International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/211594 Volume 9, Issue 1, January – February (2022)

RESEARCH ARTICLE

Energy-Aware Optimal Clustering and Secure Routing Protocol for Heterogeneous Wireless Sensor Network

Swapna M P
Department of Computer Science, Sri Ramakrishna College of Arts & Science for Women, Coimbatore, Tamil Nadu, India
mpswapna77@gmail.com

G. Satyavathy
Department of Computer Science, Sri Ramakrishna College of Arts & Science for Women, Coimbatore, Tamil Nadu, India
satyacs@srcw.ac.in

Received: 20 November 2021 / Revised: 11 January 2022 / Accepted: 16 January 2022 / Published: 28 February 2022

Abstract – Wireless Sensor Network (WSN) is a collection of low energy sensor nodes deployed in hostile complex environments. Their functionality gathers requisite data from the environment and transmits it to the base station for further processing. To enhance the performance of WSN, sensor nodes with different energy levels, capabilities and functionalities are deployed, leading to Heterogeneous WSN (HWSN). The initial energy, energy consumption rate, and residual energy differ for each node in a heterogeneous WSN. Many algorithms were proposed to accomplish an energy-efficient steady HWSN, but the performance level is not satisfactory. This paper presents a novel integrated approach, Energy-Aware Optimal Clustering & Securing Routing (EAOCSR). The algorithm amalgamated three techniques optimal clustering, reliable routing and secured transmission, considering energy retention and network lifetime as the vital parameters. Unequal clustering scheme, trust-based reliable and secure routing forms the core of EAOCSR. The performance of EAOCSR is analyzed using MATLAB simulations. It reveals that the proposed routing protocol EAOCSR has superior performance to existing protocols regarding energy utilization, throughput, network lifetime, stability and security.

Index Terms – HWSN, Unequal Clustering, Trust, Blockchain, Stability, Security.

1. INTRODUCTION

Networks are the assembly of machines that distribute the resources among the interconnected devices, and these devices can be interconnected using physical communication medium or non-physical communication medium. Wireless Sensor Networks (WSN) is an assembly of devices where these devices are interconnected with no physical communication medium. Sensors are devices that sense the changes in the surroundings where it has been placed[1], [2]. These sensors are deployed to monitor temperature variations in the atmosphere, rainfall, pollution level, etc. WSN reduce stress and increase consistency and accuracy in monitoring. The role of WSN is very vital in the monitoring process. They gather the information, and the collected details are updated in the collection server within a specific time frame. Whenever there are some changes in the deployed atmosphere, those details will be collected and updated immediately; if there is a constant situation and no changes for a long time, the update will be done on a specific time duration[3].

Heterogeneous Wireless Sensor Network (HWSN) is the predominant type of Wireless Network used today. HWSN consists of sensor nodes with different capabilities, sensing ranges and energy levels. HWSN is an ideal solution for improving the performance and cost reduction of WSN. Internet of Things (IoT) is an apt phenomenon depicting HWSN. Sensor nodes of WSN are energy-constrained devices deployed in ad-hoc hostile environments to monitor and gather information[4]. Ensuring the energy retention of nodes and prolonging the network lifetime is a mandate in WSN.

In contrast to homogeneous WSN, the energy and functionality of nodes vary in a heterogeneous WSN. The initial energy and the residual energy of nodes differ. Hence, the energy distribution must be uniform to avoid the early death of low energy nodes. The sustained functionality of the network is directly proportional to the network lifetime[5].

Optimization is an action that ends with a better result using the available resources [6]–[12]. These optimization techniques are followed by most of the living things in the world for their survival; some of the typical behaviour of

RESEARCH ARTICLE

those has given a lot of inspiration for the humans to accomplish their task in their location or area. From that inspiration, if the solution has been found to achieve the mission, then it is said to be the optimization technique[13], [14]. A pictorial representation of HWSN is shown in Figure 1.

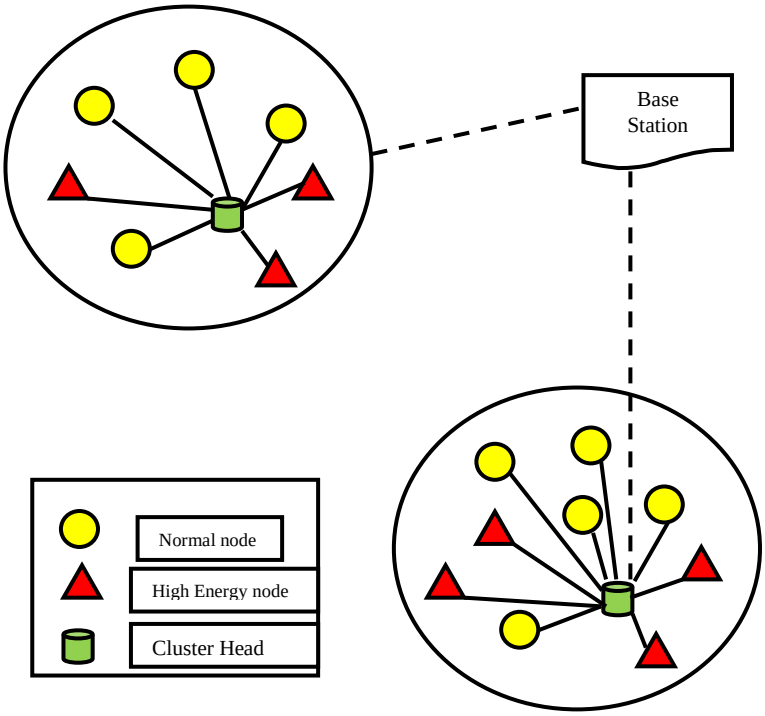

Figure 1 A Pictorial Representation of HWSN

1.1. Problem Statement

The technology and its components will face problems in various aspects, and those can be rectified. The most common problem found in the WSNs is finding the path to transport the data from the sender to the receiver end. All the nodes have to be in alert mode during this process, which consumes a lot of energy. WSNs also face some problems such as path finding, power consumption, etc. These problems are considered the main factor in WSNs hence the focus is on increasing the packet delivery ratio and avoiding the utilization of power in the unwanted situation.

1.2. Motivation

Monitoring the child is the immense task of every parent, especially the working couples keep on thinking about the safety and the activity of the child in the playschool. From the parent point of view, the child safety is the priority, and they keep on thinking about their child when they are away from their children. Their mind will not concentrate on other things while monitoring the child; if there is any delay in the response, the parent will lose their calmness; that's the emotional bond. To ensure the child safety in the virtual mode parent is dependent on the network, the data to be transferred without any delay; this motivates to propose the following work.

1.3. Objective

Any process begins with a motto. This proposed work is clear with its motto, as specified in the motivation section. The operation such as finding the correct path and focusing on the energy consumption reduction is the motto of this proposed research work which uses the optimization technique to accomplish the specified process.

1.4. Organization of the Paper

This section of the paper had a brief introduction on Heterogeneous WSN, problem statement, motivation and objective of the research. Section 2 discusses the related works. EAOCSR is proposed in Section 3. Simulation settings, performance metrics, the results of the experiment are discussed in section 4. The conclusion of the research analysis is specified in section 5.

2. RELATED WORKS

"Cross-layer Communication Protocol"[15] is proposed in the study for detecting the node boundaries of WSN, which is deployed. The sentinel and relay nodes are used for deployment, whereas the relay nodes are duty-cycled during data communication. Greedy Perimeter Stateless Routing

RESEARCH ARTICLE

protocol is enhanced, based on a Non-Unit Disk Graph fused as GPSR over Symmetrical Links. Mutual Witness is applied for planarization of Gabriel Graph, and simulation results are generated to prove its efficiency over other techniques. "Approximation Algorithm"[16] is proposed for clustering data wherein the cluster head increases the network's lifetime. Virtual grid infrastructure is enabled on the web, and a routing algorithm is proposed. Appropriate paths are detected for finding the route paths among sink and cluster. Simulation results are generated to compare its performance among other existing techniques. "Trust Aggregation Authentication Protocol"[17] is proposed for improving the authentication based on machine learning. The gateway ignores the node through which the internet gateway is derived through trust value. Support Vector Machine is incorporated for measuring the trust threshold value, and the performance is evaluated using performance metrics. "Guaranteed Lifetime Protocol"[18] is proposed to analyze energy consumption in Wireless Sensor Network. The sink nodes were assigned with active/sleep technique for every network cycle using total busy time, residual energy. Simulation results are analyzed to enhance the protocol's guarantee through evaluation metrics. "Reverse Glowworm Swarm Optimization"[19] is proposed to improve the performance and efficiency of energy through a green sensor network. Fuzzy Inference System is used for reducing the energy consumption and distance traversing, through which simulation results are retrieved. The result shows that the live sensor performs better than others in execution.

"Edge-based Device Security"[20] is proposed to diagnose the WSN framework in the current study. Low-order features are used to enhance the performance of the framework. The low-order features were extracted wherein the data type of the signal is fetched for measuring the capability of the hardware. The continuous wave interference, I/Q data are fetched for achieving better accuracy. XG Boost algorithms and Deep Neural Network were incorporated for performing classification through which optimization is established. "Bio-inspired Multi-objective Evolutionary Routing Protocol"[21] is proposed for applications based on Underwater Wireless Sensor Network. The features are exploited based on the genetic algorithm for energy-aware information fetching, and simulation results are generated to prove its efficiency over conventional algorithms. "Energy-Efficient Traffic Control"[22] is proposed in developing the traffic control system with strategy learning. The energy consumption is decreased, which uses a deep neural network for learning criteria. The optimal output path is generated as output demonstrated in the simulation results. **"**Connectivity Restoration Strategy"[23] is proposed for eliminating the loss of connectivity in multichannel-based WSN. Its main intention is to allocate channels efficiently. The channel assignment and the recovery are executed based on neighborhood-based information. A routing tree is adopted for segregating the sink node information. **"**Efficient Partial Charging Scheme"[24] is proposed to demonstrate the Partial Charging model in wireless sensor networks. A Non-dominated Sorting Genetic Algorithm is developed to integrate the halting points, and charging time for every optimal moment is fetched using a charging timer. Results were generated by simulation output and compared with other performance metrics to prove its efficiency.

"Evidence-Based Interactive Trust Management System"[25] is proposed for removing the nodes which are not in behavior nature. The routing of packets is enabled in trusted nodes, and non-trust nodes are removed. The trust reports are also generated, and the proposed technique detects compromised nodes in the network. "Automated Lightweight Encryption Scheme"[26] is proposed for designing the cryptographic structure for WSN. The sensor nodes which work better with encryption variables are selected, and secured communication is enhanced. Evaluation is carried out using the Cooja simulator, and results are generated to prove its increased performance. "Dominating Set based on Link and Degree and Connecting Tree"[27] is proposed to save energy for enhancing better routing in WSN. Two different phases called, Dominating Set and Connecting Tree algorithm are used to evaluate the connectors in the network. The performance ratio is compared with existing techniques to showcase the increased mode of construction of the topology. "Optimized Cost Effective and Energy Efficient Routing protocol"[28] is proposed to optimize the cost function in Wireless Body Area Network. The link and path loss reliability were applied to the network for optimal route detection to the sink node from the body coordinator. The distance among different sensor nodes was reduced, and inter-BAN communication was enhanced. A comparison of varying performance metric results was carried out to measure the energy of the network throughput. **"**Data Consistency Matrix Based Data Processing Model"[29] is proposed to enhance data storage in the network. Distributed data are fetched through the web, and storage time was assessed by comparing with different models. The proper neighbors are also chosen, and the route matrix factor is considered.

"Whale Optimization for Topology Control (WOTC)" [30]has been developed to enhance the network lifetime. The whale optimization technique is used in a discrete binary form. Using this technique, WSN's coverage and functionality may be preserved while its lifespan is extended. Nodes are reduced in size and energy consumption is reduced as a primary goal of this approach. "Improved Secure Directed Diffusion (ISDD)" [31] protocol enables secure end-to-end data transfer and anonymity between nodes but does not protect relay nodes from DoS assaults. Congestion was alleviated, and energy consumption was reduced, by implementing a cross-layer diffusion design. To make sure

RESEARCH ARTICLE

that relay nodes are reliable and secure, "Trust-based Secure Directed Diffusion Routing (TSDDR)" [32] employs the Energy Trust Model. The energy constraint problem of nodes is addressed using Energy Trust Value, which is based on Direct Trust Value and the remaining energy of the nodes. Session keys of the DH protocol guaranteed secure data transmission and effectively addressed the MITM attack. In addition to its intricacy, the protocol necessitates an excessive amount of communication.

3. ENERGY-AWARE OPTIMAL CLUSTERING & SECURE ROUTING (EAOCSR)

Unequal Clustering is an effective clustering scheme for balanced and uniform energy consumption among the CHs. Varying sized clusters are formed considering the networks inter and intra-cluster traffic. Competition radius is the base for unequal Clustering. Eq.(1) represents the competition radius of an HWSN.

$$R_c = [1 - \propto \frac{d_{max} - d(s_i - DS)}{d_{max} - d_{min}} - \beta(1 - \frac{E_r}{E_{max}})]R_{max} \quad (1)$$

Where d_{max} and d_{min} indicate the minimum and maximum distance between the sensor node and the base station. E_r and E_{max} represent the initial residual energy and maximum residual energy, respectively, while $R_{max}$is the maximum radius of competition. CH selection is based on DEEC for a multilevel HWSN. The number of times a node becomes CH is based on the node's residual energy (E_r) at the round(r). The mean energy of the network at round (r)with N nodes is given in Eq.(2).

$$E_m = \frac{1}{N}\sum_{i=1}^{N} E_i\,(r) \quad (2)$$

The optimal location of the CH is implemented based on the meta-heuristic hunting process of bats, called as echolocation of microbats. The characteristics of bats are listed below, and it forms the base for optimizing CH location in EAOCSR:

- Echolocation – to find the prey
- Loudness – to search and reach the prey
- Frequency – to distribute the wavelength

The unequal clustering method combined with DEEC and optimized by improved BA-UC distributes the energy evenly throughout the network, resulting in stable HWSN with prolonged network life.

Trust-based routing methodology is a recent innovation for reliable data transmission. In HWSN, each node has different energy levels and computation capabilities, so selecting a reliable forwarder is vital. Trust-based routing combined with Directed Diffusion flat routing enforces the energy trust model. Directed Diffusion is a flat routing scheme meant for peer to peer architecture. It is a query driven protocol which executes when there is user requisition, rather than forwarding all the gathered data, reducing the power consumption of the network. The energy trust value gets updated frequently in the neighbouring list of each node, a metric for choosing the trustworthy forwarder.

$$ETV = DT + ES \quad (3)$$

A node's energy consumption (E_c) is the base for calculating energy specification value (ES). $E_c$of a node is determined by the distance between any two communicating nodes, m and n, (d_{mn}), for transmitting certain bits.

$$E_C = \begin{cases} (E_b + d_{mn}^2 E_1)l, & d_{mn} < d_0 \\ (E_b + d_{mn}^2 E_2)l, & d_{mn} < d_0 \end{cases} \quad (4)$$

E_b is the energy utilized by each bit of data, the distance threshold is given by d_0. E_1 and E_2 signifies the energy consumption by the power amplifier.At a specific time(t), the energy specification of a node is given by the ratio of a node's current remaining energy and its initial energy

$$ES(t) = \frac{E_{now}^t}{E_{ini}} \quad (5)$$

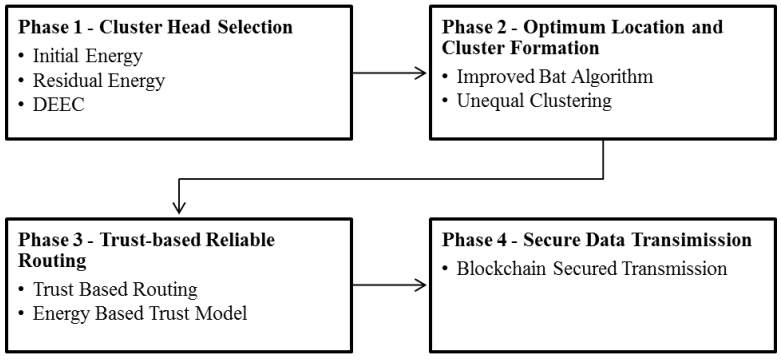

Figure 2 A Schematic Representation of EAOCSR

RESEARCH ARTICLE

Direct Trust (DT) between any two nodes is evaluated based on the successful interactions and unsuccessful interactions among the nodes. A node having high remaining energy has a higher probability of participating in data transmission, achieving balanced energy distribution in the network. These two parameters, DT and ES get updated every unit time to calculate the Energy Trust Value.

Secure Transmission – Directed Diffusion routing[33]transmits data in plain text, requiring a mechanism for secure transmission. Blockchain is used to securely send the gathered data from the CH to the sink. It is a decentralized distributed disruptive technology. Data to be transferred is encrypted, stored in blocks of Blockchain [34] and securely delivered at the destination. The phases of EAOCSR are represented in Figure 2.

3.1. Cluster Head Selection

CH selection follows the DEEC scheme considering the initial energy, residual energy of nodes, and average network energy. This methodology is essential in HWSN, where nodes are of different energy levels and capabilities. A node with high residual energy becomes the candidate for CH during each rotation.

(a) The initial energy and that of the residual energy of a node are determined.

(b) The probability of a node being a CH is represented in Eq.(6)

$$p_i = p_{op} \frac{e_i(r)}{\bar{e}(r)} \quad (6)$$

Based on the initial energy in the round r and average network energy in round r,p_{op} is said to be the reference value.

(c) Every node will have the same energy level in a homogeneous network, which is not true for a heterogeneous WSN. The initial energy of a multilevel HWSN is given as,

$$EN_{Total} = \sum_{i=1}^{N} EN_0(1 + a_i) = EN_0 (N + \sum_{i=1}^{N} a_i) \quad (7)$$

(d) The probability of a node in a heterogeneous WSN to become a CH is determined by Eq.(8)

$$p_i = \frac{p_{op} N(1 + a) e_i(r)}{(N + \sum_{i=1}^{N} a_i)\bar{e}_r} \quad (8)$$

where N represents the number of times a node becomes a CH during its lifetime.

(e) The CH selection follows DEEC, which guarantees that low energy nodes will not die earlier due to energy depletion. The energy is distributed evenly among the nodes in the heterogeneous network.

3.2. Optimal Location and Cluster Formation

Once CHs are selected, optimization should be carried to confirm and locate the CH for fast and easy convergence of clusters. Unequal clustering techniques are ideal for balancing the load between the CHs, supporting reduced network energy consumption.

(a) The CH selected in the previous phase is made temporary CH

(b) Fitness function as specified in Eq.(9). It collaborates the residual energy *(X1)* of the node and the energy consumption rate of the node*(X2)*.It is determined to confirm the temporary CH as official CH, with γ and θ as constants.

$$F = 1/[(\gamma * X1) + (\theta * X2)] \quad (9)$$

(c) Improved BA is applied to find the optimized location of CH. It is based on the echolocation of Bats to identify their prey.

(d) Unequal Clustering is the best solution to avoid hot spot problems is WSN. Unequal clusters are formed using competition radius (R_c), in HWSN, it is calculated using equation 1.

3.3. Trust-Based Reliable Routing

Routing decisions are crucial for a secure and efficient HWSN. Trust-based schemes are more reliable for selecting the next forwarder. The remaining energy of a node is also considered a vital parameter for choosing a trustworthy node.

(a) The reliable path from the CH to the sink is determined using Trust based scheme with a flat routing Directed Diffusion model.

(b) The trust model considers the Direct Trust value and Energy Value of a node called the Energy Based Trust Model.

(c) Direct Trust between any two nodes, m and n, is calculated using Eq.(10).

$$DT_{mn} = \left(\frac{x+1}{x+y+2}\right) \times \left(1 - \frac{y}{w}\right) \times \left(1 - \frac{1}{x+\delta}\right) \quad (10)$$

where x and y indicate successful interaction and unsuccessful interaction among the nodes m and n, respectively

RESEARCH ARTICLE

(d) Energy-based Trust Value indicates the trustworthiness and reliability of the node and is calculated using Eq.(11).

$$ETV_{mn} = \lambda_1 DT_{mn}\ (t) + \lambda_2 ESV_{mn}\ (t) \qquad (11)$$

where ESV_{mn} is the ratio of the node residual energy against the initial energy and it is given by Eq.(5). The remaining energy of node at a time 't' is influenced by Eq.(4), and is calculated using Eq.(12)

$$E_{now}^{t} = E_{now}^{t-1} - E_{ini} \qquad (12)$$

(e) Higher the remaining energy of a node, its Energy Specification Value increases, enhancing the chance to participate in data transmission. It leads to balanced energy retention in the network.

3.4. Secure Data Transmission using Blockchain

Directed Diffusion model transmits data as plain text without considering the security of data. The distributed technology Blockchain is used to send the encrypted information securely to the destination.

(a) Data to be transmitted is read and divided into specific classes

(b) Initialize Blockchain (BC).

(c) Generate block(bl) for the BC.

(d) For each block (bl),

(i) Choose key K from the keyset(ks) that is provided alongwith the data

$$C_k = \int Random(ks(Dataclass, size(ks)) \qquad (13)$$

(ii) Each class of data is then encrypted using a specific key(Ck)

(iii) Generate the Hash signature for the block, $bl(Hash) = Signature$

(iv) Generate pointer to the previous block, $bl(PP) = Address\ of\ the\ last\ block$

(v) Add block, bl to BC

(e) Blockchain reaches the sink through the established path in the previous phase

(f) Received block of data is decrypted at the destination using the hash code and key

$$Actual\ Data(D) = \int_{i=1}^{size\ of\ blocks} \sum D \cup d \qquad (14)$$

Where$d$ is computed using Eq.(15)

$$d = decrypt(bl, data, ks) \qquad (15)$$

Data transmission using Blockchain is more secure as data manipulation is not possible. Being a decentralized distributed technique, updation or deletion of data is possible only with the consent of all the participating nodes.

4. SIMULATION SETTING

The effectiveness of the proposed protocol, EAOCSR, is analyzed for the performance metrics such as: (a) Energy Consumption, (b) Throughput, (c) Network Lifetime, (d) Stability and (e) Security. EAOCSR is analyzed against the existing protocols WOTC, TSDDR and ISDD. The algorithm was simulated using Matlab-2019 for network simulation, on a system having 2 GB RAM, 1 TB Hard Disk, Intel i3 and Windows 10, with the initial parameters as shown in Table 1. The simulation is performed with 300 nodes are deployed randomly in the specific area of 200mx 200m.

Parameter	Values
Distribution area	200mx200m
No, of nodes	100-300
Initial Energy of Node	10J
Initial DTV	0.5
Transmission Range	100m
Data Packet Size	512bits
Number of Sink nodes	5
Location of nodes	Randomly Generated
Heterogeneity of Nodes	2 level
Time for simulation	150 sec
Simulation Run	10

Table 1 Simulation Settings

4.1. Energy Utilization Analysis

Figure 3 shows how much less energy EAOCSR consumes compared to current procedures. The number of nodes on the X-axis corresponds to the energy consumption percentage on the Y-axis. The network's energy consumption may be reduced by distributing energy evenly and reducing hotspots by unequal Clustering. The proposed EAOSCR uses a trust model based on the remaining energy of a node to make routing decisions. It aids in the uniform distribution of energy across the network, reducing consumption. Existing and suggested methods are compared in Table 3 using the energy consumption rate shown in Figure 3.

RESEARCH ARTICLE

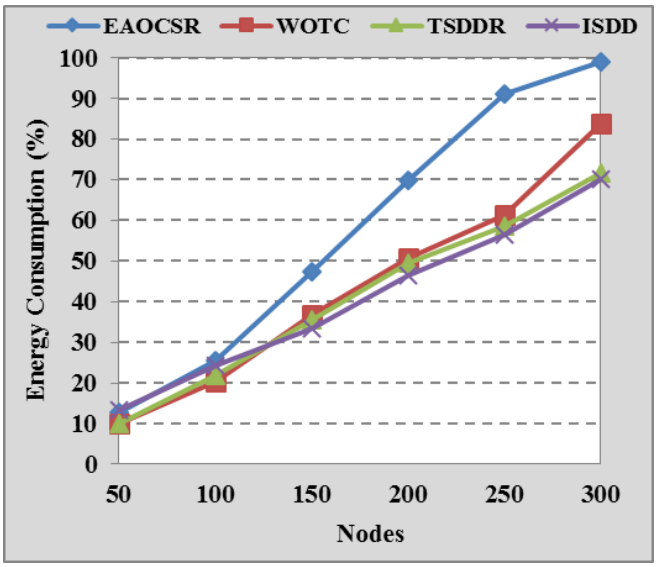

Figure 3 Energy Consumption Analysis

Protocol / No. of Nodes	EAOCSR	WOTC	TSDDR	ISDD
50	12.76	9.87	10.14	13.29
100	25.48	20.23	21.79	24.14
150	47.44	36.63	35.59	33.51
200	69.91	50.62	49.37	46.33
250	91.17	61.34	58.59	56.44
300	99.11	83.86	71.72	70.12

Table 3 Result Values of Energy Consumption Analysis

4.2. Throughput Analysis

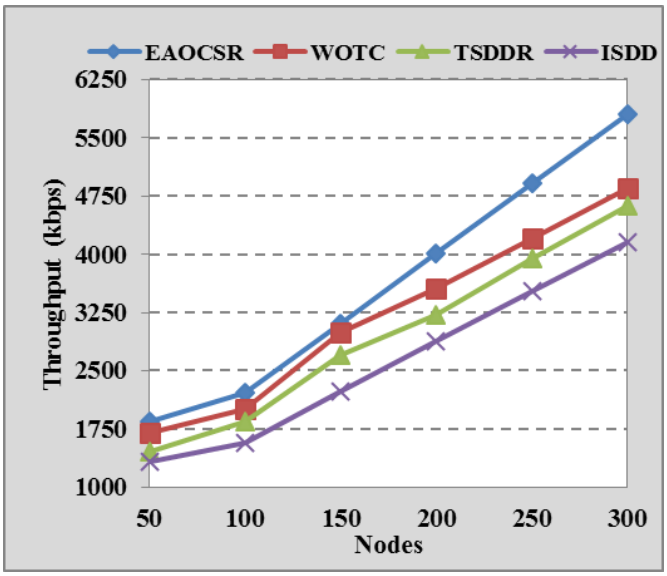

Figure 4 Throughput Analysis

Using the suggested EAOCSR protocol, Figure 4 shows an ideal throughput. The X-axis depicts the number of nodes, while the Y-axis displays throughput in kilobits per second. EAOCSR's trust-based energy-aware routing decisions tend to boost throughput compared to competing protocols. EAOCSR utilizes Directed Diffusion flat routing model ensuring path reinforcement among the participating nodes, hence reduced packet loss. The result analysis clearly specifies the increased throughput of the proposed algorithm, even when the number of nodes gets increased. Figure 4's numerical representation is depicted in Table 4.

Protocol / No. of Nodes	EAOCSR	WOTC	TSDDR	ISDD
50	1852	1700	1456	1321
100	2212	2002	1850	1564
150	3110	2988	2700	2231
200	4012	3556	3211	2875
250	4912	4200	3948	3519
300	5811	4855	4628	4163

Table 4 Result Values of Throughput Analysis

4.3. Network Lifetime

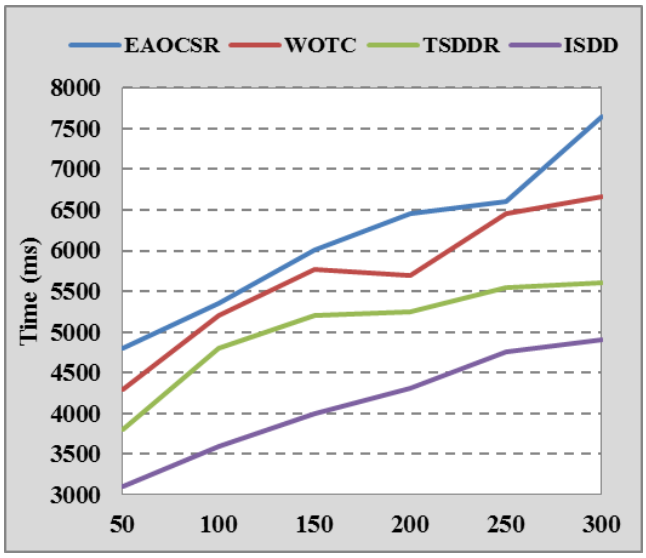

Figure 5 Network Lifetime Analysis

Figure 5 assures the prolonged network lifetime of EAOCSR compared to the existing protocols. The selection and rotation of cluster head based on residual energy and initial energy, attributed by DEEC, maintains even energy distribution in the heterogeneous WSN. The unequal clustering scheme eliminates the hotspot problem in phase 1 of the proposed protocol. The network life is not affected by the number of nodes. Being HWSN, each node will have different energy

RESEARCH ARTICLE

levels. The EAOCSR protocol assures that all nodes die simultaneously rather than the earlier death of nodes with low energy. The network lifetime (in ms) of EAOCSR is high than other protocols, and the respective numerical results are provided in Table 5.

Protocol / No. of Nodes	EAOCSR	WOTC	TSDDR	ISDD
50	4800	4299	3801	3100
100	5350	5198	4800	3600
150	6003	5775	5211	4113
200	6450	5702	5250	4311
250	6674	6451	5550	4760
300	7650	6670	5601	4913

Table 5 Result Values of Network Lifetime Analysis

4.4. Stability

The comparative analysis of stability, half node death and network lifetime of EAOCSR with that of WOTC, TSDDR, ISDD is illustrated in Figure 6. The X-axis represents the protocols, while the Y-axis represents the number of simulation rounds. The stability of the heterogeneous WSN is ensured by the energy retention capability (unequal Clustering with DEEC) and secure routing mechanism (Blockchain endorsed trust model) of the proposed protocol. The protocol EAOCSR maintains energy stability in all phases, drastically reducing malicious attacks and packet loss. The stability period, half network death of node and network lifetime of the proposed EAOCSR is superior to the existing protocols. The respective numerical values are given in Table 6.

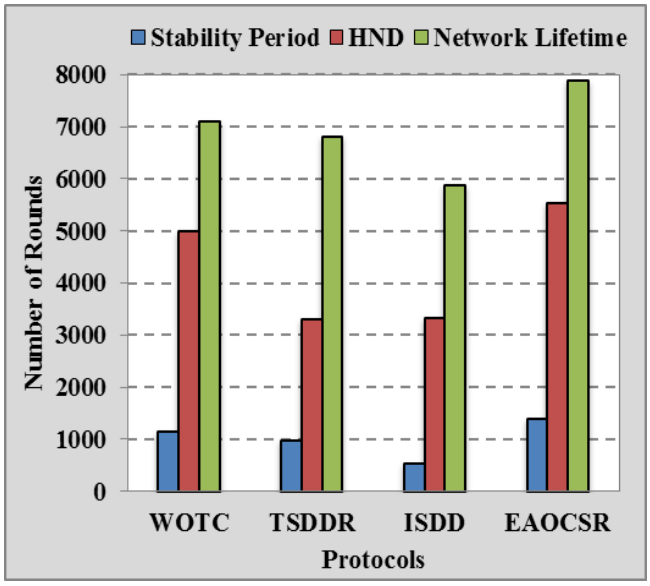

Figure 6 Stability Analysis

Protocols / Parameters	WOTC	TSDDR	ISDD	EAOCSR
Stability Period	1150	975	525	1400
HND	5000	3300	3331	5525
Network Lifetime	7100	6800	5880	7899

Table 6 Result Values of Stability Analysis

4.5. Security

Figure 7 represents the security performance of EAOCSR with that of the number of untrusted nodes. The X-axis contains the protocols for comparison, while Y-axis shows the security percentage with the increase in the number of untrusted nodes. The security provided by the proposed protocol, through Blockchain data transmission, is comparatively high when compared with WOTC, TSDDR and ISDD. The output signifies that even as the number of untrusted nodes increases, the security percentage remains stable and high. The numerical values of security percentage are provided in Table 7.

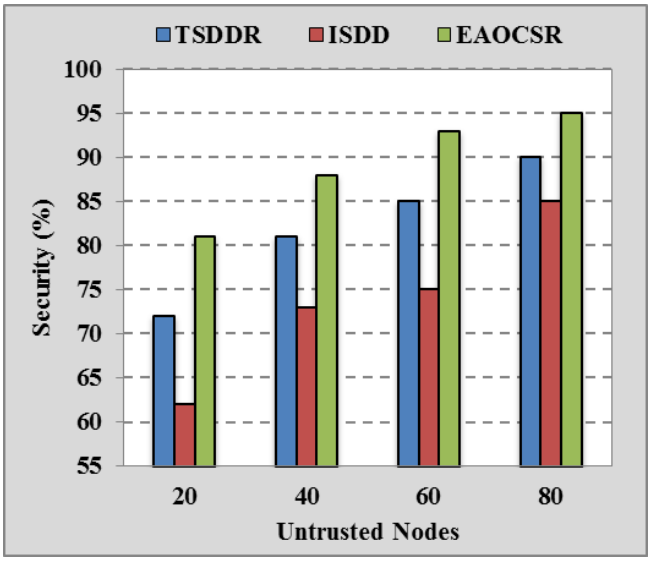

Figure 7 Security Analysis

Protocol / Untrusted Nodes	TSDDR	ISDD	EAOCSR
20	72	62	81
40	81	73	88
60	85	75	93
80	90	85	95

Table 7 Result Values of Security Analysis

RESEARCH ARTICLE

5. CONCLUSION

The energy of the constrained sensor nodes in WSN gets depleted faster. In an HWSN, nodes are of different capabilities and energy levels. The initial energy of each node varies in HWSN, and it is ideal to use initial energy and residual energy as parameters to distribute energy uniformly in the network. Appropriate dissemination of energy throughout the network is a vital issue in HWSN. This paper proposed an amalgamated protocol called Energy-Aware Optimal Clustering & Secure Routing (EAOCSR) to reduce the energy consumption in secured routing. The protocol is an energy-efficient scheme that collectively provides optimal Clustering, reliable routing and secure data transmission. Optimal Clustering is ensured using unequal Clustering supported by DEEC. For selecting the next forwarder, trust-based reliable routing is adopted in EAOSCR. Secured data transmission is guaranteed by Blockchain technology through dynamic class-specific data blocks. The stability of the network is determined by uninterrupted functionality and securing the network from malicious attacks. The proposed protocol EAOCSR ensures efficient energy utilization in all phases and distributes the energy uniformly over the network. The experimental results of the proposed EAOCSR are carried out in MATLAB, and it depicts that it has superior performance than other existing protocols in terms of energy utilization, network lifetime, stability and security percentage.

REFERENCES

[1] S. De and B. Chakraborty, "An energy-efficient wireless sensor network construction algorithm for air quality condition detection system," Comput. Electr. Eng., vol. 91, p. 107064, 2021, doi: https://doi.org/10.1016/j.compeleceng.2021.107064.

[2] A. I. Saleh, K. M. Abo-Al-Ez, and A. A. Abdullah, "A Multi-Aware Query Driven (MAQD) routing protocol for mobile wireless sensor networks based on neuro-fuzzy inference," J. Netw. Comput. Appl., vol. 88, pp. 72–98, 2017, doi: https://doi.org/10.1016/j.jnca.2017.02.016.

[3] M. Farsi, M. Badawy, M. Moustafa, H. A. Ali, and Y. Abdulazeem, "A Congestion-Aware Clustering and Routing (CCR) Protocol for Mitigating Congestion in WSN," IEEE Access, vol. 7, pp. 105402–105419, 2019, doi: 10.1109/ACCESS.2019.2932951.

[4] Z. Zhou, B. Yao, R. Xing, L. Shu, and S. Bu, "E-CARP: An Energy Efficient Routing Protocol for UWSNs in the Internet of Underwater Things," IEEE Sens. J., vol. 16, no. 11, pp. 4072–4082, 2016, doi: 10.1109/JSEN.2015.2437904.

[5] K. Kalaivanan and V. Bhanumathi, "Reliable location aware and Cluster-Tap Root based data collection protocol for large scale wireless sensor networks," J. Netw. Comput. Appl., vol. 118, pp. 83–101, 2018, doi: https://doi.org/10.1016/j.jnca.2018.06.005.

[6] J. Ramkumar and R. Vadivel, "CSIP—cuckoo search inspired protocol for routing in cognitive radio ad hoc networks," in Advances in Intelligent Systems and Computing, 2017, vol. 556, pp. 145–153, doi: 10.1007/978-981-10-3874-7_14.

[7] J. Ramkumar and R. Vadivel, "Improved frog leap inspired protocol (IFLIP) – for routing in cognitive radio ad hoc networks (CRAHN)," World J. Eng., vol. 15, no. 2, pp. 306–311, 2018, doi: 10.1108/WJE-08-2017-0260.

[8] J. Ramkumar and R. Vadivel, "Performance Modeling of Bio-Inspired Routing Protocols in Cognitive Radio Ad Hoc Network to Reduce End-to-End Delay," Int. J. Intell. Eng. Syst., vol. 12, no. 1, pp. 221–231, 2019, doi: 10.22266/ijies2019.0228.22.

[9] J. Ramkumar and R. Vadivel, "Multi-Adaptive Routing Protocol for Internet of Things based Ad-hoc Networks," Wirel. Pers. Commun., pp. 1–23, Apr. 2021, doi: 10.1007/s11277-021-08495-z.

[10] J. Ramkumar and R. Vadivel, "Bee inspired secured protocol for routing in cognitive radio ad hoc networks," INDIAN J. Sci. Technol., vol. 13, no. 30, pp. 3059–3069, 2020, doi: 10.17485/IJST/v13i30.1152.

[11] J. Ramkumar and R. Vadivel, "Intelligent Fish Swarm Inspired Protocol (IFSIP) For Dynamic Ideal Routing in Cognitive Radio Ad-Hoc Networks," Int. J. Comput. Digit. Syst., vol. 10, no. 1, pp. 1063–1074, 2020, doi: http://dx.doi.org/10.12785/ijcds/100196.

[12] R. Vadivel and J. Ramkumar, "QoS-Enabled Improved Cuckoo Search-Inspired Protocol (ICSIP) for IoT-Based Healthcare Applications," pp. 109–121, 2019, doi: 10.4018/978-1-7998-1090-2.ch006.

[13] D. Sharma and A. P. Bhondekar, "Traffic and Energy Aware Routing for Heterogeneous Wireless Sensor Networks," IEEE Commun. Lett., vol. 22, no. 8, pp. 1608–1611, Aug. 2018, doi: 10.1109/LCOMM.2018.2841911.

[14] S. Al-Sodairi and R. Ouni, "Reliable and energy-efficient multi-hop LEACH-based clustering protocol for wireless sensor networks," Sustain. Comput. Informatics Syst., vol. 20, pp. 1–13, Dec. 2018, doi: 10.1016/j.suscom.2018.08.007.

[15] A. Benzerbadj, B. Kechar, A. Bounceur, and M. Hammoudeh, "Surveillance of sensitive fenced areas using duty-cycled wireless sensor networks with asymmetrical links," J. Netw. Comput. Appl., vol. 112, pp. 41–52, 2018, doi: https://doi.org/10.1016/j.jnca.2018.03.027.

[16] R. Yarinezhad and S. N. Hashemi, "Solving the load balanced clustering and routing problems in WSNs with an fpt-approximation algorithm and a grid structure," Pervasive Mob. Comput., vol. 58, p. 101033, 2019, doi: https://doi.org/10.1016/j.pmcj.2019.101033.

[17] S. Chinnaswamy and A. K, "Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks," Comput. Electr. Eng., vol. 91, p. 107130, 2021, doi: https://doi.org/10.1016/j.compeleceng.2021.107130.

[18] B. Shah et al., "Guaranteed lifetime protocol for IoT based wireless sensor networks with multiple constraints," Ad Hoc Networks, vol. 104, p. 102158, 2020, doi: https://doi.org/10.1016/j.adhoc.2020.102158.

[19] A. Chowdhury and D. De, "FIS-RGSO: Dynamic Fuzzy Inference System Based Reverse Glowworm Swarm Optimization of energy and coverage in green mobile wireless sensor networks," Comput. Commun., vol. 163, pp. 12–34, 2020, doi: https://doi.org/10.1016/j.comcom.2020.09.002.

[20] G. D. O'Mahony, K. G. McCarthy, P. J. Harris, and C. C. Murphy, "Developing novel low complexity models using received in-phase and quadrature-phase samples for interference detection and classification in Wireless Sensor Network and GPS edge devices," Ad Hoc Networks, vol. 120, p. 102562, 2021, doi: https://doi.org/10.1016/j.adhoc.2021.102562.

[21] M. Faheem, M. A. Ngadi, and V. C. Gungor, "Energy efficient multi-objective evolutionary routing scheme for reliable data gathering in Internet of underwater acoustic sensor networks," Ad Hoc Networks, vol. 93, p. 101912, 2019, doi: https://doi.org/10.1016/j.adhoc.2019.101912.

[22] J. Lu, L. Feng, J. Yang, M. M. Hassan, A. Alelaiwi, and I. Humar, "Artificial agent: The fusion of artificial intelligence and a mobile agent for energy-efficient traffic control in wireless sensor networks," Futur. Gener. Comput. Syst., vol. 95, pp. 45–51, 2019, doi: https://doi.org/10.1016/j.future.2018.12.024.

[23] S. Chouikhi, I. El Korbi, Y. Ghamri-Doudane, and L. Azouz Saidane, "Distributed connectivity restoration in multichannel wireless sensor networks," Comput. Networks, vol. 127, pp. 282–295, 2017, doi: https://doi.org/10.1016/j.comnet.2017.08.016.

[24] S. Priyadarshani, A. Tomar, and P. K. Jana, "An efficient partial charging scheme using multiple mobile chargers in wireless rechargeable sensor networks," Ad Hoc Networks, vol. 113, p. 102407, 2021, doi: https://doi.org/10.1016/j.adhoc.2020.102407.

[25] P. S. Uma Priyadarsini and P. Sriramya, "Disaster management using evidence-based interactive trust management system for wireless sensor

RESEARCH ARTICLE

networks by Internet of Things," Comput. Electr. Eng., vol. 75, pp. 164–174, 2019, doi: https://doi.org/10.1016/j.compeleceng.2019.02.020.
[26] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," Ad Hoc Networks, vol. 115, p. 102448, 2021, doi: https://doi.org/10.1016/j.adhoc.2021.102448.
[27] C. Luo, J. Yu, D. Li, H. Chen, Y. Hong, and L. Ni, "A Novel Distributed algorithm for constructing virtual backbones in wireless sensor networks," Comput. Networks, vol. 146, pp. 104–114, 2018, doi: https://doi.org/10.1016/j.comnet.2018.09.016.
[28] N. Kaur and S. Singh, "Optimized cost effective and energy efficient routing protocol for wireless body area networks," Ad Hoc Networks, vol. 61, pp. 65–84, 2017, doi: https://doi.org/10.1016/j.adhoc.2017.03.008.
[29] G. J., S. J., S. Y., and M. V., "Data consistency matrix based data processing model for efficient data storage in wireless sensor networks," Comput. Commun., vol. 151, pp. 172–182, 2020, doi: https://doi.org/10.1016/j.comcom.2019.12.060.
[30] M. M. Ahmed, E. H. Houssein, A. E. Hassanien, A. Taha, and E. Hassanien, "Maximizing lifetime of wireless sensor networks based on whale optimization algorithm," Adv. Intell. Syst. Comput., vol. 639, pp. 724–733, 2018, doi: 10.1007/978-3-319-64861-3_68.
[31] J. Sengupta, S. Ruj, and S. Das Bit, "End to end secure anonymous communication for secure directed diffusion in IoT," PervasiveHealth Pervasive Comput. Technol. Healthc., pp. 445–450, Jan. 2019, doi: 10.1145/3288599.3295577.
[32] X. Yu, F. Li, T. Li, N. Wu, H. Wang, and H. Zhou, "Trust-based secure directed diffusion routing protocol in WSN," J. Ambient Intell. Humaniz. Comput. 2020, pp. 1–13, Nov. 2020, doi: 10.1007/S12652-020-02638-Z.
[33] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," J. Ambient Intell. Humaniz. Comput. 2020 1111, vol. 11, no. 11, pp. 4613–4641, Jan. 2020, doi: 10.1007/S12652-020-01710-Y.
[34] M. Hema Kumar, V. Mohanraj, Y. Suresh, J. Senthilkumar, and G. Nagalalli, "Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN," J. Ambient Intell. Humaniz. Comput. 2020 125, vol. 12, no. 5, pp. 5287–5295, Apr. 2020, doi: 10.1007/S12652-020-02007-W.

Authors

Swapna M P, Research Scholar (PhD), Department of Computer Science, Sri Ramakrishna College of Arts & Science for Women, Coimbatore, India. She has 8 years of teaching experience and 11 years of industry experience. She has presented 12 papers in International and National Conferences, has published 5 articles in peer viewed journals and has published 2 books. Broad field of interest includes Networking, Artificial Intelligence, Programming Paradigms, Theory of Computation. Main area of research includes WSN and Blockchain Technology.

Dr. G Satyavathy, completed her Ph.D from Anna University. Currently working as Associate Professor in the Department of Computer Science, Sri Ramakrishna College of Arts & Science for Women, Coimbatore, India. She has 21 years of teaching experience. She has published more than 25 research papers in reputed International and National peer reviewed journals, has presented more than 30 papers in International and National Conferences and has published 6 books. She is a recognized research supervisor under Bharathiar University, Doctoral committee member for various universities, University representative for Bharathiar University Examinations, editor and reviewer for various peer reviewed journals. She is the coordinator of Research & Development cell, acts are Scholarship Coordinator and serves as the Discipline committee member of the college. Her broad field of research & teaching interests include Networking, Image Processing, Information Security and Mobile Computing.

How to cite this article:

Swapna M P, G. Satyavathy, "Energy-Aware Optimal Clustering and Secure Routing Protocol for Heterogeneous Wireless Sensor Network", International Journal of Computer Networks and Applications (IJCNA), 9(1), PP: 12-21, 2022, DOI: 10.22247/ijcna/2022/211594.