INTERNATIONAL JOURNAL
ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Wireless Sensor Network Based Monitoring System: Implementation, Constraints, and Solution

Apip Miptahudin [a,*], Titiek Suryani [a], Wirawan Wirawan [a]

[a] *Electrical Engineering, Institute of Sepuluh Nopember Technology, Surabaya, Indonesia*
*Corresponding author: *apip.207022@mhs.its.ac.id*

***Abstract*— Wireless Sensor Network (WSN) is a collection of sensors communicating at close range by forming a wireless-based network (wireless). Since 2015 research related to the use of WSN in various health, agriculture, security industry, and other fields has continued to grow. One interesting research case is the use of WSN for the monitoring process by collecting data using sensors placed and distributed in locations based on a wireless system. Sensors with low power, multifunction, supported by a combination of wireless network, microcontroller, memory, operating system, radio communication, and energy source in the form of an integrated battery enable a monitoring process of the monitoring area to run properly. The implementation of the wireless sensor network includes five main parts, namely sender, receiver, wireless transmission media, data/information, network architecture/configuration, and network management. Network management itself includes network configuration management, network performance management, network failure management, network security management, and network financing management. The main obstacles in implementing a wireless sensor network include three things: an effective and efficient data sending/receiving process, limited and easily depleted sensor energy/power, network security, and data security that is vulnerable to eavesdropping and destruction. This paper presents a taxonomy related to the constraints in implementing Wireless Sensor Networks. This paper also presents solutions from existing studies related to the constraints of implementing the WSN. Furthermore, from the results of the taxonomy mapping of these constraints, new gaps were identified related to developing existing research to produce better solutions.**

***Keywords*— Wireless sensor network; taxonomy; configuration; energy; network security; optimization.**

Manuscript received 14 Jan. 2022; revised 20 Jul. 2022; accepted 25 Aug. 2022. Date of publication 31 Dec. 2022.

I. Introduction

Wireless Sensor Network (WSN) is a collection of sensors that communicate with each other at close range by forming a wireless (wireless) based network [1]. Since 2015 research related to the use of WSN in various fields of health, agriculture, security industry, and other fields has continued to grow. One interesting research case is the use of WSN for the monitoring process by collecting data using sensors that are placed and distributed in locations based on a wireless system. Sensors with low power and multifunction, supported by a combination of wireless networks, microcontrollers, memory, operating systems, radio communications, and energy sources in the form of batteries in an integrated manner allow a monitoring process of the monitoring area to run properly.

The process of implementing WSN in this monitoring system is not easy. There are at least three problems that are challenges in the WSN system, namely [1]:

- This communication system between sensors has a low/short communication range,
- Availability of limited supply of energy resources/batteries,
- Security systems that are vulnerable to data security attacks.

These problems are interesting to be raised in research to find the best solution so that the WSN-based monitoring system can be implemented optimally. The first problem is closely related to topology design and/or network architecture to build communication between sensors in sending/transmitting data so that the process can be effective and optimal.

The second problem is closely related to recharging the battery from the sensor, making it possible to recharge it so that the sensor's working time becomes longer. Another thing related to these two problems is the development of routing algorithms in collecting data from sensors and recharging the battery on the sensor.

The third problem is related to the development of a network security system to detect, contain and counter moans from hackers, both attacks on the system and attacks on their own data/information. The analysis will be carried out with a focus on the three problems that often occur in the implementation of the wireless sensor network, complete with existing solutions that already exist and are being developed in previous studies.

The rest of this paper is structured as section 2 describes the taxonomy of the scope of the discussion based on the constraints in implementing wireless sensor networks. Section 3 focuses on explaining the topology and configuration of wireless sensor networks. Section 4 describes energy and energy sensor charging systems in wireless sensor networks. Section 5 focuses on explaining the system's wireless sensor network security. Section 6 analyses the remaining solution gaps. Finally, the conclusion is provided in the last section.

II. Materials and Method

The implementation of a wireless sensor network includes five main parts: sender, receiver, wireless transmission media, data/information, network architecture/configuration, and network management [2]. Network management includes network configuration management, performance management, failure management, security management, and financing management [3].

The main obstacles in implementing a wireless sensor network include three things: an effective and efficient data sending/receiving process, limited and easily depleted sensor energy/power, network security, and data security that is vulnerable to eavesdropping and destruction [1]. Network configuration describes the arrangement scheme and relationship between sensors/nodes in a network, and the configuration also describes how the network is formed and maintained by considering the software and hardware aspects.

The arrangement and communication pattern are represented and largely determined by the WSN topology to be used. The software aspects of the WSN configuration include network protocols, signaling, and applications and algorithms that support WSN continuity and management. Hardware aspects include routers, channels, nodes/ sensors, switches, agents, and other supporting hardware with their functions and operations [4]. Research on the WSN configuration section includes several aspects, including related topics [5]–[13]:

- Topology
- Routing
- Channels
- Number of Nodes
- Number of Agents
- Geographical Conditions
- Communication Pattern
- Wave Propagation
- Computing System

Sensor energy is a resource and the amount of power consumption required by the sensor for standby, the sensing process, and the process of sending data from the sensor to the coordination center. The core discussion of the energy/power sensor includes energy consumption, energy-saving, sensor lifetime, sensor work schemes based on energy consumption, sensor battery charging techniques, smart batteries, and battery materials.

Research related to constraints on the energy sensor section of the WSN includes [14]–[19]:

- Energy Saving
- Battery Material
- Sensor power system design
- Sensor battery charging technique
- Sensor battery lifetime
- Smart battery

The network security system is the defense capability of the network in securing the network, both physical and data, from external attacks.

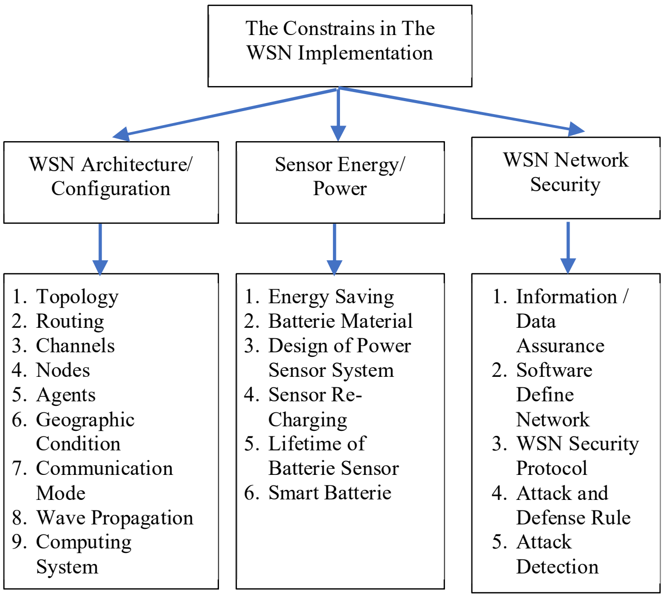

Fig.1 Taxonomy of Constraints in WSN Implementation

The WSN security system includes physical network system security, security defense systems, data, and information security, attack detection, and attack patterns. Research related to security system constraints in WSN includes several aspects, including [20]–[24]:

- Information/Data Guarantee
- Software define network
- WSN security protocol
- Attack pattern and Defense pattern
- Attack Detection

Figure 1 shows a taxonomy of constraints in implementing Wireless Sensor Networks.

III. Results and Discussion

A. *Wireless Sensor Network Configuration*

Determination of the appropriate topology for WSN needs to be planned by the objectives and designations of the WSN development itself. This is very important to ensure the reliability and energy conservation of WSN. Literature review shows that various types of topologies for WSN have been used, namely underground topology and hybrid topology [1], linear topology [2], mesh network topology and peer-to-peer topology [2], star topology [2], and tree topology [2]. A different topology is proposed because obstructions in the field/real world can limit or prevent communication between multiple nodes.

For a star topology, the coordinator (sink node) in Figure 2(a) acts as a network controller, and other devices are called "sensors/nodes". Sensors/nodes do not communicate directly with each other but operate independently. More importantly, they are not affected by other sensors/nodes when these devices are not operating.

When the star topology is active, the sensor/node communicates directly with the coordinator (sink node). In addition, sensors/nodes can be switched to standby mode or sleep mode to reduce power consumption and extend the operating time of sensor nodes. Since the sensors/nodes do not communicate via the router to the coordinator, the further the distance between the sensors/nodes and the coordinator, the more energy is spent.

Regarding the tree topology in Figure 2(b), the network consists of one coordinator, several routers, and sensors/nodes. The coordinator manages the network, selects the operating channel, and assigns addresses for routers and sensors/nodes.

The router communicates directly with the coordinator. In tree topology, routers transfer data from sensors/nodes to coordinators. Therefore, routers are always on, which consumes energy. However, the distance from the sensor/node to the router is shorter than the sensor/node to the star topology coordinator (Figure 2), so it consumes less energy than the star topology.

In terms of network formation, two general classifications of WSN formation techniques are used in research, namely centralized and distributed [2]. In the use of coordinators/sinks, existing research uses single sinks and multi sinks, where these two variations of sinks can be implemented in each type of network, including Hierarchical Networks, Defined Operational Networks, Static Networks, Application-based Networks, and Topology-based Networks.

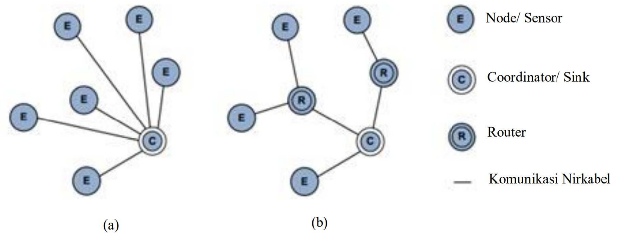

Fig. 2 Example of a Wireless Sensor Network Topology

In terms of routing, existing research discusses routing patterns in WSN by developing routing algorithms and coding protocols. One of them is the CORS (coding-aware opportunity routing) method for WSN-based underwater monitoring systems. The output is a better network performance than the hop-type and pressure-type protocols. The parameters compared are data transmission, latency, and energy consumption [3].

Other researchers developed the GCOR (Geographic and Cooperative Opportunistic Routing) Protocol to normalize Packet Data Probability (PDP) Energy and Distance [4]. In addition, variations in the number of nodes used, the number of agents that pick up data, and different scenarios of geographical conditions are also investigated in this research related to WSN [3]–[5]. Other important protocols developed related to the authentication process protocol at the time of access to the system. This was developed with the increasing frequency of drones/UAVs being used as intermediary media for data collection from sensors/nodes and battery chargers for sensors/nodes [5].

In this study, the issue of network security is also discussed. Another protocol developed is the coverage protocol. This research is intended to calculate the optimal/maximum sensor coverage in the field. This is related to the sensing of energy consumption, the connection model, and the location of the sensor placement [25].

In terms of estimating the use of channels in the WSN, many studies have developed algorithms and computing systems to calculate and determine the optimal channel estimates used [6]. Other researchers developed DSME (deterministic and synchronous multichannel extension) to improve throughput and delay [7]. Wang et al. [8] conducted a comparative analysis of channel modeling for industrial IoT wireless communication in free space loss, single slope, 3GPP model, and industrial indoor channel model. Another researcher, Mahbub [12] compared the channel model attenuation factor and log-normal shadowing path loss on four parameters: signal strength, packet loss, error, and delay. Caso performed empirical modeling for Narrow Band-IoT Path Loss technology with two models, Alpha-Beta-Gamma (ABG) and Close-In Model (CI) [9].

B. Sensor Energy in WSN

The main problem in terms of energy sensors in the Wireless Sensor Network (WSN) system is that the energy source is limited. The sensor battery has a limited life depending on the energy released during standby, the sensing process, and sending data to the center. Many researchers are developing algorithms and modeling so that sensors use energy efficiently according to their designation. The problem of battery/energy sensor limitations can be resolved if technology allows for recharging the energy sensor [1]. Although it is still in the simulation stage, Huang and Clerckx [11] developed a multi sine wave propagation model with one antenna to transmit energy with a wireless power transfer system. This spurred other researchers to design architectures using multi-antenna-multi sinusoidal. This research has only succeeded in increasing the harvested DC energy. Waveform design is a key technique for utilizing beamforming gain, channel frequency selectivity jointly, and nonlinear rectification to increase the efficiency of end-to-end power transfer from Wireless Power Transfer (WPT) [10]. Huang and Clerckx [11] continued their study using multi-antenna-multi sine and limited feedback (1 bit).

The harvested energy is higher than in the previous model. Implementing the WSN system in the monitoring system for the distribution of electrical energy in China has begun to be implemented by ensuring the energy supply to the sensor. The energy source is prepared near the sensor and the sensor technology is low energy consumption [14]. Chen et al [15] developed drones to recharge the sensor battery while also preparing a pad for charging the drone if it does not make it to the next stop. This drone's refill stage is still in the simulation stage [15]. Khisa and Moh [16] researched the design of energy-efficient routing protocols to provide efficient packet routing from source to destination. Qian et al. [17] simulate an optimization design for recharging the sensor battery by a drone introducing a new algorithm, namely black holes, with a 35% improvement in processing speed from the existing algorithm (art genetic).

Hu et al. [18] simulation in the process of collecting data from sensors using several flying ferries with routes based on an alternative genetic-based algorithm from the traveling salesman problem (TSP) algorithm. The performance results show that the proposed scheme outperforms some typical schemes, including Native, K Means, and Spiral, in calculating cumulative energy, distribution of residual energy, and fairness index.

William et al. [19] introduced the results of a survey regarding the current state of EH (Energy Harvesting) technology for small-scale WSNs in terms of EH methods, energy storage technologies, and EH system architectures. It aims to combine methods and storage, including multi-source architecture and multi-storage, as well as to highlight several other optimization considerations. Li et al. [20] simulated how to obtain energy harvesting wirelessly by setting up a relay-based two-hop communication system by setting Half-duplex (RF energy harvesting) and full-duplex (information transmission phase).

C. WSN Security Systems

WSN systems are quite vulnerable to external attacks. The attack pattern usually attacks the network system physically and non-physically, attacks and intercepts data and information, and breaks into the defense system. There are five wireless sensor network (WSN) systems, namely 5 (five) types of wireless sensor networks, including Terrestrial WSNs, Underground WSNs, Underwater WSNs, Multimedia WSNs, and Mobile WSNs.

Hsiao and Sung [21], in the study on security on WSN proposed an approach that uses blockchain-based technology to strengthen the data security of wireless sensor networks (WSN). The study integrates blockchain-based technology with data transfer to build a highly secure WSN structure. Meanwhile, Liu and Wu [22] conducted research to withstand attacks related to fragments of data packet delivery on nodes that are vulnerable to security. Research developed a combined scheme to detect selective forwarding attacks in wireless sensor networks (WSN) under chaotic (HARS) environments. This scheme uses a data clustering algorithm (DCA-Data Clustering Algorithm) to screen for "bad/dangerous" nodes by grouping their cumulative forwarding rates (CFR-Cumulative Forwarding Rates) and design a decision-making method to protect nodes under these hazardous environments from being judged as malicious nodes.

Al-Naeem [23] conducted a study to predict DDoS attacks with transmission behavior variability to obtain high accuracy. This study's pattern of security attacks is in the form of fake ACKs, which deceive the target node, where the delivery is considered successful but failed.

Alturki et al. [24] studied the importance of securing the sensor-cloud architecture from various security attacks to maintain its integrity. The main components of a sensor-cloud architecture that can be attacked are:

- Sensor nodes.
- Communication media; and
- remote cloud architecture.

Zafar et al. [26] conducted research on interface design based on nanotechnology (RFID, Chip Implants, etc.) to prevent attacks through cyber networks.

D. Next Research Gap Analysis

1) Network Configuration:

The network topology used determines the speed of data transmission from the sensor and the sensor's energy consumption. The previous research discussed the advantages and disadvantages of each topology that has been simulated in a wireless sensor network (WSN). For example, the star topology in the WSN allows short routing, and even direct transmits so that data transmission can be faster (small delay), but the energy consumption of transmission from the sensor is relatively wasteful and large. This happens the other way around in a tree topology.

The quality and speed of data transfer and energy consumption are also influenced by the location and number of sensors/nodes covered in the field. Another thing that determines the quality of WSN implementation is the use of protocols, where the protocol used from existing studies affects the routing pattern, packet data probability, energy, and distance. In addition, the authentication protocol is also very influential on the speed of the process and the system's security.

Determining the channel model in the WSN is also very influential on the signal reception strength, delivery speed, transmission error, delivery delay, and energy consumption. There is no channel model in WSN that is superior in all parameters of WSN quality.

The flexibility of using the topology in the field with adjustments to geographical conditions and network quality parameters is an interesting thing to study and research. Likewise, the selection of protocols and channel modeling is interesting to develop. Auto-configuration of WSN by taking into account aspects of topology, software/protocol, channel model, routing, number of nodes, and geographical conditions.

Developing the WSN reconfiguration algorithm from the initial configuration to the configuration that auto-adapts to the specified parameter criteria becomes a novel aspect in subsequent studies. In addition, the optimization model by combining the two

The object (hybrid model) that affects the quality of WSN is the next novelty gap, such as optimizing a model that produces a fast process but wastes energy with a model that saves energy but has a little delay. Optimization is done in terms of processing time and energy consumption.

2) Energy Sensor on WSN:

Sensor energy is crucial in the WSN system because sensors are vital for collecting field data. The sensor operating time determines the overall network operating time (network life). The problem of limited energy has been initiated and thought about for a solution by existing studies, ranging from the efficiency of use, battery recharging process, recharging routine algorithms by unmanned aircraft (drone/ ferry/ UAV), and scheduling. Another solution that already exists in existing research is setting up a communication system with two hops for mining energy from radio frequencies. In the problem of energy sensors in WSN, the gap for further research that can still be done as a novelty in this field is still wide open.

The research conducted so far is still in the simulation stage and has not yet been implemented. At this simulation stage, for example, the problem of the routing algorithm for charging the sensor battery is still using one drone one route. This is done by examining the optimization of the use of multi drones and multi-routing.

Other issues that will arise regarding routing overhead, link stability, security, and privacy, can be raised in the new research. The development of algorithms to improve the operating efficiency of electric delivery vehicles (drones/UAVs) is a challenge due to the complex dynamic environment and the need to solve difficult optimization problems to determine the best combination of routes, several vehicles, and various safety thresholds before use. This could also be the next research gap. In the new research, the scheduling system for charging energy sensors simulates one drone and two drones with one and two routes; what if, for example, using multi-agents and multiple routes. Research that has not yet been carried out is also related to the composition and components of battery materials for sensors that can last a long time. The addition of a power bank in the configuration around the sensor where the battery charging process is sufficient on the power bank and this power bank will distribute it to the sensors.

3) Security System on WSN:

The security system on the wireless sensor network (WSN) was developed based on the attack pattern: Security on sensor nodes, security on wireless communication channels, and data security on cloud platforms. Security on wireless communication channels, which includes security of data collection on sensor nodes and security of data transmission on the channel.

Type of attack at the time of data collection from sensors:

- device tempering attacks
- eavesdropping
- jamming attacks
- denial of service (DoS) attacks

Type of attack during data transmission on the channel

- false routing
- packet replication
- man, the middle attacks
- black hole attacks
- sinkhole attacks
- wormhole attacks
- Selective packet forwarding
- spoofed routing information
- acknowledgment spoofing
- node replication attacks
- passive information gathering
- Sybil attacks

Data security on cloud platforms are divided into three parts. They are types of attacks on SaaS platforms, types of attacks on the PaaS platform, and types of attacks on IaaS flat platforms.

Types of attacks on SaaS platforms

- denial of service (DoS) attacks
- distributed denial of service (DDoS) attacks
- SQL injection attacks
- Cross-site scripting

Types of attacks on the PaaS platform

- phishing attacks
- man in the middle attack
- cloud malware
- password reset
- programming flaws
- application security
- software interruptions.

Types of attacks on IaaS flat platforms

- steppingstone
- virtual machine escape
- side-channel attacks
- malicious insiders
- programming attacks
- VM rollback attacks
- cross VM attacks
- virtual cloud protection
- session hijacking
- traffic flow analysis
- defacement
- connection flooding
- DDoS
- Theft-of-Service attacks

Further research gaps regarding physical security or through the use of authorization and authentication techniques. Communication systems between sensors can also be secured using the enrichment of certain security protocols. Algorithms for Early detection attacks can be developed using Software Define Network (SDN). The development of cryptographic-based data encryption techniques can also be investigated further to ensure the security of information/data.

IV. Conclusion

The implementation of WSN in various fields faces obstacles that are not easy to overcome, thus requiring further research, especially for solutions to the following constraints: configuration optimization, energy-saving, and network security. Each constraint leaves a gap for further research to produce new solutions that are better than the existing results. Problems that can be investigated further include the routing process for data collection and charging sensor battery energy which is still not optimal. The proposed new solution that can improve and solve the problem is the proposal of a new routing algorithm using more than one UAV agent so that the data collection process becomes faster, and the time required by the UAV in the process of collecting data and charging energy to the sensor becomes shorter. This results in more efficient energy consumption. This research needs to be done because the research that has been done only uses a single UAV and a single track. By using multiple agents and modeling algorithms for multiple paths, it is hoped that better energy efficiency can be achieved because the processing time is faster and shorter.

References

[1] C. G. Thuy, "Flexible configuration of wireless sensor network for monitoring of rainfall-induced landslide," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, no. 3, pp. 1030–1036, 2018.

[2] M. Carlos-Mancilla, E. López-Mellado, and M. Siller, "Wireless sensor networks formation: approaches and techniques," *J. Sensors*, vol. 2016, 2016.

[3] D. Zhao, G. Lun, and R. Xue, "Coding-aware opportunistic routing for sparse underwater wireless sensor networks," *IEEE Access*, vol. 9, pp. 50170–50187, 2021.

[4] S. Karim *et al.*, "Corrections to 'GCORP: Geographic and Cooperative Opportunistic Routing Protocol for Underwater Sensor Networks,'" *IEEE Access*, vol. 9, pp. 67734–67735, 2021.

[5] U. C. Cabuk, G. Dalkilic, and O. Dagdeviren, "CoMAD: Context-aware mutual authentication protocol for drone networks," *IEEE Access*, vol. 9, pp. 78400–78414, 2021.

[6] S.-W. Lee, J.-H. Kwon, X. Zhang, and E.-J. Kim, "Traffic-Adaptive CFP Extension for IEEE 802.15. 4 DSME MAC in Industrial Wireless Sensor Networks," *IEEE Access*, vol. 9, pp. 94454–94469, 2021.

[7] R. Elhabyan, W. Shi, and M. St-Hilaire, "Coverage protocols for wireless sensor networks: Review and future directions," *J. Commun. Networks*, vol. 21, no. 1, pp. 45–60, 2019.

[8] W. Wang, S. L. Capitaneanu, D. Marinca, and E.-S. Lohan, "Comparative analysis of channel models for industrial IoT wireless communication," *IEEE Access*, vol. 7, pp. 91627–91640, 2019.

[9] G. Caso, Ö. Alay, L. De Nardis, A. Brunstrom, M. Neri, and M.-G. Di Benedetto, "Empirical models for NB-IoT path loss in an urban scenario," *IEEE Internet Things J.*, vol. 8, no. 17, pp. 13774–13788, 2021.

[10] B. Clerckx and E. Bayguzina, "Waveform design for wireless power transfer," *IEEE Trans. Signal Process.*, vol. 64, no. 23, pp. 6313–6328, 2016.

[11] Y. Huang and B. Clerckx, "Waveform design for wireless power transfer with limited feedback," *IEEE Trans. Wirel. Commun.*, vol. 17, no. 1, pp. 415–429, 2017.

[12] M. Mahbub, "Comparative link-level analysis and performance estimation of channel models for IIoT (industrial-IoT) wireless communications," *Internet of things*, vol. 12, p. 100315, 2020.

[13] J. D. Rodríguez, A. Pérez, and J. A. Lozano, "Sensitivity Analysis of k-Fold Cross Validation in Prediction Error Estimation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 3, 2010, doi: 10.1109/TPAMI.2009.187.

[14] J. Liu, Z. Zhao, J. Ji, and M. Hu, "Research and application of wireless sensor network technology in power transmission and distribution system," *Intell. Converg. Networks*, vol. 1, no. 2, pp. 199–220, 2020.

[15] J. Chen, C. W. Yu, and W. Ouyang, "Efficient wireless charging pad deployment in wireless rechargeable sensor networks," *IEEE Access*, vol. 8, pp. 39056–39077, 2020.

[16] S. Khisa and S. Moh, "Survey on recent advancements in energy-efficient routing protocols for underwater wireless sensor networks," *IEEE Access*, vol. 9, pp. 55045–55062, 2021.

[17] Q. Qian, A. Y. S. Pandiyan, and D. E. Boyle, "Optimal recharge scheduler for drone-to-sensor wireless power transfer," *IEEE Access*, vol. 9, pp. 59301–59312, 2021.

[18] C.-L. Hu, S.-Z. Huang, Z. Zhang, and L. Hui, "Energy-Balanced Optimization on Flying Ferry Placement for Data Gathering in Wireless Sensor Networks," *IEEE Access*, vol. 9, pp. 70906–70923, 2021.

[19] A. J. Williams, M. F. Torquato, I. M. Cameron, A. A. Fahmy, and J. Sienz, "Survey of energy harvesting technologies for wireless sensor networks," *IEEE Access*, vol. 9, pp. 77493–77510, 2021.

[20] J. Li, F. Safaei, and others, "Throughput analysis of in-band full-duplex transmission networks with wireless energy harvesting enabled sources," *IEEE Access*, vol. 9, pp. 74989–75002, 2021.

[21] S.-J. Hsiao and W.-T. Sung, "Employing blockchain technology to strengthen security of wireless sensor networks," *IEEE Access*, vol. 9, pp. 72326–72341, 2021.

[22] Y. Liu and Y. Wu, "Employ DBSCAN and neighbor voting to screen selective forwarding attack under variable environment in event-driven wireless sensor networks," *IEEE Access*, vol. 9, pp. 77090–77105, 2021.

[23] M. A. Al-Naeem, "Prediction of Re-Occurrences of Spoofed ACK Packets Sent to Deflate a Target Wireless Sensor Network Node by DDOS," *IEEE Access*, vol. 9, pp. 87070–87078, 2021.

[24] R. Alturki *et al.*, "Sensor-cloud architecture: A taxonomy of security issues in cloud-assisted sensor networks," *IEEE Access*, vol. 9, pp. 89344–89359, 2021.

[25] A. M. Wilson, T. Panigrahi, B. P. Mishra, and S. L. Sabat, "Adaptive Geman-McClure estimator for robust distributed channel estimation," *IEEE Access*, vol. 9, pp. 93691–93702, 2021.

[26] S. Zafar *et al.*, "A systematic review of bio-cyber interface technologies and security issues for internet of bio-nano things," *IEEE Access*, 2021.