IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 40, No. 3, June, 2023, pp. 905-914
Journal homepage: http://iieta.org/journals/ts

Embedded Signal Artificial Neural Network Based Intelligent Non-Dependent Feature Selection for Cyber Attack Classification in Signal-Based Networks

Ragini Mokkapati*, Venkata Lakshmi Dasari

School of Computer Science and Engineering, VIT-AP University, Amaravathi 522237, Andhra Pradesh, India

Corresponding Author Email: raginiraginimokkapati@gmail.com

https://doi.org/10.18280/ts.400307

Received: 16 November 2022
Accepted: 28 March 2023

Keywords:
signal based cyber attacks, network security, feature extraction, feature selection, redundancy, feature subset

ABSTRACT

Signal-based cyber attacks pose a significant threat to the integrity, confidentiality, and availability of information systems. Intrusion Detection Systems (IDS) monitor network and system activities for malicious activity or policy breaches, which are then reported to a management station. Due to the high volume of network traffic in cyber networks, real-time threat detection is often computationally infeasible. In this study, we explore the use of an Artificial Neural Network (ANN) for cyber network threat identification, specifically focusing on its application in nonlinear characteristics and network security domains. Data reduction is crucial for achieving real-time detection in a Signal-based Cyber Attack Detection Model (SCADM). However, traditional CADMs analyze all data features to detect patterns of intrusion or misuse, leading to redundancy in detection features. The primary objective of this research is to identify computationally efficient and effective input features for SCADM. We propose an embedded Signal with ANN-based Intelligent Non-Dependent Feature Selection Model (ANN-INDFSM) that effectively extracts signal-based cyber attack features and performs feature reduction for accurate detection of signal-based cyber attacks while maintaining security. The ANN-based feature selection method was employed for eliminating non-salient features and determining dimensionality levels. Given the diverse characteristics and pattern types of emerging cyber attacks, tracking them has become increasingly challenging. Various methods have been used for feature extraction and selection, with the ultimate goal of detecting anomalies in large cyber security datasets. Although this process is both time-consuming and computationally demanding, the efficiency of machine learning algorithms can be improved by removing unnecessary and redundant features. Feature selection (FS) serves as one such method. By utilizing datasets containing only a sufficient subset of features instead of the full dataset, the computational time required for attack detection algorithms can be reduced. When compared to existing models, the proposed ANN-INDFSM demonstrates optimized performance levels, providing a streamlined and effective solution for the detection of cyber attacks in signal-based networks.

1. INTRODUCTION

With the exponential growth of the internet, data security has become an increasingly pressing issue. Security refers to how well a system or network is protected from attacks. The three pillars of information security are privacy, data integrity, and data availability [1]. The term intrusion is commonly used to describe network attacks. Intrusion refers to any concerted effort to breach information security measures [2]. Anomaly detection is one of major information security concerns. Intrusion Detection Systems (IDS) help computers fend off malicious intrusion attempts. Network security has come a long way from its early days, when only traditional methods like encryption, firewalls, VPNs, etc. were used. It is impossible to depend fully on static protection measures. This increases the necessity of dynamic technique, which may check network nodes and identify illegal activities in the network [3]. Thus to strengthen the security protocols dynamic technique is proposed and termed as Intrusion Detection Systems [4]. Intrusion detection system takes online data collected from the network then after that observes and analyses this knowledge and partitions it into regular & harmful activities, present the result to network administrator [5]. Due to its limitations in scalability, adaptability, and veracity, data mining finds its most widespread application in IDS [6]. Info sources for IDS include network logs, host data, and more. Data analysis is challenging because of the volume of network traffic. This necessitates combining IDS with various data mining methods for intrusion detection [7].

Cyberattacks pose legitimate safety concerns, necessitating the development of a cutting-edge, malleable, and remarkably effective IDS [8]. An IDS is a framework or method used to detect and differentiate intrusions, attacks, invasions, or breaches of the safety schemes autonomously at the network level and the host level. Network-based intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS) are two types of security infrastructure that classify attacks based on their characteristics [9]. If the architecture is based on network behaviours, it is known as a NIDS. By duplicating the actions of networking equipment like switch, routers, and network taps, network tools collect data that can be used to identify assaults and other threats hiding in network

traffic [10]. The term HIDS refers to a framework that uses system workouts in the form of multiple log data acquisition on the local host machine or device to discover malware. These logs are being fetched locally, using sensors of various kinds. In contrast to HIDS's reliance on data from log documents, which may include sensor logs, event logs, application logs, file systems, disc assets, client account details, and a few other elements of each system, NIDS analyses every packet of data relied upon within network traffic streams. In some establishments, HIDS and NIDS are used together [11].

The first line of defense against a security breach is a reliable intrusion detection system. Thus, there has been a lot of focus on security solutions like firewalls, IDSs, UTMs, and IPSs. By collecting data from a wide range of systems and networks and then analysing it, intrusion detection systems can identify potential security breaches and stop them in their tracks. The packet data that traverse a network are analysed in two ways by a network based IDS [12]. The issues with anomaly based intrusion detection are that it needs to cope with unique attack in which there is no previous experience to identify the anomaly [13]. This means that anomaly - based intrusion detection is still a key topic for research. For this reason, experts have been looking at machine learning methods for the past several years in the hopes of giving the system the ability to tell good traffic from bad or to spot anomalies [14]. The IDS model is shown in Figure 1.

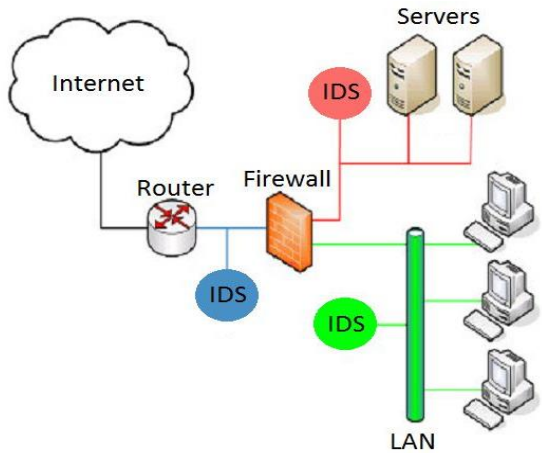

Figure 1. Intrusion detection system

When mining enormous datasets, feature selection is an essential pre-processing step that can dramatically boost the overall system's performance [15]. The final feature subset is generated by the wrapper phase, and the filter phase chooses the features with the maximum information gain and directs the start of the search procedure for that phase [16]. Feature selection's ultimate goal is to narrow down a large pool of candidate features to just those that adequately characterise the target notion. In both theoretical and practical settings, it has been shown to improve learning efficiency, boost predictive accuracy [17], and decrease result complexity [18]. The search space for the best possible feature selection is exponential in E, where E is the number of features. So, it could be excessively expensive and impracticable [19]. The wrapper model differs from the filter model in that feature selection does not rely on a learning process. The filter model's strengths lay in its superior generalizability and cheap computational cost, both of which are independent of the learning algorithms used [20]. The goal of intrusion detection is to uncover illegal actions that could compromise a system's integrity and performance. Differentiating between benign and malicious network activity is difficult in intrusion detection [21]. A machine learning algorithm is used in conjunction with feature selection algorithms to establish which feature set that yield the most significant improvements in accuracy and computational processing times [22]. The generated matrix gives users a heuristic for determining which based on deep learning.

IDS development has recently benefited from the application of Artificial Neural Networks (ANN) [23]. ANN's intrinsic speed and the ease with which nonlinear relationships between input and output can be represented are two of its greatest strengths. Incomplete or skewed data wouldn't stop a neural network from processing it [24]. An issue with neural network-based methods is that they struggle to understand the input-output relationship when the input data has a high dimensionality [25]. The primary benefits of ANNs over conventional IDSs lie in their enhanced capacities for learning, classification, rapid data processing, and self-organization. Because of these benefits, Neural Networks can enhance IDS performance [26], and AI methods can boost IDS/IPS potency. The ANN process in analyzing and generating the output is shown in Figure 2.

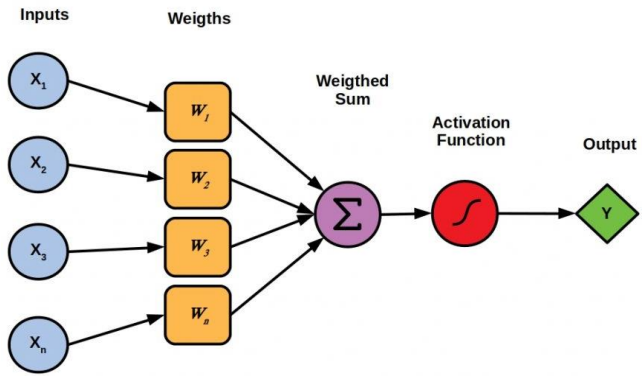

Figure 2. Artificial neural networks

Advanced IDSs are defined as host-based or network-based computer programs that monitor their surroundings and behave flexibly to improve detection accuracy [27]. These programs determine what must be done in an environment by learning that setting and then applying inference rules to the data. A smart IDS can make decisions and validate constraints. Most intelligent systems either utilize rules to make decisions or agents to do so. As a result of proposing smart methods for preprocessing and efficient categorization [28], smart intrusion prevention systems have been developed. When compared to other methods, the detection rate offered by such IDSs is superior. In order to acquire a subset of attributes that accurately characterise the given problem with a minimal loss of performance, extraction of features involves identifying the relevant characteristics and rejecting the unnecessary ones [29]. There are many benefits to doing so, including enhancing the efficiency of machine learning algorithms, better comprehending data, learning more about the process through better visualisation, reducing data size, lowering storage needs, and cutting down on processing expenses.

In classification, a classifier is trained from a training set of labelled data instances, and then used to categorize a training set into one of the groups in testing. A classifier is learned during the training phase by ingesting the available labelled

training data [30]. In the testing phase, the classifier is used to determine whether a test case is typical or out of the ordinary. Intrusion detection methods that rely on classification can be run with a single-class classifier or several classes. IDS methods based on uni class classifications presume that each training case has a unique class label. These methods use a one-class classification method to learn a racially discriminatory boundary around the typical examples. Any data sample that fails to fit the boundary established by the learning process is flagged as abnormal. In this research, an effective ANN based intellectual non dependant feature selection model is proposed that effectively extracts the signal based cyber attack features and performs feature reduction for accurate detection of signal based cyber attacks to maintain security. The proposed model feature dimensionality reduction reduces the features selected for intrusion detection. The independent features are only considered for training the ANN model that accurately detects the intrusions. The proposed model performs the memory optimization with the reduced feature set and also the time complexity levels are very much reduced than the traditional models.

2. LITERATURE REVIEW

Concerns over security and privacy have been sparked by the rapidly growing number of linked computing devices, the prevalence of wireless networking, and the inclusion of cyber-physical-social systems. Recent years have seen the incorporation of machine learning (ML) techniques into the creation of IDS, which are widely regarded as a very efficient kind of defence. Traditional ML-based IDS, which necessitates considerable computing resources such as restricted energy source, computational power, and memory, is not suited for running on Internet of Things (IoT) devices. Therefore, the goal of this research is to create a small ML-based IDS that is optimised for low-powered gadgets. In particular, IM-Personation Attack detection using the deep auto-encoder and feature-abstraction (IMPACT), a lightweight machine learning (ML)-based intrusion detection system, is proposed by Lee et al. [2]. Using a stacked autoencoder (SAE) and a C4.8 wrapper, we can reduce the number of features for deployment and execution on resource-constrained devices based on deep features training and gradient-based Support Vector Machines (SVM). In order to spot impersonation attacks, the IMPACT has been trained on the Aegean Wi-Fi Hacking Dataset (AWID).

The proliferation of wirelessly connected gadgets has both beneficial and undesirable outcomes. While it facilitates a wide variety of human activities, the wireless nature of the medium makes the system susceptible to attack. Using cutting-edge anomaly detection methods, an IDS may monitor network traffic for signs of intrusion. It has been possible to tell good traffic from bad using deep learning models. A major obstacle to using machine learning for IDS has been translating tables into images prior to image classification. New tabular data projection into 2-coded colour mapping is proposed for IDS applications. In order to achieve desirable dimensionality, the suggested approach uses a feature selection technique proposed by Aminanto et al. [3]. To determine how the traits are related to one another, the author analysed groups of attributes with varying sizes. To further categorise Wi-Fi attacks, it employs a model based on Convolutional Neural Networks (CNNs). Using the Aegean Wi-Fi Intrusion Dataset, the most popular dataset for Wi-Fi intrusions, the suggested model (AWID2) is tested.

In order to automatically and quickly identify and categorize network and host-level signal based cyber attacks, supervised learning techniques are frequently employed in the development of IDS. Malicious assaults provide a number of difficulties, however, because they are dynamic and happen in high volumes, necessitating a scalable response. The cyber security community can access a variety of publicly available malware datasets to do additional study. However, there is currently no research that compares and contrasts the efficacy of different machine learning algorithms using a wide range of publicly available datasets. Since malware is always evolving and using new attack vectors, it is important to regularly update and benchmark publically available malware datasets. Vinaya kumar et al. [5] investigated the use of a deep learning model (DNN), a form of learning algorithm, to build a robust IDS that can identify and categorise signal based cyber attacks that cannot be predicted in advance. The need to evaluate diverse datasets collected over the years using static and dynamic methods is a direct result of the dynamic nature of network behaviour and the quick growth of attacks. Research of this nature helps pinpoint the most efficient system for spotting future cyber attacks. Extensive studies comparing DNNs and other classical learning techniques classifiers on many available to the public benchmark malware datasets are presented, along with a detailed evaluation of the results. KDDCup 99 dataset is used in this model and the hyper - parameters selection techniques are analyzed to determine the best possible network parameters and topologies for DNNs.

The proliferation of IoT devices has led to an increase in cybercrime and highlights the need for better network and system protections. With the proliferation of IoT devices and services, cyber security has emerged as a complex subject to oversee. Today's network intrusion detection solutions rely heavily on deep learning-based signatures of malicious traffic IDS. Intrusion detection in networks has been a topic of deep learning methodology. An RNN has several potential uses. The first contribution of this research made by Ullah et al. [6] is a unique deep learning model for abnormal identification in IoT networks by means of a recurrent neural networks. The suggested model for IoT network anomaly detection is implemented utilizing Long Short Term Memories (LSTM), Bi-LSTM, and Gated-Recurrent Units (GRU) methods. When it comes to feature learning, CNNs shine because of their ability to examine input features without discarding any relevant information. The author then devised a convolutional/recurrent neural network hybrid model for deep learning. The author concluded by proposing a minimal deep learning approach for classification that makes use of LSTM, Bi-LSTM, and GRU based techniques. The NSL-KDD, BoT-IoT, IoT-NI, IoT-23, MQTT, MQTT-set, & Connectivity datasets are used to test the accuracy of the proposed deep learning models. The suggested classification and binary classification method outperformed state-of-the-art deep learning implementations in terms of precisions, re-call, and F1 score.

Power system reliability depends on accurate and prompt reactions to abnormal conditions. It is crucial to provide an accurate method for the categorization of activities and abnormalities in the power grid so that the operators or the automated reply system can take timely action during system crises. In order to develop dataset for event and intrusion, the humongous amounts of moment data generated by the phasor

measuring devices can be merged with logs from those other elements in the power grid. In order to better categorize emergencies and signal based cyber attacks, Hong et al. [9] presented the outcomes of implementing deep learning techniques to open dataset acquired from a power grid testbed. Three distinct recurrent neural network (RNN) architectures are explored and evaluated for their ability to classify events into binary and multiclass categories.

Due to the exponential increase in complex and an ever cyber threats and attacks, the entire IoT infrastructure is in disarray. The IoT is part of the infrastructure of connected devices, which presents serious security concerns. The primary focus of cyber threat analysis is the identification and prevention of complex network-based threats and attacks, making it an integral part of any network security infrastructure. It also necessitates the network security provided by the examination and categorization of malicious actions. In this research, Qureshi et al. [10] introduced a DL-enabled spyware detection scheme that makes use of a hybrid methodology based on the coupling of a DNN with Long Short-Term Memory (LSTM) for the important instructional of multi-class malware attacks in IoT infrastructure.

Cyber-Physical Systems (CPS) such as those used to regulate transportation, manufacturing, and utilities frequently employ deep neural networks (DNNs). DNNs, however, are susceptible to attacks from what are known as adversarial examples, which are carefully crafted input samples. One of the most useful tools for discovering vulnerabilities in neural networks and fixing them is the adversarial attack. To gain the direction of creating adversarial samples, existing methods, such as the state-of-the-art black-box attack, create faulty queries with a reduced success rate. Kuang et al. [13] presented an adversarial approach on black-box DNNs using a CMA-ES. In the first place, a powerful strategy for decreasing the quantity of bad requests is shown. Second, the author suggested a black-box assault wherein adversarial samples are generated automatically to match a high-dimensional-independent Gaussian-distribution of the local optimal solution. In order to make the procedure of perturbation reduction more seamless, a novel CMA-based perturbations compression method is employed.

The internet is expanding rapidly, with numerous web-based apps to meet the varied requirements of today's consumers. However, the widespread adoption of online services has opened them up to significant vulnerabilities in terms of data safety and dependability. Cyber threats, on the other hand, have evolved alongside technical progress, blending formerly separate attack vectors into increasingly complex and dangerous wholes. Since both the frequency and sophistication of signal based cyber attacks are only expected to rise, it is critical that strengthening of defences against them is performed. This study's goal is to evaluate competing neural network models for their ability to identify harmful from benign behavior that is analyzed by Albahar et al. [15]. Two datasets are used to train, validate, and test the models under scrutiny. The confusion matrix is used to evaluate the accuracy of the models under scrutiny. Binary categorization and multi-class categorization are used to assess the models for the cyber-physical subsystems dataset. Since the KDD dataset only has two categories—regular and harmful, a binary classification method is required. When comparing binary classification to multi-class classification, the outcomes are often more promising for binary classification. PNN models have the best results, while GRNN models are the quickest. Despite PNN's somewhat longer runtime compared to the GRNN strategy, users can confidently declare it to be the best choice for data with the achievable trade-off between performance and runtime.

Industrial Control Mechanisms (ICMs) are made far more susceptible to signal based cyber attacks due to their incorporation of communications systems and IoT, with potentially catastrophic results. Classical IDSs rely heavily on predetermined models and are primarily trained on certain cyber-attacks; they are primarily designed to support IT systems. Furthermore, many IDSs do not take into account the asymmetrical character of ICS datasets, leading to poor precision and a high rate of false positives when deployed. In this research, Al-Abassi et al. [16] suggested a deep learning approach to create novel representations of an imbalanced dataset that are more fair. With these updated representations, a deep learning detection and prevention model tailored to an ICS setting may be trained. The suggested attack detection model makes use of Deep-Neural-Network (DNN) and Decision-Tree (DT) classifiers to spot signal based cyber attacks using these updated models of data. Ten-fold cross-validation on two independent real-world ICS datasets is used to assess the quality of the proposed model.

Artificial intelligence and smart approaches have been implemented, and have become hotly discussed subjects in industrial cyber-physical systems, in tandem with the growth of the Industry 4.0 [19]. While there has been progress in the field of cyber-physical security protection, intelligent anomaly detection for recognizing cyber-physical threats to ensure the efficiency and safety of the workplace is still a hard issue. To solve the over-fitting problem and improve the precision of intelligence anomaly detection in industrial CPS, Zhou et al. [19] presented a few-shot learning model using a Siam convolutional neural network (FSL-SCNN). Using optimal feature representations, distances between input samples can be calculated using a Siam CNN encoding network. To further improve the training process's efficacy, a strong cost function design is then provided, one that takes into account three distinct losses. Finally, a smart anomaly-detection algorithm has been created.

3. PROPOSED METHODOLOGY

It is of interest to utilize statistical modeling via computational means to forecast whether unseen observations are signal based cyber attacks and the intensity of those attacks based on data from controlled cyber threat and intrusion exercises, which is essentially participatory simulation. Cyber anomaly and threat detection is a topic of intense research interest nevertheless, doing so requires analyzing a massive amount of data. This would be a Big Data challenge with high data velocity in a real-time setting. In order to enhance response time and data storage, it is necessary to identify a smaller selection of important data elements to monitor. Therefore, this research primary objective is to develop a dimensionality reduction model for cyber security, one that ranks and identifies the most important traits for threat identification. It will be achieved via the creation and implementation of a feature dimensionality reduction strategy based on classifiers.

Although linear discriminant analysis has been used in previous cyber security studies to account for error when evaluating the importance of individual characteristics, this

factor was not taken into account when deciding how many features to utilize for classification. In this research, an end-to-end methodology is established for identifying signal based cyber attacks using feature extraction from network traffic data and subsequent feature selection using classifier-based algorithms. While ANNs have been used for cyber intrusion detection before they have not yet been used to estimate the importance of cyber features. Classifier models based on ANNs are utilized to identify relevant information for threat detection. This technique is used to provide insight into what data is most relevant for detecting signal based cyber attacks by combining the classification and feature relevance ranking tasks.

Feature selection is crucial in the detection of signal based cyber attacks. It has been demonstrated that learning algorithms' efficacy might be negatively impacted by redundant and/or irrelevant features. There is currently no accessible automatic and efficient feature selection approach that can help capture the primary properties of the data across a variety of operational settings. Conventional forward feature selection based on feature ranking is commonly employed in data processing. Gain in knowledge is a popular statistic used to rank characteristics. Information gain has one major drawback: it requires joint probability distribution functions of characteristics and target classes. Training data is typically used to get the necessary information to learn these functions. When there are many classes and features to choose from, the learning process slows down. In addition, if the sample sizes of the various classes are not roughly equal, the estimation will be off.

Convolutional, pooling, and fully connected layers make up convolutional neural network (CNN) architecture that is applied on this research. The three layers that make up CNN are the convolutional layer, the pooling layer, and the fully connected layer. This group of neural networks is used to analyse information using a grid structure. In a CNN, the convolution layer performs the bulk of the processing. After applying K filters towards the input volume, K 2-dimensional activation maps are generated. The output volume is the result of stacking K activation maps all along hidden layers of intrusion data records. The fully connected (FC) layer couples every input to every neuron in the network. After that, the squished vector travels through some more FC layers, which is often where the mathematical functions operations are carried out. At this stage, the process of categorising the data is performed as normal or intrusion. If a CNN design includes an FC layer, it is usually the last layer in the network that predicts the intrusions in the network.

It is possible to keep monitoring on the entire network because the IDS module is installed on the network IDS. By scanning all data packets that traverse the network, this Intrusion Detection System can uncover any suspicious behavior. That is because the IDS host installs its module on every client in the network. Selecting and ranking features is a crucial challenge in intrusion detection. Eliminating unnecessary features improves IDS performance by increasing detection accuracy and reducing computation time. The effectiveness of the learning algorithm is affected by the uniqueness of the features and the number of features used during training. Selecting suitable training settings and a strong subset of features are crucial concerns for enhancing the IDS's accuracy and overall performance. In this research, an effective ANN based Intellectual Non Dependant Feature Selection Model is proposed that effectively extracts the signal based cyber attack features and performs feature reduction for accurate detection of signal based cyber attacks to maintain security.

Algorithm ANN-INDFSM:

do

Input: Intrusion Detection Dataset {$\mathrm{INDT_{SET}}$}

Output: Intrusion Prediction List {IPL}

The intrusion detection dataset is considered and the data set undergoes pre processing. The term data preparation refers to the steps used to clean and organize data before it is analyzed. Since raw data is not used for analyzing, the pre processing process is equally crucial for machine learning. The pre processing is performed as

$$DT_{SET} = \sum_{i=1}^{M} getV(i) + avgV(M-i,i) - G(i)$$

$$INDT_{SET} = \frac{Max\left(DT_{set}(i+1)\right) - G(i)}{\sqrt{\sum_{i=1}^{M}(\max\left(DT_{set}(i+1)\right)) - \min\left(DT_{set}(i)\right)} + T(i)}$$

Here G is the function that extracts the special symbols in the dataset. avgV() function is used to find the mean average value for every 2 records in the dataset. The removed values are filled with the threshold value T in the cleaned dataset.

After cleaning the data, the features are extracted from the dataset to initiate the training of the model. The features of the dataset are completely extracted where the process is performed as

$$\begin{aligned}\mathrm{FSet}\left(\mathrm{INDT_{SET}(r)}\right) &= \frac{\max(INDT_{SET})}{\mathrm{len}(INDT_{SET})} \\ &* \sum_{\mathrm{i=1}}^{\mathrm{M}} \mathrm{len(G)} + (\mathrm{maxValue}(i+1) \\ &- \frac{\mathrm{minValue(i)}}{2}) \\ &+ \left[\sum_{i=1} mean(i+1) \right. \\ &\left. + \frac{maxVal(i) - minVal(i-1)}{count(i)}\right]\end{aligned}$$

The features extracted are considered for allocation of weights. The weights are allocated based on the features dependency and non dependency levels. The weight allocation process is performed as

$$\begin{aligned}WeFset(FSet[M]) &= \sum_{i=1} \sum_{j=i+1} \max\left(Fset\left(getValue(i)\right)\right) \\ &- \min\left(Fset\left(getValue(j)\right)\right) \\ &+ \log\left(\max_{1\le i,j\le M} \mathrm{Fset(i)} + \mathrm{simm(i,j)}\right)\end{aligned}$$

Here WeFset is the set that contains weights that are allocated to the features. Each features is allocated a weight based on the correlation value.

The non dependant feature selection process is performed to generate the final feature subset. The feature subset features will be used to train the models. Instead of considering all features, the feature subset will consider the best and most useful features for the intrusion detection model. The proposed model framework is shown in Figure 3.

An artificial neural network is a network in which computational elements or neurons are connected in a predetermined structure. It can generalize from sparse, imperfect data and learn from examples. ANN has been used well in many types of data-heavy programs. An input layer, several hidden layers, and a output layer make up a neural network. An equal number of neurons can be found in each successive layer. A neural network receives data at its input layer, processes it at its hidden layers, and returns the result at its output layer. Figure 4 depicts a common type of neural network model that includes a hidden layer.

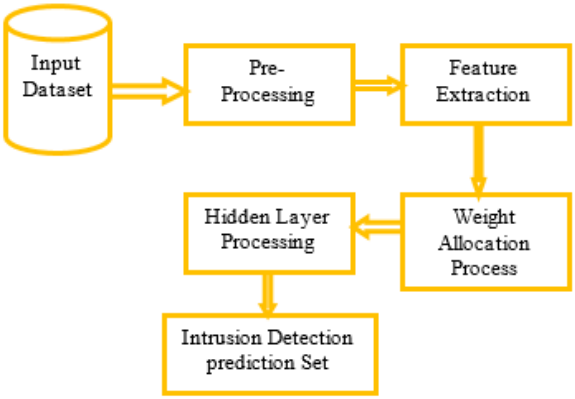

Figure 3. Proposed model framework

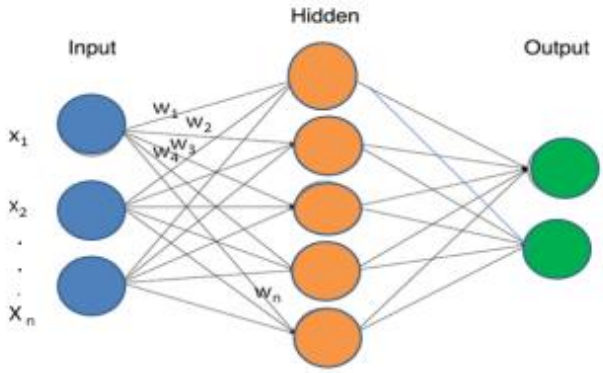

Figure 4. Neural network model

In order to increase accuracy level, a deep learning model is employed with layers representing features for intrusion detection. Weighted features are divided by a permutation layer by estimating the presence of the layer. If extracted feature mappings sets like map D and map E are created by summing their convolutions, various convolution kernels can be identified. It is standard procedure to input the attributes, add up the weighted features to make the final prediction set. The hidden layer processing is performed by providing the required inputs and the process is performed as:

$$HLayer(I,O,F,L) = \sum_{i=1,j=i+1}^{M} \max\big(WeFset(F(i))\big) - \frac{\min\left(WeFset\big(F(j)\big)\right)}{\mathrm{L}} * count(FSet) + \frac{\max\big(F(i+1,j+1)\big) + \sum_{j=j+1}^{M} \max\left(WeFset\big(F(j+1)\big)\right)}{\min\left(WeFset\big(F(j-1)\big)\right)} + T$$

Here I is the input, O is the output, F is the features allocated with weights and L is the length of the features selected.

Each neuron in this network receives input from M different sources, and the weights assigned to these sources add up to a total. B_i is the bias value that is multiplied by the activation function's input. First, we define the inputs to a neuron as B1, B2, B3,..., B_M, the weights as We1, We2, We3,..., WeM, the bias as B_i, and the output of the neuron as O, where an is the result of solving for B. where F is the activation function utilized to obtain the layer's output for use as input to the following layer. An artificial neural network consists of nodes and weights that must be learned based on the existing patterns. The activation function and the hidden layer analysis and output generation of final feature subset is performed as

$$aF = F\left(\sum_{i=0}^{M} We_i * I_i + B_i\right)$$

aF is the activation function applied on feature subset.

The final feature subset is used for intrusion detection in the cyber network. The intrusions are detected and the prediction list is generated that indicates nodes causing intrusions in the network. The prediction list is generated as

$$PredSet(WeFset[M]) = \max\Big(HLayer\big(FSet(i)\big)\Big) - \sum_{i=1} \frac{\max(\mathrm{aF(i)})}{\min(\mathrm{I_i})} * \mathrm{B_i} + \min\left(\mathrm{HLayer(Fset(i+1))}\right)$$

Done

4. RESULTS

Over the past decade, signal based cyber attacks have evolved into a major problem. There have been a number of attempts to develop ways for detecting signal based cyber attacks, each with varying degrees of success. In this research, a new feature selection approach for detecting and classifying signal based cyber attacks in a distributed setting is proposed. The network's regular state and the various attack kinds are both represented as distinct data classes. The proposed technique generates a set of pairwise feature subsets, selected for discriminating that class from each of the other classes, for each local binary classifier. This is in contrast to typical feature selection methods, which choose a distinct feature subset for each local binary classifier. It is demonstrated that the new feature selection strategy is superior in its ability to choose all pertinent features, leading to enhanced detection and classification precision.

In this research, an effective ANN based Intellectual Non

Dependant Feature Selection Model (ANN-INDFSM) is proposed that effectively extracts the signal based cyber attack features and performs feature reduction for accurate detection of signal based cyber attacks to maintain security. The proposed model is implemented in python and executed in Google Colab.

The dataset is considered from publicly available dataset provider kaggle with the link https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection. The dataset containd 125674 records in which the dataset is divided into training and testing purposes in the ratio 80:20. The dataset for the audit was provided, and it contains many different types of simulated intrusions in a military network. It simulated a common US Air Force LAN to provide a setting for collecting raw TCP/IP dump data from a network. Several simultaneous attacks were directed at the Network to make it feel more like a real world scenario. Data travels from a source IP address to a destination IP address in accordance with a predefined protocol over the course of a connection, which is specified as a sequence of TCP packets beginning and ending at a certain time period. The proposed model is compared with the traditional hybrid intrusion detection system based on a CFS-DE feature selection algorithm (HIDS-CFS-DE-FSA) [1]. The results represent that the proposed model performance in feature subset generation is high.

The choice of features is a crucial step in developing IDS. The term feature extraction is used to describe the procedure of converting unstructured data into a set of quantifiable features that may be further processed without losing any of the original data's contexts. In order to reduce the size of a dataset, feature extraction typically involves the generation of additional features from preexisting ones. As a result, this new, smaller set of features should be able to effectively describe the original set of features. The feature extraction accuracy levels of the existing and proposed models are shown in Figure 5.

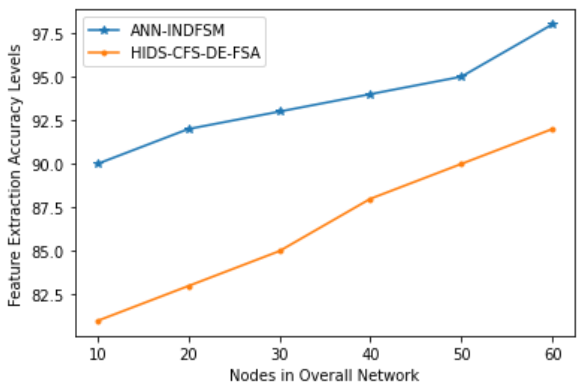

Figure 5. Feature extraction accuracy levels

Feature extraction is used to learn new features from the existing data set in order to discover relevant features in the data. By linearly combining the preexisting features, the feature extraction method provides us with a set of brand new features. All of the values for the new set of features will be different from the old set. The ultimate goal is to reduce the number of features necessary to adequately represent a problem space. The feature extraction time levels in milliseconds of the proposed and traditional models are shown in Figure 6.

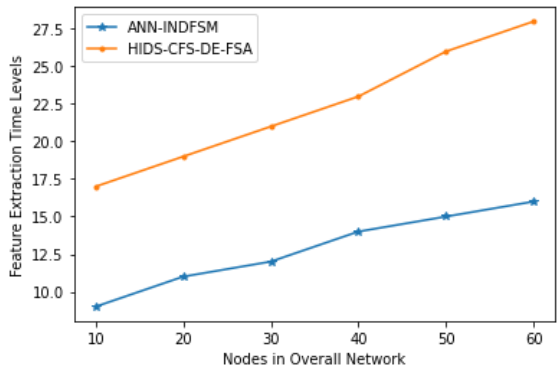

Figure 6. Feature extraction time levels

When considering features, it is common practice to give each feature a varied amount of weight in the overall feature set. The feature weights are allocated for each feature based on the correlation value. The feature weight allocation accuracy levels of the proposed and traditional models are shown in Figure 7.

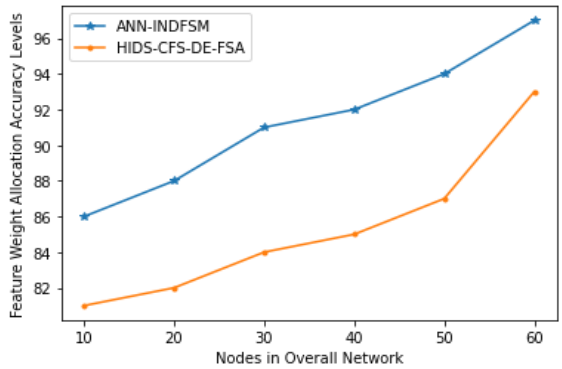

Figure 7. Feature weight allocation accuracy levels

Feature Selection is a technique for narrowing down the data used in proposed model by keeping only the most pertinent information and discarding irrelevant details. A subset generation method is a search method that uses certain search strategies as a sequential search to pick feature subsets. Feature selection, also known as spatial selection, attribute selection, or variable subset selection, is a technique used in machine learning and statistics to narrow down a large pool of potential features to a manageable subset of useful variables and predictors. The Figure 8 shows the Non Dependant Feature Selection Model Time in milliseconds Levels of the traditional and proposed models.

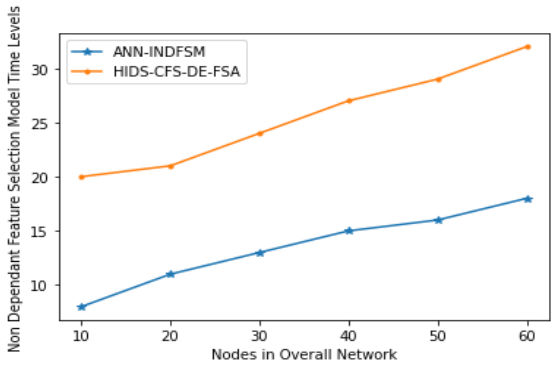

Figure 8. Non dependant feature selection model time levels

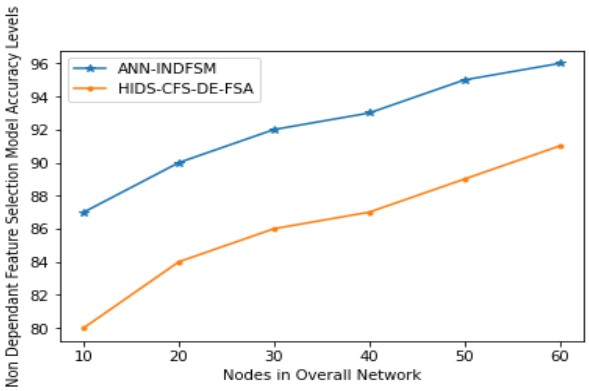

Figure 9. Non dependant feature selection model accuracy levels

Feature subset selection involves finding and discarding as much superfluous data as feasible. As a result, learning algorithms can function with greater efficiency and speed up the reduced dimensionality of the data. Feature Selection is a technique for narrowing down the data used in the model by keeping only the most pertinent information and discarding irrelevant details. The Figure 9 represents the Non Dependant Feature Selection Model Accuracy Levels of the existing and proposed models.

When a legitimate action is misidentified as malicious by IDS, this is known as a false positive or false alarm. One definition of a false positive is an unwarranted positive result. The most severe and potentially harmful state is a false negative state. This happens when an attack is actually being carried out but is mistakenly labelled as acceptable by the IDS. The false alarm rate levels of the existing and proposed models are shown in Figure 10.

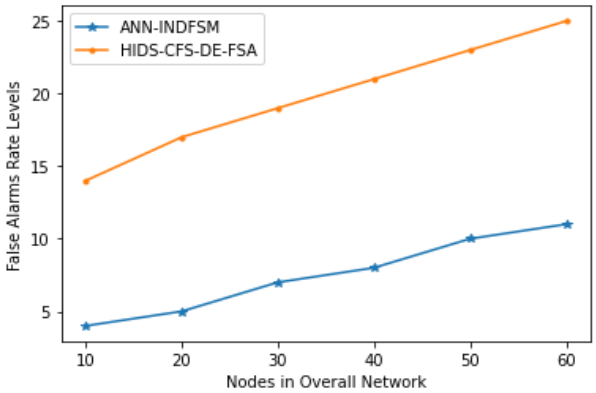

Figure 10. False alarms rate levels

In order to detect and counteract malicious activities, a network intrusion detection system is essential. An intrusion detection system's main benefit is that it may alert system administrators if there is a chance that an intrusion is taking place in the network. An intrusion detection system can be used to examine both the frequency and nature of attacks. As a result of this data, businesses will be able to improve their security measures. Businesses can also benefit from intrusion detection systems by fixing configuration errors and spotting flaws in their network devices. The Intrusion Detection Accuracy Levels of the existing and proposed models are shown in Figure 11.

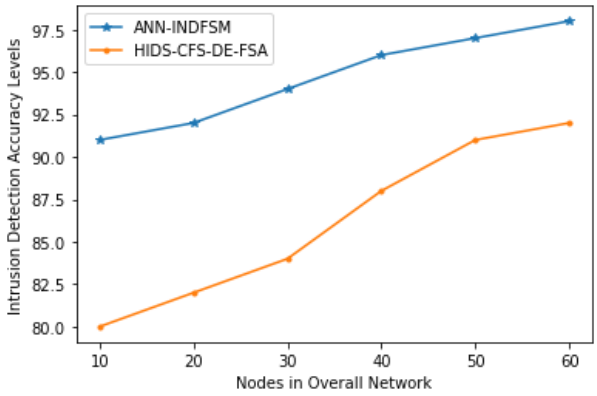

Figure 11. Intrusion detection accuracy levels

5. CONCLUSION

The Internet's popularity and the number of connected devices are expanding at a lightning rate as a direct result of the exponential development of technology. There has been a rise in the amount and heightened risk of network traffic as a result of this development. Learning intrusion detection systems have been developed with the goal of discovering previously unknown and complex attacks. Machine learning-based models are widely used in intrusion detection systems due to their high accuracy and speed. In today's technology world, where more and more people rely on electronic and digital technologies, protecting their privacy and security online has become a hot concern. As a result, cyber security researchers are always looking for novel and effective methods to combat online threats. An IDS is designed to ward off hacking attempts on a computer or network. In other words, it lessens the chances of harm occurring to a system from outside sources. Classifying design models by the feature reduction techniques they employ facilitates analysis. The results suggest that by paying close attention to the feature selection approach, the classifier's prediction performance may be enhanced in terms of high detection rate and accuracy, low false alarm rate, and shorter training and testing times. In this research, an effective ANN based Intellectual Non Dependant Feature Selection Model is proposed that effectively extracts the signal based cyber attack features and performs feature reduction for accurate detection of signal based cyber attacks to maintain security. The proposed model achieves 97% accuracy level in detecting intrusions. In future, the model can be optimized by applying hybrid optimizations models and the training samples can also be increased that further improves the detection rate.

REFERENCES

[1] Zhao, R., Mu, Y., Zou, L., Wen, X. (2022). A hybrid intrusion detection system based on feature selection and weighted stacking classifier. IEEE Access, 10: 71414-71426. https://doi.org/10.1109/ACCESS.2022.3186975

[2] Lee, S.J., Yoo, P.D., Asyhari, A.T., Jhi, Y., Chermak, L., Yeun, C.Y., Taha, K. (2020). IMPACT: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction. IEEE Access, 8: 65520-65529. https://doi.org/10.1109/ACCESS.2020.2985089

[3] Aminanto, M.E., Wicaksono, R.S.H., Aminanto, A.E., Tanuwidjaja, H.C., Yola, L., Kim, K. (2022). Multi-class intrusion detection using two-channel color mapping in IEEE 802.11 wireless Network. IEEE Access, 10: 36791-36801. https://doi.org/10.1109/ACCESS.2022.3164104

[4] Saharkhizan, M., Azmoodeh, A., Dehghantanha, A., Choo, K.K.R., Parizi, R.M. (2020). An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic. IEEE Internet of Things Journal, 7(9): 8852-8859.https://doi.org/10.1109/JIOT.2020.2996425

[5] Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A., Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7: 41525-41550. https://doi.org/10.1109/ACCESS.2019.2895334

[6] Ullah, I., Mahmoud, Q.H. (2022). Design and development of RNN anomaly detection model for IoT networks. IEEE Access, 10: 62722-62750. https://doi.org/10.1109/ACCESS.2022.3176317

[7] Li, Z., Rios, A.L.G., Trajković, L. (2021). Machine learning for detecting anomalies and intrusions in communication networks. IEEE Journal on Selected Areas in Communications, 39(7): 2254-2264. https://doi.org/10.1109/JSAC.2021.3078497

[8] Wang, X., Fidge, C., Nourbakhsh, G., Foo, E., Jadidi, Z., Li, C. (2022). Anomaly detection for insider attacks from untrusted intelligent electronic devices in substation automation systems. IEEE Access, 10: 6629-6649. https://doi.org/10.1109/ACCESS.2022.3142022

[9] Hong, W.C., Huang, D.R., Chen, C.L., Lee, J.S. (2020). Towards accurate and efficient classification of power system contingencies and cyber-attacks using recurrent neural networks. IEEE Access, 8: 123297-123309. https://doi.org/10.1109/ACCESS.2020.3007609

[10] Qureshi, S., He, J., Tunio, S., Zhu, N., Akhtar, F., Ullah, F., Nazir, A., Wajahat, A. (2021). A hybrid DL-based detection mechanism for cyber threats in secure networks. IEEE Access, 9: 73938-73947. https://doi.org/10.1109/ACCESS.2021.3081069

[11] Habibi, M.R., Sahoo, S., Rivera, S., Dragičević, T., Blaabjerg, F. (2021). Decentralized coordinated cyberattack detection and mitigation strategy in DC microgrids based on artificial neural networks. IEEE Journal of Emerging and Selected Topics in Power Electronics, 9(4): 4629-4638. https://doi.org/10.1109/JESTPE.2021.3050851

[12] Saheed, Y.K., Arowolo, M.O. (2021). Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. IEEE Access, 9: 161546-161554. https://doi.org/10.1109/ACCESS.2021.3128837

[13] Kuang, X., Liu, H., Wang, Y., Zhang, Q., Zhang, Q., Zheng, J. (2019). A CMA-ES-Based adversarial attack on black-box deep neural networks. IEEE Access, 7: 172938-172947. https://doi.org/10.1109/ACCESS.2019.2956553

[14] Wang, J., Tan, Y., Liu, J., Zhang, Y. (2020). Topology poisoning attack in SDN-enabled vehicular edge network. IEEE Internet of Things Journal, 7(10): 9563-9574. https://doi.org/10.1109/JIOT.2020.2984088

[15] Albahar, M.A., Al-Falluji, R.A., Binsawad, M. (2020). An empirical comparison on malicious activity detection using different neural network-based models. IEEE Access, 8: 61549-61564. https://doi.org/10.1109/ACCESS.2020.2984157

[16] Al-Abassi, A., Karimipour, H., Dehghantanha, A., Parizi, R.M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. IEEE Access, 8: 83965-83973. https://doi.org/10.1109/ACCESS.2020.2992249

[17] Zhu, J., Jang-Jaccard, J., Watters, P.A. (2020). Multi-loss Siamese neural network with batch normalization layer for malware detection. IEEE Access, 8: 171542-171550. https://doi.org/10.1109/ACCESS.2020.3024991

[18] Pasetti, M., Ferrari, P., Bellagente, P., Sisinni, E., de Sá, A.O., do Prado, C.B., David, R.P., Machado, R.C.S. (2021). Artificial neural network-based stealth attack on battery energy storage systems. IEEE Transactions on Smart Grid, 12(6): 5310-5321. https://doi.org/10.1109/TSG.2021.3102833

[19] Zhou, X., Liang, W., Shimizu, S., Ma, J., Jin, Q. (2020). Siamese neural network based few-shot learning for anomaly detection in industrial cyber-physical systems. IEEE Transactions on Industrial Informatics, 17(8): 5790-5798. https://doi.org/10.1109/TII.2020.3047675

[20] de Araujo-Filho, P.F., Kaddoum, G., Campelo, D.R., Santos, A.G., Macêdo, D., Zanchettin, C. (2020). Intrusion detection for cyber–physical systems using generative adversarial networks in fog environment. IEEE Internet of Things Journal, 8(8): 6247-6256. https://doi.org/10.1109/JIOT.2020.3024800

[21] Andresini, G., Appice, A., Di Mauro, N., Loglisci, C., Malerba, D. (2020). Multi-channel deep feature learning for intrusion detection. IEEE Access, 8: 53346-53359. https://doi.org/10.1109/ACCESS.2020.2980937

[22] Larriva-Novo, X.A., Vega-Barbas, M., Villagrá, V.A., Rodrigo, M.S. (2020). Evaluation of cybersecurity data set characteristics for their applicability to neural networks algorithms detecting cybersecurity anomalies. IEEE Access, 8: 9005-9014. https://doi.org/10.1109/ACCESS.2019.2963407

[23] Pacheco, J., Benitez, V.H., Felix-Herran, L.C., Satam, P. (2020). Artificial neural networks-based intrusion detection system for internet of things fog nodes. IEEE Access, 8: 73907-73918. https://doi.org/10.1109/ACCESS.2020.2988055

[24] Li, D., Li, Q., Ye, Y., Xu, S. (2021). A framework for enhancing deep neural networks against adversarial malware. IEEE Transactions on Network Science and Engineering, 8(1): 736-750. https://doi.org/10.1109/TNSE.2021.3051354

[25] Al-Abassi, A., Jahromi, A.N., Karimipour, H., Dehghantanha, A., Siano, P., Leung, H. (2021). A self-tuning cyber-attacks' location identification approach for critical infrastructures. IEEE Transactions on Industrial Informatics, 18(7): 5018-5027. https://doi.org/10.1109/TII.2021.3133361

[26] Wang, Z., Song, M., Zheng, S., Zhang, Z., Song, Y., Wang, Q. (2019). Invisible adversarial attack against deep neural networks: An adaptive penalization approach. IEEE Transactions on Dependable and Secure Computing, 18(3): 1474-1488. https://doi.org/10.1109/TDSC.2019.2929047

[27] Ma, L., Wang, Z., Liu, H., Alsaadi, F.E., Alsaadi, F.E. (2022). Neural-network-based filtering for a general class of nonlinear systems under dynamically bounded

innovations over sensor networks. IEEE Transactions on Network Science and Engineering, 9(3): 1395-1408. https://doi.org/10.1109/TNSE.2022.3144484

[28] Fotiadou, K., Velivassaki, T.H., Voulkidis, A., Railis, K., Trakadas, P., Zahariadis, T. (2020). Incidents information sharing platform for distributed attack detection. IEEE Open Journal of the Communications Society, 1: 593-605. https://doi.org/10.1109/OJCOMS.2020.2989925

[29] Wang, Y., Zhang, Z., Ma, J., Jin, Q. (2021). KFRNN: An effective false data injection attack detection in smart grid based on Kalman filter and recurrent neural network. IEEE Internet of Things Journal, 9(9): 6893-6904. https://doi.org/10.1109/JIOT.2021.3113900

[30] Li, F., Li, Q., Zhang, J., Kou, J., Ye, J., Song, W., Mantooth, H.A. (2020). Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network. IEEE Transactions on Power Electronics, 36(3): 2495-2498. https://doi.org/10.1109/TPEL.2020.3017935