International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 1, January-February 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

ANN-Based Secured Energy-Efficient Routing in Wireless Sensor Networks with Dynamic Deterministic Finite Automata (DDFA) and Particle Swarm Optimization Algorithm

Yogesh Kumar Solanki, Anshuj Jain, Laxmi Singh

Department of Electronics & Communication Engineering,
Rabindranath Tagore University, Bhopal, Madhya Pradesh, India

ABSTRACT

A wireless sensor network, or WSN, is made up of many sensor nodes that can join quickly to the base station. The information is sent to the central spot after being processed at the sensor nodes. When data is sent in a place where there is no coverage, there will be a delay. Not only is there a big delay, but the amount of energy used goes up by a big amount as well. To solve this problem, a method of network coding called energy efficiency and secure routing protocol (EESR) is used. This way is meant to make multi-hop routing protocol safer and use less energy. Some people think that using ANN to automate IDS could help improve the energy efficiency of routing in wireless sensor networks while keeping a certain level of security. Dynamic Deterministic Finite Automata (DDFA) and Particle Swarm Optimisation (PSO) are used in the suggested work to find intrusions. Also, data is sent in a safe way by figuring out and then taking the fastest and most efficient route. People have said that a new Deterministic Finite Automata) could be used to make the network more active. DDFA- PSO gives information about the node inspection, packet inspection, and route inspection. This information is used to find and get rid of hackers, so that data can be sent in the most efficient and cost-effective way along the best route. The routing through the best path improves the overall performance of the sensor network, and an analysis of the results shows that the suggested method is better than the existing routing schemes in terms of energy efficiency, network throughput, average one-way delay, and lifetime of the network.

KEYWORDS: *Intrusion Detection System, WSN, Clustering, Particle Swarm Optimization, ANN*

How to cite this paper: Yogesh Kumar Solanki | Anshuj Jain | Laxmi Singh "ANN-Based Secured Energy-Efficient Routing in Wireless Sensor Networks with Dynamic Deterministic Finite Automata (DDFA) and Particle Swarm Optimization Algorithm" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-1, February 2024, pp.18-23, URL: www.ijtsrd.com/papers/ijtsrd61295.pdf

IJTSRD61295

I. INTRODUCTION

IoT, which stands for "Internet of Things," is a worldwide network of devices that connect to each other and share networking, sensing, and information processing tools [1–4]. The main goal of the Internet of Things is to make it possible to join any two things, no matter where they are, that have the same characteristics. Radio-frequency identification, also called RFID [5–7], is an early Internet of Things technology that uses electromagnetic fields to instantly send identification data to a reader through wireless networking devices. The radio signal transponder (also called a "tag") and the tag reader are the two most important parts of an RFID device. Most of the time, radio frequency identification (RFID) tags store information electronically, which lets users organize, track, and keep an eye on the things. An RFID tag can be put on any item so that information can be gathered and the location of the object can be tracked. Wireless sensor networks (WSNs) are another important part of the Internet of Things. These networks are made up of smart gadgets called sensor nodes. These nodes are set up in a random way to collect information with limited energy, computing power, memory, and processing speed. IoT systems are hard to make secure because WSN is hard to understand and sensor nodes are limited in what they can do. As a result, it is hard to keep IoT systems safe, and a number of network

attacks could make it hard for devices to talk to each other. Internets of Things-based wireless sensor networks are also used in both staffed and unstaffed settings. Some of the things that are being watched in these settings are air pollution, water quality, and smart cities. Along with making sure data is sent reliably, improving energy efficiency is a very important problem. A cluster-based method has been suggested by a number of academics as a way for WSN to use less energy. During the clustering process, the nodes are split into different groups, and the head of each group is called the "leader node." The cluster head is in charge of getting data from the other nodes in the cluster, putting them all together, and sending them to the base station (BS). You can send data from the cluster heads to the BS using either a single hop or a multi-hop method. Most of the time, methods for clustering can be put into two groups: probabilistic and non-probabilistic. Clusters in random [8-10] are put together in any order, which makes it hard to spread out the load and use the right amount of energy. In the non-probabilistic method, on the other hand, the cluster heads are chosen by taking into account a number of different factors. But because sensor nodes are always changing [11], IoT built on WSN still has work to do to save more energy and make routing more reliable. Even though non-probabilistic methods work better than traditional probabilistic methods, this is not the case when comparing non-probabilistic methods to traditional probabilistic methods.[12-14]

II. RELATED WORK

T.R. Chenthil et.al. 2022 [15] this work creates a protocol called E-CDBR, which is a clustering-based depth coordination routing scheme that uses less energy. Its goal is to cut down on how much energy UWSN needs while also cutting down on how long it takes for messages to be sent. It uses depth coordination and position in the cluster to choose the CH, and it sends data to the surface sink whenever the cluster area is within the range of the transmission. These are depth coordination and location in the cluster. Compared to current methods, the performance results show that less overall energy is used, the network lasts longer, and there is less overall latency. The fault-tolerance feature of a network is its ability to keep working normally even if one or more of its sensors stops working. Fault-tolerant protocols use fault recovery methods and offer ways to either delay failure or stop it from happening at all.

III. PROPOSED SYSTEM

The proposed approach involves a hybrid of two machine learning algorithms, namely Dynamic Deterministic Finite Automata (DDFA) and Particle Swarm Optimization (PSO), for intrusion detection in Wireless Sensor Networks (WSNs). Additionally, Artificial Neural Network (ANN) is used for classification of detected intrusions. DDFA is used to learn and model the normal behavior of WSN nodes, and the model is used for intrusion detection by checking the deviation of current behavior from the learned model. PSO is used to optimize the path taken by data packets to minimize energy consumption and improve network lifetime. In this conversation, the goal of the suggested framework is to provide a safe and energy-efficient way to route data in a Wireless Sensor Network (WSN). The method that has been made uses Dynamic Deterministic Finite Automata (DDFA) and Particle Swarm Optimisation (PSO) to find the best way to send data securely and the best route to take. Once the network is set up, the nodes are spread out randomly across the connection-based mesh network. After that, the area is divided into three equal parts, each of which becomes a cluster. All of the sensor nodes in a cluster can only talk to the head of that cluster. DDFA is used to learn about the node, packet, and route on the fly, and

the path table is updated regularly with new information about each node. When a packet needs to be sent from the source node to the destination node, DDFA finds the open path between the two and verifies it. When a packet needs to be sent from the source node to the target node, this process happens.

The PSO algorithm is utilized to examine the path table and analyze the node, packet, and route information to detect and eliminate undesired attacks like Sybil attacks and selective forwarding, which may exist in the network. To obtain the best route, DDFA is combined with PSO, and once the optimal path is found, packets are transmitted from the source to the destination safely and efficiently. The network is initialized by randomly assigning nodes to a mesh-connected network. The nodes are dynamically selected from the network, and all feasible paths between the source and the destination are identified. DDFA verifies the validity of the path based on the path table, and if it is valid, it is updated in the path table. PSO then analyzes the node, route, and packet information in the path table and selects the best route for transmitting the packets.

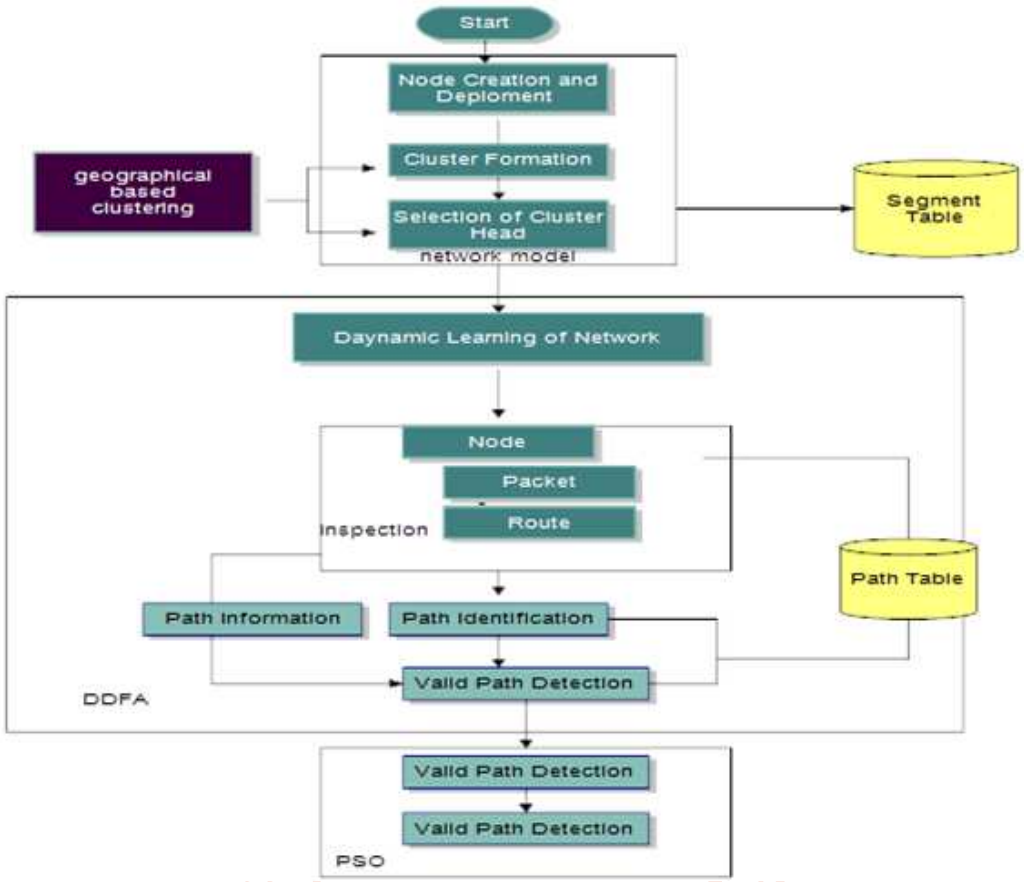

Fig.1: proposed flow diagram

Cluster and cluster head- In wireless sensor networks (WSNs), clustering is a technique used to organize the nodes into groups or clusters for efficient data routing and management. The nodes in each cluster communicate with a designated node called the cluster head, which is responsible for aggregating and forwarding the data to the sink node or gateway.

Cluster Head Selection-. Cluster head selection is the process of choosing the most appropriate node in a cluster to act as the cluster head.

DDFA- The DDFA learns the behavior of the nodes, packets, and routes in the network. It maintains a path table which contains information about the available paths from source to destination nodes. When a packet needs to be transmitted from the source to the destination, DDFA uses the path table to identify the available paths and chooses the optimal path based on certain criteria, such as energy efficiency and security.

ANN- In Wireless Sensor Networks (WSNs), intrusion detection is a crucial issue for ensuring the security of the network. ANN identifies and eliminates intruders or unwanted attacks, such as selective forwarding and Sybil attacks.

Sybil attack- A Sybil attack in a Wireless Sensor Network (WSN) is a type of attack where a malicious node creates multiple fake identities or personas to disrupt or manipulate the network's operations. In a Sybil attack in a WSN, the attacker can create multiple fake identities by either compromising existing nodes or by introducing new nodes into the network. The attacker can then use these fake identities to control a larger portion of the network, disrupt communication, or launch other attacks.[14-15]

Selective Forward Attack

The Selective Forward Attack Detection procedure is a method used in network security to detect selective forwarding attacks, where a malicious node selectively drops or forwards certain packets in a network. For each path in the network, check if the path exists in the Path Table, which is a table that stores information about the paths in the network.

Table 1 Simulation Parameters

Network Parameters	Parameters Value
Sensing Range(Meter)	36
Network Length(Meter)	200
Network Width (Meter)	200
Cluster Radius (Meter)	30
Number of Nodes	200
Initial Energy (Eo)	200
Packet Size (Bytes)	512
trans_power	0.02
recei_power	0.01

IV. PERFORMANCE EVOLUTION

The performance of the proposed systems can be analyzed based on various metrics, including packet delay, network lifetime, throughput, energy consumption, and packet delivery ratio (PDR).

Packet Delay: The packet delay is the time taken for a packet to travel from the source node to the destination node. It can be calculated using the following formula:

Packet Delay = Time taken for packet delivery- Time at which packet was sent

Network Lifetime: Network lifetime is the duration for which the network can operate until the first node runs out of energy. The network lifetime in a WSN can be estimated using the following formula:

Network Lifetime = min(Ei) / (P x A)

Where min(Ei) is the minimum energy of all the nodes in the network, P is the power consumption rate of each node, and A is the total area covered by the network.

Throughput: Throughput is the amount of data transmitted over the network per unit time. It is a measure of the network's efficiency in delivering data to the base station. A higher throughput implies better network performance.

Throughput = (Total number of bits transmitted) / (Total time taken to transmit those bits)

Energy Consumption: Energy consumption refers to the amount of energy consumed by the network during the operation. The energy consumption in a wireless sensor network (WSN) can be calculated using the following formula:

$E = P \times t$

Where E is the energy consumption, P is the power consumption rate, and t is the time for which the device is operational.

Packet Delivery Ratio (PDR):. The Packet Delivery Ratio (PDR) is the ratio of the number of packets successfully delivered to the base station to the total number of packets transmitted. The formula for PDR is as follows:

PDR = (Number of Packets Successfully Delivered to Base Station / Total Number of Packets Transmitted) * 100%

V. SIMULATION RESULTS

The simulations demonstrate that the protocol achieves a good balance between communication and energy consumption, leading to improved network lifetime and reduced energy wastage. Overall, the results indicate that the protocol is highly effective and can be relied upon to provide secure, efficient, and sustainable communication in wireless networks.

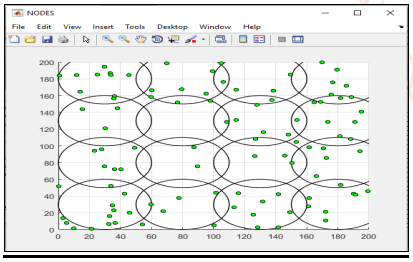

Fig.2 initial network

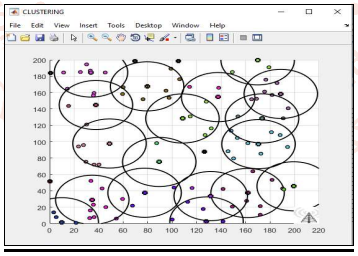

Fig.3 Cluster Head

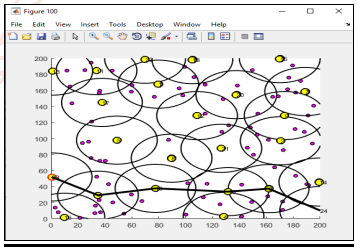

Fig.4optimum path in the network

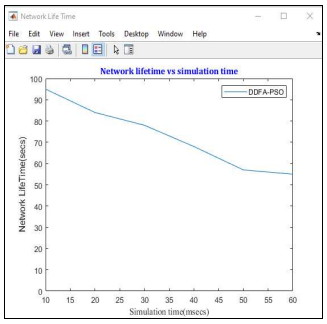

Fig.5 Network lifetime vs. simulation time

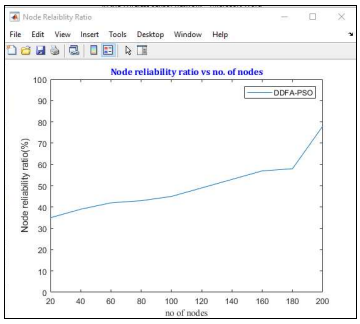

Fig.6 Node reliability ratio vs. no. of nodes

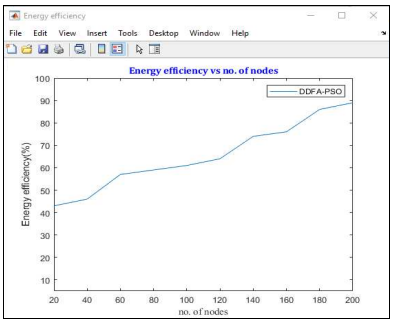

Fig.7:Energy efficiency vs. no. of nodes

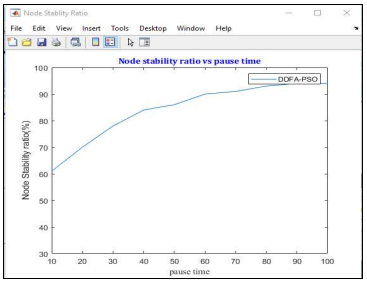

Fig. 8: node stability

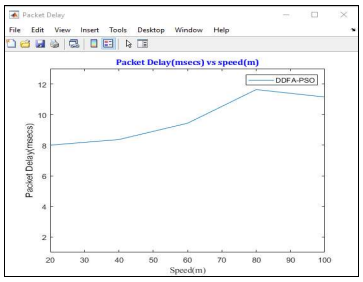

Fig. 9: Packet delay vs. speed

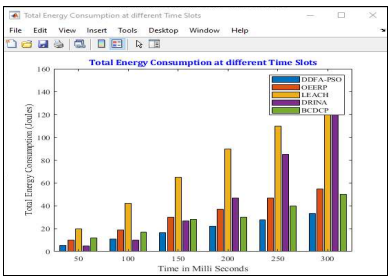

Fig.10:totalenergy consumption at different time slot

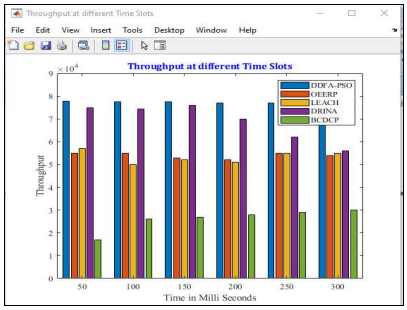

Fig.11:throughput at different time slot

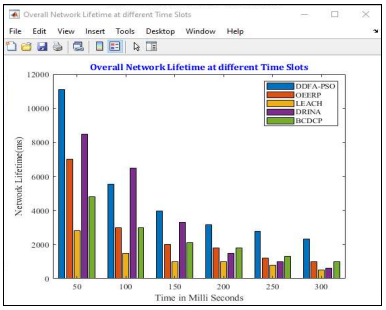

Fig.12 network life time at different time slot

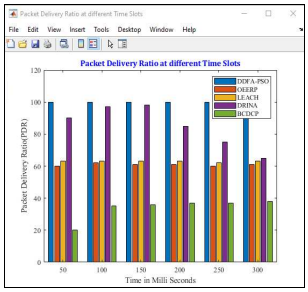

Fig.13: packet delivery ratio at different time slot

Table 2 performance of proposed algorithm

	Throughput (%)	Energy Consumption (E/j)	Packet delivery (%)	Network life (ms)
Proposed work	85(%)	11 E/j	99(%)	11000(ms) at last node

Table 2 Result comparison with existing work

	Network Lifetime (Ms.)	Energy Efficiency (%)	Node Reliability (%)	Packet Delay (%)	Node Stability (%)
Existing Work	95	38	19	4.9	61
Proposed System	96	45	36	2.8	62

Based on the table 2 provided, it can be observed that the proposed system has improved the network lifetime, energy efficiency, node reliability, packet delay, and node stability compared to the existing work.

VI. CONCLUSIONS

The development of a secure cluster energy-efficient model is an important step towards achieving network lifetime and data integrity in a Wireless Sensor Network (WSN). The model aims to optimize the energy consumption of the nodes while ensuring the security and integrity of the data transmitted within the network. The use of clustering is an effective approach to reduce communication overhead and energy consumption in WSNs. By dividing the network into clusters and allowing nodes to communicate only with their cluster head, the model can conserve energy and prolong the network lifetime. Moreover, the model's emphasis on data integrity is essential for ensuring that the data transmitted within the network is not compromised or altered by malicious nodes or attacks. This can be achieved through the use of secure data transmission protocols and the implementation of intrusion detection and prevention mechanisms. By investigating a node's behavior, the approach can determine whether it is malicious or not. The segment table is used to identify duplicate node IDs, which can be indicative of a Sybil node. Investigating all possible paths can help to identify the optimal path for transmitting data and detect selective forwarding attacks based on path ID. By comparing the discovered route for data transmission, the approach can detect and eliminate Sybil and selective forward attacks. Packet investigation is also used to detect abnormal packets by examining duplicates, injected packets, and path ID. By integrating these different investigation techniques, the proposed approach can provide comprehensive detection and prevention of various types of malicious nodes and attacks in the network. Overall, this approach can help to enhance the security and reliability of the network.hecne he DDFA-PSO approach shows promise in enhancing the security and energy efficiency of WSNs and can be further improved and optimized through future research and testing.

References

[1] Zhou, Y.Sharma, A. Masud, M., Gaba, G. S. Dhiman, G. Ghafoor, K. Z., & Lain, M. A. (2021). Urban rain food ecosystem design planning and feasibility study for the enrichment of smart cities. Sustainability, 13(9), 5205.

[2] Kothai, G. Poovammal, E. Dhiman, G. Ramana, K., Sharma, A. AlZain, M. A., Gaba, G. S., & Masud, M. (2021). A new hybrid deep learning algorithm for prediction of wide traffic congestion in smart cities. Wireless Communications and Mobile Computing, 2021

[3] Madasamy, K., Shanmuganathan, V., Dhiman, G., Vijayalakshmi, K., & Suresh Kumar, P. (2021). Materials Today: Proceedings A survey on clustering algorithms for wireless sensor networks. Computer Communications, 30, 2826–2841.

[4] M. Poongodi, M. Hamdi, M. Malviya, A. Sharma, G. Dhiman, S. Vimal, Personal and ubiquitous computing, pp. 1–11 (2021)

[5] Dhiman, G., Oliva, D., Kaur, A., Singh, K. K., Vimal, S., Sharma, A.& Cengiz, K. (2021). Knowledge-Based Systems, 211, 106560.

[6] Bhargava, N., Bharagava, R., Mathuria, M., Gupta, S., & Kumar, K. (2013). International Journal of Computer Networks and Wireless. Communications, 3(1), 32

[7] Bhola, J., Soni, S., Cheema, G. K. (2020). Genetic algorithm based optimized leach protocol for energy efficient wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 1281–1288

[8] Benyin, X., Chaowei, W., ”An improved distributed energy efficient clustering algorithm for heterogeneous WSNs”. In: IEEE Wireless Communications and Networking Conference (WCNC), pp. 19-22, San Francisco, CA (2017

[9] Trupti Mayee Behera, Umesh Chandra Samal, Sushanta Kumar Mohapatra, ”Energy-efficient modified LEACH protocol for IoT application”, IET Wirel. Sens. Syst.© The Institution of Engineering and Technology 2018, May 2018.

[10] Gopinath a, K.Vinoth Kumar b, P. Elayaraja c, A. Parameswari b, S. Balakrishnan d, M. Thiruppathi SCEER: Secure cluster based efficient energy routing scheme for wireless sensor networks S Volume 45, Part 2, 2021, Pages 3579-3584