Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January 2024 5(1), 479–484

IMPACT OF MACHINE LEARNING-BASED ROUTING PROTOCOLS FOR EFFICIENT DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS (WSNS)

Anand Kumar Dwivedi[1], Virendra Tiwari[2], Akhilesh A. Waoo[3]

[1] Department of Computer Science & Engineering, AKS University, SATNA, MP, India

ABSTRACT

Wireless Sensor Networks (WSNs) play a pivotal role in collecting and disseminating data in various applications, ranging from environmental monitoring to healthcare. The efficiency of data transmission in WSNs greatly depends on the routing protocols employed. In recent years, machine learning techniques have emerged as promising tools to enhance the performance of routing protocols in WSNs.

This review paper aims to provide a thorough examination of the impact of machine learning-based routing protocols on the efficiency of data transmission within Wireless Sensor Networks. This research delves into the fundamental challenges faced by traditional routing protocols in WSNs, such as energy consumption, network congestion, and dynamic environmental conditions. Subsequently, this research explores the application of machine learning algorithms, including supervised and unsupervised learning, reinforcement learning, and deep learning, in addressing these challenges.

Through a comprehensive analysis of the existing literature, this research highlights the strengths and limitations of various machine learning-based routing protocols. Moreover, this research discusses their adaptability to dynamic network conditions, scalability, and ability to optimize resource utilization. The aim is to provide researchers, practitioners, and stakeholders with valuable insights into the current state-of-the-art machine learning-based routing protocols for WSNs.

Keywords: Wireless Sensor Networks (WSNs), Routing protocols, Machine learning techniques, Data transmission efficiency, Environmental monitoring, Healthcare, Energy consumption, Dynamic network conditions

Corresponding Author

Akhilesh A. Waoo,
akhileshwaoo@gmail.com

DOI
10.29121/shodhkosh.v5.i1.2024.1874

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

A Wireless Sensor Network (WSN) comprises a network of distributed sensor nodes responsible for monitoring physical conditions or events. However, the deployment of WSNs poses various challenges, including design, implementation, data fusion, Energy Efficient Routing (EER), clustering, localization, scheduling, quality of service (QoS), and security [1]. These challenges arise from inherent limitations such as constrained processing power, limited storage capacity, restricted network bandwidth, and finite battery power.

1.1 WSN

WSNs involve diverse monitoring tasks, such as tracking vehicles on highways or observing object movement. The primary strength of WSNs lies not in the individual sensor nodes but in the collective interconnection of these nodes. Consequently, WSNs are expected to be extensive in scale due to their large number of nodes and their inherent self-configuring capability, essential for ensuring reliability.

Due to the cost-effectiveness of wireless sensor nodes, a significant quantity of these nodes is typically deployed within a WSN. Communication among sensor nodes occurs through a multi-hop scheme. Information flow and data transmission terminate at specific nodes known as base stations or sinks. These sink or base stations usually link the sensor network to a fixed network, facilitating the dissemination of sensed data for further processing [2].

In general, base stations possess superior capabilities compared to regular nodes. Equipped with advanced processors like PCs/laptops, featuring additional RAM, secondary storage, batteries, and computational power, base stations can handle more complex tasks than regular sensor nodes.

It is crucial to note that one of the major drawbacks of sensor networks is their power consumption, significantly influenced by the interaction between nodes.

2. ENERGY-EFFICIENT ROUTING IN WIRELESS SENSOR NETWORKS (WSNS)

It involves categorizing routing protocols based on how information is obtained, maintained, and utilized to compute paths. WSN devices face resource constraints with low processing speed, limited storage, communication bandwidth, and battery power. Implementing energy-efficient routing protocols becomes crucial to extend the network's lifetime. The performance of routing protocols is influenced by network architecture and design, impacting the energy expended during data transmission.

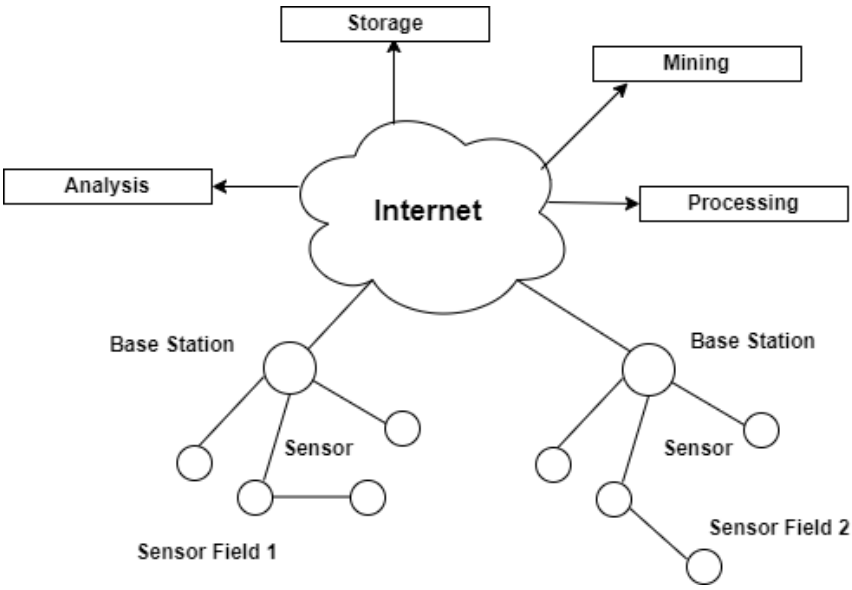

Fig.1: Structure of wireless sensor network

Energy consumption in WSNs primarily occurs during the Sensing, Processing, and Communication phases. In sensing, energy is used for sampling, analog-to-digital conversion, and modulation, influenced by node operation states (periodic, sleep/wake, etc.). Processing involves managing sensors, communicating protocols, and processing data, supporting three states of operation: sleep, idle, and run. Communication's energy consumption depends on data route complexity, distance between nodes, and transmission to the sink node or multiple sink nodes.

Communication protocols have a pivotal role in minimizing energy consumption during data transmission from source to destination. The objective is to find the most energy-efficient path and extend the network's lifetime, achieved through the utilization of Machine Learning (ML) algorithms.

3. CHALLENGES IN ENERGY-EFFICIENT ROUTING

The hurdles in achieving energy-efficient routing in Wireless Sensor Networks (WSNs) arise from the fundamental limitations of sensor nodes, such as their finite battery capacity and the imperative of sustaining network longevity. Conventional routing protocols frequently fall short of effectively tackling these obstacles, resulting in ineffective energy management and premature exhaustion of node resources. Furthermore, the dynamic landscape of WSN environments compounds energy consumption challenges, as nodes must navigate fluctuating conditions while upholding the most efficient routing pathways. Striking a balance between conserving energy and ensuring dependable data delivery

remains a paramount issue, prompting the exploration of innovative remedies like machine learning-driven methods for refining energy-efficient routing protocols.

a. **Resource-Constrained Devices:** Wireless Sensor Networks (WSNs) often comprise devices with limited processing speed, storage capacity, communication bandwidth, and battery power, posing a challenge to designing energy-efficient routing protocols.
b. **Network Architecture and Design:** The effectiveness of energy-efficient routing protocols is closely tied to the overall architecture and design of the sensor network. Ensuring optimal performance requires addressing these architectural considerations.
c. **Dynamic Environmental Conditions:** WSNs operate in dynamic environments where environmental conditions can change rapidly. Adapting routing protocols to varying conditions poses a challenge in maintaining energy efficiency.
d. **Communication Overhead:** The communication overhead associated with routing protocols can contribute significantly to energy consumption. Minimizing unnecessary communication while ensuring effective data transmission is a persistent challenge.
e. **Route Optimization:** Achieving the balance between finding the most energy-efficient route and optimizing the network's overall performance is a challenge. Routing protocols must consider factors such as distance, data complexity, and the need to extend network lifetime.
f. **Implementation of Machine Learning:** Integrating Machine Learning (ML) algorithms into routing protocols introduces the challenge of selecting, implementing, and optimizing these algorithms to enhance energy efficiency effectively [36].
g. **Data Transmission Distances:** The distance between sensor nodes directly impacts energy consumption during data transmission. Developing strategies to manage energy consumption efficiently over varying distances is a key challenge.
h. **Environmental Impact:** Energy-efficient routing protocols must be designed to minimize the environmental impact of WSNs. Balancing the need for data transmission with environmental sustainability is a challenge.
i. **Network Scalability:** As WSNs may consist of a large number of nodes, scalability becomes a challenge. Ensuring that energy-efficient routing protocols can scale effectively to accommodate network growth is essential.
j. **Security Concerns:** Integrating security measures into energy-efficient routing protocols is challenging, as the trade-off between energy efficiency and security must be carefully managed to prevent vulnerabilities and attacks.

The energy consumed for receiving data (ERx) is expressed as a product of the number of data bits (k) and energy consumption per bit during reception (e_rx). Equation (1) demonstrates the proportional relationship between energy consumption and the number of data bits for a fixed distance, while longer distances between sensor nodes result in increased energy consumption.

4. ENERGY-EFFICIENT ROUTING (EER) PROTOCOLS

Here is a list of some well-known Energy-Efficient Routing (EER) Protocols for Wireless Sensor Networks (WSN), along with brief details about each:

1. **LEACH (Low-Energy Adaptive Clustering Hierarchy):** Description: LEACH is a widely adopted hierarchical routing protocol. It utilizes a clustering approach where sensor nodes elect cluster heads to reduce communication overhead and extend network lifetime.
2. **PEGASIS:** Description: PEGASIS employs a chain-based communication structure. Sensor nodes pass data to their adjacent neighbors in a sequential manner, minimizing energy consumption during transmission.
3. **SEP (Stable Election Protocol):** Description: SEP is another clustering-based protocol that aims to achieve energy balance among sensor nodes. It elects cluster heads based on a probabilistic approach to distribute energy consumption evenly.
4. **TEEN:** Description: TEEN focuses on event-based monitoring in WSN. It utilizes threshold-sensitive mechanisms to activate or deactivate sensor nodes, reducing unnecessary data transmission and saving energy.
5. **ACRP (Adaptive Clustering-based Routing Protocol):** Description: ACRP is designed to adjust the clustering structure based on network conditions dynamically. It adapts the cluster formation to balance energy consumption and prolong the network's overall lifetime.

6. **MTE (Multicast Tree-based Energy-Efficient Routing Protocol):** Description: MTE employs a multicast tree structure to optimize data transmission in WSN. It aims to minimize energy consumption by efficiently routing data to multiple destinations simultaneously.
7. **CBEERP (Cross-Layer Based Energy-Efficient Routing Protocol):** Description: CBEERP integrates cross-layer information to make routing decisions. It considers factors from multiple protocol layers, enhancing energy efficiency by incorporating diverse network parameters.
8. **DEEC (Distributed Energy-Efficient Clustering):** Description: DEEC is a distributed clustering protocol that dynamically adjusts cluster formation. It aims to enhance energy efficiency by taking into account both residual energy and distance to the base station during the process of cluster head election.
9. **MHV (Minimum Hop-count Variant):** Description: MHV focuses on minimizing the hop count in routing paths. It aims to reduce the number of relay nodes and, consequently, energy consumption during data transmission.
10. **MGSR (Mobility-based Greedy and Sleep Routing):** Description: MGSR incorporates mobility patterns into routing decisions. It leverages information about node mobility to optimize routing paths and conserve energy.

These protocols represent a variety of approaches to achieving energy-efficient routing in WSN, considering factors such as clustering, adaptive mechanisms, and multicast strategies. Researchers often tailor these protocols to specific application scenarios and network characteristics.

5. DISCUSSION

Exploring the impact of machine learning-based routing protocols on Wireless Sensor Networks (WSNs) reveals promising prospects for overcoming persistent obstacles. With machine learning algorithms at their core, WSNs gain the capacity to dynamically optimize routing decisions in response to the ever-changing network landscape, thereby bolstering efficiency and extending network longevity. Additionally, the innate capability of machine learning models to sift through vast datasets facilitates the recognition of subtle patterns and relationships, fostering the development of more resilient and adaptable routing mechanisms.

Moreover, the incorporation of machine learning methodologies presents a transformative opportunity for WSNs to transcend traditional routing frameworks. Through continuous learning and adaptation, routing protocols stand to enhance their ability to navigate the intricacies of diverse environmental contexts, all while curtailing energy consumption and alleviating network congestion. This evolution carries profound implications across various domains, ranging from environmental monitoring to industrial automation, where the seamless and energy-efficient transmission of data underpins informed decision-making and operational efficacy.

6. CONCLUSION

This comprehensive review sheds light on the pivotal role of machine learning-based routing protocols in enhancing data transmission efficiency within Wireless Sensor Networks (WSNs). The incorporation of machine learning techniques addresses significant challenges faced by traditional protocols, including energy consumption, network congestion, and dynamic environmental conditions. The analysis underscores the strengths and limitations of various machine learning-based protocols, emphasizing adaptability, scalability, and resource optimization.

By providing valuable insights into the current state-of-the-art, this review aims to guide researchers, practitioners, and stakeholders in leveraging machine learning for WSNs. The outlined challenges in energy-efficient routing underscore the need for innovative solutions, especially in the integration of machine learning algorithms. As WSNs continue to evolve, future research directions should focus on refining these protocols to meet the demands of dynamic network conditions and contribute to the sustainable development of sensor networks. This review contributes to the ongoing discourse on the intersection of machine learning and WSNs, paving the way for advancements in efficient data transmission protocols.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Abbas, G.; Mehmood, A.; Carsten, M.; Epiphaniou, G.; Lloret, J. Safety, Security and Privacy in Machine Learning Based Internet of Things. J. Sens. Actuator Netw. 2022, 11, 38.

Bajaj, K.; Sharma, B.; Singh, R. Integration of WSN with IoT applications: A vision, architecture, and future challenges. In Integration of WSN and IoT for Smart Cities; Springer: Berlin/Heidelberg, Germany, 2020; pp. 79–102.

Pavithran, D.; Shaalan, K.; Al-Karaki, J.N.; Gawanmeh, A. Towards building a blockchain framework for IoT. Clust. Comput. 2020, 23, 2089–2103.

Sinha, P.; Jha, V.K.; Rai, A.K.; Bhushan, B. Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. In Proceedings of the 2017 International Conference on Signal Processing and Communication (ICSPC), Coimbatore, India, 28–29 July 2017; pp. 288–293.

Panda, M. Security in wireless sensor networks using cryptographic techniques. Am. J. Eng. Res. (AJER) 2014, 3, 50–56.

Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine learning in IoT security: Current solutions and future challenges. IEEE Commun. Surv. Tutor. 2020, 22, 1686–1721.

Xu, L.D.; Lu, Y.; Li, L. Embedding Blockchain Technology Into IoT for Security: A Survey. IEEE Internet Things J. 2021, 8, 10452–10473.

Kumar, D.P.; Amgoth, T.; Annavarapu, C.S.R. Machine learning algorithms for wireless sensor networks: A survey. Inf. Fusion 2019, 49, 1–25.

Alsheikh, M.A.; Lin, S.; Niyato, D.; Tan, H.P. Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications. IEEE Commun. Surv. Tutor. 2014, 16, 1996–2018.

Bout, E.; Loscri, V.; Gallais, A. How Machine Learning Changes the Nature of Cyberattacks on IoT Networks: A Survey. IEEE Commun. Surv. Tutor. 2022, 24, 248–279.

Tahsien, S.M.; Karimipour, H.; Spachos, P. Machine learning based solutions for the security of Internet of Things (IoT): A survey. J. Netw. Comput. Appl. 2020, 161.

da Costa, K.A.P.; Papa, J.P.; Lisboa, C.O.; Munoz, R.; de Albuquerque, V.H.C. Internet of Things: A survey on machine learning-based intrusion detection approaches. Comput. Netw. 2019, 151, 147–157.

Ahmad, R.; Alsmadi, I. Machine learning approaches to IoT security: A systematic literature review. Internet Things 2021, 14, 100365.

Haji, S.H.; Ameen, S.Y. Attack and Anomaly Detection in IoT Networks using Machine Learning Techniques: A Review. Asian J. Res. Comput. Sci. 2021, 9, 30–46.

Faraj, O.; Megias, D.; Ahmad, A.M.; Garcia-Alfaro, J. Taxonomy and challenges in machine learning-based approaches to detect attacks in the Internet of things. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual, 25–28 August 2020; pp. 1–10.

Mamdouh, M.; Elrukhsi, M.A.I.; Khattab, A. Securing the Internet of things and wireless sensor networks via machine learning: A survey. In Proceedings of the 2018 International Conference on Computer and Applications (ICCA), Beirut, Lebanon, 25–26 August 2018; pp. 215–218.

Mehta, A.; Sandhu, J.K.; Sapra, L. Machine Learning in Wireless Sensor Networks: A Retrospective. In Proceedings of the 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, India, 6–8 November 2020; pp. 328–331.

Baraneetharan, E. Role of machine learning algorithms intrusion detection in WSNs: A survey. J. Inf. Technol. 2020, 2, 161–173.

Dener, M.; Al, S.; Orman, A. STLGBM-DDS: An Efficient Data Balanced DoS Detection System for Wireless Sensor Networks on Big Data Environment. IEEE Access 2022, 10, 92931–92945.

Kim, T.; Vecchietti, L.F.; Choi, K.; Lee, S.; Har, D. Machine Learning for Advanced Wireless Sensor Networks: A Review. IEEE Sens. J. 2021, 21, 12379–12397.

Ramotsoela, D.; Abu-Mahfouz, A.; Hancke, G. A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study. Sensors 2018, 18, 2491. [PubMed] Future Internet 2023, 15, 200 40 of 45

Ahmad, R.; Wazirali, R.; Abu-Ain, T. Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. Sensors 2022, 22, 4730.

Jesus, E.F.; Chicarino, V.R.; De Albuquerque, C.V.; Rocha, A.A.A. A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. Secur. Commun. Netw. 2018, 2018, 9675050.

Liao, Z.; Pang, X.; Zhang, J.; Xiong, B.; Wang, J. Blockchain on Security and Forensics Management in Edge Computing for IoT: A Comprehensive Survey. IEEE Trans. Netw. Serv. Manag. 2021, 19, 1159–1175.

Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. J. Netw. Comput. Appl. 2020, 149, 102481.

Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411.

Darla, S.; Naveena, C. Survey on Securing Internet of Things through Blockchain Technology. In Proceedings of the 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 16–18 March 2022; pp. 836–844.

Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in IoT: Challenges and solutions. Blockchain Res. Appl. 2021, 2, 100006.

Pohrmen, F.H.; Das, R.K.; Saha, G. Blockchain-based security aspects in heterogeneous Internet-of-Things networks: a survey. Trans. Emerg. Telecommun. Technol. 2019, 30, e3741.

Miglani, A.; Kumar, N. Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review. Comput. Commun. 2021, 178, 37–63.

Ifzarne, S.; Tabbaa, H.; Hafidi, I.; Lamghari, N. Anomaly detection using machine learning techniques in wireless sensor networks. J. Phys. Conf. Ser. 2021, 1743, 012021.

Tiberti, W.; Carmenini, A.; Pomante, L.; Cassioli, D. A Lightweight Blockchain-based Technique for Anti-Tampering in Wireless Sensor Networks. In Proceedings of the 2020 23rd Euromicro Conference on Digital System Design (DSD), Kranj, Slovenia, 26–28 August 2020; pp. 577–582.

Ismail, S.; Khoei, T.T.; Marsh, R.; Kaabouch, N. A Comparative Study of Machine Learning Models for Cyber-attacks Detection in Wireless Sensor Networks. In Proceedings of the 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 1–4 December 2021; pp. 1–5.

Kaur, R.; Kaur Sandhu, J. A Study on Security Attacks in Wireless Sensor Network. In Proceedings of the 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 4–5 March 2021; pp. 850–855.

Patel, N.R.; Kumar, S. Wireless Sensor Networks' Challenges and Future Prospects. In Proceedings of the 2018 International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 23–24 November 2018; pp. 60–65.

Sharma S; Waoo AA., (2023) An efficient machine learning technique for prediction of consumer behaviour with high accuracy, International Journal of Computing and Artificial Intelligence 2023; 4(1): 12-15, DOI: https://doi.org/10.33545/27076571.2023.v4.i1a.59