Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 12, No. 1, December : 2023

SECURITY BASED LEARNING AUTOMATA WITH OPTIMISATION ROUTING TECHNIQUES IN WIRELESS SENSOR NETWORK

Dr. B. SANTOSH KUMAR, Associate Professor, Department of MCA, Wesley PG College, Secunderabad, India.

Abstract
Wireless Sensor Networks (WSNs) play a pivotal role in numerous applications, including environmental monitoring, healthcare, and industrial automation. However, the dynamic and resource-constrained nature of WSNs makes them susceptible to various security threats. To address this challenge, researchers have been exploring innovative approaches that integrate security-based learning automata with optimization routing techniques in WSNs. Learning automata, as adaptive decision-making algorithms, enable sensor nodes to learn and optimize their behavior based on environmental feedback, while optimization routing techniques aim to find optimal paths for data transmission. This paper provides an overview of the Security Based Learning Automata with Optimization Routing Techniques in WSN, highlighting their potential to enhance security and optimize routing in WSNs. We discuss the principles, components, and design considerations of this approach, including the integration of learning automata for adaptive security mechanisms and optimization routing techniques for efficient data transmission. Furthermore, we explore the benefits, challenges, and real-world applications of this approach in WSN scenarios. Through a comprehensive understanding of security-based learning automata with optimization routing techniques, we aim to contribute to the development of robust and secure WSNs capable of meeting the demands of diverse applications in the Internet of Things (IoT) era.

Keywords: WSN, Learning automata, Optimisation routing technique, Security, IoT.

I. Introduction

All sensor nodes in WSNs attempt to gather data and transmit sensed data to the base station (BS). In order to collect data from other sensor nodes, the wireless communication uses a fixed node named BS [1] that is located in the middle of the environment. There are occasions when the source and destination are out of the neighbourhood and have multiple hops between them, increasing the energy usage. The amount of energy each node uses to send and receive data to and from other nodes is known as node energy consumption. The network's energy consumption is revealed by adding the energy used by each network node [2]. As these energy sources cannot be replaced and directly affect the network lifespan, the introduction of new protocols or improvements to existing ones becomes necessary for greater energy savings in the network.

As a result, numerous routing protocols are implemented in WSN to lessen the quantity of transmission with the purpose of lowering the amount of power used. Data are pushed from the sensor node to the base station, which is the hub of a WSN, as its name indicates [3]. The data packet needs to travel farther and consumes more energy when the sensor node is far from the BS. Moreover, sensors close to the base station, especially in a bottleneck zone, see increased battery drain due to the high volume of traffic. As a result, the longevity and connectedness of the network are impacted [4] due to the increased rate of death of nodes in the bottleneck zone.

The primary sources of power consumption in WSNs are the sending and receiving of data packets. Thus, it is necessary to build energy-aware routing protocols for WSNs in order to effectively manage and regulate energy consumption. The energy hole problem [5] arises because of the many-to-one nature of the traffic architecture, which leads to the rapid depletion of the energy resources of the nodes in close proximity to the sink in the absence of any form of energy consumption management. The longevity of WSNs is affected by the majority of routing algorithms due to the periodic selection of the ideal path and the energy hole problem. These two issues will cause the network to become

fragmented, rendering the WSN incapable of performing its essential task. The main issue with these kinds of routing methods is that they decrease total energy usage, but do so at the expense of inefficient energy draining across the network [6].

II. Related work

Elhabyan et al. [7] presented a proposal for a PSO-based routing algorithm that might be used for clustering and routing. Energy, cluster quality, and network coverage all serve as factors in the goal function for clustering. The goal function is created throughout the routing phase by utilising energy and link quality. None of the objective functions include power control as a potential metric.

Bara'a et al. [8] proposed an evolutionary computing-based routing protocol to identify the route from each CH to the BS. It considers both the numerous CHs and the cluster's compactness (as determined by intra-cluster distance) while determining the fitness function. On the other side, the energy overhead needed by the nodes is not taken into account.

In [9], the authors provide FSFLA, a Mamdani-based fuzzy clustering method. The fuzzy rule-base is optimised in this system using the memetic Shuffled Frog Leaping Algorithm. It receives five inputs: the node history, the numerous neighbouring nodes, the remaining power, and the distance to the sink. The fuzzy rules are adjusted using these. The authors compared the FSFLA's efficacy to that of LEACH, LEACH-DT, SIF, and ASLPR. They discovered that the FSFLA might outperform current systems in terms of parameters like WSN lifespan, residual power, successfully received packets, and intra-cluster distance.

The author in [10] presented a cluster head (CH) selection method based on HSA. The parameters for the fitness function used to build this method were energy, distance, and node degree. After that, we started to derive a potential function that might be applied to assign non-CH nodes to CHs. The fitness function is derived using the same parameters, namely energy, distance, and node degree, and an HSA-based routing method is also suggested in the conclusion. Three separate test cases were evaluated for performance during the course of the investigation. Using some of the existing, relevant techniques, the suggested strategy has been assessed.

Particle Swarm Optimization Routing Protocol is the name given to the multipath protocol that was developed as a result of an optimization strategy that is detailed in [11] and employs the Particle Swarm Optimization (PSO) technique. (MPSORP). For Internet of Things applications that are based on WSN and have large traffic loads as well as unfair network flow, the MPSORP is built. An experiment is carried out utilising the NS-2 simulator in a variety of setups and parameter settings with the purpose of testing the newly established protocol. In addition, the effectiveness of MPSORP is evaluated alongside that of AODV and DSDV, two other routing protocols.

III. Proposed method

Proposed GWO-based approach

The GWO-based strategy that has been suggested will be discussed in this section. In the GWO-based technique, there are three stages: I the initialization of the wolves, (ii) the computation of the fitness value for each individual wolf, and (iii) the updating of the wolves' velocity and position.

Wolf Initializations

A mapping of sensor nodes to BS serves as the representation for each solution. The number of total sensor nodes is the same as the size of the solution. The approach offers a path from each node to the BS via the network's next succeeding nodes. $(R_{i,d}) = Rand(0,1)$where $1 \leq i \leq Ns$, is the initial random number assigned to each sensor node. Ns stands for the numerous initial solutions. A node number in the relevant solution is represented by the component d. It indicates that n_d transfers data to n k by mapping node n_k as the next succeeding gateway in the routing path from n_d to the BS. The equation below formulates the mapping of the routing path.

$$n_k = index(n_d, ceil\ (R_{i,d} \times |n_d|))$$

Where $index\left(n_d, \left(R_{i,d} \times n_d\right)\right)$ is an indexing function which returns index of nth nodefrom n_d. $ceil$ function computes the smallest integer of $\left(R_{i,d} \times |n_d|\right)$.

Computation of fitness value for each wolf

Fitness functions evaluate quality of solutions in relation to factors of Aggregation costs and Distances to involved BSs. Each time you iterate, it is beneficial to update your alpha, beta, and delta solutions. In this context, our innovative fitness function is geared towards the generation of a routing path that is both effective and economical between each sensor node and the BS.

LA approach

At this stage, each node will employ a learning automaton to select the following ideal hop to transfer its packets in each iteration of the data gathering process towards the sink. Using this strategy, each node eventually learns which neighbour to use as a forwarder of packets to the sink (the neighbour with the most relevant data). The data's final resting place is the sink. In order to find the successor nodes using learning automata, every node i maintains a basic "$Neighbor\ List$" calculated from GWO approach. LA associated to node s_i referred as LA_i has $|RL_i|$ actions whose probabilities of selections are initially set to $1/|RL_i|$. Each LA_i action causes one of the nearby nodes specified in the RL i to be chosen in order to transfer packets from the s_i to the sink. Node s_i requests its learning automaton to choose one of its surrounding nodes (actions) to pass the data towards the sink after it has been activated. During the route selection step, data are compiled. The automaton's chosen course of action will either earn praise or criticism depending on the surrounding node's acknowledgement.

Each node calculates probability for its neighbors using learning automata. AF factor of a node is calculated based on load factor & connectivity ratio values.By combining these values, the AF factor is calculated & intermediate nodes for the data transmission are determined.The AF can be formulated as:

$$AF = \min(LOF + COR)$$

Combined routing technique

In this section, we describe the combined working mechanism of both GWO and learning automata. In WSNs, each node wants to send data to a base station. Initially, each sensor node has multiple options for the next hop, based on multiple parameters. In the proposed network, the sensor nodes use GWO and learning automata together to determine the next hop nodes based on the feedback from the network. The GWO algorithm is used to find the optimal next hop nodes, based on the selection parameters. The learning automata is used to adjust the next hop selection based on the feedback from the network. The learning automata algorithm uses a reward-penalty mechanism to increase or decrease the probability of selecting a node as the next hop based on the feedback. In short, the GWO algorithm finds the optimal next hop nodes, while the learning automata adjusts the next hop selection based on the feedback from the network. The result is a more efficient and reliable routing, as the next hop selection is optimized in real-time based on the current network conditions.

IV. Results and discussion

Simulation analysis and results

NS2 simulations was used to assess the performance of the suggested mechanism and compare it to the MPSORP & CRHS method. The sensor nodes are randomly distributed around a field that is 1000m by 500m in size, with each sensor node having an initial energy of 100j. There are anywhere between 50 and 200 nodes in the network. We consider CBR and UDP agents to be traffic-generating agents. Table 1 displays the experimental parameter values.

Table1: The experimental parameters

Parameter	Value
Network area	1000x500
Many nodes	50 to 200
Initial energy	100j

Packet size	1024
Routing protocol	AODV
Traffic source	CBR (Constant bit rate)

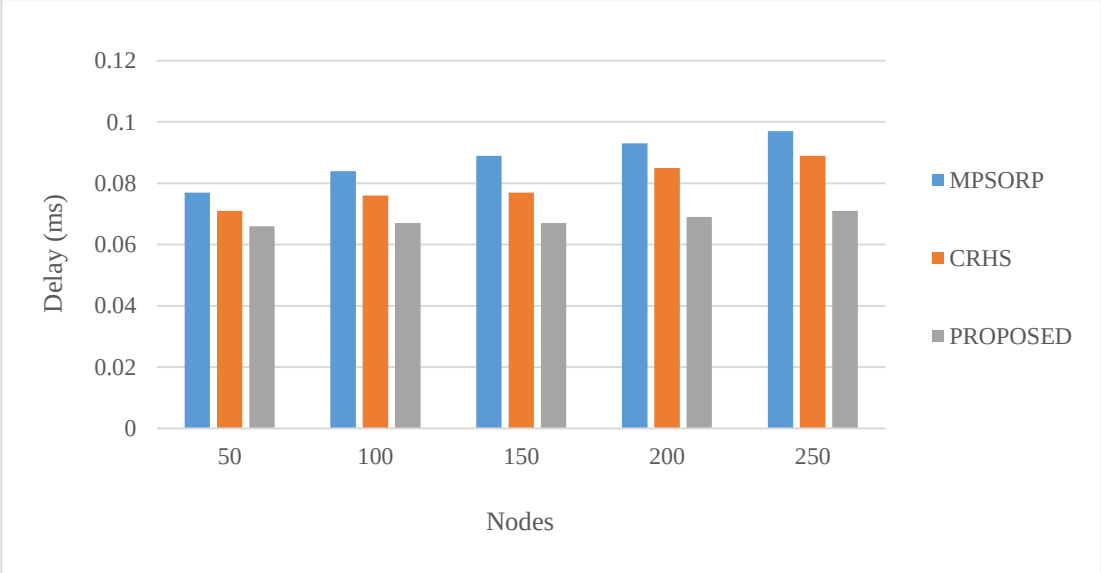

Fig. 1. End to End Delays

End-to-end delays refer to durations taken for data packets to traverse networks from their origins to destinations. In the above figure 1, the evaluation of end-to-end delay times for the proposed method across various network sizes is displayed. Generally, the end-to-end delay increases depends on the many hops involved in routing. However, the proposed method utilizes effective optimal relay selection and reduce the end-to-end delay in the proposed network, when compared to other protocols.

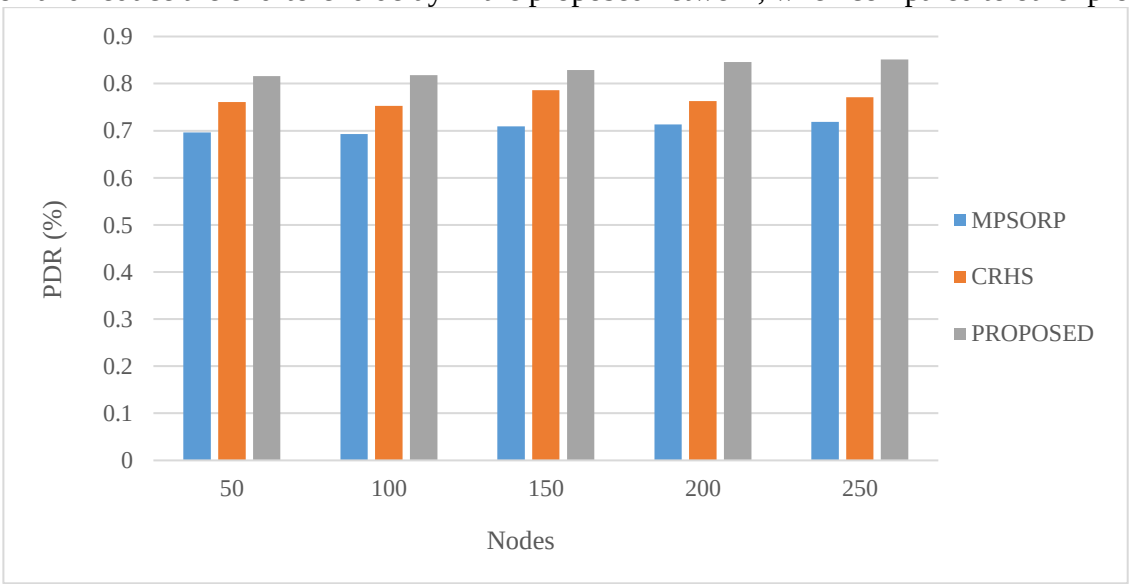

Fig. 2. Packet delivery ratio

The Packet Delivery Ratio (PDR) is a metric that measures the ratio of data packets that are received by the destination node compared to the counts of packets that were originally sent by the source node. Data aggregation and relay selection are crucial factors in enhancing the PDR of a network. By utilizing efficient neighbour node discovery and optimal relay selection, the proposed protocol identifies optimal paths, which can significantly increase the PDR rate when compared to other protocols. The proposed method demonstrated a maximum PDR of 84, while the existing methods only maintained an average PDR rate of 71, which is comparatively low. The above figure 2 graphically illustrates the PDR.

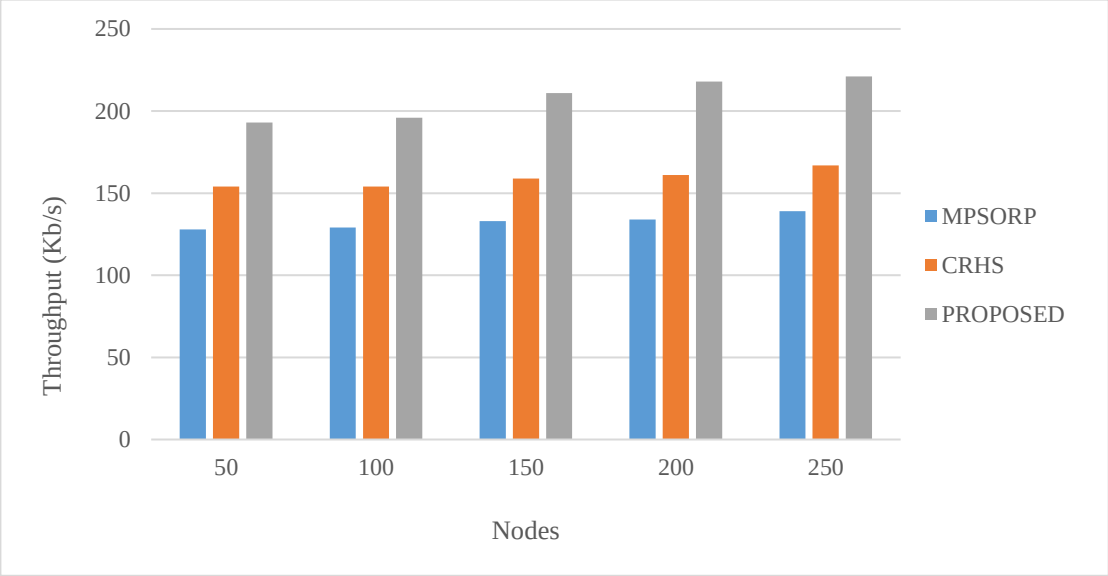

Fig. 3. Throughput

Throughput is a metric that measures the total many data units that a node can process within a given time frame. The optimal relay selection utilizing GWO & LA helps to achieve optimal data aggregation through stable relay nodes. As demonstrated in the table below, the proposed method achieves a high throughput rate compared to existing methods. In the experiment, the proposed method maintained an average throughput rate of up to 218kbps, while the existing methods had lower throughput rates compared to the proposed method. The above figure 3 illustrates the graphical view of throughput.

Conclusion

In conclusion, the integration of security-based learning automata with optimization routing techniques represents a significant advancement in enhancing the security and efficiency of Wireless Sensor Networks (WSNs). By leveraging learning automata's adaptive decision-making capabilities and optimization routing techniques' ability to find optimal paths, this approach offers a promising solution to address the dynamic and resource-constrained nature of WSNs. Through the synthesis of adaptive security mechanisms and efficient routing strategies, this approach enables WSNs to mitigate security threats effectively while optimizing data transmission. Despite potential challenges, such as complexity and overhead, further research and development efforts are warranted to refine and optimize this approach for real-world WSN deployments. In essence, security-based learning automata with optimization routing techniques pave the way for the development of robust and secure WSNs capable of meeting the diverse demands of IoT applications with enhanced resilience and efficiency.

References

[1] Nagaraju, V., Kumar, N.J., Ali, A.M., Bapu, T.B. and Partheeban, N., 2022, January. Efficient Data Transmission Scheme using Modified Wireless Communication Protocol Design. In *2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)* (pp. 1-7). IEEE.

[2] Sadrishojaei, M., JafariNavimipour, N., Reshadi, M., Hosseinzadeh, M. and Unal, M., 2022. An energy-aware clustering method in the IoT using a swarm-based algorithm. *Wireless Networks*, *28*(1), pp.125-136.

[3] Nonita, S., Xalikovich, P.A., Kumar, C.R., Rakhra, M., Samori, I.A., Maquera, Y.M. and Gonzáles, J.L.A., 2022. Intelligent Water Drops Algorithm-Based Aggregation in Heterogeneous Wireless Sensor Network. *Journal of Sensors*, *2022*.

[4] Nasri, A., Rad, F. and Fathy, M., Propose a Routing Protocol for Decreasing Energy Consumption of Wireless Body Area Networks by Using Relay Nodes. *Available at SSRN 4024168*.

[5] Azooz, S.M., Majeed, J.H., Ibrahim, R.K. and Ali, A.H., 2022. Implementation of energy-efficient routing protocol within real time clustering wireless sensor networks. *Bulletin of Electrical Engineering and Informatics*, *11*(4), pp.2062-2070.
[6] Roberts, M.K. and Ramasamy, P., 2022. Optimized hybrid routing protocol for energy-aware cluster head selection in wireless sensor networks. *Digital Signal Processing*, *130*, p.103737.
[7] Elhabyan RSY, Yagoub MCE (2015) Two-tier particle swarm optimization protocol for clustering and routing in wireless sensor network. J NetwComputAppl 52:116–128.
[8] Baraa AA, Khalil EA (2012) A new evolutionary based routing protocol for clustered heterogeneous wireless sensor networks. Appl Soft Comput 12(7):1950–1957.
[9] F. Fanian, M.K. Rafsanjani, Memetic fuzzy clustering protocol for wireless sensor networks: shuffled frog leaping algorithm, Appl. Soft Comput. 71 (2018) 568–590.
[10] Lalwani, P., Das, S., Banka, H. and Kumar, C., 2018. CRHS: clustering and routing in wireless sensor networks using harmony search algorithm. *Neural Computing and Applications*, *30*, pp.639-659.
[11] Ghawy, M.Z., Amran, G.A., AlSalman, H., Ghaleb, E., Khan, J., Al-Bakhrani, A.A., Alziadi, A.M., Ali, A. and Ullah, S.S., 2022. An Effective Wireless Sensor Network Routing Protocol Based on Particle Swarm Optimization Algorithm. *Wireless Communications and Mobile Computing*, *2022*.