RESEARCH ARTICLE

DOI: 10.54392/irjmt2428

Asian Research Association

INTERNATIONAL RESEARCH JOURNAL OF
MULTIDISCIPLINARY TECHNOVATION

A Comparative Analysis of Energy Consumption in Various Wireless Sensor Network Techniques

Suresh Vellaiyan [a], N. Vijayarani [b, *]

[a] Department of Sustainable Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai-602105, Tamil Nadu, India.

[b] Department of Computer Science, Namakkal Kavignar Ramalingam Government Arts College for Women, Namakkal-637001, Tamil Nadu, India

* Corresponding Author Email: n.vijayarani.mca@gmail.com

DOI: https://doi.org/10.54392/irjmt2428

Received: 08-09-2023; Revised: 04-02-2024; Accepted: 10-02-2024; Published: 19-02-2024

Abstract: The objective of this study is to analyze the energy consumption associated with modern methodologies utilized in wireless sensor networks and to conduct a comparative assessment with Reed Solomon (RS) codes. This paper presents three discrete techniques for wireless sensor networks. The strategies mentioned include the Self-Evolving Sensor System (SESS), the Secure and Adaptive Key Management utilizing Multipath Routing Protocol (SAKM-MRP), and the National Instruments Secure Reference-based Data Aggregation (NI-SRDA). A distinct algorithm was developed for each method to examine the energy use. Based on the experimental results, it has been shown that the RS-codes approach consumes a considerably greater quantity of energy compared to the SESS methods, which, in contrast, exhibit a significantly lower energy consumption. When comparing the efficiency of RS-codes and SESS methods, it is observed that the SAKN-MRP technique exhibits a more significant decrease in energy consumption. Compared to the RS-Codes system, the SESS scheme stands out with a significant 45.5% reduction in energy usage at the maximum delivery node. Similarly, the SAKM-MRP scheme showcases an average decrease of 35.7% in energy consumption. Notably, the NI-SRDA scheme achieves an impressive 60% reduction in energy consumption, underscoring its remarkable impact on energy efficiency. In a broader sense, it can be inferred that the NI-SDRA technique holds promise as an energy-efficient solution for wireless sensor networks in comparison to alternative strategies suggested in the current study.

Keywords: Energy Efficient, Multi-Path Routing Protocols, Wireless Sensor Network, Space Efficient Secret Sharing.

1. Introduction

The Wireless Sensor Network (WSN) is a collection of low-cost, small-scale nodes that gather and disseminate critical information. The network consists of individual nodes, each with the ability to perceive, retain, and transmit processed information to other nodes within the network [1]. In this study, we aim to investigate the impact of social media on mental health. Specifically, each individual sensing node is equipped with its own battery, central processing unit (CPU), memory, transceiver, and sensing device. WSN encompass a diverse range of applications, such as environmental monitoring, forest surveillance, animal tracking, flood detection and weather forecasting, disaster management, industrial automation, habitat monitoring, home automation, and health care [2, 3]. WSNs are currently experiencing significant growth. However, this expansion is accompanied by several obstacles. These challenges include operating in a dynamic environment, dealing with limited resources, and meeting the diverse requirements of numerous applications [4].

Numerous standards are now being developed for WSNs. The terms "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)" and "Wireless Highway Addressable Remote Transducer (HART)" are used to designate specific technologies [5]. The HART protocol has undergone expansion through the development of Wireless HART, a specialised implementation designed for industrial applications, particularly in the realm of process monitoring and control. Zigbee is a standardised mesh networking protocol that is anticipated to facilitate the development of wireless networking applications characterised by consistency, cost-effectiveness, and reduced power consumption. The 6LoWPAN protocol is an established standard developed by the Internet Engineering Task Force (IETF) that facilitates the efficient transmission of IPv6 packets across different locations. The 6LoWPAN network utilises the widely adopted transport technology called User Datagram Protocol (UDP).

Table 1. Comparison of WSN with 6LoWPAN

Features	WSN	6LoWPAN
Application	Control and Monitoring	Control and Monitoring
Memory	4-32KB	4-32KB
Battery Life	Approximately 10 to 100 days	Approximately 10 to 365 days
Number of Nodes	255 nodes	65536 nodes
Data rate/Transfer rate	Upto 250 Kbps	Upto 250 Kbps
Communication Range	1-75 m	100 m
Feature 1	Reliability, Low consumption, Low cost	IPv6 over IEEE 802.15.4
Feature 2	Isolated small-scale networks	Massively scalable networks

The use of Transmission Control Protocol (TCP), commonly referred to as TCP, is generally avoided in the context of 6LoWPAN due to the additional intricacy it introduces, along with concerns over performance and efficacy [6, 7]. Table 1 presents a comprehensive overview of the many properties of WSN and 6LoWPAN, highlighting both their similarities and differences.

Communication that fails to comply with essential security principles, including the preservation of confidentiality, authentication, and integrity, can potentially facilitate unauthorized individuals in accessing and interfering with communications throughout their transmission. Moreover, it is plausible that the perpetrator may disrupt, intercept, and modify the transmitted signals, as documented in previous studies [8, 9]. Therefore, it is of utmost significance to implement security protocols that govern and oversee the authorization and management of wireless network access with the aim of thwarting unauthorized entry and tampering with wireless communications [10, 11]. Furthermore, because of the limited transmission range of sensor nodes, it is necessary for each communication between the sensor node and the base station (BS) to traverse several intermediate nodes beforehand [9, 12]. In the context of wireless sensor networks (WSNs), the intermediate nodes that are present along the communication line can potentially serve as vulnerable points of entry for adversaries to execute malicious activities such as injecting false data and launching denial of service attacks [7, 13]. The pursuit of optimal communication and performance necessitates the identification and acquisition of crucial elements.

Therefore, it is imperative to promptly identify and eliminate the susceptible terminal nodes in light of this situation. Individuals who are not currently linked to the network have the ability to access the event data collected by the sensor nodes in WSNs [14, 15]. Therefore, it is imperative to provide data authentication and source authentication details alongside the data, as the confidentiality of the information collected from sensor nodes necessitates restricted access exclusively for authorised users. Furthermore, it is imperative for users to reach a consensus on exclusively accepting communication from nodes that possess a 100% level of authenticity. This measure is crucial in order to prevent the reception of deceptive or illicit information. While cryptographic methods can effectively safeguard the data portion of a packet, the header component of the packet remains susceptible to security breaches [16–18]. Traditional security measures are insufficient to ensure the confidentiality of communications due to the limitations of cryptographic techniques, which solely safeguard the data component of the packet. In light of this, it is imperative to use certain security measures to protect the secrecy of communication during transit. NI-SRDA finds application in various domains such as signal processing, picture denoising, genetic data analysis, and financial data interpretation. Several challenges hinder its widespread adoption, including the requirement for efficient algorithms to handle computational complexity, the necessity to choose and fine-tune models for optimal performance, the interpretability and generalizability of results, and the assurance of data availability and quality to ensure unbiased outcomes. Overcoming these issues will enable NI-SRDA to enhance its efficacy and influence across several industries by deriving meaningful insights from intricate data sets [5, 19].

The proliferation of wireless sensors is experiencing a notable surge in acceptance rates, primarily attributed to their inherent ease of deployment. Furthermore, the inclusion of wireless functionality facilitates the utilisation and exploitation of the network following its compromise. There exist multiple forms of assault that disrupt the effective functioning of a system, leading to errors, hindering appropriate channel access, and modifying data. Several researchers have already examined an almost Byzantine assault on WSN in accordance with the aforementioned limitation [19, 20].

Given the aforementioned context, the principal aim of this research is to examine and evaluate the extent of energy consumption generated by Self-Evolving Sensor System (SESS), the Secure and Adaptive Key Management utilising Multipath Routing Protocol (SAKM-MRP), and National Instruments Secure Reference-based Data Aggregation (NI-SRDA) techniques and subsequently compare these outcomes with those given by RS-codes. MATLAB/Simulink was employed for this study to prototype and simulate the methods and systems.

2. Techniques and Algorithm

2.1. Space Efficient Secret Sharing

Creating a standardized testing environment for WSNs involves defining a deployment scenario with specified node numbers, spatial distributions, and environmental factors. The present study encompasses evaluating energy efficiency under varying conditions. Assessments extend to data collection, aggregation techniques, and energy consumption patterns, highlighting the efficiency of algorithms and their impact on battery life. The SESS technique reported in this study incorporates Shamir's Secret Sharing mechanism. In a general context, it can be argued that hypothetically secure techniques for confidential communication exhibit inefficiencies in terms of space utilisation. Due to the fact that it generates n shares, each of which possesses a size that is comparable to that of the secret. Furthermore, it necessitates an increased quantity of storage space. A novel computational methodology has been developed to facilitate covert information sharing, aiming to optimise the utilisation of existing resources [21]. The encryption of the initial secret is achieved by the use of a symmetric key in this particular manner. The decrypted data is partitioned into 10 distinct segments. The use of block error correction procedures leads to the production of n shares, wherein redundancy is incorporated [22, 23]. A novel multi-path routing approach has been devised to mitigate cheating and prevent forwarding attacks. Once the secret message, denoted as m, has been partitioned into many shares, namely s1, s2, and sm, using a secret sharing technique, it is subsequently transmitted to its intended recipient across a network of distinct pathways.

The process of reconstructing the secrets entails initially interpolating a set of k shares to reconstruct the function f(x). Subsequently, the function is evaluated to reveal the secrets: si = f(i), where i ranges from the minimum value of 0 to the maximum value of T. All calculations are performed using modular arithmetic with a prime number that satisfies the following conditions: the prime number is greater than both the maximum value in the set of values {s1, s2,..., sn} and the value of n, where n is the total number of elements in the set. Additionally, the prime number is greater than zero and less than T minus one, where T is a given value. The process of recovering the concealed data in Algorithm 1 can be understood as the resolution of a set of linear equations. The equation A.v = F represents the relationship between a Vandermonde matrix A, a vector v of unknowns (polynomial coefficients ai), and a vector F of y-coordinates of shares.

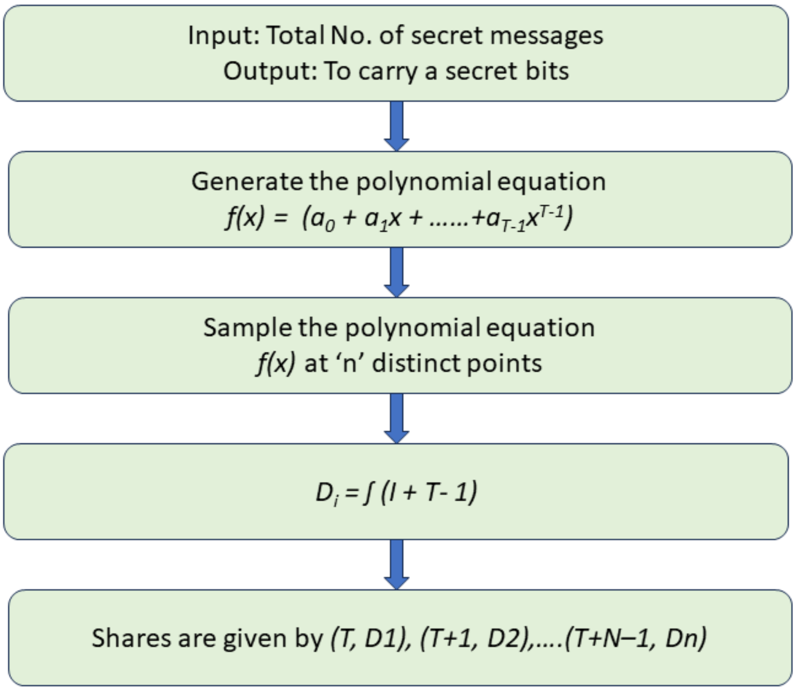
Input: Total No. of secret messages
Output: To carry a secret bits
Generate the polynomial equation
$f(x) = (a_0 + a_1x + ...+a_{T-1}x^{T-1})$
Sample the polynomial equation
$f(x)$ at ‘n’ distinct points
$D_i = ʃ (I + T- 1)$
Shares are given by $(T, D1), (T+1, D2),....(T+N–1, Dn)$

Figure 1. Algorithm for SESS scheme

The Vandermonde matrix A is constructed using the x-coordinates of any T shares. The vector v represents a set of unknowns in the T1 space, whereas the matrix A represents a T x T Vandermonde matrix. It is postulated, without any diminishment in generality, that there exist T minus 1 unit of (T, D1), (T+1, D2), etc. (2T minus 1, DT minus 1) shares within the system. Figure 1 depicts the algorithm proposed for the SESS system.

2.2. Secure authentication and key management scheme

The provided solution entails the implementation of a multipath routing mechanism to enhance load distribution and prolong network durability. In light of the malevolent actions, the implementation of encryption and decryption techniques is proposed as a means to ensure both data authentication and integrity preservation. Consequently, each node possesses the capability to ensure an authenticated route in conjunction with its own presence [24, 25]. The next section provides an explanation of the multipath and secure authentication approaches that have been recently introduced. Figure 2 illustrates the workflow of the proposed secure authentication and key management system. The figures depicting the encryption and decryption phases of the SAKM-MRP system are illustrated in Figures 3 and 4, respectively.

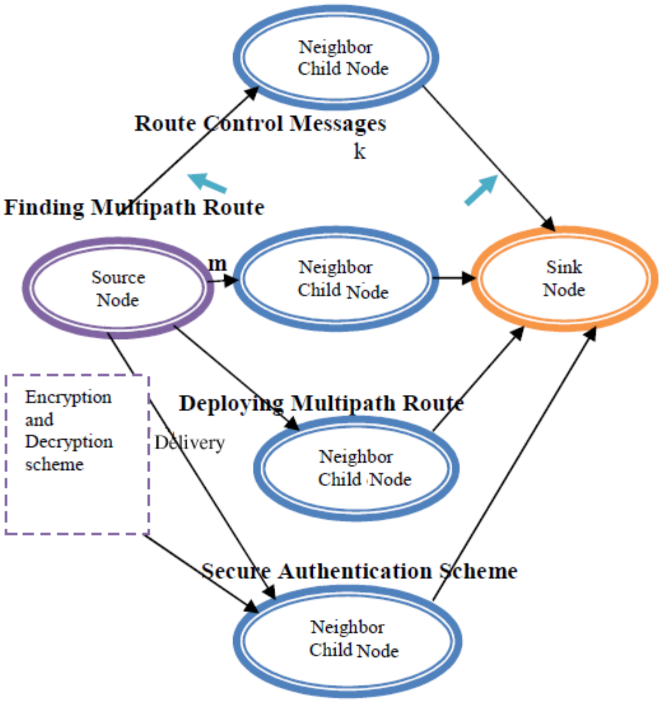

Figure 2. Workflow of secure authentication and key management approach

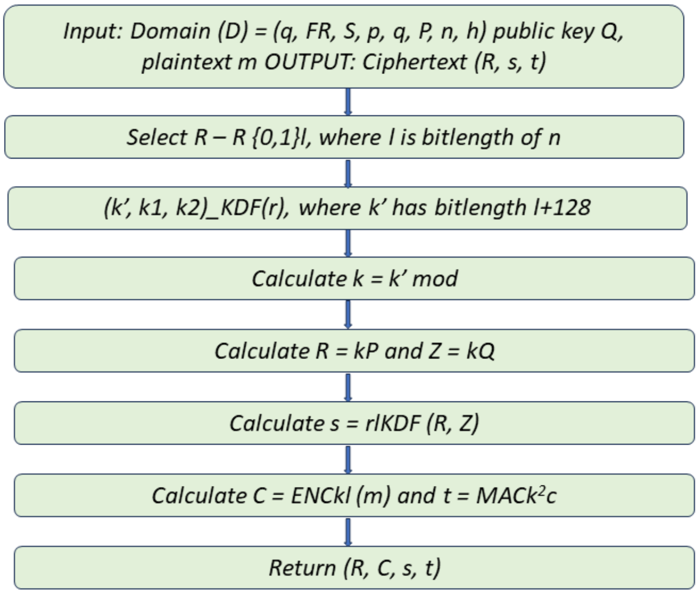
Input: Domain (D) = (q, FR, S, p, q, P, n, h) public key Q, plaintext m OUTPUT: Ciphertext (R, s, t)
Select R – R {0,1}l, where l is bitlength of n
(k', k1, k2)_KDF(r), where k' has bitlength l+128
Calculate k = k' mod
Calculate R = kP and Z = kQ
Calculate s = rlKDF (R, Z)
Calculate C = ENCkl (m) and t = MACk^{2}c
Return (R, C, s, t)

Figure 3. Encryption phase of SAKM-MRP scheme

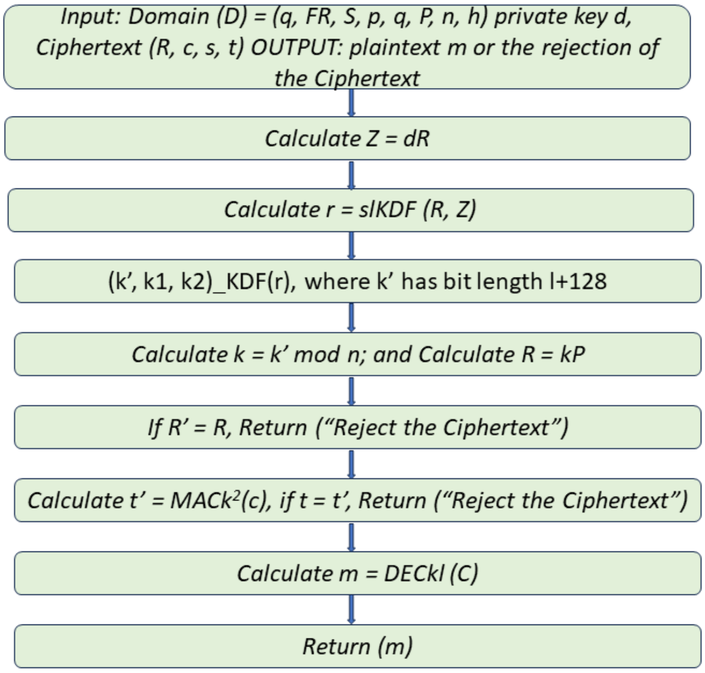
Input: Domain (D) = (q, FR, S, p, q, P, n, h) private key d, Ciphertext (R, c, s, t) OUTPUT: plaintext m or the rejection of the Ciphertext
Calculate Z = dR
Calculate r = slKDF (R, Z)
(k’, k1, k2)_KDF(r), where k’ has bit length l+128
Calculate k = k’ mod n; and Calculate R = kP
If R’ = R, Return (“Reject the Ciphertext”)
Calculate t’ = MACk²(c), if t = t’, Return (“Reject the Ciphertext”)
Calculate m = DECkl (C)
Return (m)

Figure 4. Decryption phase of SAKM-MRP scheme

2.3. Neighborhood Information Based Secured and Reliable Data Communication

In the framework of this methodology, it functions at the sensor node level. If the level of a sensor node is relatively low, there is no need to partition the information into shares. The system effectively oversees the task of partitioning data into several shares through the use of a flexible methodology capable of accommodating dynamic conditions. Furthermore, the information was distributed until it reached the designated node, which possesses a degree value and is appropriately substantial for the (t, n) threshold procedure [26]. In order to attain the intended result of recognizing shared information and the initial information packet, it is important to integrate a supplementary indicator at the early phase of the packet. Furthermore, the data includes a designated LR field that will be utilized at a later stage for the routing sequence.

3. Results and Discussion

3.1. Average Energy Consumption of SESS Technique

The parameter being referred to is the quantification of the mean discrepancy between the initial energy state and the final energy state that persists within each individual node. The degree of divergence is quantified at every individual node. The final metric that requires measurement is the aggregate energy consumption of the node. Figure 5 illustrates the comparative efficiency of the SESS scheme and RS-Codes in relation to energy consumption. The provided text consists of two numerical values enclosed in square brackets [27]. The duration of the network's existence has a direct correlation with the quantity of energy that is utilised. No more data is stored in association with the shares. The lifetime of the SESS network is far greater than that of the RS-Codes, and the SESS schemes exhibit significantly reduced energy usage compared to the RS-Coding system. In contrast to the RS-Codes system, the SESS scheme exhibits a reduction in energy usage of 45.5% for the maximum delivery node. The primary factor contributing to this phenomenon can be largely attributed to the extended duration of the network's existence.

3.2. Average Energy Consumption of SAKM-MRP Technique

Figure 6 presents a comparative analysis of the energy efficiency exhibited by the SAKM-MRP, SESS, and RS-Codes. The metric known as average energy consumption quantifies the average discrepancy between the initial energy level and the final energy level that persists in each node [28]. The subsequent action required is referred to as the energy utilization of the node. The energy consumption of SAKM-MRP techniques exhibits a notable reduction when compared to both SESS and the RS-Coding scheme. In comparison to RS-Codes, the SAKM-MRP scheme demonstrates an average decrease of 35.7% in energy consumption, while the SESS scheme exhibits an average decrease of 25% in energy consumption. One potential explanation for this phenomenon is that the SAKM-MRP scheme network exhibits greater longevity in comparison to RS-Codes and SESS schemes.

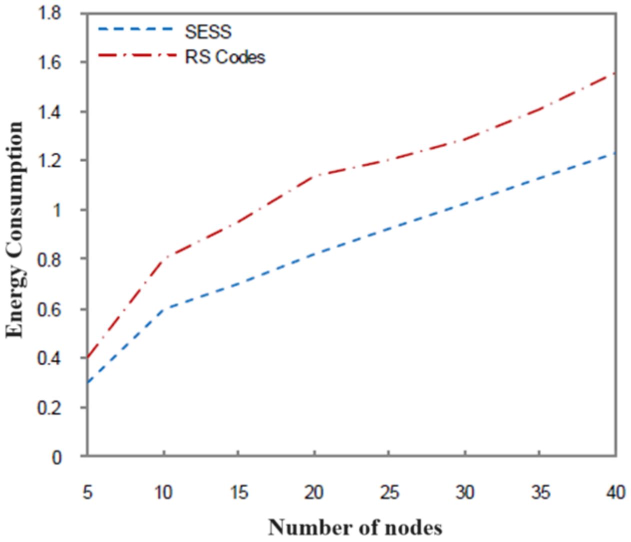

Figure 5. Performance of SESS scheme and RS-Codes reference to energy consumption

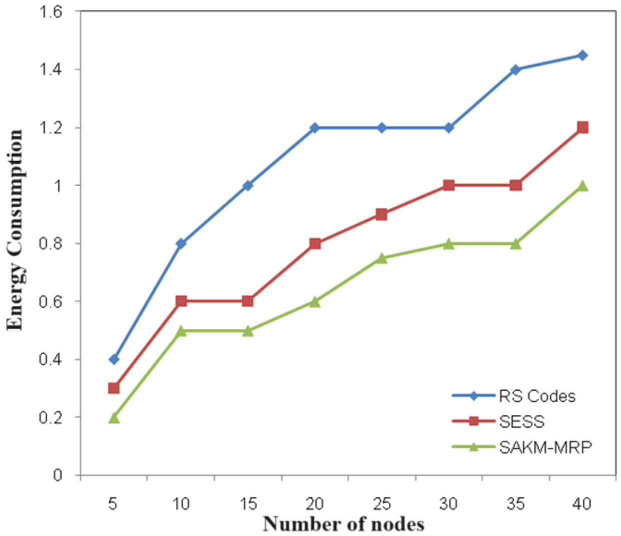

Figure 6. Performance of SAKM-MRP, SESS and RS- Codes regard to energy utilization

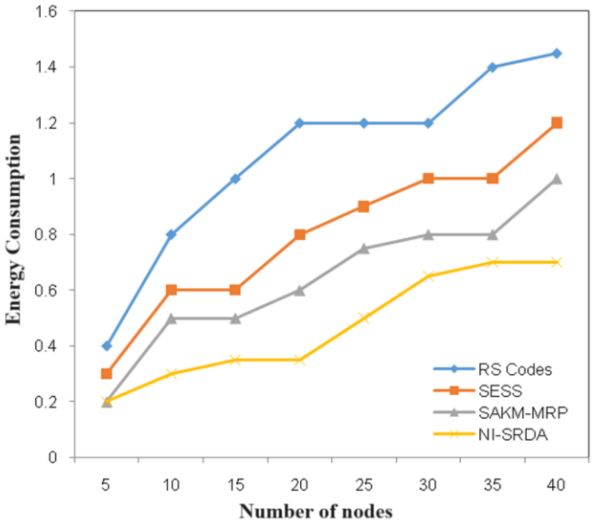

Figure 7. Energy performance of NI-SRDA, SAKM-MRP, SESS scheme and RS-Codes

3.3. Average energy consumption of NI-SRDA technique

The consistency of the divergence between the initial energy level and the final energy level is maintained across all nodes. Figure 7 presents a visual representation of the energy performance of NI-SRDA, SAKM-MRP, the SESS scheme, and RS-Codes. The energy consumption of NI-SRDA systems is significantly lower when compared to that of SAKM-MRP, SESS, and RS-Coding schemes. The utilisation of NI-SRDA demonstrates a noteworthy decrease of 60% in energy consumption in comparison to RS-Codes, particularly during periods of maximum node activity. Furthermore, there is a notable improvement of 54.5% when compared to the SESS scheme and a 44.5% improvement when compared to the SAKM-MRP scheme. This observation suggests that the NI-SRDA method has a prolonged network lifetime in comparison to alternative methodologies. The scalability of the proposed algorithm integrates energy-conscious features like sleep scheduling, data aggregation, and adaptive routing to reduce energy usage and extend the lifespan of the network in larger deployments.

4. Conclusion

Three separate strategies were developed to optimise energy use in WSNs: the NI-SRDA algorithm, the SAKM-MR methodology, and the SESS algorithm. The analysis of energy consumption for each of these algorithms was conducted and subsequently compared to the energy consumption of RS-Codes. The evaluation findings report that in contrast to RS-Codes, the SESS scheme has a consumption rate that is 45.5% lower than RS-Codes at the most elevated distribution node. The SAKM-MRP system exhibits an average reduction in energy consumption that is 35.7% lower than that of RS-Codes, and 25% lower than the SESS scheme. When comparing NI-SRDA to RS-Codes, it is shown that NI-SRDA leads to a significant 60% decrease in energy consumption, even when the node counts are at their highest. In a broader context, it can be inferred that the NI-SDRA approach holds promise as an energy-efficient solution in wireless sensor networks, demonstrating superior network longevity in comparison to the SAKM-MRP, SESS, and RS-Codes schemes. The efficacy of the NI-SDRA technique lies in its capacity to minimize energy wastage inside the network. An exploration into emerging technologies like machine learning and blockchain holds the potential to revolutionize energy optimization in WSNs, offering a forward-looking perspective that sets the stage for further innovations in the field.

References

[1] C.R. Kaur, N. Kumar, S. Batra, Trust management in social Internet of Things: A taxonomy, open issues, and challenges. Computer Communications, 150, (2020) 13-46. https://doi.org/10.1016/j.comcom.2019.10.034

[2] K. Amina, S. Gupta, S.K. Gupta, Multi-hazard disaster studies: Monitoring, detection, recovery, and management, based on emerging technologies and optimal techniques. International journal of disaster risk reduction, 47, (2020) 101642. https://doi.org/10.1016/j.ijdrr.2020.101642

[3] H.M.A. Fahmy, (2023) In Concepts, applications, experimentation and analysis of wireless sensor networks. Springer Cham. https://doi.org/10.1007/978-3-030-58015-5

[4] V. Wattana, T. Anuphaptrirong, D. Hoonsopon, when blockchain meets Internet of Things: Characteristics, challenges, and business opportunities. Journal of industrial information integration, 15, (2019) 21-28. https://doi.org/10.1016/j.jii.2019.05.002

[5] R. Álvarez, J. Díez-González, P. Verde, R. Ferrero-Guillén, H. Perez, Combined sensor selection and node location optimization for reducing the localization uncertainties in wireless sensor networks. Ad Hoc Networks, 139, (2023) 103036. https://doi.org/10.1016/j.adhoc.2022.103036

[6] A. Singh, P. Ashish, B. Sourabh, A walkthrough of the emerging IoT paradigm: Visualizing inside functionalities, key features, and open issues. Journal of Network and Computer Applications, 143, (2019) 111-151. https://doi.org/10.1016/j.jnca.2019.06.013

[7] S. Parween, Z.H. Syed, Md Asdaque Hussain, A survey on issues and possible solutions of cross-layer design in Internet of Things. International Journal of Computer Networks and Applications (IJCNA), 8(4), (2021) 311-333. https://doi.org/10.22247/ijcna/2021/209699

[8] M.H.P. Rizi, S.A.H Seno, A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. Internet of Things, 20, (2022) 100584. https://doi.org/10.1002/ett.4711

[9] M. Kingston Roberts, J. Thangavel, An improved optimal energy aware data availability approach for secure clustering and routing in wireless sensor networks. Transactions on Emerging Telecommunications Technologies, 34(3), (2022) e4711. https://doi.org/10.1002/ett.4711

[10] A. Ghosal, M. Conti, Security issues and challenges in V2X: A survey. Computer Networks, 169, (2020) 107093. https://doi.org/10.1016/j.comnet.2019.107093

[11] I.M. Varma, N. Kumar, A Comprehensive Survey on SDN and Blockchain-based Secure Vehicular Networks. Vehicular Communications, 44, (2023) 100663. https://doi.org/10.1016/j.vehcom.2023.100663

[12] K. Guleria, A.K. Verma, Meta-heuristic ant colony optimization based unequal clustering for wireless sensor network. Wireless Personal Communications, 105, (2019) 891-911. https://doi.org/10.1007/s11277-019-06127-1

[13] M.N. Halgamuge, Estimation of the success probability of a malicious attacker on blockchain-

based edge network. Computer Networks, 219, (2022) 109402. https://doi.org/10.1016/j.comnet.2022.109402

[14] G. Kalnoor, S. Gowrishankar, IoT-based smart environment using intelligent intrusion detection system. Soft Computing, 25(17), (2021) 11573-11588. https://doi.org/10.1007/s00500-021-06028-1

[15] U. Dampage, L. Bandaranayake, R. Wanasinghe, K. Kottahachchi, B. Jayasanka. Forest fire detection system using wireless sensor networks and machine learning. Scientific Reports, 12(1), (2022) 46. https://doi.org/10.1038/s41598-021-03882-9

[16] J. Grover, Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. Vehicular Communications, 34 (2022) 100458. https://doi.org/10.1016/j.vehcom.2022.100458

[17] A. Heshmati, M. Bayat, M. Doostari, S.M. Pournaghi, Blockchain based authentication and access verfication scheme in smart home. Journal of Ambient Intelligence and Humanized Computing, 14(3), (2023) 2525-2547. https://doi.org/10.1007/s12652-022-04501-9

[18] V. Sharma, S. Vats, D. Arora, K. Singh, A.S. Prabuwono, M.S. Alzaidi, A. Ahmadian, OGAS: Omni-directional Glider Assisted Scheme for autonomous deployment of sensor nodes in open area wireless sensor network. ISA transactions, 132, (2023) 131-145. https://doi.org/10.1016/j.isatra.2022.08.001

[19] M. Faris, M.N. Mahmud, M.F.M. Salleh, A. Alnoor, Wireless sensor network security: A recent review based on state-of-the-art works. International Journal of Engineering Business Management, 15, (2023). https://doi.org/10.1177/18479790231157220

[20] S. Tabibi, A. Ghaffari, Energy-efficient routing mechanism for mobile sink in wireless sensor networks using particle swarm optimization algorithm. Wireless Personal Communications, 104, (2019) 199-216. https://doi.org/10.1007/s11277-018-6015-8

[21] M.M Hazzazi, S. Attuluri, B. Zaid, K. Joshi, A Novel Cipher-Based Data Encryption with Galois Field Theory. Sensors, 23(6), (2023) 3287. https://doi.org/10.3390/s23063287

[22] G.D. Kaur, Human factor analysis of error detection and correction in hand-knotted carpet production process. Research Journal of Textile and Apparel, (2023). https://doi.org/10.1108/RJTA-10-2022-0124

[23] A. Iqbal, K.M. Chari, Concurrent fault detection and location with minimal overhead in Ling parallel prefix adders with a scheme for fault tolerant Ling prefix adders. Microelectronics Reliability, 127, (2021) 114375. https://doi.org/10.1016/j.microrel.2021.114375

[24] M.S. Azhdari, A. Barati, H. Barati, A cluster-based routing method with authentication capability in Vehicular Ad hoc Networks (VANETs). Journal of Parallel and Distributed Computing, 169, (2022) 1-23. https://doi.org/10.1016/j.jpdc.2022.06.009

[25] Z. Yang, L. Li, G.U. Fei, L. Xinghong, H. Maryam, TADR-EAODV: A trust-aware dynamic routing algorithm based on extended AODV protocol for secure communications in wireless sensor networks. Internet of Things, 20, (2022) 100627. https://doi.org/10.1016/j.iot.2022.100627

[26] G. Douglas, D. Centola, Topological measures for identifying and predicting the spread of complex contagions. Nature Communications, 12(1), (2021) 4430. https://doi.org/10.1038/s41467-021-24704-6

[27] M. Baldi, F. Chiaraluce, L. Incipini, M. Ruffini, Code-based physical layer secret key generation in passive optical networks. Ad Hoc Networks, 89, (2019) 1-8. https://doi.org/10.1016/j.adhoc.2019.02.003

[28] Z. Chunli, Y. Fengfan, C. Chen, R. Umar, Reed-Solomon Coded Cooperative Space-time Block Coded Spatial Modulation. International Conference on Wireless Communications and Smart Grid (ICWCSG), IEEE, China. https://doi.org/10.1109/ICWCSG53609.2021.00027

Authors Contribution Statement

Suresh Vellaiyan and Vijayarani N made equal contributions to the presented research work.

Funding

The authors declares that there was no funding received to carry out this work

Conflict of Interest

The authors declares that he does not have any known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

Data and materials related to the research work will be available based on the request.

Has this article screened for similarity?

Yes

About the License