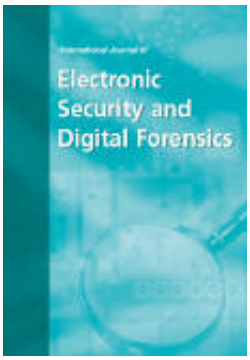
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

Analysis of smart grid-based intrusion detection system through machine learning methods

D. Ravikumar, K. Sasikala, R.S. Vijayashanthi, S. Narasimha Prasad

DOI: 10.1504/IJESDF.2024.10052832

Article History:
Received: 18 July 2022
Accepted: 05 October 2022
Published online: 12 January 2024

Analysis of smart grid-based intrusion detection system through machine learning methods

D. Ravikumar*

Department of Electronics and Communication Engineering,
Kings Engineering College,
Chennai, India
Email: ravikumar.dinakaran@gmail.com
*Corresponding author

K. Sasikala

Department of Electrical and Electronics Engineering,
Vels Institute of Science, Technology and Advanced Studies,
Chennai, India
Email: skala.se@velsuniv.ac.in

R.S. Vijayashanthi

Department of Electronics and Communication Engineering,
S.A. Engineering College,
Chennai-77, India
Email: vijayashanthirs@saec.ac.in

S. Narasimha Prasad

Department of Electronics and Communication Engineering,
Dhanalakshmi College of Engineering,
Anna University,
Chennai, India
Email: narasimha.vs@gmail.com

Abstract: This article aims to maximise network strong security and its enhancement by presenting different preventative strategies since intrusion detection is essential to computer network security challenges. In this study, intrusion detection is addressed as a challenge of extracting outliers that use the network behaviour dataset, and semi-supervised classification technique based on shared closest neighbours are suggested. First, we provide a thorough explanation of the fundamentals of cyber security assaults, supervised machine learning methods, and intrusion detection systems. Then, we discuss pertinent initiatives related to the use of supervised methods for intrusion detection. Finally, a taxonomy based on these connected works is offered. This article attempts to offer a sophisticated and distinctive intrusion detection model capable of categorising electrical network events and CDs for smart grids into binary-class, trinary-class, and multiple-class categories. As an effective machine learning model for intrusion detection, it employs the grey wolf algorithm (GWA).

Keywords: databases; support vector machines; smart grids; cyber attacks; intrusion detection systems; IDS.

Reference to this paper should be made as follows: Ravikumar, D., Sasikala, K., Vijayashanthi, R.S. and Prasad, S.N. (2024) 'Analysis of smart grid-based intrusion detection system through machine learning methods', *Int. J. Electronic Security and Digital Forensics*, Vol. 16, No. 1, pp.84–96.

Biographical notes: D. Ravikumar working as a Professor and the Head in the Department of Electronics and Communication Engineering at Kings Engineering College, Chennai, India. He received his undergraduate degree and Master's degree from Madras University and Anna University respectively and his PhD in Electronics and Communication Engineering from Vels University, India. He has published a number of research papers/article in peer review journals and book chapters, and participated in a range of forums in *Information and Communication Technology*. He has the teaching experience of more than 22 years in his area. He also presented various academic as well as research-based papers at several national and international conferences. He earned the Best Faculty Award from the Ministry of Skill Development and Entrepreneurship. Government of India for his exemplary academic performance and leadership skills He is specialised in the area of applied electronics, image processing, embedded, communication systems and IoT.

K. Sasikala obtained her Bachelor of Engineering in Electronics and Instrumentation Engineering from Bharathiyar University, Coimbatore in 2003 and Master of Engineering in Electronics Engineering from Anna University, Chennai in 2005. She received her Doctorate in from Vels Institute of Science, Technology and Advanced Studies, Chennai in 2021. She has published 22 articles in the peer review journals like, SCI, SCI-E, Scopus and UGC indexed journals. She has filed and published four patents. Her areas of interest are power electronics, embedded systems, IoT and control systems.

R.S. Vijayashanthi received his BE in Electronics and Communication Engineering in 2013 from the Velammal Engineering College affiliated to Anna University and ME degree from Sri Venkateswara College if Engineering (SVCE) affiliated to Anna University. She has five years of teaching experience and currently working as an Assistant Professor in the Department of Electronics and Communication Engineering, S.A. Engineering College, Chennai, India. Her research interests include embedded systems, networking deep learning and machine learning. She has contributed in many papers in national and international journals. She is a member of ISTE professional society.

S. Narasimha Prasad completed his BE (ECE) affiliated to Anna University in 2006, ME (Applied Electronics) in Anna University in 2013 He having 15 years of teaching experience. He is also a member in IETE. Currently, he is pursuing his PhD in Anna University as a research scholar.

1 Introduction

The process of identifying acts that attempt to jeopardise the entire privacy and consistency of a resource is known as intrusion detection. Therefore, the purpose of intrusion detection is to locate accessors who try to breach system security measures.

Even though some of the elements could be redundant and help very little to the detection method, current IDS check all data attributes to identify any intrusion and abuse tendencies. A sensor network (SN) is a complex system that integrates contemporary communications, processing techniques, and electrical grid identification. Intelligent control solutions are used in the SG, which calls for the use of high-quality, content that is error-free, along with speedy and dependable performances. SGs are still in the development phase, but being critical infrastructure and a cyber-physical system, they pose a danger of malfunction brought on by outsiders inputting harmful or incorrect data. With the introduction of the large-scale adoption of SG, cyber security has been a significant worry for power system operators in recent years. Power grids are becoming more susceptible to assaults as crucial cyber-physical technologies and high-speed networks are deployed in them. To monitor new assaults on systems, several technological techniques, including anomaly-based intrusion detection systems (IDSs), have been created and put into use. These methods may therefore result in detection rates of 98% at a high alert rate and 1% at a reduced alarm rate. This article analyses the performance metrics of several IDS.

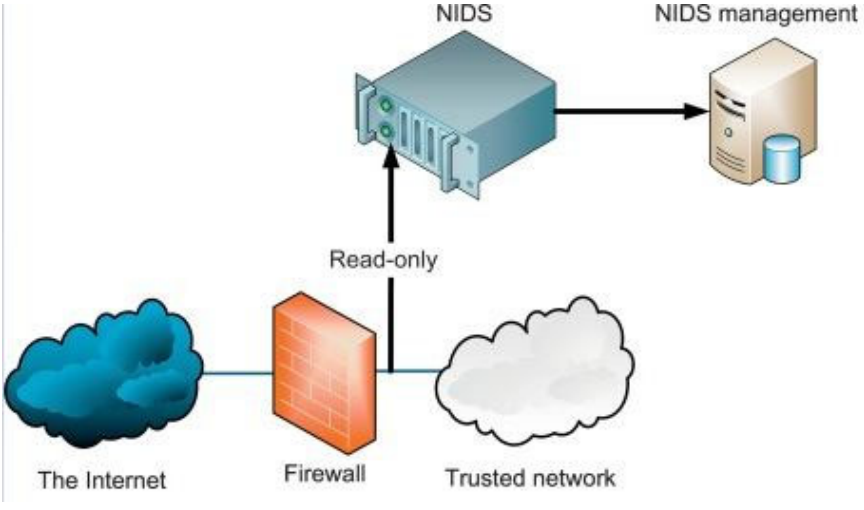
In the world of computer networking, where information and communication rule, there are a rising number of hosts and terminals. Security system flaws and illegal access to data systems are both rapidly expanding issues. Due to their capabilities of content filtering, preventing data outflow, alerting and preventing malicious activities, many techniques, including firewalls, security systems, anti-virus, anti-malware software, application security, behavioural analytic, data loss prevention, and network segmentation are frequently used in the computing world to enhance web security processes. Typically, simple rules-based algorithms are employed with firewalls and spam filters to allow and deny access to protocols, ports, or IP addresses. The disadvantage of these firewall and filtering is that they sometimes are unable to stop sophisticated denial of service (DoS) attacks and are also unable to distinguish between ‘good traffic’ and ‘bad traffic’. A computer network’s security procedures are significantly impacted by an IDS and anti-virus, which makes the case for safeguarding a computer network from unauthorised access more compelling. Any effort to undermine the integrity, reliability, confidentially, or circumvent the security mechanism of a machine or a concept is referred to as an intrusion from the viewpoint of information management.

A NIDS is made up of many modules, as indicated in Figure 2. Such components carry out the network’s intrusive content detection mechanism. Figure 1 depicts the three components of an NIDS and their respective functions. Signature-based NIDS is used for the proposed method. The detecting machines component aids in the identification of abnormalities or intrusions. The management machine oversees the detecting strategies or policies, while the detection method implements detection tactics. The data collection module is one of the various sub-modules of the detecting machine module. The communications and intrusion detection modules take data from the network. Management machine, the second module of a conventional NIDS, is used to manage and maintain detection policies depending on detection techniques. The third layer that preserves and saves recorded behaviour of feature-based intrusion detection is the databases.

In the current work, it is suggested that an intrusion diagnosing scheme be created using ANN training and the grey wolf algorithm (GWA). The name of this model is GWA-ANN. Self-organising maps, feed-backward, forward as well as neural networks

are the three main classifications of ANN structures and the placement of their neurons inside them. The hidden layer is used by feed-forward neural network (FFNN) called the multilayer perceptron (MLP), to convert inputs into outputs. The back-propagation method was used in this instance as the supervised approach to train the network. By using a GWA method, a potent swarm-based intelligent detection technique, assaults have been identified while avoiding the 'local minima' traps and sluggish convergence problems associated with ANNs (Qiao et al., 2021). In general, GWA has been regarded as being very precise and effective for resolving optimisation issues and is widely recognised for its capacity to identify the immediate vicinity of the universal optimum.

Figure 1 The elements of a network-based intrusion detection system (NIDS) (see online version for colours)



2 Literature review

In order to choose the most valuable features and categorise them using the current convolutional neural network, Riyaz and Ganapathy (2020) suggested a new feature selection technique called conditional random spectrum and linear cointegration coefficient-based features extraction algorithm. This features extraction algorithm not only drastically reduces training time but also improves model accuracy by removing unnecessary features.

Haojie et al. (2018) examined the possible security risks posed by 5G in-vehicle networks and concentrated on in-vehicle network intrusion detection techniques. From possible assaults on the vehicular network, four different situations were chosen, and actual automobile data were gathered to create the initial attack databases. Four inexpensive intrusion detection techniques are provided to identify the anomalous behaviour of the vehicular network in order to determine the best way to recognise various assaults. Additionally, the study compared the effectiveness of the four detection techniques while taking into account a wide range of assessment markers.

IDS was the study topic chosen by Zhang et al. (2021). They developed an IDS model using data mining, acquired experimental data, and came to pertinent experimental findings. Six trials were performed and the results as a comparison to conventional IDS. As a consequence, in six studies, the detection performance, false-negative rate, and false-positive rate of two distinct approaches were determined. The experiment's findings show that data mining-based IDS perform better in terms of network safety and support and have a greater capacity to identify network vulnerability intrusions. As a result, our study offers a fresh method for identifying and investigating security gaps in network protection.

Ensemble techniques to achieve greater prediction performance than any of the individual learning algorithms, several machine learning algorithms might be employed (Vasan et al., 2020). In order to enhance the detection performance, educate several classifiers simultaneously to recognise various threats.

To effectively counter these emerging attacks and detect malicious network traffic, internet security measures must continue to be efficient and robust (Chen et al., 2021). Data intrusion attacks are often the category of cyber attacks (CAs) that affect the energy grid. Denial-of-service, load reassignment, and fake data injection are the three main categories of data intrusion attacks .Such assaults provide CAs the ability to manipulate data used by the electrical grid to manage and monitor operations, disrupt the program's safe functioning, profit financially, and even remotely disable it (Meng et al., 2021).

The capacity to identify and distinguish aberrant data from regular data is a critical component of contemporary IDSs. IDSs protect networks against illegal access while protecting the integrity and confidentiality of the information and ensuring its availability. IDS technically uses the intrusion detection paradigm as its foundation. Unverified or insufficient intrusion detection might result in severe consequences for consumers and utility (Xue, 2021).

Engineering difficulties, which are nonlinear, ill- defined, and associated by noise, are addressed by IDSs. To tackle such issues, it is crucial to build a strong, dependable, and economical intrusion detection approach. In the remaining section, there has also been a description of current research on the creation of intrusion-diagnosing technologies for electrical grids.

Zhang et al. (2021) outline a number of processes and defences against malicious data assaults on control centres. They suggested the lowest residue energy heuristic for obtaining little yet incredibly devastating strikes.

The supervisory control and data acquisition (SCADA) communications making progress is used to incorporate the voltage control layout, and several methods to enhance detection mechanism and security management elements are looked at. In Dehghani et al. (2020), countermeasures against undetectable assaults are recommended.

Several data-mining approaches may be used to classify and aggregate power system disruptions.

Resilient cooperating event-triggered management and schedule have been considered when there are DoS assaults (Cong et al., 2021).

The length of the set of features for intrusion detection purposes can have a significant impact on the accuracy and accuracy of the identification process. There is no assurance that adding features would increase efficiency because doing so would require more storage, processing time, and perhaps greater noise-to-signal ratios. In systems with a lot of informational traffic, it has been demonstrated that feature selection is essential for expediting intrusion detection (Panthi, 2021).

A feature-selection-based IDS offered high detection rate based on a variety of characteristics. That model exhibited as compared to, good true-positive (TP) criterion and minimal false-positive (FP) criteria, certain other feature extraction methods. Due of its effectiveness and simplicity, in machine learning, artificial neural networks are often utilised. Additionally, this is utilised in power grids in intrusion monitoring (Reddy et al., 2021).

Although traditional training algorithms struggle to deal with sluggish convergence and localised optima, learning an ANN is currently challenging. One current development is training ANNs using heuristic optimisation techniques related to physical or biologic concepts to find the best set of weights (Cui et al., 2020).

By using a GWA method, a potent swarm-based intelligent detection technique, assaults have been identified while avoiding the 'local minima' traps and sluggish convergence problems associated with ANNs (Qiao et al., 2021). In general, GWA has been regarded as being extremely precise and effective for resolving optimisation issues and is widely recognised for its capacity to identify the immediate vicinity of the global optimum.

Current optimisation studies have introduced hybrid optimisation designs for boosting the effectiveness of primary patterns and their results (Al-Ghussain et al., 2021).

3 Research methodology

3.1 Analyses of the power grid

Figure 2 depicts the power system structure of this investigation. Two generator, G1 and G2, three bus bars, B1 through B3, two frequency lines, L1 and L2, four electrical devices, CB1 through CB4, and four relays, R1 through R4, make up this system. The SCADAs are connected to those relays through a substation switches and a network. Since relays lack any internal validation to establish whether a problem is genuine or not, they employ distance protection systems to trip the breakers on diagnosed errors and faults, irrespective of how much the defect is really present or not. Operators may manually operate these clever relays as well, allowing breakers to be manually triggered by relays. These scenarios presuppose that an attacker has already gained accessibility to a substation's network and has the ability to manage the substation via the switches, which is shown in the illustration. The power distribution centre provides electricity to numerous pieces of equipment (PDC). Numerous sophisticated electronic devices, such as the controller, Syslog, and Snort just at bottom of a diagram, can keep an eye on the entire grid.

3.2 The grey wolf proposed algorithm

Synthetic neural network using the GWA, an artificial neural network is taught to organise CAs from typical energy system occurrences. Each search agent used by the GWA-ANN to optimise a potential neural network is first initialised (NN). In an MLP network, there seem to be vectors of weights reflecting the relationships between the layer and the hidden layers as well as between the hidden layer (Qiao et al., 2021). The number of total biases and weight parameters that may have been improved using the

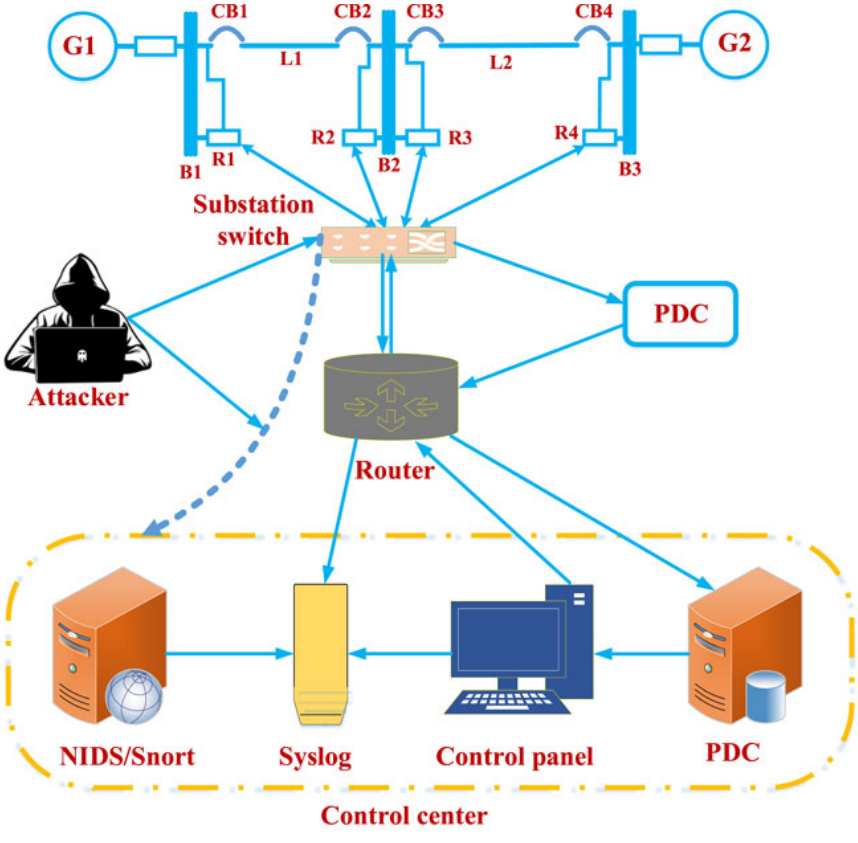
GWA in MLP systems is shown in Equation 1. Here, q represents the total number of input nodes, and p represents the total amount of nodes in the input layer.

$$V = pq + 2p + 1. \tag{1}$$

Whales acting as search agents may be able to distinguish between expected and actual classifications by employing the MSE of the MLP approach as a fitness function. MSE is seen in equation (2) where O_i is the expected result for entering instance I, O_i is the genuine outcomes for inputting instance I, and n represents the number of occurrences.

$$MSE = \frac{\sum_{i=1}^{n} \left(O_i - \hat{O}_i\right)^2}{n}. \tag{2}$$

Figure 2 Power grid architecture (see online version for colours)



3.3 Methods of intrusion detection technology

Several of the common intrusion detection technologies approaches used today are mentioned and explained below.

1 *Anomaly detection in neural networks*. This approach has the capacity for self-learning and self-adaptation to user behaviour, as well as the ability to efficiently analyse and assess the likelihood of intrusion in light of the actual observed data. A certain degree of anomalous user behaviour is reflected in the forecast of the mistake rate for the next event. Although this approach is now in widespread usage, it has not yet reached maturity, and no further full product exists.

2 *Statistical anomaly-based using probability*. According to the customer data likelihood recorded in the system, the auditing system tracks how users are using the system in real-time. based on initial evidence or patterns and past user behaviour modelling. When suspect user activity is discovered, the statistical approach is utilised to identify it and maintains track of, observes, and analyses the user's behaviour.

3 *Detection of system abuse by experts*. Expert systems are frequently employed in intrusion detection to target recognisable incursion activities. The rules of the If-Then structure are used in the implementation of the experts detection technique to convey the safety expert's information.

4 *Detecting intrusions using models*. When exploiting a system, hackers often use certain behavioural techniques, such as the behavioural sequence of password guessing. This pattern of behaviour represents a model with certain behavioural properties.

3.4 Datasets and case studies of attacks

The CAs in SG datasets from ORNL and MSU are used to assess the GWA-ANN. There are a maximum of 45 different datasets available. There are a total of 15 datasets of the binary, numerous, and trinary types. There is no such thing as an identical dataset. Every dataset has more than 5,000 samples. Each of the 37 occurrences situations is represented by one of the samples. One trinary-class dataset, as an example, has 5,236 observations total, of which 292 are sans events, 3,713 are attacks, and 1,212 are natural observation.

4 Results and discussion

Figure 3 depicts the efficiency curve of convergence for the dataset 15 binary classification task using the ANN through GWA adjusting approach. According to the graph, the performance of the model gradually increases as the number of observations increases. The accuracy increased dramatically after the 64th iteration and then quickly stabilised at around 99%.

Figures 4 and 5 demonstrate that as the proportion of compromised nodes rises, the median detection performance including both networks and devices intrusion detection rapidly decreases as the numbers of elusive opponents in the network increases.

Under various adversarial composition, we replicated our tests and analysed the detection capability for networks and device intrusion detection. The detection precision of category B gadgets is shown in Figure 6.

Figure 3 The ANN accuracy's convergence curve during the GWA tweaking procedure (see online version for colours)

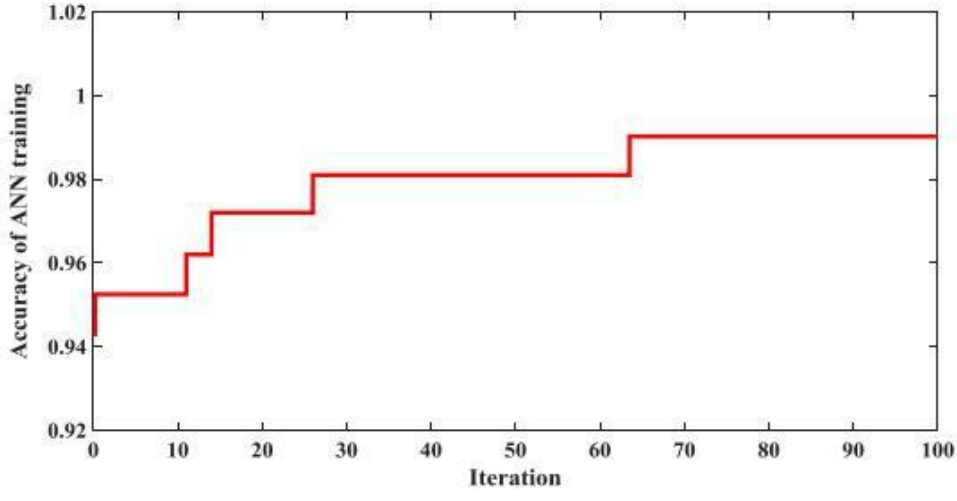


Figure 4 Average accuracy in detecting network intrusions (see online version for colours)

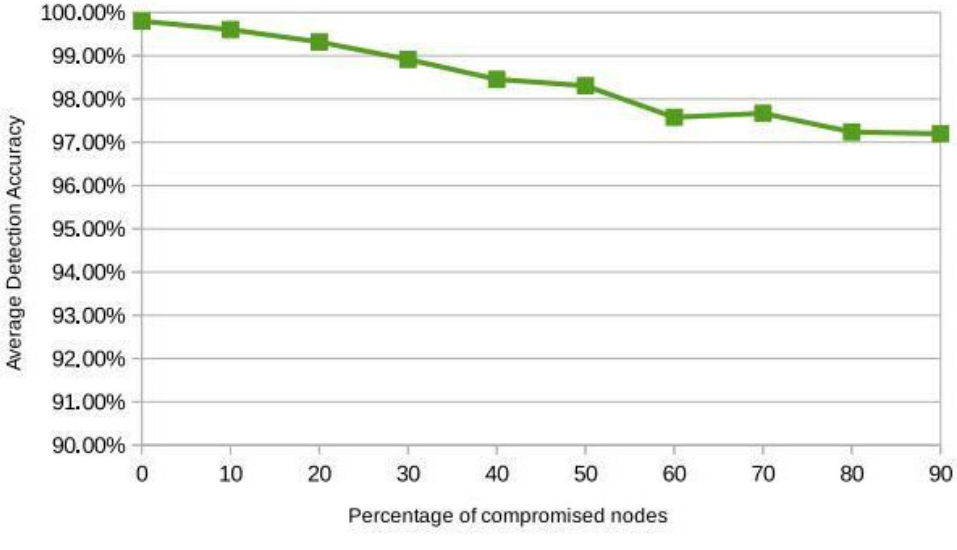


Figure 7 shows the histogram errors for dataset 15's classification model using 20 bins to indicate learning, confirmations, and trial error. The learned patterns can suit the dataset, as seen in this image. The bulk of inaccuracies, with 0.02592 being one of the most noticeable inaccuracy, have been localised in a small region close to zero.

Figure 5 Accuracy of device intrusion detection is mediocre (see online version for colours)

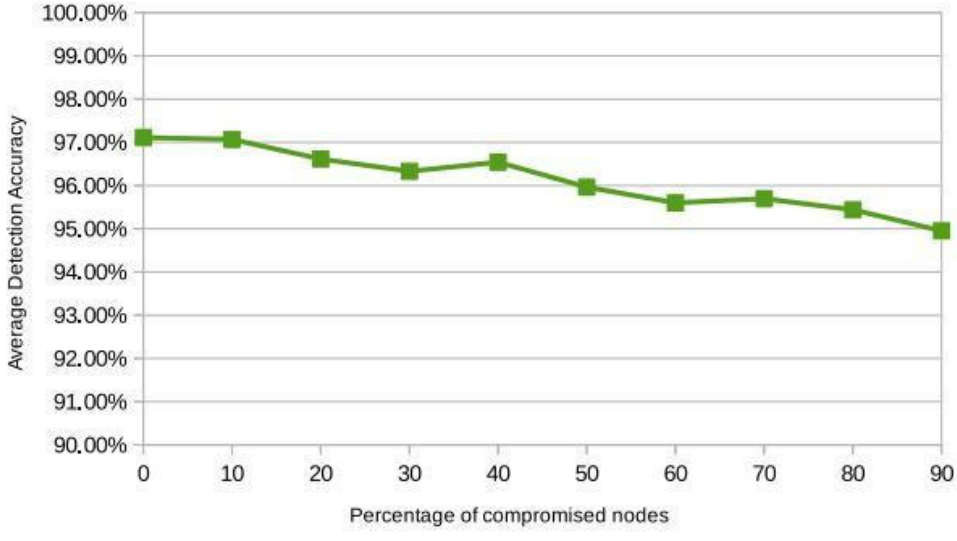


Figure 6 Accuracy of device intrusion detection (see online version for colours)

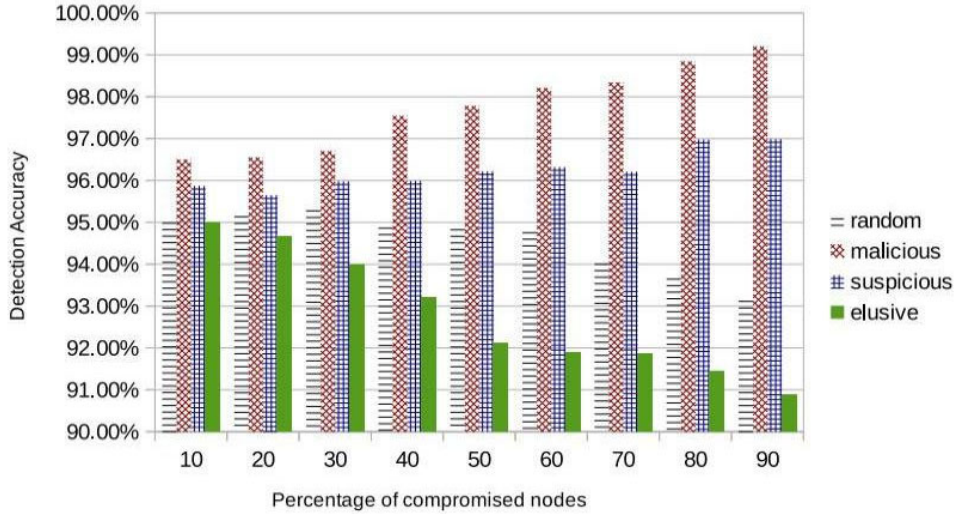
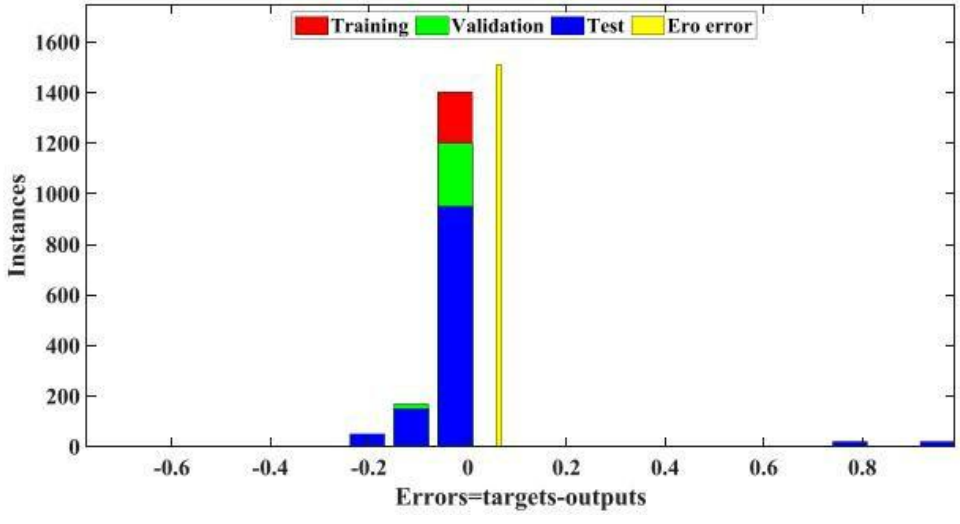


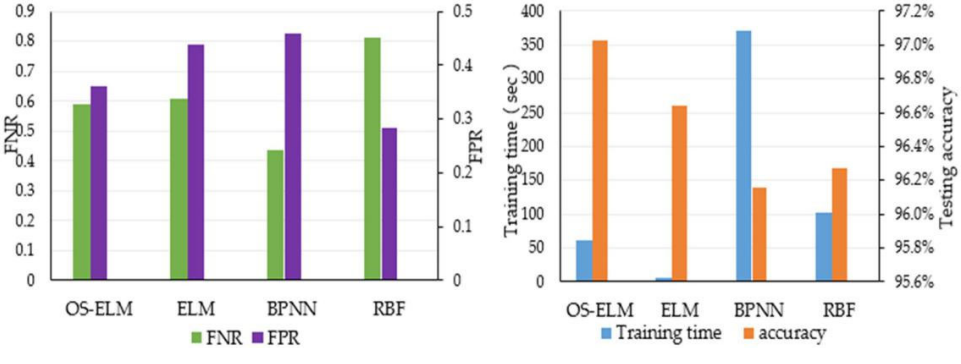
Figure 7 Error histogram training, GWA-ANN confirmation, and testing (see online version for colours)



4.1 State-of-the-art works

The comparison of the various recent algorithms are shown in Figures 8(a) and 8(b).

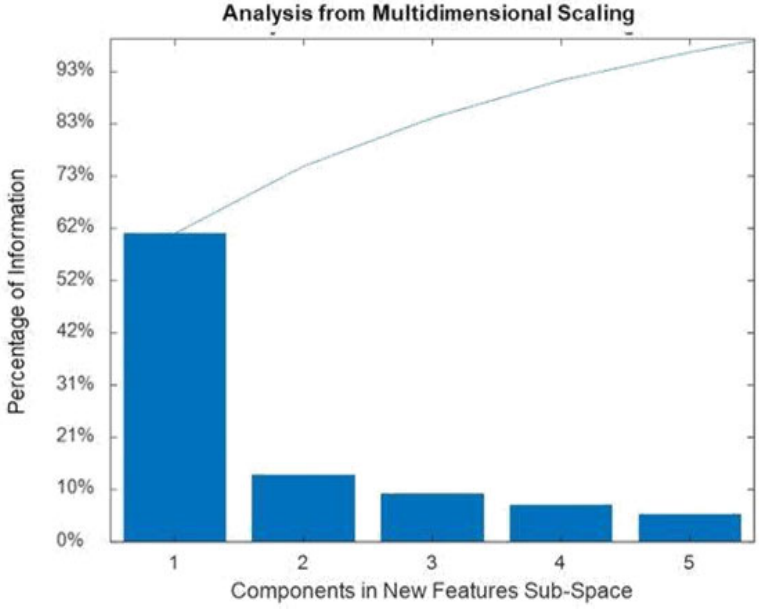
Figure 8 Comparison with the state-of-the-art methods (see online version for colours)



(a) (b)

It should have been noted that such papers in the similar work category use computationally intensive techniques since they need recursive steps like wrappers filtering. Instead, a direct approach of constructing the baseline changes in the feature space is used in this study, and the cosine of similarities is used to compare the dataset's columns rather than the Euclidean distance or PCA since, as was already noted, it produces findings that are much superior. The Pareto chart is shown in Figure 9.

Figure 9 Pareto chart showing the amount of information for each component of a new space feature (see online version for colours)



4.2 Future scope

By simulating several use-case situations and running networks and device level identification in parallel, we tested our detecting system and found that the accuracy of the findings was rather promising. We want to further minimise the detecting system's device-specific energy usage in our next research. As an alternate to regression, which only considers samples of real sensor data, we also want to investigate other techniques, such like state graphs, for assessing changes in sensors and data trends.

5 Conclusions

A dependable SG management and operation need the ability to quickly and accurately identify suspicious or unusual occurrences. Cybersecurity is a major issue since power systems rely heavily on computer infrastructure. To disseminate and handle the massive volumes of real-time data generated during system operation, this infrastructure is required. With the use of ANNs, this work addresses various flaws in traditional algorithms such the trapping of local minima. This work applies the MSU/ORNL datasets at various degrees of difficulty to the GWA-ANN model to categorise the CAs and identify electrical grid breakdowns (multiple-class, trinary-class, and binary). To offer the best bias and weights for the classification with the lowest MSE, the ANN is trained using the GWA. problem. Experiments showed that the proposed technique is effective in finding the CA data in electrical systems. The GWAANN is preferable to other classification techniques such as SVM, and NN (without GWA) daBoost + JRipOneR, because of its potent opportunity to discover and thwart local optimisation.

References

Al-Ghussain, L., Ahmad, A.D., Abubaker, A.M., Abujubbeh, M., Almalaq, A. and Mohamed, M.A. (2021) 'A demand-supply matching-based approach for mapping renewable resources towards 100% renewable grids in 2050', *IEEE Access*, Vol. 9, pp.58634–58651, DOI: 10.1109/ACCESS.2021.3072969.

Chen, J., Mohamed, M.A., Dampage, U., Rezaei, M., Salmen, S.H., Obaid, S.A. et al. (2021) 'A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks', *Appl. Sci*., Vol. 11, No. 21, p.9972, DOI: 10.3390/app11219972.

Cong, M., Mu, X. and Hu, Z. (2021) 'Sampled-data-based event-triggered secure bipartite tracking consensus of linear multi-agent systems under DoS attacks', *J. Franklin Inst*., Vol. 358, No. 13, pp.6798–6817, DOI: 10.1016/j.jfranklin. 2021.07.012.

Cui, H., Dong, X., Deng, H., Dehghani, M., Alsubhi, K. and Aljahdali, H.M. (2020) 'Cyber attack detection process in sensor of DC micro-grids under electric vehicle based on Hilbert-Huang transform and deep learning', *IEEE Sensors J*., Vol. 21, pp.15885–15894, DOI: 10.1109/jsen.2020. 3027778.

Dehghani, M., Kavousi-Fard, A., Dabbaghjamanesh, M. and Avatefipour, O. (2020) 'Deep learning based method for false data injection attack detection in AC smart islands', *IET Generation, Transm. & Distribution*, Vol. 14, No. 24, pp.5756–5765, DOI: 10.1049/iet-gtd.2020.0391.

HaoJie, Y.W., Qin, H., Wang, Y. and Li, H. (2018) 'Comparative performance evaluation of intrusion detection methods for in-vehicle networks', *IEEE Access*, Vol. 6, pp.37523–37532.

Meng, F., Zou, Q., Zhang, Z., Wang, B., Ma, H., Abdullah, H.M., Almalaq, A. and Mohamed, M.A. (2021) 'An intelligent hybrid wavelet-adversarial deep model for accurate prediction of solar power generation', *Energ. Rep*., Vol. 7, pp.2155–2164, DOI: 10.1016/j.egyr.2021.04.019.

Panthi, M. (2021) 'Identification of disturbances in power system and DDoS attacks using machine learning', in *IOP Conf. Ser. Mater. Sci. Eng*., Vol. 1022, No. 1, p.012096, IOP Publishing, DOI: 10.1088/1757-899x/1022/1/012096.

Qiao, W., Khishe, M. and Ravakhah, S. (2021) 'Underwater targets classification using local wavelet acoustic pattern and multi-layer perceptron neural network optimized by modified whale optimization algorithm', *Ocean Eng*., Vol. 219, p.108415, DOI: 10.1016/j.oceaneng.2020.108415.

Reddy, D.K., Behera, H.S., Nayak, J., Vijayakumar, P., Naik, B. and Singh, P.K. (2021) 'Deep neural network based anomaly detection in internet of things network traffic tracking for the applications of future smart cities', *Trans. Emerging Telecommunications Tech*., Vol. 32, No. 7, p.e4121, DOI: 10. 1002/ett.4121.

Riyaz, B. and Ganapathy, S. (2020) 'A deep learning approach for effective intrusion detection in wireless networks using CNN,' *Soft Computing*, Vol. 24, No. 22, pp.17265–17278.

Vasan, D., Alazab, M., Wassan, S., Safaei, B. and Zheng, Q. (2020) 'Image-based malware classification using ensemble of CNN architectures (IMCEC)', *Comput. Security*, 1 May, Vol. 92, p.101748.

Xue, P. (2021) 'Impact of large-scale mobile electric vehicle charging in smart grids: a reliability perspective', *Front. Energ. Res*., pp.101–122, DOI: 10. 3389/fenrg.2021.688034.

Zhang, Z., Deng, R., Yau, D.K.Y. and Cheng, P. (2021) 'Zero-parameter information data integrity attacks and countermeasures in IoT-based smart grid', *IEEE Internet Things J*., Vol. 8, No. 8, pp.6608–6623, DOI: 10.1109/jiot. 2021.3049818.