A review of deep learning based intrusion detection systems

Yutong Wei, Mingjia Shangguan*

Xiamen University, Xiamen, China

* Corresponding Author Email: mingjia@xmu.edu.cn

Abstract. Network security is a key issue in the era of rapid Internet development and new technologies are needed to enhance the security protection of network systems. As the first line of defence for the security of network systems, IDS is considered to be one of the important network tools for managing network security. Traditional network intrusion detection methods usually use machine learning techniques. However, deep learning, a more powerful machine learning method, has the advantages of mature technology, wide applicability and high accuracy, and has shown its advantages in various fields such as image recognition, natural language processing and computer vision. It can also be applied to network security detection, as it can effectively handle large-scale, complex datas and detect unknown, sophisticated network attacks. This paper will provide a summary of machine learning techniques and deep learning techniques in intrusion detection systems, as well as examples of IDSs using deep learning, and conclude with a summary and outlook.

Keywords: IDS, deep learning, intrusion detection.

1. Introduction

With the rapid growth of the Internet, today's society is highly integrated with networked systems, and along with this integration of all types of datas and information into networked systems, there are numerous cyber security incidents of all kinds. Cybersecurity is a major area of investigation as all government-based, military, commercial, financial and civil operations collect, process and store large amounts of datas on computers and other systems. Businesses must organise their activities through their entire information infrastructure in order to defend themselves in terms of cyber security [1]. As such, cyber security detection technology has a major role to play in maintaining the security of information in society. In general, network security technology refers to techniques that protect programmes, networks, computers and datas from being damaged, attacked or accessed by unauthorised persons [2]. Intrusion detection technology is a network security technique that checks a network or system for malicious activity or policy violations [3] and is primarily used to observe network traffic for malicious transactions and to send alerts or take proactive reactive measures as soon as they are observed. Intrusion detection systems are a key network security technology that monitors and detects potential intrusions in the network through real-time security monitoring techniques and security scanning. Real-time security monitoring technology provides real-time monitoring of network traffic and system activity in order to detect abnormal or suspicious behaviour in a timely manner. Security scanning technologies, on the other hand, are used to proactively scan network systems for known vulnerabilities or traces of attacks so that appropriate defensive measures can be taken in a timely manner. The effective use of these technologies can greatly enhance the accuracy and responsiveness of network intrusion detection systems.

However, as network attacks become increasingly complex and diverse, traditional rule-based intrusion detection methods gradually fail to meet the growing demand for network security detection [4]. To address this challenge, researchers have begun to explore the application of machine learning techniques in the field of intrusion detection. Machine learning techniques are capable of handling a large number of rules and complex problems, but there are some limitations in terms of accuracy, training time and recognition capability. Therefore, in recent years, the rapid development of deep learning techniques has provided new opportunities for network intrusion detection.

Traditional machine learning methods are widely used in intrusion detection systems, with algorithms such as Support Vector Machines, K-Means and Decision Trees. These methods typically

require datas pre-processing and feature engineering to discover important features and select machine learning algorithms suitable for classification. However, deep learning-based intrusion detection systems are able to automatically learn key features in the datas by optimising feature engineering [5] to provide meaningful discriminative information to the network. This automated feature learning can overcome the gradient disappearance problem of traditional methods and enables multi-level network learning, thereby improving the performance and effectiveness of the system.

Deep learning-based intrusion detection systems have a wide range of applications in a number of areas such as the Internet, cloud computing and in-vehicle networks. Such systems perform better and are able to effectively deal with complex network intrusions, improve detection accuracy and reduce false positives. Due to its excellent performance and adaptability, deep learning-based intrusion detection systems are widely used to secure network systems and sensitive datas.

The aim of this paper is to review the recent literature on deep learning-based network intrusion detection, to identify and analyse current trends and challenges, and to suggest suitable scenarios for applying different deep learning models to different network attacks. The paper is organised as follows: Section 1 provides a generalisation of the existing cyber security threats. Section 3 provides a brief overview of traditional approaches and their applications in cyber security detection, and identifies their shortcomings. Section 3 introduces the basic concepts and principles of deep learning and discusses the main deep learning models for cyber security detection, such as multilayer perceptrons (MLPs), convolutional neural networks (CNNs), and generative adversarial networks (GANs), and points out their advantages. Section 4 presents some example applications using different deep learning techniques to prevent various cyber threats. Section 5 summarises the paper and outlines future research directions.

2. Existing cyber security threats

Network security systems are exposed to various types of network security threats, such as computer viruses, hacking and denial of service attacks. A network intrusion is a malicious and destructive unwanted network traffic activity that causes damage to a computer network. This malicious intrusion can cause a system or network to become vulnerable and thus susceptible to multiple attacks. For example, it may be through a Denial of Service (DoS) attack, an identity theft attack to steal user identity datas, a spam or phishing attack to obtain sensitive user datas. In general, network intrusions can be divided into the following four categories: DoS (Denial of Service), R2L (Unauthorised Access to Remote Computers), U2R (Unauthorised Access to Local Root Rights), Probe (Surveillance and Another Probe).

2.1 DoS (Denial of Service)

Denial of service, also known as a flood attack, refers to an illegal attempt to interrupt or disrupt the normal operation of a host computer or network as a form of intrusion. An attacker temporarily disrupts or stops services by exhausting the network or system resources of the target computer, thereby rendering it inaccessible to normal users. Broadly speaking, it includes attacks through vulnerabilities such as buffer overflows that cause services to hang, sending a large number of packets that use up the resources allocated to the service by the system, and sending a large number of packets that use up all system resources. One common type of attack is called a distributed denial-of-service attack (DDoS attack), which is a type of attack in which hackers use two or more compromised computers on a network as "zombies" to launch a "denial-of-service" attack on a specific target. "DoS attacks are common in banks, credit card payment gateways and some web games.

2.2 R2L (Remote to Local)

R2L, an intrusion in which a remote, unauthorised user illegally gains user privileges on the local host. The attacker attempts to gain local access without an account on the target computer. This type of intrusion is often combined with a U2R attack.

2.3 U2R (User to Root)

U2R, an intrusion in which a local unauthorised user illegally obtains the privileges of a local superuser or administrator. An attacker, with local access to the target system already available, exploits a system vulnerability to escalate his privileges from those of a simple user to those of a super user/administrator. One of the most common types of U2R is a buffer overflow, where an attacker attempts to fill a buffer with root privileges and execute malicious code.

2.4 Probe (Surveillance or probe)

Probe, the illegal scanning of a host or network for vulnerabilities, searching for system configurations or network topology. The attacker explores the target network to gather information about the hosts.

3. Traditional machine learning methods for network intrusion detection

An IDS (Intrusion Detection System) is a security tool designed to detect malicious activity and security vulnerabilities in a computer system, network or application and can address existing cyber security threats. Depending on the approach used, IDS systems can be divided into traditional and machine learning or deep learning based IDS systems. Traditional IDS work on the principle that datas is collected by sensors and sent to an analysis engine, which examines the datas and detects intrusions, and once an intrusion is detected, the reporting system sends an alert to the network administrator [6]. In recent years, a range of machine learning-based IDS models have been proposed to detect and mitigate cyber security threats based on whether system or network behaviour matches known attack signatures, deviates from normal values or exceeds thresholds. The main idea behind machine learning-based approaches for network intrusion detection is that after pre-processing the datas, important features are discovered through feature engineering, machine learning algorithms for classification or regression are selected, and the models are then trained and evaluated to classify or predict security threats [7]. Commonly used machine learning algorithms include support vector machines (SVM), k-nearest neighbour (KNN) algorithms, decision trees (DTs), Bayesian, random forest and K-means algorithms.

3.1 Support vector machines (SVM)

Support vector machines (SVMs) are a basic binary classification model, a linear classifier defined by maximising the interval over a feature space.The SVM model represents instances as points in space, using a straight line to separate datas points, and classifies them by transforming the interval maximisation into a problem of solving a convex quadratic programming. It is worth noting that support vector machines require full labelling of the input datas and are only directly applicable to two-class tasks, while for multi-class tasks they need to be reduced to a few binary problems first.

3.2 K-Means

The K-Means algorithm is a clustering algorithm based on Euclidean distance, which considers that the closer two targets are, the greater the similarity. the basic idea of K-Means is to divide n points (which can be a single observation of a sample or an instance) into K clusters (clusters), assign the datas points to one of the K groups according to the characteristics of the datas set, so that each point belongs to the cluster corresponding to the nearest mean (i.e. the centre of clustering, centroid) corresponding to the cluster, and the target is classified by repeating the above process until the centre of gravity does not change.

3.3 K Nearest Neighbors (KNN)

The KNN algorithm is an instance-based classification algorithm that allows classification by measuring the distance between different feature values. The basic idea is to predict the class of an

unknown stronghold based on the class of the k nearest neighbours to the predicted unknown stronghold. It is worth noting that the k-value is a key factor in the accuracy of the prediction.

3.4 Decision Trees (DTs)

A Decision Tree is a special type of tree structure consisting of a decision diagram and possible outcomes (e.g. cost and risk) that is used to assist in decision making. Decision trees have a single output and are often used to solve classification problems. They use the idea of classification to construct a mathematical model based on the characteristics of the datas so that the datas can be filtered for a decision objective. Each node in the tree represents an object, each leaf node corresponds to a classification (decision outcome), and non-leaf nodes correspond to a division on an attribute that divides the sample into subsets based on the different values taken on that attribute.

3.5 Random Forest (RF)

Random Forest is an algorithm that integrates multiple decision trees using the Bagging idea of integrated learning. A single decision tree is a weak classifier, and a random forest of many decision trees is a strong classifier. The basic idea of a random forest is to first classify each decision tree and then vote on a number of classifications to form a strong classifier. Ideally, we choose the classification with the most votes based on each vote for each decision tree.

3.6 Bayes

Bayesian algorithm is a machine learning method based on Bayes' theorem, which presents the distribution of known dataset attributes based on the distribution of categories and features in the training samples. Commonly used probabilistic models for machine learning based on Bayes' theorem include Naive Bayes and Bayesian network. Among them, Naive Bayes is a classification algorithm that assumes conditional independence of features, which first learns the joint probability distribution of inputs and outputs based on assumptions, and then uses Bayes' theorem to compute the maximum posterior probability for new instances. Bayesian network, on the other hand, is an algorithm that relaxes the assumption of conditional independence.

3.7 Summary

ML enables machines to learn from datas without being explicitly programmed to do so. ML has proven to be very effective in dealing with problems requiring a large number of rules and inefficiently complex problems compared to earlier IDS approaches. In addition, ML has shown a strong ability to adapt to new datas and acquire features, which is important in today's changing and evolving environments such as networked systems.

However, there are a number of limitations to current traditional machine learning based IDS models. Firstly, ML methods have a weak and shallow learning behaviour, feature extraction and datas pre-processing are not optimised enough to provide low feature selection and classification performance, which will lead to high false alarm rates and low detection rates in IDS systems. Second, traditional ML algorithms are not adapted to modern datassets containing new attack classes whose features are incompatible with ML. Also, when attacks have different feature dimensions or new features are characterised by complexity, ML algorithms are unable to identify them due to their weak learning and classification capabilities, which leads to its incompatibility with intelligent evaluation and predictive foundations with large amounts of datas and high-dimensional learning. Finally, due to the high complexity of the models, they lack the flexibility and scalability to handle large amounts of network traffic datas [8].

4. Deep learning methods for network intrusion detection

Machine learning algorithms are often very concerned with the feature engineering component, which requires the algorithm to learn a model that is only as good as its input datas, and there must

be enough discriminative information in the datasset, but the performance of a machine learning algorithm can suffer greatly when the information is hidden in meaningless features. Unlike shallow machine learning, deep learning optimises feature engineering to automatically learn features from noisy datas, providing the network with meaningful discriminative information so that it can learn more effectively, which will help overcome the problem of gradient disappearance and perform multi-layer networks.

As a result, several researchers have recently proposed the use of deep learning (DL) methods to detect and mitigate security threats. Deep learning (DL) is a machine learning (ML) approach in the field of artificial intelligence (AI) that mimics the workings of biological neural networks in the human brain [9] and has been widely used and recognised in areas such as intrusion detection, has shown powerful analytical capabilities in areas such as image processing, bioinformatics, natural language processing, and is also widely used in the Internet of Things for edge/fog applications such as computing, big datas analysis, video processing and speech processing.

The main deep learning models commonly used in network intrusion detection include multilayer perceptron (MLP), convolutional neural network (CNN), recurrent neural network (RNN) and generative adversarial network (GAN).

4.1 Multi-Layer Perceptron (MLP)

Multi-Layer Perceptron (MLP) is a feed-forward artificial neural network (ANN) with multiple hidden layers and is a fundamental model for deep learning.MLPs can perform classification or regression tasks by learning mapping relationships between a set of features and targets, based on them. Such neural networks can be applied in scenarios where network anomalies or attacks are detected, such as intrusion detection, malware analysis, security threat analysis, malicious botnet traffic detection, etc [10].

The structure of an MLP usually consists of three types of layers: an input layer, a hidden layer and an output layer (Fig.1). The input layer is responsible for receiving values from the datasset, the hidden layer is responsible for processing and computing the datas, and the output layer is responsible for generating the results. the core elements of an MLP are weights, biases and activation functions. it is a fully connected network, i.e. nodes in each layer are connected to all nodes in the next layer and each connection has a weight value. Each layer also has a bias node which does not receive any input but affects the output of the next layer. the MLP calculates the output values based on the weights and biases of each layer by means of a forward propagation algorithm (1). In order for the network to learn a non-linear mapping of functions, each node also needs to use an activation function (e.g. ReLU, Tanh, etc.) to increase the complexity of the network.

$$y = f(\sum_{i=0}^{M} w_{ij} x_j) \tag{1}$$

MLP is trained using optimisation methods such as back propagation algorithms and gradient descent. The back propagation algorithm is a supervised learning technique that calculates the total error in the output layer and back propagates these errors along the network to find the gradient of each connection. Optimisation methods such as gradient descent adjust the values of the weights in the network according to the gradient, causing the error in the output layer to gradually decrease. By continually optimising the network weights, the MLP can eventually map the input to the target output accurately.

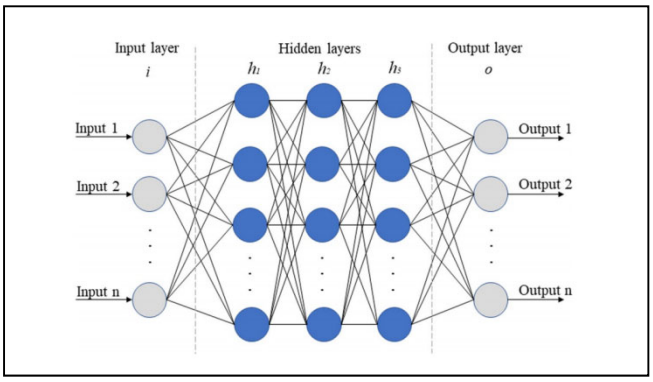

Figure 1. Basic MLP model [11]

4.2 Convolutional Neural Networks (CNN)

Convolutional Neural Networks (CNN), a deep learning model, features local perception and parameter sharing. It automatically learns feature representations from image datas by mimicking the perceptual mechanisms in the human visual system and is able to extract local features of the datas at a higher resolution and transform them into neural networks with more complex features at a lower resolution [12]. This type of network has been successfully used for recognition of images and videos, classification and text processing, and can also be used for cyber security, e.g. intrusion detection, IoT networks, classification and detection of malware variants, Android malware detection [1].

A basic neural network consists of an input layer, a hidden layer, and an output layer. Based on this, the CNN is further refined into a convolutional layer, a pooling layer (also known as a sub-sampling layer) and a fully connected layer (Fig.2). The core idea is to use the convolutional and pooling layers to extract local features in the image, and to combine and classify the features through the fully-connected layer.

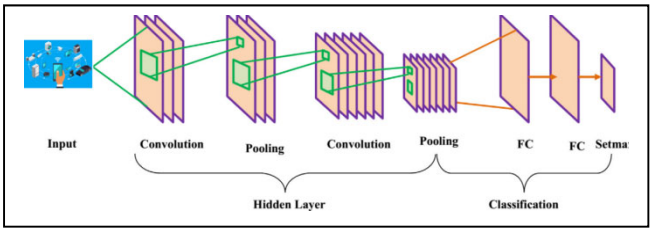

Figure 2. Structure of a convolutional neural network [13]

The convolution layer extracts features by translating over the original image. A filter (convolution kernel, a 3×3 matrix) is used to convolve with the input image to obtain a convolution feature (activation map or feature map) to extract features from different regions of the image, and then an activation function (ReLU) is used to replace all negative pixel values in the feature map with zero, introducing non-linearity and obtaining a corrected feature map. The effect of convolution varies from filter to filter, and different features such as edges, textures and shapes can be learned by changing the value of the filter matrix before the convolution operation to perform edge detection, sharpening and blurring. The convolution layer effectively reduces the number of parameters in the model and increases the efficiency of feature extraction through parameter sharing and sparse connectivity.

The pooling layer controls overfitting by reducing the number of parameters learned through post-feature sparse parameters, reducing the complexity of the network, reducing the size of the feature map and retaining important feature information. A common pooling operation is max pooling, which selects the maximum value from a local region as the pooling result, thus reducing the spatial size of the feature map and preserving the main features. By stacking the convolution and pooling layers several times, the CNN is able to gradually extract higher-level feature representations of the image.

The fully-connected layer is an MLP that performs classification, loss calculation (learning features), combines features extracted from the convolutional and pooling layers and outputs the final classification result. The fully connected layer learns the combinatorial and abstract representation of features through weight connections between neurons, and then uses an activation function (e.g. Softmax) to perform a non-linear mapping of the output of the fully connected layer to enhance the representation of the model.

CNNs are trained by a back-propagation algorithm, where the loss function is usually a Cross-Entropy (Cross-Entropy) loss function. Through back-propagation, CNNs can update the weight parameters in the network based on the difference between the actual labels and the model output, allowing them to gradually learn better feature representation and classification capabilities.

4.3 Recurrent Neural Networks (RNN) / Long Short Term Memory Recurrent Neural Networks (LSTM)

Recurrent Neural Networks (RNN) are fully connected feedback networks that can use information from the previous input to influence subsequent inputs, thus improving the reliability of the model. This network structure maintains the continuity of information and is well suited for processing time series datas [14]. As many tasks or datas related to cyber security have time-series characteristics, RNNs have a wide range of applications in various areas of cyber security.

RNNs consist of an input layer, a hidden layer and an output layer. The difference with traditional neural networks is that each cycle takes the output of the previous hidden layer as the input of the next hidden layer, i.e. the hidden layer is a circular feedback loop whose value depends not only on the input of the current cycle but also on the value of the hidden layer of the last cycle, which allows them to retain information in memory over time.

However, RNNs suffer from the problem of long-term dependency, i.e. when the time series is too long, gradients may disappear or explode, resulting in the inability to use information from farther in the past effectively. To solve this problem, an improved model based on RNN, LSTM (Long Short-Term Memory), has been proposed. LSTM is able to perform long short-term memory functions by selectively retaining or ignoring important or unimportant information from longer sequences in the past. Its neurons are connected in a temporal sequence and have a more complex hidden neuron structure that maintains the memory of previous inputs at arbitrary time intervals and allows it to achieve long-term dependency.

An LSTM cell contains three gate structures, a forget gate, an input gate and an output gate, to control the flow of information in the LSTM cell (Fig.3). The forget gate is responsible for filtering out still useful information from the previous state cell and removing obsolete or irrelevant information, the input gate is responsible for adding new information to the cell state, and the output gate is responsible for determining and controlling the output based on the cell state and the current input.

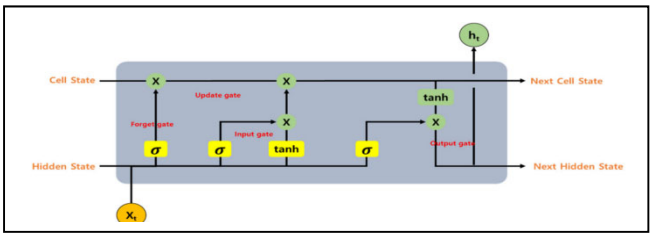

Figure 3. LSTM network architecture [15]

The LSTM network is well suited for learning and analysing sequential datas, such as classification, processing and prediction based on time-series datas, due to its long and short-term memory function [10]. It is also very suitable for handling large amounts of security sequential datas in the field of cyber security, such as network traffic datas, time-dependent malicious activities, etc.

4.4 Generative Adversarial Network (GAN)

A Generative Adversarial Network (GAN) is an adversarial model consisting of two neural networks (MLPs) that learn the distribution of generated datas by playing against each other.

The generator is a network that maps random noise to datas. Its goal is to generate datas that is as realistic as possible and trick the discriminator into deciding that it is true; the discriminator is a binary network that determines whether the datas is true or false, and its goal is to correctly distinguish between true datas (with probability 1) and generated datas (with probability 0), and reject the generator. and to reject the generator's deception (Fig.4).

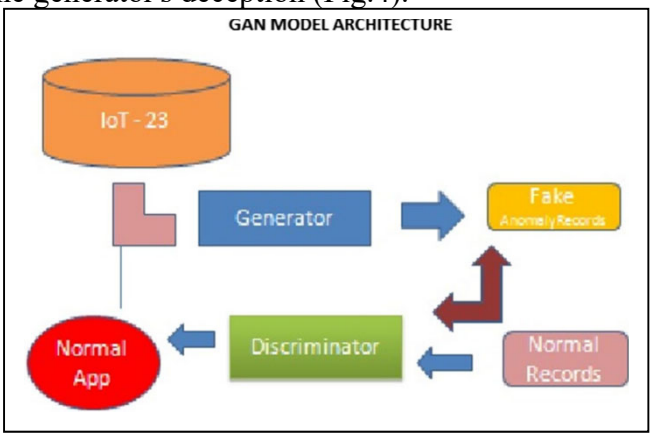

Figure 4. GAN model architecture [16]

GANs train generators and discriminators by alternating optimisation so that they reach a Nash equilibrium, i.e. the generators are able to generate datas that is consistent with the distribution of real datas, while the discriminators are unable to distinguish between real and fake datas. The optimisation process of the two networks is based on their respective loss functions (2), generally using a cross-entropy loss function, to measure their difference from the target. The performance of the two networks is continuously improved by adjusting the network parameters through error back propagation (BP) algorithms and optimisation methods such as gradient descent to eventually learn a reasonable mapping function.

$$\begin{aligned} &\min_G \max_D V(D,G) = E_{x\sim P_{data}(x)}[\log D(x)] + E_{z\sim P_z(x)}[1-\log D(G(z))] \\ &L_G = H(1, D(G(z))) \\ &L_D = H(1, D(x)) + H(0, D(G(z))) \end{aligned} \tag{2}$$

4.5 Summary

Compared to ML algorithms, DL algorithms overcome the ML slow training problem, are better suited to handle large, diverse and high-dimensional network traffic datas, and can efficiently train non-linear models and detect new forms of attacks with high accuracy. DL algorithms also enable automatic feature engineering without human intervention, providing meaningful information to the deep neural network structure so that it can learn more efficiently.

5. Examples of deep learning techniques in IDS

As the first line of defence for the security of networked information systems, IDS is considered to be one of the most important network tools for managing network security. In recent years, a range of technologies for intrusion detection systems have been introduced to detect unknown attacks, combining a variety of approaches, with deep learning being a key focus for building new intrusion detection systems that are important in environments such as in-car networks, credit card fraud, power systems, cloud computing and the Internet of Things.

5.1 CNN

For credit card fraud detection, Kang Fu et al. proposed a CNN-based fraud detection framework in 2016 [17] to capture the intrinsic patterns of fraudulent behaviours learned from labelled datas. They used a cost-based sampling approach to generate different numbers of frauds and proposed a feature transformation method that can adapt the CNN model to model more complex consumer behaviour through transaction entropy. Experimental results on actual transaction datas from commercial banks show that the method outperforms other state-of-the-art methods.

For the reliable monitoring of power systems, based on the state estimator of the phasor measurement unit (PMC), Sagnik Basumallik et al. in 2019 [18] proposed a convolutional neural network for packet-datas anomaly detection. They used a convolutional neural network (CNN) datas filter with gradient descent and categorical cross-entropy loss to validate it on PMU datas. The results show that the filter has high classification accuracy compared to other deep learning algorithms such as recurrent neural networks (RNN) and long short-term memory (LSTM) as well as machine learning algorithms such as SVM.

For intrusion detection in in-vehicle networks, based on residual neural networks (Res-Net), Araya Kibrom Desta et al. in 2022 [19] proposed an intrusion detection system (IDS) for in-vehicle networks using a convolutional neural network trained on recursive graphs. They trained the CNN with recursive images generated from the coded labels of arbitration ids of CAN frames to capture the temporal dependencies in the arbitration id sequences. The results show that the system has superior performance with an accuracy of 0.999 for the datasset test results and 0.999 for the classification of a simulated attack by the target vehicle at an attack frequency of 10 ms.

5.2 RNN

For binary classification of intrusion detection in network traffic datas, Abien Fred Agarap in 2019 [20] proposed a neural network architecture that combines a gated recurrent unit (GRU) and a support vector machine (SVM). In the final output layer of the GRU model, they introduced a linear support vector machine (SVM) as an alternative to Softmax, and the cross-entropy function should be replaced with a margin-based function. The results show that the model has a training accuracy of up to 81.54% and a testing accuracy of up to 84.15%, which is relatively higher than the traditional GRU-Softmax model.

To address the problem of security threats occurring during datas transmission in cloud environments, Varun Prabhakaran et al. proposed an attention-based recurrent convolutional neural network (RCNN) structure in 2020 [21]. They encrypt. We introduced the Elliptic Curve Cryptography (ECC) method to improve the security level performance of non-intrusive datas. The method shows maximum break time results compared to other methods and can withstand different classical attacks.

For Internet security, P. Rajesh Kanna et al. in 2022 [8] proposed an efficient hybrid IDS model built on MapReduce-based Black Widow Optimised Convolutional Long Short Term Memory (BWO-CONV-LSTM) network. They obtained a more desirable architecture through the artificial bee colony (ABC) algorithm for feature selection and the hyperparameters of the network were optimized by BWO. It is shown that the IDS model based on BWO-CONC-LSTM has a higher correct detection rate, shorter computation time and better classification coefficients.

For the problem of detecting complex intrusions and DDoS attacks in Internet of Things (IoT) and Big datas systems, Asma Belhadi et al. in 2023 [22] proposed a population intrusion detection framework using datas mining and hybrid recurrent neural networks to retrieve group traffic anomalies in the IoT. Their RNN approach identifies individual outliers from IoT datas and uses a new strategy based on decomposition to derive group outliers from IoT datas. The results show that the proposed framework is significantly superior compared to the baseline approach.

5.3 GAN

To address the security of Controller Area Network (CAN) buses in vehicles, Eunbi Seo et al. proposed a Generative Adversarial Network (GAN) based IDS in 2018 [23].They encoded a large number of CANs with a simple single heat vector to improve the performance and speed of the model, and combined a first discriminator for detecting known attack datas and a second discriminator for detecting unknown attack datas to improve the detection accuracy of the model. The results show that the model offers advantages in scalability, effectiveness and security, detecting approximately 1,954 CAN messages in just 0.18 seconds.

For Cyber-Physical Systems (CPS), Paulo Freitas de Araujo-Filho et al. proposed a novel low-latency unsupervised fog-based intrusion detection system in 2021 [24]. They used a fog computing paradigm to achieve lower detection latency and a faster method of inverting GAN generators for latency-constrained classification and retrieval tasks. Compared to MAD-GAN, the system shows lower latency and is well suited for latency-constrained applications, such as detecting intrusions in CPS.

To secure cloud computing (CC) environments, BC Preethi et al. in 2022 [25] proposed an intrusion detection system (IDS-CC-CCGAN-WSOA) built on water tracker optimization (WSO) for cycle consistent generative adversarial networks (CCGAN). They, use local least squares to handle redundancy and missing values in the datas and generate a uniformly distributed population of water-stepping (Gerridae) by the WSO algorithm to optimise the optimal parameter values for the CCGAN discriminator module generator. The results show that the method has improved sensitivity, specificity and F-score, and reduced false positive rates.

5.4 Summary

As can be seen from these application examples, network intrusion detection systems using deep learning methods are an important current technology that offers a number of advantages and is widely used in a variety of environments. Firstly, DL-based IDSs have a high detection rate. Deep learning methods can effectively detect various security threats in the network environment, such as Dos, R2L, U2R and Probe, and the performance of DL algorithms is better when there is a large amount of attack datas. Secondly, DL-based IDSs have a high detection speed. Deep learning algorithms can perform thousands of complex and repetitive tasks in a very short period of time, producing accurate results as long as the raw datas provided represents the problem. Finally, DL-based IDSs are more adaptable. When attacks become diverse and complex, deep learning algorithms can also be effective in identifying them.

6. Summary and outlook

Intrusion detection systems (IDS) play a vital role in protecting computer systems and networks. This paper reviews techniques related to intrusion detection detection: machine learning techniques and deep learning techniques, and focuses on deep learning-based IDSs. Traditional machine learning IDSs are able to deal with problems requiring a large number of rules and inefficient complex problems, however, they have several limitations, such as feature extraction and datas pre-processing that are not optimised enough, leading to low detection accuracy; the presence of redundant or irrelevant datas, leading to long training times and high risk of overfitting; and high noise interference and weak identification of novel attacks. These problems are particularly prominent when dealing with high-dimensional datas generated by massive amounts of IoT sensors and devices. Compared to machine learning, DL-based IDS overcomes the ML slow training problem, is more suitable for handling large-scale, diverse and high-dimensional network traffic datas, and can efficiently train non-linear models and detect new forms of attacks with high accuracy, making it a superior technique.

However, at present, the detection efficiency, threat detection performance and training time of deep learning in complex datas are yet to be improved. In addition, most of the current research is on basic neural networks to optimise IDSs, and most of the studied IDS solutions are methods designed

for general environments, so it is necessary to go beyond frequent retraining and self-evolving related models and focus on intrusion detection problems in special environments.

References

[1] A. F.. Jahwar and S.. Y. Ameen, "A Review on Cybersecurity based on Machine Learning and Deep Learning Algorithms", jscdm, vol. 2, no. 2, pp. 14 -25, Oct. 2021.

[2] A. L. Buczak and E. Guven, "A Survey of datas Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & amp; Tutorials, vol. 18, no. 2, pp. 1153-1176, Secondquarter 2016, doi: 10.1109/COMST.2015.2494502.

[3] M. Usama, M. Asim, S. Latif, J. Qadir and Ala-Al-Fuqaha, "Generative Adversarial Networks For Launching and Thwarting Adversarial Attacks on Network Intrusion Detection Systems," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 2019. pp. 78-83, doi: 10.1109/IWCMC.2019.8766353.

[4] D. Gümüşbaş, T. Yıldırım, A. Genovese and F. Scotti, "A Comprehensive Survey of datasbases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems," in IEEE Systems Journal, vol. 15, no. 2, pp. 1717-1731, June 2021, doi: 10.1109/JSYST.2020.2992966.

[5] Geetha, R., Thilagam, T. A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security. arch Computat Methods Eng 28. 2861-2879(2021).https://doi.org/10.1007/s11831-020-09478-2.

[6] Otoum, Y, Liu, D, Nayak, A. DL-IDS: a deep learning-based intrusion detection framework for securing IoT. Trans Emerging Tel Tech. 2022; 33: e3803. https://doi.org/10.1002/ett.3803.

[7] Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," in IEEE Access, vol. 6, pp. 35365-35381, 2018, doi: 10.1109/ACCESS.2018. 2836950.

[8] K. Premkumar et al. "Black Widow Optimization-Based Optimal PI-Controlled Wind Turbine Emulator," Sustainability, vol. 12, no. 24, p. 10357, Dec. 2020, doi: 10.3390/su122410357.

[9] LeCun, Y., Bengio, Y. & Hinton, G. Deep learning. Nature 521, 436-444 (2015). https://doi.org/10.1038/nature14539.

[10] Sarker, I.H. Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective. SN COMPUT. SCI. 2, 154 (2021). https://doi.org/10.1007/s42979-021-00535-6.

[11] Yin, Y., Jang-Jaccard, J., Xu, W. et al. IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 datasset. j Big datas 10, 15 (2023). https://doi.org/10.1186/s40537-023-00694-8.

[12] Mohamed Amine Ferrag, Leandros Maglaras, Sotiris Moschoyiannis, Helge Janicke,Deep learning for cyber security intrusion detection: Approaches. datassets, and comparative study, Journal of Information Security and Applications, Volume 50, 2020, 102419, ISSN 2214-2126, https://doi.org/ 10.1016/j.jisa.2019.102419.

[13] Priyanka Dixit, Sanjay Silakari,Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review,Computer Science Review,Volume 39,2021,100317,ISSN 1574-0137,https://doi.org/10.1016/j.cosrev.2020.100317.

[14] Dongliang Chen, Paweł Wawrzynski, Zhihan Lv,Cyber security in smart cities: a review of deep learning-based applications and case studies. Sustainable Cities and Society, Volume 66, 2021, 102655, ISSN 2210-6707, https://doi.org/10.1016/j.scs.2020.102655.

[15] S.-Y. Hwang, D.-J. Shin, and J.-J. Kim, "Systematic Review on Identification and Prediction of Deep Learning-Based Cyber Security Technology and Convergence Fields," Symmetry, vol. 14, no. 4, p. 683, Mar. 2022, doi: 10.3390/sym14040683.

[16] Kanimozhi, V., Jacob, T.P. The Top Ten Artificial Intelligence-Deep Neural Networks for IoT Intrusion Detection System. Wireless Pers Commun 129, 1451 Wireless Pers Commun 129, 1451 -1470 (2023). https://doi.org/10.1007/s11277-023-10198-6.

[17] Fu, K., Cheng, D., Tu, Y., Zhang, L. (2016). Credit Card Fraud Detection Using Convolutional Neural Networks. in: Hirose, A., Ozawa, S., Doya, K., Ikeda, K., Lee, M., Liu, D. (eds) Neural Information

Processing. ICONIP 2016. Lecture Notes in Computer Science (), vol 9949. Springer, Cham. https://doi.org/10.1007/978-3-319-46675-0_53.

[18] Basumallik S, Ma R, Eftekharnejad S. Packet-datas anomaly detection in PMU-based state estimator using convolutional neural network. international Journal of Electrical Power and Energy Systems. 2019 May; 107:690-702. doi: 10.1016/j.ijepes.2018.11.013.

[19] Araya Kibrom Desta, Shuji Ohira, Ismail Arai, and Kazutoshi Fujikawa. 2022. Rec-CNN: In-vehicle networks intrusion detection using convolutional neural networks trained on recurrence plots. Veh. Commun. 35, C (Jun 2022). https://doi.org/10.1016/j.vehcom.2022.100470.

[20] Abien Fred M. Agarap. 2018. A Neural Network Architecture Combining Gated Recurrent Unit (GRU) and Support Vector Machine (SVM) for Intrusion Detection in Network Traffic datas. in Proceedings of the 2018 10th International Conference on Machine Learning and Computing (ICMLC 2018). Association for Computing Machinery, New York, NY, USA, 26-30. https://doi.org/10.1145/3195106.3195117.

[21] Prabhakaran, V, Kulandasamy, A. Integration of recurrent convolutional neural network and optimal encryption scheme for intrusion detection with secure datas storage in the cloud. Computational Intelligence. 2021; 37: 344- 370. https://doi.org/10.1111/coin.12408.

[22] Belhadi, A., Djenouri, Y., Djenouri, D. et al. Group intrusion detection in the Internet of Things using a hybrid recurrent neural network. Cluster Comput 26, 1147-1158 (2023). https://doi.org/10.1007/s10586-022-03779-w.

[23] E. Seo, H. M. Song and H. K. Kim, "GIDS: GAN based Intrusion Detection System for In-Vehicle Network," 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, Ireland, 2018, pp. 1-6, doi: 10.1109/PST.2018.8514157.

[24] P. Freitas de Araujo-Filho, G. Kaddoum, D. R. Campelo, A. Gondim Santos, D. Macêdo and C. Zanchettin, "Intrusion Detection for Cyber- Physical Systems Using Generative Adversarial Networks in Fog Environment," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6247-6256, 15 April15, 2021, doi: 10.1109/JIOT.2020.3024800.

[25] Preethi, BC, Sugitha, G, Kavitha, G. Cycle-consistent generative adversarial network optimized with water strider optimization algorithm fostered intrusion detection framework for securing cloud computing environment. Concurrency Computat Pract Exper. 2023; 35(5): e7552. doi:10.1002/ cpe.7552.