A Review of Current Machine Learning Approaches for Anomaly Detection in Network Traffic

Wasim A. Ali
Department of Computer Science and Engineering, PG Centre, Visvesvaraya Technological University, Mysore, Karnataka, India
Public Telecommunication Corporation (PTC), Yemen

Manasa K. N
Research scholar, PET Research Center (affiliated to University of Mysore), PES College of Engineering, Mandya, Karnataka, India

Malika Bendechache
Lero Research Centre, School of Computing, Dublin City University, Ireland

Mohammed Fadhel Aljunaid
Department of Computer Science, Mangalore University, India

P. Sandhya
Department of Computer Science and Engineering, PG Centre, Visvesvaraya Technological University, Mysore, Karnataka, India

Abstract: Due to the advance in network technologies, the number of network users is growing rapidly, which leads to the generation of large network traffic data. This large network traffic data is prone to attacks and intrusions. Therefore, the network needs to be secured and protected by detecting anomalies as well as to prevent intrusions into networks. Network security has gained attention from researchers and network laboratories. In this paper, a comprehensive survey was completed to give a broad perspective of what recently has been done in the area of anomaly detection. Newly published studies in the last five years have been investigated to explore modern techniques with future opportunities. In this regard, the related literature on anomaly detection systems in network traffic has been discussed, with a variety of typical applications such as WSNs, IoT, high-performance computing, industrial control systems (ICS), and software-defined network (SDN) environments. Finally, we underlined diverse open issues to improve the detection of anomaly systems.

Keywords: Anomaly Detection, Intrusion, Networks, Supervised, Unsupervised

http://doi.org/10.18080/jtde.v8n4.307

Introduction

The detection of anomalies and abnormal activity in the network have become the most common problem in the industrial research area (Larriva-Novo *et al.*, 2020; Kusyk *et al.*, 2018). Anomaly detection is widely used in different types of applications, such as health monitoring systems, fault detection in critical systems, fraud detection, crime investigation, and cyber-intrusion detection (Bauer *et al.*, 2019; Rettig *et al.*, 2015; Shukur & Kurnaz, 2019;Meng *et al.*, 2017; Mohammadi *et al.*, 2019). With the rapid development of extensive-scale network technology along with users and services, the security of information is becoming imperative for any network system. Therefore, many studies and researches took a broad scope in the security area, with various methods and techniques that helped many researchers to work on the development of algorithms and feasible methods in the detection of abnormal activities in network traffic. The machine learning (ML) concept has been actively present in the last decade in many applications to solve various problems in network security. The major problem to which ML techniques are applied is anomaly detection in the network. Many ML techniques have been used or proposed for this purpose in different aspects and different methods, but the most used techniques are categorized under supervised and unsupervised machine learning. Based on review studies in this area, these two types of ML have received considerable attention by researchers, who suggested these techniques to be used either separately or combined (Omar *et al.*, 2013). In fact, several researchers have used these two ML techniques and their results have led to improved performance of attack detection and increased anomaly detection efficiency. The question that remains is: how do researchers decide which ML (unsupervised or supervised) technique to use for a specific problem or dataset? In other words, how do we know which ML technique is going to fit better with our dataset and lead to better results?

These questions motivated us to investigate the differences between the supervised and unsupervised approaches in recent applications related to anomaly detection systems. The main aim of this survey is to review various ML techniques used for anomaly detection to provide maximal understanding amongst the existing techniques that may help interested researchers to boost their future work in this direction.

The paper is structured as follows. In section 2, we discuss the different types of anomalies. Section 3 describes the use of ML for anomaly detection. In section 4, we explain the significant types of network attacks. Sections 5 and 6 discuss the supervised and unsupervised techniques recently used and their variations are evaluated. In section 7, we compare the supervised and

http://doi.org/10.18080/jtde.v8n4.307

unsupervised techniques. Section 8 presents the work on semi-supervised techniques briefly. Finally, we conclude our work and highlight some open issues and challenges in section 9.

Network Anomalies Types

A computer network is a combination of many individual entities assembled together to provide complete and various communication services. Anomalies in these networks are network activities that differ from standard, usual or expected behaviour, and are suspected from a security perspective. They are also known as abnormal activities that attempt to disrupt the normal functions of the network.

Chandola *et al.* (2009) define anomalies as "patterns in data that do not conform to a well-defined notion of normal behavior". Ahmad *et al.* (2017) express the term as "a point in time where the behavior of the system is unusual and significantly different from previous, normal behavior". For a common network, Zhao *et al.* (2015) says “a traffic flow with unusual and significant changes is considered as an anomaly”. According to Zhang *et al.* (2017), "Network anomaly refers to the unusual behavior of network actions or suspicious network status, which can either be malicious or benign". Additionally, Lakhina *et al.* (2004) stated that “anomalies are unusual and significant changes in a network’s traffic levels, which can often span multiple links”.

Anomalies are also called abnormalities, outliers, or exceptions. They have been defined in many ways by different authors with different backgrounds, resulting in creating confusion of the terms related to anomalies. To understanding those definitions, the first step to knowing what is abnormal in a network system is understanding the normality. There are various types of network anomalies (Mohd Ali, 2018), which can be categorized into three types: point anomalies, contextual anomalies, and collective anomalies, as shown in Figure 1.

A point anomaly is considered as the simplest type of anomaly, where any single point of data has different attributes from its group of data. For example, in credit card transactions, the daily spend of money is a hundred dollars, but on a specific day the spending rises to four hundred dollars. This type of anomaly transaction is called a point anomaly.

A contextual anomaly is also known as a conditional anomaly, where the data behave anomalously in a specific context. However, conditional anomalies are usually applied to time-series data. For example, admission for short courses during summer takes typically 30 to 40 students for each course. If the admissions in some courses are below 15 students, we considered this as an anomaly.

http://doi.org/10.18080/jtde.v8n4.307

A collective anomaly is detected when a collection of data groups behaves anomalously within the whole dataset. In this type, individual anomaly behaviour is not considered as anomalies. Nevertheless, the frequent occurrence in these data is considered an anomaly. For a better understanding of the concept, the following example is given: in the computer, there is a sequence of actions that occurs together, such as buffer-overflow, HTTP-web, FTP, HTTP-web, SSH, HTTP-web, SSH, buffer-overflow, HTTP-web. In this case, the sequence is called a collective anomaly (Fernandes *et al.*, 2019).

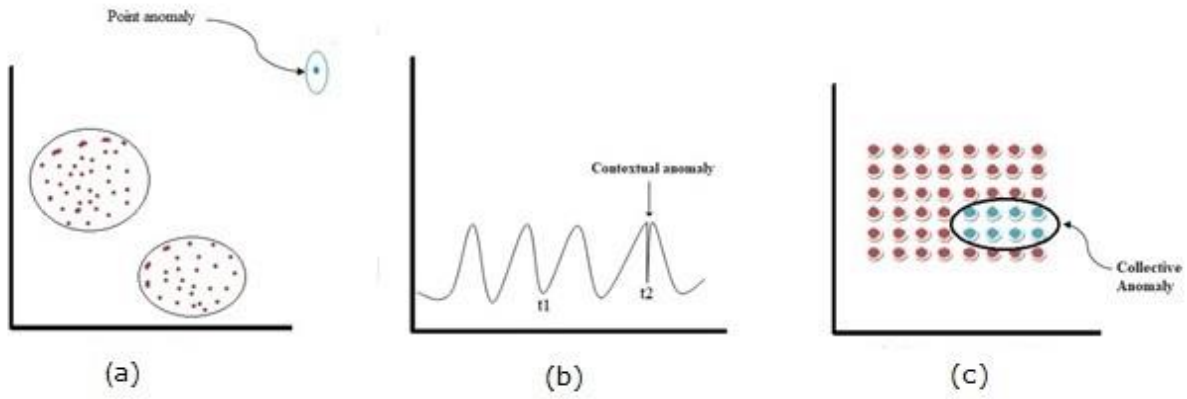

Figure1. Types of anomalies: a) point anomaly; b) contextual anomaly; and c) collective anomaly

Anomaly Detection Using Machine Learning

Anomaly detection is the process of finding an effective way to discover anomalous values in a dataset that behave abnormally in the system. The importance of this process lies in that anomalies in data are translated into important practical information in a wide range of application areas. Anomaly detection provides a method of identifying a possible threat behaviour and takes appropriate action when it occurs. Generally, the anomaly detection system is an automated security system used for monitoring, analyzing, and detecting abnormal activities within a network or host (Kotu & Deshpande, 2018; Omar *et al.*, 2013; Knapp & Langill, 2014). Besides, Lee & Stolfo (1998) report that there are four major elements to be considered when creating an anomaly or intrusion detection system: resources to protect, models to identify the typical behaviour of the resources, techniques that compare the actual activities of these resources with their healthy behaviours, and, finally, identifying what is considered anomalous or unwelcome objects. In this paper, we focus on anomaly-based intrusion detection systems (AIDS). However, the investigation of network intrusion using AIDS has been of interest to many researchers and authors. The researchers have presented a detailed description of various aspects and types of anomaly detection systems along with various models and techniques used to defend many attacks that we will discuss in detail later.

http://doi.org/10.18080/jtde.v8n4.307

In any network computer system, there is potentially a large amount of activities, traffic, and log information available on it. The majority of activities are standard, but a tiny amount of activities may be outside the border of what is usual or expected. Those unexpected activities are potential anomalies or intrusions. However, as the dataset of such systems is extremely large, diverse, and ever-growing, the patterns of the anomaly may not be evident and easy to find. The ideas of the concept of machine learning may be an essential way to find potential intrusion patterns. Machine learning aims to extract valid, potentially helpful, and significative patterns to recognize intricate patterns in existing datasets to help to make intelligent decisions or predictions, by using a nontrivial learning mechanism (Bhattacharyya & Kalita, 2013). In general, all machine learning algorithms follow standard steps to classify the anomalies and intrusions, as follows:

Data Cleaning and Noise Removal: in this stage, the data is cleaned by removing outliers and unwanted data. This will improve the quality of the training data and lead to a better and more accurate prediction model.

Classification: classify or label the data into normal or abnormal.

Named Entity Recognition: it is necessary to know some entities to predict anomalies such as packets, IP address, time, size, and activity, then classify them as positive normal, or abnormal.

Subjectivity Classification: Subjectivity is a term referring to any attributes, events, or the properties of entities.

Feature Selection: the process of automatically selecting the features which are relevant to our data to predict the interested variables or output and help the system to detect anomalies (Manasa & Padma, 2019).

The basic idea of using a machine learning algorithm is to provide the ability to learn from a given dataset and address the problems in a similar dataset automatically without human intervention. Several algorithms and methods have been used by researchers and developers to overcome the network security challenges and avoid network attacks. Primarily, the machine learning approaches can be categorized into three main classes as shown in Figure 2: supervised learning, unsupervised learning and semi-supervised learning. Supervised learning is mainly used for classification or prediction, whereas unsupervised learning is used for clustering. The semi-supervised class is a hybrid approach between supervised and unsupervised classes. Figure 2 also shows some examples of well-known classification and clustering algorithms.

http://doi.org/10.18080/jtde.v8n4.307

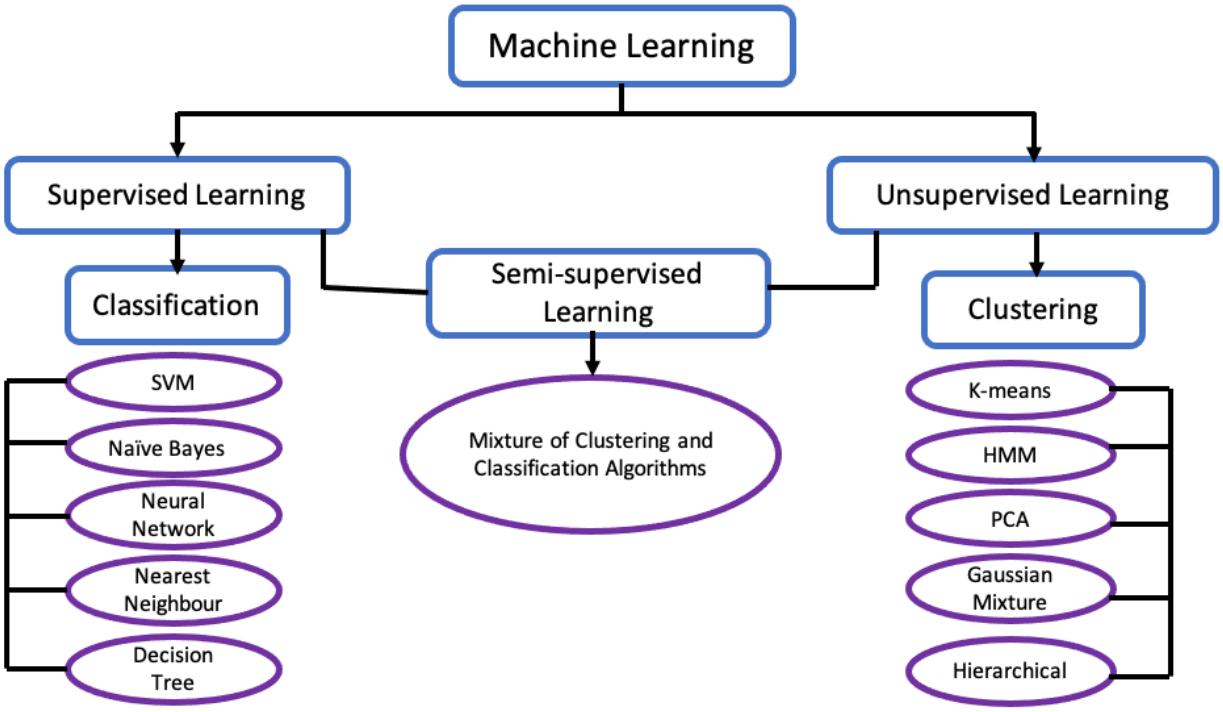

Figure 2. Machine learning techniques

In this paper, we will investigate different types of attacks handled by using supervised, unsupervised and semi-supervised algorithms. Moreover, we will review the most critical analysis methods which are related to anomaly detection techniques within the area of network traffic that have been proposed in the last five years.

Network Attacks

A network attack is an illegal attempt to avail of the vulnerability of a computer or network, attempting to break through the security of the network system. Anderson (1980) classifies attackers into two types: external and internal. External attackers are unauthorized users in the systems they attack, whereas internal attackers have the authority to access the system, but do not have access to the root or superuser. Bhattacharyya & Kalita (2013) classify attacks into seven main types based on the implementation of those attacks, as shown in Table 1.

In this survey, we will concentrate on the most critical and recent attacks from different categories with different examples. Also, we will highlight ML approaches and algorithms used to detect those attacks.

http://doi.org/10.18080/jtde.v8n4.307

Table 1. Attack categories

Main category	Definition	Examples
Infection	Aim to infect the target system either by tampering or by installing evil files in the system.	Viruses, Worms, Trojans.
Exploding	Seek to explode or overflow the target system with bugs.	Buffer Overflow.
Prop	Gather information about the target system through tools.	Sniffing, Port sweep, IP sweep.
Cheat	Typical examples of this category include attempts to use a fake identity.	IP Spoofing, MAC Spoofing, DNS Spoofing, Session Hijacking, XSS Attacks, Hidden Area Operation.
Traverse	Attempts to crack a victim system through a dull match against all possible keys.	Brute Force, Dictionary Attacks, Doorknob Attacks.
Concurrency	Victimize a system or a service by sending a mass of identical requests which exceeds the capacity that the system or the service could supply.	Flooding, DDoS (Distributed Denial of Service).
Others	These attacks attempt to infect the target system by using system bugs or weaknesses directly.	

Supervised Learning

Classification is one of the terms which refers to supervised learning. Applying supervised techniques on the network data sets allows us to build a model, and the data instances can be labelled using a set of attributes. Many supervised algorithms are used to detect anomalies and intrusions in the network traffic and have proven effectiveness and efficiency, such as Support Vector Machine (SVM), Artificial Neural Network (ANN), Nearest Neighbour algorithm, Decision Trees, K-nearest neighbour, Ensembles classifiers, and Naïve Bayes classifier. These algorithms are more commonly used in the supervised learning approach. In the following, we summarize the research works that have been done using these supervised learning algorithms for anomaly detection in the past five years.

Support Vector Machine (SVM)

Chakir *et al.* (2018) introduced a new Intrusion Detection model based on a Particle Swarm Optimization algorithm (PSO), which joins a feature selection algorithm using information gain with a SVM classifier. The authors concluded that, by combining feature selection and parameter optimization for SVM, training and testing time are reduced and the effectiveness of the SVM Classifier is improved. The proposed model FS PSO-SVM results in obtaining a high detection rate and the lowest false positive rate. They tested the effectiveness of the proposed

http://doi.org/10.18080/jtde.v8n4.307

model by using the NSL-KDD Dataset, which includes 41 features, and by testing the model through 4 types of network attacks: DoS, R2L, U2R and Prob.

Recently, Gu *et al.* (2019) proposed an intrusion detection (ID) framework based on the SVM ensemble classifier with increasing features selection. Their idea is to integrate the powerful quality-improved transformation with the SVM ensemble. They built a robust intrusion detection framework with low training complexity, powerful performance, and high accuracy. However, they considered only the binary case of intrusion detection problems. They applied their proposal on the NSL-KDD Dataset and used a cross-validation (10-fold) method to train and test the model. The result of their experiment showed that the proposed framework could achieve robust performance, a high detection rate, and a low false alarm rate.

Weerasinghe *et al.* (2019) presented a novel framework to enhance the resilience of SVMs against training-data-integrity attacks. The proposed approach uses random projections on top of the learners. This makes it challenging for the attacker to guess the specific configurations of the learners. They introduce novel indices that ensure the shrinking of the data and increase the detection accuracy. Their contribution is characterized by the use of nonlinear random projections for defense techniques for learners (SVMs/One Class SVMs). Several datasets were used in this experiment, such as MNIST, CIFAR-10, and SVHN. The results indicated that SVM and OCSVM could be significantly affected if an attacker can manipulate the trained data.

Another approach using the SVM algorithm is proposed by Hu *et al.* (2019). To address the problem of the long training time of the prediction model, the authors proposed a prediction model based on the map-reduce technique and SVM classifier. They used an SVM classifier as a base classifier for the model and optimal parameters performed by the Cuckoo Search (CS). They used the Map Reduce (MR) technique and CS algorithm to enhance the SVM classifier to optimally solve the general problem of parameter optimization. They stated that the proposed model reached better results in terms of accuracy and it reduced training-time costs.

Naïve Bayes

Han *et al.* (2015) developed a Naïve Bayesian (NB) model for network intrusion detection based on PCA (Principal Component Analysis). The model utilized NB with PCA to extract new properties that helped them to improve the traditional NB algorithm, where traditional NB cannot consider the problem of weights in attributes. KDD CUP 99 was the experimental data set, and the type of attacks that dataset included were DoS, U2L, R2L, and Probe attack. This

http://doi.org/10.18080/jtde.v8n4.307

experiment has a good result in the detection rate with weighted Naïve Bayes classification, and it solves the problem of feature redundancy.

Swarnkar & Hubballi (2016) proposed a version of a Naïve Bayesian one-class classifier, OCPAD, for payload-based anomalies detection. OCPAD is a content method that identifies network packets with untrusted payload content. They have done many experiments with a large dataset showing that OCPAD can perform at an excellent level to detect anomalies with increasing Detection Rate as well as an agreeable False Positive Rate.

Kumar & Venugopalan (2018) introduced a novel algorithm based on the Naïve Bayes model to detect attacks in data training. In their study, they conducted four testing data stages on the Kyoto 2006+ dataset. The training dataset contained 5000 average records and 5000 attacks, and all the four tests were evaluated by the Naïve Bayes model, which resulted in higher accuracy and detection rate.

Recently, Mehmood *et al.* (2018) presented a new model of using the Naïve Bayes algorithm-based intrusion detection system. The proposed approach aims to protect the Internet of Things (IoT) infrastructure from Distributed Denial of Service (DDoS) attacks generated by the intruders and the complexity of IoT, where the data comes from heterogeneous resources that helped this type of attack to spread in the IoT network. The authors implemented a multi-agent-based IDS (NB-MAIDS). An NB classifier was applied with a multi-agent system (MAS) throughout the network and agents. They collected the information from sensors which help the system to report the activities of the abnormal nodes on the IoT network. This proved the efficiency of the NB classifier with multi-agents in the proposed approach, giving better performance to prevent attacks very quickly with low execution costs. The experiment of proposed classifier effectiveness was tested on the NSL-KDD dataset.

Nearest Neighbour

The nearest neighbour classifier is one of the supervised learning techniques that is widely used for anomaly detection. Xiao *et al.* (2015) introduced an effective detection technique based on CKNN to detect DDoS attacks. This method is applied across a data centre network by utilizing the training data correlation information and CKNN classification. Their contribution provided a novel approach throughout the use of a CKNN classifier with correlation information. This helped to reduce the size of training data and to improve the classifier accuracy in detecting DDoS attacks with low cost and minimum response time. In this work, the authors used three types of dataset: broad, real, and KDD99.

http://doi.org/10.18080/jtde.v8n4.307

Regarding the new type of Software Defined Networking (SDN) and their network flow problems, Peng *et al.* (2018) presented an SDN-based anomaly flow detection. This work was implemented for DDoS anomaly detection, where the K-nearest neighbour algorithm was the classification technique performed to detect flows using P-value. The results of the experiment showed that the DPTCM-KNN algorithm increases the detection accuracy rate of the anomalous flow detection, as well as reducing the false positive rate. This confirms that the algorithm has very good performance in SDN platforms.

An Industrial Control System (ICS) is a control system and related instrumentation developed to control and monitor industrial processes using cyber-physical systems. Abnormal behaviour in these critical infrastructures can cause a significant threat to society. In this area, Yun *et al.* (2018) implemented a statistical model that provides an intrusion detection technique to detect abnormal activities in ICS networks by using Nearest-Neighbour Search (NNS). The proposed model can identify the normal and abnormal traffic patterns in the network, even the small amount of traffic variation with the lowest false rate. The NNS algorithm works fast with time complexity analysis, which allowed the method to be used in real time in ICS. The experiment assured that small changes in the traffic could be detected by the method with fast execution. This speed can be used for real-time monitoring in any ICS network.

Anomaly detection systems were not only limited to computer networks but also included several networks such as WSN, IoT, Cloud, etc. Wang *et al.* (2019) proposed a method to detect anomalous values in a Wireless Sensor Network (WSN) environment by detecting the proximity of distance based on distance. The KNN (K-Nearest Neighbour) algorithm was used in the proposed approach to analyze the data first, then to detect the data anomaly in the WSN. The authors discussed the different types of applications in WSNs, which are repeatedly attacked along with the type of attacks in WSNs. They used the QualNet network simulation tool to analyze behavioural research and statistics of a wireless mobile network. QualNet helped to cover many models, algorithms, and protocols that are useful in learning, efficiency, speed, and accuracy of processing as part of a real network. The results of the paper prove that the KNN classifier can achieve a reasonable detection rate and a low error rate. The compressed proximity algorithm is used to minimize the massive dataset.

Decision Tree

Decision Trees are counted as one of the most common classification techniques. Khraisat *et al.* (2018) introduced a data mining technique that could minimize the false rate in the system. The proposed classifier is a C5 decision tree that was examined with different data mining

http://doi.org/10.18080/jtde.v8n4.307

techniques. The authors aimed to prove that the C5 algorithm obtains the best result of detecting abnormal activities. However, they examined 4 types of algorithms: SVM, Naïve Bayes, C4.5, and C5. The results showed that the C5 decision tree has reduced both false positive rate and false negative rate and the intrusion detection is improved effectively with high accuracy. The experiment was applied using the NSL-KDD dataset. Kevric *et al.* (2017) developed a combining classifier based on the decision tree algorithm for IDS. They selected a new version of a KDDCUP'99 data set that is NSL-KDD. A detection algorithm was used to classify the traffics of the network, whether it is normal or abnormal, based on 41 features describing all patterns of the network traffic. The authors stated they achieved outstanding detection rate accuracy by combining both Naïve Bayes Tree (NBTree) with random tree classifiers with a sum rule scheme, and it was better than the individual random tree algorithm.

Rai *et al.* (2016) worked on the decision tree classifier in terms of feature selection and split value. Those issues are essential to build the classifier; the Decision Tree Split (DTS) algorithm based on the C4.5 classifier was explicitly designed to address the two issues. The approach gives a novel method in selecting the split values. The algorithm is more efficient for signature-based intrusion detection with fast finding of attacks in the network with a small number of features and minimum cost of time to build the model. Through literature, comparing the proposed algorithm with others, it found that the DTS algorithm is efficient for constructing a decision tree that is used to detect intrusions. Experimentation is performed on the NSL-KDD dataset.

Chew *et al.* (2020) proposed a sensitive pruning model-based decision tree classifier to overcome the issues of the visibility of its tree rules in the Network-based Intrusion Detection System (NIDS). They modified the pruning algorithm based on the C4.8 decision tree. The pruning framework used in this work is the Weka J48 decision tree and tested on 6 versions of GureKDD Cup IDS datasets. Evaluation and results revealed two advantages of using a C4.8 decision tree. The first advantage is the ability to maintain privacy in the decision tree by hiding only sensitive rules selected. Secondly, any small changes in the proposed pruning of the decision tree structure during tree construction do not affect the process of feature selection.

Neural Network

A Neural Network can also be known as an Artificial Neural Network (ANN). Generally, an ANN uses constructs from the human brain system, consisting of significant parallel connections of many neurons. Usually, the neurons are related to each other in a complex manner. ANNs are built with several connecting nodes with activation functions (Akhi, 2019; Agrawal & Agrawal,

http://doi.org/10.18080/jtde.v8n4.307

2015). Neural Networks (NNs) can be used for supervised and unsupervised learning. However, in this section, the survey has been carried out through the latest published papers which focused on supervised learning only.

Hodo *et al.* (2016) presented an artificial neural network system to analyze threats in IoT networks. By using internet packet traces, ANNs are trained to learn the ability to detect and prevent DDoS attacks. The proposed model was able to identify several types of attacks and proved efficient results in the perspective of true-positive and false-positive rates.

Veselý & Brechlerová (2009) are in accord with Hodo *et al.* (2016) where they claim that an artificial neural network is an appropriate technique to increase the ability of anomaly detection systems to successfully detect attacks and abnormal activities. They present an overview of the previous work that showed the applicability of NNs for building anomaly detection systems and the ability to differentiate between normal and abnormal behaviour in the system.

Haripriya *et al.* (2018) proposed a novel ANN supervised classifier by applying the back-propagation algorithm to the intrusion detection system using the R tool. The KYOTO data set was used as a filtered version of KDD-CUP-99. The authors took advantage of feature selection techniques and applied them to this dataset to remove irrelevant features and duplicate data. They compared the proposed method with different models and the outcomes show that F-measure, accuracy, and recall are enhanced and increased.

However, Wu *et al.* (2018) used a different type of neural network, that is a Convolutional Neural Network (CNN), where the network intrusion-detection is proposed as a novel model. CNN has an ability to select traffic features automatically from the raw dataset, and that encourages them to use this type of NN. The main issue which needed to be solved is the imbalanced dataset problem. The proposed model improved the accuracy of detection in a big network and in real time, along with reducing the false alarm rate. The authors also proposed a model to convert the raw traffic vector into an image format, which facilitates reducing the cost of calculation. The standard NSL-KDD dataset is applied to evaluate the performance of the proposed model.

On the other hand, Vinayakumar *et al.* (2017) preferred to use another type of neural network, that is a Recurrent Neural Network (RNN). The authors have done a comprehensive review of various RNN networks and examined traditional machine learning classifiers to come out with a clear picture of RNN effectiveness. RNN is a subset of ANN that appeared as a powerful approach to learn temporal behaviours in large-scale sequence data. To examine this model, the

http://doi.org/10.18080/jtde.v8n4.307

authors model traffic of a network as a time series, especially TCP/IP packets in a pre-defined time range using a massive number of known strong and poor network connections. They used the existing datasets, DARPA, KDD-Cup-99, and UNSW-NB15, to display the power and efficiency of the RNN architecture. An RNN has the ability to store long-term information and is able to adjust with serial connection sequence information. Moreover, this work performed well with different types of high-frequency attacks such as DoS and Probe.

Deep learning (DL) is another machine learning method based on artificial neural networks with representation learning. Learning can be supervised, semi-supervised or unsupervised. The main difference between NNs and DL is in the number of node layers, or depth, of the neural networks. Therefore, an NN is a simple version of a DL. Recently, DL techniques have been widely used for detecting unauthorized logins into computer networks. DL techniques have stepped up to deal with the shortcomings of some automated learning techniques for dealing with large amounts of data that come from heterogeneous sources.

The use of DL techniques for anomaly detection is outside the scope of this study. We intend to extend our review to include DL-based anomaly techniques in our future work.

Ensemble Methods

Training a variety of ML methods to solve the same issue and then combining their performance to enhance accuracy is known as an ensemble method or a multi-classifier system (Aburomman & Reaz, 2017). Through the literature, we can see the progressive development of a variety of IDSs based on ensemble methods. In the following, we will summarize of these works.

Gu *et al.* (2019) proposed an efficient SVM ensemble-based intrusion detection system with feature augmentation. They implemented most powerful univariate classifiers marginal density ratios transformation on the original features, in order to obtain new and better quality training data. The results of the experiments show that the SVM ensemble can achieve reasonable and robust performance, which has a competitive advantage in terms of detection rate, training speed, accuracy, and false alarm rate compared to other established methods. The experiment was performed on the NSL-KDD dataset.

Pham *et al.* (2018) introduced an ensemble classifier and feature selection with the aim of improving the performance of the IDS. The ensemble classifiers were built based on two techniques, Boosting and Bagging, with a tree-based algorithm as a base classifier. These models were evaluated using NSL-KDD datasets. The results showed that the bagging technique with

http://doi.org/10.18080/jtde.v8n4.307

the tree-based classifier (J48) can improve the performance in terms of classification accuracy as well as a false alarm rate (FAR).

Bhati *et al.* (2020) proposed a new scheme of ensemble-based techniques to detect several types of attack classes, such as DOS, R2L, U2R, and Probing. The framework was implemented using MATLAB. The basic task of the proposed method is to create individual classifiers, then train them separately. The combination of classifiers leads to powerful decisions based on majority voting. The proposed framework consists of 4 major steps: Data Collection, Pre-processing, Training & Testing, Decision. As a result, the framework gives a high detection accuracy for DOS, Probing, R2L and U2R. The KDDcup99 dataset was used to evaluate the proposed scheme.

Rai (2020) examined ensemble learning methods for IDS that were boosting and bagging methods, such as XGBoost, Gradient Boosting Machine (GBM), and Distributed Random Forest (DRF). They were implemented using a Python library (H2O) for the new intrusion identification framework. A Deep Neural Network (DNN) is also executed using the same library and it was found that the model overcomes the past aftereffect of DNN after employing the genetic algorithm as a feature selection method. The proposed approach outcomes beat the diverse old-style ML models too. NSL-KDD dataset has been used for the experiment.

Table 2 shows a comparison between the above research works that used the different supervised learning algorithms for anomaly detection. The comparison is in terms of publication year, supervised learning technique used, type of anomaly detected, dataset used, and accuracy.

Table 2. Supervised Anomaly detection approaches

Authors	Year	ML Technique	Anomaly type	Dataset	Detection Accuracy (%)
Jingjing Hu *et al.*	2016	MR-SVM classifier	generic attack in network	KDD, DARPA	96.16%
El Mostapha *et al.*	2018	PSO - SVM classifier	DoS, R2L, U2R and Prob	NSL-KDD	99.5%
Jie Gu *et al.*	2019	SVM ensemble classifier	binary case of intrusion detection problems	NSL-KDD	99.36%
Sandamal *et al.*	2019	SVM and OCSVM	training-data-integrity attacks	MNIST, CIFAR-10, SVHN	97%
Han *et al.*	2015	Naïve Bayesian with PCA	DoS, R2L, U2R, and Prob	KDD CUP 99	87%

http://doi.org/10.18080/jtde.v8n4.307

Authors	Year	ML Technique	Anomaly type	Dataset	Detection Accuracy (%)
Swarnkar & Hubballi	2016	Naïve Bayesian OCPAD	Generic attack	HTTP dataset.	100%
Kumar & Venugopalan	2018	Naïve Bayes (ANADA)	Generic attack	Kyoto 2006+	96.66%
Amjad Mehmood *et al.*	2018	NB-MAIDS	DDoS attack	NSL-KDD	90%
Peng Xiao *et al.*	2015	Nearest Neighbour CKNN	DDoS attack	KDD99	96.3%
Huijun Peng *et al.*	2018	K-nearest neighbour	DDoS attack	SDN environments	97.88%
Jeong-Han *et al.*	2018	nearest-neighbour	generic attack in ICS	ICS real-time	99%%
Wang *et al.*	2019	KNN	generic attack in WSN	WSN temporal data	99.7%
Kevric *et al.*	2016	NBTree algorithm	DoS, R2L, U2R, and Prob	NSL-KDD	89.24%
Kajal Rai *et al.*	2016	Decision Tree Split (DTS)	R2L, U2R	NSL-KDD	79.52%
Khraisat *et al.*	2018	C5 decision tree	Zero-day attack	NSL KDD	99.82%
Chew *et al.*	2019	Weka J48 decision tree	Generic attack	Gure KDD Cup	99.33%
Gu *et al.*	2019	SVM ensemble	Generic attack	NSL-KDD	99.36 %
Pham *et al.*	2018	Ensemble (Bagging and Boosting)	DoS, R2L, U2R, and Prob	NSL-KDD	84.25 %
Bhati *et al.*	2020	Ensemble techniques	DoS, prob, U2R, and R2L	KDDcup99	98.9 %
Ajeet Rai	2020	Ensemble Methods and DNN	DoS, R2L, U2R and Prob	NSL-KDD	92.7%

Unsupervised Learning

Unsupervised learning is namely clustering techniques or undirected classification. Unlike supervised learning algorithms, the training dataset (labelled data) is not required in unsupervised learning techniques. The idea of a clustering technique to group data into categories or sub-groups is known as a cluster based on similarity properties. It uses measurement or metrics to count the likeness between data instances. In brief, unsupervised techniques are an attempt to determine the hidden pattern in given data without training a model. Further, unsupervised Network Detection Systems (NDS) are used to overcome the

http://doi.org/10.18080/jtde.v8n4.307

limitation of the supervised anomaly techniques system. There are many unsupervised algorithms used to cluster given data and detect anomalous/abnormal activities in network traffic successfully, like the K-means algorithm, Hidden Markov Model (HMM), Gaussian Mixture, Hierarchical clustering, and Neural Networks (NNs) (Bhattacharyya & Kalita, 2013; Dua & Du,2016). In the following, we summarize the different research works that have used unsupervised learning algorithms for anomaly detection.

K-means algorithm

It was formally known as the most basic and straightforward algorithm in unsupervised learning, as well as a partition-based cluster and the most popular unsupervised approach. To solve clustering problems, k-means partition n observations into k clusters, where each n belongs to the k with the nearest mean, which acts as a prototype of the cluster (Karim *et al.*, 2019). According to Thakare & Bagal (2015), in K-means algorithm, k objects will be selected as initial cluster centres, then the distance between each centre and object will be calculated, and objects assigned to the nearest centre. After that, the mean of all clusters will be updated; finally, the process will be repeated.

With the need for mining big data sets, stream mining gains attention from researchers, and it causes different challenges, such as anomaly and outlier detection, fraud detection, etc. Chauhan & Shukla (2015) reviewed a different approach of outlier detection using the K-means cluster algorithm. The different areas of applications have been discussed, and this algorithm with stream data was used. Introducing different machine learning, feature selection and clustering methods have been used to give basics of the k-means concept in outlier detection for beginner researchers.

Network security is an important aspect of where this algorithm is applied. Münz *et al.* (2007) introduced a network data mining technique by proposing a novel anomaly detection method based on the K-mean cluster algorithm. The authors trained the unlabelled records in the dataset and divided it into clusters of regular traffic and anomalies using the K-means algorithm. The cluster cancroids have been used as patterns for efficient distance-based detection of anomalous traffic in new data. They concluded that the model resulted in fast anomalies detection and improving detection quality. They evaluated the capability of the model to detect DoS attacks and port scans.

However, the K-means algorithm is considered a basic algorithm for the clustering approach, where the integration with other algorithms will be more effective. Therefore, Aung & Min

http://doi.org/10.18080/jtde.v8n4.307

(2018) presented hybrid ML algorithms that contained a k-means algorithm to identify similar attack groups and a Random Forest algorithm to categorize the data into normal and attacks. The authors tested the proposed model on four categories of intrusion attacks, DoS, U2R, R2L, and Prob, in the KDD-Cup-99 dataset. Their experiments produced good results where the accuracy and recall of the normal and anomaly detection were perfect. The false-positive rate showed an enhancement result, nearly zero.

Hidden Markov Model – HMM

HMM is a statistical model used in data science and engineering as a state-based classification model. The first use of this model was in speech recognition. After that, many analysis applications were applied successfully. One of the most critical applications is anomaly detection. In this area, a lot of works have been done with very efficient results. We will discuss some of the recent research articles that used the HMM in terms of security and intrusion detection.

Chen *et al.* (2016) proposed an algorithm that can handle the massive size of data and event logs and recognize the temporal relation of unusual events. Besides, they proposed a state-based detection approach to recognizing multi-stage advanced attacks. The challenge for them was related to the large amount of data and how the big data will be handled to analyze for security purposes. Results showed that the proposed model has been active and successfully performed with a massive amount of event logs in the network.

Stefanidis & Voyiatzis (2016) have been interested in the security of Industrial Control Systems (ICS). They introduced the HMM model for intrusion detection systems in ICS. They applied the model on SCADA systems by using interconnected TCP/IP protocol. The evaluation part in their work was done by comparing the accuracy of detection with other researchers' systems which used the same datasets. The proposed system achieved a higher detection rate of the most attack vectors. They concluded that the system was more appropriate with real-time systems and high-speed environments.

Zegeye *et al.* (2019) had technical concerns about the security of 5G networks. For such a purpose, they developed a novel multi-layer approach based on the HMM model to defend the network against intruders and capture multi-phase attacks, where the CICIDS2017 dataset had been used. SVD and feature selection techniques were applied to this dataset to reduce the data. Further, K-means clustering labels were used to monitor the multi-layer HMM model. With the use of the proposed model, there is no requirement to use a big amount of training data. The

http://doi.org/10.18080/jtde.v8n4.307

layer in this model was trained in a small observation space, indicating the models were more stable and well trained.

Meanwhile, mobile networking security has unanticipated challenges. However, researchers are working hard to develop models that overcome these challenges. According to Liang *et al.* (2018), the traditional HMM algorithm used for predicting network security is not precise. Hence, they introduced a weighted HMM-based algorithm designed to predict mobile networking security. They used multiscale entropy to handle the problem of low speed of data training in the area of mobile networking, while the HMM transition matrix was optimized. Furthermore, the autocorrelation coefficient could be used in the connection between the characteristics of the given data to predict future security of the network. They implemented the model and applied the analysis on the DARPA2000 dataset to verify the effectiveness of the algorithm. The dataset contained DDOS attacks, lots of data, redundancies, and false alarm rates. The proposed model experiment showed that it is accurate and valid.

Principal Component Analysis – PCA

PCA is a statistical technique used to decrease the dimensionality of a dataset consisting of numerous variables related to each other, preserving the current variation in the dataset to the maximum extent. To apply PCA on a training set, there is no requirement for labelled data. For that, PCA is an unsupervised learning algorithm used for dimension reduction.

Ding & Tian (2016) explained how to apply the PCA algorithm to detect anomalies in Traffic Matrix (TM) analysis. The proposed approach may carry out an effective analysis of Origin-Destination flows by dividing network traffic data into a normal and anomalous subspace. The experiment on the proposed detection method was done on node disconnection and DDoS attacks in a backbone network. The proposed method could detect a single-node anomaly as well as multi-node anomalies. They used in the experiments the Abilene network dataset between 2003–2004.

Meanwhile, Vasan & Surendiran (2016) focused their work on the efficiency of PCA for anomaly detection, with the definition of the Reduction Ratio (RR), the number of Principal Components required to detect intrusions, and the noisy data effect on PCA. The experiments utilized different classifiers on two datasets, KDD-CUP and UNB-ISCX.

The experiments showed that the first 10 principal components were useful for classification. They concluded that the use of PCA to build an intrusion detection system would minimize system complexity and achieve a higher accuracy of classification.

http://doi.org/10.18080/jtde.v8n4.307

Paffenroth *et al.* (2018) introduced Robust PCA as a new anomaly detection system. The proposed approach, RPCA, uses network packet captured data to show the impact in different network attack detection systems. The DARPA dataset has been used in their experiments with different attack scenarios, such as DDoS attacks, IP sweeps, and probing and breaking. The model achieved the lowest false positive rate with a reasonable correct positive rate and successfully detected network attacks. The used method detected packet stream attacks accurately which had not been encountered or trained previously.

Hoang & Nguyen (2018) probed a different way of PCA with IoT, where network platforms need effective tools to detect intrusions in traffic data swiftly and identify attacks. They mentioned a listing of issues in applying the PCA algorithm, for example, the choice of principal components for complexity reduction. Through previous literature, they proposed a new general formula for distance calculation as well as a new method based on PCA for detecting anomalies in IoT networks. Several experiments were conducted on the dataset Kyoto Honeypot that were collected from Honeypot university networks. Quick online detection and reduced complexity of computation are the results obtained from the experiment on three random Kyoto network datasets.

Gaussian Mixture Model (GMM)

The Gaussian Mixture model is "a probabilistic model which states that the entire generated data points are derived from a mix of a finite Gaussian distribution that has unknown parameters" (Technopedia, n.d.). Many researchers have worked on this model, and they have come up with excellent results. Therefore, the following survey covers a few recent papers using the GMM method.

Lalitha & Josna (2016) applied the GMM for network traffic verification. They captured the traffic data and fed it into the proposed model for verification. It supposed that the traffic which conforms to the model is reasonable and the traffic which does not conform to the model is an anomaly. Their analysis showed that the model has the best performance in terms of response time and the packet delivery ratio. Additionally, the model is effectively used with a Wireless Sensor Network (WSN) without any effect on the performance of the network.

Alizadeh *et al.* (2015) presented unsupervised GMMs for the production of application models via two scenarios: first, traffic classification; second, traffic verification. This work aims to confirm whether traffic flow generated by the claimed application conforms to the expected model or not. The authors used GMMs with automatic learning to build a traffic model to meet

http://doi.org/10.18080/jtde.v8n4.307

the real traffic and forming ANIDS. The experiments proceeded on the "UNIBS-2009" dataset where the obtained results are positive as the model was shown to be more effective in the abnormality detection of application traffic in multi-network.

Reddy *et al.* (2017) introduced a methodology using GMMs for outlier detection in univariate network traffic. The proposed approach is useful in big data concepts as it smoothly and efficiently delivers the required information. The GMM model divided all data points into normal and outlier data points. The algorithm can be implemented in several seasonal univariate big data sets. In this work, the authors use particularly time series network traffic data to test and validate their approach. There are two stages to detect outliers in this work. Firstly, GMMs are designed to train data in each time bin of the network time-series data. Second, GMMs are redesigned after removing outliers in the training data, and the re-computed GMMs were used in test data to detect the outliers. The proposed methodology showed the possibility of detecting outliers from various types of datasets and big data scenarios, and it can be easily modified for multi-variate datasets.

Not long ago, Blanco *et al.* (2019) proposed multiple simple GMMs that can model individual features in the dataset to be considered as normal according to the GMM. They tested the approach on the NSL-KDD dataset and formulated the normal behaviour models using samples labelled as healthy. They evaluated the model using the NSL-KDD testing set. The result indicated an F1-score above 0.9 and CAP over 0.49, which is considered better than other supervised and unsupervised proposals. The authors proved that using occurrence probabilities with the unsupervised algorithm will improve the performance and quality of the anomaly detection systems.

Hierarchical Clustering Algorithm

Similar objects in the hierarchical clustering algorithm are grouped into one form called clusters. An endpoint is a group of clusters where each one is diverse from another cluster, and each object in each cluster is widely similar to each other (Bock, n.d.). It is an approach of cluster analysis which tries to build a hierarchy of clusters. Recently, there are several works that have demonstrated the use of this algorithm and clarify it.

Kim & Kim (2015) introduced new IDS using a hierarchical clustering approach. The proposal is a combination of two models: misuse detection and an anomaly detection model. The objective of this work is to improve the detection rate in IDS and reduce the computational cost. In the proposed system, the model of misuse detection is used to remove the known attacks and to

http://doi.org/10.18080/jtde.v8n4.307

reduce the redundant features that help in the detection process. NSL-KDD dataset is used to evaluate the proposed hierarchical methods, and the results showed that detection accuracy and the speed improved, whereas the computational cost was reduced.

Similarly, Tang *et al.* (2016) developed a new intrusion detection model using the hierarchy approach, which also combines two algorithms, fuzzy c-means (GAFCM) and SVM. They used the NSL-KDD dataset to evaluate the model. The experiments showed that using a hierarchical clustering model extends the hard classification detection to the soft classification in the Fuzzy interval, enabling the model to give a high detection rate (DR) and low false alarm rate, whereas SVM classifiers reduce the computation time during model training.

Besides, Liu *et al.* (2017) proposed a dynamic hierarchical clustering approach. First, to reduce the feature dimension, they used feature selection based on information gain. Then, they defined the generalized Euclidean distance to measure the cross-domain data. After that, dynamic clustering accuracy was proposed to direct the dynamic hierarchical clustering. Finally, by using training data, the anomaly detection model was built. The experiment results determined that the proposed approach can achieve a high detection rate as well as a low false alarm rate on KDD-Cup-99 datasets.

The Internet of Things (IoT) is a rapidly growing network of devices that will cover billions of devices in the future. Therefore, researchers and industry are starting to deal with the IoT security issues seriously. Amangele *et al.* (2019) explored the use of the ML approach in IoT network traffic to detect anomalies that attack the Software Defined Network (SDN). SDN allowed hierarchical clustering intending to minimize the packet level processing of intrusion detection. For the evaluation step, they compared various supervised algorithms using a CICIDS2017 dataset. The results showed that the proposed model gives a drastic decrease in per-packet processing at the network edge in SDN.

Table 3 summarizes the above publications that used unsupervised learning algorithms for anomaly detection in the last five years. The table highlights the publication year, the unsupervised learning technique used, the anomaly type addressed, the dataset used, and the accuracy of the proposed approaches. Note that some papers did not report the accuracy achieved by their approaches: they only stated that they achieved better accuracy than the state of the art.

http://doi.org/10.18080/jtde.v8n4.307

Table 3. Unsupervised anomaly detection approaches (SoA: State-of-the-art)

Authors	Year	ML Technique	Anomaly type	Dataset	Detection Accuracy (%)
Munz *et al.*	2016	k-means algorithm	DoS attacks and port scans	Cisco Netflow	Better than the SoA
Aung & Min	2018	k-means algorithm	DoS, R2L, U2R, and Prob	KDD CUP 99	99.9%
Chen *et al.*	2016	HMM	Generic network attack	Real-time network	93.2%
Stefanidis *et al.*	2016	HMM	Normal, DoS, MFCI, MPCI, MSCI, CMRI	Collected by researchers	93.4%
K. Zegeye *et al.*	2018	HMM	Benign, DoS Hulk, Port Scan, DDoS, DoS, FTP Patator	CICIDS2017	97.9%
Liang *et al.*	2018	weighted HMM	DDOS attacks	DARPA2000	Better than the SoA
Ding & Tian	2016	PCA	DDoS attacks	Abilene network dataset	93.33%
Vasan & Surendiran	2016	PCA	generic attack	KDD-CUP and UNB-ISCX	98.8%
Paffenroth *et al.*	2018	Robust PCA	DDoS attacks, IP sweeps and probing and breaking	DARPA	Better than the SoA.
Hoang & Nguyen	2018	PCA	Generic attack	Kyoto Honeypot	Better than the SoA
Lalitha & Josna	2015	Gaussian Mixture Model	Generic attack	WNS simulation	Better than the SoA
Alizadeh *et al.*	2015	Gaussian Mixture - GMMs	Zero-day	UNIBS-2009	98.7%
Reddy *et al.*	2017	GMMs	outliers	Collected by researchers	Better than the SoA
Roberto Blanco *et al.*	2019	GMMs	DoS, R2L, U2R, and Prob	NSL- KDD	Better than the SoA
Kim & Sehun Kim	2015	hierarchical approach	DoS, R2L, U2R, and Prob	NSL-KDD	96.1%
Tang *et al.*	2016	GAFCM + SVM	DoS, R2L, U2R and Prob	NSL-KDD	99.76%
Liu *et al.*	2017	dynamic hierarchical clustering	DoS, R2L, U2R, and Prob	KDD-Cup-99	98.2%

http://doi.org/10.18080/jtde.v8n4.307

Authors	Year	ML Technique	Anomaly type	Dataset	Detection Accuracy (%)
Amangele *et al.*	2019	hierarchical clustering	BOT, DoS, R2L, U2R, Prob, PSCAN, Web Attacks	CICIDS2017	99%

Comparison Between Supervised and Unsupervised Techniques

In SVM, for instance, combining feature selection and parameter optimization reduces training and testing time, as well as improving the effectiveness of the SVM Classifier. Additionally, according to the Naïve Bayesian model, combining NB with PCA to extract new properties helps to improve the traditional NB algorithm, which cannot consider the problem of weights in attributes. Based on previous studies presented in this survey, we can say supervised methods are commonly used with training data that are not real-time due to its simplicity and efficiency. Further methods employed are more flexible, with a high detection rate for known attacks. Also, by combining many classifiers, the methods can perform well, even if one is weak (Ensemble methods). However, supervised methods have some disadvantages addressed in this paper, such as the level of resource consumption and time complexity in terms of big data. Furthermore, real-time performance is not easy to acquire.

As seen in the survey, unsupervised learning does not require training data, as it is the first process for feature detection. Feature detection in unsupervised techniques is an attempt to determine the hidden pattern in given data without training data, so they are able to detect unknown attacks. For instance, in hierarchical clustering using the FCM approach, the membership function and the fuzzy interval are used both in the extended soft classification and the previous hard classification. This enables the model to detect unknown attacks. Moreover, in a robust PCA model, network packets are used to capture data which displays the effectiveness in different network attack detection systems. The method accurately detected an anomaly/attack that was not encountered or trained previously.

Given these studies in our survey, unsupervised learning techniques have been implemented in different areas and applications such as IoT, WSN, 5G mobile networks, and Industrial Control Systems (ICS), which primarily concern data all in real-time. Fast response and reduced computational complexity in large datasets are the most important advantages of unsupervised techniques, with the ability to achieve good results of accuracy combined with other classifiers in real-time networks. Detection rate is one of the essential limitations in anomaly detection, where it is dependent on proximity measures. It has a direct effect on the false alarm rate. As

http://doi.org/10.18080/jtde.v8n4.307

noted, time consumption in these algorithms is considered a problem that they have to overcome in future anomaly detection systems.

Semi-Supervised Learning

Semi-supervised machine learning could be a combination of supervised and unsupervised machine learning approaches (DataRobot AI Wiki). Typically, in semi-supervised learning, the algorithm learns from a dataset that contains both labelled and unlabelled data. Usually, the majority is unlabelled data. If there are insufficient labelled data to build an accurate model and insufficient resources to get additional data, semi-supervised techniques can be used to maximize the size of the training data. For that, we reviewed recently published papers which focused on using semi-supervised learning to detect anomalies in the network.

Aissa & Guerroumi (2016) proposed two-stage semi-supervised methods for anomaly detection. The aim of the first stage is to make a probabilistic model of normal samples and measure any deviation that exceeds an established threshold. This threshold is deduced from a regular discriminate function of greatest likelihood. The second stage is to minimize False Alarm Rate (FAR) through repetitions that reclassify anomaly clusters from the previous stage, employing a similarity distance and the anomaly's cluster dispersion rate. The authors evaluated the proposed method on NSL-KDD and Kyoto 2006+ datasets. The experimental results showed that the proposed approach outperforms the Naïve Bayes algorithm in terms of Detection Rate and False Positive Rate.

Ashfaq *et al.* (2017) designed a unique fuzziness-based semi-supervised learning method by using unlabelled samples with the assistance of a supervised learning algorithm to boost the classifier's performance for the IDS. The classifier is retrained when incorporating every class separately into the first training set. The experimental results using this method on the NSL-KDD dataset showed that unlabelled samples that belong to low and high fuzziness groups have a significant contribution to boost the classifier's performance compared to existing ones.

Borghesi *et al.* (2019) suggested a semi-supervised technique for anomaly detection in supercomputers. This approach is based on a type of neural network referred to as an autoencoder. This approach involves learning the normal state of supercomputer nodes and training them to discern anomalous conditions from normal behaviour. It is doing so to end up relying only on the availability of feature data and the standard system state. This is different from supervised techniques that require data sets with multiple examples of anomalous states.

http://doi.org/10.18080/jtde.v8n4.307

The autoencoder-based method outcome was shown to significantly outperform the supervised method, where the accuracy was increased by 12%.

Idhammad *et al.* (2018) investigated the use of semi-supervised techniques in DDoS detection. Supervised techniques in DDoS detection frequently rely on the availability of labelled network traffic datasets, whereas unsupervised techniques detect attacks by evaluating incoming network traffic. This approach used an online sequential semi-supervised machine learning method for DDoS detection based on network entropy estimation, co-clustering, information gain ratio, and other trees algorithms. The unsupervised technique of this approach enables the reduction of irrelevant average traffic data for DDoS detection, allowing the reduction of false-positive rates and increasing accuracy. They performed the experiments on different datasets, UNSW-NB15, UNBISCX 12, and NSL-KDD, with high accuracy of 93.71, 99.88, and 98.23%, respectively.

Meanwhile, Yuan *et al.* (2016) proposed a novel semi-supervised AdaBoost technique for network anomaly detection. In this approach, a combination of a tri-training approach was used with AdaBoost algorithms. The boost samples were replaced with three different AdaBoost algorithms to provide adversity. Iterations were then run for each simulation to provide average results. The simulations showed that this approach is reproducible and consistent over various runs, outperforming other competitive learning algorithms. The proposed approach has a fast execution time, as well as providing a balance between detection rate and false-alarm rate. The CUP1999 dataset was used to evaluate the result of the proposed algorithm with different types of attacks, such as DoS, U2R, probing, and R2L.

Duong & Hai (2015) also proposed a semi-supervised model called M-PCA for network traffic anomaly detection. In this approach, modified Mahalanobis distance based on PCA is used for network traffic anomaly detection. This intends to explore the effectiveness of PCA in semi-supervised methods that use small training datasets. This approach employs a K-means clustering method to create a typical profile of traffic to improve the training dataset and weights that help to select principal components of PCA. The evaluation of the proposed algorithm is done on the NSL-KDD dataset with different types of attacks, such as DoS, U2R, probing attacks, and R2L.

Table 4. Semi-Supervised anomaly detection approaches

Authors	Year	ML Technique	Anomaly type	Dataset	Detection Accuracy (%)
Aissa & Guerroumi	2016	SSAD	DoS attacks and port scans	NSL-KDD + Kyoto 2006	90%

http://doi.org/10.18080/jtde.v8n4.307

Authors	Year	ML Technique	Anomaly type	Dataset	Detection Accuracy (%)
Ashfaq *et al.*	2017	SLFN	DoS, R2L, U2R, and Prob	NSL-KDD	84.12 %
Borghesi *et al.*	2019	autoencoder	Generic network attack	Real-time data in network	93.8%
Idhammad *et al.*	2018	online sequential semi-supervised ML	DDoS	UNSW-NB15, UNBISCX 12, and NSL-KDD	93.71, 99.88, and 98.23%
Yuan *et al.*	2016	AdaBoost algorithms	DoS, U2R, probing, and R2L	CUP1999	96.63%
Duong & Hai	2015	M-PCA	DoS, U2R, probing, and R2L	NSL-KDD	87.8%

Conclusion and Open Issues

With our lives becoming more and more digitalized, computer networks are becoming more critical and dependable services. At the same time, they become more prone to anomalies and worse—malicious attacks. This motivates researchers to propose different solutions to the overarching issue of anomaly detection in network traffic, particularly machine learning techniques, whether supervised, unsupervised or semi supervised.

In this paper, we surveyed works in the field of anomaly detection using machine learning in the last five years. First, we defined the background related to our work: (i) types of network anomalies; (ii) categories of machine learning approaches; and (iii) types of network attacks. Then, we reviewed, categorized, and discussed the papers that used machine learning techniques for anomaly detection. Furthermore, we underlined some of the open issues to improve the detection of anomalies systems.

Based on our review, we are able to identify numerous aspects that require more attention from the research community within the anomaly detection area, such as detection rate, process complexity, and high false alarm rate. In addition, we identified a critical challenge of real-time anomaly detection, particularly when streaming data that is constantly shifting.

Finally, while there is a lot of work on anomaly detection in traditional computer networks, the emergence of the Internet of Things (IoT) and their pervasiveness is likely to exacerbate the need for more scalable and accurate anomaly detection techniques, that are able to deal with different data types. The security of IoT network infrastructure must be at the highest level.

http://doi.org/10.18080/jtde.v8n4.307

Acknowledgements

The authors would like to thank the postgraduate research center, Department of Computer Science and Engineering at Visvesvaraya Technological University (VTU), Mysore, Karnataka State, India for encouraging this comprehensive survey and providing access to the online resources and facilities. The author Malika Bendechache is supported, in part, by Science Foundation Ireland (13/RC/2094 and 13/RC/2106).

References

Aburomman, A. A., & Reaz, M. B. I. (2017). A survey of intrusion detection systems based on ensemble and hybrid classifiers. *Computers & Security*, *65*, 135-152.

Agrawal, S., & Agrawal, J. (2015). Survey on anomaly detection using data mining techniques. *Procedia Computer Science*, *60*, 708-713.

Ahmad, S., Lavin, A., Purdy, S., & Agha, Z. (2017). Unsupervised real-time anomaly detection for streaming data. *Neurocomputing*, *262*, 134-147.

Aissa, N. B., & Guerroumi, M. (2016). Semi-supervised statistical approach for network anomaly detection. *Procedia Computer Science*, *83*, 1090-1095.

Akhi, A. B., Kanon, E. J., Kabir, A., & Banu, A. (2019). Network Intrusion Classification Employing Machine Learning: A Survey. (Doctoral dissertation) Department of Computer Science and Engineering, United International University, Bangladesh.

Alizadeh, H., Khoshrou, A., & Zuquete, A. (2015). Traffic classification and verification using unsupervised learning of Gaussian Mixture Models. In 2015 IEEE international workshop on measurements & networking (M&N). 1-6. IEEE.

Amangele, P., Reed, M. J., Al-Naday, M., Thomos, N., & Nowak, M. (2019). Hierarchical Machine Learning for IoT Anomaly Detection in SDN. In 2019 International Conference on Information Technologies (InfoTech). 1-4. IEEE.

Anderson, J. P. (1980). Computer security threat monitoring and surveillance. Technical Report, Fort Washington, PA, James P. Anderson Co.

Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H., & He, Y. L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences*, *378*, 484-497.

Aung, Y. Y., & Min, M. M (2018). An analysis of K-means algorithm based network intrusion detection system. *Advances in Science, Technology and Engineering Systems Journal*, *3*(1), 496-501.

Bauer, F. C., Muir, D. R., & Indiveri, G (2019). Real-Time Ultra-Low Power ECG Anomaly Detection Using an Event-Driven Neuromorphic Processor. *IEEE Transactions on*

Biomedical Circuits and Systems, *13*, 1575–82. https://doi.org/10.1109/TBCAS.2019.2953001

Bhati, B. S., Rai, C. S., Balamurugan, B., & Al-Turjman, F. (2020). An intrusion detection scheme based on the ensemble of discriminant classifiers. *Computers & Electrical Engineering*, *86*, 106742.

Bhattacharyya, D. K., & Kalita, J. K. (2013). *Network anomaly detection: A machine learning perspective*. CRC Press.

Blanco, R., Malagón, P., Briongos, S., & Moya, J. M. (2019). Anomaly Detection Using Gaussian Mixture Probability Model to Implement Intrusion Detection System. In International Conference on Hybrid Artificial Intelligence Systems, 648-659. Springer, Cham.

Bock, T., Displayr blog, https://www.displayr.com/what-is-hierarchical-clustering/

Borghesi, A., Bartolini, A., Lombardi, M., Milano, M., & Benini, L. (2019). A semisupervised autoencoder-based approach for anomaly detection in high performance computing systems. *Engineering Applications of Artificial Intelligence*, *85*, 634-644.

Chakir, E. M., Moughit, M., & Khamlichi, Y. I. (2018). An effective intrusion detection model based on SVM with feature selection and parameters optimization. *Journal of Theoretical and Applied Information Technology*, *96*(12), 3873–85. https://www.researchgate.net/publication/326391656

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys (CSUR)*, *41*(3), 1-58.

Chauhan, P., & Shukla, M. (2015). A review on outlier detection techniques on data stream by using different approaches of K-Means algorithm. In 2015 International Conference on Advances in Computer Engineering and Applications. 580-585. IEEE.

Chen, C. M., Guan, D. J., Huang, Y. Z., & Ou, Y. H. (2016). Anomaly network intrusion detection using hidden Markov model. *International Journal of Innovative Computing, Information and Control*, *12*, 569-580.

Chew, Y. J., Ooi, S. Y., Wong, K. S., & Pang, Y. H. (2020). Decision Tree with Sensitive Pruning in Network-based Intrusion Detection System. In Computational Science and Technology, 1-10. Springer, Singapore.

DataRobot AI Wiki. https://www.datarobot.com/wiki/semi-supervised-machine-learning/

Ding, M., & Tian, H. (2016). PCA-based network traffic anomaly detection. *Tsinghua Science and Technology*, *21*(5), 500-509.

Dua, S., & Du, X. (2016). *Data mining and machine learning in cybersecurity*. CRC press.

Duong, N. H., & Hai, H. D. (2015). A semi-supervised model for network traffic anomaly detection. In 2015 17th International Conference on Advanced Communication Technology (ICACT), 70-75. IEEE.

Fernandes G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., & Proença, M. L. (2019). A comprehensive survey on network anomaly detection. *Telecommunication Systems*, *70*(3), 447-489.

Gu, J., Wang, L., Wang, H., & Wang, S. (2019). A novel approach to intrusion detection using SVM ensemble with feature augmentation. *Computers & Security*, *86*, 53-62.

Han, X., Xu, L., Ren, M., &Gu, W. (2015). A Naive Bayesian network intrusion detection algorithm based on Principal Component Analysis. In 2015 7th International Conference on Information Technology in Medicine and Education (ITME), 325-328. IEEE.

Haripriya, L.A., Jabbar, M., & Seetharamulu, B. (2018). A Novel Intrusion Detection System Using Artificial Neural Networks and Feature Subset Selection. *International Journal of Engineering and Technology*, *7*(4), 181. http://doi.org/10.14419/ijet.v7i4.6.20458

Hoang, D. H., & Nguyen, H. D. (2018). A PCA-based method for IoT network traffic anomaly detection. In 2018 20th International Conference on Advanced Communication Technology (ICACT), 381-386. IEEE.

Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. In 2016 International Symposium on Networks, Computers and Communications (ISNCC), 1-6. IEEE.

Hu, J., Ma, D., Liu, C., Shi, Z., Yan, H., & Hu, C. (2019). Network Security Situation Prediction Based on MR-SVM. *IEEE Access*, *7*, 130937-130945.

Idhammad, M., Afdel, K., & Belouch, M. (2018). Semi-supervised machine learning approach for DDoS detection. *Applied Intelligence*, *48*(10), 3193-3208.

Karim, S., Rousanuzzaman, P. A. Y., Khan, P. H., & Asif, M. (2019). Implementation of K-Means Clustering for Intrusion Detection. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *5*, 1232–41.

Kevric, J., Jukic, S., & Subasi, A. (2017). An effective combining classifier approach using tree algorithms for network intrusion detection. *Neural Computing and Applications*, *28*(1), 1051-1058.

Khraisat, A., Gondal, I., & Vamplew, P. (2018). An anomaly intrusion detection system using C5 decision tree classifier. In Pacific-Asia Conference on Knowledge Discovery and Data Mining, 149-155. Springer, Cham.

Kim, E., & Kim, S. (2015). A novel hierarchical detection method for enhancing anomaly detection efficiency. In 2015 International Conference on Computational Intelligence and Communication Networks (CICN), 1018-1022. IEEE.

Knapp, E. D., & Langill, J. T. (2014). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Syngress.

Kotu, V., & Deshpande, B. (2018). *Data Science: Concepts and Practice*. Morgan Kaufmann.

Kumar, D. A., & Venugopalan, S. R. (2018). A novel algorithm for network anomaly detection using adaptive machine learning. In Progress in Advanced Computing and Intelligent Engineering, 59-69. Springer, Singapore.

Kusyk, J., Uyar, M.U., & Sahin, C. S. (2018). Survey on evolutionary computation methods for cybersecurity of mobile ad hoc networks. *Evolutionary Intelligence*, *10*, 95–117. https://doi.org/10.1007/s12065-018-0154-4

Lakhina, A., Crovella, M., & Diot, C. (2004). Diagnosing network-wide traffic anomalies. *ACM SIGCOMM computer communication review*, *34*(4), 219-230.

Lalitha, K. V., & Josna, V. R. (2016). Traffic verification for network anomaly detection in sensor networks. *Procedia Technology*, *24*, 1400-1405.

Larriva-Novo, X. A., Vega-Barbas, M., Villagra, V. A., & Sanz Rodrigo, M. (2020). Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies. *IEEE Access*, *8*, 9005–14.

Lee, W., & Stolfo, S. (1998). Data mining approaches for intrusion detection In the 7th USENIX Security Symposium, San Antonio, Texas, USA.

Liang, W., Long, J., Chen, Z., Yan, X., Li, Y., Zhang, Q., & Li, K. C. (2018). A security situation prediction algorithm based on HMM in mobile network. *Wireless Communications and Mobile Computing*, 2018.

Liu, Y., Xu, H., Yi, H., Lin, Z., Kang, J., Xia, W., Shi, Q., Liao, Y., & Ying, Y (2017). Network anomaly detection based on dynamic hierarchical clustering of cross domain data. In 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 200-204. IEEE.

Manasa, K. N., & Padma, M. C. (2019). A Study on Sentiment Analysis on Social Media Data. In Emerging Research in Electronics, Computer Science and Technology, 661-667. Springer, Singapore.

Mehmood, A., Mukherjee, M., Ahmed, S. H., Song, H., & Malik, K. M. (2018). NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks. *The Journal of Supercomputing*, *74*(10), 5156-5170.

Meng, X., Mo, H., Zhao, S., & Li, J. (2017). Application of anomaly detection for detecting anomalous records of terrorist attacks. In 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 70-75. IEEE.

Mohammadi, S., Mirvaziri, H., Ghazizadeh-Ahsaee, M., & Karimipour, H. (2019). Cyber intrusion detection by combined feature selection algorithm. *Journal of information security and applications*, *44*, 80-88.

Mohd Ali, A. (2018). Anomalous behaviour detection using heterogeneous data. (Doctoral dissertation) Lancaster University.

Münz, G., Li, S., & Carle, G. (2007). Traffic anomaly detection using k-means clustering. In GI/ITG Workshop MMBnet, 13-14.

Omar, S., Ngadi, A., & Jebur, H. H. (2013). Machine learning techniques for anomaly detection: an overview. *International Journal of Computer Applications*, *79*(2).

Paffenroth, R., Kay, K., & Servi, L. (2018). Robust pca for anomaly detection in cyber networks. arXiv preprint arXiv:1801.01571.

Peng, H., Sun, Z., Zhao, X., Tan, S., & Sun, Z. (2018). A detection method for anomaly flow in software defined network. *IEEE Access*, *6*, 27809-27817.

Pham, N. T., Foo, E., Suriadi, S., Jeffrey, H., & Lahza, H. F. M. (2018). Improving performance of intrusion detection system using ensemble methods and feature selection. In Proceedings of the Australasian Computer Science Week Multiconference, 1-6.

Rai, A. (2020). Optimizing a New Intrusion Detection System Using Ensemble Methods and Deep Neural Network. In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184), 527-532. IEEE.

Rai, K., Devi, M. S., & Guleria, A. (2016). Decision tree based algorithm for intrusion detection. *International Journal of Advanced Networking and Applications*, *7*(4), 2828.

Reddy A., Ordway-West, M., Lee, M., Dugan, M., Whitney, J., Kahana, R., & Rao, M. (2017). Using Gaussian mixture models to detect outliers in seasonal univariate network traffic. In 2017 IEEE Security and Privacy Workshops (SPW), 229-234. IEEE.

Rettig, L., Khayati, M., Cudré-Mauroux, P., & Piórkowski, M. (2019). Online anomaly detection over big data streams. In Applied Data Science, 289-312. Springer, Cham.

Shukur, H. A., & Kurnaz, S. (2019). Credit Card Fraud Detection using Machine Learning Methodology. *International Journal of Computer Science and Mobile Computing*, *8*, 257-260.

Stefanidis, K., & Voyiatzis, A. G. (2016). An HMM-based anomaly detection approach for SCADA systems. In IFIP International Conference on Information Security Theory and Practice, 85-99. Springer, Cham.

Swarnkar, M., & Hubballi, N. (2016). OCPAD: One class Naive Bayes classifier for payload based anomaly detection. *Expert Systems with Applications*, *64*, 330-339.

Tang, C., Xiang, Y., Wang, Y., Qian, J., & Qiang, B. (2016). Detection and classification of anomaly intrusion using hierarchy clustering and SVM. *Security and Communication Networks*, *9*(16), 3401-3411.

Techopedia - IT Education Site. https://www.techopedia.com/definition/30331/gaussian-mixture-model-gmm

Thakare, Y. S., & Bagal, S. B. (2015). Performance evaluation of K-means clustering algorithm with various distance metrics. *International Journal of Computer Applications*, *110*(11), 12-16.

Vasan, K. K., & Surendiran, B. (2016). Dimensionality reduction using principal component analysis for network intrusion detection. *Perspectives in Science*, *8*, 510-512.

http://doi.org/10.18080/jtde.v8n4.307

Veselý, A., & Brechlerova, D. (2009). Neural networks in intrusion detection systems. *Agricultural Economics (*Zemědělská ekonomika*)*, 156-165.

Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). Evaluation of recurrent neural network and its variants for intrusion detection system (IDS). *International Journal of Information System Modeling and Design (IJISMD)*, *8*(3), 43-63.

Wang, L., Li, J., Bhatti, U. A., & Liu, Y. (2019). Anomaly Detection in Wireless Sensor Networks Based on KNN. In International Conference on Artificial Intelligence and Security, 632-643. Springer, Cham.

Weerasinghe, S., Erfani, S. M., Alpcan, T., & Leckie, C. (2019). Support vector machines resilient against training data integrity attacks. *Pattern Recognition*, *96*, 106985.

Wu, K., Chen, Z., & Li, W. (2018). A novel intrusion detection model for a massive network using convolutional neural networks. *IEEE Access*, *6*, 50850-50859.

Xiao, P., Qu, W., Qi, H., & Li, Z. (2015). Detecting DDoS attacks against data center with correlation analysis. *Computer Communications*, *67*, 66-74.

Yuan, Y., Kaklamanos, G., & Hogrefe, D. (2016). A novel semi-supervised Adaboost technique for network anomaly detection. In Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, 111-114.

Yun, J. H., Hwang, Y., Lee, W., Ahn, H. K., & Kim, S. K. (2018). Statistical similarity of critical infrastructure network traffic based on nearest neighbor distances. In International Symposium on Research in Attacks, Intrusions, and Defenses, 577-599. Springer, Cham.

Zegeye, W. K., Dean, R. A., & Moazzami, F. (2019). Multi-layer hidden Markov model based intrusion detection system. *Machine Learning and Knowledge Extraction*, *1*(1), 265-286.

Zhang, T., Wang, X., Li, Z., Guo, F., Ma, Y., & Chen, W. (2017). A survey of network anomaly visualization. *Science China Information Sciences*, *60*(12), 121101.

Zhao, Q., Zhang, Y., Shi, Y., & Li, J. (2019). Analyzing and Visualizing Anomalies and Events in Time Series of Network Traffic. In International Conference on Computing and Information Technology, 15-25. Springer, Cham.

http://doi.org/10.18080/jtde.v8n4.307