SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V10I6P109

Volume 10 Issue 6, 104-118, June 2023
© 2023 Seventh Sense Research Group®

Original Article

Investigations on IOT-Based WSN with SWIPT-NOMA Combination

Reginald Jude Sixtus[1], Tamilarasi Muthu[2]

[1, 2]Department of Electronics and Communication Engineering, Puducherry Technological University, Puducherry, India.

[1]Corressponding Author : iamjjude7893@gmail.com

Received: 03 April 2023 Revised: 29 May 2023 Accepted: 16 June 2023 Published: 30 June 2023

Abstract *- Wireless Communication provides the interconnection of different devices for the ubiquitous accessibility of intellectual capacity. Wireless Communication incorporates device interaction to provide sufficient capability in networking between intermediate devices. Conventionally, the Internet of Things (IoT) and Wireless Sensor Networks (WSN) offer sufficient information between intermediate devices. IoT-WSN devices are resource constraints (RC), compact devices, and limited battery resources. The increase in the number of users leads to challenges with security in the IoT-WSN. The data transmission between the wireless communication uses the 5G communication-based NOMA communication. Due to limited RC features, the computational complexity is higher with minimal space consumption; those are evaluated with embedded hardware features within the IoT – WSN. This paper aimed to develop an appropriate optimal routing scheduling and security model based on Long Short-Term Memory (LSTM). The performance of the proposed ORSS is evaluated for security analysis based on consideration of different attacks. With the ORSS model, the position of nodes is computed with the covariance matrix estimation. To identify the optimal route, 's Particle Swarm Optimization (PSO) algorithm is implemented for the route scheduling for the data transmission. SWIPT is implemented for effective energy harvesting to minimize energy consumption within the network. Based on the covariance estimation, optimal routes in the network are computed to detect attacks. The attacks are computed based on the utilization of the LSTM model for the detection and classification of attacks with the use of CICIDS datasets. The comparative analysis stated that the proposed ORSS exhibits ~40% higher data transmission and ~21% reduced delay than state-of-techniques.*

Keywords *- Internet of Things (IoT), Simultaneous Wireless Information and Power Transfer (SWIPT), Particle Swarm Optimization (PSO), Long Short Term Memory (LSTM), Non-Orthogonal Multiple Access (NOMA), Routing, Attacks.*

1. Introduction

The Internet of Things (IoT) comprises sensor nodes that are Wireless Sensor Network (WSN) for the efficiency improvement in network performance. Those sensors are deployed in different environmental fields with a more straightforward configuration and deployment. Sensor Nodes (SNs) with independent network infrastructure comprise the ad-hoc network [1] within this infrastructure topology for the neighbouring data transmission between nodes with consideration of different factors. Those sensed sensor data were forwarded toward the Base Station (BS) with the election of Cluster Heads (CHs) and gateways. The information is aggregated for the received data packets before transmission towards BS to create single or multihop transmission between data in the network [2]. The CHS is focused on collecting and receiving data with a transmission scheme with the forward mechanism. Usually, in a centralized manner, BS is deployed for end-user access for data collection based on web applications [3]. Nodes are deployed in either static or dynamic routing techniques to transmit sensor data. IoT technologies are now merged to increase communication to improve throughput, distribution of load and utilization of resources. WSN technologies comprise of IoT system for the physical environment data forwarding and monitoring [4].

Power capacity for processing depends on the device; hence centralized formation techniques are appropriate for WSN. Here, the device's task is to process, coordinate and manage the activities of sensed information and then transmit these data to the sink node [5-7]. However, with distributed formation, every node manages the information and decisions are made locally, limited to its single-hop neighbours. Recently used distributed techniques are self-organization. The process of forwarding information is complex; hence, robust techniques are required [8]. The network with this strategy achieves good behaviour where nodes communicate and coordinate independently. Naturally, those techniques are involved in insect colonies, bird flocks, biological cells, foraging behaviour and so on [9].

Even though several applications have proved that WSN is successful, sensor networks, a new technology, still have a few setbacks to overcome. Relatively, sensor networks are simple and hence easier to deploy, but for malicious attacks, they are highly vulnerable due to limitations in robust eight security systems [10]. As several SNs are present in WSNs, they act as an access point for the attacker in the network. Besides security risks, naturally, WSNs lead to practical issues during deployment. The low-energy and low-range devices of WSNs have to be cost-effective as they are frequently deployed in the same network [11].

Moreover, few engineers have identified that the periodic change over power on SNs extends the nodes' lifetime but leads to latency and routing overhead [12]. Generally, these issues lead to the challenge of using SNs with good battery life and transmitting abilities. Using less expensive SNs Power and performance are ongoing challenges, but using recent diagnostic tools ensures SNs function efficiently and avoid wastage of power [13].

IoT environment has enormous intelligent devices and several constraints such as processing ability, storage, limited power life, and radio range. About 25 Billion objects are anticipated to be linked; hence the present Internet structure with TCP/IP protocols finds it challenging to deal with a network as extensive as IoT, which requires a novel open structure to address several security and Quality of Service (QoS) issues. IoT is difficult to adopt without any valid privacy concerns [14]. Hence protecting data and users' privacy are the significant challenges in IoT. To develop IoT further, numerous multi-layered security frameworks have been introduced.

The sensor has vital in IoT applications which are essential too. Thus, in-situ fire detection has been spread rapidly and is chosen as a reference point for designing ecological WSN. As the application is low in cost, sensor nodes sustain a lengthy maintenance-free checking time and support a straightforward, reliable dissemination scheme [15]. Both physical weight and size are essential, particularly the transporting way for backpack dissemination. Furthermore, energy sources, batteries and maintenance have to be concentrated. WSNs, when integrated with IoT, provide four essential components: WSN, Gateway Server, Middleware, and Mobile client [16]. As WSN has a prospective future, it will be successful only when security and privacy issues are addressed. These are more significant as used generally in crucial applications. Moreover, WSNs are very vulnerable to attacks as the cost is meagre for deployment.

Recently, most of the applications related to WSN-IoT have been designed in such a way that it processes multivariate data, but still, few models process uni-variate data. While processing multivariate data, characteristics collectively form an exemption where the features are not displayed. Few handle both, but data dimension reduction is not considered [17]. The present models are designed to work online, but the cost of estimating the identifying method has to be considered as it uses more power [18]. Currently, most existing models utilize the distributed structure, which has many disadvantages.

Moreover, the previous distributed models were usually unable to describe the integration of local and global standard models. At last, due to dynamic changes in the data, these templates did not mention the suitable thresholds to update regular standard templates. The adaptability to the dynamic changes in the data of a few recent discovery models gains more calculation costs which impact the aptness of real-time identification and updates [19]. Several developed models overlook some specific WSN data features which are spatially or temporally correlated. These features are helpful during recognition. Influencing these correlations via functional reduction assists in maintaining sensor energy [20]. Few statistics and taxonomy revised model shave issues while selecting parameters. Before testing, a few parameters must be set for testing the model. The performance of different classification approaches like SVM reasonably varies as some client constraints are transformed. In an actual WSN application, the precise constraint values are not simply specified for each application. Moreover, if the dynamic data changes must be considered, using fixed values is inappropriate.

2. Related Works

In [21], different standards examined and evaluated several sensor network architectures. Through the analysis, this research identified several-security impacts on the network and provided an appropriate classification of the threats in WSN. In [22] evaluated, several security challenges in the WSN. Through analysis, the researcher stated that well-balanced infrastructure performs significantly for security challenges in WSN. The network's construction involved developing a business model and protecting confidential information for sensitive data. This research suggested that institutions need to implement an appropriate security policy for securing data in the network.

Overall, this research stated that security is considered an essential concern in case theft has a severe impact. In [23], about challenges associated with security in WSN. This research developed a standardized security model for WSN by identifying security threats. This research evaluated a theoretical evaluation of several security risks in the network. The proposed approach offers an efficient and secure mechanism for secure infrastructure development.

In [24] presented the list of attacks that affect the functionality of the WSN network. Also, this approach evaluates the vulnerabilities of a network with consideration of various network parameters. This research evaluates the functional characteristics of those identified attacks in the network. Similarly, [25] developed an algorithm for WSN through Dynamic origin routing (DSR) with a target of DDOS attack in the network. The proposed approach is implemented using Qualnet 5.2. Results stated that the WSN node is concerned about node energy level for attack prevention and detection.

In [26] proposed a Fruit Fly Optimization Algorithm (FFOA) for capturing attacks with consideration of multiple target nodes in the network with the inclusion of different targets such as the contribution of maximum keys, the contribution of nodes and expenditure of resources for optimal node identification in a network. This impacts the network's overall performance by demolishing a valuable network part cost-effectively and identifying optimal network efficiency. Simulation results illustrated that proposed for node capturing attack proposed genetic algorithm (GA) FFOA offers an excellent solution for compromised network traffic, minimal attack count and reduced network energy. Further, the proposed FFOA offers maximum network efficiency with consideration of the minimal number of nodes in the network.

2.1. Review of the Data Transmission Mechanism in WSN

In [27], it proposed a novel technique for data transmission in WSN, which is based on clustering and timestamp. In this approach, one relies on the group of sensors, and the other relies on the time stamp measurement of one sensor node to another. If a particular timestamp is reached its limits, then the declaration is provided by the malicious node and leads to jamming in the decryption state with appropriate acknowledgement. This causes disturbance to the transmission, and the network will select a different route for data transmission. The performance of the proposed approach is evaluated based on considering different parameters such as the Packet Delivery Ratio (PDR), network bandwidth, energy consumption, and overhead routing. In [28], proposed a mechanism based on an event-based approach involving data transmission based on the response received from neighbouring nodes in a network. Once the condition for the network is identified, the sensor begins to trigger for time period k; based on this target, stated are estimated, and data were transmitted to the neighbour in which the sensor node can receive data from the neighbouring node alone. This research provides significant performance for malicious attack detection in WSN and offers numerical results for the proposed approach.

[29-31] was developed a novel realistic adversary model for WSN for attack prevention and significant network performance maintenance. The proposed two approaches are evaluated considering the distribution, effectiveness, and collaboration of protocols involved in the History Information Exchange Protocol (HIP), which aligns with HOP. HIP and HOP are involved in establishing communication in single-hop with minimal network mobility, which measures differences in computation measurement. This research implemented attacks incorporated against several attacks in the network, considering various mobility models by comparing existing techniques.

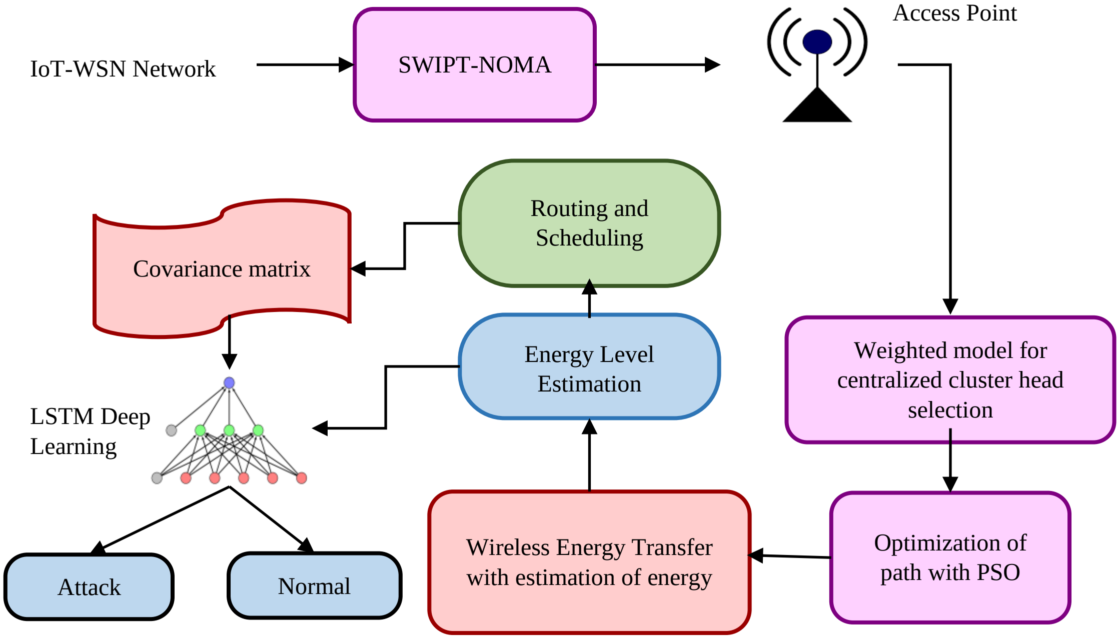

IoT-WSN Network
SWIPT-NOMA
Access Point
Routing and Scheduling
Covariance matrix
Energy Level Estimation
Weighted model for centralized cluster head selection
LSTM Deep Learning
Attack
Normal
Wireless Energy Transfer with estimation of energy
Optimization of path with PSO

Fig. 1 Architecture of ORSS

A comparative analysis of results stated that the proposed approach effectively improves the network detection rate with minimal overhead. In [32] developed, an approach for the prevention of wormhole attacks in WSN. This research proposed an approach-derived routing protocol known as AOMDV (Ad hoc On-Demand Multipath Distance Vector) along with an RTT (Round Trip Time) mechanism with the inclusion of wormhole attack characteristics. Analysis of results exhibited that the proposed approach exhibits significant performance rather than other conventional techniques used in literature. The proposed approach is simulated in the NS2 simulation software for detecting and preventing wormhole attack detection and prevention in WSN. The proposed approach did not require any hardware design. It involved measuring the route and round trip time (RTT) with identifying the network threshold. Simulation analysis of the proposed mechanism for various parameters stated that for different parameters such as Average delay, packet delivery fraction and Average throughput, AOMD exhibits significant performance.

3. Network Model

The proposed ORSS model uses the IoT application for the cluster selection for the CH formation to estimate the effective routing path for the data transmission. In an IoT environment, the data transmission between the nodes uses the cognitive radio network; those are evaluated with the NOMA model for the resource constraints computed with the SWIPT model. The optimal path selection with appropriate scheduling is performed with the optimization-based routing scheme of PSO. The proposed ORSS model computes the optimal path features and transmits data. Figure 1 provides the overall process in the proposed ORSS model.

The proposed ORSS uses the NOMA model for the computation of the data lower and upper band in the network. The symbol N data block is denoted as $[x_n = n = 0,1,\dots.,N-1]$ comprises of the carrier symbol set $[f_n = n = 0,1,\dots.,N-1]$. The estimation of frequencies are computed $f_n = n\Delta f$ with the symbol period T denoted as $\Delta f = \frac{1}{\Delta t}$. Each block data transmission $x(t)$ with 1-bit for the data transmission comprises of SWIPT denoted as in equation (1)

$$g_n(t) = \sqrt{\frac{2S_e}{D_s}} cos\left(2\pi f_c t + (2n-1)\frac{\pi}{4}\right), n = 1,2,3,4 \tag{1}$$

Here, $g_n(t)$ denoted as the data in base time, S_e energy utilized for the data transmission; D_s represented as the data transmission duration, where, f_c symbol data value. The proposed ORSS with the NOMA model unit space function is computed as in equations (2) and (3).

$$\phi_1(t) = \sqrt{\frac{2}{D_s}} cos\, 2\,\pi f_c t, \quad 0 \leq t \leq T \tag{2}$$

$$\phi_2(t) = \sqrt{\frac{2}{D_s}} sin\, 2\,\pi f_c t, \quad 0 \leq t \leq T \tag{3}$$

In the above equation (2) and (3), with data point with symbol is denoted as $\varphi_1(t)$ and $\varphi_2(t)$ the estimated points in the orthogonal scheme of data transfer is stated as in equation (4).

$$\left(\pm\sqrt{\frac{S_e}{2}}, \pm\sqrt{\frac{S_e}{2}}\right) \tag{4}$$

In equation (4), the total system power with the data factors is partitioned between 2 carriers. The carrier phase factors comprise the demodulated input data in the receiver end. The SWIPT scheme symbol sequences are stated as $p_t(t)$ for the receiving antenna sequences with the filtering, components are presented as $p_r(t)$. The composite channel symbol is stated as $H(t)$ for the receiver time domain data is presented in equation (5)

$$h_{iR,iT}(n) = \sum_{i_T=1}^{N_T} h_{iR,iT}(n) \otimes x_{iT} + N \tag{5}$$

In equation (5) uncorrelated temporal region is represented as N with the noise components for the i^{th} antenna in the time domain is stated as x_{iT}. In the receiver end, the SWIPT uses the Inverse Fast Fourier Transform (IFFT). The characteristics of the IFFT are presented in equation (6).

$$u(n) = \frac{1}{N} \sum_{n=1}^{N-1} U(k) e^{\frac{-j\pi kn}{N}}, n = 0,1,\dots..,N-1 \tag{6}$$

In the equation (6) the data transformation is represented as N with the k^{th} point FFT in the frequency state is denoted as k=0,1,…….., N-1. The simplified form is presented in equation (7).

$$U(k) = \sum_{n=1}^{N-1} u(n) e^{\frac{-j2\pi kn}{N}}, k = 0,1,\dots..,N-1 \tag{7}$$

The cognitive network-based data transmission in IoT-WSN comprises the channel characteristics for analysis. The random distribution with Gaussian distribution average mean value 0 and the identical components are represented as in equation (8)

$$n = n_p \times \left(N(0,1)\right) + i \times N(0,1) \tag{8}$$

Where, n_P represents the data points, data transmission length is denoted as (N(0, 1)).

3.1. Centralized Cluster Head Selection with Covariance Estimation

The result of PSO considered for three grids is characterized as U, S and V. The character grid of I outline the network size of m×n; those can be disintegrated into r. The character grid of I the frameworks is like this composed as in condition (9)

$$I = U * S * V^t = \sum_{i=1}^{n} \left(\sigma_i * u_i * v_i^f\right) \tag{9}$$

The singular matrix I for non-zero elements is denoted by the symbol s_i, and the positive diagonal terms are denoted by the term r. 5G data NOMA data can be calculated using linear algebra as non-negative scalar elements. The equation depicts the NOMA data I matrix as in equation (10)

$$\mathrm{I} = \mathrm{USV}^{\mathrm{T}} \tag{10}$$

The diagonal matrix component of element S is represented by the singular value of I in the equation mentioned above, and the element eigenvalues of the NOMA datas are denoted as in the equation above (11)

$$S = \begin{bmatrix} \sigma_1 & 0 & 0 & 0 \\ 0 & \sigma_2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sigma_M \end{bmatrix} \tag{11}$$

Where $\sigma_1 \geq \sigma_2 \geq \sigma_3 \geq \cdots \geq \sigma_{\mathrm{r}} \geq \cdots \geq \sigma_{\mathrm{M}} = 0 \quad 1$ the principal component (PI) matrix of the elements for matrices U and S is obtained. The unique feature components of the matric are evaluated based on false positive value, as shown in equation (12)

$$PC = U \times S \tag{12}$$

Regarding multi-goal investigation and analysis capabilities, wavelet decomposition performs admirably; In addition, it has been utilized in a few NOMA data exhibits, such as the pressure guidelines, that feature advances in desire handling. SWIPT shows incredible execution. Consequently, a widespread watermarking scheme is utilized for efficient performance. Entropy-based SWIPT can divide a picture into four subgroups, as shown in Figure 3. The NOMA data approximation components are represented by the sub-band low-frequency (LL), whereas the high-recurrence sub-groups represent the itemized sections of a picture. There are one low-frequency (LL) and three high-frequency sub-bands, such as LH, HL, and HH. The LL subband is suitable for sophisticated applications because it has a constant frequency. The letters H and L stand for high pass sifting and lowpass, separating on lines and segments, respectively. Equation 13 depicts the procedure in the proposed model:

$$LL(\mathrm{x}, y) = \frac{\mathrm{p(x, y) + p(x, y+1) + p(x+1, y) + p(x+1, y+1)}}{2}$$
$$HH(x, y) = \frac{\mathrm{p(x,y) - p(x,y+1) - p(x+1,y) + p(x+1,y+1)}}{2} \tag{13}$$

Equation (14) depicts the SWIPT's data constellation points.

$$I_{MPTS} = \sum_{i=1}^{c} \sum_{j=1}^{z} \sum_{k=1}^{x} \sum_{l=1}^{y} [\propto \mu_{i,j,k,l}^{m} \left(d_{ijkl}\right)^2 + (1-\alpha) u_{ijkl}^{m} \left(f_{ijkl}\right)^{-1} \left(d_{ijkl}\right)^2] \tag{14}$$

The developed ORSS comprises the two constraints that are represented as follows (15),

$$\sum_{l=1}^{c} \mu_{i,j,k,l}^{m} = 1 \; and \; \sum_{l=1}^{c} u_{i,j,k,l}^{m} = 1 \quad \forall i, j, k, l \tag{15}$$

The global membership function for the NOMA data's global features is denoted by _(i,j,k,l)m, and the local membership function is denoted by $u_{i,j,k,l}^{m}$. By regularizing the variables, the optimal data function is denoted by m>1.0 as (0.0 1.0). The distance between each NOMA data is shown as $d_{i,j,k}$, and the vector distance is estimated as a_(i,j,k,l) for each data vector. The Euclidean distance is estimated as $d_{i,j,k}$, and the neighbour distance is estimated as t_j using likelihood estimation. The NOMA's data sequence is represented by the equations d_(i,j,k,l) and f_(i,j,k,l) (16)

$$\left(d_{i,j,k}\right)^2 = \left\| a_{j\mu} - t_j \right\|^2 \forall i, j, k, l$$

$$\left(\bar{d}_{i\hbar l}\right)^2 = \frac{1}{N} \sum_{x_i \in N_{ik}} \left\| x_{j\mu l} - t_j \right\|^2 \quad \forall i, j, k, l \tag{16}$$

Equation (16) calculates the data vector using N for NOMA data's central frequency. The constraints in estimating the iterative function are considered when calculating the uncertainties in the NOMA data. The iterative function is evaluated by equating the partial derivatives. The data sequence's iterative equations are shown in equations (17) and (18).

$$\mu_{i,j,k,l} = \frac{1}{\sum_{k-1}^{c} \left(\frac{\alpha[\left(d_{ijkl}\right)^2 - ln(\mu_{i,j,k,l}^{m} - 1)]}{\alpha[\left(d_{ijkl}\right)^2 - ln(\mu_{i,j,k,l}^{m} - 1)]}\right)^{\frac{1}{m-1}}} \; \forall i, j, k, l \tag{17}$$

$$u_{i,j,k,l} = \frac{1}{\sum_{k-1}^{c} \left(\frac{(1-\alpha)[(f_{ijkl})\left(d_{ijkl}\right)^2 - ln(u_{i,j,k,l}^{m} - 1)]}{(1-\alpha)[(f_{ijkl})\left(d_{ijkl}\right)^2 - ln(u_{i,j,k,l}^{m} - 1)]}\right)^{\frac{1}{m-1}}} \; \forall i, j, k, \tag{18}$$

The estimated weighted features of the data are denoted as g_{ijkl} stated as in equation (19):

$$g_{i,j,k,l} = \frac{(\mu_{i,j,k,l}^{m})^{p}(u_{ijkl}^{m})^{q}}{\sum_{i-1}^{c}(\mu_{i,j,k,l}^{m})^{p}(u_{ijkl}^{m})^{q}} \tag{19}$$

The NOMA data weighted function's parameters, which have an impact on the NOMA values, are denoted by (1 ≤ p, q ≤ 3) in the preceding equation (19). Based on NOMA data contours and texture components, the SWIPT representation of NOMA data's coefficient variation is evaluated. The proposed ORSS used the SWIPT model system to reduce PAPR in NOMA data processing in this paper. Creating constellation points in the NOMA data is a component of the developed ORSS system. The information contained in the generated sequences is embedded in the NOMA data.

The set of generated keys that must be implemented within the NOMA data is the foundation for incorporating the desired symbol. The procedure includes information generation, processing, and embedding. This information is NOMA data that has been processed using the sequences generated and is embedded within the NOMA data. The data processing is based on the sequence of NOMA data and the generated key. After the ORSS process depicted in Figure 2, the internal architecture concentrated on the SWIPT and GA processes.

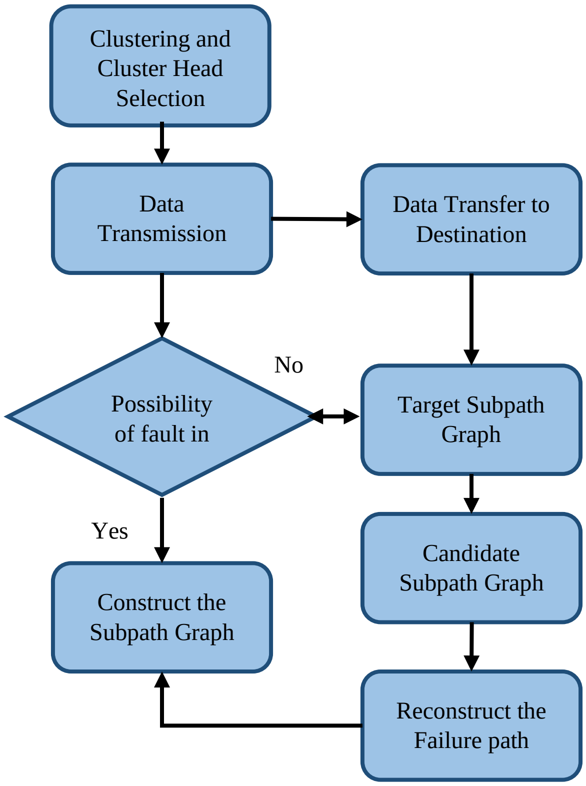

Clustering and Cluster Head Selection
Data Transmission
Data Transfer to Destination
Possibility of fault in
No
Target Subpath Graph
Yes
Candidate Subpath Graph
Construct the Subpath Graph
Reconstruct the Failure path

Fig. 2 Route estimation with SWIPT-GA

The Genetic Optimization (GA) PSO algorithm performs clustering in the proposed model ORSS, reducing the energy consumption's chaotic nature. The subsequent neighbour nodes for inter-cluster routing are then selected using a multi-service queue-based ant optimization algorithm technique. Additionally, this approach maintains network lifetime and energy efficiency in dense networks. Figure 3 depicts the architecture of the proposed model with optimization.

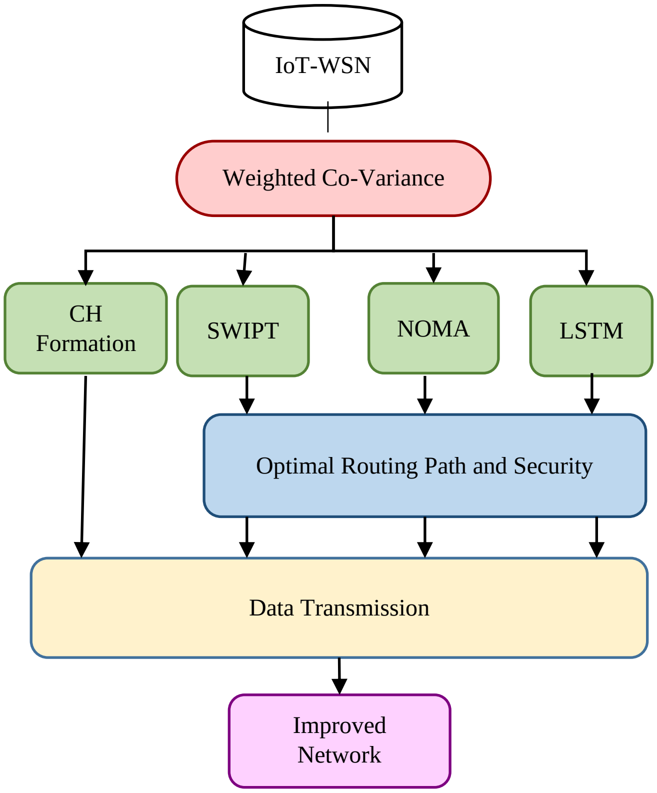


Fig. 3 Optimization process with SWIPT

3.2. Energy Model

A sensor node is chosen as CH in the current rotation round using the weighted covariance PSO method only if the random number chosen by SN is less than the threshold specified in equation (20).

$$T(i) = \begin{cases} \frac{PCH}{1-PCH\times\left(Roundmod\frac{1}{p}\right)} & if\ i \in Z \\ \qquad\qquad i & \\ 0 & otherwise \end{cases} \tag{20}$$

In WSNs, PCH denotes the preferred CH percentage, Round denotes the current Round's number, and Z denotes the set of nodes that were not CH 1/CH rounds previously. The equation describes the radio energy dissipation model used in WSN for transmitting a message with an "m" bit over a "d" distance in equation (21)

$$ET_{x}(m,d) = \begin{cases} m * E_{elec} + m * \varphi_{fs} * d^{2}, \Delta\, d < T_{i} \\ m * E_{elec} + m * \varphi_{fs} * d^{4}, \Delta\, d \geq T_{i} \end{cases} \tag{21}$$

Where Eelec supports electrical energy, the ratio of and is always written into account the amplifier's energy to maintain an appropriate data-to-noise ratio. The model of free space channel (d2 power loss)) If the gap is less than the threshold value Ti; However, the multipath fading channel model is utilized when it is more significant than Ti. In the receiver, it performs the same actions. Equation depicts the consumed radio energy (22)

$$E_{Rx}(m) = m * E_{elec} \tag{22}$$

The amount of energy required for measuring and storing is lower when compared to the contact time. For simplicity's sake, only the energy used in contact is taken into account and calculated as follows in equation (23)

$$E_{Dx} = s * k * E_{merge} \tag{23}$$

Eelec of equations (22) and (23) refers to the energy expended during transmission or receipt of 1-bit message.

A specified transmitter and receiver that make use of the sensor pair's model for connected probable resolution in the probability domain of probable routes. Equal probability in the distribution has been used to operate an equal chance for each parent throughout the process of offspring generation. It is a widespread stage and provides the ability to conduct the best research possible in the explanation domain. Single convergence point capability has been connected that the hub conveyed for qualities association, while average hub bunch for each parent make the likely locus for convergence point. The same random progression has been linked to the specific selection when the centre has more than one possible set. The length changes in the introduced offspring may also be caused by the investigated solution for these intersections in the probability domain.

The method of dynamic mutation preserves the variation in use for each centre of offspring with the slightest possible change in possibility. The group member consists of every possible connection with sensor nodes preceding existing nodes by likely mutational members. Once more, these tasks have been held by the likelihood of the concentrated arrangement. When the number of offspring produced was the same as that of the parents' population, the population was combined to form the selection pool while the tournament selection process continued. Each member and their opponent were randomly chosen for the selection process based on the declared match score and robustness comparison. A new population of members with higher scores has been created.

An illustration of the chromosome is a restriction based on the population's immediate resolution and the nodes' definition of the connection between the node's transmitter and receiver. The following stages are used to configure each member, with the initial population shown in equation (24) – (26).

$$U_pD = A.Best\ w(t) - d(t) \tag{24}$$

$$D(t+1) = d(best)\ (t) - A\ U_pD \tag{25}$$

$$F_i = \min\ (MSE) \tag{26}$$

When selecting the threshold for nodes with initial energy, nodes with residual energy, the network's total energy, and nodes with average energy, the proposed ORSS protocol considers four energy characteristics. The energy circulation of every hub has been adjusted, and this proposed procedure upgrades energy proficiency. Additionally, energy consumption will be reduced, and the node closest to the base station will not be a factor in CH selection for cluster formation. As a result, the network's longevity and reliability are enhanced. In addition, the energy consumption of single-hop and multihop data transmission methods has been compared to this proposed method. Finally, an energy-efficient method of communication has been found.

3.3. LSTM Model for the Secure Data Transmission

Because its output will directly reflect the importance and position of each factor in the final results, the weighting system is essential for combining and making decisions based on multidimensional information. Assume that there are n sensors in the network during the fusion process and that i is the node's weight. As a result, the equation shows the weight of all nodes as in equation (27),

$$\beta_1 + \beta_2 + \cdots \ldots + B_n = 1 \tag{27}$$

The weighted nodes are determined by their constructive behaviour to overcome the dependence on neighbour nodes. The cluster head uses a decision table to identify the evidence that makes the most of the construction result during each round decision. It should be noted that the sequence number for the deviation factor is indicated as (mi)

The proposed algorithm prevents malicious nodes from revealing and manipulating network data. An asymmetric encryption method ensures data security between the BS (Bi) and the cloud server. In this method, the BS and the cloud server generate a pair of keys (kp and ku), which correspond to the public and private keys, respectively, with privacy protection only available to the BS and cloud server. A publicly accessible directory on a cloud server is used to share the created public keys, which are used to encrypt data. The generated system ID is also linked to the public keys kept on a cloud server. In contrast, the private keys are kept secret and are not made public. What is more, the PC on which it was planned is not left.

4. Performance Evaluation

With a distance of 100 meters, the proposed ORSS estimated the various nodes. The five sources and one drain comprise the static workload implemented for the nodes. The sensors are working, and they give the packet reliable energy. In accordance, the nodes parameter was created to disperse resources. MATLAB is used for simulation in this work. MHRM (Minimum Hop Routing Model) and DEBR (Distributed Energy Balanced Routing) tolerant clustering algorithms were used to analyze the results of some all-encompassing experiments conducted with the proposed methods. Event packet delivery rate and transmission delay were utilized as output metrics for the supervisory applications. In point of fact, wasted energy may have a more significant impact on these delays. As a result, the ORSS was proposed and evaluated using the output metrics listed below.

Packet delivery ratio is the average ratio of the total packets accepted successfully to the total packets sent initially, as in equation (28).

$$PDR = \frac{\sum p(rx)}{\sum p(tx)} \tag{28}$$

Where p(rx) is the number of packets received, and p(tx) is the number of packets transmitted.

Average delay is the ratio of the average latency to the time sink received by the packet. Consequently, the mathematical term in equation (29) with consumer K's M(K) is calculated in different periods.

$$M(K) = \frac{\sum_{t=0}^{T} M(K).(t)}{T} \tag{29}$$

Where T is the interval of time where the delay of the instant packets is averaged.

Dissipated energy is the sum of energy dissipated to total nodes in the network. Latency is the time between triggering and beginning data transmission. Low latency will provide higher network quality networks and vice-versa. Throughput is the data flow rate through a channel used for communication, i.e. bits or packets delivered successfully over a channel in the network. In WSN-IoT applications, throughput is necessary and estimated using equation (30).

$$Throughput\ (bits/sec) = \sum \frac{suc(pkt)\times avg(pkt)}{t} \tag{30}$$

Where = the number of successful packets avg(pkt)= average packet size and t= = total time spent delivering the data. Network lifetime is defined as the simulation time of the network while performing the dedicated task(s). The highest interval of time throughout which employed sensors can observe the phenomenon of interest is presented in equation (31)

$$Lifetime\ of\ Network\ (LTN) = \frac{TIE}{EPS} \tag{31}$$

Where TIE is Total Initial Energy. EPS is Energy per Second.

Energy consumption in a sensor node depends on the average rate of the power consumption of the node during the time of operation is presented in equation (32)

$$Energy\ Consumption\ (EC) = \frac{\sum p(tx)\times(SE+PE)}{1+p(rx)\times(R+PE)} \tag{32}$$

Where, p(tx) is the packet sent, p(rx) is the packet received, and SE is Sending energy. PE is Processing Energy, RE is Residual Energy. In Table 1, the simulation parameters for the proposed ORSS model are presented.

Table 1. Simulation setting

Parameter	Value
Simulation time	1500s
Network Size	500 m × 500 m
Number of nodes	500
Data packet size	400 bytes
ET_x	30 nJ /BIT
E_{elec}	46 nJ /bit
E_{RX}	27nJ

Table 2. Comparison of PDR

Number of Nodes	Data packet delivery ratio (%)			
	MHRM	DEBR	GBEOM	ORSS
10	40	48	66	92
20	46	53	69	93
30	51	55	73	94
40	53	59	78	82
50	54	61	77	84
60	58	62	83	88
70	59	67	81	91
80	61	69	82	94
90	63	75	87	96
100	66	76	89	96

Table 2 provides the simulation analysis of the proposed ORSS compared with the state-of-art technique such as MHRM, DEBR and GBEOM.

The data packet delivery ratio is analyzed by combining the existing methods with the proposed ORSS technique. The proposed ORSS method employs secure data transmission and optimal route discovery for transmitting data packets with a higher delivery ratio. The route path is created, and the secure distribution of the data packet is based on the distribution of control messages. As a result, the ORSS method that has been proposed outperforms the MHRM, the DEBR, and the GBEOM by 40%. Based on the preceding result, the ORSS method had a higher data packet delivery ratio than other methods. Steering above is expressed as the time taken for the information parcel course from the source to the objective hub with the insignificant loss of the information. Table 3 compares the routing overhead for the proposed ORSS with the conventional state-of-art methods.

Table 3. Comparison of routing overhead

No. of Nodes	Routing Overhead (ms)			
	MHRM	DEBR	GBEOM	ORSS
10	21	19	23	11
20	33	24	34	22
30	41	49	38	31
40	49	51	46	36
50	54	56	51	41
60	62	64	54	46
70	67	69	62	52
80	73	71	67	56
90	77	79	72	57
100	83	83	74	60

The experimental result of routing overhead using the proposed and existing method is tabulated in Table 3 . The table compares proposed and existing methods according to various data packets transmitted between two sensor nodes of various sizes. The proposed ORSS technique provides better data transmission between nodes with minimum routing overhead compared to other existing methods, such as MHRM, the DEBR and GBEOM. With route request and reply, message distribution is an ORSS technique, efficient route discovery is presented for transmitting the data packets. From the produced route path, the shortest route path is selected between the source node and the destination node. This helps to attain minimum time for data packet transmission. As a result, routing overhead is reduced in ORSS technique reduced by 21% when compared with other methods. From the result analysis, the ORSS technique provides an enhanced result of routing overhead. The packet loss in the network is comparatively presented in Table 4. Table 4 demonstrates the experimental data packet loss ratio values concerning a different data packet in the network. Table 4 compares the proposed ORSS technique with existing MHRM, DEBR and GBEOM. From the tabulated values, the ORSS technique provides a better result of a reduced packet loss rate when compared with the existing methods. Based on secured data transmission with minimum routing overhead, occurrences of data packet loss get minimized.

Table 4. Comparison of Data Packet Loss

No.of Nodes	Data packet loss rate (%)			
	MHRM	DEBR	GBEOM	ORSS
10	63	48	43	11
20	53	39	37	13
30	46	42	38	13
40	44	39	36	19
50	45	41	38	13
60	41	33	31	11
70	39	30	27	9
80	37	27	23	13
90	33	25	22	11
100	31	26	21	7

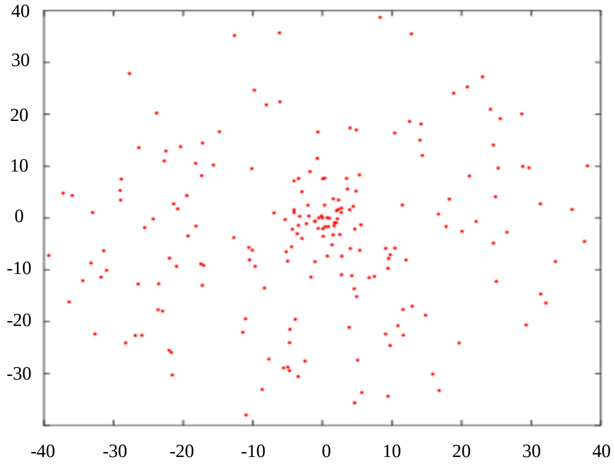
Table 5. Comparison of energy consumption

No. of Nodes	Energy Consumption (EC) (J)			
	MHRM	DEBR	GBEOM	ORSS
10	33	41	53	21
20	66	49	61	38
30	84	53	68	54
40	94	67	76	54
50	112	88	89	74
60	128	105	97	89
70	131	112	106	94
80	139	126	113	98
90	143	138	127	103
100	167	141	138	112

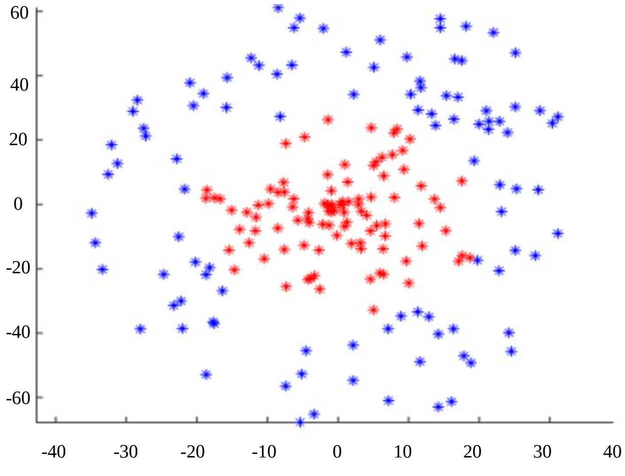
Data encryption and decryption are carried out to perform better data transmission. Similarly, the ORSS technique was reduced by 61% compared to other existing methods. Therefore, the proposed ORSS technique resulted in a reduction compared with MHRM, DEBR and GBEOM. Table 5 provides the energy consumption for the proposed ORSS compared with MHRM, DEBR and GBEOM.

The proposed ORSS evaluate the security analysis based on consideration of the CICIDS dataset. The PSO-based optimization model computes the optimal features in the dataset and applies them over the LSTM network. The LSTM network classifies the attack and improves security. The attributes for the security analysis of ORSS are presented in Table 6.

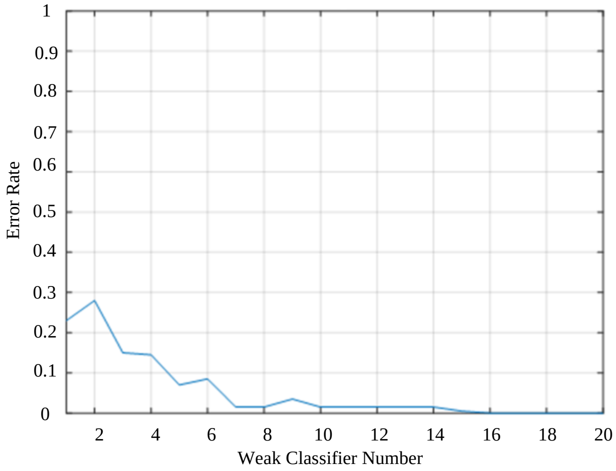
The dataset utilized for the training and testing, in Table 6, comprises four attacks: DoS, U2R, R2L and Probe attack. Figure 4(a)-4(d) provides the distribution of training datasets provides the distribution of training and testing datasets with the proposed ORSS.



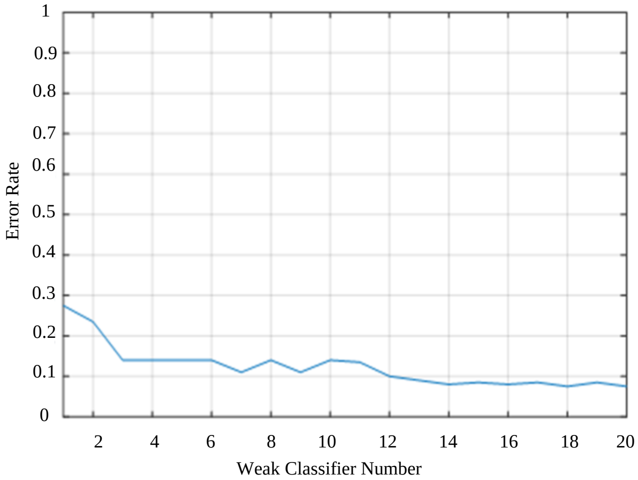
(a)



(b)



(c)



(d)

Fig. 4 (a) Training data (b) distribution of dataset (c) training error (d) testing error

In the Figure above, the red dots indicate the training and the blue dot indicates the training data. Figures 4(c) and 4(d) provide the LSTM network's training and testing errors. The above figure provides the training with a testing error estimated value of 0.29.

Figure 5 shows that the proposed ORSS approach effectively improves the number of nodes involved in the operation. Up to 1000 iterations, the operational performance of nodes is higher, but later it begins to degrade. This implies that the comparative performance analysis of the proposed approach is significantly higher in terms of accuracy, which leads to increased operational performance. Figure 6 shows the number of active nodes using the proposed approach. From the graphical representation, it is observed that 1200 transmissions are stable. In Figure 7, the energy consumption of sensor nodes is provided as in the simulation setup for the assigned energy level amount of energy consumed by the sensor are provided.

Table 6. Classification of training and testing data

Data Classes	Normal Node	Anomaly Detection Node	Identification of DoS	Evaluation of Probe	U2R	R2L
Training set	65,675	51,234	42,244	10,562	46	856
Testing set	8,347	11,572	6,632	2,256	61	1,657

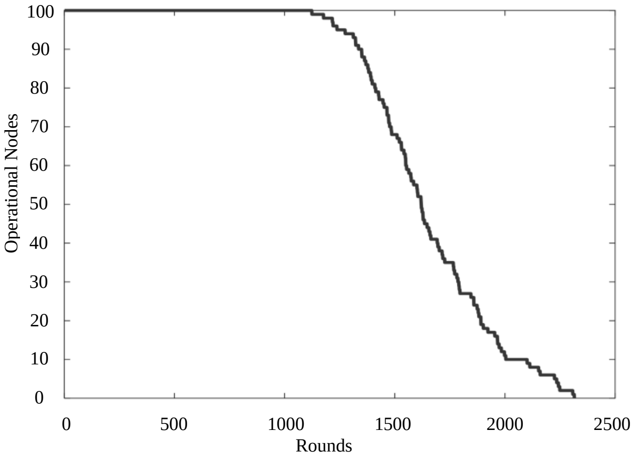


Fig. 5 Operational performance of WSN

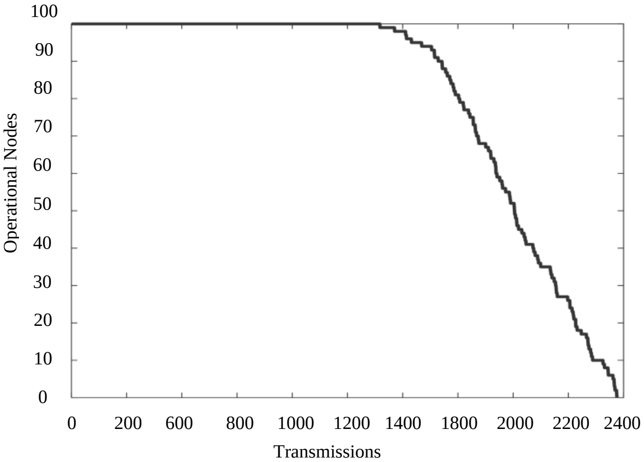


Fig. 6 Number of active nodes (data (counts))

The figure illustrates that the minimal energy consumption of nodes is 0.1 Joules, and the maximum energy consumption is observed as 0.24 Joules. This implies that the energy utilization of sensor nodes varies from 0.1J to 0.24Joule alone, which is ten times the variation. This illustrates that the energy consumption of nodes is minimal, which means less possibility of an attack in the network.

Figure 8 demonstrates that the energy consumption of nodes varies between 0.1 to 0.24Joules. In Figure 8, average energy utilization is presented this shows that average energy utilization is 0, so it is concluded that the energy consumption rate of the proposed ORSS approach is minimal.

The attack detection and classification performance of the proposed ORSS model is evaluated with the state-of-art CNN and LSTM model. Table 7 and Figure 9 provide a comparative analysis of the classifier performance.

According to the comparative analysis of classifier performance, the proposed classifier has a lower false negative value and a higher actual positive rate. For a similar CICIDS dataset, the proposed ORSS gives a TN worth of 40573, FN of 625, FP of 638, and TP worth of 20691. TN is 43624 and 41372 for conventional CNN and LSTM classifiers, respectively. For CNN and LSTM, the FN values are calculated as 1356 and 1689, respectively.

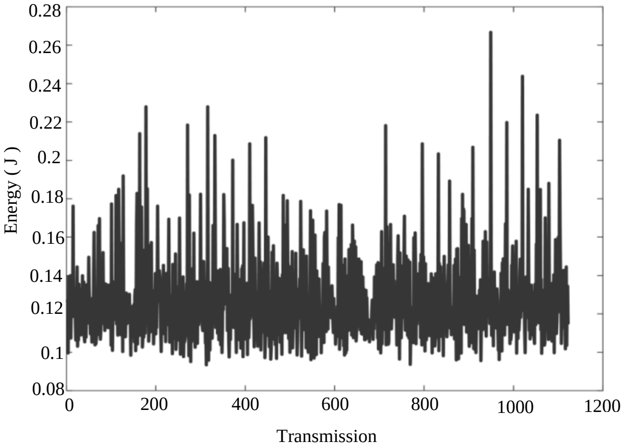


Fig. 7 Energy consumption

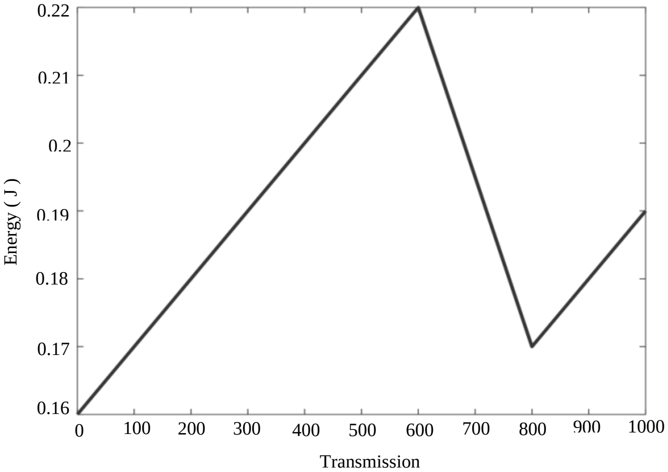


Fig. 8 Average energy consumption

Table 7. Performance of classifier

Parameters	CNN	LSTM	ORSS
TN	43624	41372	40573
FN	1356	1689	625
FP	947	195	638
TP	23671	22689	20691

Table 8. Comparative analysis of classifier

Parameters (%)	CNN	LSTM	ORSS
Accuracy	89	92	99
Precision	90	91	98
Recall	93	92	99
F1 – Score	91	93	98

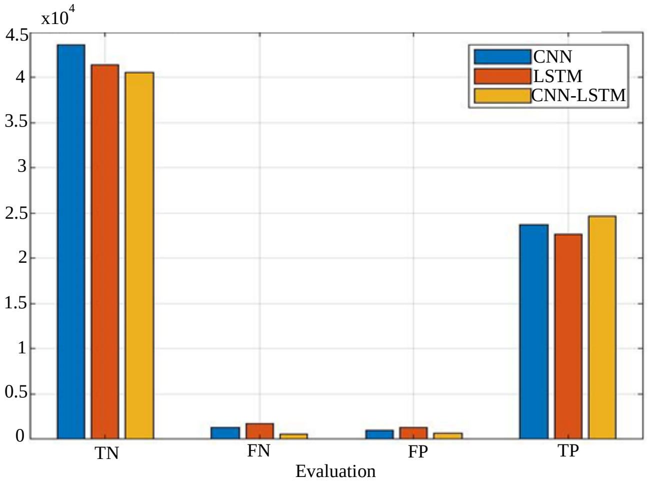


Fig. 9 Comparison of classification performance

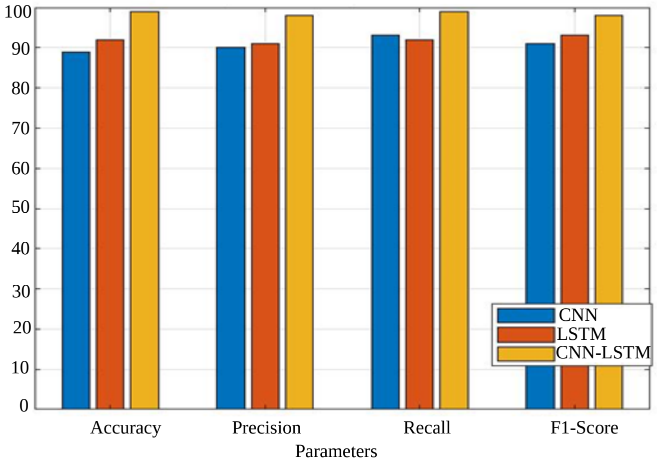


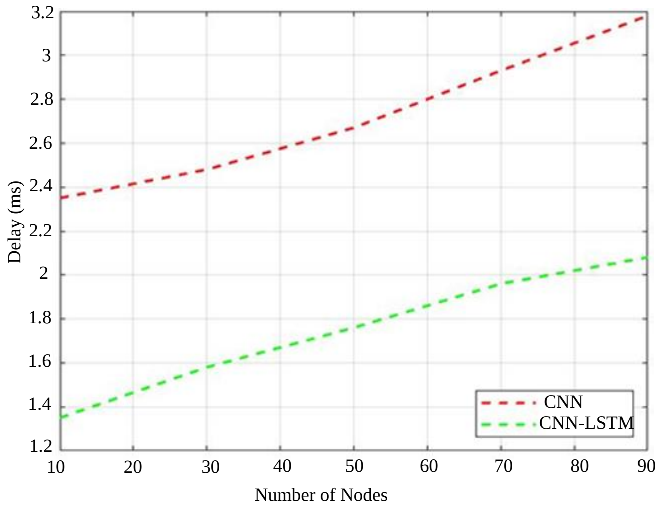
Fig. 10 Comparative analysis of classifiers

It is computed through estimation because the proposed hybrid deep learning model (CNN-LSTM) performance is significantly superior to that of other classifiers. The performance of the proposed ORSS when compared to conventional classifiers like the LSTM classifier and CNN is shown in Table 8 and Figure 10.

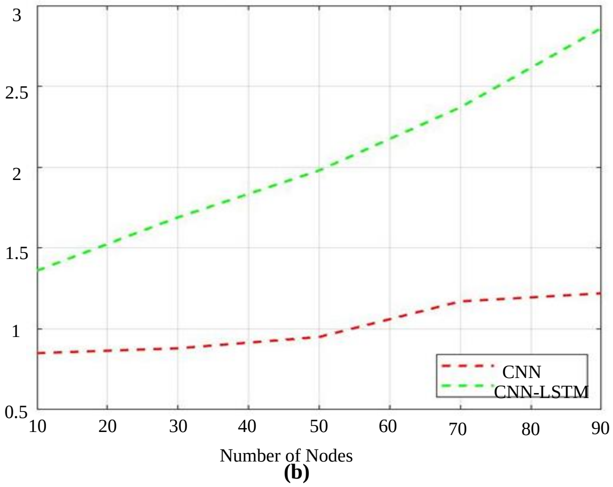
Table 9. Comparison of performance

Delay		
No.of Nodes	**With attack**	**HDL(CNN-LSTM)**
10	2.35	1.35
20	2.48	1.58
30	2.67	1.76
40	2.93	1.96
50	3.18	2.08
Jitter		
No.of Nodes	**With attack**	**ORSS**
10	0.88	1.36
20	0.85	1.69
30	0.95	1.98
40	1.17	2.37
50	1.22	2.86
PDR		
No.of Nodes	**With attack**	**ORSS**
10	62	99
20	71	99
30	74	98
40	81	98
50	86	98
Throughput		
No.of Nodes	**With attack**	**ORSS**
10	62	99
20	69	99
30	73	98
40	77	99
50	83	98

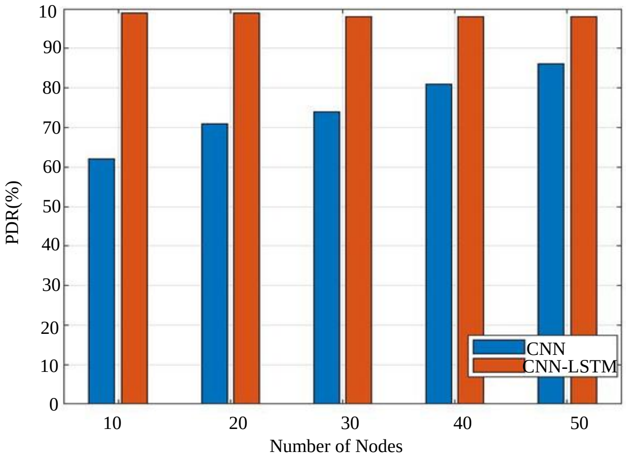
According to the attack classification performance, the proposed ORSS scheme has an accuracy of 99 percent, while CNN and LSTM each have an accuracy of 89 percent and 92 percent, respectively. This suggests that the proposed ORSS scheme performs well when identifying attacks. Similarly, the proposed deep hybrid learning (CNN-LSTM) model outperforms CNN, ANN, and LSTM classifiers regarding recall at a higher percentage. The proposed ORSS has a recall of 97%, about 3% higher than the standard CNN and LSTM classifier. In terms of accuracy and recall, the performance of the proposed CNN-LSTM model is superior. The proposed CNN-LSTM performs worse than the LSTM classifier regarding precision.



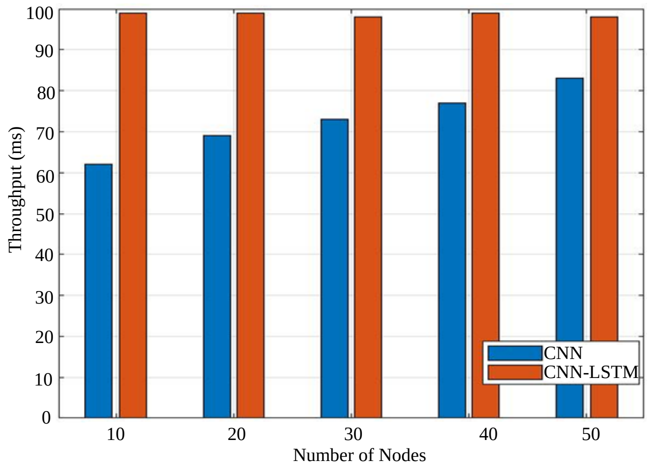
(a)



(b)



(c)



(d)

Fig. 11 Attack analysis with attack and proposed HDL (CNN-LSTM) (a) Delay (b) Jitter (c) PDR (d) Throughout

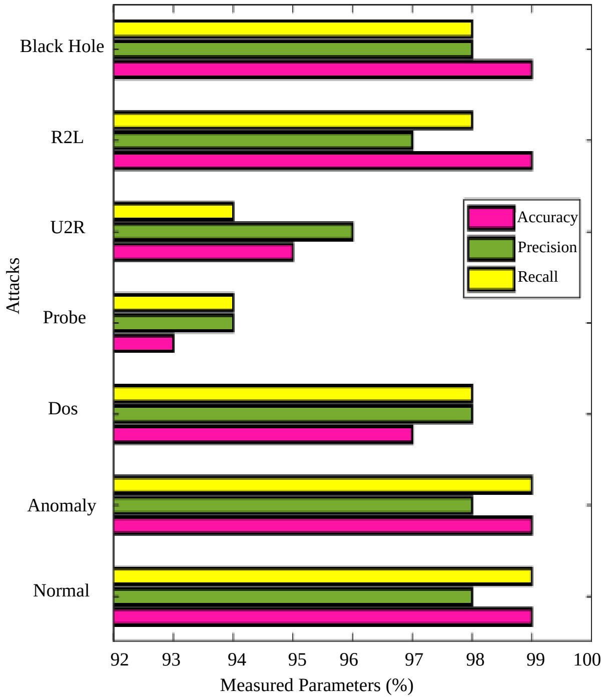


Fig. 12 Comparative analysis of different attacks

An increase in the number of hidden layers may cause decreased precision. The attack's detection is estimated by estimating the classifier's proposed ORSS. With the proposed HDL, parameters can be calculated for changing the environment, usually with or without an attack. For a speed of 10 meters per second, the estimation is calculated. The scenario's performance for both an attack and the proposed ORSS is shown in Table 9 and Figure 11(a)-11(d). The evaluation of the variables computed for the proposed CNN-LSTM considered both an attack and no attack scenario. According to the performance analysis, rather than incorporating an attack, the proposed HDL scheme improves network performance.

Table 10. ORSS performance for the different attacks

	Accuracy	Precision	Recall
Normal activity	99	98	99
Anomaly	99	98	99
DoS	97	98	98
Probe Attack	93	94	94
U2R (User to Root) Attack	95	96	94
R2L (Root to Local)	99	97	98
Black Hole Attack	99	98	98

The proposed CNN-LSTM attack detection rate is calculated for varying mobility and nodes. Table 10 and Figure 12 display the proposed ORSS's attack classification performance.

The performance of the proposed ORSS scheme classifier for various attacks is computed for analysis. According to the analysis, the proposed ORSS scheme has a higher anomaly accuracy value of 99%. The classification accuracy in the event of a black hole attack is estimated to be 99%. Similarly, it is estimated to be 99% and 99% for precision DoS and Blackhole attacks, respectively. The recall value is estimated to be higher at 98 percent for anomaly detection.

5. Conclusion

Using an automated intelligence model, this paper proposed an ORSS model for effective data transmission in the IoT-WSN application. The proposed ORSS perform the data routing using covariance matrix-based estimation over the NOMA-based SWIPT model. The position of nodes is estimated with the covariance matrix, and data were optimized using the PSO model. Data transmission is performed in the network by implementing the SWIPT-based optimal routing. The security analysis is performed based on the consideration of the CICIDS dataset. The experimental analysis expressed that ORSS improved performance for higher data transmission with reduced data loss, delay and energy consumption.

References

[1] Nayef Abdulwahab Mohammed Alduais, Jiwa Abdullah, and Ansar Jamil, “RDCM: An Efficient Real-Time Data Collection Model for IoT/WSN Edge with Multivariate Sensors,” *IEEE Access*, vol. 7, pp. 89063-89082, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] Adeniyi Onasanya, Sari Lakkis, and Maher Elshakankiri, “Implementing IoT/WSN Based Smart Saskatchewan Healthcare System,” *Wireless Networks*, vol. 25, no. 7, pp. 3999-4020, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] Tea Osmëni, and Maaruf Ali, “LoRa IoT WSN for E-Agriculture,” *International Conference for Emerging Technologies in Computing*, pp. 85-93, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] A. Onasanya, and M. Elshakankiri, “Secured Cancer Care and Cloud Services in IoT/WSN Based Medical Systems,” *International Conference on Smart Grid and Internet of Things*, pp. 23-35, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] Nitesh M Sureja, and Sanjay P Patel, “An Improved Particle Swarm Optimization Algorithm for A Variant of TSP,” *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 5, pp. 16-20, 2020. [CrossRef] [Publisher Link]

[6] Haytham Baniabdelghany, Roman Obermaisser, and Ala’ Khalifeh, “Reliable Task Allocation for Time-Triggered IoT-WSN using Discrete Particle Swarm Optimization,” *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 11974-11992, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Neeraj Kumar Jarouliya, and Nirupama Tiwari, “Utilization of Particle Swarm Optimization (PSO) Use as Clustering Algorithm in MANET,” *SSRG International Journal of Computer Science and Engineering*, vol. 6, no. 11, pp. 10-14, 2019. [CrossRef] [Publisher Link]

[8] Bahaa Hussein Taher et al., “A Secure and Lightweight Three-Factor Remote User Authentication Protocol for Future IoT Applications,” *Journal of Sensors*, vol. 2021, pp. 1-18, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] JoonYoung Lee et al., “PUFTAP-IoT: PUF-Based Three-Factor Authentication Protocol in IoT Environment Focused on Sensing Devices,” *Sensors*, vol. 22, no. 18, pp. 1-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Vinodkumar Mohanakurup et al., “5G Cognitive Radio Networks using Reliable Hybrid Deep Learning Based on Spectrum Sensing,” *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ziyad Almudayni, Ben Soh, and Alice Li, “A Comprehensive Study on the Energy Efficiency of IoT from Four Angles: Clustering and Routing in WSNs, Smart Grid, Fog Computing and MQTT & CoAP Application Protocols,” *International Conference on Internet of Things as a Service*, pp. 54-70, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Roba Alsaigh, Rashid Mehmood, and Iyad Katib, “AI Explainability and Governance in Smart Energy Systems: A Review,” *Frontiers in Energy Research*, vol. 11, pp. 1-12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Irin Loretta G, and V. Kavitha, “Privacy Preserving using Multi-Hop Dynamic Clustering Routing Protocol and Elliptic Curve Cryptosystem for WSN in IoT Environment,” *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 821-836, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Norouzi Shad M, Maadani M, and Nesari Moghadam M, "GAPSO-SVM: An IDSS-Based Energy-Aware Clustering Routing Algorithm for IoT Perception Layer," *Wireless Personal Communications*, vol. 126, no. 3, pp. 2249-2268, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Nevine Makram Labib et al., "Design of An Enhanced Threshold Sensitive Distributed Energy Efficient Clustering Routing Protocol for WSN-Based IoT," *International Journal of Electronics*, vol. 110, no. 8, pp. 1373-1392, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Rushdi A. Hamamreh, Moath M. Haji, and Ahmad A. Qutob, "An Energy-Efficient Clustering Routing Protocol for WSN Based on MRHC," *Communities & Collections*, 2018. [Google Scholar] [Publisher Link]

[17] Yan Xu, Zhanwei Yue, and Lingling Lv, "Clustering Routing Algorithm and Simulation of Internet of Things Perception Layer Based on Energy Balance," *IEEE Access*, vol. 7, pp. 145667-145676, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] Deyu Lin, and Quan Wang, "A Game Theory Based Energy Efficient Clustering Routing Protocol for WSNs," *Wireless Networks*, vol. 23, no. 4, pp. 1101-1111, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[19] Leila Abbad et al., "A Weighted Markov-Clustering Routing Protocol for Optimizing Energy Use in Wireless Sensor Networks," *Egyptian Informatics Journal*, vol. 23, no. 3, pp. 483-497, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Jiguo Yu Shaoqing Wang et al., "CRPD: A Novel Clustering Routing Protocol for Dynamic Wireless Sensor Networks," *Personal and Ubiquitous Computing*, vol. 22, no. 3, pp. 545-559, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[21] Quan Wang et al., "An Energy-Efficient Compressive Sensing-Based Clustering Routing Protocol for WSNs," *IEEE Sensors Journal*, vol. 19, no. 10, pp. 3950-3960, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[22] De-gan Zhang et al., "Novel Unequal Clustering Routing Protocol Considering Energy Balancing Based on Network Partition and Distance for Mobile Education," *Journal of Network and Computer Applications*, vol. 88, pp. 1-9, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[23] Shun Yang et al., "Optimization of Heterogeneous Clustering Routing Protocol for Internet of Things in Wireless Sensor Networks," *Journal of Sensors*, vol. 2022, pp. 1-9, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Trupti Mayee Behera et al., "I-SEP: An Improved Routing Protocol for Heterogeneous WSN for Iot-Based Environmental Monitoring," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 710-717, 2019. [Google Scholar] [Publisher Link]

[25] Qi Huamei et al., "An Energy-Efficient Non-Uniform Clustering Routing Protocol Based on Improved Shuffled Frog Leaping Algorithm for Wireless Sensor Networks," *IET Communications*, vol. 15, no. 3, pp. 374-383, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] Zijing Wang, Xiaoqi Qin, and Baoling Liu, "An Energy-Efficient Clustering Routing Algorithm for WSN-assisted IoT," *2018 IEEE Wireless Communications and Networking Conference*, pp. 1-6, 2018. [Google Scholar] [Publisher Link]

[27] Rakesh Kumar Lenka et al., "Cluster-Based Routing Protocol with Static Hub (CRPSH) for WSN-Assisted IoT Networks," *Sustainability*, vol. 14, no. 12, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[28] Rajasekar V et al., "Enhanced WSN Routing Protocol for Internet of Things to Process Multimedia Big Data," *Wireless Personal Communications*, vol. 126, no. 3, pp. 2081-2100, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[29] Kanchan K. Masade, and D. M. Bhalerao, "Fifth Generation of Mobile Wireless Communication: 5G," *International Journal of P2P Network Trends and Technology*, vol. 7, no. 3, pp. 1-5, 2017. [CrossRef] [Publisher Link]

[30] Anita Kulkarni, and K. Sridevi, "Improved Resource Scheduler using Kalman Filter in Wireless Communication," *International Journal of Engineering Trends and Technology*, vol. 71, no. 2, pp. 129-136, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[31] Subramani N et al., "Controlling Energy Aware Clustering and Multihop Routing Protocol for IoT Assisted Wireless Sensor Networks," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[32] Gobi Natesan et al., "A Hybrid Mayfly-Aquila Optimization Algorithm Based Energy-Efficient Clustering Routing Protocol for Wireless Sensor Networks," *Sensors*, vol. 22, no. 17, pp. 1-25, 2022. [CrossRef] [Google Scholar] [Publisher Link]