International Journal of Bio-Inspired Computation

ISSN online: 1758-0374 - ISSN print: 1758-0366
https://www.inderscience.com/ijbic

Intrusion detection via optimal tuned LSTM model with trust and risk level evaluation

Ranjeet B. Kagade, N. Vijayaraj

DOI: 10.1504/IJBIC.2023.10060572

Article History:

Received:	03 October 2022
Last revised:	17 August 2023
Accepted:	26 August 2023
Published online:	22 January 2024

Intrusion detection via optimal tuned LSTM model with trust and risk level evaluation

Ranjeet B. Kagade* and N. Vijayaraj

Department of Computer Science and Engineering,
VelTech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Chennai, Tamilnadu-600 062, India
Email: ranjeetbharat4@gmail.com
Email: vijaiphdraj@gmail.com
*Corresponding author

Abstract: Different heterogeneous wireless sensor networks (WSNs) linked with the cloud platform make up a sensor cloud framework. The optimal cluster head (CH) is chosen from among the SNs in this work's introduction of the IDS model, in which the SNs with the highest energy are given priority as the CH. In particular, the energy, latency, QoS, inter-cluster distance, and intra-cluster distance are taken into account when choosing the CH. Additionally, the suggested self updated CA optimisation (SU-COA) aids in the choosing. An improved LSTM model identifies the existence of intrusions in the network. By adjusting the model's ideal weights using the SU-COA algorithm, the detection portion is improved. For the maximum case, a less error of 1.068 is gained using LSTM+ SU-COA, while CMBO, PRO, CSO, GWO, and CA have acquired comparatively high errors of 1.097881, 1.082925, 1.090536, 1.087563 and 1.06696 for the maximum case.

Keywords: wireless sensor network; WSN; cluster head; intra-cluster distance; trust and risk; SU-COA algorithm.

Reference to this paper should be made as follows: Kagade, R.B. and Vijayaraj, N. (2024) 'Intrusion detection via optimal tuned LSTM model with trust and risk level evaluation', *Int. J. Bio-Inspired Computation*, Vol. 23, No. 1, pp.39–52.

Biographical notes: Ranjeet B. Kagade obtained his BE in Computer Science and Engineering from Solapur University, Solapur, Maharashtra and ME in Computer Network from Savitribhai Phule Pune University, Pune in 2010 and 2014, respectively. He is currently a research scholar in the Department of Computer Science and Engineering, Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology (Deemed to be University) Avadi, Chennai, Tamilnadu, India. He is a member of IEI and IEEE. He has over 13 years of experience in technical education and in the areas of teaching and IT industry. His research interests are in the area of trust management, wireless sensor network, mobile computing, machine learning and network security.

N. Vijayaraj is currently working as an Associate Professor in the Department Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu-600 062, India. He obtained his UG in Roever Engineering College, Perambalur and PG degrees in Jayaram College of Engineering and Technology, Trichy. He received his PhD degree from Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu-600 062, India in 2020. He has been in the teaching profession for the past 14 years and handled various courses for both UG and PG programs. He is guiding 'five' research scholar. He has more than '14' publications in national and international journals. He has also published three book chapters. He is a life member of various bodies such as ISTE and IAENG.

1 Introduction

The market for inexpensive wireless sensor network (WSN) solutions to deploy and have low node costs will steadily grow. WSN products are capable of evading conventional identification techniques. They significantly cut the labour-intensive procedure of using conventional testing methods and the costs associated with environmental testing. The WSN is a novel network deployed in industry and is being extensively researched by scientists (Gope et al., 2017; Anand and Gnanamurthy, 2016; Nirmal Raja and Marsaline Beno, 2014).

WSN nodes have several difficulties when dealing with complicated situations, including:

1 the relatively low computational and storage capabilities of a single node

2 poor inter-node connection

3 the SN is situated in a challenging physical environment

4 certain mobile nodes could make the network structure unpredictable and dynamic (Fan et al., 2011; Son et al., 2013).

The optimisation technique can be used for multidimensional space solutions (Naruei and Keynia, 2021; Safaldin et al., 2020; Jadhav and Gomathi, 2019). As a result, the safety of WSN sensors is generally poor, network attacks against them are simpler, and their security issues are worsening. The second pathway for network security is intrusion detection. An intrusion detection system (IDS) can prevent unauthorised users from attacking the network while also bolstering the system's defences against known threats (Vijayakumar et al., 2018; Gill et al., 2012; He et al., 2012; Kagade and Satao, 2013, 2014; Kagade and Santhosh, 2021; Balamurugan and Kagade, 2020.

We may categorise IDS into three groups based on their data sources (Shamshirband et al., 2014):

1 Host-based IDS that exclude network data from involvement and solely use the data from the system's intrusion detection library to determine whether the information is abnormal. IDS was used to provide security in WSN. It recognises the intruder with the help of a single sensor or multi-sensor (Umarani and Kannan, 2020; Tapiador and Clark, 2013; Soliman et al., 2012). There are many devices that we use for daily tasks that are both connected to the internet and to each other. Low-cost sensor nodes are created to carry out data collecting, data transfer, and remote monitoring as the internet of things (IoT) based WSNs expand quickly (Muzammal et al., 2020; Shafiq et al., 2021). This approach consumes a significant amount of CPU power, making it unsuitable for using tiny distributed devices.

2 Network-based IDS may collect actual network packets of data and build an associated anti-malware library to conduct pattern matching, frequency analysis, and judgement on the packets of data. However, this approach entails exorbitant prices for the database update (Borkar et al., 2019; Selvakumar et al., 2019; Sedjelmaci et al., 2017).

3 Decentralised IDS, in which the systems can fully take into account the two intrusion above detection methods, i.e., it can both detect network data and host operating data (Zha and Li, 2018; Baykara and Das, 2018).

The primary goal of an IDS is to detect harmful attacks in advance, before they may access data or compromise the confidentiality of crucial systems. The need for security systems to protect against both known and unidentified threats presents a challenge for the scientific community and the industry to develop reliable and secure systems against cyberattacks. This raises the question of how to successfully protect against known and unexpected threats. Due to the escalating amount of threats each year, there is no simple solution to this. Recently, AI-based technologies have become increasingly important in learning from historical data gathered from prior attacks, including machine learning and deep learning. The knowledge gained from the proposed models is utilised to increase IDS's level of confidence.

The contributions are as follows:

- Using the SU-COA method, optimal CHS is performed while taking various limitations into account.
- Using an improved LSTM model, a novel trust and risk evaluation technique is used to assess the performance of the chosen cluster head (CH) and nodes.
- By adjusting the optimal LSTM weights using the suggested SU-COA algorithm, it improved the detection accuracy.

Here, Section 2 analyses traditional works on IDS. Section 3 describes a novel IDS system. Sections 4 and 5 depict the objectives and parameters considered for CHS. Sections 6 and 7 depict the optimised LSTM and SU-COA algorithms. The results and conclusion are described in Section 8 and Section 9.

2 Literature review

2.1 Related works

Safaldin et al. (2021) suggested an improved IDS in 2021 by combining GWOSVM-IDS. The GWOSVM-IDS utilised 3, 5, and 7 wolves to determine the ideal number of wolves. The suggested approach intends to minimise process time in WSN by decreasing false alarm rates, the number of features produced by IDSs within the WSN environment, and IDS accuracy and detection rate. The findings demonstrated that the seven-wolf GWOSVM-IDS suggested it outperformed all other proposed and comparison algorithms.

To meet QoS metrics like energy, longevity, and security in 2021, Maheswari and Karthika (2021) created a unique safe cluster-based method with an intrusion detection approach. Using an adaptive neural fuzzy-based clustering approach, the TCHs are first chosen by the proposed model utilising three input parameters, including remaining energy, proximity to BS, and proximity to neighbours. The DHO method picks the best CHs after the TCHs compete for the final CHs. The cluster maintaining stage is used for load balancing to increase the performance of the recommended technique.

Using a unique F-CSO and OLSR protocol in 2021, Qureshi and Shandilya (2021) effectively delivered safe data transfer from the sender to the receiver using a trust-based channel. The best nodes are considered throughout the optimisation process and must meet the three requirements of shorter data transmission distances between nodes, higher transmission degrees, and higher transmission energies. The OLSR method can also be used to implement routing.

Zhang et al. (2021) developed an intrusion detection model in 2021 based on SVM, PCA, and TVP-IPSO. By condensing the information to save energy, the PCA is used to lower the size of the data set. An SVM-based intrusion detection method is also considered to guarantee high accuracy. The TVP-IPSO is employed to enhance the detection accuracy and convergence speed of IDS and improve the SVM classifier and discover its optimal parameters.

In 2020, Sinha and Paul created a robust and effective AIDS that uses methods based on NN and fuzzy logic. The suggested system was executed in each node since it is small and overhead-light. Additionally, it can autonomously observe local node behaviour and determine if a node is friendly, hostile, or neutral. The system's accuracy is improved by using a trained NN to filter out false alarms caused by the fuzzy logic used in the first stage.

HADS, also known as artificial immune systems in WSNs, was suggested by Umarani and Kannan in 2020. The HTGA is used in this framework to construct a unique intrusion detection algorithm for detecting the presence of abnormalities in cells and effectively sending data packets. This method is made in two distinct advancements, the NTG model and the STG algorithm. The suggested HADS technique's simulation results outperform current techniques in terms of performance.

In their study effort from 2020, Thangaramya et al. created a novel secured communication model based on fuzzy temporal clustering that includes trust analysis and outlier identification. A novel fuzzy temporal rule-based cluster-based routing method with trust modelling and outlier identification has been presented to monitor the nodes taking part in the communication. In addition, a fuzzy technique is also described in this research. It has been incorporated into the secured routing algorithm to help identify the hostile nodes from other nodes inside each network cluster.

In 2020, Abhale and Manivannan built intrusion detection using supervised classification models such as random forest classifier, support vector machine, decision tree classifier, LGBM classifier, extra tree classifier, gradient boosting classifier, Ada boost classifier, K nearest neighbour classifier, MLP classifier, Gaussian naive Bayes classifier and logistic regression classifier. The NSLKDD data set is used for checking these algorithms. Investigational resultants showed the maximum accuracy compared to other categorisation systems in SVM.

In 2022, Ramana et al. has deployed the novel whale optimised gate recurrent unit (WOGRU) IDS for WSN-IoT networks is proposed in this research. To achieve low computational overhead and excellent performance, the deep long short-term memory's hyperparameters were tuned using the whale algorithm in the suggested framework. Last but not least, validations are performed using the WSN-DS dataset, and the performance of the proposed work is assessed using the metrics accuracy, recall, precision, specificity, and F1-score.

In 2023, Gokul Pran and Raja have combining a hybrid genetic algorithm and the particle swarm optimisation approach (GPSO), the feature selection is carried out. The data is categorised as BENIGN, DOS Hulk, PortScan, DDoS, and DoS Golden Eye using the selected features input into an adaptive artificial neural network (AANN). Finally, the oppositional crow search algorithm (OCSA) is used to control the hyper parameter of the AANN to improve the classification of network intrusions.

2.2 Problem statement

Strategies for intrusion reaction and repair have not been extensively studied. Evicting individual infected nodes, isolating affected segments (microgrid or greater scope), and modifying detection intensity are possible intrusion countermeasures. For instance, the IDS can function more effectively if it modifies the detection accuracy depending on the kind and power of the attacker it encounters. Possible repair methods include locating the compromised segments, stopping all operations for each one, rolling back all nodes to approved software configurations and loads, rekeying or resetting passwords, and then gradually resuming operations from the manufacturing side of the network towards the users. Another possible area for study is analysis methods that might alert users to impending assaults. These methods would act as an enabler and catalyst for pre-detection reactions. Another area of investigation is the ability to discriminate between early warnings and detections using the level of confidence associated with existing analytic techniques.

To establish wireless IDS performance measurements, more investigation is required. Only recognition rate, FNR, and FPR are often provided when numerical findings are offered at all. Nevertheless, detecting latency is an important statistic that is hardly reported on by academics. Even if IDS may have a 100% detection rate, the attacker might still have time to harm the target system if it takes an hour to find intruders. Although it is undoubtedly an important parameter, we have not discovered detection latency being explored in the literature.

3 Description of novel IDS system

This work introduces a new IDS model via optimised DL with ensuing stages.

- At first, optimal CH is selected among SNs, where the SNs with high energy are prioritised as CH.
- Particularly, CHS is done by considering energy, QoS, delay, inter-cluster distance, intra cluster distance.
- Moreover, the selection is assisted by the proposed SU-COA.
- Finally, the selected CH and nodes are evaluated via a new trust and risk evaluation strategy that determines the node's security. An optimised LSTM model defines intruders' presence in the network.

- This detection part is enhanced by tuning the optimal weights of the model via the proposed SU-COA algorithm.
- The illustrative depiction of the SU-COA model is exposed in Figure 1.

4 Optimal CHS in WSN: objectives

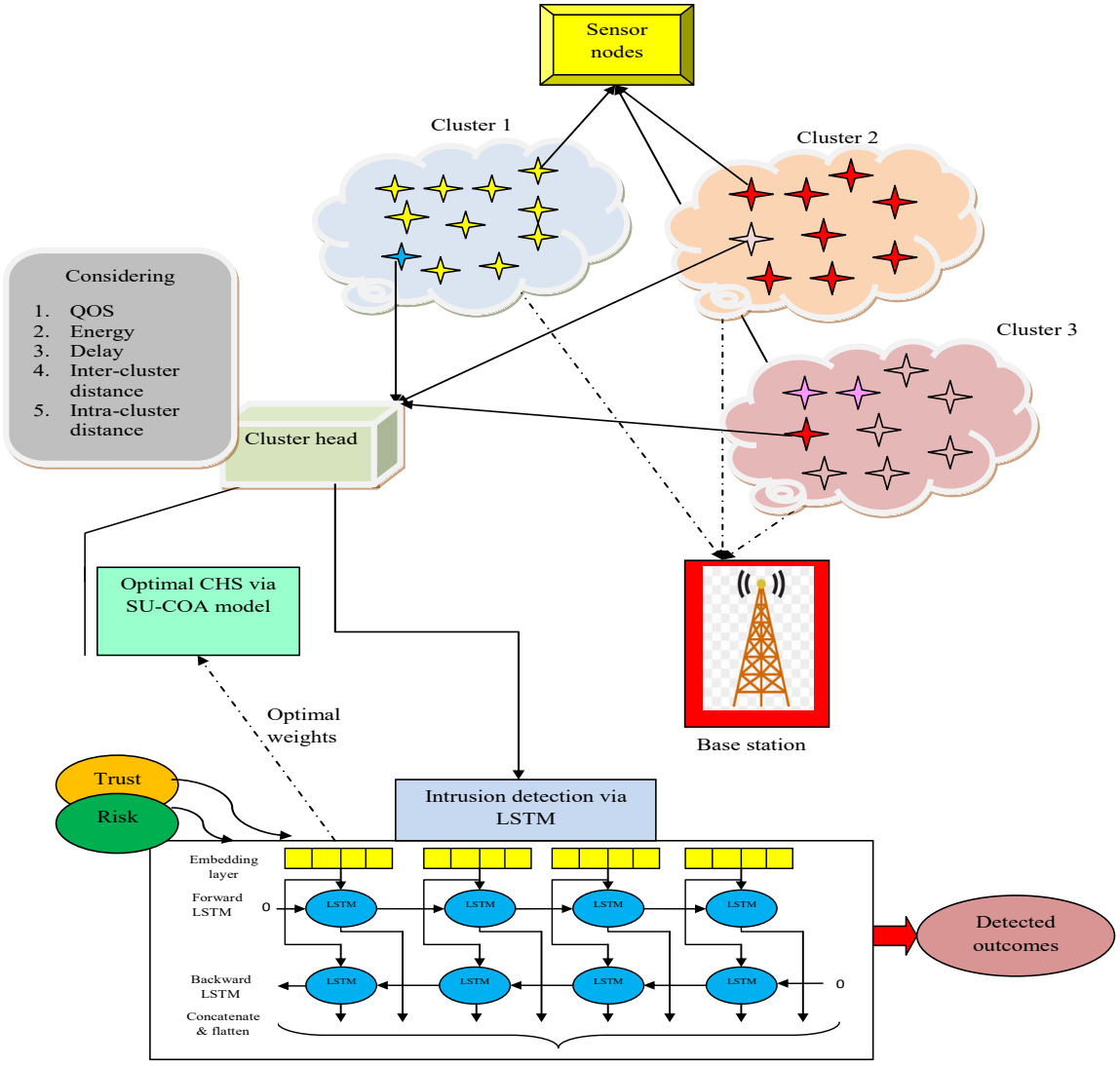
Let WSN contain n^C clusters, which CL_u points out the cluster (u = 1, 2, …. n^C). The total node count is denoted by m and CH_j refers to CH. From cluster nodes, the CH CH_j is chosen that acts as the lead for all nodes in the cluster. The CH interrelates directly with BS BS_s. Furthermore, a novel SU-COA algorithm is deployed for electing the optimal CH by considering energy, delay, QoS, inter-cluster distance, and intra-cluster distance. Finally, the selected CH and nodes are evaluated via a new trust and risk evaluation strategy that determines the node's security. An optimised LSTM model defines intruders' presence in the network. This detection part is enhanced by tuning the optimal weights of the model via the proposed SU-COA algorithm.

4.1 Objective model

This initiative seeks to shorten distances between and within clusters and speed up data transmission. As an alternative, the system's remaining energy and QOS should be at their highest following effective data transfer. The objective of the developed approach is portrayed in equation (1). Here, $W1$–$W5$ refers to the weight value allocated to each objective. The summation of these weights should be one.

$$OBJ = MIin\left[\begin{pmatrix} W1*(1-F1)+W2*F2+W3) \\ *(1-F3+W4*F4+W5*F5 \end{pmatrix}*\frac{1}{5}\right] \quad (1)$$

Figure 1 Pictorial model of SU-COA method (see online version for colours)



5 Parameters considered for CHS

- *Energy model (Khan et al., 2018):* energy extraction is the main problem with WSN (Khan et al., 2018). Since the WSN battery does not use the re-energising mechanism, it cannot provide energy if the battery runs out. Additionally, data transmission from all SNs to BS is skilfully made using additional resources. Utilising energy effectively is crucial for data transmission. Due to its numerous transmission, reception, aggregation, and sensing operations, the network requires additional energy. Equation (2) implies the amount of energy required for data broadcasting, which EG_{el} refers to electronic energy, EG_{ea} refers to energy for data time aggregation. E_{el} is shown in equation (3). $EG_{TX}(Z: di)$ refers to the whole energy essential to converse Z packet bytes at a distance di.

  The energy required at the receiver EG_{RX} to get Z bytes of packets at di is exposed in equation (4) and in equation (5), E_{am} which refers to the energy required for amplification.

$$EG_{TX}(Z:di)=EG\begin{cases}EG_{el}*Z+EG_{rs}*Z*di^2, if\ di<di_0\\ EG_{el}*Z+EG_{pw}*Z*di^2, if\ di\geq di_0\end{cases} \quad (2)$$

$$EG_{el}=EG_{TX}+EG_{ea} \quad (3)$$

$$EG_{RX}(Z:di)=EG_{el}Z \quad (4)$$

$$EG_{am}=EG_{fr}di^2 \quad (5)$$

$$di_0=\sqrt{\frac{EG_{fr}}{EG_{pam}}} \quad (6)$$

  Here,

  EG_{pam} energy of PA

  di_0 threshold distance

  EG_{fr} necessary energy for free space

  EG_1 energy for the whole inactive state

  EG_C energy cost for the entire sense stage.

  The total energy to broadcast data is shown in equation (7).

$$F1=EG_{total}=EG_{TX}+EG_C+EG_{RX}+EG_1 \quad (7)$$

- *Delay (Sekaran et al., 2020):* the delay amongst SNs is exposed in equation (8), and it lies amid [0, 1]. The delay is lessened significantly with minimal node counts. Equation (8), CH_j points out CH in WSN and m points out the whole count of nodes.

$$F2=\frac{\max_{j=1}^{L}\left(CH_j\right)}{m} \quad (8)$$

- *QoS (F3):* QoS includes every aforementioned constraint. Any system that controls data flow, packet loss, latency, and distortion on a network is called QoS. By establishing priority for particular types of network traffic, QoS regulates and maintains the network's resources.

$$QoS=1-PDR \quad (9)$$

- *Intra-cluster distance (Brindha and Sudha Juliet, 2021):* it is defined as the distance between CH and cluster nodes. The distance is evaluated as revealed by equation (10), in which, n points out CH count and m points out cluster node count, $\left\|\frac{s_j-s_i}{\varepsilon}\right\|$ which refers to distance among j^{th} and i^{th} node in the cluster and $\varepsilon 1$ refers to the normalising factor.

$$F4=\frac{1}{n*m}\left[\sum_{j=1}^{n}\sum_{i=1}^{m}\left\|\frac{s_j-s_i}{\varepsilon 1}\right\|^2\right] \quad (10)$$

- *Intercluster distance (Brindha and Sudha Juliet, 2021):* it is defined as the distance between two clusters. The distance is evaluated as shown in equation (11), which, $\left\|\frac{s_j-s_i}{\varepsilon 2}\right\|$ refers to distance among CH_j and i and $\varepsilon 2$ refers to normalising factor.

$$F5=\frac{1}{n^2}\left[\sum_{j=1}^{n}\sum_{i=1}^{n}\left\|\frac{s_j-s_i}{\varepsilon 2}\right\|^2\right] \quad (11)$$

Further, the optimal CH is chosen using the SU-COA model.

6 Detection of intruders in WSN via optimised LSTM

Then, the selected CH and nodes are evaluated via a new trust and risk evaluation strategy that determines the node's security. An optimised LSTM model is used to define the presence of intruders in the network.

6.1 Trust

Trust value (Rouissi et al., 2019) can be computed for the chosen CH. Two types of trusts can be computed, such as:

1 direct trust

2 indirect trust.

- Direct trust: it is computed as shown in equation (12), which *ER* refers to the leftover energy of the node A, $d(Node\ B, Node\ A)$ points out distance among nodes B and A. Here, distance is computed using squared Euclidean distance.

$$DT(B-A)=\frac{ER}{d(Node\ B, Node\ A)} \quad (12)$$

- Indirect trust: it is the recommendation of nodes. It is the sum of trust values calculated by other nodes. It is computed as shown in equation (13).

$$IT(B-A)=\sum DT(B-C)*DT(C-A) \quad (13)$$

Trust value is computed based upon direct and indirect trusts as shown in equation (14), wherein, w refers to the weight associated with the trust of the node and it is computed using FMF as exposed in equation (14). In equation (15), a, b, c refers to lower, medium and upper bounds and they are the vertices of TMF.

$$Trust(B-A)=w*DT(B-A)+(1-w)IT(B-A) \quad (14)$$

$$w=\begin{cases}0; & if\ x<a\\ \dfrac{x-a}{b-a}; & if\ a\le x\le b\\ \dfrac{c-x}{c-b}; & if\ b\le x\le c\\ 0; & if\ c\le x\end{cases} \quad (15)$$

6.2 Risk

Risk is calculated as exposed in equation (16), which, *sd* and *sr* refers to security rank and security needs.

$$CH_{risk}=\begin{cases}0, & if\ sd-sr\le a\\ 1-e^{\frac{sd-sr}{2}}, & if\ 0<sd-sr\le 1\\ 1-e^{\frac{3(sd-sr)}{2}}, & if\ 1<sd-sr\le 2\\ 0, & if\ 2<sd-sr\le 5\end{cases} \quad (16)$$

Based on these trust and risk values, the intrusion is detected via LSTM.

6.3 LSTM classifier

It (Zhou et al., 2019) included: a forget gate, input gate, and output gate. Assume that variables Y and A are concealed and cell states. (D_t, A_{t-1}, Y_{t-1}) and (Y_t, A_t) be input and output layers.

LSTM is exploited G_t to set up the data as shown in equation (17), in which $\sigma_{\rightarrow}$ activation function, (P_{YG}, G_{YG}) (P_{IG}, F_{IG}) implied weight, and bias to map input and concealed layers to forget gate, time → t, the forget gate → G_t, input gate → I_t and output gate → L_t.

$$G_t=\sigma\left(P_{IG}X_t+P_{YG}Y_{t-1}+F_{IG}+F_{YG}\right) \quad (17)$$

I_t is exploited in LSTM as in equations (18)–(20), here, (P_{YV}, L_{YV}) and (P_{IV}, V_{IV}) → weight and bias factors to map input and hidden layers to the cell gate. (P_{YI}, F_{YI}) and (P_{II}, F_{II}) imply weight and bias constraints to map input and concealed layers to I_t. It gets output concealed layer from L_t as in equation (21) and (22), in which, (P_{YL}, F_{YL}) and (P_{IL}, F_{IL}) → weight and bias to map L_t.

$$V_t=\tanh\left(F_{IV}+P_{IV}D_t+F_{YV}+P_{YV}Y_{t-1}\right) \quad (18)$$

$$I_t=\sigma\left(P_{II}D_t+P_{YI}Y_{t-1}+F_{II}+F_{YI}\right) \quad (19)$$

$$A_t=G_tA_{t-1}+I_tV_t \quad (20)$$

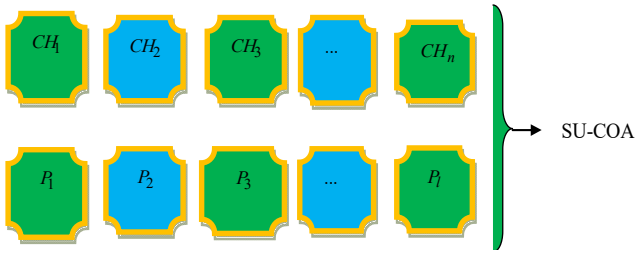
$$F_t=\sigma\left(L_{IF}+J_{IF}X_t+L_{YF}+J_{YF}Y_{t-1}\right) \quad (21)$$

$$Y_t=L_t\tanh\left(A_t\right) \quad (22)$$

7 Optimal CH and weight selection assisted by SU-COA algorithm

Here, the CH as well as LSTM weights implied as (P) are optimally elected via the SU-COA scheme as shown in Figure 2. The LSTM weights are represented by P_1, P_2 …. P_l and the cluster header is denoted by CH_1, CH_2 … CH_n.

Figure 2 Solution encoding (see online version for colours)



7.1 Proposed SU-COA algorithm

The findings were not very good because the current CA (Nirmal Raja and Marsaline Beno, 2014) paradigm has several advantages. As a result, special adjustments are required, and SU-COA is set up. Typically, conservative optimisation methods may improve themselves (Mitchell and Chen, 2014).

There are two routes for the coots to transition from the first stage to the second. The first entails speeding up a few nearby coot followers, moving them into place with other coots, and improving the leaders' positions. The second tactic is swiftly elevating perspective coot followers to leadership positions as substitutes for underwhelming leaders. The density of coots determines the amount of time it takes to transition from one phase to the other. The remaining fraction of the anticipated coot population M_{po} comprises coot followers, while the flock's leaders make up the majority.

Following equations (23), and (24), respectively, are the beginning locations of follower (pos_{ct0}) and leader (pos_{lea}).

$$pos_{ct0}=ra_{ct}(up-lp)+lp \quad (23)$$

$$pos_{lea}=ra_{lea}(up-lp)+lp \quad (24)$$

Here, up → upper bound and lp → lower bound.

The new position of Coot is computed as shown in equation (25). Conventionally, A it is computed as in equation (26), wherein L refers to the current iteration, $L_{\max}$ is the maximum iteration. As per SU-COA, L is computed as shown in equation (27), wherein α refers to constant value 5.

$$pos_{coot}(i)=pos_{coot}(i)+Ar2_{coot}\times\left(Q-pos_{coot}(i)\right) \quad (25)$$

$$A = 1 - L \times \left(\frac{1}{L_{\max}} \right) \tag{26}$$

$$A = 1 - \left(\frac{L}{L_{\max}} \right)^{\frac{1}{\alpha}} \tag{27}$$

Chain movement: it is feasible to integrate chain movement by using the overall average of two coots. We may also transfer the Coot towards the other Coot by roughly halving the distance between them after first calculating the distance vector among them. This phase is often calculated using equation (28). As per SU-COA, this phase is calculated by equation (29), in which, *we*1 and *we*2 implies weights that are evaluated using weighted harmonic mean of positions.

$$pos_{coot}(i) = 0.5 \times \left(pos_{coot}(i-1) + pos_{coot}(i) \right) \tag{28}$$

$$pos_{coot}(i) = \frac{we1 + we2}{(we1 + we2) / \left(pos_{coot}(i) + pos_{coot}(i-1) \right)} \tag{29}$$

The Coot's followers update their positions appropriately. This is shown in equation (30). Whereas the coot leaders' values r_{lea} are randomly produced, so are the coots' followers' values r_{coot}. Conventionally, $r1$ is a random integer among [0, 1]. As per SU-COA, $r1$ is computed using the ICMIC map as shown in equation (31).

$$pos_{coot}(i) = 2.r1_{coot}.\cos(2\pi r)\left[pos_{lea}(k) - pos_{coot}(i) \right] \tag{30}$$

$$r1 = \sin\left(\frac{e}{ek} \right) \quad a \in (0, \beta), r1 \in (-1, 1) \tag{31}$$

The leader's positions are enhanced as shown in equation (32), where, gbe_{pos} points out best global position and B is evaluated as in equation (33).

$$pos_{lea} = B.r3_{lea}2.r_{coot} \cos(2\pi r)\left\lfloor gbe_{pos} - pos_{lea}(i) \right\rfloor + gbe_{pos} \tag{32}$$

$$B = 2 - L \times \left(\frac{1}{L_{\max}} \right) \tag{33}$$

8 Results and discussion

8.1 Simulation set up

Python was used to execute this project. The effectiveness of LSTM+ SU-COA was demonstrated over LSTM+ CMBO, LSTM+ PRO, FRNN (Selvakumar et al., 2019), LSTM+ CSO, GWOSVM-IDS (Baykara and Das, 2018), LSTM+ CA, SVM, RNN, CNN, DBN and SI-SLnO + NN (Kagade and Jayagopalan, 2022). The study was done regarding energy, throughput, delay, PDR, distance and various other metrics. The sample model of data travelling from varied nodes via CH to BS is exposed in Figure 3.

8.2 Performance analysis

The study on LSTM+ SU-COA model is computed over LSTM+ CMBO, LSTM+ PRO, FRNN (Selvakumar et al., 2019), LSTM+ CSO, GWOSVM-IDS (Safaldin et al., 2021), LSTM+ CA, SVM, RNN, CNN, DBN and SI-SLnO + NN. The estimation of LSTM+ SU-COA-based IDS done over CMBO, PRO, FRNN (Selvakumar et al., 2019), CSO, GWOSVM-IDS (Safaldin et al., 2021), WOA, GA and CA are exposed in Figures 4 and 5 as well as in Table 1 (MCC, NPV, and F-measure). The analysis of LSTM+ SU-COA over varied methods, namely, RNN, SVM, CNN, DBN, and SI-SLnO + NN, is shown in Table 2 for diverse LPs. Here, LSTM+ SU-COA has accomplished the best values for accuracy and other positive metrics, while LSTM+ SU-COA has accomplished lesser values for FPR and FNR. The NPV attained by LSTM+ SU-COA at 150th LP is 93.83495, which is said to be higher than those attained by LSTM+ SU-COA at other LPs. The MCC attained by LSTM+ SU-COA at 150th LP is 96.92716, while, at 100th LP, the MCC attained by LSTM+ SU-COA is 87.42809. Thus, the adopted LSTM+ SU-COA has predominantly revealed better results at the 150th LP than at other LPs from 25–150. The accuracy of LSTM+ SU-COA is high at 150th LP, i.e., around 0.95, while CSO has attained less accuracy than LSTM+ CMBO, LSTM+ PRO, FRNN (Selvakumar et al., 2019), GWOSVM-IDS (Safaldin et al., 2021), WOA, GA and LSTM+ CA for all LPs. The analysis of classifiers (SVM, RNN, CNN, DBN, and SI-SLnO + NN) also proved the enhancement of our scheme, as noted in Table 2. As we have done enhancements in optimal CHS and trust and risk level evaluation, our technique's results look finer than others.

Figure 3 Sample model of data travelling from varied nodes via CH to BS at diverse simulations, (a) 1, (b) 2, (c) 3, (d) 4 (see online version for colours)

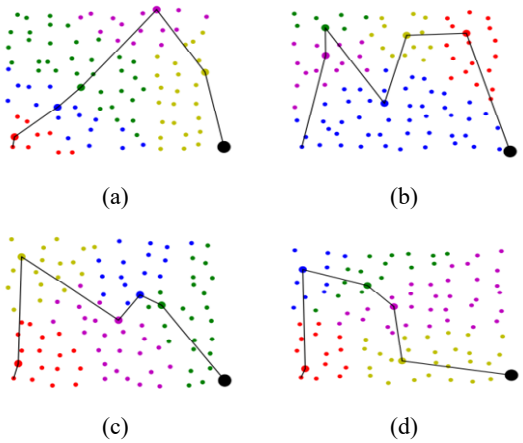
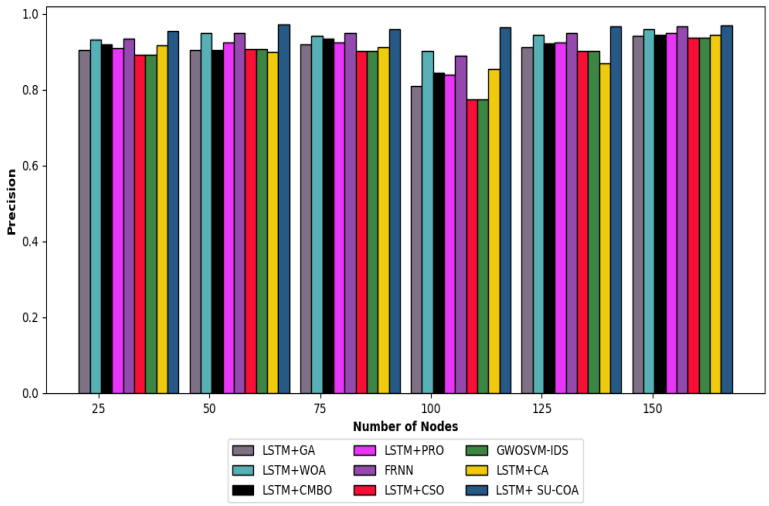
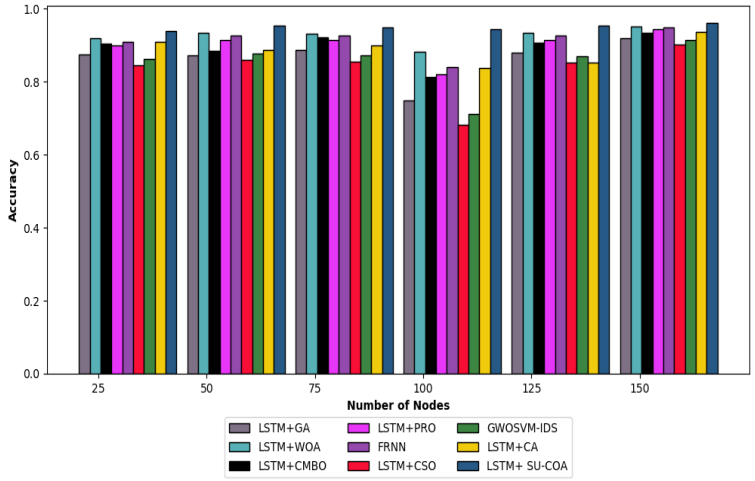


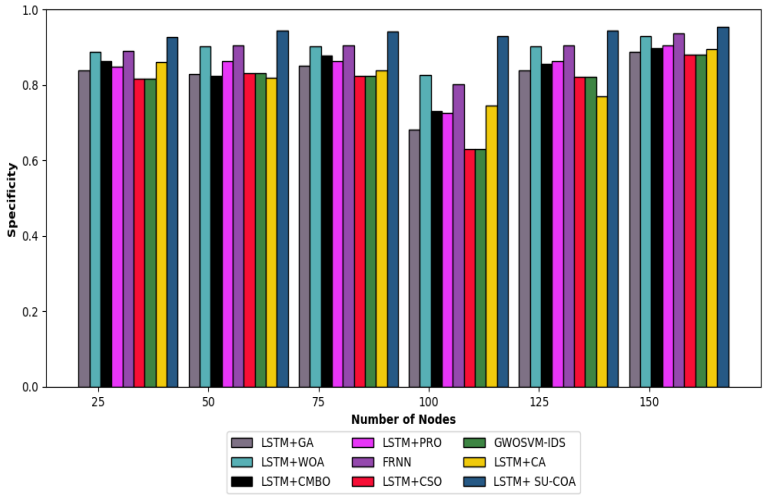
Figure 4 Investigation on LSTM+ SU-COA over existing schemes for, (a) precision, (b) accuracy, (c) specificity, (d) sensitivity (see online version for colours)



(a)

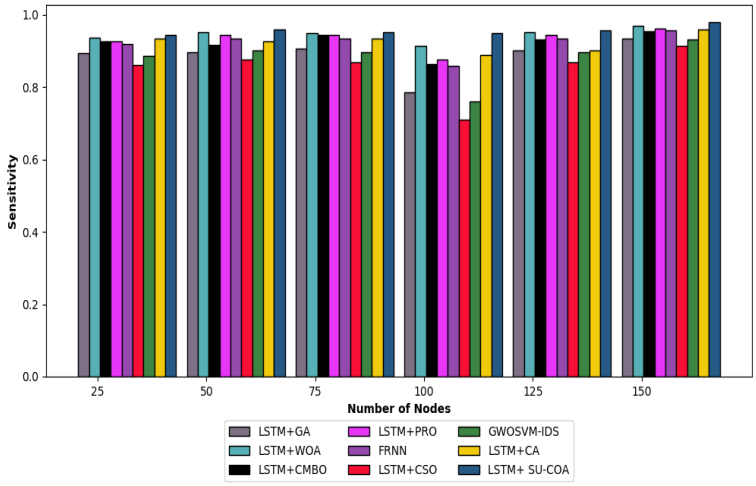


(b)



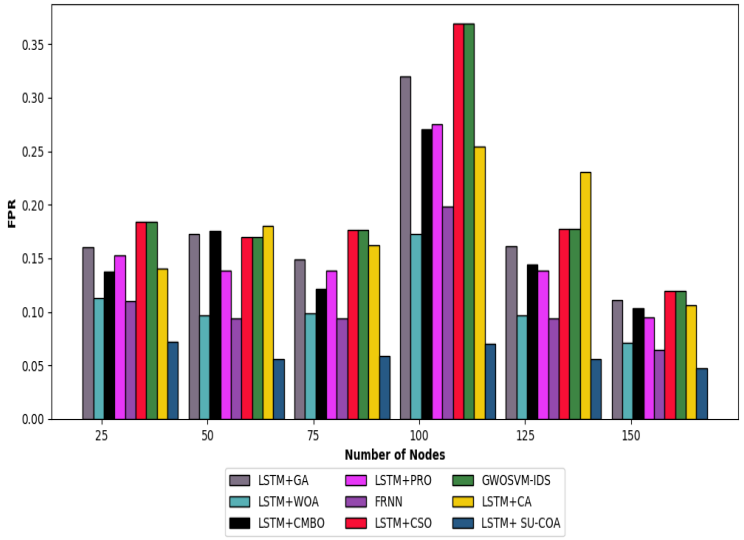
(c)

Figure 4 Investigation on LSTM+ SU-COA over existing schemes for, (a) precision, (b) accuracy, (c) specificity, (d) sensitivity (continued) (see online version for colours)

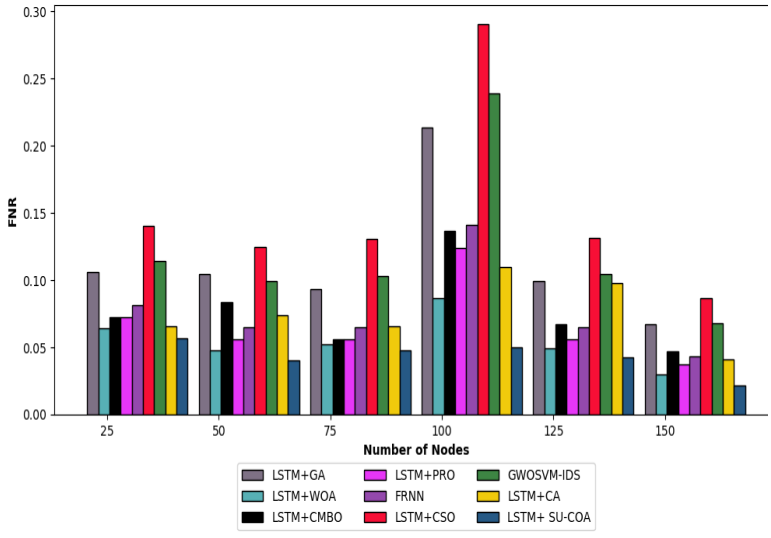


(d)

Figure 5 Investigation on LSTM+ SU-COA over existing schemes for (a) FPR, (b) FNR (see online version for colours)



(a)



(b)

Table 1 Investigation on LSTM+ SU-COA over existing schemes for MCC, NPV and F-measure

MCC							
LP	*LSTM+ CMBO*	*LSTM+ PRO*	*FRNN (Selvakumar et al., 2019)*	*LSTM+ CSO*	*GWOSVM-IDS (Safaldin et al., 2021)*	*LSTM+ CA*	*LSTM+ SU-COA*
25	81.09583	79.84475	82.01402	68.32165	71.67127	81.7301	88.33964
50	74.52878	81.25368	83.46123	69.52726	72.93598	75.44271	89.89848
75	82.52685	81.25368	83.46123	68.26976	71.79002	77.97322	91.19948
100	59.77437	61.0183	65.10835	33.2239	38.96889	64.57945	87.42809
125	79.2735	81.25368	83.46123	68.00566	71.54905	68.10936	90.85786
150	85.29572	87.21652	88.77059	78.47485	81.02433	85.84416	96.92716
NPV							
LP	*LSTM+ CMBO*	*LSTM+ PRO*	*FRNN (Selvakumar et al., 2019)*	*LSTM+ CSO*	*GWOSVM-IDS (Safaldin et al., 2021)*	*LSTM+ CA*	*LSTM+ SU-COA*
25	87.81217	87.81217	86.28234	76.42911	80.56041	88.99562	90.70708
50	84.57584	89.3617	87.80488	77.77778	81.98198	86.23853	92.30769
75	89.3617	89.3617	87.80488	76.92308	81.25	87.65432	92.74463
100	75.90361	77.96818	75.20661	55	61.37339	80.17621	90.47619
125	87.40818	89.3617	87.80488	76.74419	81.09641	82.14286	92.74471
150	91.03139	92.74047	91.6318	84	87.22045	92.06349	93.83495
F-measure							
LP	*CMBO*	*PRO*	*FRNN (Selvakumar et al., 2019)*	*CSO*	*GWOSVM-IDS (Safaldin et al., 2021)*	*CA*	*LSTM+ SU-COA*
25	92.31326	91.85232	92.63701	87.54607	88.85088	92.53257	94.87752
50	91.00968	93.47314	94.27169	89.09091	90.41874	91.33093	96.55172
75	93.94222	93.47314	94.27169	88.60759	89.98764	92.26977	95.58194
100	85.32731	85.78236	87.39496	74.03846	76.71968	87.17843	95.68345
125	92.76169	93.47314	94.27169	88.50575	89.89672	88.54962	96.15209
150	94.93375	95.61025	96.15807	92.45283	93.40176	95.1223	96.70562

Table 2 Analysis of LSTM+ SU-COA over varied classifiers

Metrics	*SVM*	*RNN*	*CNN*	*DBN*	*SI-SLnO +NN*	*LSTM+ SU-COA*
Accuracy	0.840199	0.712153	0.90099	0.922899	0.946667	0.959716
Sensitivity	0.871134	0.784483	0.92126	0.919355	0.976744	0.978337
Specificity	0.784483	0.601276	0.863014	0.93007	0.90625	0.952487
Precision	0.879227	0.750996	0.926471	0.963768	0.933333	0.970768
F-measure	0.875162	0.767374	0.923858	0.941038	0.954545	0.967056
MCC	0.653262	0.391036	0.782377	0.831786	0.966667	0.969272
NPV	0.771689	0.64539	0.854015	0.850746	0.913043	0.93835
FPR	0.215517	0.398724	0.136986	0.06993	0.09375	0.047513
FNR	0.128866	0.215517	0.07874	0.080645	0.023256	0.021663

Table 3 Statistical study

Metrics	*Standard deviation*	*Mean*	*Median*	*Maximum*	*Minimum*
CMBO	0.011826	1.052404	1.04519	1.097881	1.04519
PRO	0.005464	1.061497	1.059025	1.082925	1.059025
CSO	0.017489	1.059727	1.049997	1.090536	1.049997
GWO	0.012859	1.064494	1.061298	1.087563	1.045928
CA	0.005464	1.045532	1.04306	1.06696	1.04306

Table 3 Statistical study (continued)

Metrics	*Standard deviation*	*Mean*	*Median*	*Maximum*	*Minimum*
LSTM+GA	0.008898	1.057945	1.052436	1.078683	1.052436
LSTM+WOA	0.006031	1.052496	1.047942	1.062587	1.047942
LSTM+ SU-COA	0.006011	1.043553	1.041163	1.06813	1.041163

8.3 Statistical study

Table 3 depicts the study on error via LSTM+ SU-COA oriented model over CMBO, PRO, CSO, GWO, and CA. The met heuristic schemes are stochastic, and to substantiate their fair evaluation, each model is analysed quite often to accomplish less error. For the maximum case, a less error of 1.068 is gained using LSTM+ SU-COA, while CMBO, PRO, CSO, GWO, WOA, GA and CA have acquired comparatively high errors of 1.097881, 1.082925, 1.090536, 1.087563 and 1.06696 for the maximum case. Also, for the mean case, the LSTM+ SU-COA gained less error. Thus, it is proven that the adopted optimisation approach offers less error on resolving the optimisation issue regarding precise detection. The enhancements in CHS and trust and risk level evaluation offer finer results for our method over others.

8.4 Convergence study

The convergence rate of the SU-COA technique over CMBO, PRO, CSO, GWO, WOA, GA and CA is exposed in Figure 6. In Figure 6, a less cost of 1.045 is achieved by SU-COA from the 20th to 50th iterations. Since optimisation holds a very important role in our work. During the primary iterations, even the SU-COA algorithm shows higher error rates. However, as the iterations are raised, the error gets lessened, and the SU-COA algorithm obtains the slightest error. The enhancements in CHS and weight training in LSTM offer finer results for our method than others.

Figure 6 Convergence analysis of SU-COA technique over others (see online version for colours)

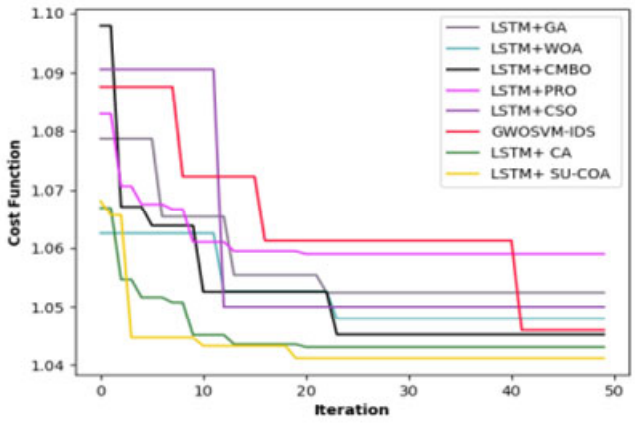
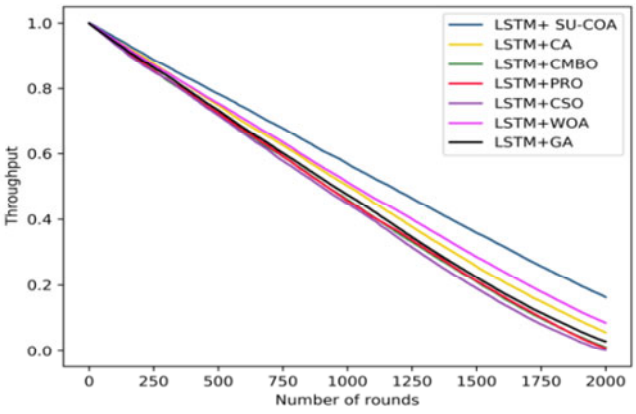
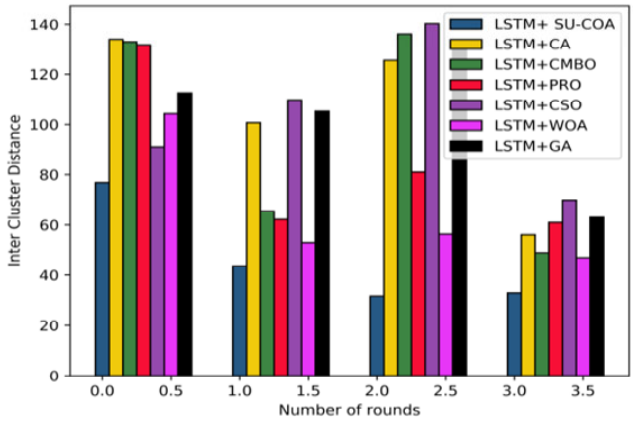


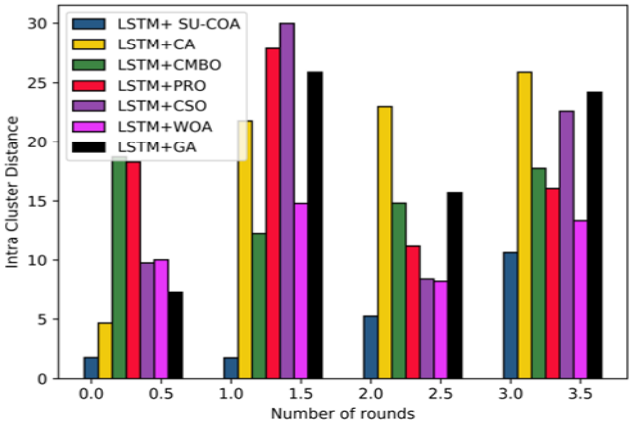
Figure 7 Analysis of (a) throughput, (b) inter, (c) intra cluster distance (see online version for colours)



(a)

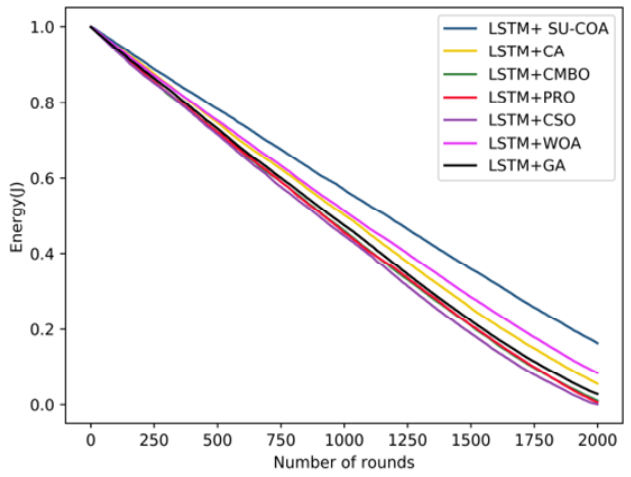


(b)

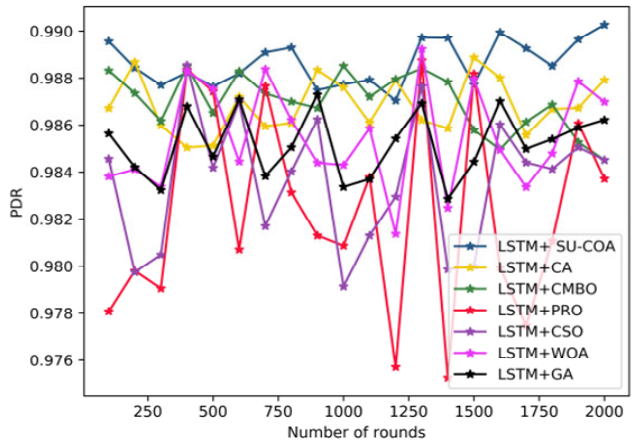


(c)

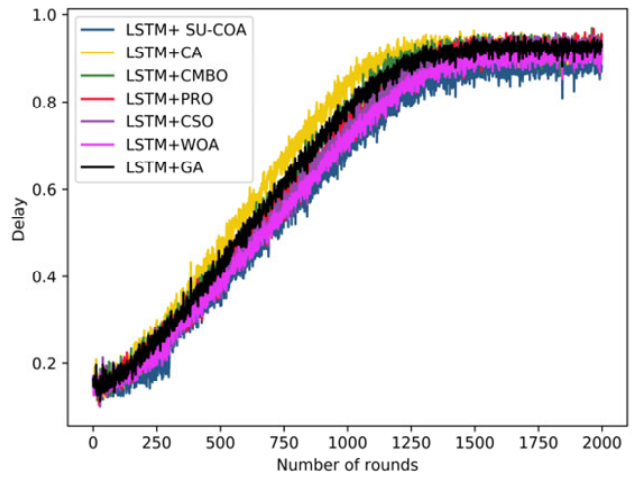
Figure 8 Analysis on (a) energy, (b) PDR, (c) delay (see online version for colours)



(a)



(b)



(c)

8.5 *Analysis of throughput, inter and intra-cluster distance*

The examination of proposed LSTM+ SU-COA over others regarding throughput, inter and intra-cluster distance is given in Figure 7. In the case of throughput from Figure 7(a), it is noted that throughput is lessened with an increase in the count of rounds. However, LSTM+ SU-COA provided higher throughput over CMBO, PRO, CSO, WOA, GA and CA. At initial rounds, the throughput is higher about 1.0, but with a rise in the count of rounds, the throughput is minimised to about 0.001 at the 2,000th round. In Figures 7(b) and 7(c), inter and intra-cluster distances are computed. The inter-cluster distance for LSTM+ SU-COA is low than CMBO, PRO, CSO, WOA, GA and CA. Particularly, the inter-cluster distance for LSTM+ SU-COA is less when the count of rounds is at 2.0. Chiefly, the intra-cluster distance for LSTM+ SU-COA is less when the count of rounds is at 0.0 and 1.0. The enhancements in CHS and trust and risk level evaluation proffer finer resultants for the LSTM+ SU-COA scheme over others.

8.6 *Analysis of energy, PDR and delay*

The analysis of energy, PDR, and delay using LSTM+ SU-COA is given in Figure 8. Here, the delay in Figure 8(c) increases with an increase in the count of rounds for the proposed method as well as compared methods like LSTM+ CMBO, LSTM+ PRO, LSTM+ CSO, WOA, GA and LSTM+ CA. In the case of energy from Figure 8(a), it is noted that energy is lessened with the increase in the count of rounds; however, LSTM+ SU-COA provided higher energy over LSTM+ CMBO, LSTM+ PRO, LSTM+ CSO, WOA, GA and LSTM+ CA. At initial rounds, the energy is higher about 1.0, but with raise in the count of rounds, the energy is minimised to about 0.001 at the 2,000th round. The PDR is high using LSTM+ SU-COA, while LSTM+ CMBO, LSTM+ PRO, LSTM+ CSO, WOA, GA and LSTM+ CA acquired less PDR values. The PDR for LSTM+ SU-COA is high at the 1500th round. The enhancements in CHS and trust and risk level evaluation proffer finer resultants for the LSTM+ SU-COA scheme over others.

9 Conclusions

This work introduced the IDS model, where the highest energy SNs are given priority as CH and the optimal CH was chosen among SNs. In particular, CHS was completed by taking into account several restrictions. The suggested SU-COA also helped with the selection. Finally, a novel trust and risk evaluation technique was utilised to assess the chosen CH and nodes. This strategy determined the security of each node, and an optimised LSTM model was employed to determine the existence of intruders in the network. By adjusting the model's ideal weights with the help of the suggested SU-COA algorithm, this detection portion was improved. At initial rounds, the energy was higher, about 1.0, but with raise in the count of rounds, the energy was minimised to about 0.001 at the 2,000th round. The PDR was high using LSTM+ SU-COA, while LSTM+ CMBO, LSTM+ PRO, LSTM+ CSO, LSTM+ CA, WOA and GA acquired less PDR values. The PDR for LSTM+ SU-COA

was high at the 1,500th round. The enhancements in CHS and trust and risk level evaluation proffer finer resultants for the LSTM+ SU-COA scheme over others. When compared to other algorithms, the results demonstrate that the suggested approach has the highest accuracy values for the normal activities and scan intrusion types and acceptable values for the other intrusion types. It also has the excellent quality of the suggested strategy. By doing this, it is made sure that the prediction is not biased toward the dominant group. The effectiveness of IoT networks and their applications is significantly impacted by the quick and precise identification of IoT attacks. By adding another layer to the suggested approach, future work can be expanded to produce a more precise prediction for the subcategories of the intrusion.

References

Abhale, A.B. and Manivannan, S.S. (2020) 'Supervised machine learning classification algorithmic approach for finding anomaly type of intrusion detection in wireless sensor network', *Opt. Mem. Neural Networks*, Vol. 29, pp.244–256, https://doi.org/10.3103/S1060992X20030029.

Anand, C. and Gnanamurthy, R.K. (2016) 'Localized DoS attack detection architecture for reliable data transmission over wireless sensor network', *Wireless Personal Communications*, Vol. 90, No. 2, pp.847–859.

Balamurugan, P. and Kagade, R.B. (2020) 'Two level intrusion detection mechanism for context and trust in wireless sensor network', *Int. J. Recent Technol. Eng. (IJRTE)*, Vol. 8, No. 6, pp.65–71, DOI: 10.35940/ijrte.F7141.038620.

Baykara, M. and Das, R. (2018) 'A novel honeypot based security approach for real-time intrusion detection and prevention systems', *Journal of Information Security and Applications*, August, Vol. 41, pp.103–116.

Borkar, G.M., Patil, L.H., Dalgade, D. and Hutke, A. (2019) 'A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: a data mining concept', *Sustainable Computing: Informatics and Systems*, September, Vol. 23, pp.120–135.

Brindha, G. and Sudha Juliet, P. (2021) 'An energy-aware cluster head selection protocol based on multi-objective dolphin swarm optimization in wireless sensor network' *International Journal of Intelligent Communication, Computing and Networks Open Access Journal* (ISSN: 2582-7707), https://doi.org/10.51735/ijiccn/001/14.

Fan, R., HeEm, D-J., Pan, X-Z. and Ping, L-D. (2011) 'An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks', *Journal of Zhejiang University Science C*, Vol. 12, No. 7, pp.550–560.

Gill, K., Yang, S. and Wang, W. (2012) 'Scheme for preventing low-level denial-of-service attacks on wireless sensor network-based home automation systems', *IET Wireless Sensor Systems*, December, Vol. 2, No. 4, pp.361–368.

Gokul Pran, S. and Raja, S. (2023) 'An efficient feature selection and classification approach for an intrusion detection system using optimal neural network', *Journal of Intelligent & Fuzzy Systems Preprint*, Vol. 44, No. 5, pp.1–11.

Gope, P., Lee, J. and Quek, T.Q.S. (2017) 'Resilience of DoS attacks in designing anonymous user authentication protocol for wireless sensor networks', *IEEE Sensors Journal*, 15 Jan., Vol. 17, No. 2, pp.498–503.

He, D., Chen, C., Chan, S. and. Bu, J. (2012) 'DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks', *IEEE Transactions on Wireless Communications*, May, Vol. 11, No. 5, pp.1946–1956.

Jadhav, A.N. and Gomathi, N. (2019) 'DIGWO: hybridization of dragonfly algorithm with improved grey wolf optimization algorithm for data clustering', *Multimedia Research*, Vol. 2, No. 3, pp.1–11.

Kagade, R.B. and Jayagopalan, S. (2022) 'Optimization assisted deep learning based intrusion detection system in WSN with two-tier trust evaluation', *Int. J. Network Mgmt.*, Vol. 32, No. 4, http://doi:10.1002/nem.2196, 2022.

Kagade, R.B. and Santhosh, J. (2021) 'State context and hierarchical trust management in WSN for intrusion detection', in *2021 International Conference of Techno-Societal 2020*, Springer, Cham, pp.103–116.

Kagade, R.B. and Satao, R.A. (2013) 'Robust topology, self-scheduling approach based on remaining energy for WSN', *Int. J. Comput. Sci. Inf. Technol.*, Vol. 4, No. 6, pp.800–803.

Kagade, R.B. and Satao, R.A. (2014) 'Enhanced lifetime distributed power saving algorithm in wireless sensor networks', in *2014 International Conference on Information Communication and Embedded Systems (ICICES2014)*, IEEE, pp.27–28.

Khan, M., Shankar, A., Jaisankar, N., Balamurugan, B. and Patan, R. (2018) 'A hybrid model for security-aware cluster head selection in wireless sensor networks', *IET Wireless Sensor Systems*, DOI: 10.1049/iet-wss.2018.5008.

Maheswari, M. and Karthika, R.A. (2021) 'A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks', *Wireless Pers. Commun*., Vol. 118, pp.1535–1557, https://doi.org/10.1007/s11277-021-08101-2.

Mitchell, R. and Chen, I-R. (2014) 'A survey of intrusion detection in wireless network applications', *Computer Communications*, 1 April, Vol. 42, pp.1–23.

Muzammal, S.M., Murugesan, R.K. and Jhanjhi, N.Z. (2020) 'A comprehensive review on secure routing in internet of things: mitigation methods and trust-based approaches', *IEEE Internet of Things Journal*, Vol. 8, No. 6, pp.4186–4210.

Naruei, I. and Keynia, F. (2021) 'A new optimization method based on COOT bird natural life model', *Expert Systems with Applications*, Vol. 183, p.115352, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2021.115352.

Nirmal Raja, K. and Marsaline Beno, M. (2014) 'On securing wireless sensor network-novel authentication scheme against DOS attacks', *Journal of Medical Systems*, Vol. 38, No. 84, pp.1–5.

Qureshi, S.G. and Shandilya, S.K. (2021) 'Novel fuzzy based crow search optimization algorithm for secure node-to-node data transmission in WSN', *Wireless Pers. Commun*., https://doi.org/10.1007/s11277-021-08352-z.

Ramana, K. et al. (2022) 'WOGRU-IDS – an intelligent intrusion detection system for IoT assisted wireless sensor networks', *Computer Communications*, Vol. 196, pp.195–206.

Rouissi, N., Gharsellaoui, H. and Bouamama, S. (2019) 'Improvement of watermarking-LEACH algorithm based on trust for wireless sensor networks', *23rd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems*, *Procedia Computer Science*, Vol. 159, pp.803–813.

Safaldin, M., Otair, M. and Abualigah, L. (2020) 'Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks', *Journal of Ambient Intelligence and Humanized Computing*, https://doi.org/10.1007/s12652-020-02228-z, Received: 16 January 2020/Accepted: 13 June 2020.

Safaldin, M., Otair, M. and Abualigah, L. (2021) 'Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks. *J. Ambient Intell. Human Comput*., Vol. 12, pp.1559–1576, https://doi.org/10.1007/s12652-020-02228-z.

Sedjelmaci, H., Senouci, S.M. and Ansari, N. (2017) 'Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: a Bayesian game-theoretic methodology', *IEEE Transactions on Intelligent Transportation Systems*, May, Vol. 18, No. 5, pp.1143–1153.

Sekaran, K., Rajkumar, Y., Latchoumi, T., Kadry, S. and Lim, S. (2020) 'An energy-efficient cluster head selection in wireless sensor network using grey wolf optimization algorithm', *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, Vol. 18, pp.2822–2833, DOI: 10.12928/TELKOMNIKA.v18i6.15199.

Selvakumar, K., Karuppiah, M., SaiRamesh, L., Hafizul Islam, S.K. and Choo, K-K.R. (2019) 'Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs', *Information Sciences*, September, Vol. 497, pp.77–90.

Shafiq, M. et al. (2021) 'Robust cluster-based routing protocol for IoT-assisted smart devices in WSN', *Computers, Materials & Continua*, Vol. 67, No. 3, pp.3506–3521.

Shamshirband, S., Amini, A., Anuar, N.B., Kiah, L.M. and Furnell, S. (2014) 'D-FICCA: a density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks', *Measurement*, September, Vol. 55, pp.212–226.

Sinha, S. and Paul, A. (2020) 'Neuro-fuzzy based intrusion detection system for wireless sensor network', *Wireless Pers. Commun*., Vol. 114, pp.835–851, https://doi.org/10.1007/s11277-020-07395-y.

Soliman, H.H., Hikal, N.A. and Sakr, N.A. (2012) 'A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks', *Egyptian Informatics Journal*, November, Vol. 13, No. 3, pp.225–238.

Son, Y-H., Hong, J-K. and Bae, K-S. (2013) 'Authentication masking code against DoS of T-MAC protocol', *Journal of Central South University*, Vol. 20, No. 7, pp.1889–1895.

Tapiador, J.E. and Clark, J.A. (2013) 'The placement-configuration problem for intrusion detection nodes in wireless sensor networks', *Computers & Electrical Engineering*, October, Vol. 39, No. 7, pp.2306–2317.

Thangaramya, K., Kulothungan, K., Indira Gandhi, S. et al. (2020) 'Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN', *Soft Comput*., Vol. 24, pp.16483–16497, https://doi.org/10.1007/s00500-020-04955-z.

Umarani, C. and Kannan, S. (2020) 'Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network', *Peer-to-Peer Netw. Appl.*, Vol. 13, pp.752–761, https://doi.org/10.1007/s12083-019-00781-9.

Vijayakumar, K.P., Pradeep Mohan Kumar, K., Kottilingam, K., Karthick, T., Vijayakumar, P. and Ganeshkumar, P. (2018) 'An adaptive neuro-fuzzy logic based jamming detection system in WSN', *Soft Computing*, Vol. 23, pp.1–13.

Zha, Y. and Li, J. (2018) 'CMA: a reconfigurable complex matching accelerator for wire-speed network intrusion detection', *IEEE Computer Architecture Letters*, 1 Jan.-June, Vol. 17, No. 1, pp.33–36.

Zhang, T., Han, D., Marino, M.D. et al. (2021) 'An evolutionary-based approach for low-complexity intrusion detection in wireless sensor networks', *Wireless Pers. Commun*., https://doi.org/10.1007/s11277-021-08757-w.

Zhou, X., Lin, J., Zhang, Z., Shao, Z. and Liu, H. (2019) 'Improved itracker combined with bidirectional long short-term memory for 3D gaze estimation using appearance cues', *Neuro Computing*, in press, corrected proof, available online 20 October, Vol. 390, pp.271–225.

Nomenclature

Abbreviation	*Description*
BS	Base station
CA	Coot optimisation
CSO	Crow search optimisation
CNN	Convolutional neural network
CH	Cluster head
DBN	Deep belief network
DHO	Deer hunting optimisation
IOT	Internet of things
IDS	Intrusion detection system
FRNN	Fuzzy and rough set based nearest neighbourhood
F-CSO	Fuzzy-based crow search optimiser
FNR	False negative rate
FMF	Fuzzy membership function
FPR	False positive rate
GWO	Grey wolf optimiser
HADS	Hybrid anomaly detection systems
HTGA	Hybrid tissue growing method
LSTM	Long short-term memory
LP	Learning percentage
NN	Neural network
NTG	Networked tissue growing
OLSR	Optimised link state routing protocol
PDR	Packet delivery ratio
PSO	Particle swarm optimisation
PRO	Poor rich optimisation
QOS	Quality of service
RNN	Recurrent neural networks
STG	Swarm tissue growing
SN	Sensor node
SI-SLnO	Self improved sea lion
SVM	Support vector machine
GWOSVM-IDS	SVM-modified binary GWO
TCHs	Tentative cluster heads
TMF	Triangular membership function
TVP-IPSO	Time-varying parameter improved PSO
WSN	Wireless sensor network