International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/217700 Volume 9, Issue 6, November – December (2022)

RESEARCH ARTICLE

Minimalistic Error via Clibat Algorithm for Attack-Defence Model on Wireless Sensor Networks (WSN)

K Abdul Basith
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
khateebabdulbasith2020@gmail.com

T.N. Shankar
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
tnshankar2004@kluniversity.in

Received: 07 July 2022 / Revised: 20 September 2022 / Accepted: 26 October 2022 / Published: 30 December 2022

Abstract – Wireless Sensor Networks have become the recent trend to effectively solve the problem in medical fields, primarily in agriculture and others in IoT monitoring. The expenses for ease of use in current domains are particular for cost and energy-effective solutions estimating different for different attack types on Wireless Sensor Network designs. Even though the energy, Routing problems are effectively solved, due to its wireless operative effects, the performance, such as speed and attackers, are reduced due to unevaded attacks. Hence, reducing this problem with energy-featured node optimization, network rate, and unevaded or random attack types like wormholes and black holes would implicate a significant problem in real-time modelling. On this basis, we postulate a solution analysis with the CLIBAT algorithm that implicates different possibilities and its probabilistic approaches, considering a proposed hybrid routing protocol on novel attack and defence algorithms to reduce the attack pattern with Wormhole and black hole attacks. In this perspective, an attack and defence pattern with an intuitive approach is implemented via the Improved Conditionally Expected Criteria feature to emphasize the type of attack (Wormhole or black hole attacks). Also, the Defense algorithm on improved sigmoid function on node characteristics is utilized to implicate with minimum distance formulations on the defense model effectively, MATLAB simulations with the solutions on WSN with CLIBAT algorithm inclusive of attack and defences are effectively removed.

Index Terms – Attacks, DDoS, Firefly, Leach, Conditional Logistic Intuitive BAT Algorithm (CLIBAT), Wireless Sensor Networks (WSN), Distributed Energy-Efficient Clustering (DEEC), Least Probability Gradient algorithm (LPA), Intuitive Cumulative Expected Conditionality (ICEC), Multi-Point Route (MPR).

1. INTRODUCTION

WSNs are made up of a vast number of sensor nodes that are capable of detecting, communicating, calculating, and moving. These sensor nodes are dispersed around a difficult-to-reach region or in an unmonitored setting. For example, environmental monitoring, weather forecasting, traffic management, and natural catastrophe avoidance (such as earthquakes, hurricanes, and tsunamis) may all benefit from multi-hop data transmission from sensors. However, WSNs are vulnerable to various malicious attacks, including route fabrication and packet eavesdropping. Additionally, the whole network's structure might be ruined by such assaults. One of the malicious attacks on WSN is the wormhole attack. The wormhole attacks by establishing a tunnel between one or more malicious nodes, as depicted in Fig. 1. Since the behaviour of malevolent and detecting nodes is the same in terms of mobility and communication, nodes within the transmission range of a wormhole will get information about their neighbours from another wormhole through the tunnel, whether it is wireless or physically based. As a result, nodes that a wormhole assault has hit will choose the incorrect route, which might lead to high battery use and an unstable topology.

Routing schemes play an essential aspect with the cooperating nodes linked by tunnels providing the communication transfer with route requests and topological messages via any network. To avoid attacks on the network via nodes, estimating the node distances ensures the quickest and best possible approach for routing and identifying the new tunnels. Since the attackers utilize a tunnel to access the data or control messages subjecting them to pick the MPRs as random or in sequence depending upon the attack types at each layer. With the wrong information on the structure of topologies, the network is implicated in providing different attack perspectives as black or wormhole tunnels. Thus, it avoids the establishment of linkages between the source and the destination. Even a wormhole attacker may fall prey to its success because of this phenomenon. Using the term "in-band

RESEARCH ARTICLE

wormhole assault," a specific wormhole attack is described. In order to identify network infiltration, a game theoretic technique was used. It is believed that a central authority will monitor the network. "Out-of-of-band" wormhole attacks need a hardware channel to link two collaborating nodes and are called "in-band" wormhole attacks that use a covert overlay on an existing wireless medium. According to [1], there are two types of wormhole assaults in-band: one that targets just the colluding nodes and the other that uses wormholes that extend outside the colluding nodes. Some of the conspiring nodes assault some of their nearby nodes and entice all the traffic their neighbour receives to transit through them. It is possible to differentiate between two types of wormhole assaults: a) hidden attacks, where malicious nodes are concealed from view on the network, and b) exposed attacks, where malicious nodes are visible but cannot be identified on the network.

1.1. Contributions

This paper's main objective is to implicate the type of attack via the CLI model and control feature with the CLIBAT algorithm improving overall features such as energy minimization, bitrate and minimum error optimization using the IBAT algorithm. This paper contributes two featured algorithms on attack and defence model control via hybrid distance and routing protocols to improve the performance features in any network chosen

1.2. Problem Statement

- Implement a CLI solution for attack patterns for different types of Attacks using a conditional logistic intuitive model via the Improved Conditionally Expected Criteria feature.
- Implement a Defence pattern model with the CLIBAT algorithm.
- Implement a Hybrid Route with effective minimal distance via Chi-square distance and entropy means.
- Estimate the error probability with CLIBAT and other algorithms such as LEACH, GA, and DEEC algorithm.
- Finally, a CLIBAT feature with DEEC protocol is implemented to solve the energy minimization and low cluster head feature effectively.

1.3. Overview

This paper in section -1 provides an introduction to types of attack and defence algorithms implemented with wormholes and black holes. In section -2 multiple features of attack and defence patterns are utilized with wormhole attacks and DDOS attacks. Section -3 a detailed analysis of hybrid routing and defence control models using node replaying and traffic tampering scenarios. In section 4, our proposed design with CLI and CLIBAT algorithm has been utilized to implicate the different features of types of attack and defence for wormholes and black hole attacks. Also, performance features on different algorithms are implemented to reduce energy and improve bitrate. In section 5 the results are discussed and section 6 concludes the paper.

2. RELATED WORK

Data Intrusion has been prominent in WSN with the development of improved structures on WSN. So many researchers have dedicated their work to intrusion detection, improved routing and other topological models with practical features that have initiated network, neighbors and sensor capabilities with different algorithms. So as to provide such implementations on the network, researchers have depicted unprecedented changes in every possible feature of WSN problems.

Intrusion is one such problem still researching and affects the different aspects of the WSN network where novel algorithms fail to attain performance. In order to suffice such solutional features, a novelty with which intrusion detection becomes more accessible and less complex to design is to be established. In [2], the design model with intrusion attack has been introduced with a wormhole feature indicating the different attack scenarios, detection and defense accuracy. The comparison of the in 2022, [3] depicted different survey models and their functional aspects on the nodes' misbehaviour while the intrusion is detected. This design perspective reduces the effects on the node's performance. A cooperative timer logic is implicated in influencing the entire network. However, the throughput of the designed system was not improved. The throughput improvements with different hybrid routing systems indicated on the intrusion and detection have been depicted by analyzing the architecture in [4]. Though the route and other packets are terminated due to packet loss, a collaborative-based contact feature was established with self-centered nodes to the different literature surveys have been affected by the type of algorithms chosen, as mentioned in table 1 analytical models indicated in the network structural aspect with the Sybil attack and its intrusion detection model in [5].

In 2020, [6] devised a solution for IDS with different machine learning algorithms introducing the different structural aspects of the model, indicating the design with different attack models and its effective detection accuracies maintained at 96% via RFR and voting classifiers. Similarly, the importance of energy problems with the battery or even low power dissipations with node inducing different changes with machine learning algorithms and optimization algorithms [7]. The sinkhole attacks the design of EABC-ACO is optimized with different learning models initiating the low energy feature on the design in [8].

RESEARCH ARTICLE

Table 1 Summary of the Literature Survey

Scheme and Year	Technique Used	Detection Rate	Attack Accuracy	Defense Accuracy
2022				
Raniyah Wazirali et.al[1]	Navie bayes, MLP other machine learning algorithms	98.12	98.42	95.54
Karen Avila et.al [2]	mitigation attack feature with optimization algorithms with Genetic and other populated algorithms	98.75	98.17	96.75
Kale Navnath Dattatraya et.al [3]	Energy efficient Algorithms with novel routing scheme via intuitive detection protocols.	96.48	95.42	98.08
2021				
c.ceken et.al [16]	black hole attack prevention scheme using block chain-block approach S DN-enables WSN	98.02	97.67	98.2
s.suchitra et.al [17]	Energy efficient witness-based done and jamming attack detection WSN	97.84	95.13	97.752
y.wu,B.kang et.al[19]	Strategies of attack-Defense game for wireless sensors network considering and effect of confidence level in fuzzy environment	97.59	96.81	95.19
a.jagadeesan et al.[14]	Detection of blackhole and wormhole attacks in WSN enabled by optimal feature selection using self-adaptive multi-verse optimiser with deep learning	95.68	97.56	98.32
s.Nosratian et al[29]	Fuzzy-based reliability prediction model for secure routing protocol using GA and TLBO for implementation of black hole attacks in WSN	98.5	98.64	96.72
m.a.rezvi et al[30]	Data mining approach to analysing intrusion detection of wireless sensor network	98.63	97.41	95.19

Similarly, in [9-11], Sybil attack intrusion models with MPI (multiple pseudonym Intrusion) algorithms have been dedicated to improvising a solution to avoid fewer errors while optimizing the nodes. The attack detection metrics with time, reliability and average sequence number is improvised to indicate the structure of protocol utilized for the OSLR model as in [12-14]. In [15], the design feature indicates the specific functionality of the algorithm with an intrusion feature with a learning-based model indicating the different aspects of learned usage of the nodes and their positions and power capabilities. All such features are collected to establish a novel learning model indicating the different aspects of design.

Node capturing and analyzing the different power capabilities in [16] have been challenging. A fruit fly optimization (FFOA) model is indicated to capture the different aspects of the resource utilizing the network with effective cost [17] and maximum efficiency. A solution with FFOA is introduced with complete rounds of traffic flow, lower attacking rounds, and lower cost energy compared with existing algorithms such as Genetic algorithms. DDOS must improvise bogus access and requests due to a lack of servers or connectivity issues. The overflow of different attack flooding would cause the detection and prevention of resources more frequently. In order to eliminate such attack floods the design, novel features of the learning model with improved accuracy feature have been dedicated in this work [18].

We are enabling the different information feature-based selection via the self-adaptive multi-verse optimization (SA-MVO) model utilized with a unique solution to establish

RESEARCH ARTICLE

detection and intrusion via deep learning architectures based on Deep belief network (DBN) in [19-20].

When discovering neighbors, [21] relies on an algorithm randomly selecting a set of neighbors. However, in a single-hop network, the performance was not explained. neighbors will need to be informed in advance of this project. A novel method for locating neighbors was put out in [22]. Using a multiuser detection strategy is the key to this system's success. However, this approach can only be used if all nodes in the network are in sync and each node has the signatures of the other nodes.

While in [23], the watchdog architecture for event detection was introduced as a modality-neutral approach. The framework combines sensors to satisfy the particular detection accuracy required by the user at runtime. As a result, energy consumption is significantly reduced. This approach was developed by Kim et al. [24] to ensure the safety of wireless networks. The "algebraic watchdog" is the name given to this strategy. Probabilistic detection of harmful conduct is possible with this method. It takes advantage of the overheard conversations to keep an eye on its neighbors downriver. A self-validating global network is provided by the algebraic watchdog [25].

The challenge for Wireless Sensor Networks (WSN) [27] is with merging features relating to the Internet of Things (IoT) with a secure network. Secure WSN is indicated with the implication of layer-wise protocols establishing the WSN. This work enables a newer opportunity to enhance the defense mechanism with better accuracy and remove the different problems associated with securities [28-30].

On this perspective of the implicating of selection of neighbors, their exact location with different networks implemented via neural modality approaches, multidimensionality scaling, mismatch graphs, SECTOR and RTT are utilized to deal with such situations but still requires much research on the performance features of Network energy utilization and bit rate with minimal errors. So, with these features in consideration, we have to implement an intuitive approach to analyze the problems of the above network features with the CLIBAT algorithm. This design with minimum distance formulations via IBAT algorithm and CLI feature is improvised on the different aspects of the node characterization via cluster node creation and its functional features.

3. HYBRID ROUTING PROTOCOL

3.1. Hybrid Routing Protocol for Energy Minimization

The descriptive data analysis applied to the system parameters was included in this architecture to enhance it. Figure 1 includes an insight into creating significant change in energy optimization with nodes, routing, and cluster head feature emerging to improvise network parametric parameters. The author presents a ubiquitous stochastic model to ensure the optimality of both the node and the route in every possible instance of observed energy values. An augmented distance technique with SCI inequality is implemented for better energy reduction. The routing would create a distance feature model for every set of chosen nodes based on the OLS algorithm.

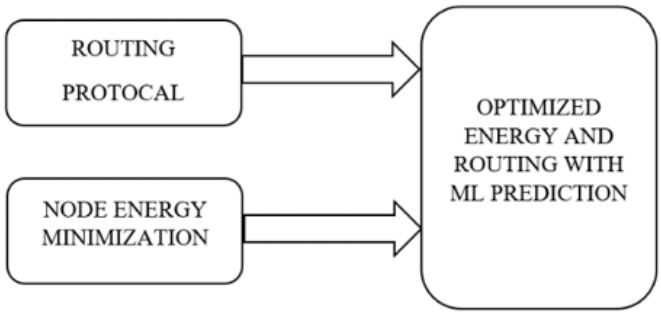


Figure 1 Representing Optimization of Routing and Energy Minimization Block Diagram

3.2. Topology Models for Energy Minimum

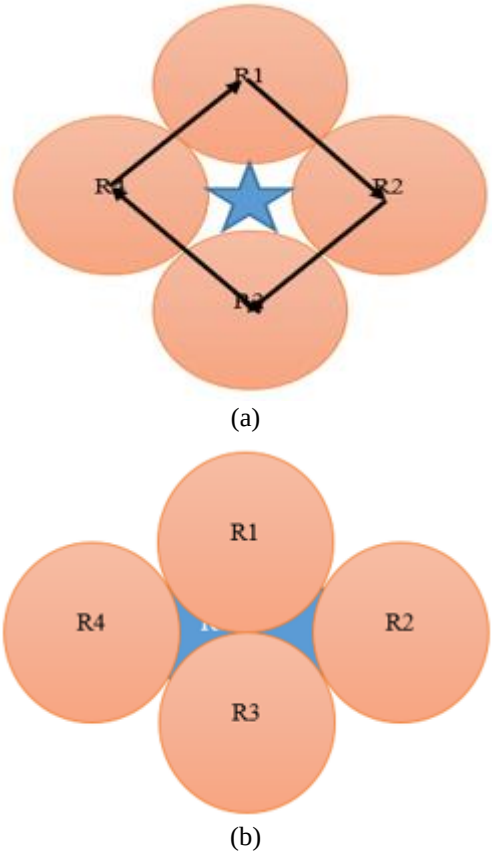


Figure 2 a) Representing the Pervasive Tangential Transform Model b) Region Tangential with Projection Transform

RESEARCH ARTICLE

In figure 2 (a), we improvise a design that estimates R1, R2, R3, and R4's distances from the centre as d1, d2, d3, and d4. Section 3 gives each region's optimal distances (1-4). Figure 2 (b) star-filled zone displays the best regional transform for each tangential l point.

Let p I (i:1 to 4) be the tangential points for the star area studied, where arcs R1-R2 and R1-R4 entail point P1. Connect star edges E j circles with p I i=1:4, j=1-10. The tangential distance transform is performed even to edge point values, as shown in equation (1).

$$\sum_{i=1}^{N}\sqrt{(D_{xi}^2+D_{yi}^2)*\cos(\emptyset_i)}-\sqrt{(D_{xi}^2+D_{yi}^2)*\sin(\emptyset_i)} \quad (1)$$

3.3. Hybrid Routing Model

Our design incorporates the OLS algorithm [28] as a proactive model thanks to the routing of the hybrid feature, and it also incorporates the hybrid Manhattan distance feature for each OLS model, which estimates the node minimum values for each node that is taken into consideration. The OLS algorithm makes improvements to the design of the MPR's multi-point relays, which are anticipated to have minimum values of distance based on the distance formulations that are listed below from equations (2)-(6):

Hybrid Distance Formulations:

$$Dx1 = \sqrt{x_i\cos(45)}+\sqrt{y_i\sin(45)} \quad (2)$$

$$Dx2 = \sqrt{x_i\cos(15)}-\sqrt{y_i\sin(75)} \quad (3)$$

$$Dx = \min(Dx1, Dx2) \quad (4)$$

$$Final_{dist} = \sqrt{Dx1^2+Dx2^2} \quad (5)$$

$$dist_{xy} = \frac{x_i}{2*pi*final_{dist}}-y_i\sqrt{2*pi*Final_{dist}} \quad (6)$$

4. PROPOSED METHOD USING CLIBAT ALGORITHM

The purpose of the proposed intuitive algorithm with CLIBAT is to implicate the design with a conditional model on attack forwarding feature, logistically solve the different predictive places on the node possible attack on the Nodes and its positional changes with Improved BAT algorithm on hybrid distances in [29-30]. Figure 3 describes the intuitive feature of possible chances of attacking positional nodes and their location while operating the WSN. Here we have considered two sensor data features to implicate a solution analysis on attack features via the ICEC module. From this perspective, a hybrid feature of distances is utilized to identify the node's position and functional features while operating it. These features are effectively implicated with the ICEC module in the first phase of iteration. Attack for the WSN has been challenging to ensure what type of attack its pattern would affect the network. The proposed design postulates the different attack and defense features of the WSN model. Wormhole attack on the design feature for each set of nodes and its corresponding cluster head considered. In section 2 and section 3, practical solutions with the attack or defense features have been implicated with consideration of the routing algorithms on the design. The features of the proposed design model would improvise on three different intuitive algorithms with attack, defense and A-D Prevention algorithms on different structures of network size. The distance, and its algorithm implemented using LPA as stated algorithm 1.

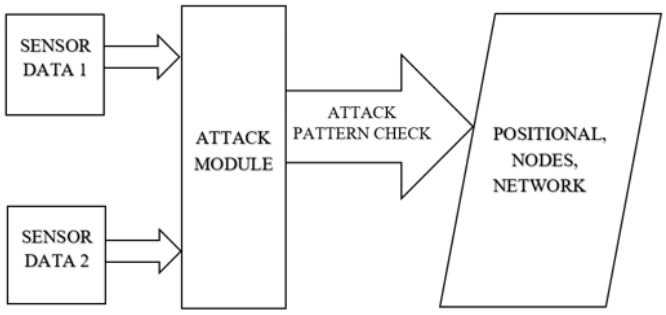


Figure 3 Representing the Attack Pattern for Positional Attack (Wormhole and Tampering Attacks).

4.1. Least Probability Gradient Algorithm (LPA)

Require: $n_i \geq 0$

Procedure: Output $\leftarrow E\left(\frac{1}{1-e^x}\right)$

1. $y \leftarrow 1$
2. $X \leftarrow$ x
3. $N \leftarrow$ n
4. $while\ N \neq 0\ do$
   a. $if(N < P(x_i * e^x))then$
   b. X$\leftarrow X \times e^{-x}$
   c. N$\leftarrow$N
   d. $else\ if\left(N > P\left(\frac{1}{e^x}\right)\right), then$
   e. y$\leftarrow y \times x_i \log\left(\frac{1}{1-e^{-x}}\right) + \sum_{i=1}^{N} x_i(1 + \log(x_i n^i))$
   f. N$\leftarrow$N+1
   g. End if
5. End while.

Algorithm 1 Least Probability Gradient Algorithm (LPA)

The algorithm 1, LPA (Least Probability Gradient algorithm) depicts the condition for which attack position would affect the node and its next node chances. So, the update values for each type of node positional changes affect the tamper attacks with the node initiated. Utilizing the LPA algorithm, the module with ICEC is improvised with an effective distance

RESEARCH ARTICLE

location using the LPA algorithm for every iteration chosen. At the same time, the attack algorithm ICEC is explained in algorithm 2 for wormhole and tampering attacks.

4.2. Attack Algorithm

The conditional model for the attack is considered with Wormhole, tampering and selective forwarding with which each of the design parametric with energy, size and other characteristics of the network would gradually demonetize the WSN. Let us consider the attack pattern with the proposed design model on the Wormhole with conditional probability expectations on each type of node characterized with expected probabilities. On this EP, the values of each node are assigned, and their centralities of the normal nodes with $c_1, c_2 \ldots$ cin. Since the wormhole attack feature modifies the positional changes with its node effect. This effect would suffice the relative change in the centrality of the node before the attack and after the attack. Hence, the prevention scheme would expect a node with corrupted centrality on the regular and attack stage of the node directed. The formulation of the attack pattern is shown in Algorithm 2.

$Input\ n \geq 0$

$Output\ c_h = E(P(CH_n^i))$

1. $Procedure$: $Initialize\ the\ attack\ pattern\ with\ ICEC$
2. $y \leftarrow CH_n^i$
3. $X \leftarrow x_i$
4. $N \leftarrow n_i$
5. $while\ N \neq 0\ do$
6. $if\ N \geq P\big(E(CH_i^n)\big) then$
7. $X \leftarrow X \times X$
9. $N \leftarrow N/2$
10. $else\ if\ N < P\big(E(CH_i^n)\big) then$
11. $y \leftarrow E(CH_n^i) \times Var(x_i) * \sum_{i=1}^{N} n(x^i)$
12. $N \leftarrow N + 1$
13. $end\ if$
14. $end\ while$

Algorithm 2 Improved Conditionally Expected Criteria (ICEC)

The algorithm 2 improvises specific criteria for the attack as Improved Conditionally Expected Criteria feature with probabilities on the cluster nodes attack problem. As in most cases, the attack node will be the least significant node for which the model will consider a typical case. Hence results in an attack on the WSN. As per the attack case, the least significant model will become prominent on the cluster node, which effectively remains the wormhole attack. Also, the prominence feature will change its positional features in CH-node at every iteration of the model implemented.

4.3. Block Diagram for Defense Pattern

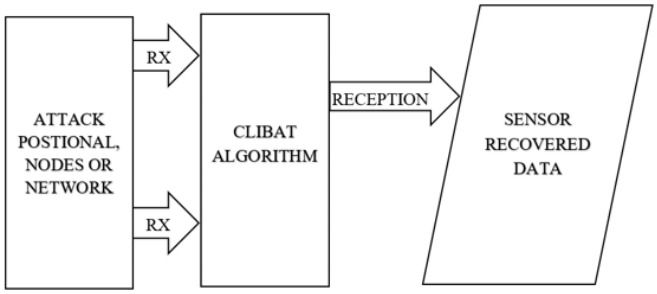


Figure 4 Representing the Defense Block Diagram using the CLIBAT Algorithm with LPA (Node Position)

The defense/prevention mechanism feature with Wormhole attack is modelled with figure 4 representing the different sensing node data as formulated with a logical feature on a sigmoid function to estimate the weights characterized on the CH Nodes. This feature on the sigmoid function as has depicted below:

$$F(x) = \frac{1}{1-e^x} \qquad (7)$$

From equation (7), the solving of the differential weights with expected probability is calculated using the weight prediction formulation:

$$W(K+1) = W(k) + x_i \log\big(F(-x) + \sum_{i=1}^{N} x_i * \log(x_i * n_i)\big) \qquad (8)$$

The equation (7)-(8) is improvised with a log feature for estimating the probabilities on the different weights of the CH-nodes, extracting the different possible locations on traversing for every iteration. Every possible update on equation 2 is implicated with the algorithm mentioned below. In algorithm 2, our design with the sigmoid function is improvised with characteristic nodes on each case of expected probability with nodes on WSN, as mentioned in figure 5. The distance formulation and its minimization of energy features are explained in section 3.

4.4. WSN Network Implementation

4.4.1. Distributed Energy-Efficient Clustering (DEEC) Protocol

The concept of aggregation, which is based on the similarity of sensors and provides energy savings and scalability, forms the backbone of sensor networks and helps prolong the lifetime of sensor networks. This way, the nodes that make up the WSN collaborate by grouping them into clusters [3]. However, the benefits of distributing energy in a more

RESEARCH ARTICLE

balanced manner throughout the network have been explored in some of the research published on the topic. Different cluster size structures are the concerns that should be used as a foundation, and they should be determined based on the heterogeneous structure of the nodes in the network. This work applies whether the nodes are near the BS or not. Only homogeneous nodes were employed in part of the research, while in other research, the idea of distributed energy was not even considered.

Presently, the proposed model aims to identify such a situation with energy reduction and performance estimation on the heterogeneous structure of the DEEC protocol, as mentioned in figure 6. The protocol with the structure inculcates features of the probability of finding the nodes utilized to sense the data Let r be the rounds in R predicted values where all energy parameters are represented with full Nodes N.

$$R = \frac{E_{total}}{E_{Around}} \qquad (9)$$

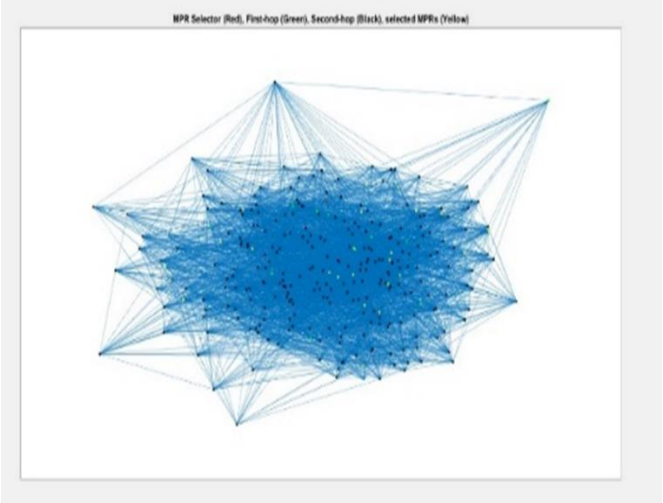


Figure 5 Representing WSN Structure using the DEEC-LIA Protocol

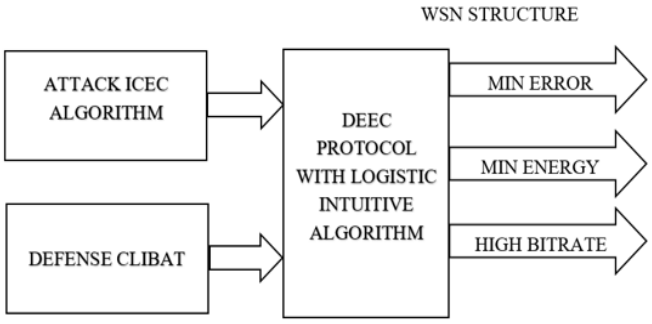


Figure 6 Representing the Overall Attack and Defense Algorithm with DEEC Protocol with LIA

4.4.2. Conditional Logistic Intuitive BAT (CLIBAT) Algorithm

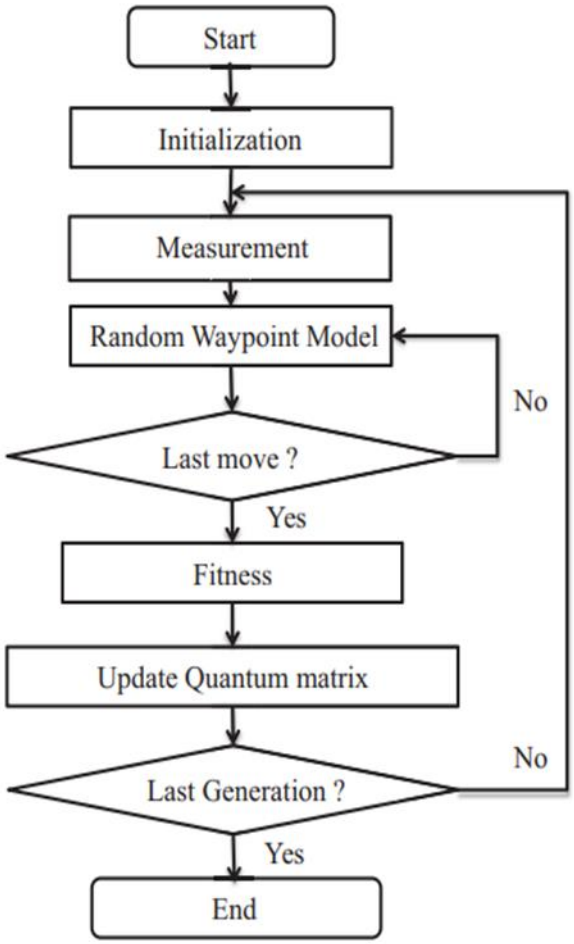


Figure 7 Representing LIA Flow Diagram using the LPA Algorithm

The flow diagram observed in figure 7, the proposed design feature with the intuitive model on routing with a predictive algorithm, initiates the scenario of a wormhole attack based on the different distances calculated with cluster nodes and its MPR's distances on the OLS algorithm. As in [29-30], "Based" have improvised with a hybrid OLS scheme with firefly and even with GA. This feature of the predictive models with the routing distances has improvised on the different attack patterns and defense patterns with prevention and control models. Mostly the attack control is depicted with changes in Nodes and their locations for each type of attack considered. Wormhole and other attacks like tampering, black hole, and selective forwarding feature effectively improvise with machine learning and nature-based optimizing feature. This diagram effectively conditionalizes with different features on the optimization functionality as a fitness function for the type of algorithm chosen.

RESEARCH ARTICLE

4.5. Mathematical Formulation for Energy Minimization Using CLIBAT

CLI refers to conditional logistically improved features with nature-inspired optimization (I-BAT) to structure node features and their positional changes on WSN. The cluster head discussion is shown in Algorithm 3.

1. $procedure\ CH - HDCA$
2. $for\ each\ node\ i \in N\ do$
3. $calculate\ the\ centrality\ of\ each\ node$
4. $let\ C_i(i) \in N(i) * U_i$
5. $C(i) \leftarrow \max(\frac{\sqrt{X_i^2 - Y_i^2}}{X_i} + \sqrt{\frac{Y_i}{X_i^2 + Y_i^2}})$
6. $MPRSet(i) = \sqrt{\sum_{i=1}^{N} CM_i}$
7. $end\ for$
8. $end\ procedure$

Algorithm 3 Cluster Head Distance Minimization Algorithm

We improvise an optimal solution for implicating Node estimations for hybrid routing as proposed, using formulations as mentioned for each set of nodes and selected clusters as equations from (10)-(11):

$$CM_i(i) = \sqrt{(X_i^2 - \frac{Y_i^2}{X_i}) + (\frac{Y_i}{X_i^2 + Y_i^2})} \quad (10)$$

$$MPR(i) = \sqrt{\sum_{i=0}^{N} CM_i} \quad (11)$$

4.5.1. CLBAT Algorithm

In the algorithm 4, the influential nodes are clustered using a hybrid mean feature model to calculate the different centralities of the WSN. The defected nodes with the attack are classified with a Logistic model improvising on different features MPR attack to be true or false.

Input: $x_i = c_1 x_1 \dots c_n x_n \rightarrow clibat\_population$

Output: $x^{best} \& F_{min} \rightarrow optimal\ solution$

1. Initialize the population with randomization on distance and energy equations.
2. Evaluate x_i and generate new population x_{i+1}
3. Compute x^{best} and global best.
4. While $(t_h \leq t_{max1})$ do
5. $for\ i = 1{:}\ N_x$ do
6. $update\ the\ frequency\ using\ equation\ 7$
7. $update\ the\ velocity\ using\ equation\ 8$
8. $update\ the\ position\ and\ distance\ using\ equation\ 9$
9. If $(P(n) > r_i^t)$, then
10. $x_i^t = equation\ 10$
11. End
12. If $F_{new} = compute\ x_i^t$ generates a new solution
13. Evaluate = evaluate +1
14. If $(f_{min1}^{new} < f_{old}\ and\ P(n) < X_i^t)$, then
15. $x_i = x_i^t, f_{old} = f_{min1}^{new}$
16. $end\ if$
17. $f_{min1} = \min\left(F(x^{best})\right)$
18. $end\ for$
19. End while

Algorithm 4 CLI-BAT

Since the model is with the model, our design improvises on the specific features of the attack pattern and its corresponding node's attack chances. With the feature, the IBAT algorithm comprises featured models with expected attack chances with nodes, its energy minimization feature for each iteration. The above algorithm expects to improvise nineteen steps for the IBAT to provide fitness values for each type of attack or defense mechanism chosen. The best solution is observed with simulated factors in the simulation setup. The solutional model for expected values of probability of different energies is estimated with formulation as mentioned below.

4.5.2. Energy Model

The energy minimization with the CLIBAT algorithm ensures the design network parametric to suffice the predicted values and its corresponding MPR estimation from [28-29]. The overall Energy efficient formulations are stated below.

Let "S" be the substantial weights acquired with MPR and proposed CL algorithms ensuring expected probabilities estimated with formulation on characteristics nodes generated during the IBAT algorithms for energy minimization and A-D pattern classification.

$$S(i) = \sum_{j=1}^{K} \sum_{i=1}^{N} \boldsymbol{\omega_i} * \boldsymbol{W_i(j)} + \boldsymbol{\epsilon_i} * \boldsymbol{MPR(i,j)} \quad (12)$$

RESEARCH ARTICLE

The values $\boldsymbol{\omega}$ **and** $\boldsymbol{\epsilon}$ are the error and weight features estimated with the attack and defense pattern.

$$\boldsymbol{CLI(i > j) = \sum_{i=1}^{N}(n_i * CM_{min}(i) + \sigma * S(i))} \quad (13)$$

$$\boldsymbol{CLI(i \leq j) = \sum_{i=1}^{N}(n_i * CM_{avg}(i))} \quad (13\ (1))$$

CLI implicates the different conditional probabilities for the design and its nodes with hybrid routing protocols representing the WSN model. The nodes with the attack or even dense state for which the centralities of the nodes with distances average and minimum scenarios are estimated as the nodes n, i and $\boldsymbol{\sigma}$being the effective probabilities on exceptional features with energy and A-D patterns.

$$\boldsymbol{P^E_{CLIBAT} = CLI(i > k) + CLI(i \leq j)} \quad (14)$$

$$\boldsymbol{P^E_{Head\_cluster} = \gamma * W_i * D_{min} + \mu CLI(i) + E^{entropy}_{CLI}(i)} \quad (15)$$

Here$E^{entropy}_{CLI}(i)$ effectively improvises on which

Hence the total Network energy estimated is:

$$\boldsymbol{P^E_T = P^E_{Head\_cluster} + P^E_{CLIBAT}} \quad (16)$$

The practical problem with A-D pattern analyzing and its simulation features with bit rate, energy minimization on the network while inflicting the changes with nodes and its plotting feature on active and passive nodes are estimated in the next section.

5. RESULTS AND DISCUSSION

5.1. Simulation Setting

The simulation model with Area size from 100 to 1000 is varied till 1000X1000 from references in [28-29] were till 200X200. The WSN network size for 300-1000 was estimated in our design as proposed in figure 5. The design of WSN is modelled with an initial setup as mentioned from the different aspects of the energy parametric from references [28-29]. These values are effectively estimated with the CLIBAT feature on the current model with each of the pattern accuracies and its improved solution features on OLS and AODV routing for the proposed WSN.

The proposed design has depicted the results with its bit rate and energy minimization values depending upon the algorithms implemented on references [14,16,30] which have a more accurate design when compared to the proposed CLIBAT. In this simulation, we emphasize different parametric such as accuracy, bit rate and energy minimization, as mentioned below, since the attack and defence accuracies are depicted in table 1, which provides the overall newer research feature improvements on the Security based problem for Wireless sensor networks.

5.2. Performance Evaluation

The overall simulation is operated with node variations from 100 to 1000, respectively. Since the practical feature improvements with bit rate is a prime aspect of the design, which is controlled with the different sensor active nodes as presented with simulation parameters in table 2. The energy model estimation is done with formulation as modelled from the fig 10 – fig 15, have been depicted for both attack and defence patterns indicating the overall bit rate for the design Model with CLIBAT. This feature with energy equations depicts the possible active cases on the WSN, which effectively reutilizes the design parametric depending upon the weight prediction in equation (8).

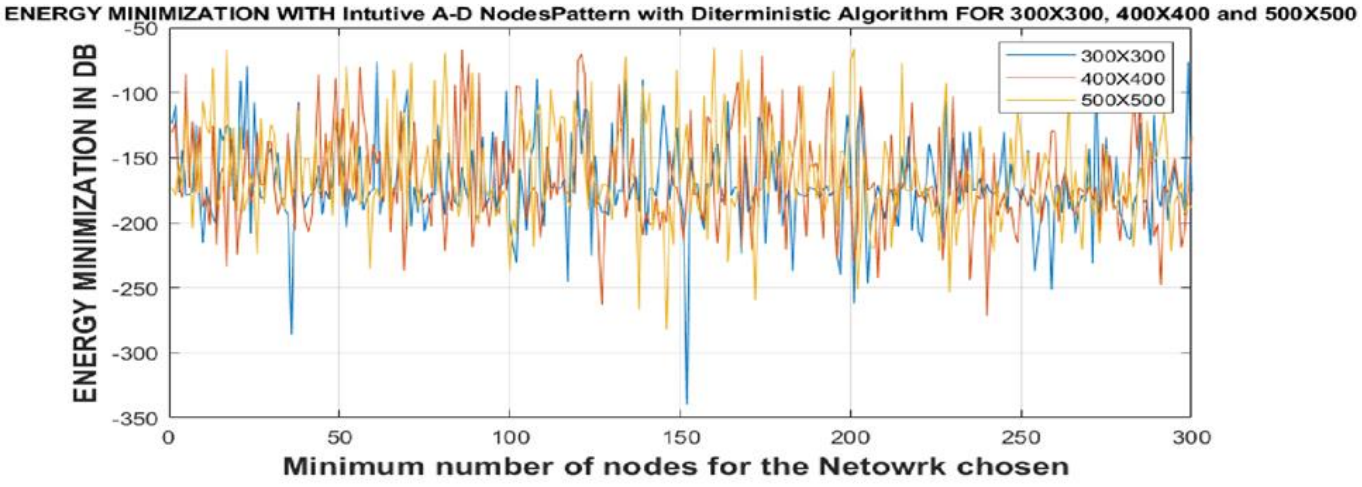


Figure 8 Representing the Energy Minimization at 300X300- 500X500 Nodes

RESEARCH ARTICLE

Cluster Head Energy and CLIBAT energy are estimated with every possible change in gamma, Mu, and CLI, as mentioned in equation (14). In figure 8 the overall design feature with minimization of the energy is considered to evaluate the different iteration values as tabulated. The minimum energy is estimated with the factor of gamma (varied for (0,1) randomly). The $\boldsymbol{\mu}$feature has been depicted with different solutions indicating the CLI model to vary from 100-300 dB values.

Figure 8 describes the information on the least possible energy while implementing the number of iterations from 300 to 500. From the graph, iteration 150 with a gamma value of 0.8945 would observe the minimum energy values as -346dB. At the same time, the other iteration values would achieve values between -250 to -300 dB.

Similarly, the design features with Mu values would improvise the other performance factor as tabulated in Tables 3 and 4. These accuracy values for each attack and defence pattern from the CLI and BAT algorithms are designed to outmatch the other existing models, as mentioned below in figures (11) – (14).

Table 2 Representing the Different Energy Values and Initial Values Affecting the WSN Structure Proposed

Parametric Criteria	Values
No of iterations	10000, 62500,90000,105625
No of Nodes	100,250,300,325, 500,600,750,800,950,1000
Energy initial values	0.5J
No Sensor Nodes	100
Base station	(75,75)
Cluster radius	25 m
Constants α, β, μ, σ, ω, λ	(0,1)

The overall parametric changes and expected values for iterations are presented in Table 2. Since the minimum node energy required to initiate the design is 0.5 J, our design is to provide a solution with which fewer energy values are observed in terms of $10^{-10} to\ 10^{-20}$ values for energy for the ideal case. While in practicality, we observe factors $10^{-3} to\ 10^{-8}$ depending upon the equations (1)-(20).

5.2.1. Parametric Changes for Energy Minimization

This study effectively depicts the different MPR-selected nodes for the minimization energy mentioned below, creating distinct features varying from (100-1000) nodes. The design is implemented with LPA and ICEC algorithms for the Attack checking and CLIBAT algorithm for the defence mechanism.

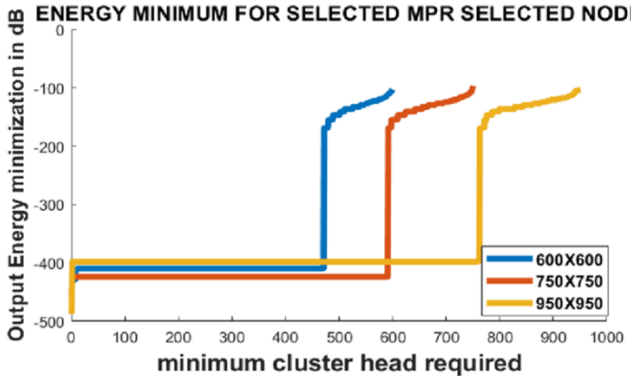


Figure 9 Representing the Energy Minimization for MPR Selected Nodes with a Minimum Energy of -168dB.

Figure 9, with MPR nodes varying from 600 to 950, area size have been depicted with different values of gamma varied from 0.5 to 0.8 as presented for CLIBAT DEEC protocol. The overall cluster head formulation with equations 11 to 14 defines the overall energy possible values observed in the DEEC CLIBAT algorithm. As mentioned below, new features with CLIBAT have been depicted with bit rate calculations. Our design with bit rate parametric is utilized mainly for attack and defence patterns to analyse the protocol based on the sensed data as mentioned in equations (17) - (18).

5.2.2. Bit Rate Calculations

The bit rate is implicated within the design implementation of WSN with DEEC protocol. Different bit rates are estimated when each transmitted bit receives the correct feature of sensed data with and without an attack/defence pattern. Finally, these values are implemented in MATLAB, simulating 10000, 62500, and 1,05,625 iterations on the design with high-performance PC-i7-6th generation and 32 GB RAM. The formulation for bitrate is defined as:

$$BR = N * BS\_sensed_{data} \quad (17)$$

Here in equation (17), N represents no of iterations BS base station sensed data for Tx and Rx for all alive cases.

$$BS_{sensed_{data}} = Alive_{status} * n_x \quad (18)$$

For n_x be the number of alive cases for each N iteration.

Below, figure 10 represents the overall bit rate estimated based on equations (17) and (18), inculcating max value is attained with 2Mpbs for all the different iterations considered.

Figure 10 depicts the graphs with nodes varying from 600 to 950 for the formulations utilized in equations (17-18). The bit rate variations are consistent and increase linearly as the

RESEARCH ARTICLE

number of nodes increases. The maximum value is obtained at$5 * 10^6$. The total iterations are considered from 100 to 5000, as mentioned in figure 10. With similar aspects, the overall accuracy for attack and defence patterns for the DEEC-CLIBAT algorithm, as proposed from the formulations in 14, would demonstrate different values for each accuracy for the sensed data as depicted in figures (11) and (14).

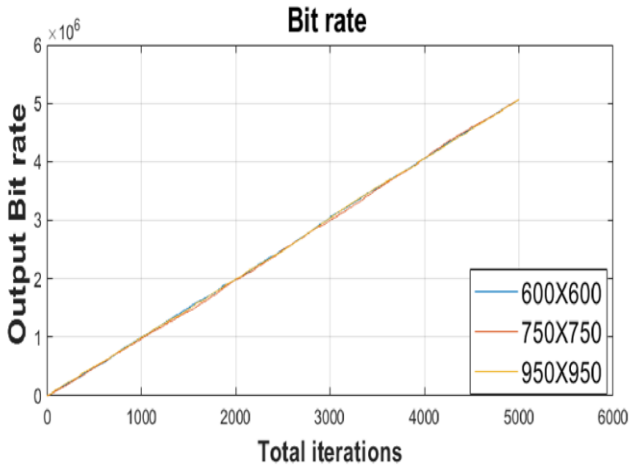


Figure 10 Representing the Overall Bit Rate for CLIBAT with Nodes Varying from 600X600 to 950X950

5.2.3. Accuracy Calculations

The overall accuracy of the above figure is estimated based on the alive status on each iteration, with a minor error estimated. The log entropy estimation is calculated via

$$F = \log(entropy(G)) \quad (19)$$

The above equation (19) represents the overall log minimization with which minimum values are represented and calculated. This value is observed for each type of iteration, and the total number of nodes varies accordingly to minimize the error. Suppose the error is less than the threshold value which is randomly assigned during the iteration. The overall accuracy for the attack and defence features is represented below.

Table 3 depicts existing approaches indicating the different weight values formulated in equation (14). The effective weight from the CLIBAT feature is utilized to encapture the error loss obtained from the accuracy output for each attack and defence pattern algorithm, as mentioned.

Since the tabulated values, we have observed that with accuracy and bit rate, our design outperforms with different values observed with genetic firefly algorithms, as mentioned in table 3. The state of art features is compared with random probability values with different time instants for the bit rate comparisons, as mentioned in figure 15.

Table 3 Representing the Parametric Comparison for Existing and Proposed Algorithms

SNO	PROTOCOLS	MINIMUM ENERGY VALUES (DB)	BITRATE (Mbs)	ENERGY ERROR OPTIMIZED (DB)
1	DEEC-GA	-91.34	1.39	4.67
2	LEACH-GA	-90.4	1.256	6.82
3	DEEC-SCI-HITTA	-152.87	1.9	15.78
4	DEEC-FIREFLY	-128.85	1.8	12.75
5	DEEC-CLI	-158.94	1.98	16.74
6	DEEC-CLIBAT	-167.17	2.07	18.84

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/217700 Volume 9, Issue 6, November – December (2022)

RESEARCH ARTICLE

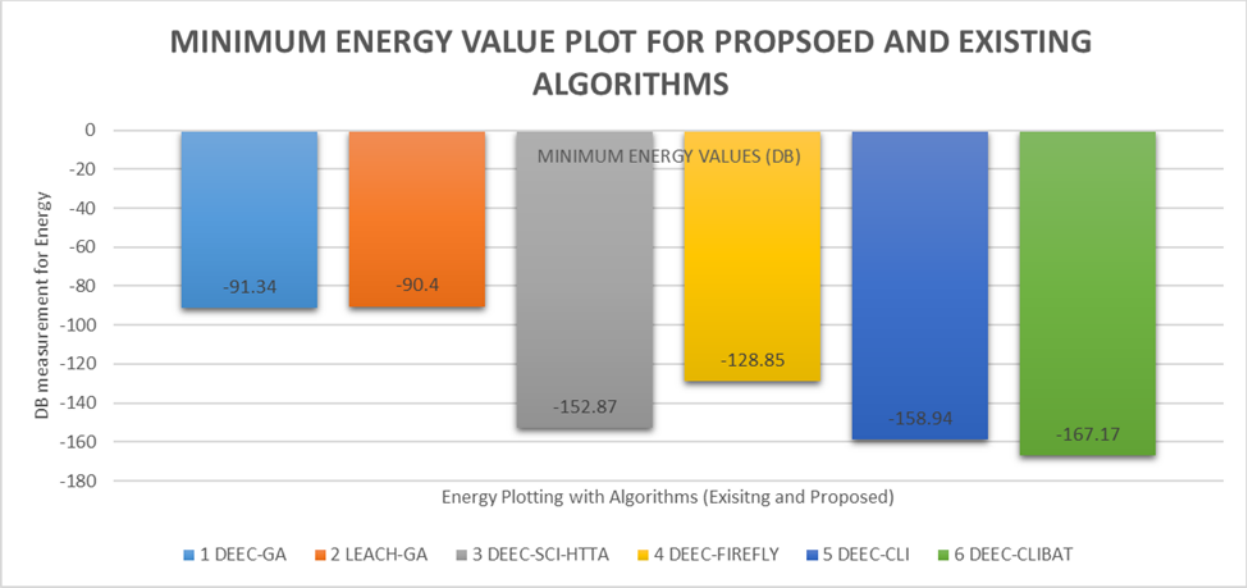


Figure 11 Representing the Minimum Energy Values Plotting for Existing Algorithms [28-29] and Proposed Algorithms

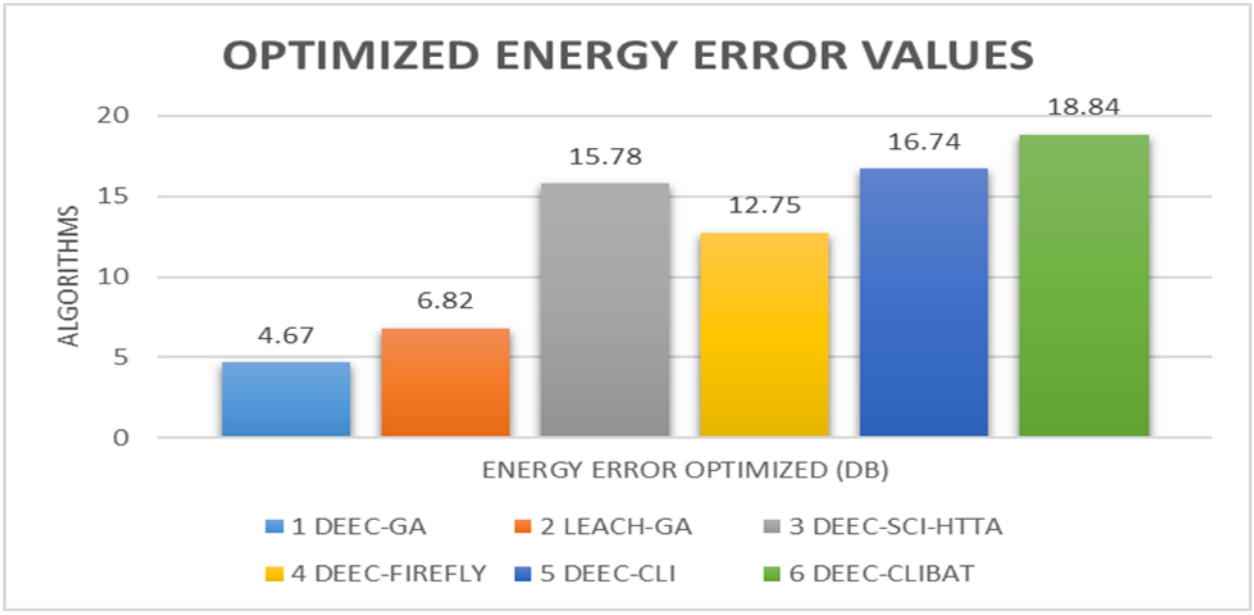


Figure 12 Representing the Error Values for Existing and Proposed Algorithms

The tabulations for the proposed model with CLI and CLIBAT features are modelled and tabulation with corresponding network parameters from references 28-29 for improved features observed. In table-3, our design with the different parametric values of the minimum energy, bit rate and error features are compared with the references mentioned. Figure 11 describes the different features of the DEEC protocol with the CLIBAT algorithm utilized with the highest minimum energy values at the value of 167.17dB. While the other algorithm with CLI is approached with a 158.94dB value, as mentioned in the chart. The DEEC-GA and LEECH-GA provision less parametric values observed.

Regarding references, 28-29 are good enough for the attack control and prevention features measured in table 3. The Highest bit rate is observed with the CLIBAT feature in figure 12, with the DEEC protocol improving the different attack and defence prediction weights for every iteration. In figure 12, error-optimized dB values are implicated with the

RESEARCH ARTICLE

algorithm proposed and existing from the references [28-29]. Our CLIBAT featured algorithm has consistently improved all the parametric network features considered as tabulated in table 3.

The overall error model and its analysis are implicated with different parametric methods and DEEC and CLIBAT models as proposed. The equations governing the different features of the data are prescribed with values of Mu, as depicted in section 3. We consider Mu variation within the limit (0,1) as the overall probability density function for the proposed model on the energy is always one. So overall, the design on the CLIBAT has depicted an error formulation as (eq 20):

$$\text{error}_{\text{obtained}} = 1 - \log(\text{entropy}(G)) \qquad (20)$$

Here in this above equation, we depict the values of G depending upon the predicted defence mechanism observed per the design.

In table 4, we demonstrate the overall protocols from state-of-the-art to currently utilized algorithms and compare them with the proposed models. This table 4 indicates the accurate features estimated based on the entropy for each sensed data while the sensors are active on every iteration. From 1-5001, iterations are considered with different nodes varying from 100 to 1000, as depicted in figures 6-14.

The attack parametric and its features are designed based on the scenarios considered with no nodes relating to the minimization of the attack rate and defence rate, as mentioned in table 1 for different researchers. So, we have proposed a solution that governs the attack and defence patterns based on the type of input stream chosen and its random nature. All mathematical formulations are depicted from equations (3) to (14), analysing the overall network architecture. Since the sensing structure for each pattern on the attack and defence are implicated based on the routing algorithm in reference [28-29].

Table 4 depicts the references' different attack and defence accuracy as stated below. We could see that our proposed design has been depicted with different references as [14,16,30] have depicted the detection accuracies higher when compared to the others, having better results in accuracies and bit rate.

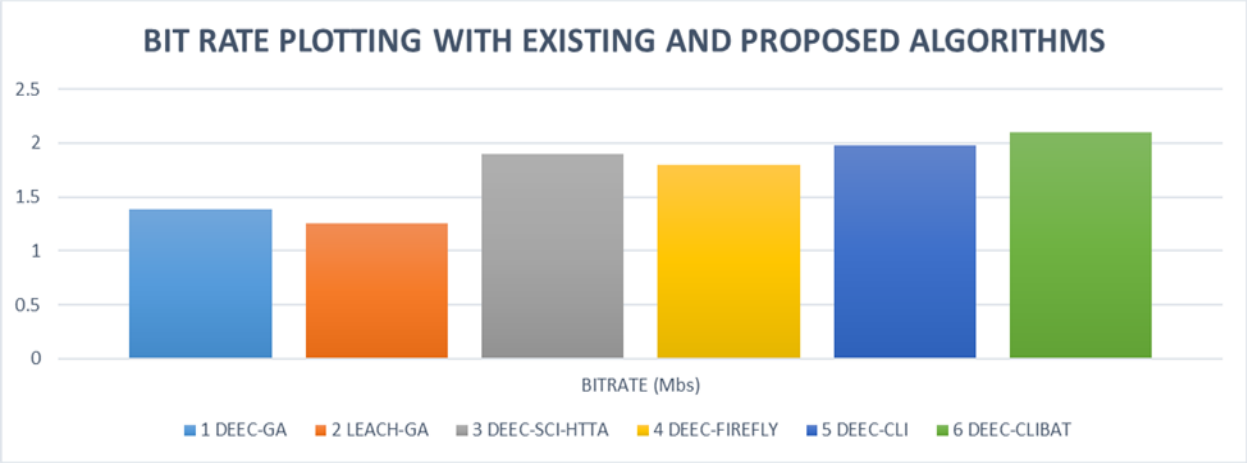


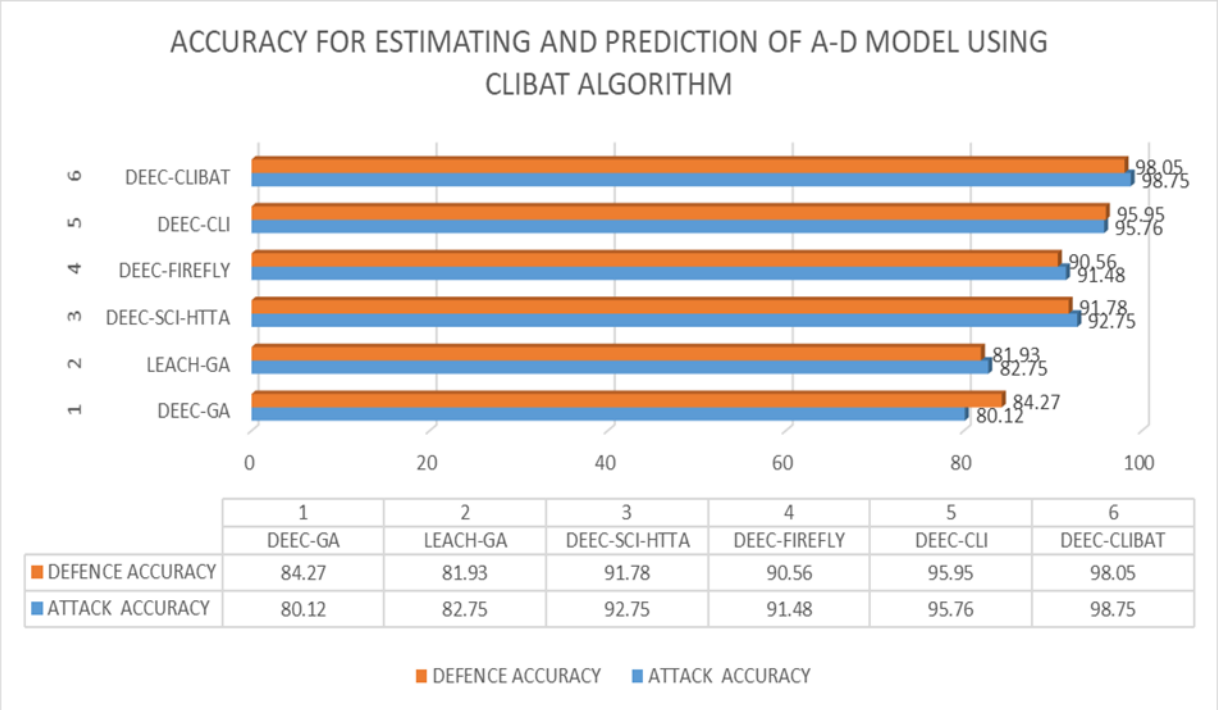
Figure 13 Representing the Bit Rate for Algorithms WSN with Existing and Proposed Algorithms

Table 4 Representing the Accuracies for Attack and Defence Patterns in WSN with Algorithms Mentioned

SNO	PROTOCOLS	ATTACK ACCURACY	DEFENCE ACCURACY
1	DEEC-GA	80.12	84.27
2	LEACH-GA	82.75	81.93
3	DEEC-SCI-HITTA	92.75	91.78
4	DEEC-FIREFLY	91.48	90.56
5	DEEC-CLI	95.76	95.95
6	DEEC-CLIBAT	98.75	98.05

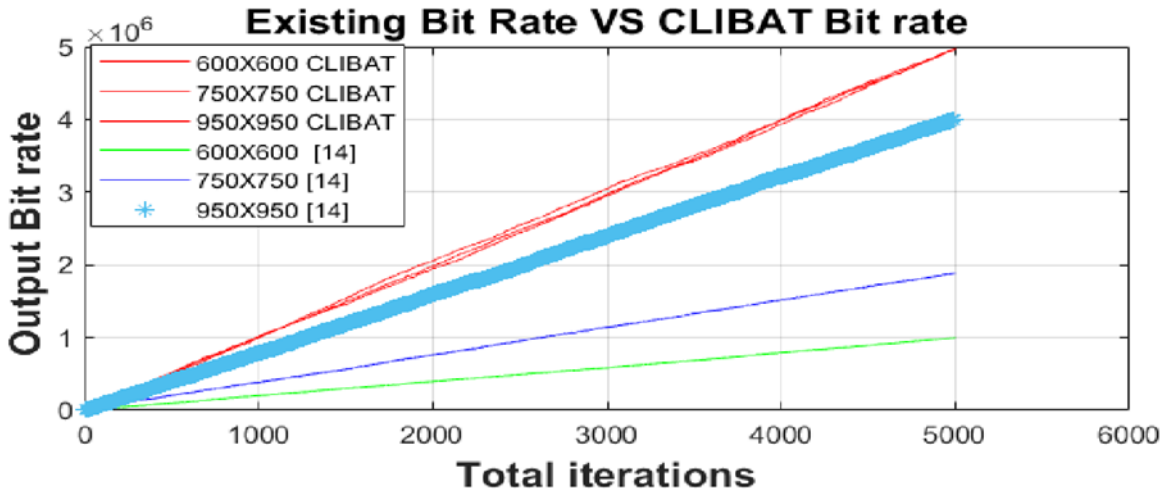
RESEARCH ARTICLE

7	[14]	97.56	98.3
8	[16]	97.67	98.2
9	[30]	97.41	97.19



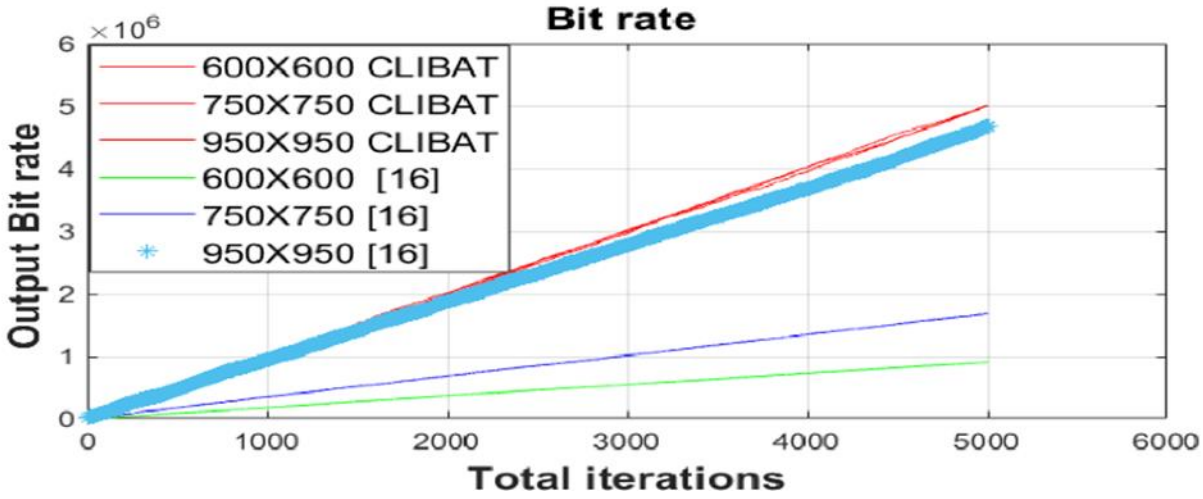
	1 DEEC-GA	2 LEACH-GA	3 DEEC-SCI-HTTA	4 DEEC-FIREFLY	5 DEEC-CLI	6 DEEC-CLIBAT
DEFENCE ACCURACY	84.27	81.93	91.78	90.56	95.95	98.05
ATTACK ACCURACY	80.12	82.75	92.75	91.48	95.76	98.75

Figure 14 Representing the Accuracies bar Plot for Prediction of the A-D Model

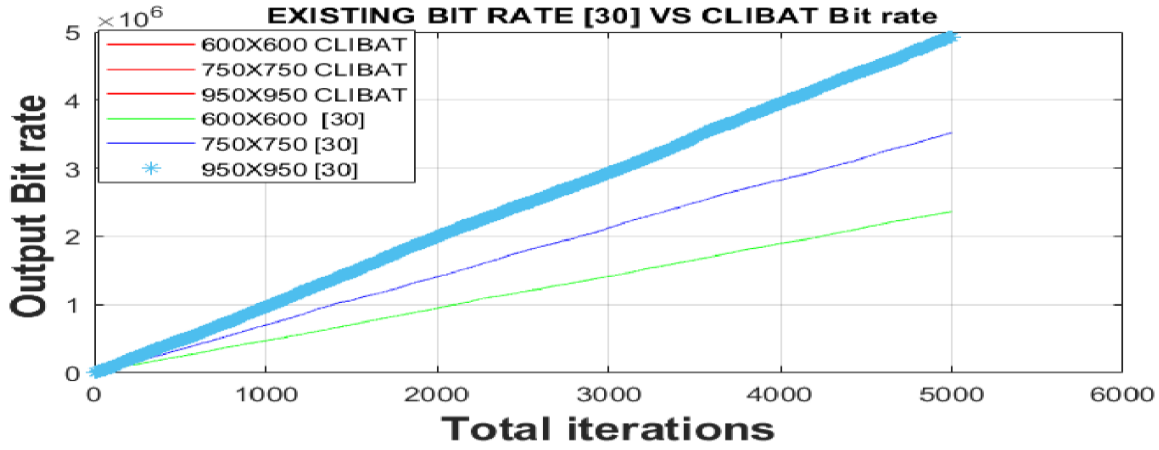


(Reference [14] vs CLIBAT Bit Rate)

RESEARCH ARTICLE



(Reference [16] vs CLIBAT Bit Rate)



(Reference [30] Vs CLIBAT Bit Rate)

Figure 15 The Comparative Graph for bit Rate from 600-1000 Nodes for Proposed and Existing Models [14, 16, 30]

This feature on the design with CLIBAT has proven better attack and defence accuracies. Also, the overall detection rate is defined with an overall estimation of the attack and defence based on the formulation shown in (eq 21):

$$\text{Acc} = \frac{\text{TP}}{\text{TP} + \text{TN}} * 100 \qquad (21)$$

The overall features for the actual cases of attack detected and the overall series of iterations have been dedicated to the entire dataset chosen for the results. Hence, we have observed 98.75% detection accuracy, which is far better than the references [14,16 and 30].

In figure 14, our design with the predictive feature of the weights estimated from the formulation's equation (1-9) has improved accuracies over the existing models. The overall accuracy for the CLIBAT algorithm for the attack is 98.75, and for the defence, the feature is 98.05. Hence an average accuracy of 98% is implicated with the formulations mentioned above. Considering the parametric features in table 3 and table 4, CLIBAT has been more accurate and stable for attack and defence patterns.

From the figure 15, our proposed design has depicted improved changes in the design, which have been improvised with different bit rate comparisons based on the references [14,16 and 30]—at the same time, indicating the design on the changes of different size of nodes mentioned in figure 15 with improved bit rate feature that is affected with and without the attack. The proposed work effectively concludes with improved energy minimization and sufficient accuracy and defence accuracies on different literature surveys mentioned in table 1, with which we could observe that most of the recent design models have accuracies ranging from 95- 98.4.

RESEARCH ARTICLE

Only two researchers achieved greater than 98.5. With these features of the designs, our proposed model on the A-D feature with CLIBAT has successfully dedicated the architectural changes via routing as proposed in [28]. While this feature in the comparison of figure 15 has been observed, a linear graph dedicates the different features of the design as the formulations mentioned in equation (17-18) for bit rate. So we could see that references [14 and 16] underperformed with the same features as formulated based on the proposed design structure. While reference 30 has shown similar status, the proposed design outperforms the state of the arts for attack and defence criteria.

6. CONCLUSION

A practical solution with an A-D pattern model with the CLIBAT algorithm has been implicated with different distances features and conditional probabilities with expected values on each characteristic node affected. The attack pattern for Wormholes successfully demolishes the WSN, while the defence pattern can solve tampering and selective mapping problems with an accuracy of 98.8%. In the case of Wormhole with CLIBAT on DECC routing protocol utilizes the parametric criteria on minimization of energy at 5000 iterations and for other iterations, we could see that at 950 similar behavioural structure of minimizations is observed in figure (10)-(15). The overall design of the CLIBAT is compared with Firefly, GA, with DEEC algorithms proposed in [28]. With the CLI_BAT algorithm, our design reduces the energy as minimum as possible from the tabulations mentioned in table 3 and table 4 improvises the attack pattern accuracies with logistics, decision tree and SVM algorithms compared with existing algorithms.

REFERENCES

[1] RaniyahWazirali, Rami Ahmad, “Machine learning approaches to detect DoS and their effect on WSNs lifetime” Computers, Materials and Continua (2022).

[2] Karen Ávila Paul Sanmartin Daladier Jabba, Javier Gómez, “An analytical Survey of Attack Scenario Parameters on the Techniques of Attack Mitigation in WSN” Wireless Personal Communications (2022).

[3] Kale NavnathDattatrayaK. Raghava Rao, "Hybrid-based cluster head selection for maximizing network lifetime and energy efficiency in WSN", Journal of King Saud University - Computer and Information Sciences (2022).

[4] P. Gite, K. Chouhan, K. Murali Krishna, C. Kumar Nayak, M. Soni, and A. Shrivastava, “ML Based Intrusion Detection Scheme for various types of attacks in a WSN using C4.5 and CART classifiers,” Materials Today: Proceedings, 2021, DOI: 10.1016/j.matpr.2021.07.378.

[5] A. Arshad, Z. M. Hanapi, S. Subramaniam, and R. Latip, “A survey of Sybil attack countermeasures in IoT-based wireless sensor networks,” PeerJ Computer Science, vol. 7, 2021, DOI: 10.7717/peerj-cs.673.

[6] B. A. Ashwini and S. S. Manivannan, “Supervised Machine Learning Classification Algorithmic Approach for Finding Anomaly Type of Intrusion Detection in Wireless Sensor Network,” Optical Memory and Neural Networks (Information Optics), vol. 29, no. 3, 2020, DOI: 10.3103/S1060992X20030029.

[7] R. Fotohi and S. Firoozi Bari, “A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms,” Journal of Supercomputing, vol. 76, no. 9, 2020, DOI: 10.1007/s11227-019-03131-x.

[8] N. Nithiyanandam and P. Latha, “Artificial bee colony-based sinkhole detection in wireless sensor networks,” Journal of Ambient Intelligence and Humanized Computing, 2019, DOI: 10.1007/s12652-019-01404-0.

[9] S. V, “Detection of Localization Error in a WSN under Sybil Attack using Advanced DV-Hop Methodology,” IRO Journal on Sustainable Wireless Systems, vol. 3, no. 2, 2021, DOI: 10.36548/jsws.2021.2.003.

[10] S. Ilavarasan and P. Latha, “Detection and elimination of black hole attack in WSN,” International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 1, 2019, DOI: 10.35940/ijitee.L3908.119119.

[11] S. Singh and H. S. Saini, “Learning-Based Security Technique for Selective Forwarding Attack in Clustered WSN,” Wireless Personal Communications, vol. 118, no. 1, 2021, DOI: 10.1007/s11277-020-08044-0.

[12] R. Bhatt, P. Maheshwary, P. Shukla, P. Shukla, M. Shrivastava, and S. Changlani, “Implementation of Fruit Fly Optimization Algorithm (FFOA) to escalate the attacking efficiency of node capture attack in Wireless Sensor Networks (WSN),” Computer Communications, vol. 149, 2020, DOI: 10.1016/j.comcom.2019.09.007.

[13] A. Dogra and T. Kaur, “DDOS attack detection and handling mechanism in WSN,” International Journal of Recent Technology and Engineering, vol. 8, no. 3, 2019, DOI: 10.35940/ijrte.C5644.098319.

[14] M. v. Pawar and A. Jagadeesan, “Detection of blackhole and wormhole attacks in WSN enabled by optimal feature selection using self-Adaptive multi-verse optimizer with deep learning," International Journal of Communication Networks and Distributed Systems, vol. 26, no. 4, 2021, DOI: 10.1504/ijcnds.2021.115573.

[15] V. Saini, J. Gupta, and K. D. Garg, “WSN protocols, research challenges in WSN, integrated areas of sensor networks, security attacks in WSN,” European Journal of Molecular and Clinical Medicine, vol. 7, no. 3, 2020.

[16] E. Karakoç and C. Çeken, “Black hole attack prevention scheme using a blockchain-block approach in SDN-enabled WSN,” International Journal of Ad Hoc and Ubiquitous Computing, vol. 37, no. 1, 2021, DOI: 10.1504/IJAHUC.2021.115125.

[17] M. Jeyaselvi, S. Suchitra, M. Sathya, and R. Mekala, “Energy efficient witness based clone and jamming attack detection in wsn,” Journal of Green Engineering, vol. 11, no. 2, 2021.

[18] D. Dhadwal, V. Bhatia, and P. N. Hrisheekesha, “Method & implementation of fault detection & prevention attack in WSN,” International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue, 2019, DOI: 10.35940/ijitee.I1126.0789S19.

[19] Y. Wu, B. Kang, and H. Wu, "Strategies of attack–defence game for wireless sensor networks considering the effect of confidence level in fuzzy environment," Engineering Applications of Artificial Intelligence, vol. 102, 2021, DOI: 10.1016/j.engappai.2021.104238.

[20] C. Hongsong, M. Caixia, F. Zhongchuan, and C. H. Lee, "Novel DDoS attack detection by Spark-assisted correlation analysis approach in wireless sensor network," IET Information Security, vol. 14, no. 4, 2020, DOI: 10.1049/iet-ifs.2018.5512.

[21] P. D. Halle and S. Shiyamala, “Secure routing through refining reliability for WSN against DOS attacks using AODSD2V2 algorithm for AMI,” International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, 2019, doi: 10.35940/ijitee.I8178.0881019.

[22] S. Godala and R. P. v. Vandella, "A study on intrusion detection system in wireless sensor networks," International Journal of Communication Networks and Information Security, vol. 12, no. 1, 2020.

[23] Y. Prathyusha Reddy, B. Manasa, V. Jyothi, and V. Srikanth, "Detection and defence of DDOS attack for WSN," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 7, 2019.

[24] M. Alotaibi, “Security to wireless sensor networks against malicious attacks using Hamming residue method,” Eurasip Journal on Wireless

RESEARCH ARTICLE

Communications and Networking, vol. 2019, no. 1, 2019, DOI: 10.1186/s13638-018-1337-5.
[25] S. Dong, X. gang Zhang, and W. gang Zhou, "A Security Localization Algorithm Based on DV-Hop Against Sybil Attack in Wireless Sensor Networks," Journal of Electrical Engineering and Technology, vol. 15, no. 2, 2020, DOI: 10.1007/s42835-020-00361-5.
[26] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, "Data collection for security measurement in wireless sensor networks: A survey," IEEE Internet of Things Journal, vol. 6, no. 2, 2019, DOI: 10.1109/JIOT.2018.2883403.
[27] M. A. Elsadig, A. Altigani, and M. A. A. Baraka, "Security issues and challenges on wireless sensor networks," International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, no. 4, 2019, DOI: 10.30534/ijatcse/2019/78842019.
[28] Basith, K. Abdul, and T. N. Shankar. "Hybrid state analysis with improved firefly optimized linear congestion models of WSNs for DDOS & CRA attacks." PeerJ Computer Science 8 (2022): e845.
[29] S. Nosratian, M. Moradkhani, and M. B. Tavakoli, "Fuzzy-Based Reliability Prediction Model for Secure Routing Protocol Using GA and TLBO for Implementation of Black Hole Attacks in WSN," Journal of Circuits, Systems and Computers, vol. 30, no. 6, 2021, DOI: 10.1142/S0218126621500985.
[30] M. A. Rizvi, S. Moontaha, K. A. Trisha, S. T. Cynthia, and S. Ripon, "Data mining approach to analyzing intrusion detection of a wireless sensor network," Indonesian Journal of Electrical Engineering and Computer Science, vol. 21, no. 1, 2021, DOI: 10.11591/ijeecs.v21.i1.pp516-523.

Authors

K. Abdul Basith received B.Tech from JNTU and M.Tech CSE from VTU in 2003 and 2007, respectively, currently pursuing PhD in the Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation and working as an Associate professor in the Department of CSE in Marri Laxman Reddy Institute of Technology and Management.

T N Shankar, obtained his M.Tech and PhD from Birla Institute of Technology, Mesra, Ranchi, India. Presently working as a professor in the Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation. His research interest includes information security and neural networks. He published book title Neural Networks, University Science Press, New Delhi. He has 30 publications in his credit. He is a life member of ISTE and ACM.

How to cite this article:

K Abdul Basith, T.N. Shankar, "Minimalistic Error via Clibat Algorithm for Attack-Defence Model on Wireless Sensor Networks (WSN)", International Journal of Computer Networks and Applications (IJCNA), 9(6), PP: 661-677, 2022, DOI: 10.22247/ijcna/2022/217700.