Heterogeneous Wireless Sensor Network Design with Optimal Energy Conservation and Security through Efficient Routing Algorithm

D. Bhanu*, R. Santhosh

Department of Computer Science and Engineering, Karpagam Academy of Higher Education, Coimbatore, India
Emails: bhanu.saran@gmail.com; santhoshrd@gmail.com

Abstract

A heterogeneous wireless sensor network (H-WSN) comprises multiple sensor nodes having varied abilities, like diverse processing power and sensing range. H-WSN deployment and topology control seem to be more difficult than homogeneous WSNs. Research on H-WSNs has increased in the last few years to improve real-time sensor networks' reliability and deliver better networking services than a homogenous WSN does. When it comes to H-WSN's energy consumption and security, the major problem remains the efficient routing process. To that end, this research aims at demonstrating how an efficient routing algorithm of hierarchical H-WSN can greatly enhance the network's performance. It is important to note that the nodes' capabilities mostly determine the suitability of a given routing algorithm. Hence, the H-WSN design issues for routing in a heterogeneous environment are discussed in this paper. This research designs an Optimal Energy Conservation and Security-aware Routing Algorithm (OECS-RA) for H-WSN using clustering and a secure-hop selection scheme. In this proposed model, the optimal cluster head selection and routing have been found through various computational stages based on the energy conservation of each sensor node. It further secures the transmission by selecting the secured node with credential factor computation and comparing each hop of the optimal route. The MATLAB simulation scenario finds the significant performance of the routing mechanism with security compared to existing models. The proposed OECS-RA gives highly recognizable throughput, lifetime, energy efficiency, and reliability. With these results, this proposed algorithm is suggested for real-time implementation in the medical industry, transportation, education, business, etc.

Keywords: Heterogeneous Wireless Sensor Network; Energy Optimization; Cluster; Security; Routing

1. Introduction

Wireless sensor networks consist of a large number of small nodes with various features, like conscience, broadcasting across small distances, and multi-hop routing [1]. They are tiny nodes with numerous capabilities, including the provision of wireless transmissions, processing, and high sensitivity and selectivity. They are deployed in remote places to acquire, monitor data, and communicate sensitive details regarding specific processes that are intended to be monitored in that domain. According to the purposes and goals that are being met, sensor nodes can be deployed in a variety of ways: either in a uniform, random, or linear fashion [2-3]. Nevertheless, WSNs can be used in a variety of ways to gather data and conduct mission-critical operations more quickly and effectively. In this context, mission-critical activities require an extremely high number of nodes that are responsible for information sensing, data processing, and the establishment of a communication link between other nodes [4]. Due to a large number of sensor nodes and the need to analyze and monitor data, WSNs often conserve more energy than other types of networks.

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

In general, the batteries are used to energize WSN nodes. WSN energy consumption seems to be an important factor to consider while designing and implementing a real-time network. Various strategies, algorithms, and protocols have been used to reduce energy consumption and increase the network's lifespan [5]. There are two types of WSN environments such as heterogeneous and homogenous WSNs. When all nodes have the same starting energy and hardware capabilities, a homogeneous mechanism has been used, while a heterogeneous mechanism can be used when all nodes have varying degrees of energy and hardware capabilities, respectively. In recent years, low-energy adaptive clustering algorithms, multiple heterogeneous routing protocols, and energy management have become offered [6-7]. When it comes to sensor networks, clustering is often taken into account since it provides for greater flexibility in routing. In addition to acting as fusion points for data aggregation, cluster heads help minimize the quantity of data sent to the base station. Battery life and hardware complexity are about the same among sensors in homogenous networks. In a homogeneous network, it is obvious that the cluster head nodes will be overloaded with long-range broadcasts to the far base station and the additional processing required for data aggregation and protocol coordination when using static clustering only [8]. As a result, the cluster's head nodes are the first to die. For maximum efficiency, the system should be shut down with as little lost energy as possible, such that each node's battery runs out at around the same time.

On the other hand, the disadvantage of a homogenous network and role rotation is that all nodes must have the hardware capabilities sufficient to operate as cluster heads. When a heterogeneous sensor network is deployed, on the other hand, different nodes with various battery capacities and capabilities are employed [9]. To ensure cost efficiency, just a few cluster head nodes can have the more complicated technology and additional battery power, which can be housed in those nodes. However, fixing the cluster head nodes prevents role rotation. Because of this, the sensor nodes that are farthest away from the cluster heads always consume more energy than those that are nearest to them. When nodes employ multi-hopping to reach the cluster head, the nearest nodes have the biggest energy cost since they are repeating information back and forth [10-11]. As a result, the network's energy drainage pattern is never consistent. WSNs are more likely to be heterogeneous networks than homogeneous ones because of the radio communication features, random occurrences, and failures such as short-term connection failures or the morphological characteristics of the field. On the other hand, in homogeneous networks, the routing protocols can operate effectively, and in heterogeneous networks, they struggle to distribute energy equally amongst nodes, and this results in a decrease in their performance compared to protocols that work in both circumstances [12].

Another aspect of H-WSNs is the challenge of ensuring network security for reliable communication. Confidentiality, integrity, availability, authentication, and non-repudiation are among the security objectives that drive the need for secure communication between heterogeneous devices in H-WSNs [13]. Numerous security mechanisms have to be designed and implemented to ensure that the communication should not be harmed by any assault. These networks can allow communication to go easy at the cost of possible hazards, however, these threats are rising in scope as technology advances. The establishment of trust between the transmitting devices is a critical step in initiating communication among these systems [14]. Security mechanism becomes critical in these systems due to their diverse nature, dynamic and powerful transmission system, and lack of dependability among the gadgets along with energy management. The trust in energy-efficient network frameworks is the confidence or certainty that exchange points based on historical correspondence are reliable with minimal energy consumption [15]. Before devices begin communicating with one another or doing any computational activity inside the framework, a basic stage seems to be the establishment of trust. Thereby, this article works contributes the following features:

This paper includes clustering and a secure-hop selection technique to develop an OECS-RA (Optimal Energy Conservation and Security-aware Routing Algorithm) for H-WSNs.

The ideal cluster head selection and routing have been determined in several computational phases based on the energy conservation of each sensor node to pick the best possible path.

It uses credential factor computation which selects the secure node and compares each hop of the best path.

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

The upcoming section involves extended literature study followed by proposed work. After covering detailed explanation of the proposed OECS-RA, this article presents the result and discussion section. Finally, this article endsup with conclusion and the future scope.

2. Related works

The extended literature study on related works concentrated on the two major challenges to H-WSNs such as energy efficiency and security. Some of the related works are discussed below:

To increase the energy efficiency of H-WSNs, Abdul Qawy et al., [16] suggested the Threshold-oriented and Energy-harvesting enabled Multi-level Stable Election Protocol (TEMSEP) implementing reactive protocols based on hierarchical clustering, energy-harvesting relay nodes, and heterogeneous sensor nodes that provide infinite battery initial energy. In their protocol, rather than transmitting data continuously, the network nodes in TEMSEP could adapt to changes in key parameters or events of interest by sending their data only when necessary. Using heterogeneous threshold values and a sliding window formulation, they presented a novel thresholding model with a reactive behavior detection mechanism. By decreasing network traffic load by up to 53% and saving up to 73% of the total dissipated energy, TEMSEP significantly enhanced network performance, according to substantial simulation results.Abbas et al., [17] proposed and evaluated a Heterogeneous Network Protocol with Energy Efficient Approach (HPEEA) delivering energy-efficient routing protocol design solutions. They used clustering protocols to create efficient routing for heterogeneous WSNs in this work. Their HPEEA was based on the location data and residual energy of sensor nodes. By employing the suggested HPEEA protocol and its ideal delays of the initial node in a heterogeneous WSN, the stability period in network lifespan was increased using stable concentric clustering by selecting a cluster head using coupling rate and the location of aggregate nodes, leveraging K-theorem. With this protocol, the number of dead nodes decreases dramatically throughout 5000 rounds as the number of nodes in the network grows. Compared to existing protocols, these two novel techniques have a longer network lifespan. WSN clustering has been afflicted by the challenge of selecting cluster heads from a pool of network nodes or members of an associated cluster regularly.

An enhanced energy-efficient network-integrated super-heterogeneous routing protocol (E-BEENISH) was presented by Zhang et al., [18], which could analyze the communication energy consumption of WSN clusters and a vast variety of energy levels. As the remaining energy and the distance from the sink to the node were weighted, E-BEENISH calculated the probability of each node becoming a cluster head. Furthermore, they investigated the effect of node heterogeneity on energy consumption in the simulated H-WSN. After examining the sensitivity of their stable election process, they discovered that the E-BEENISH had the longest stability area for the appropriate weight and distance of the heterogeneity parameters that capture energy imbalance in the network. It is critical for many applications that the E-BEENISH could extend the system lifespan by an order of magnitude compared to conventional clustering procedures. When an attacker has access to a wireless sensor network's pre-existing information, existing security measures for data sharing among heterogeneous sensor nodes were examined by Parande, S., & Mallapur, J. D. [19]. Although certain security vulnerabilities were observed in H-WSNs, there is still scope for improvement in the methods that are being used today. They incorporated several static sink nodes scattered throughout a geographical region and mobile sensor nodes of the H-WSNs. Analytical modeling was used to create a lightweight encryption technique to obtain a dynamic authentication policy. Their proposal was developed in MATLAB and the results of the model showed that it offers lower memory reliance and cheaper cost in comparison to conventional security techniques. However, they did not concentrate on the energy consumption of H-WSN, which is the crucial parameter for network lifetime assurance.

Mall et al., [20] employed a drone-enabled architecture that could be utilized in an unsupervised environment to receive information from the sensor node. They proposed a lightweight mutual authentication and session key agreement technique for H-WSNs. They were focused on building a security protocol using Physically Unclonable Function (PUF) technology with a hash function to ensure lightweight features. No security vulnerabilities were found in Scyther Simulation findings for the proposed CoMSeC++, according to their results. According to non-formal security analysis, the suggested CoMSeC++ was impenetrable to many threats. PUF technology could help CoMSeC++ secure itself from drone and sensor node compromise assaults, which are

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

both vital and potentially damaging. So even if an attacker gets hold of the sensor node or drone, they would not have had access to any sensitive data. In addition, their model performance aspect is remarkable with lower computation and communication costs.

According to Bhushan, B., and Sahoo, G. [21], the efficient clustering architecture could overcome many security issues and improve the energy efficiency and lifespan of the network. The suggested Intelligent and Secured Fuzzy Clustering Algorithm with Balanced Load Sub-cluster Formation (ISFC-BLS) routing protocol for WSNs and the accompanying maintenance techniques and routing algorithms was established as a safe and energy-efficient approach. They proposed a strategy for selecting cluster heads in hierarchical topology based on a fuzzy-based clustering technique that promoted cooperative communication in the network, and a balanced load sub-cluster creation that could help to identify the nodes that join the cluster. They used ant colony optimization to find the most efficient route to the target. The authors claimed that ISFC-BLS is more effective and secure than existing clustering strategies, such as energy-efficient heterogeneous ring clustering by reducing the number of control messages and the node energy consumption for increasing network lifetime and reducing energy consumption. These existing approaches were influenced by proposing heterogeneous wireless sensor network design with optimal energy conservation and security through efficient routing algorithms. The extended literature study helps to fix the research problem and opens up the path to finding a research solution that improves the performance of many real-time applications using H-WSNs with optimal energy consumption and the highest security. The following section gives the design methodology of the proposed Optimal Energy Conservation and Security-aware Routing Algorithm (OECS-RA) for H-WSN using clustering and a secure-hop selection scheme.

3. Optimal Energy Conservation and Security-Aware Routing Algorithm (OECS-RA)

The proposed OECS-RA is intended for H-WSNs having a network of sensors having wireless links with dissimilar communication ranges for example, as shown in Figure 1. The H-WSNs can have different communication technology like IEEE 802.3, IEEE 802.11, and ZigBee. In H-WSNs, varied nodes with multiple sensing ranges or computing capabilities, or a WSN in which nodes are outfitted with distinct sensors to provide different sensing services. While deploying WSNs, we can achieve the right balance between cost and performance by mixing high-end and low-end sensors. This is because the high-end sensors have high process throughput and long communication or sensing range, while the low-end sensors have low process throughput and short communication or sensing range. WSNs benefit from clustering since it increases their scalability and lifespan. Since sensors in WSNs are battery-powered and often unattended, energy consumption must be minimized to extend the network's lifespan in all areas. Routing protocols in H-WSNs are application-dependent, and the goals they are designed to achieve vary depending on the applications they are used for.

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

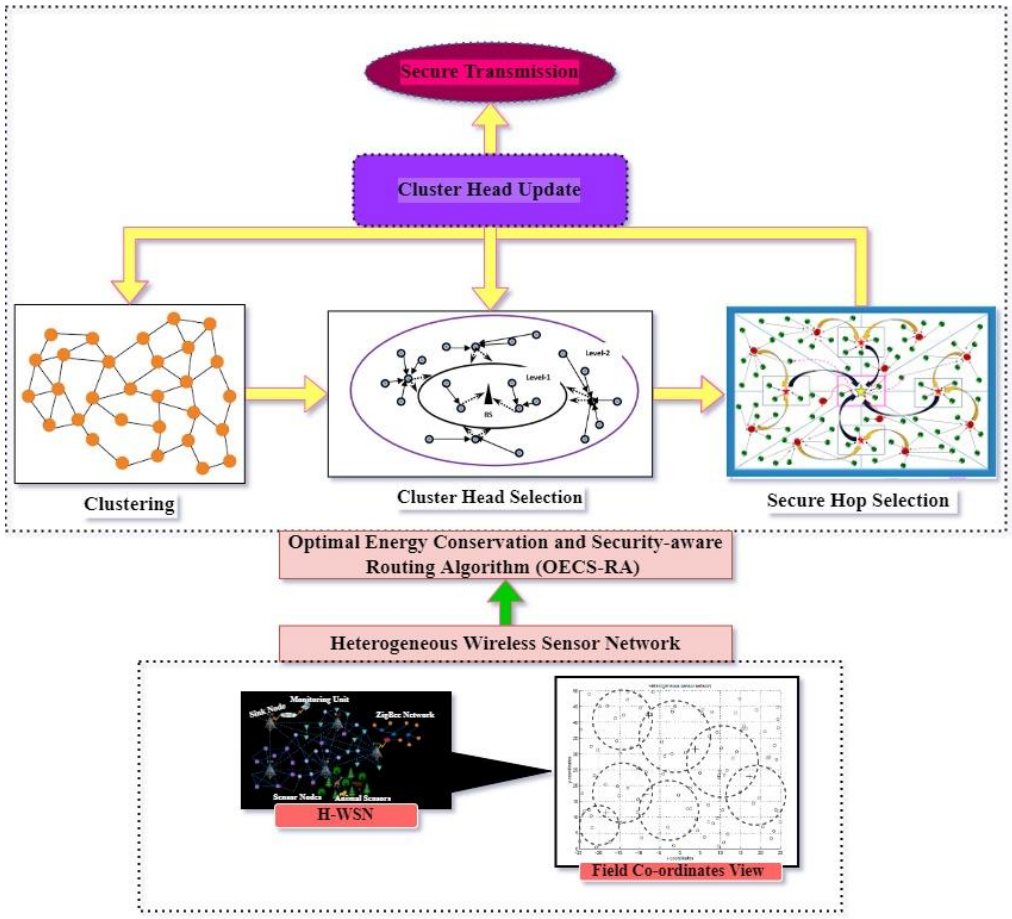

Figure 1: Architectural Model of H-WSN using OECS-RA

The H-WSN can be constructed of hundreds of sensor nodes spread randomly. To extend the life of a sensor network, clustering has become one of the greatest techniques to reduce energy usage. The scalability and lifespan of the network can both be improved as well through clustering. Clustering techniques for HWSNs should be energy efficient to leverage the advantages of node heterogeneity. The proposed OECS-RA ensures security and improved energy efficiency by integrating an optimized clustering scheme and secure hop selection as seen in figure 1. The real-time implementation of H-WSN with OESC-RA begins with the establishment of various sensors having different characteristics to achieve a common goal or to assist in significant decision-making. After implementing H-WSN, the clustering technique is applied with the assurance of minimal energy conservation. In this scheme, the cluster nodes and cluster heads are selected based on the probability values of communication cost and residual energy. The lesser communication cost and residual energy of a node become the criterion for selecting a node as a cluster head.

The routing technique for the data transmission in the H-WSN using OECS-RA have minimal distance and low power consumption for each hop. Eventually, the security scheme of the proposed OECS-RA ensures the confidentiality, availability, and integrity of the data to be communicated through the H-WSN. As a result of the open nature of H-WSN communication channels, they are vulnerable to a variety of attacks, such as denial-of-service attacks, sibyl attacks, wormhole attacks, spoofing, selective forwarding attacks, tempering attacks, and flooding attacks. The secured hope scheme uses a hybrid evolutionary algorithm to prevent various security attacks.

Mathematical Model for Optimised Energy-Efficient Clustering and Routing

In Figure 2, the green circles indicate overlay sensors while the orange circles represent standard sensors in a square sensing area with side lengths of M meters. All information gathered by the sensors must be sent to a receiver/collector that is beyond the sensing area. In what follows, "receiver" and "collector" are used synonymously. The sensing field is placed at L meters from the collector's position of $(0, -L)$. Assume this spot to be permanent. This work presumes that the

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

sensors have pre-configured or self-configured such that they all know where the receiver is. The number of regular sensors out there is larger than overlay sensors and denoted by S.

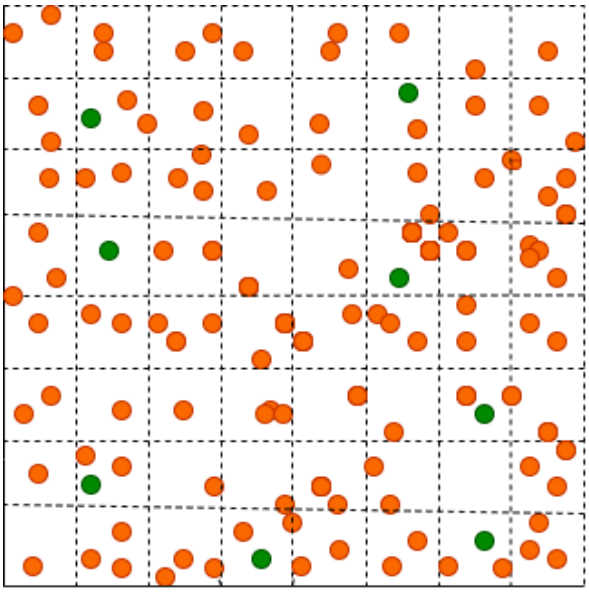

Figure 2: Sample Square Sensing Area of H-WSN

It is presumed that they are dispersed evenly around the playing surface. Furthermore, there are $N.p$ (where $N, q > 1$) randomly placed overlay sensors out there. It has been shown that, on average, only p overlay sensors are functioning at any given moment (the average number of clusters becomes p). Overlay sensors can rotate through the role of cluster leader as detailed below. A particularly unequal topology owing to randomization in installing these overlay sensors can lead to quick energy depletion of a single overlay sensor, which in turn can have a negative influence on the life span of the network, which is why redundancy is used. To "even out" the random impact of deployment, it is possible to deploy more overlay sensors than are strictly necessary and then randomly select a subset to be active at any one time.

The working hypothesis is that sensed data is collected at regular intervals, with each interval being called a "round." During this time, which this work calls a round, one packet of data is detected and sent to the cluster head. This packet, along with the packets from each sensor in the cluster, is sent to the collector during the circuit. When the overlay sensors are turned on, this work presumes that all the other sensors have a continual supply of raw data to transmit. This means that in every iteration, each sensor can have m bits of data to transmit. At the beginning of each cycle, the overlay sensors decide in real time which nodes will serve as cluster heads. If this is the case, it announces its presence to the regular sensors and begins gathering information from the sensors that have joined its cluster. When deciding which cluster to join, normal sensors consider the intensity of the broadcast signal. The fact is that the closer a head is, the stronger its signal, therefore the closest head is the one that gets picked. Overlay sensors that opt out of becoming cluster heads for the current round enter a sleep state during which they do not participate in any activity. Each sensor in the cluster contributes data, which is then sent to the collector. The current round has concluded, and the next one has begun. To guarantee that there are typically clusters in the network, this work mandate that each overlay sensor be active exactly once each round. The following deliberates the proposed energy model statistically. Let ε_t be the transmission energy, ε_r be the reception energy, and ε_s be the sensing energy. The proposed energy model can then be represented as follows:

$$E_{model} = \begin{cases} \varepsilon_t = (\mathrm{E}_l * m * l^{\beta}) + (\mathrm{E}_\tau * m); \\ \varepsilon_r = \mathrm{E}_\gamma * m; \\ \varepsilon_s = \mathrm{E}_\varsigma * m; \end{cases} \quad (1)$$

Equation 1 gives the basic model description which describes how each node spent energy for transmission, reception, and sensing. The energy transmission includes the dissipation of energy per bit E_l chosen as $100\mathrm{X}10^{-12}$ and bitwise transmission energy E_τ chosen as $50\mathrm{X}10^{-9}$. The l is the

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

length from sender to receiver and transmits m bits with a constant $\beta \geq 2$ depending on the signal attenuation in the sensing and transmission environment. This work has experimented with two different aspects of having constant values of $\beta = 4$ and $\beta = 6$. The E_γ and $E_\varsigma$are the energy received and spent per m bits. Apart from this, cluster formation and data processing with high confidentiality demand more energy in the heterogeneous wireless sensor network.

Analyzing how long it can take a sensor in the network to run out of power is considered in this research. With this in mind, this work explains how energy should be distributed between overlay sensors and conventional sensors, and how many clusters should be used. As long as there are at least N rounds in a row, each overlay sensor has been cluster head at least once in the selected H-WSN. This analysis model evaluates the cluster head energy efficiency along with the normal sensors.

$$\mathcal{E}_c = C' + [C'' + (K' * \left|E\left[l^\beta\right]\right|)] * D_{ch-rc}(p) \quad (2)$$

$$\mathcal{E}_n = C''' + [C'''' + (K'' * \left|E\left[X^\beta\right]\right|)] * D_{\overline{ch}}(T/p) \quad (3)$$

Equations 2 and 3 represent the energy consumption of the cluster head $\mathcal{E}_c$ and normal cluster $\mathcal{E}_n$ respectively. The variables $C', C'', C''', C'''', K' \text{ and } K''$ are the constant variables depending on the number of sensors, heads, and bits in each packet, and the amount of energy consumed by the circuitry to process each bit. The random variable X denotes the distance between the normal sensor and the cluster head. A successful transmission from a cluster head ch to a remote collector rc can be predicted by the number of active cluster heads and denoted by $D_{ch-rc}(p)$. As a function of the average size of the cluster, the number of transmissions required to ensure a successful transmission is denoted by $D_{\overline{ch}}(T/p)$. The T is the total number of sensors in the chosen H-WSN.

Table 1: Constants and their Formulas

Sl. No:	Constants	Formula
1	C'	$([2 * m_b * E_l * M^2] + [m_b * E_\tau]) + \left(\left[\frac{T}{p} - 1\right] * E_\gamma * m_s\right) + (m_s * E_\varsigma)$
2	C''	$\frac{T}{p} * m_s * E_\tau$
3	C'''	$(N * m_b * E_\gamma) + (N * m_s * E_\varsigma)$
4	C''''	$N * m_s * E_\tau$
5	K'	$\frac{T}{p} * m_s * E_l$
6	K''	$N * m_s * E_l$

Table 1 gives the computation formulas of various constants used in the energy efficiency analysis model. The m_b represents the number of bits to be transmitted in the broadcast network. The $\frac{T}{p}$ should be lies in the natural numbers set, $\frac{T}{p} \in \mathbb{N}$. In the H-WSN, the heterogeneous sensors are assumed to be distributed in a uniform manner (Gaussian Distribution), both in x and y axis.

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

$$|E[Y]| = \left[{}^{1}/_{3} * ({}^{M}/_{2})^{2}\right]^{2} + {}^{M^2}/_{3} + (L * M) + L^2; |E[l^2]| \quad \text{where } l = x + (y + M)^2 \quad (4)$$

$$|E[Y^2]| = {}^{193}/_{720} * \left(l\right)^4 + {}^{7}/_{6} * (L * M^3) + {}^{25}/_{12} * (L^2 * M^2) + (2 * L^3 * M) + L^4; |E[l^4]|$$

where $l^2 = (x + (y + M)^2)^2$ (5)

Equations 4 and 5 are used to represent the sensor distribution in the H-WSN environment, where $Y = l^2$. For the heterogeneous scenario, the above equations can assist to estimate an appropriate distribution of energy, as well. With diverse types of sensors and a certain cost and task in mind, the energy should be allocated to the overlay sensors and the normal sensors. Sensors with different life expectancies can be compared using this criterion. Sensors that are not deemed retrievable and reusable would fall under this category.

$$\frac{\propto}{\delta} = \frac{C' + [C'' + (K' * |E[l^{\beta}]|)] * D_{ch-rc}(p)}{C''' + [C'''' + (K'' * |E[X^{\beta}]|)] * D_{\overline{ch}}({}^{T}/_{p})}; \qquad \frac{\propto}{C' + [C'' + (K' * |E[l^{\beta}]|)] * D_{ch-rc}(p)} = \frac{\delta}{C''' + [C'''' + (K'' * |E[X^{\beta}]|)] * D_{\overline{ch}}({}^{T}/_{p})}$$

(6)

Equation 6 gives the ratio of energy allocated to the overlay sensors to the normal sensors. The network lifetime in terms of the round can be computed as follows:

$$N_L = N\left(\frac{\propto}{C''' + [C'''' + (K'' * |E[X^{\beta}]|)] * D_{\overline{ch}}({}^{T}/_{p})}\right) \quad (7)$$

Equation 7 computes the last round of the active transmission in the H-WSN and is denoted by N_L. The $\propto$ represents the energy allocated to the overlay sensors, and δ represents the energy allocated to the normal sensors. These equations are challenging to conclude from because they lack a closed-form solution in some circumstances. This work obtained some insight, though, by solving the equations numerically under certain conditions. To keep things simple, it is assumed that flawless scheduling is accomplished at the MAC layer and that $D_{\overline{ch}}({}^{T}/_{p}) = D_{ch-rc}(p) = 1$. In other words, the structure of the study does not change even though the MAC scheme has a different function. In the absence of such a limit, the additional overlay sensors would raise the network's overall energy consumption and therefore its lifespan.

$$P_{Avg} = \frac{1}{T}\sum_{k=1}^{T} P_k(ch) = \sum_{k=1}^{T} P_{opt_k}(ch) * \left(1 - \frac{\overline{\varepsilon_b} - \varepsilon_b}{\overline{\varepsilon_b}}\right) \quad (8)$$

The selection of cluster after clustering has been decided based on equation 8, in which the average probability P_{Avg} of a node to become the cluster head is performed by computing the probability of each sensor node $P_k(ch)$. The residual energy and its mean are used to find the cluster head and denoted by ε_b and $\overline{\varepsilon_b}$ respectively. The secure routing model of the proposed OECS-RA has been discussed as follows:

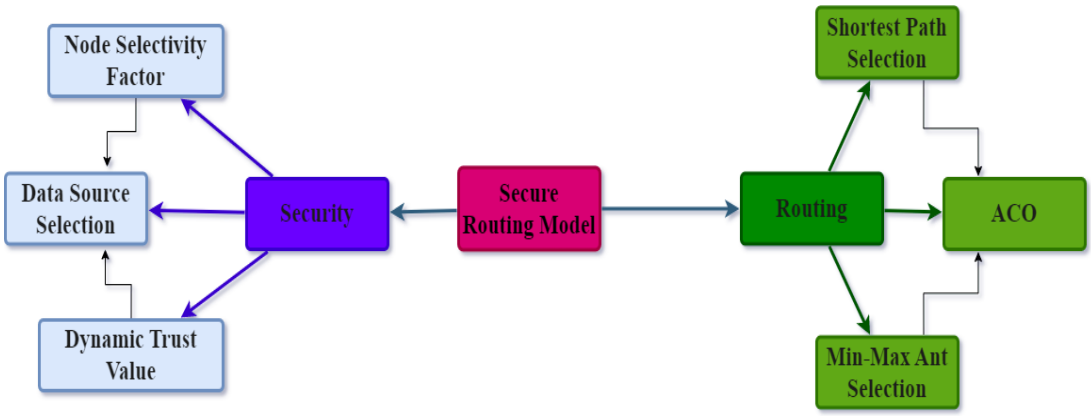

Figure 3: Secure-Hop Selection Scheme of the Proposed OECS-RA

The hybrid evolutionary algorithm combines the security computation model and the ant colony optimization (ACO) algorithm-based routing as seen in figure 3, to ensure secure routing in H-WSN with minimal effort and maximum efficiency. Due to the legal identity of the malicious node, node

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

capture, a common technique for a security attack in H-WSNs, is the most difficult to defend against. The behavior of a malicious node differs significantly from that of typical sensor nodes, even though inside assaults are hard to protect against. As a result, it is possible to distinguish damaged nodes apart from healthy ones based on their behavioral characteristics. By sending their data solely through trustworthy nodes, the non-compromised nodes can subsequently steer clear of these compromised nodes on the routing path. The source node uses the trust factor to identify the neighboring node that is most dependable and to defend against internal assaults. The two aspects of the above-drawn model have been discussed subsequently. The security computation model computes the dynamic trust value and the node selectivity factor to prevent various H-WSN attacks specifically blackhole and flooding attacks by selecting trusted data sources. These parameters are assessed while selecting the secure transmission path for hopping from one node to another node. For real-time event-driven applications, this securing routing mechanism is suggested in this article. In such scenarios, the events happen at random and at irregular frequency throughout the active region denoted by $A[Ev_i]$, implying they might happen anywhere in the monitoring area. The active region of an event in the target field provides the context of the HWSN. The following equation represents the computation formula of $A[Ev_i]$.

$$A[Ev_j] = \{n_k\} \; where \; k = 1,2,3,\dots T \; and \; D\left(n_{Ev_j}, n_k\right) \leq S_r \tag{9}$$

In equation 9, the constraint $D\left(n_{Ev_j}, n_k\right) \leq S_r$ represents the distance between the event-exhibiting node n_{Ev_j} and the other normal nodes in the active region should not exceed the sensing range S_r. The proposed detection model detects the event Ev_j happening around the active region $A[Ev_j]$. This detection model presents the binary output and is denoted by,

$$D_{out} = \begin{cases} 0; \; n_k \nexists A[Ev_j] \\ 1; \; n_k \exists A[Ev_j] \end{cases} \tag{10}$$

The event radius Ev_R decides the size of the active region $A[Ev_j]$ as formulated in equation 10. An event spanning a larger region can cause a greater number of sensor nodes to notice the event Ev_j, hence the larger the value of Ev_R, the more sensors there are in $A[Ev_j]$. All of the sensors that are currently picking up the event Ev_j are included in $A[Ev_j]$, and $A[Ev_j] \subseteq Ve$ is required. Similar data is gathered by the sensor nodes in set $A[Ev_j]$. These sensors pick a leader node named data source from among themselves to prevent the transmission of redundant information and conserve energy. The data source n_l creates and sends the data packets on behalf of all the sensors observing that event. The data source has been selected using the rule as follows,

$$n_l = \underset{i \in A[Ev_j]}{\operatorname{argmin}} (\varepsilon_b * D(n_i, n_l) * Dt_v) \tag{11}$$

$$Dt_v = \omega_1 * \left[\frac{m_g}{m_{max} * N}\right] + \omega_2 * \left[\frac{m_r + m_g - m_b}{m_r + m_g}\right] \tag{12}$$

A more trustworthy node can be chosen as a data source from the result of the dynamic trust value Dt_v computation and evaluation of the node n_i.The suggested method begins with Dt_v = 1, and varies as per the node characteristics in the active region. The value of Dt_v has an inverse relationship with a node's trustworthiness, meaning that the lower the value of Dt_v, the more trustworthy the node is. The residual energy ε_b in equation 11 is considered to ensure the lifetime of the leader node. Along with this process, the proposed security scheme ensures the maximum trusted nodes in the H-WSN. In equation 12, the weights ω_1 and ω_2 represent the relative weights of packet transmission behavior and packet dropping behavior, respectively, N represents how many rounds the node has participated in the network. m_{max} is the maximum number of bits a node can send using the initially available energy, where m_r is the number of bits received by a node, m_g represents the number of bits created by the node itself, m_b is the number of bits transmitted by the node. The three objectives of minimizing total energy cost, minimizing delay, and maximizing Dt_v are combined into a single heuristic known as the node selectivity factor by assigning weights to each of the three objectives to evaluate a sender's neighbors and identify the most appropriate forwarding node. The node selectivity factor denoted by SF_k at a sender node n_k is computed as follows.

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

$$SF_k = \omega_\varepsilon * \min \varepsilon_c^T + \omega_d * \min d^T + \omega_t * \max Dt_v \quad (13)$$

In equation 13, the parameters $\omega_\varepsilon, \omega_d, \omega_t$ are the weights associated with the total energy cost ε_c^T, path node delay d^T, and dynamic trust value Dt_v. These parameters should follow the constraints such as $0 \leq \omega_\varepsilon, \omega_d, \omega_t \leq 1$ and $\omega_\varepsilon + \omega_d + \omega_t = 1$. Routing in WSNs is a well-known NP-hard problem, making it difficult for traditional optimization approaches to get a solid result quickly. Such complex optimization problems are particularly suited for metaheuristic approaches. Metaheuristic approaches have been widely employed to solve problems relating to WSNs and have been demonstrated to perform better than traditional optimization strategies.

The optimal routing part of the secure-hop selection scheme uses an ant colony optimization algorithm that performs a min-max ant system to select the shortest path for every hop. Since ACO is a construction-based method, it is more suited for routing needs. The construction graph seems to be a common weighted graph used to represent the solution space of ACO. Problems with predetermined and precise sources and destinations are better suited for ACO. The main goal of ACO is to find the best path across the building graph. To discover a solution to the issue at hand, ACO imitates the foraging activity of ants.

The shortest route between an ant colony's nest to a source of food can be found by examining how quickly they assemble. The ants leave behind a flammable chemical, known as a pheromone, on their return journey from the food source, and they favor the path with the highest pheromone level. The pheromone level on the shorter pathways rises as a result of the quicker travel times and therefore greater frequency of visits on the shorter paths. As a result, more ants are drawn in, the strength of the pheromone rises, and eventually, most of the ants congregate along the shortest path.

The primary element in an ant colony's collective learning behavior that determines the shortest route from the colony's nest to a food source is thereby the pheromone. Several ants are formed at each source node in the network, and they are tasked with finding a route to the leader node. To update the pheromone values, or routing tables, at intermediate nodes, these ants store information about the quality of the nodes they pass while hopping from the source to sink including energy consumption, residual energy, bits generated, bits received, bits transmitted, and delay. Pheromone value ρ_k and a heuristic function $\emptyset_{jk}$ are indeed used by the ants to choose a neighboring node. The quality of the leader node is represented by the pheromone values. Heuristic function values $\emptyset_k$ represent a node's local information.

$$SF_{jk} = \frac{1}{\emptyset_{jk}};\ \emptyset_{jk} = \frac{1}{\omega_\varepsilon * \min \varepsilon_c^T + \omega_d * \min d^T + \omega_t * \max Dt_v} \quad (14)$$

The node selectivity factor is the inverse of the heuristic value for the routing problem as shown in equation 14. The sensor nodes in the H-WSNs keep track of their surroundings, and when anything happens, the nodes closest to the node provide sensing reports and begin the routing mechanism. There are X nodes formed at every source node. By selecting the following hop for data forwarding, each of these ants creates a routing path in the network. The following describes the mathematical formulation of the rules used in the proposed ACO algorithm with a min-max system.

Rule 1:

$$k = \begin{cases} P_{jk}^n; & r > t \\ \underset{k \epsilon N^b(n_j)}{\operatorname{argmax}} \left[(\rho_{jk})^a * (\emptyset_{jk})^b \right]; & r \leq t \end{cases} \quad (15)$$

$$\text{Where } P_{jk}^n = \begin{cases} \frac{\left[(\rho_{jk})^a * (\emptyset_{jk})^b \right]}{\sum_{k \epsilon N^b(n_j)} \left[(\rho_{jk})^a * (\emptyset_{jk})^b \right]}; & n_k \epsilon N^b(n_j) \\ 0; & Otherwise \end{cases} \quad (16)$$

Rule 2:

$$\rho_{jk}(it^{++}) \leftarrow [1 - \mathrm{C}^e] * \rho_{jk}(it) + \mathrm{C}^e * \Delta\rho_{jk} \quad (17)$$

$$\text{Where } \Delta\rho_{jk} = \begin{cases} \frac{K}{SF_{jk}}; & if\ v(j,k) is\ the\ best\ path \\ 0; & Otherwise \end{cases} \quad (18)$$

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

Rule 3:

$$\rho_{max}(it) = \sum_{j=1}^{it} \frac{C_{it-1}^{e}}{SF_{min}} + C_{it}^{e} * \rho_{min}(it) \quad (19)$$

Where $\rho_{min}(it) = \frac{1}{(1-C^{e})*SF_{min}}$ (20)

Under the above rules, each ant at the node n_j chooses one of its neighbors at the node n_k. The parameters used in these rules are described as follows,

$\rho_{jk} \rightarrow Pheromone\ level\ of\ the\ link\ between\ n_j\ and\ n_k$

$P_{jk}^{n} \rightarrow Probability\ of\ selecting\ neighbor\ node\ n_k\ by\ n_j$

$N^{b}(n_j) \rightarrow Set\ of\ neighbor\ nodes\ of\ n_j$

$a\ and\ b \rightarrow Relative\ significance\ level\ of\ \rho_{jk}\ and\ \emptyset_{jk}, respectively$

$r \rightarrow Generate\ random\ number$

$t \rightarrow Fixed\ Threshold\ value\ determining\ exploitation\ and\ exploration\ by\ ants$

$it \rightarrow Iteration\ index$

$C^{e} \rightarrow Evaporation\ coefficient\ due\ to\ exploration\ by\ ants$

$\Delta\rho_{jk} \rightarrow Pheromone\ level\ variation\ from\ \rho_{min}\ to\ \rho_{max}\ where\ \rho_{min} > 0$

If $\rho_{jk} < \rho_{min}$, then $\rho_{jk} = \rho_{min}$, and if $\rho_{jk} > \rho_{max}$, then $\rho_{jk} = \rho_{max}$.

The algorithm finds a routing path that provides the least value of SF_{jk} for each component of the path given the H-WSN topology and other network factors. It runs through a certain number of iterations. At the source node, a certain number of ants are created per iteration. A path to the leader node is built by each ant in the colony using a probability distribution. The optimal path, or the one with the lowest value of hop distance, is chosen from among all the routing pathways built by the ants, and it is used to update the pheromone levels on the linkages between the nodes. The goal of this is to get the ants to congregate on the most direct route from the source to the sink.

4. Numerical results and discussion

This section covers the simulation analysis and results observed in this research. The simulation for the proposed OECS-RA was performed using MATLAB 2021 installed in the system having the specification of an Intel i5-x86 processor with 8GB RAM, 1TB SSD, and 2GB GPU. This simulation analysis observed energy-efficient clustering and secure transmission with minimal hop. The simulation was carried out in a 250 x 250-meter square environment with sensors distributed at random. The number of sensor nodes in the field varied from 50 to 250, taking into account varying circumstances. Along with the regular nodes, the compromised nodes are evenly dispersed over the sensor field. In this scenario, the sink node was placed near the center of the sensing field, such that, at (125, 125). The experiment takes 1024-bit data packets and 128-bit control packets for evaluating transmission efficiency and security. Assume that the network's overall energy is constrained to a maximum of 30 joules in each scenario. The malicious node count was chosen in five varying ratios of 20%, 30%, 40%, 50%, and 60%. The performance of the proposed OECS-RA was compared with TEMSEP [16], HPEEA [17], E-BEENISH [18], CoMSeC++ [20], and ISFC-BLS [21] in terms of throughput, lifetime, energy efficiency, and reliability. The following results give the analysis outcomes of the proposed research.

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

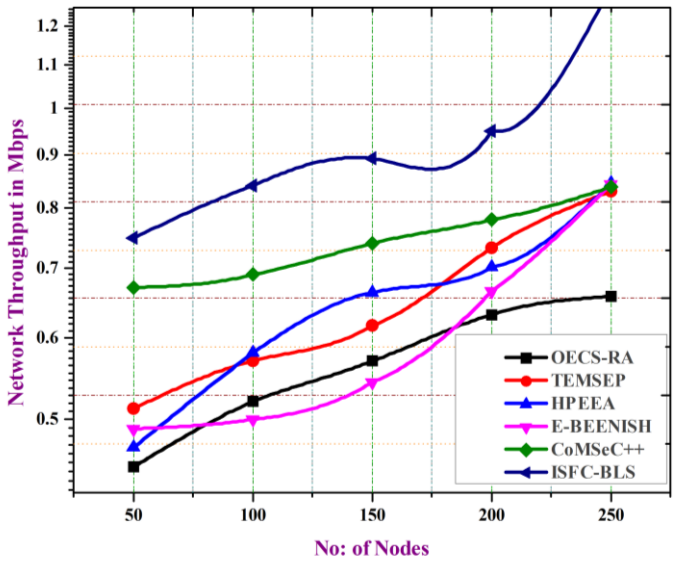

Figure 4: Network Throughput Analysis in Mbps

In figure 4, the network throughput of the simulated H-WSN with the proposed OECS-RA approach shows the lowest network throughput compared to the existing model TEMSEP [16], HPEEA [17], E-BEENISH [18], CoMSeC++ [20], and ISFC-BLS [21]. The simulation was performed with two different aspects of having constant values of β=4 and β=6 and chosen the best result (β=6) was noted in the above figure. It is observed that the signal attenuation in the sensing and transmission environment was dependent on the constant β as noted in equation 1. The varying number of nodes from 50 to 250 showed that the increase in node length also increases the network throughput. Even though, this proposed OECS-RA gives consistent performance by giving an average throughput of 0.5658mbps which is the lowest compared to existing models.

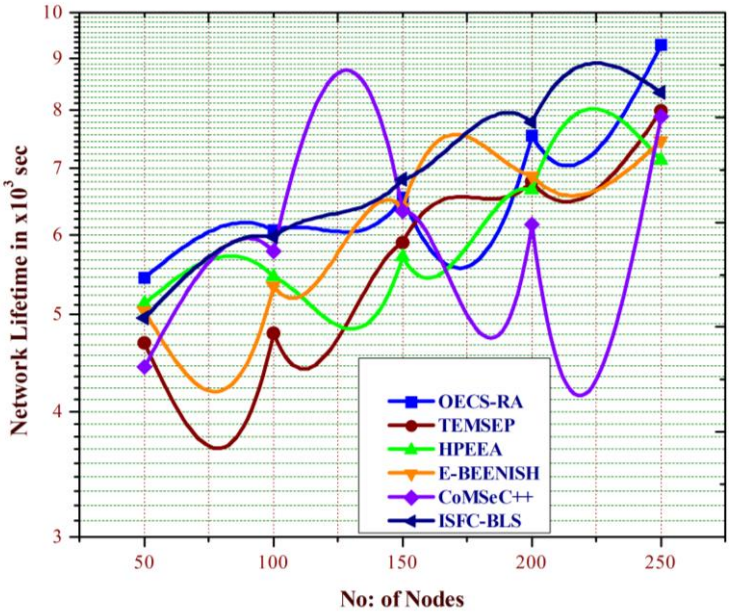

Figure 5: Network Lifetime Analysis in $\times \mathbf{10^3}$ seconds

In figure 6, the network lifetime compared to other existing models discussed above was the highest even if clustering and trust evaluation were performed in each round. The proposed OECS-RA uses the minimum number of transmissions by obtaining an optimized and secured route from source to destination. This characteristic of the proposed model ensures the highest network lifetime which

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

proves the significant energy efficiency. The node selectivity factor and optimized cluster head selection played a crucial role in ensuring improved performance over other models.

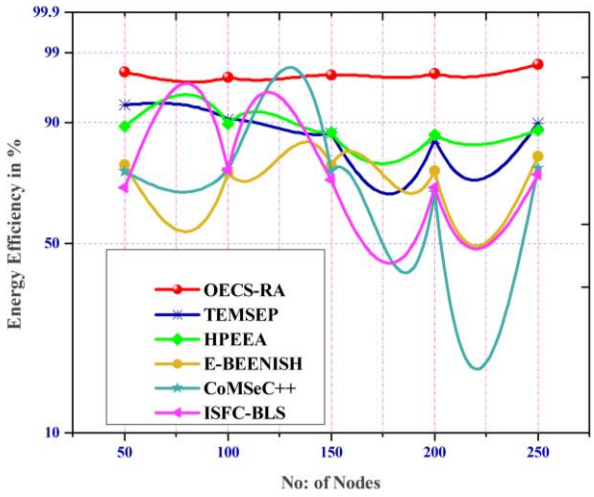

Figure 6: Energy Efficiency Analysis in Percentage

The energy efficiency of the proposed OECS-RA was analyzed in terms of energy consumed by cluster head and overlay sensors. Based on the equations 4, 5 and 6, the energy consumed by the H-WSN implemented using OECS-RA approach had given highest energy efficiency ratio over other existing models discussed in this article. The average energy efficiency of the proposed model was the highest with value 98.61% and given the optimal route selection and security. The node selectivity factor with the three objectives of minimizing total energy cost, minimizing delay, and maximizing dynamic trust value was computed for heurisitic analysis for ACO algorithm [21] – [22] implemented for secure hop selection.

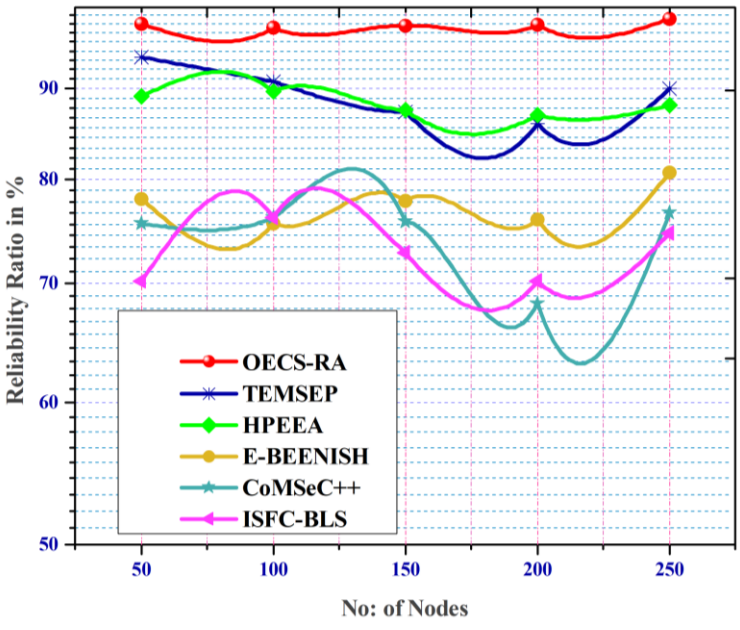

Figure 7: Reliability Analysis in terms of Percentage

The reliability ratio of the proposed model was observed and plotted in the above figure. In figure 7, the comparative analysis of the OECS-RA model over existing models TEMSEP [16], HPEEA [17], E-BEENISH [18], CoMSeC++ [20], and ISFC-BLS [21] was effectively presented. The TEMSEP [16] and HPEEA [17] did not consider security in their implementation, however this work tried to incorporate the secure hop selection model in the simulation. The result observed after this was significant compared to their original performance. The min-max system of the ACO and the single heusitic function values $\emptyset_k$ helped to find the secured node to each hop with the optmal route with

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

minimal cost, energy consumption, and maximum trust. This work concludes that the proposed OECS-RA can be implemented in the real-time H-WSN environment which ensures lowest throughput, highest network lifetime, energy efficiency, and reliability compared to existing models TEMSEP [16], HPEEA [17], E-BEENISH [18], CoMSeC++ [20], and ISFC-BLS [21]. Accurate distance, forwarding direction, ideal cluster size, and numerous pathways for packet transmission were employed to optimize routing. The proposed model choosen a node depending on how much energy it uses for transmission to sink compared to how much energy it has left over. A node closer to the sink could use less energy and have a higher probability of selection than a node closer to the source node since energy usage has been dependent on the distance between communicating nodes. As a result, there are fewer nodes on the routing path, which causes less latency.

5. Conclusion

This study used clustering and a secure-hop selection method to create the Optimal Energy Conservation and Security-aware Routing Algorithm (OECS-RA) for H-WSN. According to the energy conservation of each sensor node, the best cluster head selection and routing in the proposed model have been discovered through a number of computational steps. By choosing the protected node using credential factor computation and comparing each hop of the ideal route, it further secures the transmission. A clock-driven or constant update sensor network was examined with the OECS-RA approach in this article as a heterogeneous wireless sensor network. This model explained the creation of dynamic clusters, provided a method for calculating the ideal number of clusters for a particular set of parameters, and displayed numerical results. Similar problems would be investigated in the future using sensor networks that are query-driven and event-driven. It is indeed important to take into account the likelihood of many collectors spread out across the country.

References

[1] Samadi, R., & Seitz, J. (2022, January). EEC-GA: Energy-Efficient Clustering Approach Using Genetic Algorithm for Heterogeneous Wireless Sensor Networks. In 2022 International Conference on Information Networking (ICOIN) (pp. 280-286). IEEE.

[2] Ou, X., Wu, M., Pu, Y., Tu, B., Zhang, G., & Xu, Z. (2022). Cuckoo search algorithm with fuzzy logic and Gauss–Cauchy for minimizing localization error of WSN. Applied Soft Computing, 125, 109211.

[3] Feng, Q., Chu, S. C., Pan, J. S., Wu, J., & Pan, T. S. (2022). Energy-Efficient Clustering Mechanism of Routing Protocol for Heterogeneous Wireless Sensor Network Based on Bamboo Forest Growth Optimizer. Entropy, 24(7), 980.

[4] Lei, Y., Qu, M., Lei, C., Kong, Z., Tian, J., & Wang, S. (2022). Two FCA-Based Methods for Reducing Energy Consumption of Sensor Nodes in Wireless Sensor Networks. Scientific Programming, 2022.

[5] Li, Z., Verma, S., & Jin, M. (2021). Power allocation in massive MIMO-HWSN based on the water-filling algorithm. Wireless Communications and Mobile Computing, 2021.

[6] Susan Shiny, G., & Muthu Kumar, B. (2022). E2IA-HWSN: Energy Efficient Dual Intelligent Agents based Data Gathering and Emergency Event Delivery in Heterogeneous WSN Enabled IoT. Wireless Personal Communications, 122(1), 379-408.

[7] Lakshmi, M., & Prashanth, C. R. (2022). A Back propagation Neural Network Model for HWSNs Using IMIMO with a Secured Routing Mechanism. IETE Journal of Research, 1-14.

[8] A. Sariga, J. Uthayakumar, Type 2 Fuzzy Logic based Unequal Clustering algorithm for multi-hop wireless sensor networks, Journal of International Journal of Wireless and Ad Hoc Communication, Vol. 1 , No. 1 , (2020) : 33-46 (Doi : https://doi.org/10.54216/IJWAC.010102)

[9] Lakshmi, M., & Prashanth, C. R. (2022). Throughput Improvement in Energy Efficient Heterogeneous Wireless Sensor Network. In ICDSMLA 2020 (pp. 17-34). Springer, Singapore.

[10] Alshawi, I. S., Abbood, Z. A., & Alhijaj, A. A. (2022). Extending lifetime of heterogeneous wireless sensor networks using spider monkey optimization routing protocol. TELKOMNIKA (Telecommunication Computing Electronics and Control), 20(1), 212-220.

[11] Manoharan, G., & Sumathi, A. (2022). Efficient routing and performance amelioration using Hybrid Diffusion Clustering Scheme in heterogeneous wireless sensor network. International Journal of Communication Systems, 35(15), e5281.

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024

[12] Chauhan, R., & Ahluwalia, P. (2022, October). Novel scheme to resolve coverage and connectivity issue in wireless sensor networks. In AIP Conference Proceedings (Vol. 2555, No. 1, p. 050018). AIP Publishing LLC.

[13] Bozkaya, E., Karatas, M., & Eriskin, L. (2022). Heterogeneous wireless sensor networks: Deployment strategies and coverage models. Comprehensive Guide to Heterogeneous Networks, 1.

[14] Irshad, M. A Novel Method formulated on Secure Clustering and Secure Routing (SCSR) to bring forth advanced security for Hierarchical WSN's.

[15] Abdul-Qawy, A. S. H., Nasser, A. B., Guroob, A. H., Saad, A. M. H., Alduais, N. A. M., & Khatri, N. (2021). TEMSEP: Threshold-Oriented and Energy-Harvesting Enabled Multilevel SEP Protocol for Improving Energy-Efficiency of Heterogeneous WSNs. IEEE Access, 9, 154975-155002.

[16] Abbas, N. A. F., Majeed, J. H., Al-Azzawi, W. K., & Ali, A. H. (2021). Investigation of energy-efficient protocols based on stable clustering for enhancing lifetime in heterogeneous WSNs. Bulletin of Electrical Engineering and Informatics, 10(5), 2643-2651.

[17] Zhang, Y., Zhang, X., Ning, S., Gao, J., & Liu, Y. (2019). Energy-efficient multilevel heterogeneous routing protocol for wireless sensor networks. IEEE Access, 7, 55873-55884.

[18] Parande, S., & Mallapur, J. D. (2022). Cost-Effective Modeling for Incorporating Flexibility by Securing Wireless Mobile Sensors Network. Wireless Personal Communications, 123(1), 727-744.

[19] Sathya Preiya V, Kumar VDA. Deep Learning-Based Classification and Feature Extraction for Predicting Pathogenesis of Foot Ulcers in Patients with Diabetes. Diagnostics. 2023; 13(12):1983. https://doi.org/10.3390/diagnostics13121983.

[20] Abedallah Zaid Abualkishik, Ali A. Alwan, Trust Aware Aquila Optimizer based Secure Data Transmission for Information Management in Wireless Sensor Networks, Journal of Journal of Cybersecurity and Information Management, Vol. 9 , No. 1 , (2022) : 40-51 (Doi : https://doi.org/10.54216/JCIM.090104)

[21] Mall, P., Amin, R., Obaidat, M. S., & Hsiao, K. F. (2021). CoMSeC++: PUF-based secured light-weight mutual authentication protocol for Drone-enabled WSN. Computer Networks, 199, 108476.

[22] Bhushan, B., & Sahoo, G. (2020). ISFC-BLS (intelligent and secured fuzzy clustering algorithm using balanced load sub-cluster formation) in WSN environment. Wireless Personal Communications, 111(3), 1667-1694.

[23] P. Sherubha, P Amudhavalli, SP Sasirekha, "Clone attack detection using random forest and multi-objective cuckoo search classification", International Conference on Communication and Signal Processing (ICCSP), pp. 0450-0454, 2019.

[24] Hemamalini, Selvamani, and Visvam Devadoss Ambeth Kumar. 2022. "Outlier Based Skimpy Regularization Fuzzy Clustering Algorithm for Diabetic Retinopathy Image Segmentation" Symmetry 14, no. 12: 2512. https://doi.org/10.3390/sym14122512.

[25]Kumar, V.D.A., Sharmila, S., Kumar, A. et al. A novel solution for finding postpartum haemorrhage using fuzzy neural techniques. Neural Comput & Applic 35, 23683–23696 (2023). https://doi.org/10.1007/s00521-020-05683-z

[26] S. Dinesh, K. Maheswari, B. Arthi, P. Sherubha, A. Vijay, S. Sridhar, T. Rajendran, and Yosef Asrat Waji, "Investigations on Brain Tumor Classification Using Hybrid Machine Learning Algorithms", Hindawi Journal of Healthcare Engineering, Volume 2022.

[27]Anita Soni, A Concentrated Energy Consumption Wireless Sensor Network by Symmetric Encryption and Attribute Based Encryption Technique, Journal of Journal of Cybersecurity and Information Management, Vol. 12 , No. 1 , (2023) : 08-18 (Doi : https://doi.org/10.54216/JCIM.120101)

Doi : https://doi.org/10.54216/JCIM.130211
Received: January 14, 2024 Revised: Mrach 06, 2024 Accepted: May 04, 2024