Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 5s (2024)

Hybrid Model for Intrusion Detection in Wireless Sensor Network: An Improved Class Imbalance Processing

Sravanthi Godala[1], Dr. M. Sunil Kumar[2]

[1]Research Scholar, Department of CSE, JNTUA, Ananthapuramu 515002, AP, India Email:vmsravanthi@gmail.com

[2]Professor, Department of CSE, Sree Vidyanikethan Engineering College (Autonomous), Tirupati 517102,AP, India. Email:sunilmalchi1@gmail.com

Article History:

Received: *15-05-2024*

Revised: *20-06-2024*

Accepted: *01-07-2024*

Abstract

A significant difficulty in WSN settings is recognizing the abnormalities as security threats become divergent in various fields. The major drawbacks of WSN including insufficient memory, limited energy, and low compute power, and a small communication range. Thus, enhancing the detection accuracy of intrusion detection in such contexts is critical. However, this work intends to propose intrusion detection in WSN with improved class imbalance processing. The input data is pre-processed to balance the data with modified class imbalance process. Here, the SMOTE-ENN and Tomek link algorithm is employed to pre-process the raw data. Then the entropy and improved correlation based features are retrieved from the balanced data. Later, these features are trained by subjecting those features into the hybrid model that includes Deep Maxout and Bi-GRU model and then the final detection is predicted with the classifier outcomes. Further, at the training rate 90%, the proposed yielded the least FPR rate (0.1038) than the other 60, 70 and 80 training percentages.

Keywords: Intrusion detection, WSN, SMOTE, improved correlation, and entropy features.

1. Introduction

WSNs play a major role that connects the digital with the physical worlds. WSNs allow us to research physical world environmental phenomena by utilizing a large number of sensors that gather information in digital format to be processed and transported through network and then preserved and examined in fog nodes [3] [7]. WSN is made up of a multitude of low-power, low-cost, self-organizing wireless nodes that are used to manage and monitor the environment. Furthermore, WSNs may be employed in a variety of applications such as earthquake monitoring, ocean monitoring, machine performance monitoring, and a variety of military applications [5]. Furthermore, advanced uses like pollution observing, building security, highway traffic, and water quality observing are involved in the idea of WSN architecture. Furthermore, five key features must be addressed while developing a WSN: they are dependability, self-healing, robustness, scalability, and security [1] [6].

It is necessary for vital programs that make use of WSN to have a high level of assurance in order to safeguard their information as well as their systems contrary to attacks. IDS ought to be employed to identify abnormal behaviours and incursions. Sensors in WSN collect information from the environment in which they are deployed and relay it to the base station node [2]. With the cryptographic security measures the confidential information was secured but it is insufficient to safeguard the data. Thereby, the another functionality of defensive technique referred as IDS, is

necessary. Because of the benefits of categorization, self- learning, and resilience, NNs have drawn a significant number of academics to explore the intrusion detection algorithm based on neural network and have produced very good results [4] [8].

The effectiveness of ML and DL models in satisfying security requirements has been established. Furthermore, ML techniques find patterns using statistical ideas. DL is a more sophisticated variation of ML that has its foundation on ANN. The DL technique is an important process in AI that is used to extract characteristics from data [9]. To avoid these difficulties, numerous IDSs have been implemented to identify attacks in WSN including maximum false alarm alert, low detection accuracy, as well as maximum processing time, still they are suffering. Moreover, the most important restrictions in WSNs are storage space, bandwidth, and power consumption. Mostly, the sensors are placed in an unattended position where the battery recharge or replacement becomes impossible [10]. Hence, this research proposes novel intrusion detection in WSN with improved class imbalance processing.

The main contribution of this work is as follows:

- Proposing improved data imbalance process to balance the data with SMOTE-ENN and Tomek link algorithm.
- Proposing improved correlation based features to extract the features from the pre-processed data accompanied with entropy based features is extracted.

The remaining part of this research including literature review on existing methods correspond to intrusion detection in WSN are explained in section 2. Then the proposed model of intrusion detection in WSN with improved class imbalance processing is described in section 3. Next, the results are discussed by conducting various experiments are analyzed in section 4. Further, the conclusion part is concluded in section 5 relevant to proposed model.

2. Literature Review

In 2021, Safaldin, M., et al [1] have suggested improved IDS with modified GWOSVM. The proposed model intended to enhance attack detection reliability and rate of identification while decreasing the duration of processing in the WSN system. This can be performed by lowering false alarm rates and the features set generated through IDSs in the WSN scenario. As a result, the presented model GWOSVM- IDS outperformed every one of the presented and scrutinized algorithms.

In 2021, Maheswari, M., & Karthika, R.A., [2] have developed a revolutionary safe uneven clustering technique with detection of intrusion that accomplished QoS metrics such as longevity, energy, and security. Moreover, an adaptive neural FCM was employed to select the TCHs based on three constraints comprises of distance to BS, distance to neighbours, and residual energy. Further, the TCHs then contend for the position of CHs, and optimal CHs were picked via DHO method.

In 2022, Zhang, T., et al [3] have implemented the TVP- IPSO technique, an evolutionary based strategy for low complexity intrusion detection in WSN. Furthermore, the PCA was used to minimize size of the dataset with suppressing the data to save energy. Also, high detection accuracy was assured with an IDS based on SVM. Besides, the convergences speed of the IDS was progressed with the suggested model.

In 2023, Salmi, S., & Oughdir, L., [4] have introduced deep learning based intrusion detection systems.

These systems were trained on a WSN-DS specific dataset to detect four forms of DoS assaults that affect WSNs. The Grayhole, Blackhole, Flooding, and Scheduling assaults were among them. Finally, the proposed approach assessed and contrasted the outcomes and discussed potential future projects.

In 2020, Zhang, W., et al [5] have proposed an organizational intrusion detection approach that groups nodes in a WSN based on their roles. Furthermore, in order to increase the detection precision of unusual activities in IDS while lowering the false alarm rate, the use of the classification algorithm of k-ELM, based on the Mercer Property, was considered in research to synthesize multi- kernel functions. By evaluating and implementing the multi- kernel function, the proposed model achieved the best linear combination and created a multi-k-ELM for IDS.

3. Implementing A Novel Intrusion Detection In WSN with Improved Class Imbalance Process

A. Proposed architect of intrusion detection in WSN

WSNs are a heterogeneous system made up of tiny actuators and sensors with general-purpose computer units. WSNs offer several advantages, mainly, the capability of transforming raw data into understandable categorized information. Moreover, while modelling the WSN, the key

B. Pre-processing

Consider the input data D is subjected to the pre- processing phase to obtain error free and denoised data. In this work, improved class imbalance process is employs to balance the raw data. For the improved class imbalance process, a novel SMOTE-ENN and Tomek link algorithm is deployed.

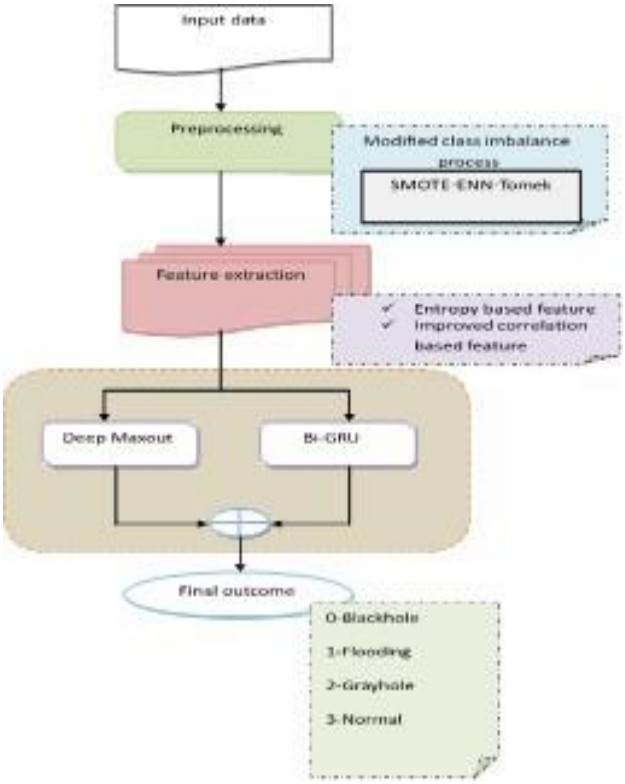


Fig. 1. Entire process of proposed model

1) SMOTE-ENN and Tomek link algorithm

The input data D is subjected to the SMOTE-ENN and Tomek link algorithm [12], in which the following

processes are performed. Let $f(D)$ be the function, which resolves the order. Initially, the degree of noise and overlapping is computed with k- DN and LDA, respectively. Then it finalize the outcome based on noise and overlap value. When the noise is higher than the overlap, then the function of order decision is resultant as 1. On the other hand, when the noise is lesser than the overlap, it is resultant as 0. Then the resampling method with their ratio and order are computed according to the measured values. Let $rm(D)$ be the ratio of resampling method, which are determined with ENN and $r_n^{(D)}$ be the ratio of resampling method, whichare determined with Tomek links. If the resultant is 1, then the SMOTE determines the imbalance by accomplishing the low level instances and also, the noise can be suppressed with ENN and eventually, the overlap is also suppressed with Tomek link. Moreover, based on the ratio of $r_m(D)$ and $r_n(D)$, the ENN and Tomek link ratio is evaluated with

the ratio determination function. Traditionally, the ratio of ENN and Tomek link is computed with ratio determination function but in this proposed work, information ratio is deployed instead of ratio determination function that can be stated as in Eq. (1). Here, for calculating r_m, the r_p takes D' and r_b takes D' value and then for calculating r_n, the r_p, takes D value and b takes D value.

$$InfoR = \frac{r_p - r_b}{\sigma_a - \sigma_b} \qquad (1)$$

2) Pseudo-code of proposed algorithm

Algorithm 1: SMOTE-ENN and Tomek link algorithm		
Input: D		
	Evaluate $kDN(D)$	
	Evaluate $LDA(D)$	
	If $kDN(D) - LDA(D) \geq 0$ **then**	
		$f(D) \leftarrow 1$
	else	
		$f(D) \leftarrow 0$
	end if	
	Evaluate $r_m(D)$ and $r_n(D)$	
	If $f(D) \geq 1$ **then**	
		$D' \leftarrow SMOTE(D)$
		$D'' \leftarrow ENN(D').r_m(D)$
		$D'' \leftarrow Tomek\ link(D'').r_n(D)$
	else	
		$D' \leftarrow SMOTE(D)$

		$D'' \leftarrow Tomek\ link(D').\ r_m(D)$
		$D''' \leftarrow ENN(D'').\ r_n(D)$
	end if	
return		
Output: D'''		

C. An overview on retrieving features including entropy and improved correlation-based feature

1) Entropy based feature:

The entropy based feature [11] is extracted from the pre-processed data D to evaluate the dissimilarity of non- linear and non-stationary time sequence. The traditional entropy can be formulated as in Eq. (2). Here, D_{pre} specifies pre-processed data, and $P(D^{pre})$ specifies probability of pre-processed data.

$$Ent = -\sum_{i=1}^{n} P\left(D^{pre}\right)^{2} * \log_2\left(P\left(D^{pre}\right)\right) \qquad (2)$$

2) Improved correlation based feature

Correlation is a measure that quantifies the strength of the association or relationship between two features from the pre-processed data D. It can be used to predict one feature from the other feature. The tradition Pearson correlation can be formulated as in Eq. (3).

$$Pcor = \frac{\sum(u-mu)(v-mv)}{\sqrt{\sum(u-mu)^2 \sum(v-mv)^2}} \qquad (3)$$

The above Eq. (3) is improved to correlate the best features highly for detecting the intrusion efficiently. Then the improved correlation can be formulated as in Eq. (4). Here,

u specifies u values, v specifies v values, mu refers to mean of u values, and mv refers to mean of v values.

$$IPcor = \frac{\sum(u-mu)(v-mv)}{\sqrt{\sum(u-mu)^2 \sum(v-mv)^2}} * CV \qquad (4)$$

Further, CV function is evaluated with the coefficient of variation can be formulated as in Eq. (5). Here, □ specifies standard deviation of pre-processed data and □ specifies mean of pre-processed data.

$$CV = \frac{\sigma}{\mu} \qquad (5)$$

Thereby, the entropy and correlation based features retrieved from the balanced data can be represented as $ext^F = \lceil \lfloor H(x), IPcor \rfloor \rceil$.

D. Intrusion detection

In the intrusion detection phase, the retrieved features ext F is subjected to the hybrid model of classifier to speed up the detection processing time that including Deep Maxout and Bi-GRU models. These features ext are fed into both classifiers to train the feature set. After train the features, the average outcome of both classifiers determines the final detection.

1) Deep Maxout

The Deep Maxout model [13] is a multilayer perceptron that deploys a maxout unit, which is a kind of activation function. The maxout hidden layer employs the function to generate maximum output function with the given retrieved features ext F can be stated as in Eq. (6).

$$h\left(ext^{F}\right)=\max_{j\in(1,k)} g_{ij} \qquad (6)$$

Where, $g_{ij} = ext^{\cdot}\ \varpi \quad + b^{\nu}\ \varpi \quad b^{\nu}$ ..... and

are the learned constraints. A maxout feature map is implemented with the consideration of maximum over k affine kernel map in the convolutional network. Also, the element-wise multiplication is applied in the dropout layer at the time of training the dropout. A piecewise linear approximation is performed for each maxout function, which makes the connection between the activation function of hidden layers.

2) Bi-GRU

In ANN, a gating mechanism is referred as GRU, which is equivalent to LSTM framework. The difference from LSTM network is this GRU analysis and provides better performance while considering low to medium level dataset.

In this work, the GRU deploys to train the retrieved feature ext ^{f}*. The GRU is implemented with the following equations that can be formulated as in EQ. (7). here,* H_t *indicates hidden state, u indicates update gate,* $\otimes$*indicates element-wise multiplication,* $\tilde{H}_t$ *indicates candidate gate,* H_t-1 indicates specifies hidden state input in the previous layer, σ refers to sigmoid function, ω refers to weight,B refers to bias vector, ^{rg} specifies reset gate and tanh indicates hyperbolic tangent function.

$$\begin{aligned} H_t &= u\otimes\tilde{H}_t+(1-u)\otimes H_{t-1} \\ u_t &= \sigma\left(\zeta_{uH} H_{t-1}+\zeta_{uext^{F}} ext^{F}_{t}+B_{u}\right) \\ H_t &= \tanh\left(\zeta_{Hext^{F}} ext^{F}_{t}+\zeta_{HH}\left(rg\otimes H_{t-1}\right)+B_{H}\right) \\ rg_t &= \sigma\left(\zeta_{rgH} H_{t-1}+\zeta_{rgext^{F}} ext^{F}_{t}+B_{rg}\right) \end{aligned} \qquad (7)$$

In Bi-GRU model [14], the input of prior and further available series are given as input to the model, which has two cell in terms of both forward and backward processing of input series. That is, the one cell considers the input in usual form of sequence whereas, the other cell considers the input in reverse form.

4. Results And Discussion

A. Simulation Procedure

The proposed intrusion detection in WSN was implemented in PYTHON and the WSN-DS dataset was gathered from [15]. In order to express the efficiency of the proposed model, it analyses the performance with benchmarking the existing classifiers like Deep Maxout, LSTM, RNN and DBN. Also, it is examined with the consideration of sensitivity, NPV, accuracy, FPR and other measures for distinct number of learning percentages.

B. WSN-DS Dataset Description

The WSN-DS dataset has been defined to gather data from Network Simulator 2 (NS-2) and then processed to produce 23 features, such as, JOIN-REQ-RCVD, JOIN- REQ-SENT, and so on. The collected dataset has been trained to classify different DOS attacks, including, Grayhole, Blackhole, scheduling attacks and Flooding.

C. Intrusion Detection analysis on proposed and traditional methods correspond to positive metric

The assessment on proposed is compared to the Deep Maxout, LSTM, RNN and DBN with considering the specificity, precision, accuracy and sensitivity for detecting the intrusion in WSN framework is displayed in fig 2. For the exact detection of intrusion, the model needs maximal positive metric ratings. Considering the fig 2(a), the proposed generated the greatest precision of 0.9102 in the learning rate 60%, whilst the Deep Maxout, LSTM, RNN and DBN scored the least precision rates of 0.8638, 0.7865, 0.8917 and 0.8816, respectively. Subsequently, the specificity of the proposed work is higher (0.9401) over the Deep Maxout, LSTM, RNN and DBN, as per fig 1(b). Additionally, the detection accuracy attained by the proposed is maximal in almost all the learning percentages. More particularly, while fixing the training percentage to 90%, the proposed obtained the accuracy rate of 0.9498, thought is higher than the Deep Maxout=0.8027, Bi- GRU=0.8667, LSTM=0.8420, RNN=0.8267 and

DBN=0.8165, correspondingly. In addition, the sensitivity of the proposed is much greater in the entire learning percentages. Thus, the proposed affirmed that their results are more precise and achieve the highest level of detecting accuracy. This enhancement is made possible by the Improved correlation based feature extraction as well as the hybrid model like Deep Maxout and Bi-GRU.

D. Intrusion Detection analysis on proposed and traditional methods correspond to negative metric

The negative measure evaluation on proposed and the established approach detecting the intrusion in WSN is shown in fig 3. Also, the proposed is compared with the models like Deep Maxout, LSTM, Bi-GRU, DBN and RNN in terms of FNR and FPR. Mainly, the proposed offered least negative measure ratings over extant strategies. In particular, the FPR of the proposed approach is 0.0987, whereas the Deep Maxout, Bi-GRU, LSTM, RNN and DBN hold the minimized FPR of 0.1991, 0.2937, 0.1568, 0.1739 and 0.2543, respectively. Further, at the training rate 90%, the proposed yielded the least FPR rate (0.1038) than the other 60, 70 and 80 training percentages. As we have performed intrusion detection using the enhanced derivation of feature with hybrid classifiers including Deep Maxout and Bi-GRU have accomplished superior negative metric findings. Thus, the hybrid algorithm's successful performing the functions and ensured to increase other metrics through an improved correlation

feature extraction method, which is much successful in detecting the intrusions.

E. Intrusion Detection analysis on proposed and traditional approach correspond to other metric

Fig 4 explains the other measure assessment on proposed over the Deep Maxout, RNN, Bi-GRU, LSTM, and DBN for intrusion detection in WSN. The other measure needs to be increased for the appropriate detection of intrusion in WSN framework. Further, for the training percentage 70%, the proposed accomplished the F-measure of 0.9243, mean while the Deep Maxout is 0.8504, Bi-GRU is 0.8127, LSTM is 0.8869, RNN is 0.8722 and DBN is

0.8438, respectively. Concerning the fig 4(b), the NPV of the proposed for the training rate 90% is 0.9378 with accurate detection of intrusion in WSN system.

F. Impact on proposed, model with devoid of improved correlation and model with devoid of feature extraction for Intrusion Detection in WSN

Table I explain the impact on model with devoid of improved correlation, model with devoid of feature extraction and proposed for the intrusion detection in WSN framework. Here, the proposed with improved correlation based feature extraction have provided superior outcomes with exact detection of intrusion in WSN framework. For instance, the accuracy of the proposed is 0.9366, model with devoid of improved correlation is 0.8976 and model with devoid of feature extraction is 0.8274. Additionally, the FNR obtained by the proposed=0.0889, model without improved correlation=0.1887 and model with devoid of feature extraction=0.1980, correspondingly. Consequently, the proposed acquired the greatest MCC (0.9300), Sensitivity (0.9230) and NPV (0.9198). Altogether, the improved correlation based feature extraction with hybrid classifiers method allows the proposed to detect the intrusion more appropriately.

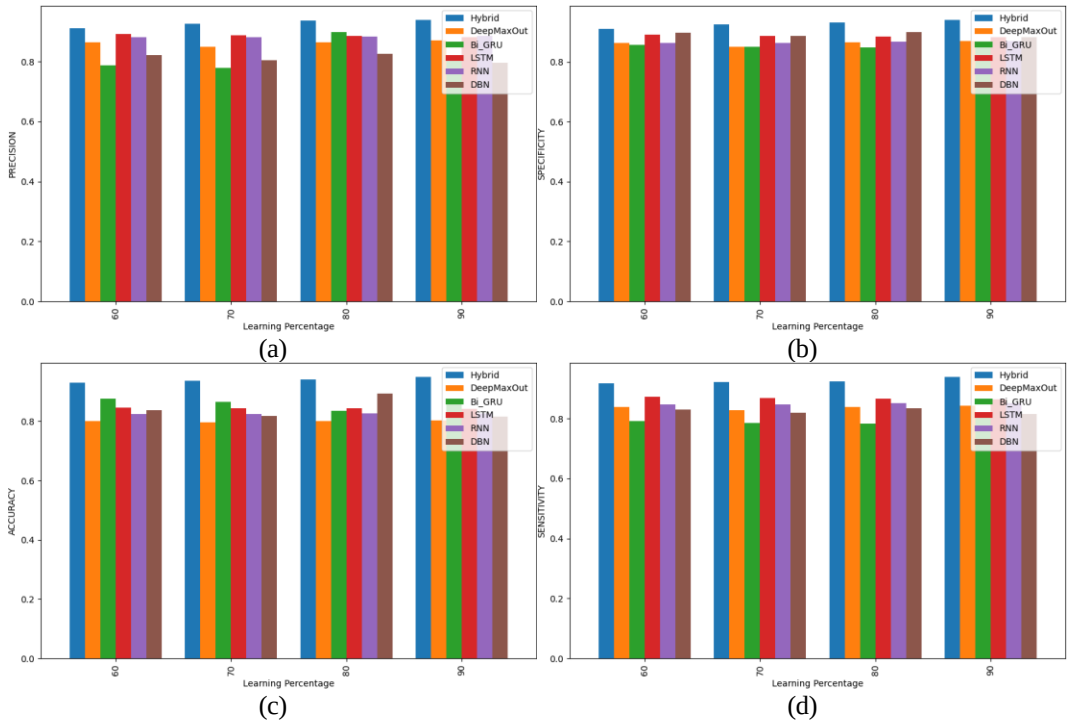


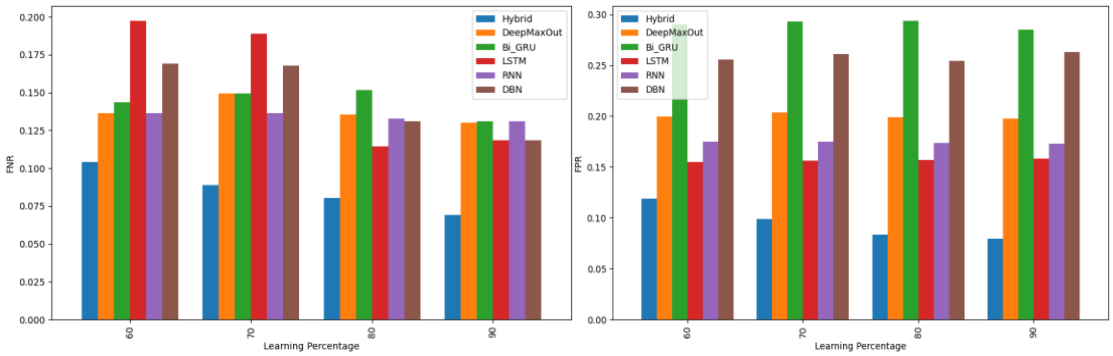
Fig. 2. Positive measure evaluation on proposed and conventional schemes for intrusion detection in WSN

G. Statistical evaluation on proposed and the existing methods for intrusion detection in WSN framework with respect to accuracy

The statistical study on proposed over the RNN, Deep Maxout, Bi-GRU, LSTM, and DBN for detecting the intrusion in WSN framework is illustrated in table II. Besides, it is assessed in terms of accuracy under numerous kinds of statistical measures.

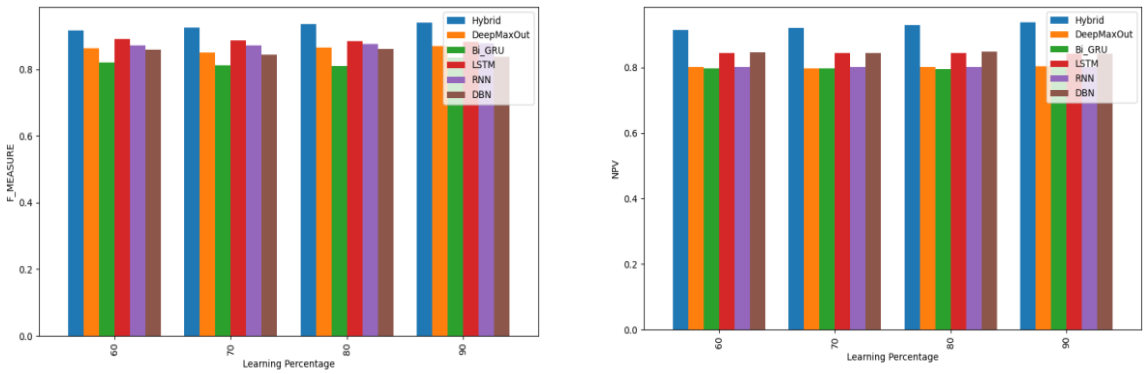
TABLE I. Impact On Proposed, Model Without Improved Correlation And Model Without Feature Extraction For Intrusion Detection In Wsn

Measures	Model without Improved Correlation	Model without feature extraction	Proposed
Sensitivity	0.8468	0.8368	0.9230
FNR	0.1887	0.1980	0.0889
F-measure	0.8177	0.8347	0.9244
Accuracy	0.8976	0.8274	0.9498
FPR	0.2032	0.1726	0.0987
Precision	0.8977	0.8918	0.9268
MCC	0.8848	0.8668	0.9300
NPV	0.7976	0.8282	0.9198
Specificity	0.8219	0.8737	0.9250

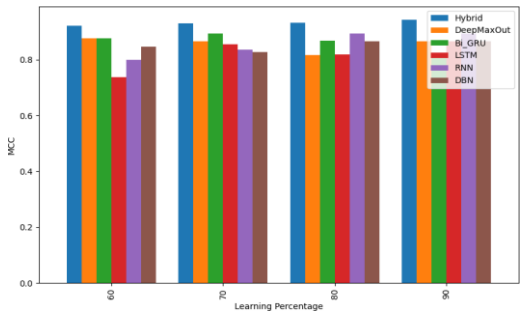


(a) (b)

Fig. 3. Negative measure evaluation on proposed and conventional schemes for intrusion detection in WSN



(a) (b)



(c)

Fig. 4. Other measure evaluation on proposed and conventional schemes for intrusion detection in WSN

In particular, the proposed obtained the accuracy ratings of 0.9295 at the minimum statistical measure, this is considerable greater than Deep Maxout=0.9295, Bi- GRU=0.7963, LSTM=0.8421, RNN=0.8249 and DBN=0.8166, respectively. Additionally, evaluating the median statistical measure, the accuracy of the proposed is 0.9389, whereas the Deep Maxout, Bi-GRU, LSTM, RNN and DBN hold the least accuracy ratings. Finally, under the statistical measure analysis, the proposed determined to be more effective than the conventional methods for intrusion detection in WSN framework.

TABLE II. Statistical analysis on proposed and the extant strategies with regard to accuracy for intrusion detection in WSN

Statistical Measures	Proposed	Deep Maxout	Bi-GRU	LSTM	RNN	DBN
Mean	0.9393	0.8001	0.8607	0.8435	0.8257	0.8409
Median	0.9389	0.8007	0.8657	0.8434	0.8256	0.8272
Stand ard Deviation	0.0074	0.0023	0.0150	0.0011	0.0008	0.0309
Minimum	0.9295	0.7963	0.8358	0.8421	0.8249	0.8166
Maximum	0.9498	0.8027	0.8757	0.8451	0.8268	0.8927

5. Conclusion

This paper proposed intrusion detection in WSN with improved class imbalance processing. Initially, the input data was pre-processed to balance the data with improved imbalance process, in which SMOTE-ENN-Tomek technique was employed. Then the features such as entropy and improved correlation based features were retrieved from the pre-processed data. Further, these features were subjected to the hybrid model, which including Deep Maxout and Bi- GRU classifiers and then the classifiers outcome predicted the attack detection. More particularly, while fixing the training percentage to 90%, the proposed obtained the accuracy rate of 0.9498, thought is higher than the Deep Maxout=0.8027, Bi-GRU=0.8667, LSTM=0.8420,

RNN=0.8267 and DBN=0.8165, correspondingly.

References

[1] Safaldin, M., Otair, M. & Abualigah, L., “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, 2021. https://doi.org/10.1007/s12652-020-02228-z

[2] Maheswari, M., & Karthika, R.A., “A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks”, Wireless Pers Commun, vol. 118, pp. 1535–1557, 2021. https://doi.org/10.1007/s11277-021-08101-2

[3] Zhang, T., Han, D., Marino, M.D., Lin Wang & Kuan-Ching Li, "An Evolutionary-Based Approach for Low-

Complexity Intrusion Detection in Wireless Sensor Networks", Wireless Pers Commun., vol. 126, pp. 2019–2042, 2022. https://doi.org/10.1007/s11277-021-08757-w

[4] Salmi, S., & Oughdir, L., "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network", J Big Data, vol. 10, 2023. https://doi.org/10.1186/s40537-023-00692-w,

[5] Zhang, W., Han, D., Li, KC., & Francisco Isidro Massetto, "Wireless sensor network intrusion detection system based on MK-ELM", Soft Comput., vol. 24, pp. 12361–12374, 2020.https://doi.org/10.1007/s00500-020-04678-1

[6] Umarani, C., Kannan, S., "Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network", Peer-to-Peer Netw. Appl., vol. 13, pp. 752–761, 2020. https://doi.org/10.1007/s12083-019-00781-9

[7] Ghosh, D., Sharma, A., Shukla, K.K., "Globalized robust Markov perfect equilibrium for discounted stochastic games and its application on intrusion detection in wireless sensor networks: Part I—theory", Japan J. Indust. Appl. Math., vol. 37, pp. 283–308, 2020. https://doi.org/10.1007/s13160-019-00397-9

[8] Fotohi, R., Firoozi Bari, S., "A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms", J Supercomput., vol. 76, pp. 6860– 6886, 2020. https://doi.org/10.1007/s11227-019-03131-x

[9] Mohd, N., Singh, A. & Bhadauria, H.S., "A Novel SVM Based IDS for Distributed Denial of Sleep Strike in Wireless Sensor Networks", Wireless Pers Commun., vol. 111, pp. 1999–2022, 2020. https://doi.org/10.1007/s11277-019-06969-9

[10] Ramesh, S., Yaashuwanth, C., Prathibanandhi, K., Adam Raja Basha &T. Jayasankar, "An optimized deep neural network based DoS attack detection in wireless video sensor network", J Ambient Intell Human Comput., 2021. https://doi.org/10.1007/s12652-020-02763-9

[11] Saif Nalband, Amalin Prince, & Anita Agrawal, "Entropy-based feature extraction and classification of vibroarthographic signal using complete ensemble empirical mode decomposition with adaptive noise", IET Science, Measurement & Technology, 2017. doi: 10.1049/iet- smt.2017.0284

[12] Taisho Sasadaa, Zhaoyu Liuc, Tokiya Bababb, Kenji Hatanod, & Yusuke Kimura, "A Resampling Method for Imbalanced Datasets Considering Noise and Overlap", Procedia Computer Science, vol. 176, 2020.

[13] Jyothi Peta and Srinivas Koppu, "An IoT-Based Framework and Ensemble Optimized Deep Maxout Network Model for Breast Cancer Classification", Electronics, vol. 11, 2022. https://doi.org/10.3390/electronics11244137

[14] Medari Janai Tham, "Bidirectional GRU for Shallow Parsing", Indian Journal of Computer Science and Engineering, vol. 11, pp. 517-521, 2020. DOI:10.21817/indjcse/2020/v11i5/201105167 Iman Almomani, Bassam Al-Kasasbeh, and Mousa AL-Akhras, "WSN- DS: A dataset for intrusion detection systems in wireless sensor networks", Journal of Sensors, 2016.