Poonam Tiwari, 2024, 12:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Survey on Wireless Sensor Network Optimization, Routing and Applications

Poonam Tiwari, Professor Rani Kushwaha
Mittal Group of Institutes, Bhopal, (M.P), INDIA

Abstract- A Wireless Sensor Network (WSN) represents an innovative type of embedded real-time device, which finds utility in numerous applications where traditional networking solutions are impractical or unfeasible. One of the primary challenges associated with WSNs is the energy production and consumption of the individual sensor nodes, which can significantly impact the overall stability and performance of the system. To address these challenges, researchers have developed a variety of methods and strategies aimed at reducing the energy consumption of wireless sensor networks. This paper provides a concise overview of the structure of WSNs, focusing particularly on optimizing communication through advanced routing techniques. Given the inherent vulnerability of these networks, the paper also delves into the specifics of various routing strategies designed to enhance network security and reliability. Additionally, the paper compiles some of the latest research efforts that not only aim to optimize energy usage within the network but also strive to increase its robustness and durability. Furthermore, the paper outlines several applications of WSNs, demonstrating their significant importance and the diverse contexts in which they can be effectively employed.

Keywords- Wireless Sensor Network, Communication Routing, Virtual machines.

I. INTRODUCTION

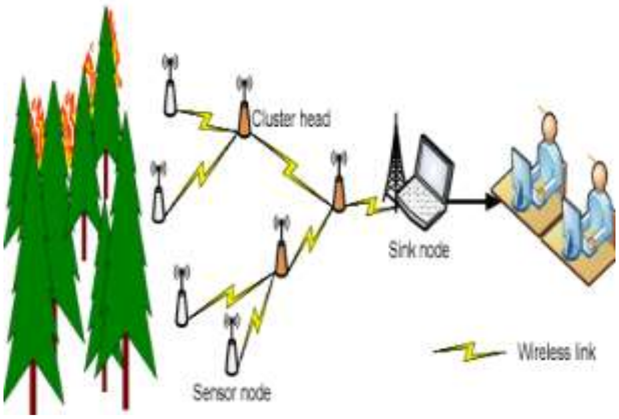
Wireless communication technologies are experiencing rapid and significant advancements. Over the past few years, there has been considerable growth in research dedicated to wireless sensor networks (WSNs). WSNs have emerged as one of the most valuable and practical technologies of the twenty-first century [1, 2]. These networks are composed of a large number of sensor nodes that are inexpensive, low-power, and multi-functional. These nodes can be deployed in a wide range of environments where they are needed to perform various tasks.

The advent of large-scale sensor networks, which can connect several hundred to a few thousand sensor nodes, introduces numerous technical challenges along with vast application opportunities. WSNs have evolved from theoretical research subjects to practical tools used in real-world applications, facilitated by the commercial availability of sensors equipped with networking capabilities. Companies like Crossbow and Sensoria have emerged as leading suppliers, providing the essential hardware and software building blocks necessary for these networks [3, 4].

This work places a particular emphasis on the security issues associated with WSNs. Typically, WSNs are employed to gather data from different areas of the physical world and are deployed in both controlled and uncontrolled locations. This inherent deployment nature makes wireless sensor networks vulnerable to security threats. These networks face a variety of limitations, including [5, 6]:

- **Node Limitations:** The individual sensor nodes possess limited computational power, memory, and energy.
- **Network Limitations:** The network often functions as a mobile ad-hoc network, which presents additional challenges.
- **Physical Limitations:** WSNs are often deployed in diverse environments, including public spaces and hostile settings, increasing their susceptibility to security attacks.

One of the main challenges affecting the security and reliability of sensor networks is their ad-hoc nature. Due to the restricted computational and processing capacities of the sensor nodes, conventional security methods and strategies are not suitable for maintaining essential security aspects such as authentication, availability, and integrity in WSNs. These networks are particularly vulnerable to both external and internal attacks, given that they consist of numerous devices with limitations such as limited memory, low energy reserves, and reduced battery power [7]. Communication in WSNs occurs over wireless links, which further exacerbates security concerns.



Despite extensive research efforts, many security issues remain unresolved, making security one of the most pressing research areas in the field of WSNs. The deployment of WSNs in hostile environments adds to the complexity of ensuring their security. This paper aims to underscore these security vulnerabilities and discuss various potential solutions for enhancing the security and reliability of wireless sensor networks.

In summary, the rapid development of wireless communication technologies, coupled with the increasing deployment of WSNs, underscores the importance of addressing their inherent security challenges. This work highlights the critical need for robust security strategies tailored to the unique constraints of WSNs to protect them against a wide array of security threats, thereby ensuring their effective and reliable operation in various applications and environments.

II. WSN STRUCTURE

WSN Sink

The core components of a Wireless Sensor Network (WSN) are the sensor nodes, which are crucial for the network’s functioning. These nodes collect raw data that must be processed before it can be utilized effectively. This "data" can include aggregated statistical information or detailed measurements of various factors indicating the state of an object or environment. One of the key applications of WSNs is tracking and monitoring moving objects such as vehicles, animals, and people.

WSNs with the Cluster Structure

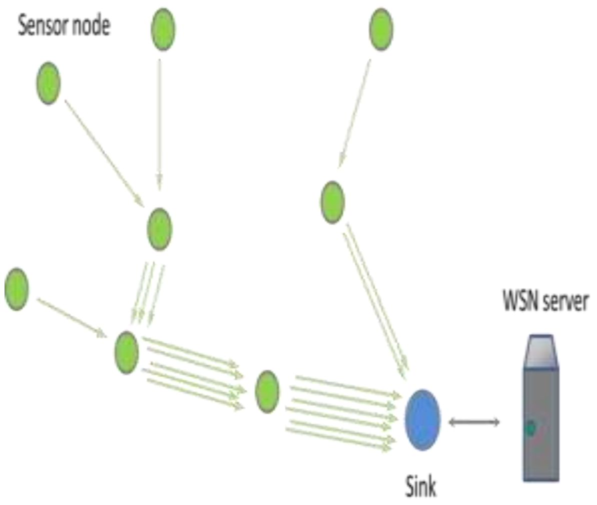


Figure 2: Data streaming from sensor nodes.

However, due to the limited computational power and energy efficiency of sensor nodes, they typically cannot handle complex data processing. Instead, this task is usually delegated to the WSN server, which performs the final data processing steps. The WSN server is linked to the network through a single sink or base station sensor node. The sink collects data from all the sensor nodes and communicates with the WSN server, acting as an intermediary.

Efficient use of the limited and nonrenewable energy stored in sensor nodes is critical. Figure 2 illustrates how data travels from sensors to a collection point. Periodically, the sink gathers information from all sensors, with each arrow in the figure representing the transfer of a specific number of measurements over a given time period.

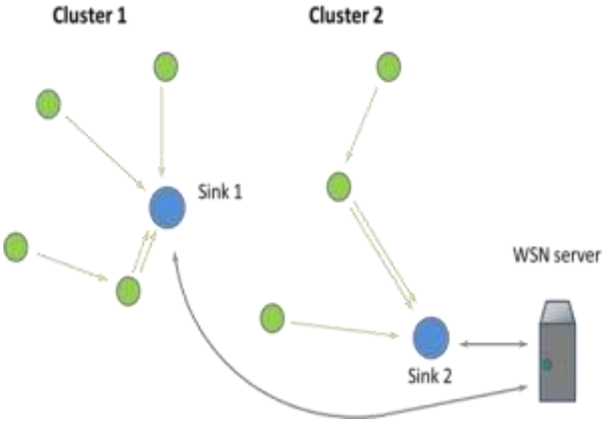


Figure 3: Multiple-sink WSN

Because all sensor nodes participate in data gathering, those closest to the sink must also relay measurements from distant nodes. This leads to the transceivers of nearby nodes retransmitting significantly more data, resulting in higher energy consumption. Consequently, the nearest sensor nodes exhaust their energy much sooner than those farther away, disrupting network operations since all nodes are of the same type and have the same energy capacity.

In applications requiring periodic data collection, this frequent retransmission dramatically reduces the operational lifespan of the nodes closest to the sink. As the WSN grows, the volume of data transmitted increases, making a single-sink network inefficient from an energy perspective.

Multiple-sink To address this issue, WSNs can be divided into smaller networks or clusters, each with its own sink. These clusters operate as individual WSNs, each communicating independently with the central hub. Figure 3 shows a system with two sinks, demonstrating that the number of retransmissions is significantly reduced, alleviating the load on sensor nodes near the sinks. The subdivision of a WSN into clusters is not arbitrary but typically occurs automatically during deployment and usage. The destination for data from a sensor node is determined by the WSN protocol's algorithm, which considers criteria such as minimal data transfer time, fewest retransmissions, and balanced traffic distribution across nodes.

WSN gateway In discussing WSN organizational schemes, it has been assumed that all parts of the WSN are located in the same physical area. However, remote access to WSN data is often necessary. For example, a WSN deployed in a suburban forest might need to send data to a city center for processing. To facilitate this, specialized gateways receive data from the sink and retransmit it using different wireless communication standards, ensuring delivery to a remote server. Figure 4 illustrates how a WSN server can be connected via the Internet.

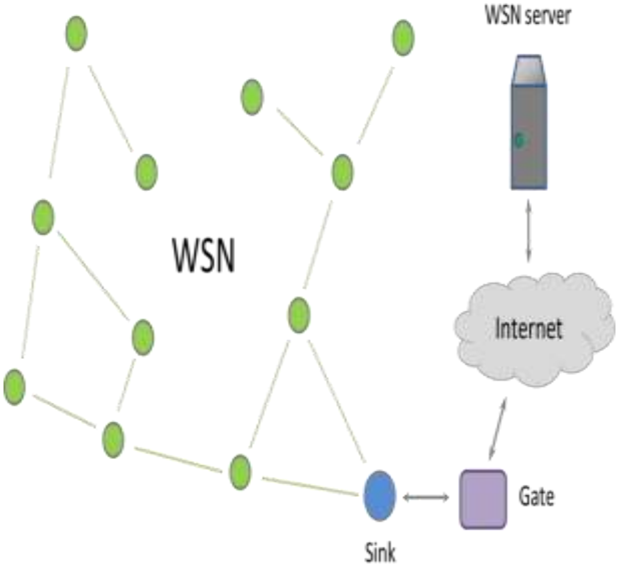


Figure 4: WSN server is connected via the Internet

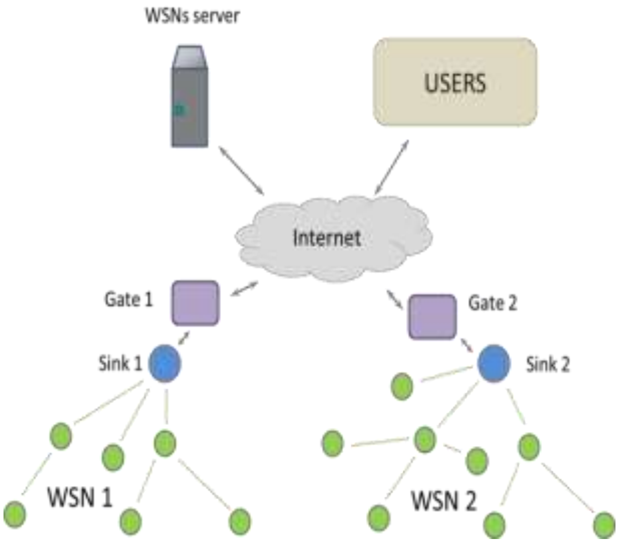


Figure 5: Scheme of provision of WSN services

Gateways also enable the coordination of service delivery. In the modern era, connecting WSNs to the Internet is straightforward due to ubiquitous connectivity options like cellular, cable, and satellite networks [11]. Figure 5 depicts the user-WSN interaction pattern, highlighting the integration of WSNs with broader communication networks. This comprehensive structure allows for efficient data collection, processing, and utilization in various applications, ensuring robust and scalable WSN deployments.

III. RELATED WORK

Longteng et. al. in [12] proposed a chaotic substitution box which was also known as S-Box was used for the security of wireless nodes. Use chaotic shuffling for security enhancing of data increases energy loess as more shuffling or rounds need processor execution time which ultimately enhance the energy requirement. It was found that wireless nodes clustering has reduced its communication cost.

Turki A. et. al. in [13] works on WSN energy and security optimization by involving the clustering based data transmission to the base station. However self organized technique was used by the work for clustering leads to congestion in network as most node wait for their data transfer turn. Hence this paper security by Dij-Huff method was good for security but self organized technique for clustering reduce the network performance.

Zhiqiang Liu, et.al. [14] resolved the buffering problem by finding the long term and short term packet waits. This paper has proposed a greedy sub optimal resource allotment for buffer utilization when transmitting data from sensor to sink node. Whole work focus on resource management but energy optimization was missing and life span of network get reduced.

Jingjing Yan et. al. in [15] summarized various misuses of WSN where energy optimization and routing has its own importance. It was showed in paper that scholars has proposed different clustering algorithm but for dynamic adoption algorithm compromised some other parameter like high machine requirement for calculation, limited area, security, etc. It was obtained that routing of packet by cluster center node always increase the life span of network.

Suraj Sharma, et. al. in [16] has proposed a grid based data routing to the base station. In this model network was divided into equal size grid and one node from the grid transfer data to the next node of other grid. Node grids were in active or sleep state as per sequence. This sleeping and active concept increase the energy utilization of the work. But in this paper when grid node in sleep state then other node seek near by active grid node this increase communication cost of the work, which increases the energy waste in the system.

Mohit Mittal et. al. in [17], proposed an Levenberg–Marquardt neural network (LMNN) to improve performance in terms of energy efficiency. Furthermore, a sub-cluster LEACH-derived methodology is developed in order to improve performance. The Sub-LEACH with LMNN surpassed its competitors in terms of energy efficiency, according to simulation data. Furthermore, the end-to-end delay was assessed, and the Sub-LEACH technique was shown to be the most effective among existing solutions. Furthermore, an intrusion detection system (IDS) based on the support vector machine (SVM) approach for optimal feature selection has been presented for anomaly detection.

G. Jegan et. al. in [18], proposed an Energy Efficient Intrusion Detection System (EE-IDS) for IEEE 802.15.4-based WSNs that has been proposed to detect and reduce the effect of wormhole attacks. Statistical Analysis/Methods: Using the enhanced watchdog system, the wormhole attack is identified. The optimal watchdog mechanism is a trust-based approach for determining the authenticity of all of the network's nodes. The suggested approach optimizes the selection of watchdog nodes in order to consume less energy than previous approaches. The three primary variables of trustworthiness, packet delivery ratio, and end-to-end delay are also used to detect wormhole attacks. Findings: The proposed EE-IDS is put through its paces in thorough simulations, taking into account both static and mobile models, before being compared to existing IDS for detecting wormhole assaults.

W. Xu et. al. in [19], identifies four types of attacks. The first strategy is based on signal strength, because signal strength might fluctuate abnormally during an attack. The Carrier sense intervals are the second method. During an attack, the Carrier sense intervals are widened. Controlling packet arrival rates is the other option. These values, of course, are insufficient on their own. Under certain circumstances, these ratios may exhibit unexpected changes even if there is no attack on existing nodes in the network.

S. Anitha et. al. in [20], presented a secured Ant Colony Optimization (SACOP) based on a trust sensing model. To begin, the malicious node in the clustered network is identified by estimating the node's trust value using direct and indirect trust evaluation models. Second, the ant colony routing algorithm is used to identify the secure best path for data forwarding by using probability to select the next hop node. Energy expenditure among all nodes is balanced since the likelihood is determined using residual energy, trust, and pheromone levels.

S. K. Chaurasiya et. al in [21], proposed an Energy-Efficient Hybrid Clustering Technique for IoT-based HWSN that minimizes the energy consumption in clusters' formation and distributes the network load evenly irrespective of the heterogeneity level to prolong network lifetime. It appropriately utilizes dynamic and static clustering strategies to formulate the load-balanced clusters in the network. EEHCT establishes its supremacy over state-of-the-art schemes via an extensive set of simulations and experimentation in terms of multiple network performance metrics like stability, throughput, and network lifetime.

IV. ROUTING IN WSN

One of the primary goals of WSN setup is information exchange while making an effort to extend the lifespan of the system and prevent integration degradation via the use of robust energy management techniques [11, 22]. Several factors in testing have been found to impact the setup of steering conventions.

Node Deployment WSNs allow for manual (deterministic) or random node organization, depending on the needs of the application. Sensors are physically placed and information is routed in predetermined ways in manual transmission. In contrast, in an ad hoc configuration, the nodes are placed at random to form a guiding structure.

Energy Consumption The battery life of a sensor node is a major factor in how long it will last. Each node in a multi-bounce WSN acts as both a data transmitter and a data router. Some sensor nodes failing as a result of power failure might result in significant topological changes, necessitating the possible rerouting of packets and a complete overhaul of the system.

Fault Tolerance Lack of force, bodily injury, or natural impedance might cause certain sensor nodes to fall short or be blocked. Failures at individual sensor nodes shouldn't have an effect on the system as a whole. The alternative path that may be used to route the data to the sink node has to be the primary focus of the steering convention.

Scalability Sensor nodes in the detection area might number in the hundreds, thousands, or even millions. In order to manage steering among the many sensor nodes, any proposed strategy must be able to be scaled up. Nodes in the sensor network are typically in a dormant state and are switched to an active one when an event is detected.

Coverage Every sensor node in a WSN has its own unique view of the planet. The range and precision of any one sensor's view of Earth are limited. There is a limited geographical area it can reach. Therefore, the scope of the communication's range is also an important WSN design option. In a WSN, information is exchanged between nodes as it travels across the network. However, there are many uses for sensor systems that need knowledge of node area. This regional information allows early anticipation of the wonder, so reducing the severity of any potential dangerous catastrophe. The nodes' area information contributed in the easy finding of a guiding path between the source and the destination, which reduced the amount of lag time inherent in the data transmission process.

V. APPLICATION OF WSN

Many of application area of WSN network that need to be secured from intruders are:

- **Environmental Applications:** Environmental applications that demand continuous monitoring of ambient conditions at hostile and remote areas can be improved with the utilization of WSNs.
- Patient Wearable Monitoring Health monitoring applications can be combined with wearable hardware with embedded biomedical sensors that provide the patient’s health status in a remote environment or within a healthcare facility.
- Military Applications The military domain is not only the first field of human activity that used WSNs but it is also considered to have motivated the initiation of sensor network research.
- Emergency Alerting Proactive monitoring of the causes of natural disasters, can help to avoid these disasters or/and lower their cost. WSNs can be utilized for monitoring common disastrous causes in real time to provide proactive alerts in order to lower damage or even prevent disaster.

VI. CONCLUSION

Given the limited energy supply of battery-powered sensor nodes, extending the lifespan of Wireless Sensor Networks (WSNs) is a critical concern. This paper highlights that numerous researchers have enhanced WSNs by boosting the capacity of sensor nodes and optimizing their architecture. Improving the network's lifespan hinges significantly on efficient energy usage. This study finds that node routing based packet movement. Additionally, ensuring the robustness of the network is crucial due to its open nature and limited channel range. Various application were possible by WSN networks were also discuss in the paper. Future research can focus on developing models that minimize energy waste while further improving the network's robustness.

REFERENCES

1. Azarhava, H.; Niya, J.M. Energy efficient resource allocation in wireless energy harvesting sensor networks. IEEE Wirel. Commun. Lett. 2020, 9, 1000–1003.
2. Erdelj, M.; Mitton, N.; Natalizio, E. Applications of industrial wireless sensor networks. In Industrial Wireless Sensor Networks: Applications, Protocols, and Standards; CRC Press: Boca Raton, FL, USA, 2013; pp. 1–22.
3. Manfredi, S.; Tucci, E.D. Decentralized control algorithm for fast monitoring and efficient energy consumption in energy harvesting wireless sensor networks. IEEE Trans. Industr. Inform. 2003, 13, 1513–1520.
4. Harb, H.; Makhoul, A. Energy-efficient sensor data collection approach for industrial process monitoring. IEEE Trans. Industr. Inform. 2017, 14, 661–672.
5. Xie, J.; Zhang, B.; Zhang, C. A Novel Relay Node Placement and Energy Efficient Routing Method for Heterogeneous Wireless Sensor Networks. IEEE Access 2020, 8, 202439–202444.

6. Liu, X.; Wu, J. A method for energy balance and data transmission optimal routing in wireless sensor networks. Sensors 2019, 19, 3017.
7. Hung, L. Energy-Efficient Cooperative Routing Scheme for Heterogeneous Wireless Sensor Networks. IEEE Access 2020, 8, 56321–56332.
8. Cui S, Cao Y, Sun G, et al. A new energy-aware wireless sensor network evolution model based on complex network. EURASIP J Wireless Commun Netw 2018; 2018(1): 218.
9. Kim B-S, Park H, Kim KH, et al. A survey on real-time communications in wireless sensor networks. Wireless Commun Mob Comput 2017; 2017: 1864847.
10. Behera TM, Samal UC, Mohapatra SK. Energy-efficient modified leach protocol for IoT application. IET Wireless Sens Syst 2018; 8(5): 223–228.
11. Shazana Md Zin, Nor Badrul Anuar, Miss Laiha Mat Kiah, Al-Sakib Khan Pathan, Routing protocol design for secure WSN: Review and open research issues, Journal of Network and Computer Applications, Volume 41, 2014.
12. Longteng Yi, XiaojunTong , Zhu Wang, Miao Zhang, Honghong Zhu, And Jing Liu "A Novel Block Encryption Algorithm Based On Chaotic S-Box For Wireless Sensor Network " IEEE Access Volume: 7 2019.
13. Turki A. Alghamdi "Secure And Energy Efficient Path Optimization Technique In Wireless Sensor Networks Using DH Method" IEEE Access Volume: 6 2018.
14. Zhiqiang Liu, Bin Liu, And Chang Wen Chen "Buffer-Aware Resource Allocation Scheme With Energy Efficiency and QoS Effectiveness in Wireless Body Area Networks" IEEE Access Volume 52017.
15. Jingjing Yan, Mengchu Zhou, And Zhijun Ding, "Recent Advances in Energy-Efficient Routing Protocols for Wireless Sensor Networks: A Review" IEEE Access Volume: 42016.
16. Suraj Sharma, Deepak Puthal, Sabah Tazeen, Mukesh Prasad, And Albert Y. Zomaya . "MSGR: A Mode-Switched Grid-Based Sustainable Routing Protocol for Wireless Sensor Networks". IEEE access October 12, 2017.
17. Mohit Mittal, Rocío Pérez de Prado, Yukiko Kawai, Shinsuke Nakajima and José E. Muñoz-Expósito. "Machine Learning Techniques for Energy Efficiency and Anomaly Detection in Hybrid Wireless Sensor Networks". MDPI Energies 2021.
18. G. Jegan and P. Samundiswary "Wormhole Attack Detection in Zigbee". Indian Journal of Science and Technology, Volume: 9, Issue: 45 2016.
19. W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '05), pp. 46–57, Chicago, Ill, USA, May 2005.
20. S. Anitha, P. Jayanthi, K. Lalitha and V. Chandrasekaran. "Secured Ant Colony Optimization based on Energy Trust System for Replica Node Attack Detection". International Journal on Emerging Technologies 11(2): 2020.
21. S. K. Chaurasiya, S. Mondal, A. Biswas, A. Nayyar, M. A. Shah and R. Banerjee, "An Energy-Efficient Hybrid Clustering Technique (EEHCT) for IoT-Based Multilevel Heterogeneous Wireless Sensor Networks," in IEEE Access, vol. 11, pp. 25941-25958, 2023.
22. Manuel, A.J.; Deverajan, G.G.; Patan, R.; Gandomi, A.H. Optimization of Routing-Based Clustering Approaches in Wireless Sensor Network: Review and Open Research Issues. Electronics 2020, 9, 1630.