

A Lightweight Wireless Sensor Protocol for Power and Computational Efficiency

Matt Bowden

Computer Science and Engineering, Australian National University, Australia.
mat.den@outlook.com

Article Info

Journal of Computer and Communication Networks
<https://www.ansispublications.com/journals/jccn/jccn.html>

Received 18 April 2025
Revised from 30 July 2025
Accepted 23 August 2025
Available online 28 September 2025

© The Author(s), 2025.

<https://doi.org/10.64026/JCCN/2025019>

Published by Ansis Publications

Corresponding author(s):

Matt Bowden, Computer Science and Engineering, Australian National University, Australia.
Email: mat.den@outlook.com

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract – In this article, Simple Wireless Sensor Protocol (SWSP) has been introduced as an efficient and new protocol meant for Wireless Sensor Networks (WSNs). TCP/IP is a non-specialized set of protocols, while SWSP is developed specifically for WSNs, which, due to the limited capabilities of their nodes and their purpose of being used only for specific applications, are distinguished from general-purpose networks. The present work provides an analysis of the concern regarding the formation of WSNs with a focus on how to address the constraint due to the power, storage, processing, and computation capability of the sensor nodes. Accordingly, this work defines the SWSP based on the synthesis of literature and findings of previous researches. Sub-topics such as semantics of SWSP protocol, design of the protocol, and implementation issues are discussed in more detail. Several performance evaluations are demonstrated to illustrate that the protocol is applicable to diversified network environments and to estimate the capability of decreasing the power consumption and enhancing the performance of networks. We also analyze the impact of the SWSP protocol on the header overhead, latency, control packet overhead, and the network throughput, which is useful in understanding more about the relevance of the protocol. The findings of this study underscore the need to incorporate SWSP for constructing accurate and efficient WSNs with more advancements in several segments such as health care systems, military security, and the environment.

Keywords – Simple Wireless Sensor Protocol (SWSP), Wireless Sensor Networks (WSNs), Quality of Service (QoS), Model-Driven Engineering (MDE), Modelling and Analysis of Real Time and Embedded Systems (MARTE).

I. INTRODUCTION

Wireless Sensor Network (WSN) has emerged as one of the critical research areas in recent past because of the growing demand and use of this technology. This is mainly due to the fact that sensor networks hold immense potential in providing application interfaces that can link the physical and the virtual worlds. If several tiny sensor nodes are integrated into a single network, it becomes feasible to acquire data on the physical surroundings, which was incredibly challenging, if not wholly unattainable. In the future, as advanced micro-fabrication techniques are used to have cheaper sensors, it is expected that WSNs will be incorporated. These networks are expected to grow and become larger, and some may include thousands of nodes. However, the application of such large WSNs can be seen in a number of sectors like medical surveillance [1], environmental surveillance [2], security, home security and monitoring, military use and manufacturing machine surveillance.

An end-user can get informed about the environments through the help of surveillance applications that are developed on sensor networks. As in the case of any network, the traffic patterns in a sensor network include multiple sources that transmit information to a single destination. The data being transmitted might vary from raw sensor data to a detailed explanation of the events happening in the ecosystem, provided that data dispensation is performed locally. The sensor network will be subject to certain quality of service (QoS) requirements imposed by the application. For example, there may be requirements for the minimum percentage of sensor coverage in a predicted phenomenon's area or the maximum probability of missing an event. Simultaneously, the model is anticipated to sustain this level of service over an extended period (months or even years) by utilizing the network's limited asserts (such as sensor energy and channel bandwidth) with

minimal or no external intervention. Achieving these objectives necessitates meticulous planning of both the network protocols and the sensor hardware.

Pawgasame [3] examined a hybrid WSN that included both mobile and stationary nodes. Static sensors are used to monitor the surrounding ecosystem and provide information about events happening in the area they cover. The mobile sensors' travelling pathways were scheduled in an energy-composed manner to maximise their general lifetime. It has been demonstrated that this is a problem that falls within the category of NP-complete. The researchers suggested both a centralised and a distributed approach to develop heuristics for scheduling the travelling patterns of mobile sensors. Their heuristics incorporated the ability to accommodate any number of event locations and mobile sensors in each round, while also prioritising energy balance. The centralised heuristic aims to minimise the energy expended by mobile sensors during movement, while also maintaining a balanced energy consumption among them. Deif and Gadallah [4] introduced a novel probabilistic coverage technique (referred to as Probabilistic Coverage Protocol) that took into account probabilistic sensing models. Probabilistic Coverage Protocol (PCP) was widely applicable and utilised with many sensor models. Specifically, PCP necessitated the calculation of a solitary parameter based on the chosen sensing model, while all other factors remained same. Kumar and Lobiyal [5] demonstrated the basic derivation of this parameter, as well as the computations for two specific sensing models: (i) the widely-used deterministic disc sensing model and (ii) the probabilistic exponential sensing model. The researchers examined their procedure with two current protocols and asserted that their suggested technique demonstrated superior performance.

Bhattacharyya, Kim, and Pal [6] introduced a robust and effective routing technique designed specifically for WSNs. They asserted a reduction of over 90% in the number of transmissions contrasted to the message flooding technique when utilising the same channel for transmitting data messages. The savings grew dramatically as the transmissions number augmented over the same path. The protocol was extremely lightweight to deploy in WSNs since it only used up 16% of the RAM that was available and 12% of the programme memory in the MICAz platform. Section II provides a review of wireless sensor network system design. In Section III, a discussion of the SNSP has been provided, and its analysis and performance has been provided in Section IV. Section V provides a critical discussion of energy efficiency, reliability and failure recovery, throughput and latency, packet overhead, and scalability in regard to SWSP. Lastly, Section VI provides a summary to the research.

II. WIRELESS SENSOR NETWORK SYSTEM DESIGN

The primary obstacles in the development of a WSN are the constraints on dispensation, storage, power, and computational capabilities of the detector. Within this sector, we will outline the wireless detector and WSN structures for our structure, as they are closely connected to the design of the model protocol. Our structure design collects findings from previous research studies [7, 8, 9, 10] conducted in this field. While [11] and [12] provide a hardware-oriented perspective, [13] offers a topological approach to system design.

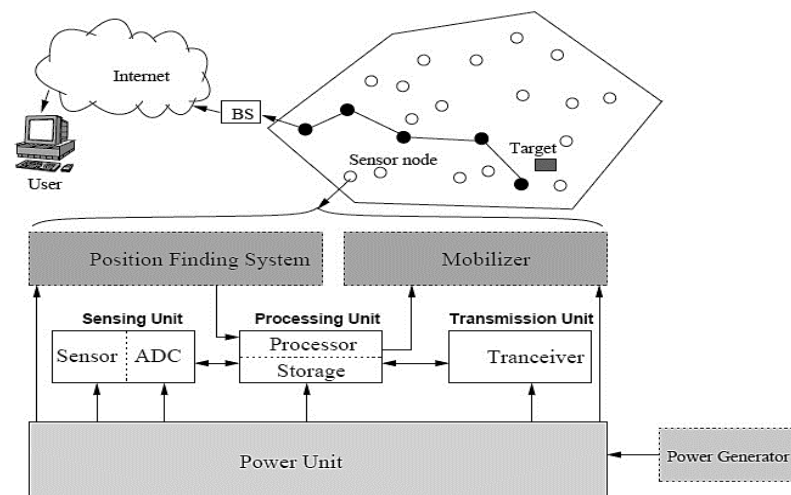


Fig 1. The Elements of a Sensor Node.

A sensor node comprises four fundamental elements: a power unit, a processing unit, a sensing unit, and a transceiver unit, as showed in **Fig. 1**. Furthermore, it includes utilization-specific supplementary elements like a mobilizer, a power generator, and a positioning system. In most cases, analogue to digital converters (ADCs) and sensors make up a sensing unit [14]. It can be seen that the sensors yield analogue indicators that are then transformed by an ADC into digital indicators which are then sent to the central processor. The central processor is often connected to a miniature storage device and has the capacity to monitor the tasks that will allow the mote to interact with other nodes in order to accomplish the specific sensing responsibilities.

A transceiver unit is a device that enables a node to communicate within the network. The power unit is considered as one of the most significant elements in the mote. In addition to power units, a power scavenging device for instance solar

cells can also be employed. The other components of the node are dependent on the application of the node system. **Fig. 2** illustrates a schematic representation of a versatile wireless sensor node. The furniture design is modular which is flexible and can accommodate all the needs required in the various applications. Depending on which sensors are to be used in the design, this can be changed or modified using the signal conditioning block. This makes it possible to incorporate a large number of varieties of sensors with the wireless sensing node. Likewise, the radio link may be modified as desired based on the wireless span needed in a given application and whether or not voice intercom is needed. WSNs have been regarded as the key component in numerous utilizations including ecosystem monitoring [15], military scrutiny [16], and medicine [17].

They enable the interaction, reliable inspection, and the completion of many tasks. WSNs consist of large sum of motes that are often deployed in a dense manner and communicate with each other over the wireless media to exchange information regarding the environment. Every mote is prepared with at least one or more sensors, a power supply subsystem, a wireless transceiver, and a microprocessor. Designing WSNs is always a challenging task because of the complex nature of these systems. Moreover, there are several important requirements that have to be considered when designing a WSNs: the fundamental condition is to consume as less power as possible. As a result, many ongoing researches focus on the analysis of WSNs.

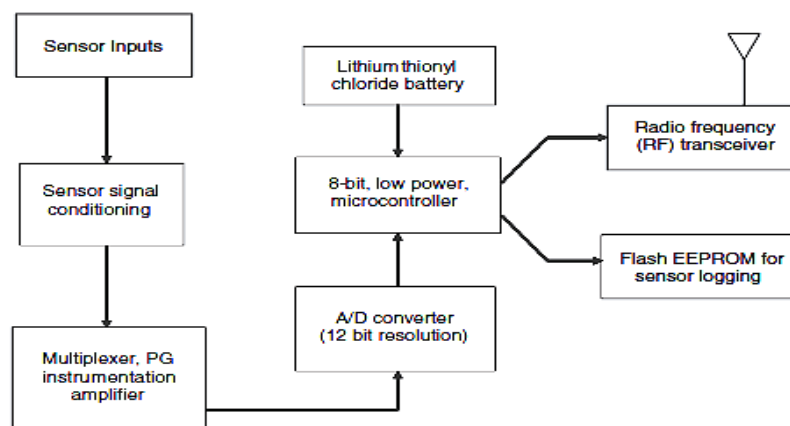


Fig 2. A Sensor Node's Functional Block Diagram.

Bhushan and Sahoo [18] have elaborately described the various generations, routing protocols, architectural framework, and storage management systems of WSNs. Akkaya and Younis [19] offer a detailed description of the existing routing protocols being implemented in the setting of the detector models. In their study, the authors presented a number of existing middleware approaches for sensor networks. In their work, the authors presented a detailed analysis of the available sensor localization algorithms and the hierarchical classification of such systems, as well as their potential use in different scenarios. The researchers proposed new sensor localization algorithms and elucidated their use and operation for IoT environment. Similarly, Zhou et al. [20] did a review on the gadget-free localization of sensors for the smart environment.

Sharma, Vashisht, and Singh [21] conducted a survey of modelling methodologies for WSNs in [22]. They demonstrated how each technique characterizes the behaviour of individual nodes and the behaviour of the network as a whole. In addition, they also demonstrated the modelling tool for each technique. However, only a limited number of publications have examined and analyzed the primary programming methodologies and modelling techniques that are currently employed in the development of WSN. Inspired by this concept, we conducted an examination that consolidates and deliberates on current approaches for designing Wireless Sensor Networks (WSNs). Heydarishahreza et al. [23] examine low-level-based techniques that concentrate on the application level and high-level-based methods that depend on the model perception for designing WSN structures.

The authors explore the viability and implementation of high-level-based methods to reduce the intricacy of developing WSN structures and enhance their maintainability and portability. Currently, there is significant focus on high-level abstraction design utilizing the Model-Driven Engineering (MDE) approach [24], particularly through the utilization of standard mechanisms like the Modelling and Analysis of Real Time and Embedded Systems (MARTE) [25] design and profile patterns [26]. By representing the WSN structure at higher stages of abstraction, it becomes possible to decrease the complexity of the system while simultaneously enhancing the flexibility and reusability of the frameworks. It also enables mechanization and improves the value of the model. Furthermore, it offers the opportunity to identify faults before to the actual implementation of the network, at the initial design phase.

Somov et al. [27] mention various research studies on the development of WSNs. Wehrmann and Barros [28] commence by introducing low-level-based methodologies to examine the necessity for suitable high-level design techniques. **Fig. 3** depicts the categorization of WSN design methodologies. Nujoom, Mohammed, and Diabat [29] examined a collection of criteria for comparison that are associated with the design ecosystem, performance evaluation, reconfiguration state, and power supply design. This study examines the design of the Simple Wireless Sensor Protocol (SWSP) and compares it to TCP. Next, we proceed to delineate the protocol semantics. TCP is a commonly utilized protocol at the transport layer. The

system excels in its ability to effectively manage network congestion, regulate data flow, and ensure dependable communication. Nevertheless, it also possesses certain disadvantages when applied in wireless networks.

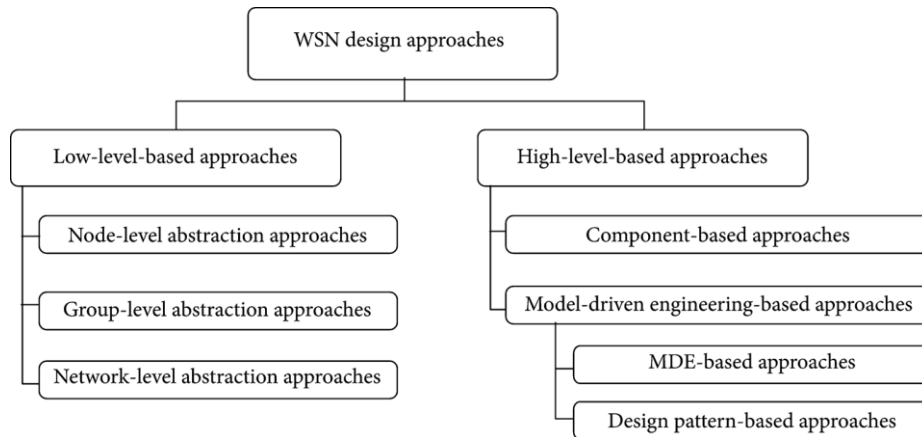


Fig 3. WSN Design Approaches.

III. SWSP: DESIGN AND SEMANTICS

Sensor networks consist of numerous minuscule devices that perform sensing and computing tasks. Each of these units, referred to as motes, possesses extremely restricted communication, computing, and energy resources. These networks are typically found in uncontrolled physical environments and need distributed algorithms to process data efficiently. Additionally, individual motes need to exhibit highly concurrent and reactive behavior in order to operate efficiently. Sensor networks have numerous challenges that are unique to their nature, unlike other types of networks [30]. When designing protocols for sensor systems, it is important to take into account power disadvantages, restricted hardware, reduced reliability, and the often-larger density and number of nodes compared to ordinary networks. Fig. 4 depicts a standard and uncomplicated WSN.

A Simple WSN typically encompasses one or more base gateways, many motes, and the end user. Sensor nodes are utilized for the purpose of quantifying physical attributes such as temperature, location, humidity, pressure, and so forth. The sensor nodes broadcast their output wirelessly to the base station for the purpose of collecting, analyzing, and logging data. End users can remotely access and control the data collected by the sensor through a website or console terminal programmes [31]. Nevertheless, developers prioritize obtaining firsthand knowledge on the feasibility and reflectivity of implementing such networks before proceeding with the hardware implementation, as they are aware of the high costs, time, and complexity connected with implementing these networks.

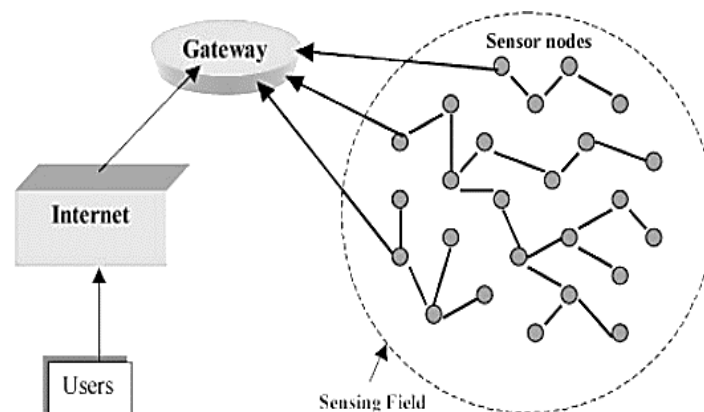


Fig 4. A Simple Wireless Sensor Network.

Without an RR message, a sensor node cannot communicate with the data collecting node, hence it gets unregistered. In this case, a mobile sensor will re-register with the other data-collecting node if it gets an RR message from that node. In order to ensure reliability, an acknowledgement is required for every data packet that is sent. In a typical TCP implementation, a collective acknowledgment is transmitted for a series of segments. Due to the configuration of our structure, where a single data assortment node delivers recognition to numerous sensors, it is possible to consolidate all sensor data into a single acknowledgement packet. By doing this, it will guarantee efficient allocation of available network capacity and minimize the overall computational expense for handling acknowledgements. TCP necessitates the use of retransmission timers for each individual data packet that is transmitted. If a response is not established within the stated time limit, the packet will be sent again. A sensor lacks the ability to maintain a timer for each data segment of every

assortment. In [32], the act of retransmission is substituted with negative recognitions received from the requester. Nevertheless, sensors can also transmit unrequested data to the data assortment site.

Our solution involves the implementation of a relaying counter for every sent data packet, which is responsible for monitoring and managing the retransmission process. The number is incremented upon receiving a group recognition from the data gathering point. If the counter surpasses the retransmission counts, the data will be resent. After covering the fundamental aspects of the protocol, we will now provide a comprehensive description of SWSP. SWSP is a protocol that operates based on events. **Fig. 5** displays the state conversions for the sensor. The sensor can move to six states: disconnecting, connecting, disconnected, connected, wait, requested, ack. The initial state and the last two states pertain to the sensor's ingress and egress into the network. A sensor mostly operates in the second, third, and fourth states. The state conversions are governed by straightforward events that do not necessitate the use of timers or elaborate input/output interactions. Now, we will provide a detailed description of each state and its corresponding protocol characteristics.

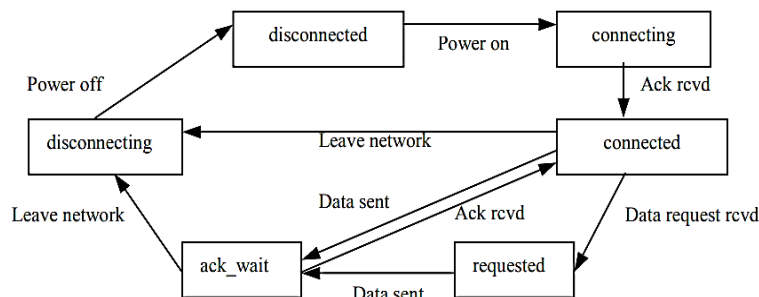


Fig 5. SWSP State Transition Diagram.

An unpowered sensor remains continuously disconnected. When turned on, a sensor moves into the 'connected' state. The device retrieves the application and configuration data that is stored in the integrated circuit. The procedure unit produces a 'register' message and sends it to the model via broadcasting. The radio interface hardware employs the broadcast address for this particular objective. The 'register' message comprises a list of services (utilizations) that it can manage, as well as the MAC address of its hardware border. The previous pertains to a unique and separate identification of the service, as put out by the Simple Wireless Sensor Protocol (SWSP). The latter must be attained from the radio unit. This data is enough for identifying the gadget and its facilities. To ensure exclusive recognition of the 'register' message by a single data collecting node, it is imperative to synchronize the receiving nodes. In the event that the 'register' message does not get an acknowledgement following the receipt of an RR message, it will be delivered again. After receiving confirmation, the sensor switches to the 'linked' state.

The recognition assigns a distinct identify to the detector, which remains unchanged all over its interaction with the data assortment node. A detector in a 'linked' state possesses the capacity to either send data automatically or remain idle until a request is received from the data assortment node. Secondly, when data is requested, the sensor goes into a "requested" state and starts collecting data, which it then delivers to the data collecting node. After the information is broadcast, the detector goes into the 'ack_wait' phase, where it stays in a state of waiting until it receives the acknowledgement. So as to decrease the message exchanges` number, we utilize piggybacking to incorporate data acknowledgements within RR messages. If the acknowledgment is not received within the specified timeframe of 3 RR messages, the data will be resent. The SWSP system can concurrently process up to 2 pending acknowledgements. This is because there are a limited buffer capacity and a decreased requirement for retaining state information.

Due to the fact that sensors have a low duty cycle, it requires a substantial amount of energy to process multiple connection states simultaneously. A sensor possesses the capability to independently disengage itself from the model by transmitting a 'disconnect' message and transitioning into a 'disconnecting' state. Alternatively, it could be disengaged using the methods defined previously.

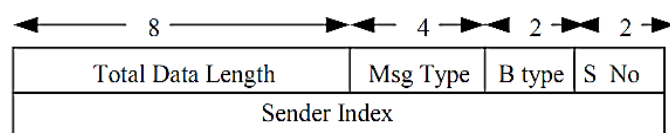


Fig 6. SWSP Header.

Fig. 6 depicts the SWSP's Protocol Header. The 4-bit 'Msg Type' field indicates the specific type of mail, such as Keep Alive (KA), Data Acknowledgement, Request-Response (RR), Data, and so on. The 2-bit 'B. type' in the SWSP header specifies the transmission way, which can be either from the sensor to the wireless network or from the wireless network to the detector. The 2-bit 'S. No.' denotes the sequential number assigned to the received data parcel. This indicates that the detector is capable of accommodating up to 4 concurrent data flows. In the SWSP header, there is a sender index field, which is 16-bit in size. The size of the header in the SWSP will be considerably lower than the extent of the TCP/IP header. The

building of outgoing packets in TCP/IP involves two challenging tasks: the calculation of the checksum and the proper sequencing and acknowledgment of numbers [33]. To reduce the amount of work that is needed, one should avoid using a large number of digits and use instead limited and reusable numbers. One can decrease the packet size as it is reasonable to decrease the chance of errors resulting from an unstable connection when using wireless networks.

IV. SWSP PERFORMANCE AND ANALYSIS

The Simple Wireless Sensor Protocol (SWSP) [34] is a low-complexity reliable protocol for WSNs but it is an asymmetrical protocol. The factors used in measuring the protocols in a wireless network include the total consumption of energy, size and sensor's cost, time taken in formation of network and time taken to come out of failure. There are basically four key parameters that should be taken into consideration when evaluating the efficiency of the protocol: Latency, network throughput, header overhead and control packet overhead are the key parameters that are used to estimate the display of any network. When it comes to the implementation of SWSP there were several aspects that were incorporated so as to reduce the power consumption as well as computational requirement.

However, in an attempt to boost dependability and reduce the time taken to regain functionality should there be a failure, we incorporated the RR and KA mails in SWSP. These mails need the detector radios to be on for utmost of the time their total operational time. The threshold of RR and KA signals can be modified according to the specific needs of the application, allowing for a balance among failure recovery and power consumption. Network conformation time refers to the speed at which a network responds to changes in its configuration, such as the addition or connection of sensors. The registration of a sensor in the model necessitates the synchronization of the data assortment nodes. The time needed for this synchronization is the primary limiting factor and is contingent upon the size of the data assortment node model.

There will be an increase in packet queuing latency when there are more than 2 packets waiting to be transferred if the window size is decreased to 2. The acknowledgment is transmitted at regular intervals and attached to the RR message. Minimizing the delay can be achieved by precisely adjusting the frequency of RR messages. Furthermore, this could potentially raise the expenses associated with receiving communications and requires a careful balance between several factors. By decreasing SWSP header's size, we aim to decrease the computational burden associated with the header. To reduce the complexity of the protocol, we remove certain non-vital elements of TCP, such as slow start and congestion control techniques. The overhead associated with KA (Keep-Alive) and RR (Request-Response) control packets appears to be substantial. In the case of a sensor that transmits data often, control packets are utilized to carry data and acknowledgements simultaneously through piggybacking. Sensors that have low-frequency data transfers can deactivate their radios during periods of inactivity.

Compared to the TCP throughput, the anticipated throughput of transferable data is likely to be lower. This is because of the group acknowledgement technique and the window's limited dimensions. The low throughput is considered satisfactory because sensor networks have modest-bandwidth requirements. Part two of this section delves into the correlation between network sensor density and throughput. Since we want to see how a larger number of detectors affects the latency and throughput of the model, this is pertinent. We expect a decrease in the system's performance when the number of sensors is raised. Next, we will investigate whether SWSP has any participation in it. At first, we conducted the SWSP presentation valuation by implementing the protocol on a personal computer running the Linux operational structure.

We conducted an analysis of the current lightweight applications of TCP, primarily focusing on LwIP and Tiny-TCP. These applications offered valuable guidance in preparing the SWSP's source code. Regrettably, we do not have the sufficient features to convert the procedure application into hardware. Meanwhile we presume that contemporary PC computers are far quicker than sensor processing, we did not prioritize tweaking the code to enhance processing. To mimic several sensing gadgets, we implemented them as individual procedures on a single personal computer. Due to the high processing speeds and fast network cards, we are certain that there will be no performance bottleneck. The wireless network access point or data collection node is situated on a distinct personal computer. The two personal computers are connected by a wireless means. The network interfaces consist of WaveLAN cards that adhere to the 802.11b standard.

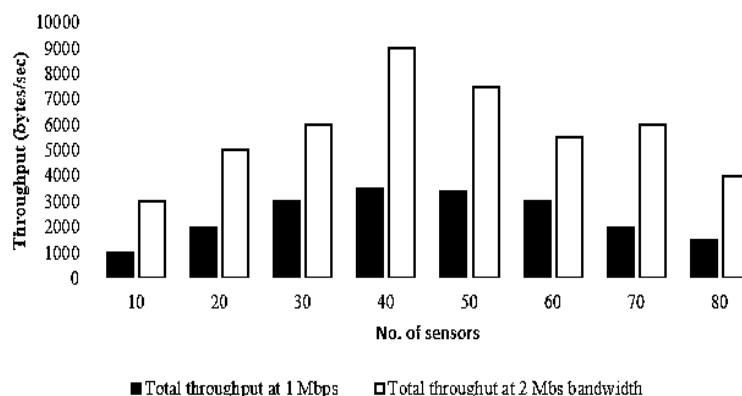


Fig 7. Total Throughput Against the Number of Sensors.

We carried out a series of performance assessments. Our primary emphasis throughout each test is on the network's performance and round-trip latency. Throughput refers to the total amount of information that is received by the access point during a designated period of time. The round-trip delay was determined by measuring the duration among the transmission of a packet from the reception and the sender of its acknowledgement. Throughout each iteration, the data length remained consistent while the quantity of devices was progressively raised from 20 to 80, with an increase of 10 for each iteration. Originally, the WaveLAN card was set up with a bandwidth of 1 Mbps. Afterwards, we repeated the complete set of trials, this time employing a bandwidth of 2 Mbps. **Fig. 7** illustrates the correlation between the network's throughput and the quantity of sensors, using a data length of 60 bytes. An upward trend in throughput is observed, reaching a peak value before declining. The association between the rise in the quantity of sensors and the enhancement in throughput is apparent.

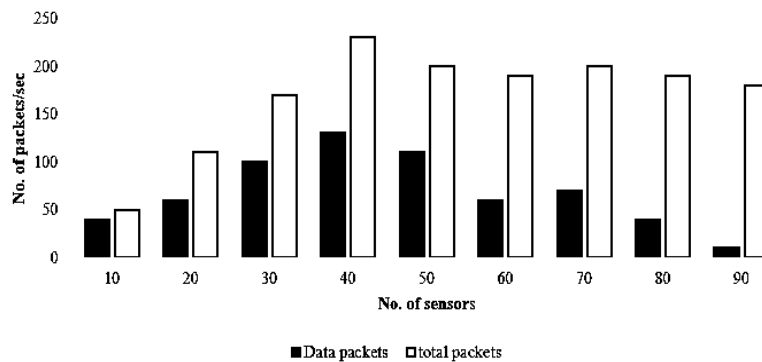


Fig 8. Number of Packets Against the Number of Sensors.

Once the sensors` number surpasses a specific frequency, the wireless network becomes incapable to handle the excessive influx of parcels. Consequently, a substantial amount of data packets necessitate retransmission. This is demonstrated in **Fig. 9**, where the number of retransmissions has increased dramatically from almost zero to a notable value. The number of sensors at which the throughput achieves its maximum value is nearly same, specifically 50, for both bandwidths.

Furthermore, the consistency of our series of studies for various data lengths persists. Nevertheless, the peak quantity value varies for each individual scenario. We saw persistent resetting of the cellular frontier card at the recipient caused by buffer overflow issues. Therefore, we may deduce that the observed output conduct in the aforementioned test situations is a consequence of the features of the access connection. **Fig. 8** displays a graph illustrating the total data packets number gained per second at the wireless network. The graphic demonstrates a perceptible decline in the amount of received data parcels when the sensors number is raised. Nevertheless, the overall quantity of received packets did not diminish to the same extent.

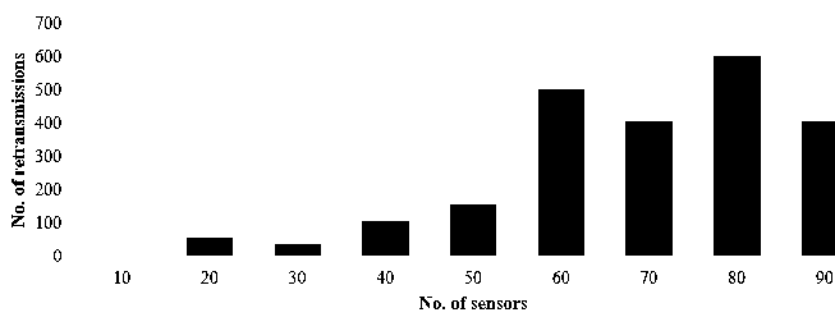


Fig 9. Number of Retransmissions Against the Number of Sensors.

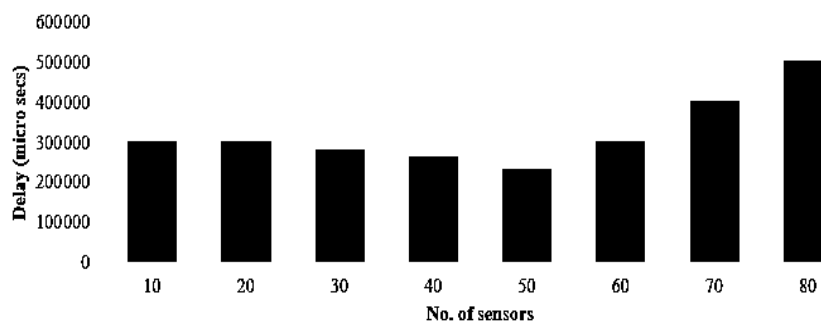


Fig 10. The Round-Trip Delays Against the Number of Sensors.

Consequently, there was a significant surge in the control packets quantity. This is anticipated as the sensors are required to wait for a duration of 3 RR formerly, they can broadcast the parcel again. Additionally, the round-trip latency for the model has been illustrated in **Fig. 10** using 60 bytes data extent. The round-trip delay is minimized when there are 50 sensors, and the throughput is maximized.

V. DISCUSSION

Within the performance evaluation of Simple Wireless Sensor Protocol (SWSP), it is important to balance different things such as energy consumption, reliability and protocol performance metrics which are throughput and latency. The reason why these features are important is that they determine how well this system works in WSN in terms of its efficiency and effectiveness.

Energy Efficacy

The reason why energy efficacy is one of the top priorities in SWSP lies in the statistic that motes are inherently resource-inhibited gadgets usually powered by batteries with limited capacity. If we look at this from a different angle, maximum conservation of energy increases the useful life of sensors thereby reducing maintenance costs and making it possible to deploy them in remote or hard-to-reach areas where replacing batteries is not feasible. Another thing about SWSP is that it incorporates power-saving methods as part of its design which can help to prolong network lifetime and reduce operational expenses as well. Nevertheless, it is important to ensure that there should be no imbalance between responsiveness and efficiency within the system; Therefore, trade-offs must be made very carefully [35]. For instance, when it comes to KA RR message exchanges, turning the sensors on increases reliability, but this will lead to increased power usage in case messages are being exchanged frequently under certain conditions. To achieve these balances there is need to be conversant with the needs of the applications and how the networks operate in dynamic nature.

In sustainable IoT deployments, actors such as SWSP, with the goal of saving energy, are very useful mainly due to the fact that they assist in the optimization of power usage which is in conformity with environmental and economic goals [36]. Due to prevention of power consumption at the protocol level, SWSP is useful in reducing the overall carbon dioxide footprint of WSNs. However, enhancing perfect on energy efficiency often entails complex trade-offs between various needs such as reliability against latency and throughput in the process; therefore; we still need more studies that will propose dynamic energy management approaches that can support adaptive alterations of protocol behaviours in accordance with changes in the environment and the networks' needs.

Moreover, even if it is beneficial to be designed for energy saving, the performance of SWSP can vary depending on such factors as network topology, traffic patterns or characteristics of the hardware but this should not hinder real world implementation as there may be other unknown challenges regarding power consumption hence the need to constantly monitor and enhance the power saving efforts [37]. However, compatibility of any standard or device should always be the first consideration before they are widely adopted since interoperability with industry standard wireless technologies and protocols makes its usability better while at the same time ensuring that there is no disruption of the existing system due to adoption of new systems such as SWSP.

Reliability and Failure Recovery

The use of SWSP KA and RR messages shows that the protocol is reliable and fast in failure recovery for wireless sensor networks. These techniques are essential in diagnosing and addressing communication breakdowns, ensuring data accuracy, and maintaining the connection in fluctuating environments [38]. KA and RR messages imply that sensor radios ought to be 'ON' for most of their working time, thereby promoting proactive network management and enabling a swift response to possible failures. This kind of approach to identifying faults before they cause major problems also enhances the ability of the system to handle shocks and knocks at the same time as reducing the likelihood of either losing important data or interrupting services.

In [39], it is described that KA and RR messages' frequency may be adjusted to better fit certain application requirements and, therefore, develop the overall presentation of the model. This is significant because in conditions where power is scarce such as in the developing world where this technology is widely used, reliability and power consumption cannot go hand in hand. The reliability of systems is important to SWSP because it always aims at maintaining reliability while not necessarily having a direct impact on energy efficiency as this is achieved through the use of adaptive mechanisms during the design phase of the system. What is more, it is important to know that SWSP was created with the focus on how things go wrong and how they should recover; in particular, this is true when it comes to mission-critical applications like industrial automation or healthcare systems used for monitoring the environment around us. In this area, small conversation errors or network interruptions mean a great deal; therefore, insisting on effective communication measures such as SWSP.

However, to achieve high dependability and at the same time ensure fast failure identification one has to have a round understanding of what goes on in the network; such information should include, for instance, topology changes, interferences and so on caused by physical factors. It is therefore important that there should be constant researches that will assist in refining the fault tolerant mechanisms that are included in SWSP so that they can be applicable in various altered conditions of their application.

Throughput and Latency

The two key performance indicators in wireless sensor networks are latency and throughput which define user satisfaction and productivity. Their treatment of these metrics shows that they viewed the optimization of network performance as a trade-off between various factors. SWSP aims at achieving high data transfer rate with low delay and consumption of power and reliability techniques that also reduces packet overheads in the resource constrained sensor nodes using wireless links [40]. One thing noticed about SWSP during performance tests was its behaviour where increasing the number of sensors leads to better throughput until congestion caused by too many packets being sent at once occurs thereby reducing this quantity again thus highlighting a challenge of managing traffic under dynamic conditions in networks. While more sensors enhance the acquisition and coverage of information, the issue of scalability is challenged when addressing access points because they can become bottlenecks due to their capacity constraints. The final quality that has been observed in SWSP is demonstrated by the fact that it maintains a constant level of performance when challenged with different sizes or configurations of networks which shows that it can adapt to new working conditions.

SWSP's approach of reducing delay with the trade-off of bandwidth is excellent, but this may not always be sufficient for meeting low latency demands of some real-time applications such as live monitoring or control systems. Often, the attainment of low latency involves a complex trade-off like the inclusion of other overheads or a reduction in power consumption. Reliability and energy consumption against ultra-low latency is guaranteed in the philosophy of SWSP which could be a disadvantage in certain applications that require near zero latency [41]. Moreover, the results of the analysis of the correlation between the characteristics of the wireless interface and the problems with buffer overflow in connection with the throughput and latency of SWSP show that the further development of the protocol, it is necessary to take into account not only the characteristics of the hardware platform but also the conditions in which the network operates. When SWSP is implemented in real world applications there may be emergent issues that may impact on the system's performance hence monitoring, testing and optimization should be conducted until the system runs smoothly in all circumstances.

Packet Overhead

Another significant factor influencing efficiency and reliability in SWSP is packet overheads; control packets such as KA and RR messages. The control packets keep the network connection stable; they also discover problems and help in the rapid failure recovery but with a price of consuming more resources hence negatively impacting the network performance. The management of packet overhead by SWSP is a trade-off among consumption of energy, the overhead involved and reliability that is most effective under certain network environment. This means that SWSP has been designed to be reliable whereas reliability is attained at the outlay of data throughput [42]. In a bid to maintain the strength in the communication while at the same time managing the power usage, low power has been incorporated in the SWSP design principles as well as mechanisms for modifying the frequency according to the control packets. However, one has to consider the effect of packet overhead especially in the current world where bandwidths are limited or there is high rated data transmission.

Control packets such as KA and RR messages have influence overheads depending on the network topology, traffic patterns, and environmental characteristics [43]. Sometimes when the congestion is high or when there is much interference in a certain region, having many control packets can make the congestion with in the networks worse while at the same time reducing the overall throughput. Whatever it means in that regard, it implies that SWSP is capable of dynamically adjusting protocol parameters depending on this frequency of sending control packet in turn it will assist network operators reduce these impacts and at the same time augment the protocol performance whenever such operating conditions are embraced. Another factor is that compatibility between SWSP and the current and future wireless communication standards as well as protocols should not be assumed because they are critical to SWSP integration into the diverse IoT environments. This can be achieved by ensuring it supports industry standard technologies since they make deployment easier by making it compatible thus the scalability by which many of the application requirements are effectively met by SWSP. However, there is still a huge research issue which demands the further research combined with the standardization work to strive for the fact that during inter-operationality the packet overhead must be minimal whereas the efficiency of protocols cannot be questioned.

Scalability and Stability

Stability and scalability are the major components of SWSP performance measurement since they reveal the ability of the protocol to adapt to various sizes or different network topologies and still maintain efficient and effective data spread. In this case, the fact that the scaling of SWSP is proportional to the various parameters such as the throughput and latency that are constant in the network proves that it can work effectively in large networks [44]. This is much needed so as to facilitate the installation of WSN for as small as simple installations to as large as industrial or even environmental system. Another aspect that makes SWSP to be more stable is the ability to work under different situations; this shows that SWSP is strong in the areas of change that occurs in the networks such as traffic change, topology change, environmental changes among others. In other words, through setting of performance levels that do not vary with the kind of network that is being used, it provides for standardized or like quality and reliability of communication during use of the experience in making calls thus enhancing the efficiency while in operation. However, it calls for experimentation conducted on real environments and then a validation process for the purpose of identifying the sources that can cause instability and then fix them like the packet loss or congestion that might be caused by a large number of devices using a single access point in the detection of hardware failure.

The use of SWSP and its integration with the currently used wireless communication standards and protocols make it scalable and interoperable hence making its wider adoption and implementation across various IoT ecosystems possible [45]. Compatibility with commonly used industry technologies is helpful in compatibility with various devices and infrastructural components. This in the IoT ecosystem allows for proper and smooth interaction as well as compatibility. However, to be able to handle increased amount of work and to maintain a constant and effective performance while ensuring compatibility with other systems may need planning and fine tuning of the protocol especially with the additional data and processing that the protocol adds, limitations on resources, and the constantly changing nature of the network. Secondly, the expandability and dependability of SWSP are directly attached to factors that enable it to give optimum data transfer, control of network assets and reduction of constraints. Due to the focus on the efficient usage of resources and great congestion control, SWSP improves the scalability and stability of WSN.

VI. CONCLUSION

The research provided valuable insights that helped in understanding the design and deployment of efficient WSNs through the establishment and evaluation of the SWSP. SWSP provides a scalable and generic solution for enabling reliable information exchange in environments with limited resources since it addresses the challenges of power, storage, processing, and computation capacity within sensor nodes. The event-driven protocol, which suggests the system's capabilities in the operation; the dependable data transfer schemes and controls; and minimum control overheads prove that the anticipated protocol is efficient in enhancing the performance of the model as well as in the energy optimization. Accordingly, the performance appraisal of SWSP has demonstrated that SWSP can effectively handle different network situations and can contribute to the improvement of the performance of WSN systems. Besides, the simplicity and flexibility of the proposed protocol ensure its effectiveness when interfacing different sorts of sensors and applications, thus providing easy scalability to meet the emergent WSN demands. The conclusions of this work reveal the importance of SWSP in the enhancement of the subsequent WSNs' evolution, which can be used in a wide range of application fields, such as environmental control, industrial processes, healthcare, and others.

CRediT Author Statement

The author reviewed the results and approved the final version of the manuscript.

Data Availability

No data was used to support this study.

Conflicts of Interests

The authors declare no conflict of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests.

References

- [1]. A. Milenković, C. Otto, and E. Jovanov, "Wireless sensor networks for personal health monitoring: Issues and an implementation," *Computer Communications*, vol. 29, no. 13–14, pp. 2521–2533, Aug. 2006, doi: 10.1016/j.comcom.2006.02.011.
- [2]. Dunfan Ye, Daoli Gong, and Wei Wang, "Application of wireless sensor networks in environmental monitoring," 2009 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS), pp. 205–208, Dec. 2009, doi: 10.1109/peits.2009.5407035.
- [3]. W. Pawgasame, "A survey in adaptive hybrid wireless Sensor Network for military operations," 2016 Second Asian Conference on Defence Technology (ACDT), pp. 78–83, Jan. 2016, doi: 10.1109/acdt.2016.7437647.
- [4]. D. S. Deif and Y. Gadallah, "Classification of Wireless Sensor Networks Deployment Techniques," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 834–855, 2014, doi: 10.1109/surv.2013.091213.00018.
- [5]. S. Kumar and D. K. Lobiyal, "Sensing Coverage Prediction for Wireless Sensor Networks in Shadowed and Multipath Environment," *The Scientific World Journal*, vol. 2013, no. 1, Jan. 2013, doi: 10.1155/2013/565419.
- [6]. D. Bhattacharyya, T. Kim, and S. Pal, "A Comparative Study of Wireless Sensor Networks and Their Routing Protocols," *Sensors*, vol. 10, no. 12, pp. 10506–10523, Nov. 2010, doi: 10.3390/s101210506.
- [7]. M. V. Ramesh, "Design, development, and deployment of a wireless sensor network for detection of landslides," *Ad Hoc Networks*, vol. 13, pp. 2–18, Feb. 2014, doi: 10.1016/j.adhoc.2012.09.002.
- [8]. A. Abdullah et al., "Development of wireless sensor network for monitoring global warming," 2012 International Conference on Advanced Computer Science and Information Systems (ICACSIS), pp. 107–111, Dec. 2012, [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6468777
- [9]. Chien-Liang Fok, G.-C. Roman, and Chenyang Lu, "Rapid Development and Flexible Deployment of Adaptive Wireless Sensor Network Applications," 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), pp. 653–662, doi: 10.1109/icdcs.2005.63.
- [10]. D. Gordon, M. Beigl, and M. A. Neumann, "Dinam: A wireless sensor network concept and platform for rapid development," 2010 Seventh International Conference on Networked Sensing Systems (INSS), pp. 57–60, Jun. 2010, doi: 10.1109/inss.2010.5573290.
- [11]. J. Blumenthal, M. Handy, F. Glatowski, M. Haase, and D. Timmermann, "Wireless sensor networks - new challenges in software engineering," EFTA 2003. 2003 IEEE Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No.03TH8696), vol. 1, pp. 551–556, doi: 10.1109/etfa.2003.1247755.
- [12]. K. K. Hasan, U. K. Ngah, and M. F. M. Salleh, "Efficient Hardware-Based Image Compression Schemes for Wireless Sensor Networks: A Survey," *Wireless Personal Communications*, vol. 77, no. 2, pp. 1415–1436, Jan. 2014, doi: 10.1007/s11277-013-1588-8.

- [13]. C. A. Oroza, J. A. Giraldo, M. Parvania, and T. Watteyne, "Wireless-Sensor Network Topology Optimization in Complex Terrain: A Bayesian Approach," *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17429–17435, Dec. 2021, doi: 10.1109/jiot.2021.3082168.
- [14]. S. Kazemina and S. Mahdavi, "Highly-matched sub-ADC cells for pipeline analogue-to-digital converters," *International Journal of Electronics*, vol. 106, no. 12, pp. 1785–1813, Jun. 2019, doi: 10.1080/00207217.2019.1625969.
- [15]. J. Yang, C. Zhang, X. Li, Y. Huang, S. Fu, and M. F. Acevedo, "Integration of wireless sensor networks in environmental monitoring cyber infrastructure," *Wireless Networks*, vol. 16, no. 4, pp. 1091–1108, Jun. 2009, doi: 10.1007/s11276-009-0190-1.
- [16]. C. V. Mahamuni, "A military surveillance system based on wireless sensor networks with extended coverage life," 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPIC), pp. 375–381, Dec. 2016, doi: 10.1109/icgtspic.2016.7955331.
- [17]. A. Lounis, A. Hadjidi, A. Bouabdallah, and Y. Challal, "Healing on the cloud: Secure cloud architecture for medical wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 266–277, Feb. 2016, doi: 10.1016/j.future.2015.01.009.
- [18]. B. Bhushan and G. Sahoo, "Routing Protocols in Wireless Sensor Networks," *Computational Intelligence in Sensor Networks*, pp. 215–248, May 2018, doi: 10.1007/978-3-662-57277-1_10.
- [19]. K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325–349, May 2005, doi: 10.1016/j.adhoc.2003.09.010.
- [20]. R. Zhou, H. Hou, Z. Gong, Z. Chen, K. Tang, and B. Zhou, "Adaptive Device-Free Localization in Dynamic Environments Through Adaptive Neural Networks," *IEEE Sensors Journal*, vol. 21, no. 1, pp. 548–559, Jan. 2021, doi: 10.1109/jsen.2020.3014641.
- [21]. R. Sharma, V. Vashisht, and U. Singh, "Modelling and simulation frameworks for wireless sensor networks: a comparative study," *IET Wireless Sensor Systems*, vol. 10, no. 5, pp. 181–197, Oct. 2020, doi: 10.1049/iet-wss.2020.0046.
- [22]. E. F. Nakamura, A. A. F. Loureiro, and A. C. Frery, "Information fusion for wireless sensor networks," *ACM Computing Surveys*, vol. 39, no. 3, p. 9, Sep. 2007, doi: 10.1145/1267070.1267073.
- [23]. N. Heydarishahreza, S. Ebadollahi, R. Vahidnia, and F. J. Dian, "Wireless Sensor Networks Fundamentals: A Review," 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 0001–0007, Nov. 2020, doi: 10.1109/iemcon51383.2020.9284873.
- [24]. F. D. Giraldo, S. España, Ó. Pastor, and W. J. Giraldo, "Considerations about quality in model-driven engineering," *Software Quality Journal*, vol. 26, no. 2, pp. 685–750, Dec. 2016, doi: 10.1007/s11219-016-9350-6.
- [25]. B. Selić and S. Gérard, "Modeling Cyber-Physical Systems," *Modeling and Analysis of Real-Time and Embedded Systems with UML and MARTE*, pp. 165–179, 2014, doi: 10.1016/b978-0-12-416619-6.00008-0.
- [26]. R. Saida, Y. H. Kacem, M. S. BenSaleh, and M. Abid, "A UML/MARTE Based Design Pattern for a Wireless Sensor Node," *Intelligent Systems Design and Applications*, pp. 590–599, Apr. 2019, doi: 10.1007/978-3-030-16657-1_55.
- [27]. A. Somov, A. Baranov, A. Savkin, D. Spirjakin, A. Spirjakin, and R. Passerone, "Development of wireless sensor network for combustible gas monitoring," *Sensors and Actuators A: Physical*, vol. 171, no. 2, pp. 398–405, Nov. 2011, doi: 10.1016/j.sna.2011.07.016.
- [28]. J. Wehrmann and R. C. Barros, "Movie genre classification: A multi-label approach based on convolutions through time," *Applied Soft Computing*, vol. 61, pp. 973–982, Dec. 2017, doi: 10.1016/j.asoc.2017.08.029.
- [29]. R. Nujoom, A. Mohammed, and A. Diabat, "Manufacturing system reconfiguration towards sustainable production: a novel hybrid optimization methodology," *Environmental Science and Pollution Research*, vol. 30, no. 51, pp. 110687–110714, Oct. 2023, doi: 10.1007/s11356-023-29233-x.
- [30]. V. C. Gungor and G. P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009, doi: 10.1109/tie.2009.2015754.
- [31]. S. G. Nikhade, "Wireless sensor network system using Raspberry Pi and zigbee for environmental monitoring applications," 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), pp. 376–381, May 2015, doi: 10.1109/icstm.2015.7225445.
- [32]. X. Wang, X. Zhang, G. Chen, and Q. Zhang, "Opportunistic Cooperation in Low Duty Cycle Wireless Sensor Networks," 2010 IEEE International Conference on Communications, pp. 1–5, May 2010, doi: 10.1109/icc.2010.5502561.
- [33]. J. Kay and J. Pasquale, "Profiling and reducing processing overheads in TCP/IP," *IEEE/ACM Transactions on Networking*, vol. 4, no. 6, pp. 817–828, 1996, doi: 10.1109/90.556340.
- [34]. P. Agrawal, Tan Sun Teck, and A. L. Ananda, "A lightweight protocol for wireless sensor networks," 2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003., vol. 2, pp. 1280–1285, doi: 10.1109/wcnc.2003.1200557.
- [35]. T. Rault, A. Bouabdallah, and Y. Challal, "Energy efficiency in wireless sensor networks: A top-down survey," *Computer Networks*, vol. 67, pp. 104–122, Jul. 2014, doi: 10.1016/j.comnet.2014.03.027.
- [36]. A. A. Bazmi and G. Zahedi, "Sustainable energy systems: Role of optimization modeling techniques in power generation and supply—A review," *Renewable and Sustainable Energy Reviews*, vol. 15, no. 8, pp. 3480–3500, Oct. 2011, doi: 10.1016/j.rser.2011.05.003.
- [37]. J. Singh, R. Kaur, and D. Singh, "A survey and taxonomy on energy management schemes in wireless sensor networks," *Journal of Systems Architecture*, vol. 111, p. 101782, Dec. 2020, doi: 10.1016/j.sysarc.2020.101782.
- [38]. H. Singh, A. D. Naik, R. Rao, and L. A. Petersen, "Reducing Diagnostic Errors through Effective Communication: Harnessing the Power of Information Technology," *Journal of General Internal Medicine*, vol. 23, no. 4, pp. 489–494, Mar. 2008, doi: 10.1007/s11606-007-0393-z.
- [39]. A. L. Ramaboli, O. E. Falowo, and A. H. Chan, "Bandwidth aggregation in heterogeneous wireless networks: A survey of current approaches and issues," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1674–1690, Nov. 2012, doi: 10.1016/j.jnca.2012.05.015.
- [40]. A. Alanazi and K. Elleithy, "Real-Time QoS Routing Protocols in Wireless Multimedia Sensor Networks: Study and Analysis," *Sensors*, vol. 15, no. 9, pp. 22209–22233, Sep. 2015, doi: 10.3390/s150922209.
- [41]. H. Tatenguem, A. Strano, V. Govind, J. Raik, and D. Bertozzi, "Ultra-low latency NoC testing via pseudo-random test pattern compaction," 2012 International Symposium on System on Chip (SoC), pp. 1–6, Oct. 2012, doi: 10.1109/issoc.2012.6376370.
- [42]. M. A. Kafi, J. B. Othman, and N. Badache, "A Survey on Reliability Protocols in Wireless Sensor Networks," *ACM Computing Surveys*, vol. 50, no. 2, pp. 1–47, May 2017, doi: 10.1145/3064004.
- [43]. F. Xia, H. B. Liaqat, J. Deng, J. Wan, and S. K. Das, "Overhead Control with Reliable Transmission of Popular Packets in Ad-Hoc Social Networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7647–7661, Sep. 2016, doi: 10.1109/tvt.2015.2484418.
- [44]. X. Meng, V. Pappas, and L. Zhang, "Improving the Scalability of Data Center Networks with Traffic-aware Virtual Machine Placement," 2010 Proceedings IEEE INFOCOM, pp. 1–9, Mar. 2010, doi: 10.1109/infcom.2010.5461930.
- [45]. S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," 2017 8th International Conference on Information Technology (ICIT), pp. 685–690, May 2017, doi: 10.1109/icitech.2017.8079928.

Publisher's note: The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. The content is solely the responsibility of the authors and does not necessarily reflect the views of the publisher.