensor networks," *IEEE Sensors Journal*, vol. 21, no. 7, pp. 9457–9464, Apr. 2021, doi: 10.1109/JSEN.2021.3054943.
- [27] S. K. S. Tyagi, A. Mukherjee, S. R. Pokhrel, and K. K. Hiran, "An intelligent and optimal resource allocation approach in sensor networks for smart agri-IoT," *IEEE Sensors Journal*, vol. 21, no. 16, pp. 17439–17446, Aug. 2021, doi: 10.1109/JSEN.2020.3020889.
- [28] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 29, no. 1, pp. 518–526, Jan. 2022, doi: 10.11591/ijeecs.v29.i1.pp518-526.
- [29] D. Xue and W. Huang, "Smart agriculture wireless sensor routing protocol and node location algorithm based on internet of things technology," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 24967–24973, Nov. 2021, doi: 10.1109/JSEN.2020.3035651.
- [30] R. L. Rosa, C. Dehollain, A. Burg, M. Costanza, and P. Livreri, "An energy-autonomous wireless sensor with simultaneous energy harvesting and ambient light sensing," *IEEE Sensors Journal*, vol. 21, no. 12, pp. 13744–13752, Jun. 2021, doi: 10.1109/JSEN.2021.3068134.
- [31] N. Kumar and D. P. Vidyarthi, "A green routing algorithm for IoT-enabled software defined wireless sensor network," *IEEE Sensors Journal*, vol. 18, no. 22, pp. 9449–9460, Nov. 2018, doi: 10.1109/JSEN.2018.2869629.
- [32] S. Javaid, S. Zeadally, H. Fahim, and B. He, "Medical sensors and their integration in wireless body area networks for pervasive healthcare delivery: a review," *IEEE Sensors Journal*, vol. 22, no. 5, pp. 3860–3877, Mar. 2022, doi: 10.1109/JSEN.2022.3141064.
- [33] X. Zhong and Y. Liang, "Scalable downward routing for wireless sensor networks and internet of things actuation," in *2018 IEEE 43rd Conference on Local Computer Networks (LCN)*, Oct. 2018, pp. 275–278, doi: 10.1109/LCN.2018.8638125.
- [34] F. F. Jurado-Lasso, K. Clarke, A. N. Cadavid, and A. Nirmalathas, "Energy-aware routing for software-defined multihop wireless sensor networks," *IEEE Sensors Journal*, vol. 21, no. 8, pp. 10174–10182, Apr. 2021, doi: 10.1109/JSEN.2021.3059789.
- [35] Z. G. Al-Mekhlafi *et al.*, "Efficient authentication scheme for 5G-enabled vehicular networks using fog computing," *Sensors*, vol. 23, no. 7, p. 3543, Mar. 2023, doi: 10.3390/s23073543.
- [36] W. Osamy, A. Salim, A. M. Khedr, and A. A. El-Sawy, "IDCT: intelligent data collection technique for IoT-enabled heterogeneous wireless sensor networks in smart environments," *IEEE Sensors Journal*, vol. 21, no. 18, pp. 21099–21112, Sep. 2021, doi: 10.1109/JSEN.2021.3100339.
- [37] Z. Xue, "Routing optimization of sensor nodes in the internet of things based on genetic algorithm," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25142–25150, Nov. 2021, doi: 10.1109/JSEN.2021.3068726.




- [38] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, "Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure SECS/GEM communications," *Sustainability*, vol. 14, no. 23, p. 15900, Nov. 2022, doi: 10.3390/su142315900.
- [39] W. Osamy, A. M. Khedr, and A. Salim, "ADSDA: adaptive distributed service discovery algorithm for internet of things based mobile wireless sensor networks," *IEEE Sensors Journal*, vol. 19, no. 22, pp. 10869–10880, Nov. 2019, doi: 10.1109/JSEN.2019.2930589.
- [40] H. H. Qasim, A. E. Hamza, H. H. Ibrahim, H. A. Saeed, and M. I. Hamzah, "Design and implementation home security system and monitoring by using wireless sensor networks WSN/internet of things IoT," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 2617–2624, Jun. 2020, doi: 10.11591/ijece.v10i3.pp2617-2624.
- [41] N. Boonnam, J. Pitakphongmetha, S. Kajornkasirat, T. Horanont, D. Somkiadcharoen, and J. Prapakornpilai, "Optimal plant growth in smart farm hydroponics system using the integration of wireless sensor networks into internet of things," *Advances in Science, Technology and Engineering Systems Journal*, vol. 2, no. 3, pp. 1006–1012, Jul. 2017, doi: 10.25046/aj0203127.
- [42] M. A. Al-Shareeda and S. Manickam, "COVID-19 vehicle based on an efficient mutual authentication scheme for 5G-enabled vehicular fog computing," *International Journal of Environmental Research and Public Health*, vol. 19, no. 23, p. 15618, Nov. 2022, doi: 10.3390/ijerph192315618.
- [43] O. Tas and F. Kiani, "Detection and prevention of attacks on the internet of things (IoT) and wireless sensor networks," *Journal of Polytechnic-Politeknik Dergisi*, vol. 24, no. 1, pp. 219–235, 2021.
- [44] M. W. Rasooli, B. Bhushan, and N. Kumar, "Applicability of wireless sensor networks & IoT in saffron & wheat crops: a smart agriculture perspective," *International Journal of Scientific & Technology Research*, vol. 9, no. 2, pp. 2456–2461, 2020.
- [45] H. Guo, R. Wu, B. Qi, and Z. Liu, "Lifespan-balance-based energy-efficient routing for rechargeable wireless sensor networks," *IEEE Sensors Journal*, vol. 21, no. 24, pp. 28131–28142, Dec. 2021, doi: 10.1109/JSEN.2021.3124922.
- [46] M. A. Al-Shareeda et al., "Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU)," *Sustainability*, vol. 14, no. 16, p. 9961, Aug. 2022, doi: 10.3390/su14169961.
- [47] R. Al-Zaidi, J. C. Woods, M. Al-Khalidi, and H. Hu, "Building novel VHF-based wireless sensor networks for the internet of marine things," *IEEE Sensors Journal*, vol. 18, no. 5, pp. 2131–2144, Mar. 2018, doi: 10.1109/JSEN.2018.2791487.
- [48] A. Kumar and S. Sharma, "Participation of 5G with wireless sensor networks in the internet of things (IoT) application," in *Wireless Sensor Networks and the Internet of Things*, New York: Apple Academic Press, 2021, pp. 229–244.
- [49] V. G. Rajeshwarkar, S. M. Jagade, and P. C. Reddy, "Multi parameter approach for low energy adaptive efficient wireless sensor networks for IoT applications," 2019.
- [50] S. Gupta, S. Gupta, and D. Goyal, "Wireless sensor network in IoT and performance optimization," *Recent Advances in Computer Science and Communications*, vol. 15, no. 1, pp. 14–22, Jan. 2022, doi: 10.2174/2666255813999200831123235.
- [51] K. Kaczmarek, L. Dymova, and P. Sevastjanov, "Intuitionistic fuzzy rule-base evidential reasoning with application to the currency trading system on the forex market," *Applied Soft Computing*, vol. 128, p. 109522, Oct. 2022, doi: 10.1016/j.asoc.2022.109522.
- [52] R. K. Pattanaik, S. K. Mohapatra, M. N. Mohanty, and B. K. Pattanayak, "System identification using neuro fuzzy approach for IoT application," *Measurement: Sensors*, vol. 24, p. 100485, Dec. 2022, doi: 10.1016/j.measen.2022.100485.
- [53] A. P. Atmaja, A. El Hakim, A. P. A. Wibowo, and L. A. Pratama, "Communication systems of smart agriculture based on wireless sensor networks in IoT," *Journal of Robotics and Control (JRC)*, vol. 2, no. 4, 2021, doi: 10.18196/jrc.2495.
- [54] D. García-Orozco, V. G. Alfaro-García, J. M. Merigó, I. C. E. Moreno, and R. G. Monge, "An overview of the most influential journals in fuzzy systems research," *Expert Systems with Applications*, vol. 200, p. 117090, Aug. 2022, doi: 10.1016/j.eswa.2022.117090.
- [55] D. Dell'Anna and A. Jamshidnejad, "Evolving fuzzy logic systems for creative personalized socially assistive robots," *Engineering Applications of Artificial Intelligence*, vol. 114, p. 105064, Sep. 2022, doi: 10.1016/j.engappai.2022.105064.
- [56] P. S. Pandey, D. E. Chaitanya, V. K. Minchula, D. Sreekanth, V. Premchandran, and T. Keerthika, "IoT-enabled wireless sensor networks for controlled and safe routing," *International Journal of Aquatic Science*, vol. 12, no. 2, pp. 1712–1718, 2021.
- [57] E. Inga, J. Inga, and A. Ortega, "Novel approach sizing and routing of wireless sensor networks for applications in smart cities," *Sensors*, vol. 21, no. 14, p. 4692, Jul. 2021, doi: 10.3390/s21144692.
- [58] P. K. Sharma, J. Singh, Yogita, and V. Pal, "Low power communication in wireless sensor networks and IoT," in *Smart Sensor Networks Using AI for Industry 4.0*, Boca Raton: CRC Press, 2021, pp. 221–233.
- [59] R. K. Saini and C. Prakash, "Internet of things (IoT) for Agriculture growth using wireless sensor networks," *Global Journal of Computer Science and Technology*, vol. 20, pp. 27–34, 2020.
- [60] R. Kashyap, "Applications of wireless sensor networks in healthcare," in *IoT and WSN Applications for Modern Agricultural Advancements: Emerging Research and Opportunities*, 2020, pp. 8–40.
- [61] S. Gupta and S. Gupta, "Internet of things and the role of wireless sensor networks in IoT," in *Smart Agricultural Services Using Deep Learning, Big Data, and IoT*, 2020, pp. 113–127.
- [62] B. S. Chaudhari, S. Ghorpade, and M. Zennaro, "Towards green computing: intelligent bio-inspired agent for IoT-enabled wireless sensor networks," *International Journal of Sensor Networks*, vol. 35, no. 2, p. 121, 2021, doi: 10.1504/IJSNET.2021.10036232.

BIOGRAPHIES OF AUTHORS






Fu Zijie received his Bachelor's degree from Tung Wah University of Technology and is currently studying for his Master's degree at USM Penang, Malaysia. He was awarded the undergraduate scholarship for three consecutive years and won the second prize in the China Student Computer Works Competition in 2019. His research interests include soft computing, machine learning, and intelligent systems. He can be contacted via email: zijie0625@student.usm.my.






Mahmood A. Al-Shareeda    obtained his Ph.D. in Advanced Computer Network from University Sains Malaysia (USM). He is currently a postdoctoral fellowship at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include network monitoring, internet of things (IoT), vehicular Ad hoc network (VANET) security, and IPv6 security. He can be contacted at email: alshareeda022@usm.my.






Murtaja Ali Saare    is an assistant professor at the Department of Computer Technology Engineering, Shatt Al-Arab University College, Iraq. He received his master's degree in information technology at Universiti Utara Malaysia (UUM), in 2017. He completed his Ph.D. at School of Computing, Sintok, UUM, Kedah, Malaysia, in 2021. His research interest includes aging and cognition, e-health, and human-centered computing. He has published his research work in reputable scopus indexed journal. He can be contacted at email: mmurtaja88@gmail.com and murtaja.a.sari@sa-uc.edu.iq.



Selvakumar Manickam    is currently working as an associate professor at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include cybersecurity, internet of things, industry 4.0, and machine learning. He has authored and co-authored more than 160 articles in journals, conference proceedings, and book reviews and graduated 13 PhDs. He has 10 years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile, and web-based applications. He can be contacted at email: selva@usm.my.



Shankar Karuppayah    is received the B.Sc. degree (Hons.) in computer science from Universiti Sains Malaysia, in 2009, the M.Sc. degree in software systems engineering from the King Mongkut's University of Technology North Bangkok (KMUTNB), in 2011, and the Ph.D. degree from TU Darmstadt with his dissertation titled advanced monitoring in P2P Botnets, in 2016. He has been a senior researcher/a postdoctoral researcher with the Telecooperation Group, TU Darmstadt, since July 2019. He has also been a senior lecturer at the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, since 2016. He is currently working actively on several cybersecurity projects and working groups, e.g., the National Research Center for Applied Cybersecurity (ATHENE), formerly known as the Center for Research in Security and Privacy (CRISP). He can be contacted at email: kshankar@usm.my.