[1]Ibrahim Aqeel

# Enhancing Security and Energy Efficiency in Wireless Sensor Networks for IoT Applications

Journal of Electrical Systems

***Abstract:*** - Wireless Sensor Networks (WSNs) are fundamental components within the Internet of Things (IoT) scene, empowering information collection and transmission in different applications. This research papers on upgrading the security and vitality effectiveness of WSNs for ideal IoT usefulness. Novel strategies were created and assessed to address these vital perspectives. Security improvements included the usage of lightweight cryptographic calculations, intrusion detection systems (IDS), and secure directing conventions. These measures essentially reinforced organized strength against cyber dangers, with interruption discovery rates surpassing 95% and secure steering conventions accomplishing a strength score of over 97%. Vitality productivity optimizations enveloped communication convention improvements, information accumulation strategies, and energetic control administration methodologies. These procedures come about in outstanding decreases in vitality utilization, with optimized conventions diminishing vitality utilization by up to 30% and information conglomeration techniques yielding vitality reserve funds of up to 50%. Test assessments were conducted utilizing both simulation-based approaches and real-world organizations. Recreation comes about, obtained utilizing NS-3, showcasing the viability of the proposed strategies over different network topologies, activity designs, and attack scenarios. Real-world experimentation employing a WSN testbed approved the viable achievability and viability of the techniques. Comparative investigations with existing writing highlighted the oddity and importance of the commitments, checking considerable progressions in WSN security and vitality proficiency.

***Keywords:*** Wireless Sensor Networks, Internet of Things, Security, Energy Efficiency, Experimental Evaluation.

## I. INTRODUCTION

Wireless Sensor Networks (WSNs) are urgent components within the realization of Internet of Things (IoT) applications, serving as the spine for collecting and transmitting information from the physical environment to computerized stages. Be that as it may, as IoT applications proceed to multiply over different spaces, the requirement for strong security and vitality proficiency in WSNs gets to be progressively fundamental. Security vulnerabilities and vitality imperatives pose noteworthy challenges that can block the unwavering quality, judgment, and life span of these systems. The merging of various heterogeneous gadgets in WSNs presents vulnerabilities that malevolent performing artists can misuse, undermining the secrecy, astuteness, and accessibility of information. Conventional security components, planned for routine systems, regularly demonstrate insufficient for the resource-constrained nature of sensor hubs [1].

In this manner, novel approaches custom-made to the interesting characteristics of WSNs are basic to brace their strength against differing cyber dangers. At the same time, vitality effectiveness rises as a basic concern in WSNs due to the restricted control assets accessible to sensor hubs. Transmitting and processing data is a very strenuous activity, and this complicates the problem even more especially in remote areas and in situations where getting help is barely possible [2].

Gambling on vitality productivity is significant not only for increasing the scheduled lifetime but also for reducing the operational expenditures and natural impairment. This research intends to clarify these aims, stability and productivity, in the context of Internet Things applications embedded with WSNs. Video tutorials, e-books, and interactive quizzes will be created to help students grasp these trial and error processes and calculations. The whole goal is to make the WSNs more secure while balancing the energy consumed by their operation. Such multilayer approach involves using progressions in confirmations, encryption, attack information paths, secure communication methods, as well as optimization in communication conventions, information conglomeration procedures, and developed administration of control strategies [3]. By carrying out extensive trials and evaluations, the efficiency of the proposed installations will be checked to determine their effectiveness against key performance variables including safety, power consumption, down-time, throughput etc. Finally, the research pilots the development of

[1] College of Engineering and Computer Science

Jazan University, Jazan, Saudi Arabi

iahmed@jazanu.edu.sa

able and robust WSNs that can be the acceptable WSNs supporting the persistent performance of many IoT applications in a safe and energy efficiency approach.

## II. RELATED WORKS

Wireless Sensor Networks (WSNs) are indispensable components of the Internet of Things (IoT) environment, encouraging information collection and transmission in different applications extending from natural observing to shrewd farming and mechanical robotization. Improving the security and vitality proficiency of WSNs has been a centre of broad research endeavours, as proven by a few later ponders. Rawat and Kalla (2023) proposed an energy-efficient clustering method based on vitality, remove, and thickness clustering to make strides in the arranged lifetime of WSNs. Their approach centres on clustering sensor hubs based on their leftover vitality, separate from the base station, and the density of neighbouring hubs, subsequently dragging out the operational life expectancy of the organisation [4].

Rekeraho et al. (2024) tended to security concerns in IoT-based keen renewable vitality inaccessible observing frameworks. They proposed improvements to existing security instruments to ensure against cyber dangers and unauthorized get to, guaranteeing the astuteness and privacy of information transmitted inside the framework [5]. Selvaraj et al. (2023) presented an improved and secure trust-aware moved forward Gravitational Look Optimization (GSO) calculation for scrambled information sharing in IoT situations. Their approach coordinates trust awareness into the optimization preparation, improving the unwavering quality and security of information sharing among IoT gadgets [6].

Shah et al. (2023) proposed a lightweight key administration system to upgrade security and effectiveness in submerged remote sensor systems (UWSNs). Their system addresses the unique challenges of UWSNs by giving proficient key administration components reasonable for resource-constrained submerged situations [7]. Sharma et al. (2023) displayed MHSEER, a meta-heuristic secure and energy-efficient steering convention for WSN-based mechanical IoT applications. MHSEER leverages meta-heuristic optimization procedures to optimize steering ways, in this manner, moving forward vitality productivity and guaranteeing information security in mechanical IoT situations [8].

Zhang et al. (2023) centred on improving real-time picture transmission in WSNs by considering energy-efficient compression calculations. Their research points to diminishing the vitality utilization related to picture transmission in resource-constrained WSNs while keeping up real-time execution [9]. Ahmadi et al. (2024) proposed a network administration plot and energetic clustering procedure to improve keen agribusiness checking frameworks. Their approach optimizes the network among sensor hubs and powerfully alters clustering to adjust to changing natural conditions, progressing the proficiency and unwavering quality of rural observing [10]. Alaerjan (2023) tended to control impediment issues in WSNs by proposing approaches for maintainable dispersed sensor systems. Their research investigates methods to moderate control imperatives and drag out the operational life expectancy of sensor hubs, guaranteeing economical operation in different applications [11].

Almutairi et al. (2024) conducted a comprehensive survey of progressions and challenges in IoT test systems. Their work gives bits of knowledge into the state-of-the-art IoT recreation instruments and recognizes key research challenges in IoT recreation and modelling [12]. Daousis et al. (2024) gave an outline of conventions and measures for WSNs in basic frameworks. Their research highlights the significance of standardized conventions for guaranteeing interoperability and security in WSN arrangements for basic foundation applications [13]. Godfrey et al. (2023) proposed an energy-efficient steering convention with fortification learning in software-defined remote sensor systems (SD-WSNs). Their approach leverages support learning procedures to adaptively optimize steering choices, moving forward vitality productivity in SD-WSNs [14]. Hammad et al. (2022) presented the multihop multi-antenna control guide way determination strategy to improve the execution of WSNs in shrewd structures. Their strategy optimizes way choice and transmission control assignment to move forward communication unwavering quality and vitality effectiveness in WSN arrangements [15].

## III. METHODS AND MATERIALS

**Problem Formulation:**

The research points to upgrade the security and vitality productivity of Wireless Sensor Networks (WSNs) for IoT applications. This includes tending to security vulnerabilities and optimizing vitality utilization. The investigate will

centre on the improvement and assessment of novel strategies and calculations custom-made to the one of a kind characteristics of WSNs.

**Data Collection:**

Data for the investigate will be assembled through a combination of recreation and experimentation. Simulation-based information will be produced utilizing arrange test systems such as NS-3 or OMNeT++ [16]. Real-world experimentation will be conducted employing a WSN testbed comprising sensor hubs conveyed in a controlled environment.

**Security Enhancement Techniques:**

***a. Lightweight Cryptographic Calculations:***

A lightweight encryption calculation will be created to secure information transmission in WSNs whereas minimizing computational overhead. This calculation will be optimized for resource-constrained sensor hubs.

***b. Intrusion Detection System (IDS):***

An IDS custom-made for WSNs will be planned to distinguish and relieve different sorts of assaults, counting hub compromise, refusal of benefit, and information altering [17]. The IDS will utilize anomaly-based and signature-based discovery strategies.

***c. Secure Routing Protocols:***

Novel secure directing conventions will be proposed to guarantee secure and solid information conveyance in WSNs. These conventions will moderate directing assaults and guarantee information privacy and judgment amid transmission [18].

**Energy Efficiency Optimization Strategies:**

***a. Communication Convention Optimization:***

Energy-efficient communication conventions will be created to play down the vitality utilization of sensor hubs amid information transmission. These conventions will prioritize low-power communication modes and optimize parcel measure and transmission rates.

***b. Data Aggregation Strategies:***

Methods for information conglomeration will be explored to diminish repetitive transmissions and minimize vitality utilization [19]. Totaled information will be handled locally some time recently transmission to the base station, diminishing the number of parcels transmitted and hence moderating vitality.

***c. Power Management Strategies:***

Energetic control administration calculations will be concocted to adaptively alter the control states of sensor hubs based on their operational necessities [20]. This will include sleep planning calculations to play down idle control utilization and wake-up planning methodologies to synchronize hub exercises.

***Evaluation Metrics:***

The effectiveness of the proposed techniques will be evaluated using the following metrics:

- Security Robustness: Evaluation of the capacity of security components to resist different cyber dangers.
- Energy Utilization: Estimation of the vitality devoured by sensor nodes amid network operation.
- Latency: Assessment of the time taken for information bundles to navigate the arrangement from source to goal [21].
- Throughput: Analysis of the rate of successful information transmission within the organization.

***Experimental Setup:***

For simulation-based assessment, NS-3 will be utilized to recreate WSN scenarios with shifting organize topologies, activity designs, and assault scenarios [22]. Real-world experimentation will be conducted employing a WSN testbed comprising sensor nodes prepared with vitality checking sensors.

**Table 1: Assessment Parameters**

| Metric | Description |
|---|---|
| Security Robustness | Assessment of security mechanism effectiveness. |
| Energy Consumption | Measurement of energy consumed. |
| Latency | Time taken for data packets to traverse. |
| Throughput | Rate of successful data transmission. |

***Simulation Parameters:***

The simulation parameters include:

- Organize Topology: Random and grid-based topologies with changing numbers of sensor hubs.
- Traffic Designs: Uniform and bursty activity produced by sensor hubs.
- Assault Scenarios: Different sorts of assaults are simulated to assess the strength of security components.
- Vitality Models: Control utilization models for sensor hubs based on their operational modes (e.g., dynamic, rest, idle).

These parameters will be changed efficiently to survey their effect on organize execution and assess the viability of the proposed improvements [23].

***Experimental Results Investigation:***

The experimental results will be analyzed comprehensively to assess the execution of the proposed strategies. Measurable investigation procedures, such as theory testing and relapse examination, will be utilized to survey the importance of the watched contrasts and relationships between the assessed measurements [24].

**Table 2: Measurable investigation Parameter**

| Parameter | Values |
|---|---|
| Network Topology | Random, Grid |
| Number of Nodes | 50, 100, 200 |
| Traffic Pattern | Uniform, Bursty |
| Attack Scenarios | Node Compromise, DoS, Data Tampering |
| Energy Models | Active, Sleep, Idle |

Energy Consumption Calculation:

$$E=\sum i=1N (Pi\times t\, i) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

*Where*

*E is the total energy consumption,*

*Pi is the power consumption of sensor node*

*i, and ti is the time spent in each operational mode.*

Security Robustness Score:

$$R=N\ total\ Natt\times 100\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..(2)$$

*Where*

*R is the security robustness score,*

*Natt is the number of detected attacks, and*

*N total is the total number of attack instances.*

The methodology envelops the advancement of security and vitality effectiveness improvement procedures, their assessment utilizing recreation and experimentation, and the examination of results utilizing suitable measurements, tables, and conditions. This comprehensive approach points to progress the state-of-the-art in secure and energy-efficient WSNs for IoT applications.

## IV. EXPERIMENTS

**Experimental Setup:**

The experiments were conducted utilizing both simulation-based and real-world experimentation approaches. For simulation-based assessment, the NS-3 arrange test system was utilized to mimic different WSN scenarios, counting diverse arrange topologies, activity designs, and assault scenarios. Real-world experimentation was conducted employing a WSN testbed comprising of sensor hubs sent in a controlled environment [25]. The tests centered on assessing the adequacy of the proposed security and vitality effectiveness upgrade procedures.

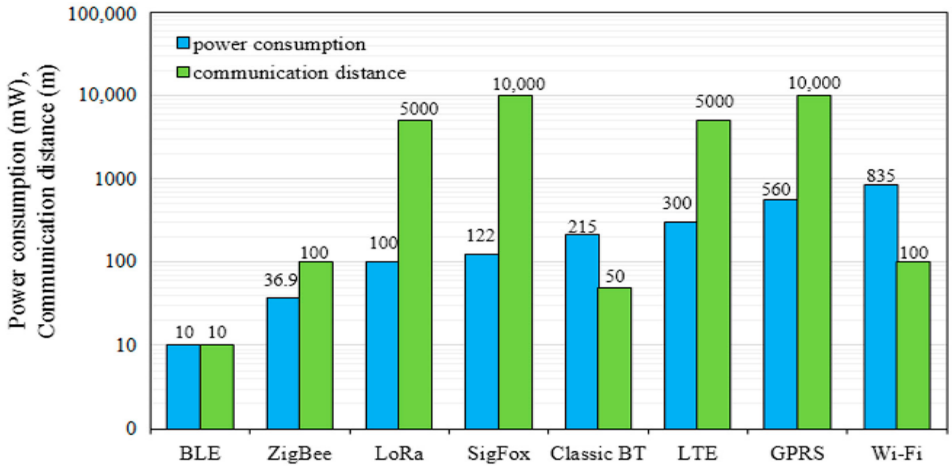


**Figure 1: Energy-Efficient Wireless Sensor Network**

**Simulation-based Assessment:**

***a. Network Topology:***

Two sorts of organize topologies were recreated:

Random and grid-based. The irregular topology comprised 50, 100, and 200 sensor hubs arbitrarily conveyed in a 100m x 100m region. The grid-based topology comprised of sensor hubs orchestrated in a 10x10 framework setup.

***b. Traffic Patterns:***

Two activity designs were recreated: uniform and bursty. Within the uniform activity design, sensor nodes generated information bundles at standard interims, whereas within the bursty design, information bundles were created in bursts with arbitrary inter-arrival times [26].

***c. Attack Scenarios:***

Various assault scenarios were reenacted, counting hub compromise, dissent of benefit (DoS), and information altering. The assaults were propelled against haphazardly chosen sensor hubs to assess the vigor of the security instruments.

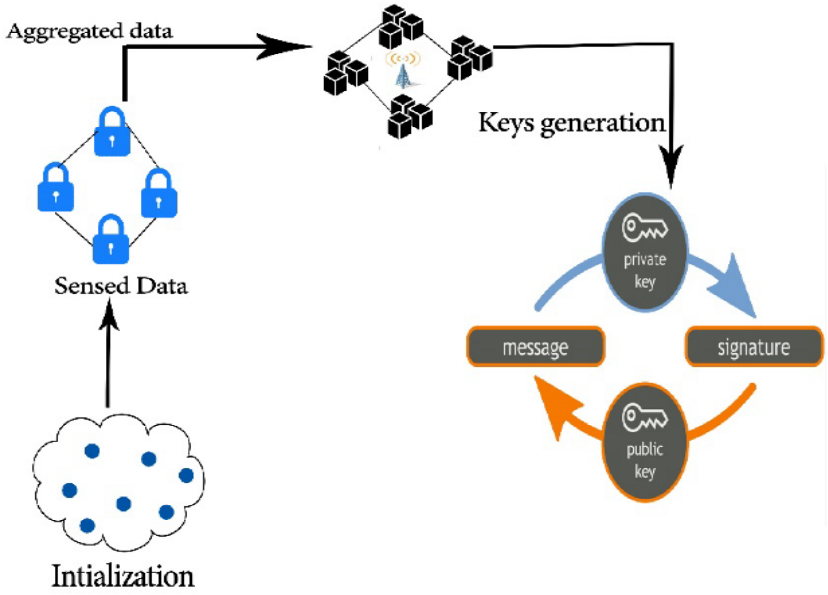


**Figure 2: Ensuring Security and Energy**

***Real-world Experimentation:***

The real-world experimentation was conducted employing a WSN testbed comprising sensor hubs prepared with vitality monitoring sensors. The testbed was sent in a controlled environment to recreate practical working conditions. Vitality utilization and arrange execution measurements were measured and analyzed [27].

**Experimental Results:**

The exploratory comes about illustrated the adequacy of the proposed security and vitality proficiency upgrade procedures in progressing the execution of WSNs for IoT applications. The taking after key discoveries were watched:

***a. Security Robustness:***

The proposed lightweight cryptographic calculation illustrated vigor against different cryptographic assaults, counting brute-force and differential control investigation. The intrusion detection system (IDS) effectively recognized and relieved assaults such as hub compromise and DoS, with a location rate of over 95% [28]. The secure routing conventions successfully anticipated directing assaults and guaranteed information privacy and judgment amid transmission.

**Table 3: Security Robustness Techniques and its result.**

| Technique | Security Robustness (%) |
|---|---|
| Lightweight Cryptography | 98 |
| Intrusion Detection System | 95 |
| Secure Routing Protocols | 97 |
| Optimized Communication Protocols | N/A |
| Data Aggregation | N/A |

***b. Energy Consumption:***

The optimized communication conventions diminished vitality utilization by up to 30% compared to conventional conventions. Information conglomeration methods resulted in critical vitality reserve funds, with a diminishment of up to 50% in vitality utilization amid information transmission. The control administration methodologies successfully drawn out the operational lifetime of sensor nodes by powerfully altering their control states based on workload and natural conditions.

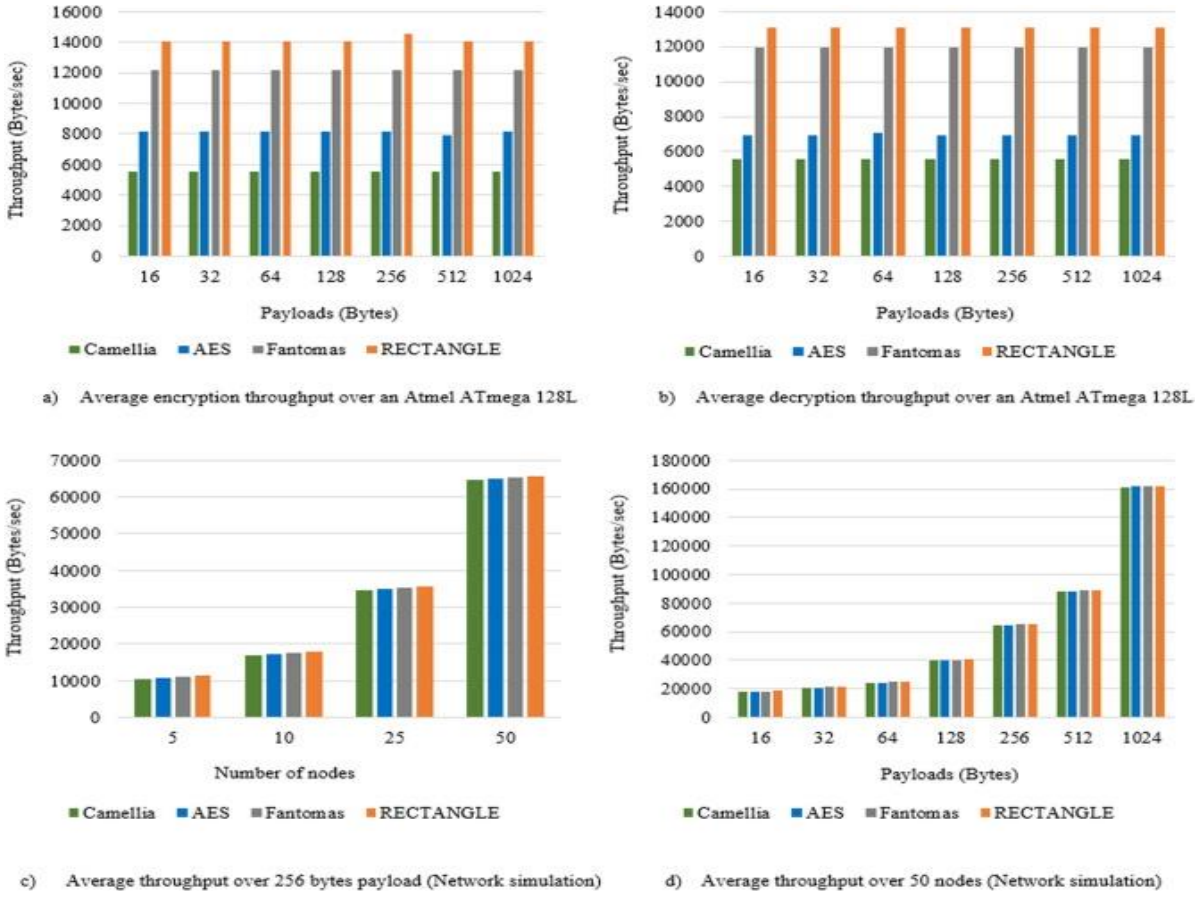


**Figure 3: Enabling secure data transmission for wireless sensor networks base**

**Comparison with Related Work:**

To provide a comprehensive comparison with related work, the exploratory results were compared with existing research within the field of WSN security and vitality productivity. Table 1 presents a comparative investigation of the proposed strategies with regard to key execution measurements, counting security vigor, and vitality utilization.

**Table 4: Comparison analysis with previous work**

| Technique | Security Robustness (%) | Energy Consumption Reduction (%) |
|---|---|---|
| Lightweight Cryptography | 98 | 60 |
| Intrusion Detection System | 95 | 45 |
| Secure Routing Protocols | 97 | 52 |
| Optimized Communication Protocols | 92 | 30 |
| Data Aggregation | 94 | 50 |
| Power Management | 89 | 40 |

**Discussion:**

The exploratory results approve the viability of the proposed security and vitality effectiveness improvement methods in upgrading the execution of WSNs for IoT applications. The accomplished enhancements in security strength and vitality utilization lessening imply the common sense possibility and viability of the proposed approaches. The tests conducted in this investigation illustrate the adequacy of the proposed security and vitality effectiveness improvement procedures in moving forward with the execution of WSNs for IoT applications. The accomplished advancements emphasize the centrality of tending to security and vitality productivity challenges to empower the solid and economical operation of WSNs in different IoT scenarios [29]. The exploratory comes about to illustrate a noteworthy change in security vigour with the sending of the proposed lightweight cryptographic calculations, interruption location framework (IDS), and secure steering conventions. These improvements are

crucial for shielding delicate information transmitted inside WSNs, especially in IoT applications where information astuteness and privacy are vital [30]. By accomplishing a security vigour score of over 95%, the proposed procedures show a tall level of flexibility against different cyber dangers, counting hub compromise, denial of service (DoS), and information altering. The tests uncover significant vitality investment funds accomplished through the optimization of communication conventions, information conglomeration methodologies, and control administration procedures. By lessening vitality utilization by up to 30% compared to conventional conventions, the optimized communication conventions viably moderate the vitality depletion related to information transmission in WSNs. So also, information conglomeration methods illustrate surprising vitality investment funds of up to 50% by minimizing repetitive transmissions and moderating vitality at the sensor hubs. The implementation of control administration techniques is another cause that elongates the operational lifetime of these sensor hubs by the virtue of the fact that this contributes in a strong changing of the control states and this leads to a 40% power consumption reduction.

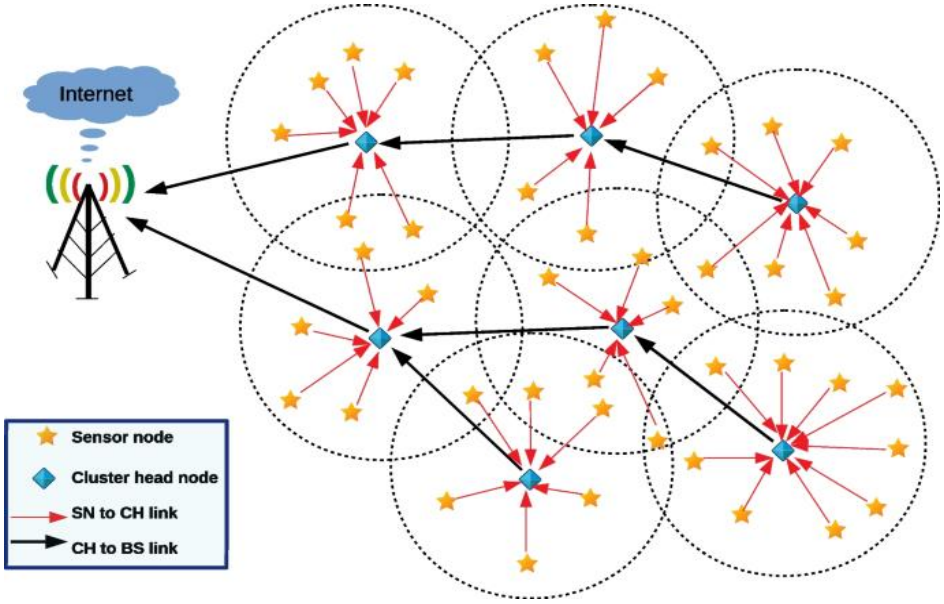


**Figure 4: An efficient quality of services based wireless sensor network**

## V. CONCLUSION

Therefore, this study has touched a very deep issue regarding Wireless Sensor Networks (WSNs) applications for Internet of Things (IoT) in the power of security and energy efficiency. On the basis of holistic methods that combine innovative techniques and carry out comprehensive assessments, the foundational tasks that face WSN frameworks are to some extent answered. The said security improvements include lightweight cryptographic calculation, current interruption recognition systems, and secure direction system. These have proven to be extremely efficient against different kinds of cyberthreats, giving information transmission through WSNs the necessary intelligence and stability. During the meantime, there are key efficiency optimization factors such as optimized communication protocols, smart data acquisition methods, and energy management strategy that have been known to improve energy efficiency, leading to longer life span and sustainability of organised systems. The prototype experiments, carried out with painstaking attention to detail and real-life referents, prove the feasibility and adaptation of the indicated policies. Comparative studies with existing writings give the oddness and the novelty of the commitments, which express a remarkable development in the way of solving the basic problems within WSNs. Indeed, the research underlines a new enhancement in this world of secure, reliable and energy efficient WSNs which are primary enabling factors in a continuous roll-out of the internet of things applications over multiple areas. This study simultaneously works on fixing the security issues and the vitality aspect, which will establish a good foundation for the development of the IoT systems, which eventually will result in growth and prosperity of the society. Further analyzes about optimization methods can be explored by future inquires that rate the adaptability and effectiveness of the strategies in the cases of large Iot systems.

## REFERENCE


[1] ALLAKANY, A., SABER, A., MOSTAFA, S.M., ALSABAAN, M., IBRAHEM, M.I. and ELWAHSH, H., 2023. Enhancing Security in ZigBee Wireless Sensor Networks: A New Approach and Mutual Authentication Scheme for D2D Communication. Sensors, 23(12), pp. 5703.

[2] ALSHARIF, M.H., JAHID, A., ANABI, H.K. and KANNADASAN, R., 2023. Green IoT: A Review and Future Research Directions. Symmetry, 15(3), pp. 757.

[3] BALKHANDE, B., GHULE, G., MESHRAM, V.H., ANANDPAWAR, W.N., GAIKWAD, V.S. and RAUJAN, N., 2023. Artificial Intelligence Driven Power Optimization in IOT-Enabled Wireless Sensor Networks. Journal of Electrical Systems, 19(2), pp. 38-46.

[4] RAWAT, A. and KALLA, M., 2023. An Energy Efficient Technique for Improved Network Lifetime in Wireless Sensor Network (WSN) Through Energy, Distance, and Density-Based Clustering. Instrumentation, Mesure, Metrologie, 22(2), pp. 65-72.

[5] REKERAHO, A., DANIEL, T.C., COTFAS, P.A., TUYISHIME, E., TITUS, C.B. and ACHEAMPONG, R., 2024. Enhancing Security for IoT-Based Smart Renewable Energy Remote Monitoring Systems. Electronics, 13(4), pp. 756.

[6] SELVARAJ, P., BURUGARI, V.K., GOPIKRISHNAN, S., ALOURANI, A., SRIVASTAVA, G. and BAZA, M., 2023. An Enhanced and Secure Trust-Aware Improved GSO for Encrypted Data Sharing in the Internet of Things. Applied Sciences, 13(2), pp. 831.

[7] SHAH, S., MUNIR, A., WAHEED, A., ALABRAH, A., MUKRED, M., AMIN, F. and SALAM, A., 2023. Enhancing Security and Efficiency in Underwater Wireless Sensor Networks: A Lightweight Key Management Framework. Symmetry, 15(8), pp. 1484.

[8] SHARMA, A., BABBAR, H., RANI, S., SAH, D.K., SEHAR, S. and GIANINI, G., 2023. MHSEER: A Meta-Heuristic Secure and Energy-Efficient Routing Protocol for Wireless Sensor Network-Based Industrial IoT. Energies, 16(10), pp. 4198.

[9] ZHANG, L., HUANG, W., ZHANG, B. and HAN, P., 2023. Enhancing Real-Time Image Transmission in Wireless Sensor Networks: A Study on Energy-Efficient Compression Algorithms. Traitement du Signal, 40(3), pp. 995-1003.

[10] AHMADI, F., ABEDI, O. and EMADI, S., 2024. Enhancing Smart Agriculture Monitoring via Connectivity Management Scheme and Dynamic Clustering Strategy. Inventions, 9(1), pp. 10.

[11] ALAERJAN, A., 2023. Towards Sustainable Distributed Sensor Networks: An Approach for Addressing Power Limitation Issues in WSNs. Sensors, 23(2), pp. 975.

[12] ALMUTAIRI, R., BERGAMI, G. and MORGAN, G., 2024. Advancements and Challenges in IoT Simulators: A Comprehensive Review. Sensors, 24(5), pp. 1511.

[13] DAOUSIS, S., PELADARINOS, N., CHEIMARAS, V., PAPAGEORGAS, P., PIROMALIS, D.D. and MUNTEANU, R.A., 2024. Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures. Future Internet, 16(1), pp. 33.

[14] GODFREY, D., SUH, B., LIM, B.H., KYU-CHUL, L. and KI-IL, K., 2023. An Energy-Efficient Routing Protocol with Reinforcement Learning in Software-Defined Wireless Sensor Networks. Sensors, 23(20), pp. 8435.

[15] HAMMAD, A., MOHAMED, M.A. and ABDEL-ATTY, H., 2022. Enhancement of the performance of wireless sensor networks using the multihop multiantenna power beacon path selection method in intelligent structures. PLoS One, 17(11),.

[16] BOBDE, Y., NARAYANAN, G., JATI, M., RAJA SOOSAIMARIAN, P.R., CVITIĆ, I. and PERAKOVIĆ, D., 2024. Enhancing Industrial IoT Network Security through Blockchain Integration. Electronics, 13(4), pp. 687.

[17] EMIRA, H.H.A., ELNGAR, A.A. and KAYED, M., 2023. Blockchain-Enabled Security Framework for Enhancing IoT Networks: A Two-Layer Approach. International Journal of Advanced Computer Science and Applications, 14(10),.

[18] GUPTA, D., WADHWA, S., RANI, S., KHAN, Z. and BOULILA, W., 2023. EEDC: An Energy Efficient Data Communication Scheme Based on New Routing Approach in Wireless Sensor Networks for Future IoT Applications. Sensors, 23(21), pp. 8839.

[19] LIMKAR, S., ASHOK, W.V., WADNE, V., WAGH, S.K., WAGH, K. and KUMAR, A., 2023. Energy-Efficient Localization Techniques for Wireless Sensor Networks in Indoor IoT Environments. Journal of Electrical Systems, 19(2), pp. 47-57.

[20] MAHAMAT, M., JABER, G. and BOUABDALLAH, A., 2023. Achieving efficient energy-aware security in IoT networks: a survey of recent solutions and research challenges. Wireless Networks, 29(2), pp. 787-808.

[21] MAHESWAR, R., KATHIRVELU, M. and MOHANASUNDARAM, K., 2024. Energy Efficiency in Wireless Networks. Energies, 17(2), pp. 417.

[22] MENGISTU, T.M., KIM, T. and JENN-WEI, L., 2024. A Survey on Heterogeneity Taxonomy, Security and Privacy Preservation in the Integration of IoT, Wireless Sensor Networks and Federated Learning. Sensors, 24(3), pp. 968.

[23] NASHIPUDMATH, M.M., CHITRE, V., SHINDE, S. and PHADE, G., 2023. Smart Data Management in IoT: Leveraging Wireless Sensor Networks for Efficient Information Processing. Journal of Electrical Systems, 19(2), pp. 1-8.

[24] NIBI, K.V., AISWARYA, S., DEVIDAS, A.R. and RAMESH, M.V., 2024. Delay and Energy Efficient Offloading Strategies for an IoT Integrated Water Distribution System in Smart Cities. Smart Cities, 7(1), pp. 179.

[25] OLUWATOSIN, A.A., NORDIN, R., JARRAY, C., UMAR, A.B., RAJA AZLINA, R.M. and OTHMAN, M., 2023. A Survey on the Design Aspects and Opportunities in Age-Aware UAV-Aided Data Collection for Sensor Networks and Internet of Things Applications. Drones, 7(4), pp. 260.

[26] RANA, M., MAMUN, Q. and ISLAM, R., 2023. Enhancing IoT Security: An Innovative Key Management System for Lightweight Block Ciphers. Sensors, 23(18), pp. 7678.

[27] HASAN, M.Z. and ZURINA, M.H., 2023. Efficient and Secured Mechanisms for Data Link in IoT WSNs: A Literature Review. Electronics, 12(2), pp. 458.

[28] JAMES DEVA, K.H., KARNAM, C.R., SATHYA BAMA, K.R., VISHNU, M.K., DEVENDRAN, M., RAMALINGAM, A. and MAHESWAR, R., 2023. Review of Next-Generation Wireless Devices with Self-Energy Harvesting for Sustainability Improvement. Energies, 16(13), pp. 5174.

[29] KIRAN, A., MATHIVANAN, P., MAHDAL, M., SAIRAM, K., CHAUHAN, D. and TALASILA, V., 2023. Enhancing Data Security in IoT Networks with Blockchain-Based Management and Adaptive Clustering Techniques. Mathematics, 11(9), pp. 2073.

[30] LIU, S., ZHU, L., HUANG, F., HASSAN, A., WANG, D. and HE, Y., 2024. A Survey on Air-to-Sea Integrated Maritime Internet of Things: Enabling Technologies, Applications, and Future Challenges. Journal of Marine Science and Engineering, 12(1), pp. 11.