How to Cite:
Reddy, M. S., Laxmi, M., & Kumar, B. A. (2022). An hybrid optimization driven deep residual network for attack detection and attack mitigation in wireless sensor networks. *International Journal of Health Sciences*, *6*(S5), 2254–2271. https://doi.org/10.53730/ijhs.v6nS5.9133

An hybrid optimization driven deep residual network for attack detection and attack mitigation in wireless sensor networks

M. Sowjanya Reddy
Geetanjali College of Engineering and Technology, Hyderabad, Telangana-500083
Corresponding Author: msowjanya.ece@gcet.edu.in

M. Laxmi
Geetanjali College of Engineering and Technology, Hyderabad, Telangana-500083
Corresponding Author: laxmireddy.mitta9@gmail.com

Bandani Anil Kumar
B V Raju Institute of Technology, Narsapur, Medak District, Telangana,

***Abstract*---**Wireless sensor network (WSN) comprises small sensor nodes that have the ability of sensingplatform, store and send data. In addition, the sensor nodes pose limited resource such as energy, computing power. Clustering is an effective manner for diminishing energy usage utilized by sensor nodes for sending data from source to base station (BS). The multi-path routing is utilized for routing data amongst nodes. However, the WSN are susceptible to several types of security issues which can degrade network performance. WSN are susceptible to various types of attacks, which degraded the performance of entire network. Hence, the primary purpose of this research is to design and develop attack detection and attack mitigation system in WSN for detecting the attackers. This paper devises an energy efficient and optimization aware deep model for attack detection and mitigation in WSN. Here, the first step is the simulation of WSN nodes. The overall procedure of the proposed model includes simulation of WSN, cluster head selection, routing to BS, Sybil attack detection in BS and finally attack mitigation in BS. The first step is WSN simulation and then the selection of energy efficient cluster head is done using Lower Energy Adaptive ClusteringHierarchy (LEACH) protocol. Then, the routing of the accumulated data is done using Fractional artificial bee colony (FABC) algorithm. Once the data is accumulated at BS, the attack detection and attack mitigation is performed using the accumulated data. From data, the imperative feature is selected using Jaro-Winkler distance. After determining the optimum features, the Sybil attack detection is performed with deep residual network (DRN). The training of DRN using proposed

Manuscript submitted: 18 Feb 2022, Manuscript revised: 27 April 2022, Accepted for publication: 9 June 2022

Competitive Multi-Verse Rider Optimizer (CMVRO), which is devised by combining Competitive Multi-Verse Optimizer (CMVO) and Rider Optimization Algorithm (ROA). The mitigation of Sybil attack is performed using data rates. Here, the data rate is reduced when the attacker is detected.

***Keywords*---**WSN, Sybil attack, Attack detection, deep residual network, Attack mitigation.

1. Introduction

WSN consist of several miniature devices termed as sensor nodes and sink node. This kind of network is beneficial to monitor and pass ecological and corporal concerns, such as pressure, temperature and noise with respect to the centrally positioned BS. The BS helps to handle data to present essential actions. A WSN can either unstructured or structured on the basis of locality wherein a sensor network establish for controlling the regions using sensor. A controlled network are reliable in region, such as streets, parking places, buildings and highways wherein amorphous networks are feasible in desert, disaster areas, and forest. In both types of network, a huge region is splitted in clusters and all clusters comprise small sensors and CH. The cluster contains sensor nodes, which are associated amongst each other considering coverage capacity and classical sensors nodes, and cluster poses CH for communicating with new clusters. The cluster are linked using its CH, and then collected data from all clusters is sent to sink node for processing the information in order to send the data to other heterogeneous network. The CH is considered as an imperative routing that helps all nodes of same cluster to send obtained data to BS through single hop or multiple hops. The member does not unswervingly send accumulated data to base station. The members pose the ability to save routing energy expenditure using routing support offered by CH.

2. Proposed ECMVRO based on DRN for attack detection

An energy efficient optimization aware deep model is developed for Sybil attack detection and mitigation in WSN. Here, the preliminary step is the simulation of WSN nodes. The complete process of the proposed model includes simulation of WSN, cluster head selection, routing to BS, Sybil attack detection in BS and finally attack mitigation in BS. The first step is WSN simulation and then the selection of energy efficient cluster head is done using Lower Energy Adaptive Clustering Hierarchy (LEACH) protocol. Then, the routing of the accumulated data is done using Fractional artificial bee colony (FABC) algorithm. Once the data is accumulated at BS, the attack detection and attack mitigation is performed using the accumulated data. From data, the imperative feature is selected using Jaro-Winkler distance. After determining the optimum features, the Sybil attack detection is performed with Deep residual network (DRN). The training of DRN using proposed Competitive Multi-Verse Rider Optimizer (CMVRO), which is devised by combining Competitive Multi-Verse Optimizer (CMVO) and Rider Optimization Algorithm (ROA). The mitigation of Sybil attack is performed using data rates. Here, the data rate is reduced when the attacker is detected. Figure 1 displays the architecture of proposed model for attack detection and mitigation in WSN.

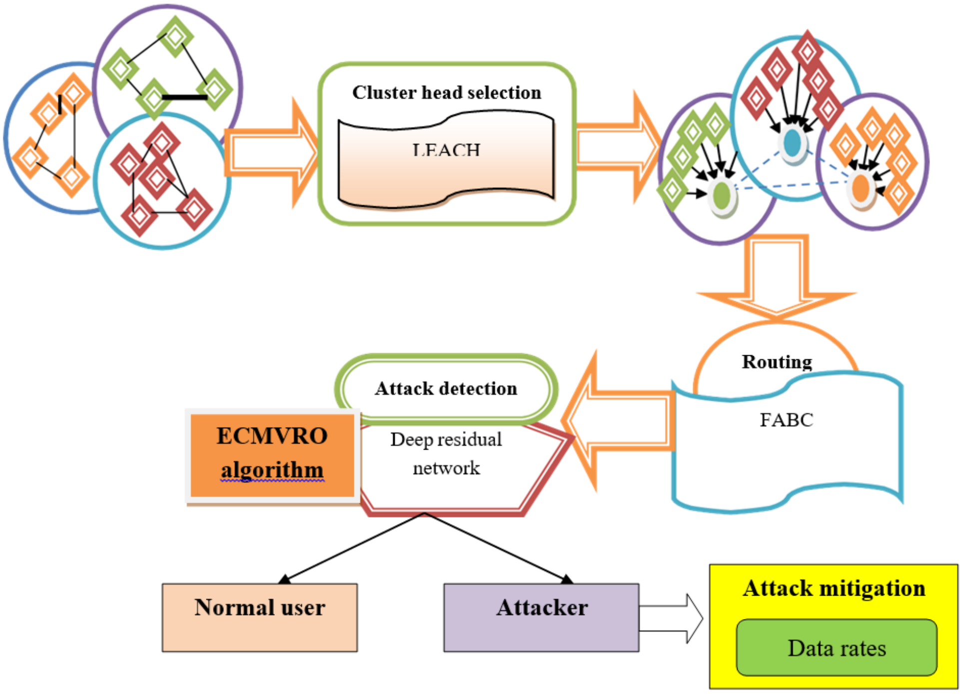

Figure 1. Architecture of proposed model for attack detection and mitigation in WSN

Simulation of WSN

WSN comprises base station and sensor nodes with each sensor nodes induced with a power unit, memory, transceivers and processor. Here, various nodes are incorporated in WSN to sense network. Hence, whenever node is active, it is liable to transmit and receive the data while if node is inactive, then the node never contribute to data transmission. Here, the lifetime of network is considered as an imperative measure to monitor and sense. In WSN, it may fail to fulfil the monitoring needs as of various reasons, like disconnection of network or termination of sensor nodes. Thus, it is essential to maximize the energy for prolonging the Lifetime of network. Assume D sensor nodes d_1, d_2, d_D are deployed in WSN in an Arbitrary manner to cover G targets g_1, g_2, g_G. Each sensor node contains an initial energy □ and attains the capacity to regulate itself for transmitting data. The range of sensing is l_1, l_2, lq based on energy consumption m_1, m_2, m_q. In addition, the BS is located in communication range of each sensor. Here, the goal is to arrange set of sensors such that it is liable to sense targets.

Cluster head selection using LEACH protocol

Clustering is an effectual process for meeting the energy crisis faced by WSN due to the battery-operated sensor nodes. The issues of energy are solved by CH selection using LEACH algorithm. Using LEACH, the clustering of nodes is done in such a way that CH is selected via efficient sensor nodes. For cluster head selection, LEACH algorithm is devised wherein the sensor nodes are arranged in clusters according to the similarities instead of hard- partitioning them in one cluster. The LEACH protocol [1][2] adapts an intense sensor network that contains nodes with equal energy, and goal is to transmit data to BS. Hence, an optimum CH is selected for accumulating and transmitting data to BS. Here, the sink node is positioned in a distant place, and hence CH needs more energy for attaining communication amongst the nodes. Hence, LEACH protocol helps to choose best CH such that selected node contains high energy. Thus, the LEACH protocol utilizes arbitrary CH rotations for consistently splitting energy throughout sensor nodes. Moreover, the LEACH is organized in a discovered using size wt, where w symbolize total nodes in t rounds. Here, the set up phase comprises three sub-phases, which involves advertisement, setup of cluster, and scheduling broadcast. In advertisement phase, each node w generates an arbitrary number and compute using specific threshold. The threshold is expressed as,

$$\tau(w) = \begin{cases} \dfrac{t}{1 - t \times (c \bmod \frac{1}{t})} & ;if \quad e \in \alpha \\ 0 & ;Otherwise \end{cases} \tag{1}$$

where, □ symbolize node, which is not CH, t express CH percentage, and c signifies update period of recent topology. Hence, nodes, which made a choice to a CH notify its adjoining nodes using advertisement packet. In setup of cluster, all nodes contained in network reply CH advertisement to notify its decisions. In broadcast phase, the replies of all the nodes are accumulated to make decision regarding the membership of specific cluster. Thus, the CH produces a TDMA schedule using total nodes present in cluster. This schedule smack a harmony amongst node regarding the time for broadcasting message in particular time. At last, for data transmission, the data are accumulated in CH, and then the generated data is fed to base station. Thus, the CH selected by LEACH is expressed as,

$$K = \{K_1, K_2, \square, K_g, \square, K_o\} \qquad ;1 \le g \le o \tag{2}$$

where, o symbolize total CH.

Routing using FABC

Here, the routing is done amongst the cluster heads K obtained from clustering phase. The routing is essential in WSN as it assists to send data between the sensor nodes and the BS. The routing is required for transmitting data between the nodes and the BS to **establish** communication. Here, FABC [3] algorithm is employed for initiating routing to transfer the collected data to the BS. The FABC is designed by incorporating FC in ABC algorithm. FC [5] is termed as an expansion of classical mathematics and is adapted for evaluating the best solutions from previous iterations and is interpreted to update the solutions in the current iteration. Meanwhile, ABC [4] is an evolutionary technique devised by the motivation of intellectual foraging behaviour. Thus, the incorporation of FC and ABC is done to enhance solution search space. Thus, the FABC assists to solve exploration and exploitation issues and provide improved usage of global information. The algorithmic steps of FABC algorithm for routing are illustrated below:

Step 1: Initialization

Consider Q_R be a food source initialized in a random manner and the food source size is assumed as Q_R [illegible] g.
The values of integer are filled in the matrices in a random manner ranging between 1 to p . Here, the sensor nodes are deployed in the network and the energy is initialized to all nodes. The location information of each node is known to the sink node for performing routing.

Step 2:. Employed bee

In FABC, the food sources are encoded, and each attribute of the food source is represented as the index of sensor node and the length of the food source is assumed to be the count of CH in the IOT. The food source of the bee are updated and the production of new bee phaseis done based on ABC [4] using the equation given as,

$$Q_{u,v}^{s+1} = Q_{u,v}^{s} + A_{u,v}\left(Q_{u,v}^{s} - Q_{l,v}\right) \tag{3}$$

where, Q^{u}_{v} represents u^{th} food source of v^{th} value in s^{th} iteration, $A_{u,v}$ indicates the random value in [-1,1], $u \in \{1,2,\ldots,g\}$ and l indicates the index of neighbour in such a way that $l \in \{1,2,\ldots,Q_R\}$.

After rearranging the original food source for enhancing the solution derivative order, the obtained equation is expressed as,

$$Q^{s+1}_{u,v} - Q^{s}_{u,v} = A_{u,v}(Q^{s}_{u,v} - Q_{l,v}) \tag{4}$$

Here, $Q^{s+1}_{u,v}$ represents the discrete version of derivative with order $\alpha_Q = 1$ is represented as,

$$D^{\alpha_Q}[Q^{s+1}_{u,v}] = A_{u,v}(Q^{s}_{u,v} - Q_{l,v}) \tag{5}$$

The order of food source is modelled in a real number, if the FC [5] perception is adapted, that results in the smooth variation and long memory effects. Thus, the aforementioned equation is obtained by assuming two terms of differential derivatives and is formulated as,

$$Q^{s+1}_{u,v} - \alpha_Q Q^{s}_{u,v} - \frac{1}{2}\alpha_Q Q^{s-1}_{u,v} = A_{u,v}(Q^{s}_{u,v} - Q_{l,v}) \tag{6}$$

$$Q^{s+1}_{u,v} = \alpha_Q Q^{s}_{u,v} + \frac{1}{2}\alpha_Q Q^{s-1}_{u,v} + A_{u,v}(Q^{s}_{u,v} - Q_{l,v}) \tag{7}$$

$$Q^{s+1}_{u,v} = \left|\alpha_Q Q^{s}_{u,v} + \frac{1}{2}\alpha_Q Q^{s-1}_{u,v} + A_{u,v}(Q^{s}_{u,v} - Q_{l,v})\right| \tag{8}$$

After the generation of a new food source, the optimization models the bound constraints forcapturing the value of solution in specific integer interval.

Step 3: Evaluation of fitness function

The obtained food source is analyzed with the fitness function. If the fitness of updated food source $Q^{s+1}_{u,v}$ is less than the old food source $Q^{s}_{u,v}$ then, the solution is updated with the old best solution $Q^{s}_{u,v}$ or otherwise, the solution is based on the new food source $Q^{s+1}_{u,v}$.

Step 4: Onlooker bee

The food sources of the second half of the population are updated with onlooker bee phasewherein the food source is chosen using the equation represented as,

$$y_u = \omega_1 \times \frac{fit_u}{\underset{u=1}{\overset{Q}{Max}}\, fit_u} + \omega_2 \tag{9}$$

where, ω_1 and ω_2 indicate constant and fit_u represent the fitness function employed for selecting the best path. The chosen food source is replaced with new solution $Q^{s+1}_{u,v}$. The bee searches for the new food source if fitness of $Q^{s+1}_{u,v} < Q^{s}_{u,v}$, otherwise remains same.

The fitness of FABC algorithm is formed considering three attributes, distance, energy and delay. When selecting a path, the distance should be less, energy of nodes present in the path should be high, and delay must be less. Thus, these design constraints are employed for path selection. Thus, the goal is to reduce the objective function which is represented as,

$$fit_u = \eta_1 h_u^{loc} + \eta_2 h_u^{energy} + \eta_3 h_u^{delay} \tag{10}$$

where, η_1, η_2 and η_3 represent weighted constants, and h_u^{loc} indicates the distance of cluster member to CH. Similarly, h_u^{energy} indicates the energy of the nodes present in a path and h_u^{delay} is the delay incurred in the transmission.

Step 5: Scout bee

These phases are implemented if no food sources are altered for the past Z cycles. Here, the chosen food source is discarded and updated with a randomly produced new food source.

Step 6: Termination

The aforementioned steps are repeatedly executed till s reaches utmost cycles Z_{max}. The best food source is solution output. After determination of shortest paths, the communication between the CH and the BS is performed for exchanging information of sensor nodes.

Attack detection using proposed ECMVRO-DRN

At BS, the attack detection is done. Here, DRN [6] is adapted for making effective decision wherein the decision regarding attacker or genuine user is done. The DRN consist of different layers, namely residual blocks, convolutional (conv) layers, linear classifier and average pooling layers. Figure 4 depicts the architecture of deep residual network.

-Convolutional (conv) layer:

The conv layer processes the input data with the series of filter termed as kernel considering local connection. The computation process of conv layer is expressed as,

$$B2d(M) = \sum_{a=0}^{E-1}\sum_{s=0}^{E-1} X_{a,s} \bullet M_{(u+a),(v+s)} \tag{11}$$

$$B1d(M) = \sum_{Z=0}^{Cin-1} G_Z * M \tag{12}$$

where, M denote CNN feature of input image, u and v are used for recoding coordinates, G symbolize $E \times E$ kernel matrix and is also known as learnable parameter, and a and s denote position index of kernel matrix. Thus, G_Z symbolize size of kernel for Z^{th} input neuron, and $*$ denote cross correlation operator.

-Pooling layer: The average pooling is selected to function on each slice and depth of featuremap.

$$a_{out} = \frac{a_{in} - Z_a}{\lambda} + 1 \tag{13}$$

-Pooling layer: The average pooling is selected to function on each slice and depth of featuremap.

$$a_{out} = \frac{a_{in} - Z_a}{\lambda} + 1 \tag{13}$$

$$s_{out} = \frac{s_{in} - Z_s}{\lambda} + 1 \tag{14}$$

where, a_{in} signifies input matrix width, s_{in} symbolize height of input matrix, a_{out} and s_{out} are those respective output value. Moreover, Z_a and Z_s signifies width and height of kernel size.

-Activation function: The non-linear activation function is employed for learning non-linear and complex features such that it is used to enhance non-linearity of mined features. The ReLU function is modelled as,

$$\operatorname{Re}LU(M) = \begin{cases} 0 \ ; & \mathrm{K} < 0 \\ \mathrm{K} \ ; & \mathrm{K} \geq 0 \end{cases} \tag{15}$$

Here, K signifies feature.

-Batch normalization: Here, the input layers are normalized by altering and scaling theactivations to increase the reliability and speed of training.

-Residual blocks: For different size, the dimension matching factor is employed for matchinginput with the output.

$$O = \Re(M) + M \tag{16}$$

$$O = \Re(M) + \square_M M \tag{17}$$

Here, M and O symbolize input and output residual blocks, O signifies mapping relationship, and $\square_H$ denote dimension matching factor.

-Linear classifier: After the completion of conv layer, linear classifier carries the process to determine noisy pixels from input image. It is integration of softmax function and fully connected layer.

$$O = \square O + \upsilon \tag{18}$$

Here, $\square$ denote weight matrix, and υ indicate bias. Figure 2 present structural design of DRN. Here, the output of DRN is expressed as O which helps in determining whether the user is attack or normal user.

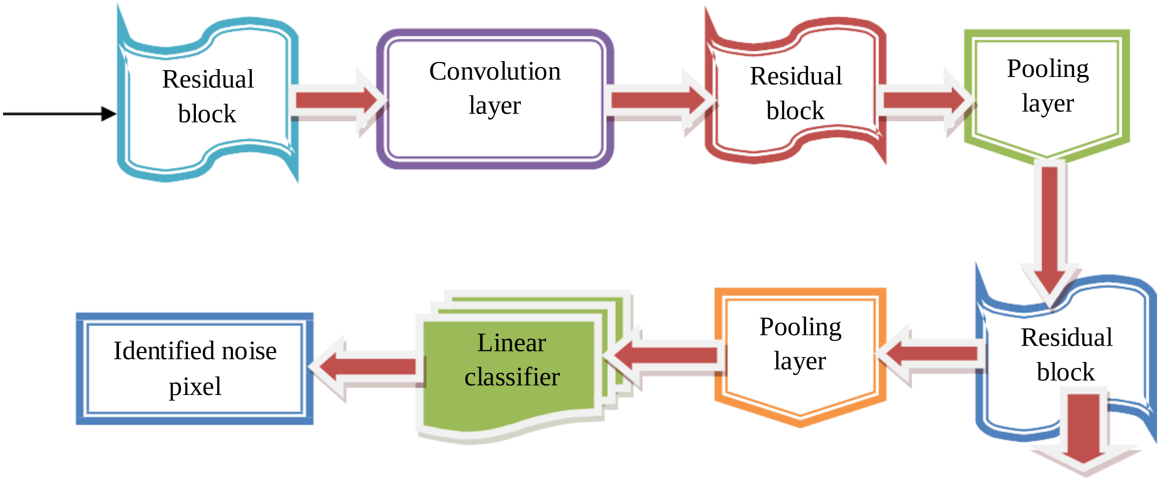

Figure 2. Architecture of deep residual network

4.2.2. Training of Deep residual network

The deep residual network training is carried out using proposed technique namely ECMVRO algorithm. Here, the classifier weight is trained with proposed ECMVRO for generating optimum solution. ECMVRO enhance deep residual network by integrating CMVO [8] and ROA [7] to choose optimum weights for acquiring effectual training of internal model parameters of classifier. The steps of ECMVRO algorithm is given below.

Step 1. Initialization

The first step is solution initialization wherein the solutions and other attributes such as iteration count c are initialized. The solutions are expressed as,

$$G = \{G_1, G_2, \ldots, G_s, \ldots, G_t\} \tag{19}$$

where, t signifies total solutions, G_s signifies s^{th} solution.

Step 2. Computation of error

The best solution is discovered using error function, and is considered as minimization issue, and hence solution producing least Mean Square Error (MSE) is chosen as best solution. Thus, MSE is computed as,

$$MS_{err} = \frac{1}{g}\sum_{h=1}^{g}[\xi_h - O]^2 \tag{20}$$

where, ξ_h symbolize expected output and O express output generated from the combination of DRN and NN classifier, g refers count of data samples, such that $1 < h \leq g$.

Step 3. Discovering update position of riders

The position of rider in each set is updated to discover the leader. Hence, the update position of rider using unique feature of each rider is described below. The update position of each rider is given below.

a) Position update based on bypass rider

As per ROA [7], the bypass riders pose a recognizable path and its update position is expressed as,

$$L_{n+1}^{B}(w,u) = \alpha[L_n(\beta, u) * \eta(u) + L_n(\rho, u) * [1-\eta(u)] \tag{21}$$

where, α symbolize random number, β signifies arbitrary number amongst 1 to P, ρ denotea arbitrary number in 1 to P and η express arbitrary number between 0 and 1.

Assume $\beta = w$

$$L_{n+1}^{B}(w,u) = \alpha[L_n(w,u) * \eta(u) + L_n(\rho, u) * [1-\eta(u)] \tag{22}$$

$$L_{n+1}^{B}(w,u) = \alpha L_n(w,u) * \eta(u) + \alpha L_n(\rho, u) * [1-\eta(u)] \tag{23}$$

The CMVO is effective in increasing the computational efficiency and speed of convergencerate. From CMVO [8], the update equation is given as,

$$L_{n+1}^{B}(w,u) = o_1 * TDR + o_2 * (L_n(s,u) - L_n(w,u)) + o_3 * (L_u - L_n(w,u)) \tag{24}$$

Where, $L_n(s,u)$ refers winner universe in the u^{th} round of competition, $L_n(w,u)$ signifies loser universe in the u^{th} round of competition, L_u symbolize mean position value of relevant universe, TDR is coefficient and o_1, o_2 andThe o_3 signifies random numbers between [0, 1].

TDR is given as,

$$TDR = 1 - \left(\frac{n^{1/\square}}{\quad}\right) \tag{25}$$

Where, □ = 6, current iteration is denoted as n, and maximum iteration is expressed as N.

$$L^B_{n+1}(w,u) = o_1 * TDR + o_2 * L_n(s,u) - o_2 * L_n(w,u) + o_3 * L_u - o_3 * L_n(w,u) \tag{26}$$

$$L^B_{n+1}(w,u) = o_1 * TDR + o_2 * L_n(s,u) + o_3 * L_u - L_n(w,u)(o_2 + o_3) \tag{27}$$

$$L_n(w,u)(o_2 + o_3) = o_1 * TDR + o_2 * L_n(s,u) + o_3 * L_u - L^B_{n+1}(w,u) \tag{28}$$

$$L_n(w,u) = \frac{o_1 * TDR + o_2 * L_n(s,u) + o_3 * L_u - L^B_{n+1}(w,u)}{o_2 + o_3} \tag{29}$$

Substitute equation (24) in equation (19),

$$L^B_{n+1}(w,u) = \alpha\left(\frac{o_1 * TDR + o_2 * L_n(s,u) + o_3 * L_u - L^B_{n+1}(w,u)}{o_2 + o_3}\right) * \eta(u) + \alpha L_n(\rho, u) * [1-\eta(u)] \tag{30}$$

$$L^B_{n+1}(w,u) = \frac{\alpha o_1 * TDR + o_2 * L_n(s,u) + o_3 * L_u}{o_2 + o_3} * \eta(u) - \frac{L^B_{n+1}(w,u)}{o_2 + o_3} * \alpha * \eta(u) + \alpha L_n(\rho, u) * [1-\eta(u)] \tag{31}$$

$$L^B_{n+1}(w,u) + \frac{L^B_{n+1}(w,u)}{o_2 + o_3} * \alpha * \eta(u) = \frac{\alpha o_1 * TDR + o_2 * L_n(s,u) + o_3 * L_u}{o_2 + o_3} * \eta(u) + \alpha L_n(\rho, u) * [1-\eta(u)] \tag{32}$$

$$L^B_{n+1}(w,u)\left(1 + \frac{\alpha * \eta(u)}{o_2 + o_3}\right) = \frac{\alpha o_1 * TDR + o_2 * L_n(s,u) + o_3 * L_u}{o_2 + o_3} * \eta(u) + \alpha L_n(\rho, u) * [1-\eta(u)] \tag{33}$$

$$L^B_{n+1}(w,u)\left(\frac{o_2 + o_3 + \alpha * \eta(u)}{o_2 + o_3}\right) = \frac{\alpha o_1 * TDR + o_2 * L_n(s,u) + o_3 * L_u}{o_2 + o_3} * \eta(u) + \alpha L_n(\rho, u) * [1-\eta(u)] \tag{34}$$

The final update equation of proposed CMVRO is given as,

$$L^B_{n+1}(w,u) = \frac{o_2 + o_3}{o_2 + o_3 + \alpha * \eta(u)}\left[\frac{o_1 * TDR + o_2 * L_n(s,u) + o_3 * L_u}{o_2 + o_3} * \eta(u) + \alpha L_n(\rho, u) * [1-\eta(u)]\right] \tag{35}$$

Step 5) Riding Off time:

The steps are iterated repeatedly till time attains off time N_{OFF}, in which attacker is determined. The pseudo code of developed CMVRO is illustrated in table 1.

Attack mitigation with data rates

If the output O is attacker, then mitigation of attack is done. A detection and preservation strategy is utilized for safeguarding network, application and server by IT admin for reducing the impact of suspicious traffic and attack while handling the functionality for users. Data rate is reduced when the attacker is detected. For provided time interval Δt, let $L(\Delta t)$ indicate number of packets, l_k indicate packet size of k^{th} packet and l_{max} represent maximal packet size. The mean of packet size is expressed as,

$$\vec{l} = \frac{1}{c}\sum_{k=1}^{c} l_k ; 60 \le \vec{l} \le l_{max} \tag{36}$$

If $\vec{l}$ of a user is beyond the limit, then reduce the data rate to 50%.

Flow chart of the proposed Sybil attack detection model

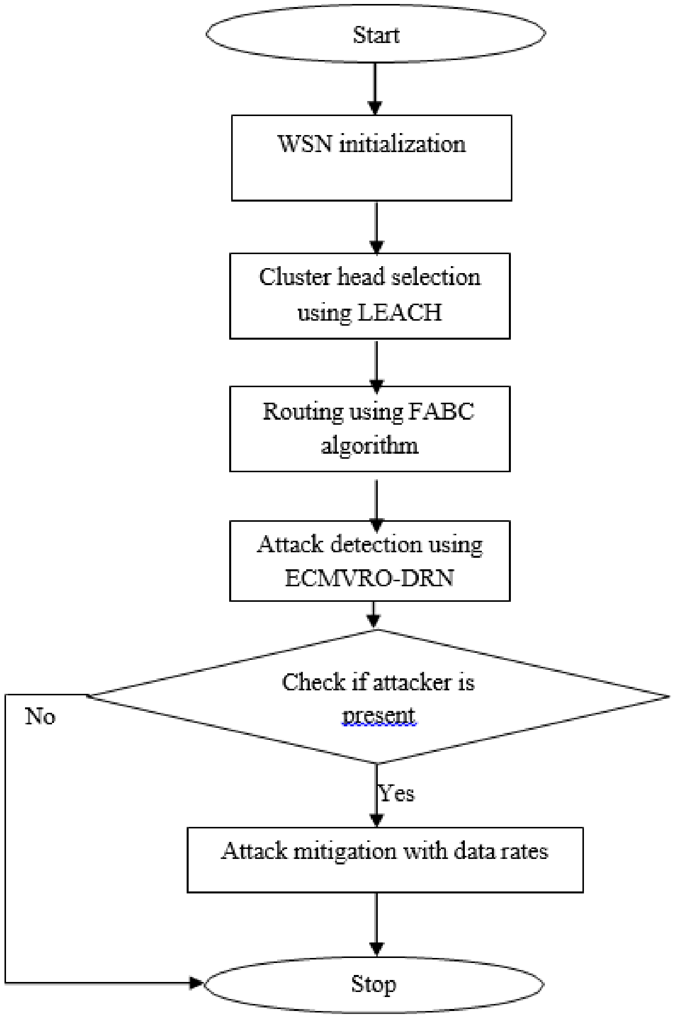

Figure 3. Flow chart of proposed Sybil attack detection and mitigation model in WSN

3. Experimental results

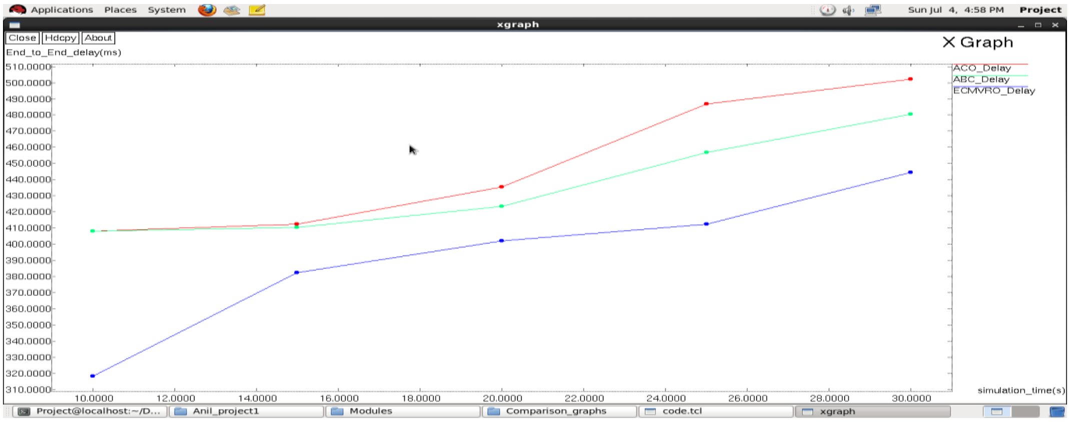

Figure 4. Assessment of techniques with delay

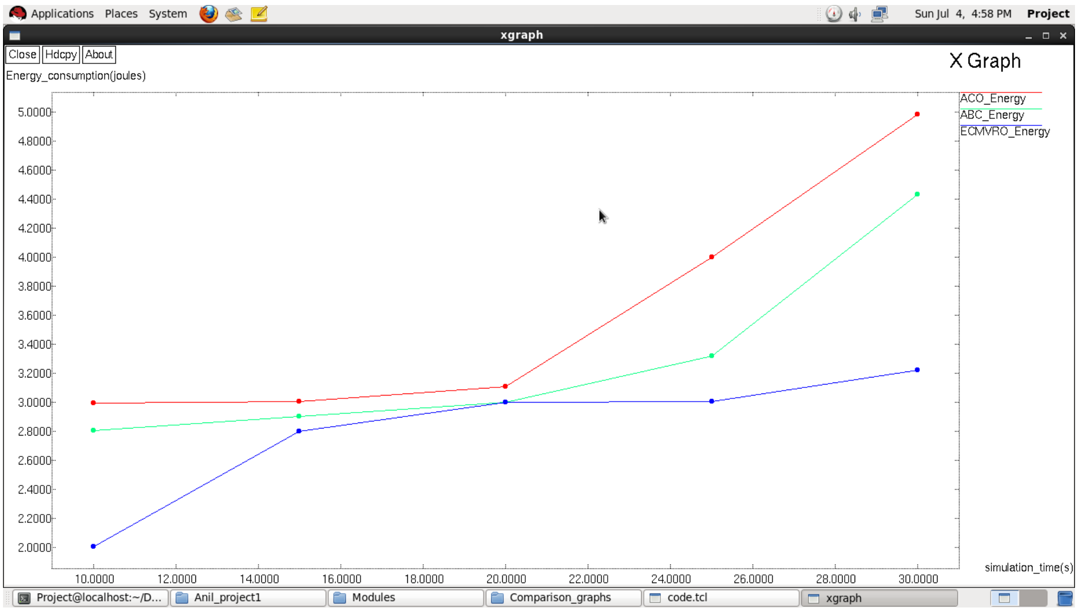

Figure 5. Assessment of techniques with energy

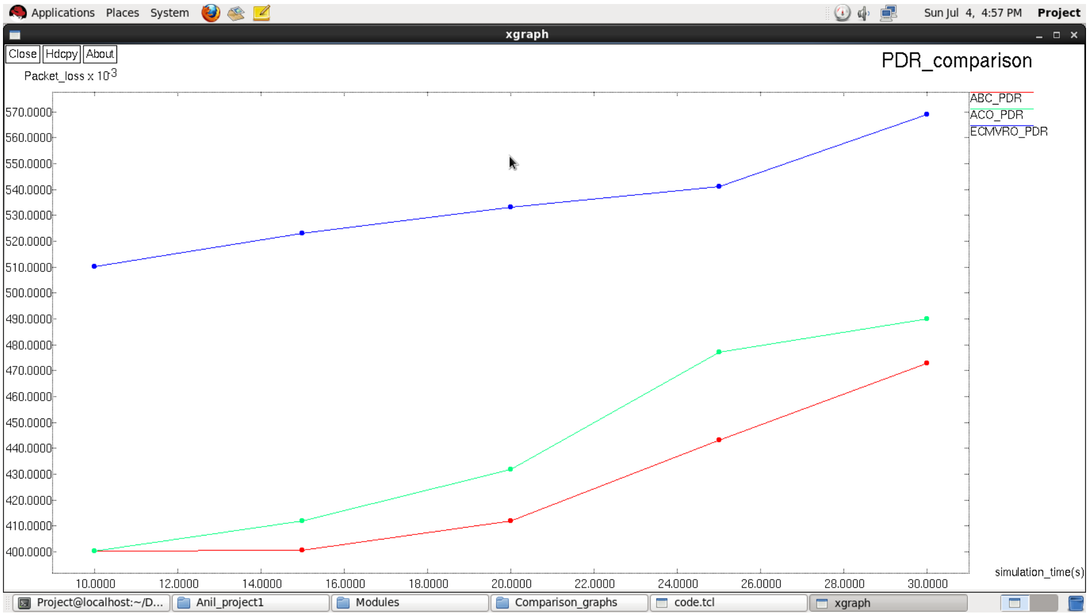

Figure 6. Assessment of techniques with PDR

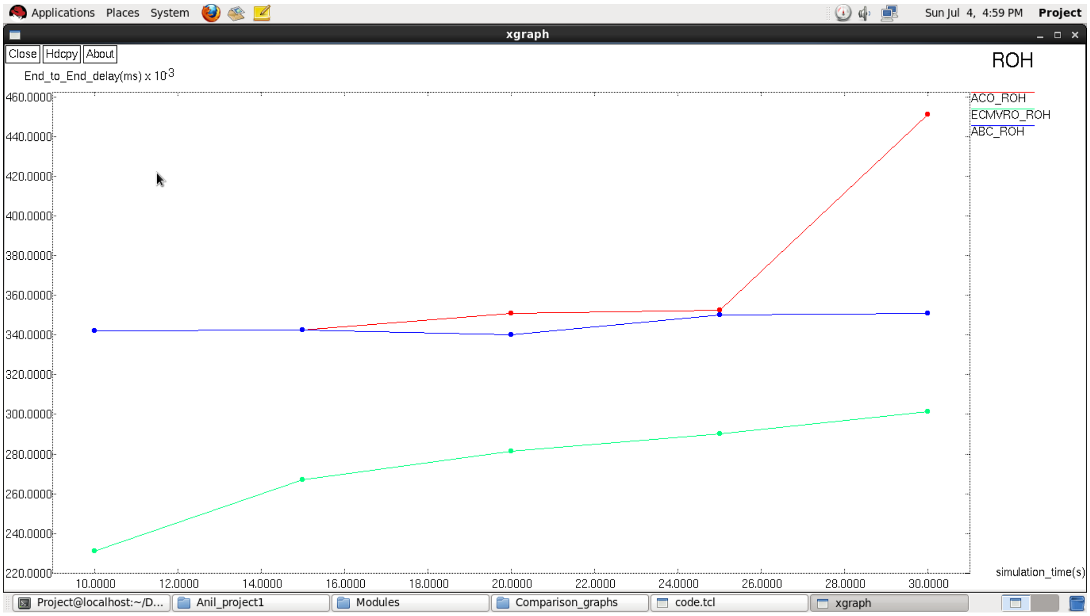

Figure 7. Assessment of techniques with ROH

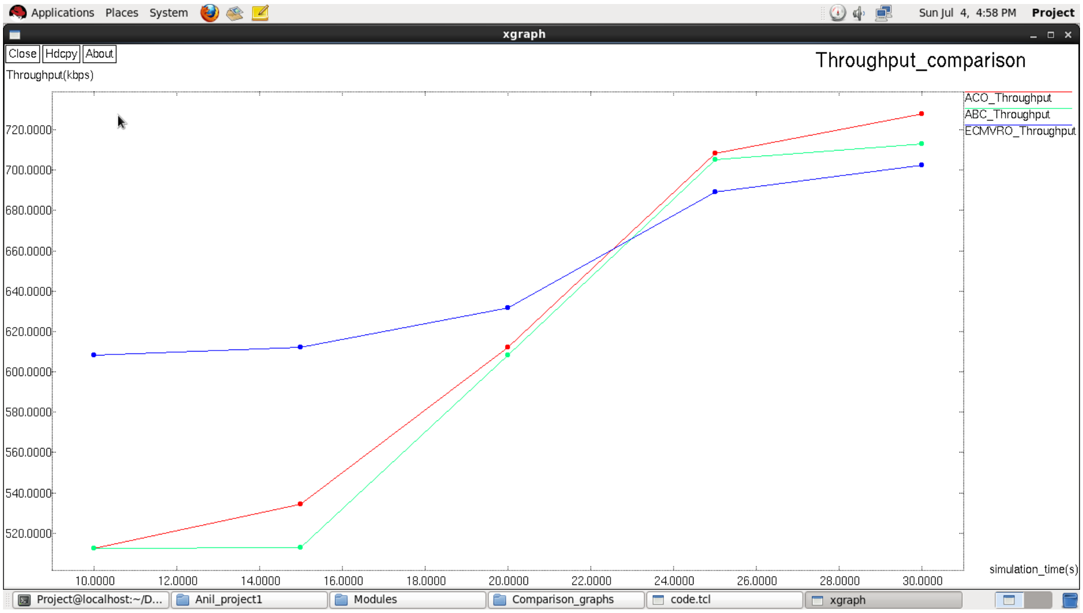

Figure 8. Assessment of techniques with throughput

4. Conclusion

An energy efficient optimization aware deep model is developed for Sybil attack detection and mitigation in WSN. Here, the preliminary step is the simulation of WSN nodes. The complete process of the proposed model includes simulation of WSN, cluster head selection, routing to BS, Sybil attack detection in BS and finally attack mitigation in BS. The first step is WSN simulation and then the selection of energy efficient cluster head is done using Lower Energy Adaptive Clustering Hierarchy (LEACH) protocol. Then, the routing of the accumulated data is done using Fractional artificial bee colony (FABC) algorithm. Once the data is accumulated at BS, the attack detection and attack mitigation is performed using the accumulated data. From data, the imperative feature is selected using Jaro-Winkler distance. After determining the optimum features, the Sybil attack detection is performed with Deep residual network (DRN). The training of DRN using proposed Competitive Multi-Verse Rider Optimizer (CMVRO), which is devised by combining Competitive Multi-Verse Optimizer (CMVO) and Rider Optimization Algorithm (ROA). The mitigation of Sybil attack is performed using data rates. Here, the data rate is reduced when the attacker is detected.

References

[1] M. Masdari, S. M. Bazarchi, and M. Bidaki, "Analysis of Secure LEACH-Based Clustering Protocols in Wireless Sensor Networks," J. Netw.Comput.Appl., vol. 36, no. 4, pp. 1243–1260, 2013.

[2] Mohapatra H, Rath AK., "Fault tolerance in WSN through PE-LEACH protocol", IETwireless sensor systems, vol.9, no.6, pp.358-65, July 2019.

[3] Rajeev Kumar & Dilip Kumar , " Multi-objective fractional artificial bee colony algorithm to energy aware routing protocol in wireless sensor network", Wireless Networks, vol.22, pp.1461–1474, 2016.

[4] Karaboga, D., Okdem, S., & Ozturk, C, "Cluster based wireless sensor network routing using artificial bee colony algorithm," Wireless Network, vol.18, pp.847–860, 2012.

[5] Pires, E. J. S., Machado, J. A. T., Oliveira, P. B. M., Cunha, J. B., & Mendes, L, "Particle swarm optimization with fractional-order velocity," Nonlinear Dynamics, vol.61, pp.295– 301, 2010.

[6] Chen, Z., Chen, Y., Wu, L., Cheng, S. and Lin, P., "DRN based fault detection and diagnosis of photovoltaic arrays using current-voltage curves and ambient conditions," Energy Conversion and Management, vol.198, p.111793, 2019.

[7] Binu, D. and Kariyappa, B.S., "RideNN: A new rider optimization algorithm-based neural network for fault diagnosis in analog circuits", IEEE Transactions on Instrumentation and Measurement, vol.68, no.1, pp.2-26, 2018

[8] Benmessahel, I., Xie, K. and Chellal, M., "A new competitive multiverse optimization technique for solving single-objective and multiobjective problems", Engineering Reports, vol.2, no.3, pp.e12124, 2020.

[9] Suwija, N., Suarta, M., Suparsa, N., Alit Geria, A.A.G., Suryasa, W. (2019). Balinese speech system towards speaker social behavior. *Humanities & Social Sciences Reviews, 7*(5), 32-40. https://doi.org/10.18510/hssr.2019.754

[10] Widana, I.K., Dewi, G.A.O.C., Suryasa, W. (2020). Ergonomics approach to improve student concentration on learning process of professional ethics. *Journal of Advanced Research in Dynamical and Control Systems*, *12*(7), 429-445.

[11] Widana, I.K., Sumetri, N.W., Sutapa, I.K., Suryasa, W. (2021). Anthropometric measures for better cardiovascular and musculoskeletal health. *Computer Applications in Engineering Education*, *29*(3), 550–561. https://doi.org/10.1002/cae.22202