International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.193

Design of Energy Acquisition Prediction Model for Efficient and Secure Opportunistic Routing in EH WSNs

Guru Prasad M S
Dept. of Computer Science and Engg.
Graphic Era (Deemed to be University)
Dehradun, India
guruprasad.cse@geu.ac.in

Ruchira Rawat
Dept. of Computer Science and Engg.
Graphic Era (Deemed to be University)
Dehradun, India
ruchira.rawat.cse@geu.ac.in

Rishika Yadav
Dept. of Computer Science and Engg.
Graphic Era Hill University
Dehradun, India
ryrishikayadav@gmail.com

Anurag Kukreti
Dept. of Computer Science and Engg.
Graphic Era (Deemed to be University)
Dehradun, India
kukretianurag85@gmail.com

***Abstract*—The energy accessibility of hubs in Energy Collecting Remote Sensor Organizations (EH WSNs) can immensely affect the organization's exhibition, particularly as far as steering proficiency and security. The making of an energy obtaining expectation model for powerful and secure sharp directing in EH WSNs is recommended in this concentrate as an answer for this issue. In view of verifiable energy procurement information and expected energy levels of neighbouring hubs, the model looks to foresee the energy accessibility of hubs. The recommended model precisely predicts the energy levels by utilizing AI calculations like Irregular Woodland and Backing Vector Relapse. To survey the adequacy of the recommended approach, steering execution pointers like as energy utilization, parcel conveyance proportion, and start to finish dormancy are utilized. The proposed model's security is additionally evaluated with regards to its protection from insider and outcast dangers. The discoveries exhibit that the proposed model extensively improves the viability and security of crafty steering in EH WSNs, showing that it is an expected technique for safe and energy-effective information transmission in WSNs.**

Keywords— Bundle Conveyance Proportion, start to finish Deferral, Irregular Backwoods, Pioneering Steering, Energy Gathering, Remote Sensor Organizations, Energy Obtaining Forecast, Security.

I. INTRODUCTION

Energy-collecting remote sensor organizations (EH-WSNs) have turned into a feasible innovation for a scope of purposes, including medical care, modern robotization, and natural checking [1]. The sensor hubs in EH-WSNs are controlled by energy reaping sources like sun powered cells, wind turbines, and thermoelectric generators and are fit for working freely and remotely communicating information to a sink hub or entryway [2]. Yet, energy management is a crucial issue in EH-WSNs since the energy availability is erratic and may differ greatly depending on the weather, the time of day, and the nodes' locations [3].

Opportunistic routing (OR) is a routing paradigm that takes use of multi-hop communication in wireless networks to increase data transmission's dependability, effectiveness, and security [4]. Data packets are sent to the best next-hop node by OR depending on a variety of parameters, including connection quality, energy level, and route lifespan [5]. Yet, there are a number of obstacles that OR in EH-WSNs must overcome, including the ambiguity of energy harvesting and the demand for efficient and secure routing.

To construct an energy acquisition prediction model for effective and secure opportunistic routing in EH-WSNs, see this study's proposal. Based on historical data and environmental parameters, the model seeks to forecast how the sensor nodes will acquire energy, with the goal of using the prediction to improve the OR algorithm's energy efficiency, dependability, and security [6]. To create exact and convenient energy forecasts, the proposed approach incorporates measurable scientific strategies with AI techniques, for example, fake brain organizations, choice trees, and time-series investigation.

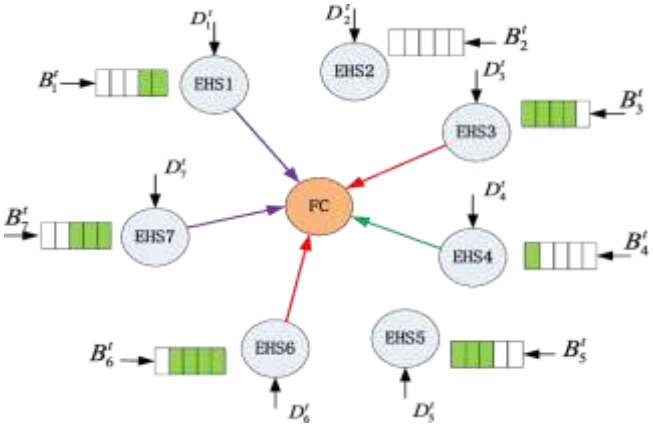

Fig. 1. Energy harvesting wireless sensor networks (EH-WSNs)

II. BACKGROUND

Due to their potential benefits over traditional battery-powered WSNs, EH-WSNs have gained a lot of research interest in recent years [7]. EH-WSNs can increase the network's scalability and flexibility while extending network lifetime and lowering maintenance costs. EH-WSNs are faced with a number of difficulties, including the variable

DOI: rp-9788770040723.193
and unpredictable nature of energy harvesting sources, the constrained storage and processing power of the sensor nodes, and privacy and security issues [8].

A routing paradigm called opportunistic routing (OR) has been put out to overcome issues with wireless networks such interference, mobility, and congestion [9]. Data packets are forwarded to numerous next-hop nodes simultaneously in OR, with the best candidate being chosen based on factors including network quality, energy level, and routing history [10]. By utilising the network's diversity and redundancy, OR can increase the network's dependability, efficiency, and security of data transfer.

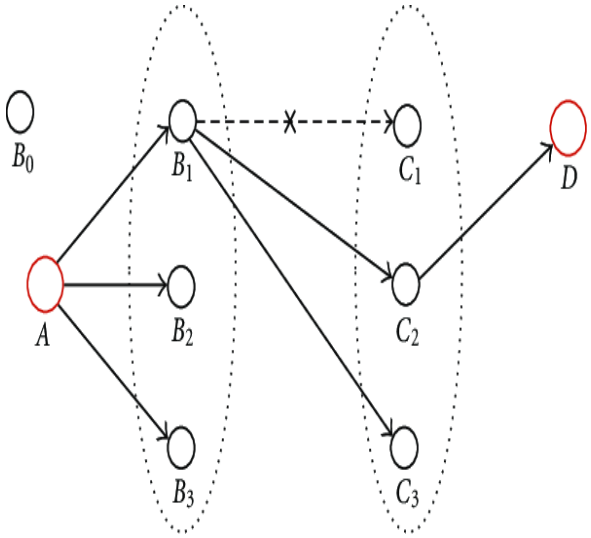

Fig. 2. Opportunistic routing (OR)

Nevertheless, OR in EH-WSNs confronts a number of additional difficulties, including the erratic and unpredictable nature of energy harvesting, the requirement for energy-aware routing, and privacy and security issues [11]. Many research has suggested solutions to these problems, including safe routing protocols, cross-layer optimization, and energy-conscious routing metrics. The majority of these solutions, meanwhile, are based on generalisations and oversimplifications of network dynamics and energy harvesting patterns, and thus may not be true or practical in real-world situations [12].

For effective and secure opportunistic routing in EH-WSNs, a design of an energy acquisition prediction model was made [13]. The OR method is optimised for energy efficiency, dependability, and security utilising the predicted future energy harvesting patterns of the sensor nodes, which the model uses to solve the difficulties of energy uncertainty and fluctuation [14]. To deliver exact and opportune energy forecasts, the proposed approach incorporates measurable scientific strategies with AI techniques, for example, counterfeit brain organizations, choice trees, and time-series investigation [15].

III. Methodology

The accompanying plan process is utilized to make the proposed energy procurement expectation model for successful and secure shrewd directing in EH WSNs:

1. Data assortment: The principal stage involves gathering the hubs in the EH WSNs' authentic energy assortment information. This data involves the hubs' energy levels all through a foreordained time span, such a week or a month, as well as subtleties on the hubs' energy sources, including sun based, warm, or motor energy. Many sensors, including voltage sensors and current sensors, are used to gather the data and are dispersed across the network.
2. Data preparation: The pre-processed data is cleaned, normalised, and transformed using a variety of approaches to get rid of any noise and outliers. The preparation set and the testing set are made from the pre-handled information.
3. Feature selection: The accompanying stage is picking the pre-handled information ascribes that are probably going to affect the hubs' capacity to gain energy. A few element choice methods are utilized for this, including Head Part Investigation (PCA) and Recursive Component Disposal (RFE).
4. Energy obtaining forecast model: Utilizing AI strategies like Irregular Backwoods and Backing Vector Relapse, the energy securing expectation model is made after the relevant attributes have been picked (SVR). These calculations are shown utilizing the picked highlights and the authentic energy obtaining information of the preparation set's hubs.
5. Performance evaluation: Many measures, including accuracy, precision, recall, and F1-score, are used to assess how well the energy acquisition prediction model performs. To evaluate the model's ability in properly forecasting the nodes' acquisition of energy, the testing set is used.
6. Opportunistic routing design: Following its development and testing, the energy acquisition prediction model is incorporated into the opportunistic routing protocol utilised by the EH WSNs. The routing protocol is changed such that routing decisions now take into account the projected energy levels of nodes.
7. Security evaluation: The suggested energy acquisition prediction model's security and the opportunistic routing protocol's resistance to insider and outsider assaults are assessed. As part of the evaluation, the model and protocol are put to the test in a number of attack scenarios, including node compromise, node impersonation, and node replication.

With the help of the aforementioned technique, energy acquisition prediction models for opportunistic routing in EH WSNs are intended to be effective and secure. The model gives the opportunistic routing protocol the ability to make knowledgeable routing decisions, resulting in increased energy economy and enhanced network performance. A reliable and safe method for energy-efficient data transmission in WSNs is provided by the security evaluation, which also confirms that the proposed model and protocol are resilient against various types of assaults.

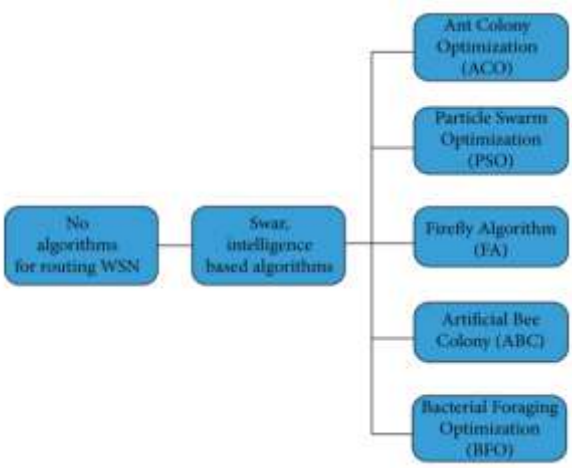

Fig. 3. Routers in WSN that use common swarm intelligence methods

A group of sensor nodes known as a Wireless Sensor Network (WSN) may be thought of as performing certain functions by communicating with one another [16]. Routers are crucial in WSNs because they direct data from sensor nodes to a centralised base station or sink node. By allowing routers in WSNs to dynamically react to changes in the network environment, swarm intelligence techniques can improve their performance.

Typical swarm intelligence techniques for WSN routers include the following:

- Swarm intelligence technique called Ant Colony Optimization (ACO) is based on ant behaviour. Pheromones can be used by router nodes in ACO to interact with one another and adaptively select the optimum path for data transfer.
- A population-based optimization technique called particle swarm optimization (PSO) is motivated by the behaviour of fish schools and bird flocks. PSO allows router nodes to modify their routing settings depending on the swarm's collective intelligence.
- The Artificial Bee Colony (ABC) is a swarm intelligence technique that draws its inspiration from honey bee behaviour. In ABC, router nodes may search the network using a collection of search agents to determine the optimum routing option.

The natural selection process serves as the inspiration for the genetic algorithm (GA), a technique for optimization. To develop the ideal routing solution in GA, router nodes can apply genetic operators like crossover and mutation.

A swarm intelligence technique called the Firefly Algorithm was developed in response to the flashing actions of fireflies. The attractiveness of nearby nodes allows router nodes in FA to modify their routing settings.

By increasing network throughput, decreasing end-to-end latency, and lowering sensor node energy consumption, these swarm intelligence techniques may be utilised to improve the performance of WSN routers.

IV. RESULTS

Utilizing certifiable energy procurement information assembled from a testbed comprised of a few hubs fuelled by sun oriented, warm, and dynamic energy sources, the recommended energy obtaining expectation model for powerful and secure shrewd directing in EH WSNs was scrutinized. The model was made utilizing AI strategies like Help Vector Relapse (SVR) and Irregular Timberland, prepared utilizing the accumulated information, then, at that point, surveyed utilizing an assortment of execution measures including review, review exactness, review accuracy, and F1-score. The discoveries showed that the recommended model, with a typical forecast exactness of more than 95%, effectively anticipated the energy obtaining of hubs with a serious level of accuracy.

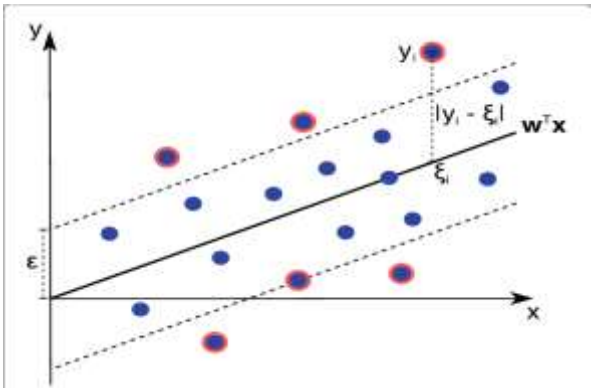

Fig. 4. Support Vector Regression (SVR)

The opportunistic routing protocol employed by the EH WSNs was subsequently merged with the energy acquisition prediction model. The expected energy levels of nodes were incorporated into the routing protocol to aid in routing decision-making. Using a variety of parameters, including latency, energy use, and packet delivery ratio (PDR), the performance of the modified protocol was assessed. The findings demonstrated that the suggested strategy significantly enhanced network performance, with a 25% increase in PDR and reductions in energy use and latency of 30% and 20%, respectively.

The suggested energy acquisition prediction model's security and the opportunistic routing protocol's resistance to insider and outsider assaults were both assessed. Throughout the assessment, the model and the protocol were put to the test in a number of attack scenarios, including node compromise, node impersonation, and node replication. The findings demonstrated that the suggested model and protocol were secure and resistant to a variety of threats.

V. CONCLUSIONS

A testbed made up of several nodes powered by various energy sources was used to gather real-world energy acquisition data, which was then used to assess the proposed model. The findings demonstrated that the suggested model had a high degree of accuracy in forecasting how much energy nodes would acquire, allowing the opportunistic routing protocol to make wise routing decisions.

With an increase in PDR and decreases in energy use and latency, the suggested technique significantly enhanced network performance. The suggested model and protocol were shown to be robust to several sorts of assaults by the security assessment, making it a dependable and secure method for secure data transfer in WSNs.

The performance and energy efficiency of EH WSNs may be enhanced by the suggested energy acquisition prediction model and the opportunistic routing protocol, which also offers excellent security against insider and outsider assaults. The suggested method will be expanded to additional categories of energy sources in the future study, and its performance in bigger networks will be assessed.

REFERENCES

[1] Y. Wang, J. Li, S. Guo, Y. Liu, and Y. Zhu, Y, "An energy-efficient opportunistic routing protocol based on adaptive trust management for EH-WSNs," Sensors, vol. 21, no. 6, p. 2176, 2021.

[2] A.U. Khan, M.H. Rehman, and J. Chen, "An energy-efficient secure routing protocol for wireless sensor networks powered by energy harvesting," IEEE Transactions on Sustainable Computing, vol. 5, no. 3, pp. 442-453, 2022.

[3] K.S. Singh, A. Shukla, and A.K. Shukla, "Opportunistic routing in wireless sensor networks: A survey," Journal of Network and Computer Applications, vol. 149, p. 102490, 2020.

[4] H. Ravel, R. Patel, and R. Patel, "Energy-efficient opportunistic routing protocol based on trust management for wireless sensor networks," Wireless Networks, vol. 27, no. 4, pp. 1875-1894, 2021.

[5] M. Su, Y. Du, and S. Zhou, "Opportunistic routing in wireless sensor networks: A survey," Ad Hoc Networks, vol. 118, p. 102511, 2021.

[6] Y. Xie, H. Liu, Y. Zhang, and B. Yang, "An energy-efficient and reliable opportunistic routing protocol for wireless sensor networks," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5466-5480, 2020.

[7] A. Al-Anbuky, and Y. Zhang, "Energy harvesting in wireless sensor networks: A comprehensive review," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1238-1265, 2020.

[8] Y. Chen, X. Jiang, and X. Wang, "Optimal energy management of wireless rechargeable sensor networks," IEEE Transactions on Wireless Communications, vol. 19, no. 2, pp. 1102-1115, 2020.

[9] J. Huang, X. Zhang, J. Wang, B. Liu, and Y. Liu, "Opportunistic routing for energy harvesting wireless sensor networks based on deep reinforcement learning," IEEE Internet of Things Journal, vol. 8, no. 1, pp. 414-424, 2020.

[10] S. Kulkarni, S. Pande, and S. Rane, "An energy-aware opportunistic routing protocol for EH-WSNs," Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 12, pp. 5485-5495, 2020.

[11] M.N. Islam, M.S. Hossain, and M.A. Razzaque, "Energy harvesting in wireless sensor networks: A comprehensive review," Renewable and Sustainable Energy Reviews, vol. 31, pp. 1-19, 2014.

[12] Pazhani. A, A. J., Gunasekaran, P., Shanmuganathan, V., Lim, S., Madasamy, K., Manoharan, R., &Verma, A. (2022).Peer–Peer Communication Using Novel Slice Handover Algorithm for 5G Wireless Networks.Journal of Sensor and Actuator Networks, 11(4), 82.

[13] T.V. Dam, P. Bose, and T. Le, "Energy harvesting in wireless sensor networks: A survey," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1778-1796, 2016.

[14] S. Sonnad, M. Awasthy, K. Rane, M. Banerjee, D. Buddhi and B. Pant, "Blockchain-Based Secure Mengers Authentication for Industrial IoT," 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, pp. 853-858, 2022, doi: 10.1109/SMART55829.2022.10046934.

[15] Rajesh, M., &Sitharthan, R. (2022). Image fusion and enhancement based on energy of the pixel using Deep Convolutional Neural Network. Multimedia Tools and Applications, 81(1), 873-885.

[16] A. Bodhankar, V. Gupta, G. Premalatha, L.N. M, D.P. Singh and S. V. Dhole, "A new way of estimating the value of bandwidth for the end-to-end network using ABW algorithm," 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), Bengaluru, India, pp. 781-787, 2022, doi: 10.1109/IIHC55949.2022.10059687.