Measurement: Sensors 26 (2023) 100578

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

Fuzzy based intrusion detection system in MANET

C. Edwin Singh *, S. Maria Celestin Vigila

Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, India

ARTICLE INFO

Keywords:
Mobile adhoc network
Intrusion detection system
Security
Fuzzy extreme learning
Principal component analysis
Knowledge discovery and data mining tools competition

ABSTRACT

The rapid development and popularization of the Mobile Adhoc Network (MANET) have brought many security issues in network. Intrusion detection system, an effective security technology which can efficiently detect malicious data in complex network environments and ensure computer network security. Because of the complexity of MANET, traditional Intrusion Detection system IDSs are ineffective in this new context, several methods including Support Vector Machine (SVM) have been used to detect intrusion. Most existing technologies strive for low execution times and energy efficiency while achieving accurate detection rates. To overcome these disadvantages, a novel Principal Component Analysis based Fuzzy Extreme learning machine (PCA-FELM) has been proposed in this paper. Initially, the features are extracted by using Principal Component Analysis and then the extracted features are classified by using Fuzzy Extreme Learning Machine. The proposed PCA-FELM is implemented using MAT LAB simulator. The proposed PCA-FELM is compared with existing methods such as DBN-IDS, GOA-SVM and SDAE-ELM and the proposed method achieves higher accuracy of 99.08% than other existing methods. Experiments on the Knowledge Discovery and Data Mining Tools Competition, KDD Cup99 dataset show that the proposed PCA-FELM model have superior performance than other existing techniques.

1. Introduction

A MANET, is made up of a huge number of wireless nodes which are connected in a network for a set amount of time in order to communicate, with no specific infrastructure or administration [1]. MANETs have several advantages over networks without a permanent design, including the ability to build an ad hoc network anywhere with mobile devices, the ability to easily add more nodes to the network, and cheaper administrative costs [2,3].

The absence of memory, power, and weight distinguishes mobile nodes. Because there is no centralized management over the network, wireless networks have more security vulnerabilities than wired networks [4,5]. Because of the dispersed nature, security vulnerabilities are more prevalent, including routing, configuration, and the lack of an intrusion technique [6]. MANETs are more vulnerable than agitated networks due to movable networks, vulnerabilities from compromised nodes in a network, weak body encryption, fluctuating layout, extensibility, and absence of leadership [7,8].

IDS is an important target that focuses on computer and network security research. An IDS is designed to warn network users of malicious user behaviour [9,10]. One of the most serious network security issues is infiltration, which occurs when a persistent unauthorized user steals or destroys data from legitimate users or the MANET [11–14]. Today's IDS technologies come in a variety of shapes and sizes [15]. The IDS technologies are separated into four categories, such as Host-based IDS (HIDS) [16], Network-based IDS (NIDS) [17], Wireless-based IDS (WIDS) [18], Network Behaviour Analysis (NBA) [19], and Mixed IDS (MIDS) [20] each of which is used to identify anomalous behaviours and detect network activity.

Because of the complexity of MANET, traditional IDSs are ineffective in this new context. Nodes in movable networks may depart and re-join the association at any time. As a result, a network with a dynamic topology is formed. Because there is no established framework, it is complicated to discern flanked by trusted and non-trusted nodes and an interloper may quickly join the network and launch attacks.

To overcome this challenge, this paper proposes a novel PCA based Fuzzy Extreme learning machine (PCA-FELM) in MANET. The main contributions of the proposed, a novel Principal Component Analysis based Fuzzy Extreme learning machine (PCA-FELM) technique are given as follows. The remaining portions of the research are structured as follows:

* Corresponding author.
E-mail address: edwinspapers@gmail.com (C. Edwin Singh).

https://doi.org/10.1016/j.measen.2022.100578
Received 16 September 2022; Received in revised form 29 October 2022; Accepted 19 November 2022
Available online 6 December 2022

- The major aim of PCA-FELM is to detect the intrusion using ML features as inputs to distinguish and classify the nodes misbehaviour patterns.
- Initially, the features are extracted by using Principal Component Analysis and then the extracted features are classified by using Fuzzy Extreme Learning Machine.
- PCA-FELM feature can make use of such strategy in all Green Smart Transportation network scenarios.
- KDD Cup99 dataset show that the suggested PCA-FELM method have superior performance than other existing techniques.

The remainder of the paper is structured as follows. A detailed explanation of the literature review is described in Section II. The proposed method is described in Section III. The results and discussion are described in Section IV. The conclusion is covered in Section V.

2. Literature survey

Due to mobility nodes, malicious nodes are present inside the network. Because of these weaknesses, MANET is more likely to be attacked by malicious entities. So, many researchers gave an attempt to detect intrusion detection in MANET by using machine learning and deep learning methods. Among those, only a few methods have been examined in this section.

In 2019 Wei, P., [21], proposed a new concurrent optimization strategy for enhancing the structure of DBN in the context of a DBN-based intrusion detection classification model (DBN-IDS) optimization problem. The proposed method optimizes DBN network setup in the hidden layer range with a limited number of hidden layers.

In 2019, Ye, Z., et al. [22] proposed a support vector machine based on the Grasshopper Optimization method (GOA-SVM) to augment Support Vector Machine (SVM) precision in vulnerability scanning. In order to increase the precision of SVM in detecting intrusion, this paper introduces GOA-SVM and utilizes it to invasion diagnosis. According to the experimental results, this method performs better than existing methods.

In 2019, Gao, J., et al. [23] provided a robust network intrusion detection system based on the Extreme Learning Machine (ELM) and Multi-Voting Technology (MVT). Numerous different ELM networks can be developed at the same time because to ELM's real-time capability. The proposed method in this study can achieve detection accuracy while using the extensive information set in a much shorter period.

In 2020, Thirumalairaj, A. and Jeyakarthic, M., [24], presented a new Hybridization of a Cuckoo Search Tuning Method for Deep Neural Network (HCSTS-DNN). The HCSTS technique given here tunes the parameters of a DNN structure that consists of several auto encoder layers cascaded to an SM classification layer. The tough dataset is used to determine the presence of intrusions once the model has been trained and the proposed method showed better results.

In 2021, Wang, Z., et al. [25] provided an innovative deep intrusion detection model based on SDAE-ELM to eliminate the intensive training time and less configuration precision of existing DNN models, as well as to enable quick reply to malicious behaviour. According to the experimental results, this method performs better than existing methods.

In 2021 Rao, P.V., et al. [26] proposed an adaptive network-based fuzzy inference system (ANFIS) with a Bloom Filter by using legitimate nodes' identities as cover, this attack has the ability to undermine faith in them, disrupt packet routing, and other issues that could lead to network confusion. The results of this experiment demonstrate that the overhead of simultaneously hearing all nodes is reduced by the suggested strategy. It will be possible to listen to every node for half as much money.

In 2022 Ali, M., et al. [27] proposed hybrid ACO-OSELM outperformed the counterpart models for wheat yield prediction. The ACO-OSELM model outperformed the ACO-ELM and ACO-RF models. The hybrid ACO-OSELM model demonstrated its ability to be executed as a decision-making system for crop yield prediction in regions where a significant association with the historical agricultural crop is very well.

According to the Literature Review they have some drawbacks such it is found that most of the existing models network structure is simple, and lacking pertinence and some existing model have less accuracy. To overcome these drawbacks, a novel Principal Component Analysis based Fuzzy Extreme learning machine (PCA-FELM) has been proposed.

3. Proposed method

The proposed intrusion detection system discovers the attacks by using PCA-FELM model that employs PCA for feature extraction and Fuzzy ELM for classification. The overall representation of the proposed PCA-FELM model has been shown in Fig. 1.

3.1. Principal Component Analysis

PCA is a dimensionality-decline technique that reduces the dimensionality of large data sets by modifying an outsized compilation of

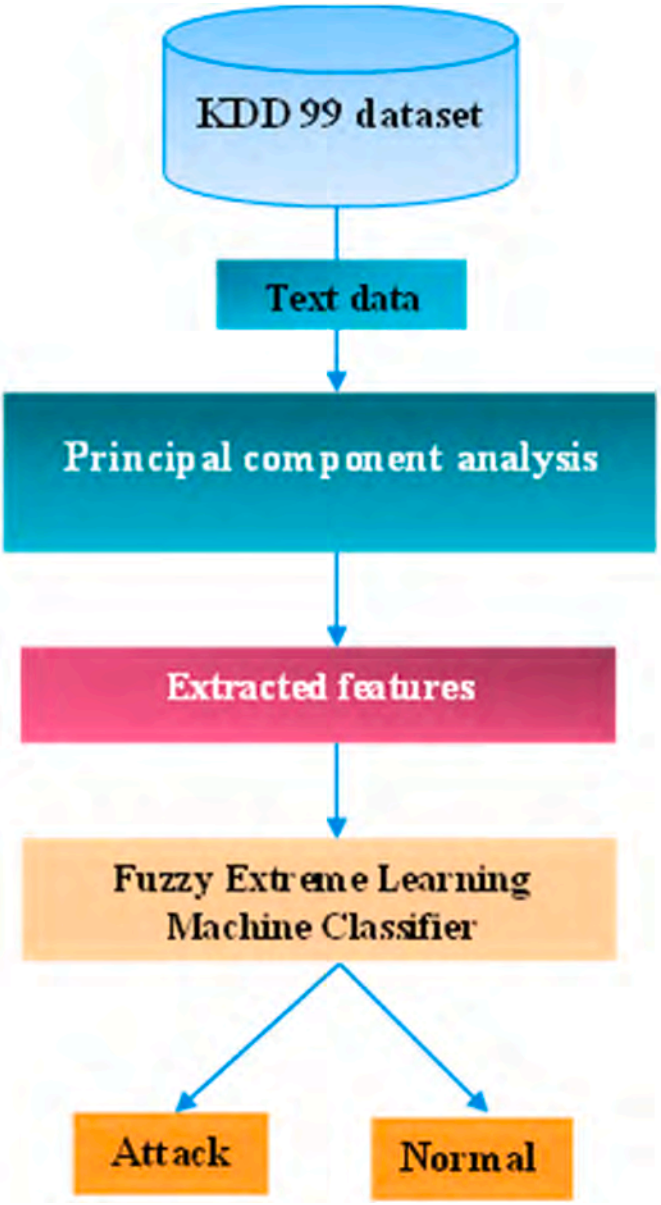

Fig. 1. Block diagram for proposed E-FELM model.

variables into a smaller set that preserves the bulk data in the larger set. A linear combination of random variables is called a principal component (PC) v_1, v_2, …v_p in algebra, However, in geometry, a linear combination refers to the creation of a new coordinate by rotating the old point v_1, v_2 …, v_p. The covariance matrix is used in the PCA, Σ or correlation matrix ρ of v_1, v_2 …, v_p only. The random variable v' = [v_1, v_2 …, v_p], covariance matrix Σ and eigen value $\lambda_1 \geq \lambda_2 \geq \ldots. \geq \lambda_p$. The linear combination.

$$Y1 = a'1V = a11V1 + a12V2 + \ldots.a1pVp \quad (1)$$

$$Y2 = a'2V = a21V1 + a22V2 + \ldots a2pVp \quad (2)$$

$$Y_p = a'_pV = a_{p1}V_1 + a_{p2}V_2 + \ldots.a_{pp}V_p \quad (3)$$

So, variance $\mathrm{Var}(Y_i)$ and covariance $\mathrm{Cov}(Y_i, YK)$ is

$$\mathrm{Var}\ (Yi) = ai,\Sigma ai;\ i = 1, 2\ldots p \quad (4)$$

$$\mathrm{Cov}\ (Y_i, Yk) = a_{i,}\Sigma a_k;\ i = 1, 2\ldots.p \quad (5)$$

The steps in PCA are.

1. Consistency: This phase is employed to normalize the variety of incessant initial variables and hence they all supply evenly to the analysis.

$$Z = \frac{Value - mean}{Standard\ deviation} \quad (6)$$

2. Calculation of the covariance matrix: This set is used to see if there is a link between both the factors in the input data set that deviate from of the mean. For a 2-dimensional data set with two variables x and y, the covariance matrix is a 2 x 2 matrix of the following form:

$$\mathrm{cov}\ (x, x)\ \mathrm{cov}\ (x, y)$$

$$\mathrm{cov}\ (y, x)\ \mathrm{cov}\ (y, y)$$

3. Computing Eigen values and Eigen Vectors: The linear algebra concepts of Eigenvectors and Eigen values should be derived from the covariance matrix in attempt to discover the principal gears of the facts.
4. Characteristic Vector: In this stage, the decision is made whether to preserve all of these components or to reject the ones that aren't as important, and then comprise the residual ones into a matrix of vectors referred to the characteristic vector.
5. Recasting the data: The primary aim would be to employ the trait vector created by the eigenvectors of the convolution to reposition the information from the unique axis to the ones illustrated by the principal components. Multiply the transposed original data set by the classification model flip.

$$\text{Final data} = \text{Characteristic Vector}^T\ *\ \text{Standard Data}^T \quad (7)$$

After the features of the data has been extracted, the extracted data will be classified using the Fuzzy ELM technique.

3.2. Fuzzy Extreme learning

The Extreme Learning Machine (ELM) Single Hidden Layer Feedforward Neural Network (SLFN) was created to address the issue with single hidden layer feedforward neural networks. Then they were expanded to include SLFNs without hidden layers resembling neurons. The fuzzy ELM is employed in the proposed model, that is on the basis of conventional ELM. ELM is a good learning strategy because it has a high accuracy rate. There may be a chance of not exactly assigning input feature points to a class due to imbalance or weighted classification issues. Conventional ELMs are not capable of solving these problems. As part of the proposed model, a fuzzy ELM has been added to increase performance. For classification, FELM uses the extracted features from the PCA. The consequences of the training points would change depending on the weights in categorization inconvenience in the real world. A set of labelled training points, including (b_1, l_1, x_1) … (b_m, l_m, x_m), is combined with a fuzzy membership. For each training point b_j, a label l_j and a fuzzy membership $\sigma \leq x\_j \leq 1$ with an appropriately small $\sigma > 0$ is known.

$1/2||\xi\_j\ ||$ is the measurement of error, and fuzzy membership x_j is the location of the corresponding point a_j to a class. A limited fuzzy ELM's categorization conundrum can be explained as follows:

$$\mathrm{mini}:\ H = 1\ 2\ ||\beta||2 + d\ 1\ 2\sum \mathrm{xj}\ ||\xi||2\ \mathrm{m}\ \mathrm{j} = 1$$

$$\mathrm{sub\ to}:\ G\ (\mathrm{aj})\ \beta = \mathrm{kj}\ \mathrm{K} - \xi \mathrm{jK}\ \ldots\ldots\ldots\ldots \quad (8)$$

Here, i-1,2 ……, m. Based on the KKT theorem, training fuzzy ELMs is equivalent to solving a dual optimization problem.,

$$H = 1\ 2\ ||\beta||2 + d\ 1\ 2 \times \sum \mathrm{xj}\ ||\xi||\mathrm{m}\ 2\ \mathrm{j} = 1 - \sum\sum \alpha \mathrm{j}(\mathrm{G}(\mathrm{bj}\ )\beta \mathrm{i} - \mathrm{kj} + \xi \mathrm{j})\ \mathrm{n}\ \mathrm{j} = 1\ \mathrm{m}\ \mathrm{j} = 1\ \ldots\ldots.. \quad (9)$$

In terms of optimality conditions for the G derivation based on the KKT be,

$$\partial H \partial \beta = \beta - \sum \alpha \mathrm{j}\mathrm{G}(\mathrm{aj})\ \mathrm{m}\ \mathrm{K} = 0 \Longrightarrow \beta = \mathscr{H}\mathrm{K}\ \mathrm{j} = 1\ \alpha\ \ldots\ldots\ldots \quad (10a)$$

$$\partial H \partial \xi = \mathrm{dxj}\xi \mathrm{j} - \alpha \mathrm{j} = 0 \Longrightarrow \alpha \mathrm{j} = \mathrm{dxj}\xi \mathrm{j}\ \ldots\ldots\ldots \quad (10b)$$

$$\partial H \partial \alpha = \mathrm{G}(\mathrm{bj}\ )\beta - \mathrm{Kj}\ \mathrm{k} + \xi \mathrm{j}\ \mathrm{K} = 0 \Rightarrow \mathscr{H}\beta - \mathrm{Kj}\ \mathrm{k} + \xi \mathrm{j}\ \mathrm{K}\ \ldots\ldots\ldots \quad (10c)$$

To make equation (11) equivalent, consider substituting equations (10a), (10b), and (10c). (11)

$$\mathrm{X}\ \mathrm{d} + \mathscr{H}\mathscr{H}\mathrm{K})\ \alpha = \mathrm{K}\ \ldots\ldots\ldots\ldots \quad (11)$$

By combining equations (10a) and (11)

$$\beta = \mathscr{H}\mathrm{K}\ (\mathrm{Ad} + \mathscr{H}\mathscr{H}\mathrm{K}) - 1\ \mathrm{K}\ \ldots\ldots\ldots\ldots \quad (12)$$

As a result, The learning rate of the target weights can vary depending on the unique fuzzy matrices of the inputs. The target function of the FELM classifier can be expressed as follows:

$$(\mathrm{b}) = \mathrm{G}(\mathrm{b})\beta = \mathrm{G}(\mathrm{b})\mathscr{H}\mathrm{K}\ (\mathrm{X}\ \mathrm{d} + \mathscr{H}\mathscr{H}\mathrm{K}) - 1\ \mathrm{K}\ \ldots\ldots\ldots\ldots\ldots\ldots \quad (13)$$

For the discovered class label, the performance index for the output units with the highest value is used. The fuzzy matrix Z can also be adapted flexibly based on the model. An attack or normal is the output are generated by the FELM.

4. Results and discussion

To implement the experimental setup of this paper, we used the MATLAB 2019b machine learning toolbox. Based on the KDD 99 dataset, the PCA-FELM has been constructed to identify malicious nodes. The training data set includes 11.34% of each type's instances, with the exception of the U2R class, which covers 51.45% of the test cases. PCA-FELM used the KDD dataset to create a training dataset that included 10.12% of the preliminary cases, with the remaining 90.86% being used

Table 1
KDD Dataset for Training and Testing data.

Class	Training DataSet	Test Dataset
Normal	9192	81292
PRB	250	2241
U2R	39	49
R2L	123	928
DoS	5819	51345

in the testing procedure. The occurrences used in the research training sets of data used in our findings are represented in Table 1.

Table 2 lists the parameters and values used to evaluate the design for each dataset. The Mean-F-Measure (σ- FM) approach was used to suggest the adequacy of our model.

4.1. Performance analysis

When evaluating and comparing the QoS model, the performance measures are taken into account.

- Precision (P) = $TP/(TP + FP)$, this is the part of classification invasions that really happen
- Recall (R) = $TP/(TP + FN)$, this is the fraction of successfully anticipated intrusions in the overall number of intrusions
- *Accuracy* (A) = $TP + TN/TP + TN + FP + FN$, which can be defined as the percentage of correctly classified instances.

The ROC curve for the PCA-FELM model is shown in Fig. 2. As a result, the normal and attack classifications are both increased by 0.990 and 0.978, respectively.

Fig. 3 depicts the accuracy curve for the suggested PCA-FELM model. From the graph, it is found that the execution of the proposed PCA-FELM model enhances as the epoch value increases. Fig. Fig. 4 illustrates how the model loss decreases as epoch increases. As a result, the model accurately predicted the results. This research calculated the number of training epochs required to get the maximum test accuracy. Throughout training epochs, 99.6% of the classifications were accurate.

The cumulative performance of both the adaptive and static methods is depicted in Fig. 5. The adaptive strategy's reign is supported by all preventative measures. Aside from the accuracy and Attack Detection Ratio parameters, the remaining metrics demonstrate that the proposed PCA-FELMS strategy is superior. The suggested PCA-FELMS technique efficiently coordinates Recall and Precision in dataset class, according to the statistic.

4.2. Comparative analysis

In order to demonstrate the high accuracy of each machine learning classifier's output, its classification performance was evaluated. Table 3 shows the comparison of proposed technique with traditional ML classifiers. When classifying objects, each classifier's specificity, sensitivity, and accuracy are considered, and the PCA-FELM classifier has a 99.8% accuracy rate. According to the classification accuracy rate given in Table 3, the proposed method is more effective than currently available machine learning classifiers. Several ML classifiers, including Naive Bayes, Random Forest, Multilayer Perceptrons, and NB trees, are compared to the PCA-FELM.

Fig. 6 shows that PCA-FELM produces more accurate results than conventional classifiers. As a result, the proposed technique was shown to be much more effective than existing models. By combining PCA with FELM classifier, the accuracy rate is higher than currently used models. Three other models are compared to the proposed model.

The suggested PCA-FELM method is compared with existing techniques such as DBN-IDS [21], GOA-SVM [22], and SDAE-ELM [25]. As shown in Fig. 7, the PCA-FELM outperforms the existing models while maintaining a 99.8% accuracy range.

Table 2
Test parameter values for each dataset.

Symbol	Parameters	KDD Dataset
Class	List of Class	8
β	Beta value	45
σ	SD	4
F	List of features	27
I	No.of Iterations	1500

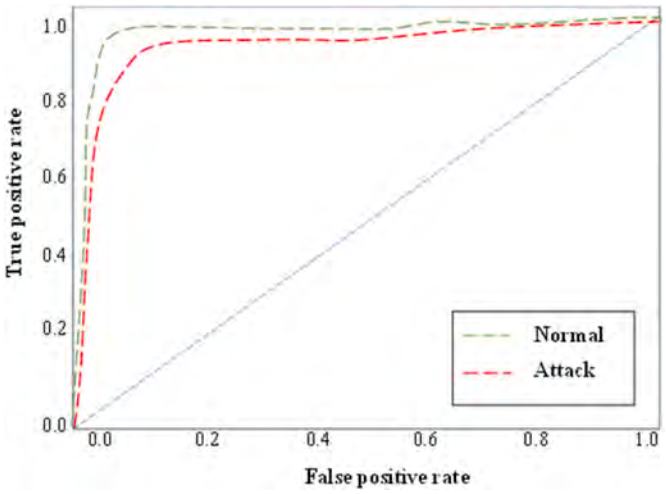

Fig. 2. ROC curve for the proposed PCA-FELM model.

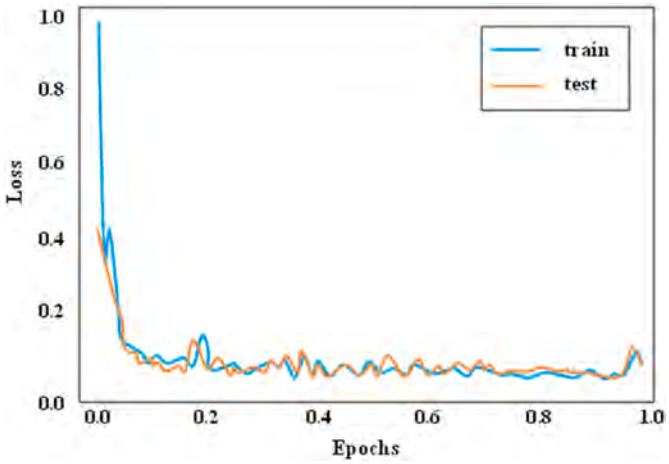

Fig. 3. Loss graph for testing training of PCA-FELM model.

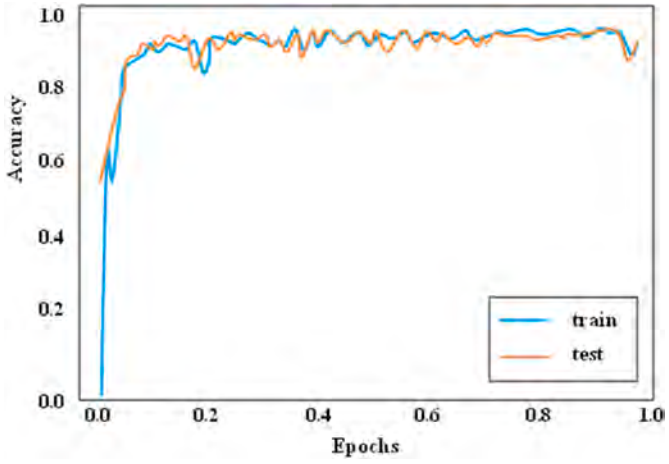

Fig. 4. Accuracy graph for testing training of PCA-FELM model.

Fig. 8 shows the performance comparison of proposed method with different datasets. From Fig. 3, it is clear that the proposed PCA-FELM produces more accurate results than conventional classifiers. As a result, the dataset technique was shown to be much more effective than

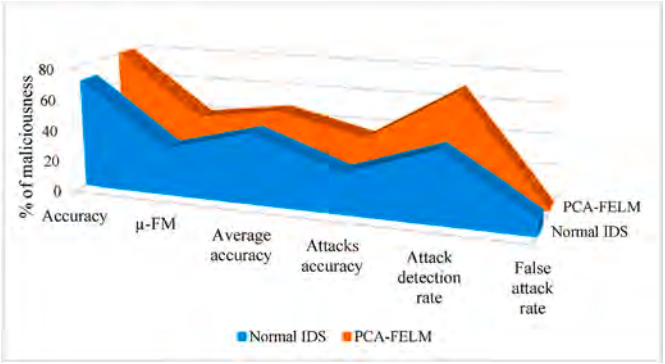

Fig. 5. Percentage of maliciousness in performance analysis.

Table 3
Comparison of proposed model with traditional ML classifiers.

ML Classification	Precision	Recall	Accuracy
Naïve Bayes	0.718	0.682	0.929
Random Forest	0.918	0.9387	0.993
Multilayer Perception	0.827	0.729	0.937
NB Tree	0.891	0.791	0.948
PCA-FELM	0.920	0.9412	0.998

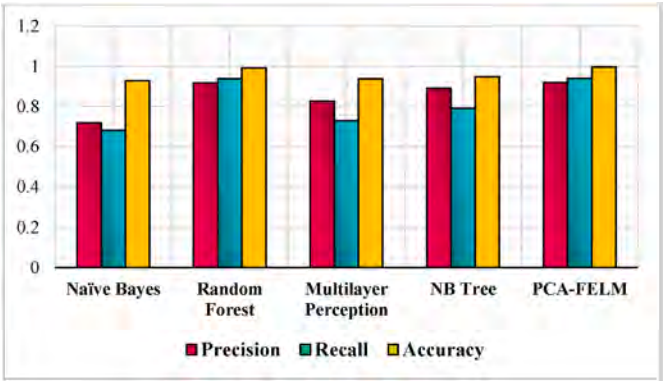

Fig. 6. Performance comparison of four ML classifiers.

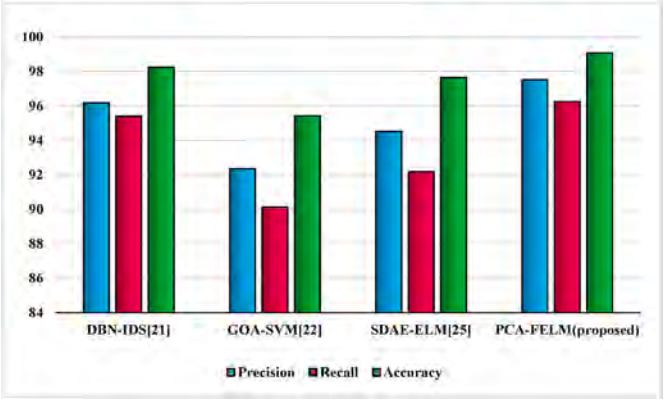

Fig. 7. Performance comparison of PCA-FELM with existing methods.

existing models. By combining KDD CUP 99, NSL-KDD and Giga Word Corpus with FELM classifier, the accuracy rate is higher than currently used models. Three other models are compared to the proposed dataset.

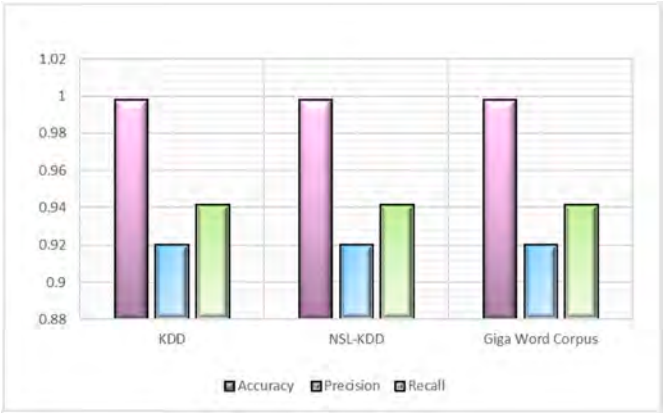

Fig. 8. Performance Comparison of proposed method with different datasets.

5. Conclusion

In this paper a novel Principal Component Analysis based Fuzzy Extreme learning machine (PCA-FELM) has been proposed. Initially, the features are extracted by using Principal Component Analysis and then the extracted features are classified by using Fuzzy Extreme Learning Machine. In this way, network security can be improved by increasing detection rates. The proposed PCA-FELM is implemented using MAT LAB simulator. The proposed PCA-FELM is compared with existing methods such as DBN-IDS, GOA-SVM and SDAE-ELM and the proposed method achieves higher accuracy of 99.08% than other existing methods. Experiments on the KDD Cup99 dataset show that the suggested PCA-FELM model have superior performance than other existing techniques. By adding more parameters to the proposed attack detection technique, the system will soon be improved to identify more number of network attacks. Future work may take into account various attacks to enhance network performance. In order to prevent network failure and unwanted compute overhead in addition to these attacks, preventative mechanisms can be included.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgements

The author with a deep sense of gratitude would thank the supervisor for his guidance and constant support rendered during this research.

References

[1] S. Singh, A. Pise, O. Alfarraj, A. Tolba, B. Yoon, A Cryptographic Approach to Prevent Network Incursion for Enhancement of QoS in Sustainable Smart City Using MANET, vol. 79, Sustainable Cities and Society, 2022, 103483.
[2] S. Dalal, B. Seth, V. Jaglan, M. Malik, N. Dahiya, U. Rani, D.N. Le, Y.C. Hu, An adaptive traffic routing approach toward load balancing and congestion control in Cloud–MANET ad hoc networks, Soft Comput. 26 (11) (2022) 5377–5388.
[3] O. Faker, E. Dogdu, Intrusion detection using big data and deep learning techniques, in: Proceedings of the 2019 ACM Southeast Conference, 2019, April, pp. 86–93.
[4] S. Rajabi, S. Jamali, J. Javidan, An intrusion detection system in computer networks using the firefly algorithm and the fast learning network, Int. J. Wine Res. 3 (1) (2020) 50–56.
[5] S. Kanthimathi, J.R. Prathuri, Classification of misbehaving nodes in MANETS using machine learning techniques, in: 2020 2nd PhD Colloquium on Ethically

Driven Innovation and Technology for Society (PhD EDITS), IEEE, 2020, November, pp. 1–2.
[6] M.R. Ghori, T.C. Wan, G.C. Sodhy, Bluetooth low energy mesh networks: survey of communication and security protocols, Sensors 20 (12) (2020) 3590.
[7] H.M.A. Fahmy, Wireless sensor networks essentials, in: Wireless Sensor Networks, Springer, Cham, 2020, pp. 3–39.
[8] S.S.S. Sugi, S.R. Ratna, Investigation of machine learning techniques in intrusion detection system for IoT network, in: 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), IEEE, 2020, December, pp. 1164–1167.
[9] H. Zhang, K.Y. Lin, W. Chen, L. Genyuan, Using machine learning techniques to improve intrusion detection accuracy, in: 2019 IEEE 2nd International Conference on Knowledge Innovation and Invention (ICKII), IEEE, 2019, July, pp. 308–310.
[10] Y. Koizumi, Y. Kawaguchi, K. Imoto, T. Nakamura, Y. Nikaido, R. Tanabe, H. Purohit, K. Suefusa, T. Endo, M. Yasuda, N. Harada, Description and Discussion on DCASE2020 Challenge Task2: Unsupervised Anomalous Sound Detection for Machine Condition Monitoring, 2020 *arXiv preprint arXiv:2006.05822*.
[11] A. Divekar, M. Parekh, V. Savla, R. Mishra, M. Shirole, Benchmarking datasets for anomaly-based network intrusion detection: KDD CUP 99 alternatives, in: 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), IEEE, 2018, October, pp. 1–8.
[12] N. Singh, A. Dumka, R. Sharma, A novel technique to defend DDOS attack in manet, J. Comput. Eng. Inf. Technol. 7 (2018) 5, https://doi.org/10.4172/2324.*9307*, p.2.
[13] S. Kanthimathi, J.R. Prathuri, Classification of misbehaving nodes in MANETS using machine learning techniques, in: 2020 2nd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS), IEEE, 2020, November, pp. 1–2.
[14] T.V. Nguyen, T.N. Tran, T. Huynh-The, B. An, An Efficient QoS Routing Protocol in Cognitive Radio MANETs: Cross-Layer Design Meets Deep Reinforcement Learning, 2021.
[15] S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, H. Karimipour, Cyber intrusion detection by combined feature selection algorithm, J. Inf. Secur. Appl. 44 (2019) 80–88.
[16] A. Chawla, B. Lee, S. Fallon, P. Jacob, Host based intrusion detection system with combined CNN/RNN model, in: Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Springer, Cham, 2018, September, pp. 149–158.
[17] P. Bedi, N. Gupta, V. Jindal, I-SiamIDS: an improved Siam-IDS for handling class imbalance in network-based intrusion detection systems, Appl. Intell. 51 (2) (2021) 1133–1151.
[18] J. Granjal, J.M. Silva, N. Lourenço, Intrusion detection and prevention in CoAP wireless sensor networks using anomaly detection, Sensors 18 (8) (2018) 2445.
[19] S. Raja, S. Pran, N. Pandeeswari, P. Kiruthiga, D. Nithya, G. MuthuPandi, Contemporary PCA and NBA based hybrid cloud intrusion detection system, EAI Endorsed Transac. Energy Web 8 (36) (2021).
[20] R. Andersson, CAN-Bus Multi-Mixed IDS: A Combinatory Approach for Intrusion Detection in the Controller Area Network of Personal Vehicles, 2021.
[21] P. Wei, Y. Li, Z. Zhang, T. Hu, Z. Li, D. Liu, An optimization method for intrusion detection classification model based on deep belief network, IEEE Access 7 (2019) 87593–87605.
[22] Z. Ye, Y. Sun, S. Sun, S. Zhan, H. Yu, Q. Yao, Research on network intrusion detection based on support vector machine optimized with grasshopper optimization algorithm, in: 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 1, IEEE, 2019, September, pp. 378–383.
[23] J. Gao, S. Chai, C. Zhang, B. Zhang, L. Cui, A novel intrusion detection system based on extreme machine learning and multi-voting technology, in: 2019 Chinese Control Conference (CCC), IEEE, 2019, July, pp. 8909–8914.
[24] A. Thirumalairaj, M. Jeyakarthic, Hybrid Cuckoo Search optimization based tuning scheme for deep neural network for intrusion detection systems in cloud environment, J. Res. Lepid. 51 (2) (2020) 209–224.
[25] Z. Wang, Y. Liu, D. He, S. Chan, Intrusion detection methods based on integrated deep learning model, Comput. Secur. 103 (2021), 102177.
[26] Rao, P.V., Murthy, K.S., Krishnan, V.G., Divya, V. and Sathyamoorthy, K., Detection of Sybil Attack in Manet Environment Using Anfis with Bloom Filter Algorithm.
[27] M. Ali, R.C. Deo, Y. Xiang, R. Prasad, J. Li, A. Farooque, Z.M. Yaseen, Coupled online sequential extreme learning machine model with ant colony optimization algorithm for wheat yield prediction, Sci. Rep. 12 (1) (2022) 1–23.