

Flow-Based Intrusion Detection on Software-Defined Networks: A Multivariate Time Series Anomaly Detection Approach

Sultan ZAVRAK (✉ sultanzavrak@duzce.edu.tr)

Duzce University: Duzce Universitesi <https://orcid.org/0000-0001-6950-8927>

Murat İskefiyeli

Sakarya University: Sakarya Universitesi

Research Article

Keywords: Intrusion detection, flow anomaly detection, deep learning, semi-supervised learning, software-defined networks, time series anomaly detection

Posted Date: April 19th, 2022

DOI: <https://doi.org/10.21203/rs.3.rs-1141416/v1>

License:  This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Abstract

In this study, SAnDet architecture, which can do an anomaly-based intrusion detection by taking advantage of the capabilities offered by SDN architecture, is presented and implemented as controller application. A detailed description of this system which consists of three main modules which are statistics collector, anomaly detector, and anomaly prevention is given. More specifically, Replicator Neural Networks (RNN) which is a special variant of the autoencoder, and EncDecAD methods which a special type of LSTM networks that can produce successful results especially in given data series, were used to identify unknown attacks using flow features collected from OpenFlow switches. In experiments, flow-based features extracted from network traffic data including different types of attacks, are given as input into models as time series. The results of the methods are calculated in terms of the ROC and AUC metrics. Experimental results show that EncDecAD outperforms RNN and the methods proposed in the literature.

1. Introduction

Cyber-attacks are defined as a set of malicious activities that hinder, obstruct, or destroy information and services that exist in computer networks. Intrusion Detection and Prevention Systems (IDPS) are the mechanisms that perform the functions of detecting and mitigating or preventing these attacks at the network level. The fundamental principle of attack detection is based on the hypothesis that unauthorized behaviors are prominently distinct from the normal ones and thus they are detectable. In addition to many attack detection approaches in the literature, researchers are now focusing more on anomaly-based network intrusion detection methods, since they can identify unknown attacks as well as known attacks [1].

Software-Defined Networking (SDN) is an innovative network paradigm that promises to transform the limitations of traditional network infrastructure that is currently used [2]. This paradigm takes the control logic of the network from forwarding devices such as routers and switches, and places it on the logically centralized controller [3]. From a network security perspective, SDN defines a single control point for forwarding data flows across the entire network infrastructure. By preparing a high-level reactive security monitoring, analysis, and response system, SDN architecture can be exploited to increase network security. [4], [5]. With network security applications implemented using the OpenFlow (OF) protocol, which is an implemented version of the SDN paradigm, it is also possible to implement flows that can handle complex logic rather than simply allow or block [6].

Network traffic analysis or anomaly detection methods frequently generate security-related data transmitted to the central controller. On the controller, applications can be run to analyze and associate the feedback gathered across the entire network. New or updated security policies can be deployed to network components in the form of flow rules based on the results of the analysis. This unified approach can effectively accelerate and protect against security threats to the network [4]. As OF security applications, intrusion detection and intrusion prevention or mitigation methods can be implemented.

The main contributions of the study are summarized as follow:

- This study focuses on the identification of network attacks from flow-based features based on an anomaly-based approach on SDN environments. More specifically, the SAnDet (a shorthand of SDN Anomaly Detector) architecture, which is designed to detect intrusions by taking advantage of the facilities offered by the SDN architecture, is presented and implemented as a controller application. A detailed description of SAnDet consisting of three main modules which are statistics collector, anomaly detector, and anomaly prevention is given.
- The anomaly detectors RNN and EncDecAD are built using a semi-supervised learning approach. In addition, unlike the other studies, this one is unique in that it uses deep learning techniques to detect intrusions by feeding flow-based data as a multivariate time series.
- Based on AUC and accuracy findings, it is proved that EncDecAD-based anomaly detection outperforms RNN and other approaches in the literature.

The following is a breakdown of how the article is structured. The works on flow-based attack detection in SDN environments are discussed in the next section. The third section contains theoretical information regarding the research methodologies. The fourth section contains the experimental methods and results. The final section explains the results.

2. Related Work

The goal of the anomaly detection technique is to create a statistical model that can be used to characterize typical traffic patterns. [7]. In such a situation, any deviation from this pattern is counted an anomaly and identified as an attack. There have been a number of studies that have investigated the effectiveness of anomaly-based attack detection in SDN environments. In this section, a summary of the studies in the literature is given in five categories, taking into account the taxonomy done by Jafarian et al. [7], flow-count-based schemes, information theory-based schemes, entropy-based schemes, and deep learning-based schemes, and hybrid schemas. A more in-depth look at studies on anomaly-based intrusion detection on SDN networks can be found in [8] and [7].

Traffic flows in the network are initially obtained and aggregated according to a subnet prefix in flow counting-based anomaly detection methods. Although this process brings extra load to the system, it accurately detects abnormal conditions in the network [7]. Zhang et al. [9] suggested a prediction-based scheme that dynamically alters the level of detail of the measurement across both spatial and temporal dimensions to better balance surveillance overhead and anomaly detection accuracy to detect anomalies. Ha et al. [10] provide a traffic sampling strategy for an intrusion detection system capable of operating on large-scale SDN networks that maximizes the usage of malicious traffic's control capacity while keeping the sampled traffic's overall aggregation volume below the control computing capacity. Granby et al. [11] design SDNPANDA, a plug-in software package to identify anomalies in a software-defined data center. In DoS attacks, Hommes et al. [12] investigate the flow table saturation problem of OF switches. Attack cases were determined in the study by assessing the variation in the network's logical topology for

various attack kinds and measuring the distance requirements on a table. Using traffic analysis of packet flows, Carvalho et al. [13] demonstrated a real-time anomaly detection and prevention system in SDN. The digital signature of flows acquired using the OF protocol is created by profiling normal traffic behavior. Existing traffic is compared to a previously developed traffic profile in order to identify any suspicious traffic events that deviate from expected behavior. As a result, reporting is done to verify prevention and results in the event of an attack. He et al. [14] presented an anomaly detection scheme in SDN by selecting the required features of the data set and using a density peak-based clustering algorithm. Carvalho et al. [15] presented an ecosystem based on SDN to proactively identify anomalies by scanning network traffic. Peng et al. [16] proposed a preprocessing module that normalizes flow property vectors to detect DDoS attacks in SDN based on central control, as well as a scheme that processes these vectors and detects anomalies using the KNN method.

Information theory methods are based on the assumption that an existing anomaly in traffic causes a change in the information of traffic data sets. Mehdi et al. [17] focus on traffic anomaly detection in SDN environments. Multiple anomaly detection algorithms in SOHO environments have been experimentally tested to verify their applicability. The study provides experimental results on the efficiency of TRW-CB [18], Rate-Limiting [19], Maximum Entropy Detector [20] and NETAD [21] intrusion detection algorithms using only low network traffic speeds. Dotcenko et al. [6] proposed a method that uses fuzzy logic as well as a mechanism for analyzing network traffic to classify network traffic into attack traffic and normal traffic. Kokila et al. [22] conducted a study examining different machine learning techniques for identifying DDoS attacks in SDN environments and their performance in intrusion detection. In SDN networks, Sathya and Thangarajan [23] investigated gathering data and applying the Decision Tree approach for anomaly detection using the NSL-KDD data set rather than the intended properties of the network traffic.

In determining the randomness of a data set, entropy-based anomaly detection algorithms have proven to be particularly beneficial in spotting network anomalies [7], [24]. Wang et al. [25] proposed a method that could be applied to low-layer switches of SDNs such as OpenvSwitch to detect low-throughput DDoS flooding attacks based on the entropy level. On the other hand, Giotis et al. [26] offers a scalable and effective mechanism for anomaly detection and mitigation in SDN architectures. Unlike the study in [17], this study offers a mechanism that uses sFlow [27] monitoring data instead of OF statistics, which reduces the controller process load and therefore works at higher line speeds, and gives their experimental results. Besides, when an anomaly is detected, it is shown that the network anomaly is successfully reduced (mitigation) by making modifications in the flow tables using the OF protocol. Also, when the sampled statistical data are given as an input to the anomaly detection algorithm, it is seen that the anomaly detection rate is lower than [17]. Francois and Festor [28] capture the flow inputs of each device by the SDN controller, such as switches for anomaly detection in SDN. After the attack has been identified and the characteristics of the attack packets have been discovered, surveillance will be undertaken on the switch where the attack has been detected, depending on the advantages offered by the controller.

Deep learning methods include a knowledge-based learning-based development algorithm, and the keywords for deep learning are: unsupervised machine learning, multi-layer learning, and artificial intelligence [29][7]. Instead, the deep learning structure has solid capability for adaptability in SDNs in terms of its features and the ability to learn process data on its own [30]. Dey and Rahman [30] propose a network breach detection system based on deep learning for SDN environments. They used the ANOVA F-Test and the REF feature selection scheme to show that the Gated Recurrent Unit LSTM is the best classifier based on several performance assessment metrics. Three components are proposed by Niyaz et al. [31] for a DDoS detection system for SDN environments. A deep learning method is used in the proposed system for feature selection and traffic regulation. A deep learning-based solution for flow-based anomaly identification in SDN is proposed by Tang et al. [32]. To detect suspicious flows in SDN, Garg et al. [33] suggested an anomaly detection method based on a hybrid and real-time constrained Boltzmann machine and gradient decay-based SVM. For SDN-based 5G networks, Li et al. [34] proposed an intelligent hybrid IDS. In the suggested system, the k-means algorithm was used for flow classification in addition to the random forest method for feature selection.

In addition to all the aforementioned methods, hybrid schemes have been proposed in the literature for anomaly-based violation detection in SDN networks. For SDN, Santos Da Silvo et al. [35] propose an anomaly detection and traffic classification based on machine learning techniques. Anomaly detection and classification is the lightweight phase based on entropy analysis with low computational cost to instantly detect possibly malicious flows, and heavyweight using SVM (Support Vector Machine) to categorize such flows according to their abnormal behavior.) is carried out in two complementary stages, one stage. Pang et al. [36] proposed a new high throughput and highly accurate anomaly detection scheme FADE in SDN. FADE generates a few custom flow rules on these flows to precisely measure its statistics and commands the loading and timeout of these reserved flow rules. Cui et al. [37] proposed a scheme that includes four modules in SDN to overcome DDoS: attack detection trigger, attack detection, traceback, and attack prevention. In the study conducted by Braga et al. [38], the forwarding plane of the network device is managed using OF, and the flow statistics are collected, focusing only on Distributed Denial of Service (DDoS) attacks on the data plane, and the performance analysis presented is restricted to the suggested attack detection method and does not include information with entire performance of the system. The method used in the detection of attacks is Self Organizing Maps (SOM), a type of unsupervised artificial neural network. The parameters input to this method are traffic flow statistics.

3. Theoretical Background

This section focuses on the basic components of the SDN architecture, and how it solves the problems in traditional networks. Besides, theoretical information of RNN and EncDecAD anomaly detection methods are also presented.

3.1. Software-Defined Networking

As stated by the Open Networking Foundation (ONF) [39], SDN is a fresh architecture that separates network forwarding and control tasks. This allows network control to be directly programmable and the architecture for network services and applications to be conceptualized. Infrastructure devices operate as simple forwarding engines in this architecture, dealing with incoming packets according to a number of rules that are instantaneously produced by a controller in the control layer along with the prescribed program logic. The controller typically executes on a distant machine and communicates with the forwarding elements over a secure link utilizing a few standardized commands. For SDN, ONF offers a high-level architecture [40] that is divided vertically into three main essential layers: i) Infrastructure Layer consists of forwarding elements, which include physical and virtual switches that can be accessed with an open interface. ii) The Control Layer is composed of a collection of software-based SDN controllers that provide unified control capabilities via open APIs for handling forwarding behavior. Controllers can communicate with one another via three communication interfaces: Southbound, Northbound, and East/Westbound. iii) The Application Layer mainly comprises of end-user apps that make use of SDN communication and network services. The main parts of this architecture such as the control layer, application layer, infrastructure layer, and communication interfaces between these three layers are shown in detail in Figure 1.

Through three open interfaces, the SDN controller communicates with these three layers: a) The southbound interface enables communication between the controller and the forwarding components of the infrastructure layer. The OF protocol, which is managed by ONF, is an essential element for generating SDN solutions according to ONF and can be seen as an encouraging implementation of such an interaction. b) The northbound interface enables the controllers to be programmable by exposing the controllers' universal network abstraction and other features for usage by programs at the application layer. Rather than a protocol, it is viewed as a software API that enables the programming and management of the network. While there is no standardization effort for this, many brands offer REST-based APIs for applications to use to provide a programming interface to their controllers. c) East / Westbound interface, considered as a communication interface, is not backed by a recognized standard yet. This is primarily intended to allow inter-controller communication to synchronize the situation for high availability.

Forwarding elements (usually switches) is required to verify a southbound API to be useful in SDN architecture. OF switches come in two types: Software-based (eg Open vSwitch) and hardware-based implementations. Software switches are generally well designed and contain all the features. However, even the latest implementations suffer from being slow. Hardware-based OF switches are usually implemented as ASICs. Although they offer line speed forwarding for a large number of ports, unlike software implementations, they lack flexibility and feature completeness.

The OF-enabled switch can be divided into three main elements [42]. These elements; data path, control path, and OF protocol: a) The data path contains one or more group tables flow tables that search and forward packets. A flow table consists of flow entries associated with actions that tell the switch how to handle the flow. Flow tables are often created by the controller and enable the controller to explain

alternative methods of transferring flows. b) A control path is a channel that connects the switch to the controller in programming terms. The OF protocol is used to substitute commands and packets across this channel. c) The OF protocol is responsible for interconnecting switches and controllers. It may include information about messages exchanged, packets sent and received, statistics collecting, and actions to be executed in certain flows.

A flow table entry consisting of several fields in an OF-enabled switch can be organized as follows:

- a. Matching Fields are used to identify network packets based on their 15-tuple packet header, ingress port, and optional packet metadata. In Figure 2, packet header fields arranged in accordance with OSI L1-4 layers are shown.
- b. The priority of flow entry gives precedence to the matching order of the flow input.
- c. The action set shows the specific actions to be executed on the packets when the title matches.
- d. Counters are used to keep track of traffic statistics. (The total quantity of bytes and packets in each flow, as well as the time at which the final packet matches the flow).
- e. Timeouts define the maximum amount of time or idle time before the switch overrides the flow.

OF messages can be grouped into three main categories [41]. There are three types of connections: controller-to-switch, asynchronous, and symmetric. Controller-to-switch messages are those initiated by the controller and used to monitor the state of the switches. A switch can initiate asynchronous messages to notify the controller of network events and to modify the switch's state. Finally, symmetric messages are generated automatically by the switch or controller. As soon as an ingress packet arrives at the OF switch, pipeline processing does a scan of the flow tables. The entry into the flow table is determined by matching fields and priority. If the values in the packet correspond to the values in the entry's fields, the packet corresponds to the incoming flow table entry. Any (wildcard field or no field) value in a flow table input field matches all possible values in the header. Only the most critical flow entry should be chosen. If several flow inputs match with the same priority, the chosen flow input is clearly indefinite. To address such a situation, the OF specification offers an optional mechanism that allows to validate whether the new flow input matches an present input. In this way, a packet can be precisely matched to a flow with wildcard fields (macroflow), matched to a flow (microflow), or not matched to any flow. If the match is located, some actions defined in the match flow table entry are performed. If there is no match, the switch passes the packet (or only the header) to the controller for decision. After checking the related policy in the management plane, the controller responds to the switch to add new entries to the switch's flow table. The switch uses the last input to control both the queued packet and subsequent packets in the same flow.

The controller stands at the heart of SDN networks, connecting applications and network devices. The SDN controller is responsible for managing all network flows by loading flow entries into switch devices. There are two distinct forms of flow configuration: proactive and reactive. Proactive settings preload flow rules into flow tables. Thus, the flow configuration procedure is completed before the first packet of a flow reaches the OF switch. The primary advantage of proactive setup is that it reduces the frequency with

which the controller is contacted, resulting in a minor installation delay. However, it has the potential to overload switch flow tables. In the reactive setup mode, the controller adds a flow rule to the flow table only when there is no input, which occurs when the first packet of a flow arrives at the OF switch. As a result, communication between the controller and the switch is initiated by a single packet. After a specified period of inactivity, these flow entries are overridden and erased from the table. To respond against the flow setup request, the controller first evaluates the flow to the application's policies and then determines the necessary steps to execute. Following that, it determines a route for this flow and loads new flow entries, including launching requests to each switch along that path.

Transferring information between switches and controllers provides an overview of switch traffic. There are two ways for the switch to provide statistics to the controller. There are two types of flow monitoring: pull-based and push-based. The controller accumulates counters for numerous flows that fit a specified flow specification in the pull-based approach. This technique can optionally generate a report that includes all flows that match a wildcard specification. While this minimizes switch-to-controller traffic, it makes the controller ineffective at learning about the actions of other flows. The pull-based strategy necessitates an improvement in the latency between controller requests, as this can impair the scalability and reliability functions based on statistics collecting. In the push-based approach, statistics are delivered to the controller of each switch to alert it of certain occurrences, such as the creation of a new flow, a timeout, or the deletion of a table entry due to inactivity. Before the input timeout, this procedure does not notify the controller about the flow's behavior (which indicates that it is unsuitable for scheduling).

3.2. Anomaly Detection

3.2.1. Replicator Neural Network based anomaly detection

RNNs are neural networks and are specific examples of autoencoders [43] originally proposed as a compression technique [44]. The first study to suggest its use as an anomaly detection technique is recommended by Hawkins et al. [45]. Typically, input vectors in multilayer neural networks are mapped to the target output vectors. However, RNN also uses input vectors for output vectors. In other words, the input values in the output is reproduced by RNN. The RNN's weights are chosen in such a way that the mean squared error is as small as possible. As a result, while standard models are more probable to be successfully replicated by the trained RNN, models characterizing outliers are less accurately represented and have a greater error. Data exclusion is quantified using reconstruction error.

Cordero et al. propose an approach that uses RNN to identify anomalies in network flows [46]. In this method, an RNN [45] is used primarily to create a model that represents the normal network flow. While it has been demonstrated that the original RNN may be lowered to three layers [47], using the original five layers with the dropout regularization technique [48] produces superior results and avoids overfitting.

Each layer in an RNN is completely connected to every other layer. The activation function of layers 2 and 4 is nonlinear hyperbolic tangent. The output layer's activation function is linear or identical. The sole

distinction between the original RNN and the one used in [46] is in the middle layer's activation function (Layer 3). The original RNN makes use of a stepwise activation function that, in theory, aims to reduce the dimensionality of input data by clustering data samples [45]. While the stepwise activation function possesses intriguing theoretical properties, backpropagation approaches based on gradient reduction do not work adequately with it [46]. Because the gradient components of progressive functions are nearly zero, the learning process stalls. Instead of this activation function, it employs the sigmoid activation function, which has been shown to be effective as an intermediate activation function for RNNs [49].

The features extracted from different network flows are used to build RNN models. Depending on the tools used, many different features can be extracted from the network for training. The number of selected features is proportional to the number of input neurons. At each training stage, the RNN is fed the extracted flow features as an input. A validation set is used to ascertain the degree to which the learning process is capable of generalization. After training, the RNN can be used as a normal model for the purpose of calculating anomaly scores (AS). ASs that exceed a predetermined threshold are considered abnormal.

Let $X = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_N\}$ represent the set of all N training samples where $\mathbf{x} = \{x^1, x^2, \dots, x^D\}$ is a flow with D features and the function $f(\mathbf{x}) = \hat{\mathbf{x}} + \vec{\epsilon}$ correspond to the output of an RNN. The reconstruction of \mathbf{x} is represented with the vector $\widehat{\mathbf{x}}$ and the vector $\overrightarrow{\epsilon} = \{\epsilon^1, \epsilon^2, \dots, \epsilon^D\}$ is the error elements of the reconstruction. The weights of the neural network are updated employing backpropagation with particular gradient descent techniques such as Stochastic Gradient Descent (SGD). In the learning process, the loss function being minimized is formulated in Eq 1.

$$\mathbf{L} = \frac{1}{N} \sum_{i=1}^N \left(\left\| \mathbf{x}_i - \widehat{\mathbf{x}}_i + \overrightarrow{\epsilon}_i \right\|^2 \right) \quad (1)$$

The network aims to achieve a combination of weights such that $\widehat{\mathbf{x}} \approx \mathbf{x}$ and $\epsilon \approx 0$ since the purpose of backpropagation with gradient descent is to minimize L . The noise is added throughout the network by randomly detaching units in each learning iteration with the dropout method [48] to evade learning the trivial identity solution $f(\mathbf{x}) = \mathbf{x}$. The residual value $\overrightarrow{\epsilon} = \mathbf{x} - \widehat{\mathbf{x}}$ is employed to calculate the AS, which determines how anomalous a set of features is. The AS of the set of flow features \mathbf{x} is defined in Eq. 2.

$$AS(\mathbf{x}) = \frac{1}{D} \sum_{i=1}^D \left(\left\| x^i - \widehat{x}^i \right\|^2 \right) = \frac{1}{D} \sum_{i=1}^D \left(\left\| \epsilon^i \right\|^2 \right) \quad (2)$$

To determine whether the network flow \mathbf{x} is an anomaly or not, a threshold is selected to decide if the AS is too high for a flow to be counted as normal. The threshold is assigned to the highest reconstruction error E found during training after the elimination of the outliers.

3.2.2. LSTM based encoder-decoder for anomaly detection

LSTM networks [50] are recurrent models used for a variety of learning tasks such as handwriting recognition, speech recognition, and emotion analysis. To map an input sequence to a vector representation of constant dimensionality, an LSTM-based encoder is used. The decoder is another LSTM network that generates the desired sequence using this vector representation.

Malhotra et al. [51] suggest an LSTM-based Encoder-Decoder (EncDecAD) scheme for time series anomaly detection. In this architecture, the encoder generates a vector representation of the input time series, which the decoder uses to reproduce it. The EncDecAD is trained to recreate samples of "normal" time series using the input time series as the output. Following that, the reconstruction error is used to determine the probability of an anomaly occurring at that location. It is demonstrated that using an encoder-decoder model trained on solely normal sequences, anomalies in multivariate time series may be detected. According to this theory, the encoder-decoder have only seen and understood normal examples of the training data during the training phase. Given an abnormal sequence, the trained model fails to reproduce it well by resulting in higher reconstruction errors in contrast with normal sequence reconstruction errors.

The definition of the EncDecAD approach is mathematically expressed as follows. Given a time series $X = \left\{ \left\{ \text{x}^{\left(1\right)} \right\}, \left\{ \text{x}^{\left(2\right)} \right\}, \dots, \left\{ \text{x}^{\left(L\right)} \right\} \right\}$ of length L , where each point $\mathbf{x}^{\left(i\right)} \in \mathbb{R}^m$ is an m -dimensional vector of readings for m variables at a time t_i . The case is explored where many such time series are available or can be acquired by selecting a window of length L over a longer time series. To recreate the normal time-series, the EncDecAD model is trained. Following that, the reconstruction errors are used to determine the likelihood of a point in a test time series being anomalous in order to produce an anomaly score $a^{\left(i\right)}$ for each point $\mathbf{x}^{\left(i\right)}$. A greater score for anomaly indicates that the point is more likely to be abnormal.

To reconstruct examples of normal time-series, an LSTM encoder-decoder is trained. The LSTM encoder approximates the input time series with a fixed-length vector representation. Using the current hidden state and the value calculated by the LSTM decoder at the previous time-step, this representation is used to reconstruct the time-series.

The input $\mathbf{x}^{\left(i\right)}$ is used to achieve the state $\mathbf{h}_{D}^{\left(i-1\right)}$ and thenceforth $\text{x}^{\left(\prime\right)\left(i-1\right)}$ corresponding to target $\mathbf{x}^{\left(i-1\right)}$ is predicted by the decoder in the training phase. The decoder uses the predicted value $\mathbf{x}^{\left(\prime\right)\left(i\right)}$ as input, and then predicts $\mathbf{x}^{\left(\prime\right)\left(i-1\right)}$ in the inference phase. Given a set of normal training

sequences as $\{s_{N}\}$, the objective of the model training is to minimize the function $\sum_{X \in \{s_{N}\}} \sum_{i=1}^L \{ \|\text{text}(x)^{\left(i\right)} - \text{text}(x)^{\left(\prime\right)}\left(i\right)\|^2 \}$. To achieve the encoder's hidden state $\{\mathbf{h}\}_{E}^{\left(i\right)}$ at the time $\{t\}_{i}$, the value $\{\mathbf{x}\}^{\left(i\right)}$ at time $\{t\}_{i}$ and the encoder's hidden state $\{\mathbf{h}\}_{E}^{\left(i-1\right)}$ at the time $\{t\}_{i-1}$ are used. The prediction $\{\mathbf{x}\}^{\left(\prime\right)}\left(i\right)$ and $\{\mathbf{h}\}_{D}^{\left(i\right)}$ is used to achieve the next hidden state $\{\mathbf{h}\}_{D}^{\left(i-1\right)}$ by the decoder.

Normal time series are subdivided into four groups as $\{s_{N}\}, \{v_{N1}\}, \{v_{N2}\}$ and $\{t_{N}\}$. Additionally, the anomalous time series are divided into two groups as $\{v_{A}\}$ and $\{t_{A}\}$. The LSTM encoder-decoder reconstruction model is developed using the set of sequences $\{s_{N}\}$. When the encoder-decoder model is being trained, the set $\{v_{N1}\}$ is used for early stopping. The formula of $\{\mathbf{e}\}^{\left(i\right)} = \text{mid} \{\mathbf{x}\}^{\left(i\right)} - \text{mid} \{\mathbf{x}\}^{\left(\prime\right)}\left(i\right) \text{mid}$ is used to calculate the reconstruction error vector for $\{t\}_{i}$. The parameters μ and $\{\Sigma\}$ of a normal distribution $\text{mathcal}\{N\}(\mu, \{\Sigma\})$ are estimated by using the error vectors for the points in the sequences in the set $\{v_{N1}\}$ with maximum likelihood estimation. After that, the anomaly score is calculated by

$$a^{(i)} = (\mathbf{e}^{(i)} - \mu)^T \Sigma^{-1} (\mathbf{e}^{(i)} - \mu)$$

for any point $\{\mathbf{x}\}^{\left(i\right)}$. In a supervised approach, if $\{a\}^{\left(i\right)}$ is greater than threshold τ , a point in a sequence can be expected to be "anomalous", otherwise "normal". If sufficient anomalous sequences are present, a threshold τ over the probability values is learned to optimize $\{F\}_{\beta} = \left(1 + \{\beta\}^2\right) \times P \times R / \left(\{\beta\}^2 P + R\right)$, where R is recall and P is precision. Here, "normal" refers to the negative class, while "anomalous" refers to the positive class. If a window contains an anomalous pattern, the entire window is marked as "anomalous." This method is particularly advantageous in a variety of practical applications where the precise location of the anomaly is unknown. On the validation sequences in $\{v_{N2}\}$ and $\{v_{A}\}$, the parameters τ and c are determined with maximum $\{F\}_{\beta}$.

3.3. Evaluation Metrics

The proposed approach should be validated using a relevant metric. The binary classification results can be classified into four categories [52]: 1) True Positive (TP): Positive instances have been classified accurately; 2) False Negative (FN): Positive instances have been classified incorrectly; 3) False Positive (FP): Negative instances have been classified incorrectly; 4) True Negative (TN): Negative instances have been classified incorrectly. Furthermore, additional metrics can be determined by starting with the prior ones [53]:

Accuracy: This metric is expressed as the proportion of correct predictions to total instances:

$$\begin{array}{c} \text{Accuracy} = \\ (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN}) \end{array}$$

True Positive Rate (TPR): This metric is equivalent to the proportion of all "correctly identified instances" to all "examples that should be identified".

$$\text{TPR} = \text{TP} / (\text{TP} + \text{FN})$$

4

False Positive Rate (FPR): This metric denotes the proportion of the "number of misclassified negative instances" to the "total number of negative instances".

$$\text{FPR} = \text{FP} / (\text{FP} + \text{TN})$$

5

Receiver Operating Characteristics (ROC): In the case of a class imbalance problem in the dataset, ROC curve [54][55] is being used as a normal criterion for testing classifiers [56]. When faced with an issue of class imbalance, the area under the receiver operating characteristic curve (AUC) metric is frequently utilized as a de facto criterion for evaluating the effectiveness of classifiers. After sorting by classification probabilities, the AUC can be used to determine how frequently a random instance of a positive class ranks higher than an instance of a negative class.

4. Anomaly-based Intrusion Detection System For Sdn

Some principles should be taken into consideration in SAnDet (SDN Anomaly Detector), which is designed to work in SDN environments and can actively use the opportunities offered by this architecture. In the design of SAnDet, the key principles given in the following were considered taking into account the potentials offered by OF in addition to a few principles determined by Giotis et al. [26]:

- a. Separating data collection, anomaly detection and prevention (mitigation) with modular design.
- b. Compatibility with OF-enabled Layer 2 and Layer 3 devices.
- c. Fast anomaly detection and prevention (mitigation) in real-time environments using separate data and control planes.
- d. Utilizing OF's capabilities for gathering statistics and mitigating attacks.

The proposed approach is based on a set of 12-tuple flow definition associated with four specific variables, usually included as a flow entry in the OF switch. These variables are; i) action rule specifying how to forward when any packet matches its associated flow entry, ii) a soft timeout variable in place of the flow being invalidated after the final packet match, iii) the quantity of packets matching that flow since the flow input processing, iv) in the event of a packet match conflict, a specific priority is delegated to each flow input, indicating which flow rule will be determined in the event of an occurrence.

SAnDet's architecture consists of three main modules as in illustrated in Figure 5 [26]:

- **Statistics Collector Module:** The collector module is in charge of collecting the data necessary for flow-based anomaly detection. This module collects flow data on a periodic basis and passes it to the Anomaly Detection module. Two distinct data collection strategies have been described in the literature. The first of these is the OF approach, which works by periodically querying the switch and accumulating the incoming responses. The second is a flow monitoring mechanism that makes use of packet sampling. Giotis et al. use sFlow, which is vendor-independent [26]:
- **Anomaly Detection Module:** At specified periodic time intervals, the collection module sends data to the Anomaly Detection module. It has been designated as a ten-second time slot. Giotis et al. [26] utilized an algorithm based on entropy. They also mentioned that this module can be utilized with any statistical anomaly detection, machine learning-based anomaly detection, or data mining-based anomaly detection technique.
- **Mitigation Module:** The anomaly prevention module attempts to mitigate identified attacks or breaches by adding (or modifying) flow entries to the OF switch's flow table in order to prohibit the targeted malicious traffic [26]. These flow entries have a higher priority than other flows in the flow table. Adding certain host-related rules to a whitelist table allows for the avoidance of blocking legal network flows that exhibit anomalous behavior that resembles malicious behavior. Additionally, malicious rules are added to a blacklist (malicious address) table.

4.1. Data collection and feature extraction

The OF approach uses the OF protocol to collect flow statistics from switches. As required by the OF protocol, the controller handles periodic flow statistics requests by aggregating them with the relevant counters for all flow entries in the OF switch [26]. The switches' flow counters are updated only when a forwarding query procedure matches an entry in the flow table. As a result, the gathering of flow statistics in a native OF environment is inextricably linked to the controller's packet forwarding mechanism [26]. In our scenario, when the forwarding logic is dictated by the anomaly detection strategy, layer 3 and 4 protocol fields are utilised. As a result, the flow table's necessary entries are reduced to a single flow, and a single flow input is formed by evaluating forward and backward direction based on the source IP, source port, destination IP, destination port, and protocol fields. The remainder of the fields in the flows contain wildcards, which allow them to match any value in the fields.

The OF approach sends a message (FlowRemoved) to the controller when a flow entry is deleted from the switch, along with this information, as well as other data such as counter values of the flow input. Gathering statistics with the OF approach can be performed when a switch responds (FlowStatsReply) to a flow statistics request (FlowStatsRequest message querying the switch for flow statistics) from the associated OF controller. By using these two messages together, data collection of flow inputs can be accomplished [57]. Every new packet that arrives initially is added to a table at the controller. Later, messages are expected from these inputs that are programmed to send a message when the flow input is deleted at a certain time. If these messages are received from all entries in the table during this period, it is assumed that all flow statistics have been obtained and these data are transferred to the detection

code. If there is no deleted message from at least one flow entry, the statistics collection message is sent to the OF switch and a response message is expected. The algorithm of this approach can be given as in Figure 6. As a result, the switch reacts to huge portions of the flow table's content. Each stack includes a subset of the flow entries, as well as packet counters for each flow. The anomaly detection algorithm, on the other hand, only includes counter contents from the counters as a consequence of the query, such as the number of packets matching each flow entry within a certain timeframe, whereas flow table records' packet counters contain the total number of packets after each rule was instantiated. Therefore, to find the number of packets corresponding to the specified time window, a record of the status of the flow chart for previous time windows must be kept and compared with valid data for each flow input. Due to the absence of sampling in the OF data collecting process, it is able to collect and analyze in great detail all network traffic streaming through the switch [26]. As a result, this approach has proven to be effective in monitoring networks of low to medium traffic volumes [38][17]. The derived features in Table 1 are also calculated for the flow, which is the corresponding pair of a flow, and added separately to the data set. In Table 1, P , B , n and D corresponds to the number of packets, the number of bytes, the number of flows and active duration, respectively.

Table 1
Flow features

	Feature Name	Description	Flow direction	
			Forward	Backward
Flow Id	Source IP			
	Destination IP			
	Protocol type	TCP, UDP ve ICMP		
	Type of Service			
	Source Port			
	Destination port			
Basic features	Byte count		X	X
	Packet count		X	X
	Active duration in seconds		X	X
	Packet rate in seconds		X	X
	Byte rate in seconds		X	X
Derived Features ¹ [38], [58]	Average number of packet per flow (APf)	$APf = \frac{1}{n} \sum_{i=1}^n \{P\}_i$	X	X
	Average number of bytes per flow (ABf)	$ABf = \frac{1}{n} \sum_{i=1}^n \{B\}_i$	X	X
	Average active duration per flow (ADf)	$ADf = \frac{1}{n} \sum_{i=1}^n \{D\}_i$	X	X
	The growth of single flows (GSf)	$GSf = \frac{\text{Num_Flows} - (2 \times \text{Num_Pair_Flows})}{\text{interval}}$		
	The growth of different ports (GDP)	$GDP = \frac{\text{Num_Ports}}{\text{interval}}$		
	The number of flows from same source IP			

4.2. Attack detection and prevention

A method should be developed that takes the features extracted from the flows as input and detects whether there is an attack on the network. The deep learning-based methods, which are popular recently and have contributed significantly to the solution of many problems, have been preferred as the detection method, and their performance has been examined.

In SAnDet architecture, the focus is to employ anomaly-based techniques which are capable for detecting both known and zero-day attacks. In deep learning methods, RNN and EncDecAD were able to successfully detect anomalies in data sets according to studies in the literature. In addition to the flow statistics collected from the network, the features derived from them are given as input to these two methods and the detection performances are calculated according to certain evaluation criteria. Although AUC is recommended to be used as a criteria in the evaluation of anomaly-based methods, it has been stated that accuracy criteria should also be taken into account in data sets with imbalanced class distribution [56].

5. Performance Evaluation

In this section, performance evaluation is made as the attack detection and prevention mechanism of OF protocol. Also, the benefits of OF are investigated to prevent identified malicious traffic, by using SDN controller facilities.

Floodlight [59] is an open-source OF controller with a modular architecture. Through the API provided by the Floodlight controller, periodic and aperiodic data collection are performed. After that, the derivation of new features from the basic features of the flow inputs collected, and implementation of three different components responsible for flow entry modification tasks were performed. The Statistics Collector module, which collects statistics and generates new features, has been implemented. An anomaly detector module has been implemented, where models developed from both RNN and EncDecAD methods can be applied and together with which different detection algorithms can be easily integrated. The results of this action are then sent to the Anomaly Prevention module to provide intrusion countermeasures. This enables the user to create or employ their preferred anomaly detection technique as long as it can transmit the required information to the Anomaly Prevention module. Performance assessment trials were conducted with some of the network traffic in the ISCX2012 data set.

5.1. Testbed environment and traffic generation

SAnDet system were implemented as Floodlight controller modules for anomaly detection and prevention functions. OF-enabled switches are required to run experiments. Open vSwitch [60], a software switch capable of handling the necessary traffic loads, is used for this purpose. The experimental environment of the study was provided by Mininet [61] emulation software, which is an open-source tool that is frequently used in the literature. This emulation environment supports OpenFlow vSwitch [60], which is superior to hardware switches in its features and is designed to develop SDN-supported network prototypes. The emulation environment was hosted on a virtual server with 16 GB of RAM, a quad-core 3

GHz processor. Besides, Floodlight [59] is used as controller software because of the open source functionality that it provides. Figure 8 shows the experimental setup together with Floodlight modules used to evaluate the two approaches mentioned above. The controller software is run in a virtual machine on the server. Network traffic captured for performance evaluation is injected into a single switch (in this case software-based Open vSwitch). It should be made clear that the proposed mechanism can be applied to multiple OF enabled switches and to more general network topologies with the corresponding prevention rules.

Some parameters need to be set in OF based statistics collection. In particular, a specific value has to be set for the idle timeout for each flow entry. This is because the collector module requests any flow entry to expire to gather the relevant flow statistics. Therefore, the time window is specified by assigning the statistical collection period to 10 seconds, and the idle timeout to 3 seconds.

Table 2
The number of all flows collected from traffic generated

Day	Normal	Attack type	
		DoS	Portscan
11 June Friday	3452552	0	0
12 June Saturday	557885	210569	252874
16 June Wednesday	2213469	0	0
Total	5820763	463443	

Normal or benign traffic of the ISCX2012 data set is used to evaluate the performance of the attack detection and prevention mechanism. To be more precise, traffic captured on "Friday 11 June" and "Wednesday 16 June" is used as normal network traffic. Besides, benign traffic, which includes the "Saturday" traffic track, is played normally, and specified DoS and port scanning attacks are performed at certain time intervals.

The ISCX2012 dataset [62] was produced in 2012, catching traffic in the network emulation environment for more than a week. The authors describe attack scenarios while α profiles, a dynamic approach to creating an attack detection dataset with normal and malicious network behavior, whereas β profiles describe typical user behavior such as email writing or web browsing. These profiles are used to create a different data set that is packet-based and flow-based in both directions. The dynamic strategy enables the ongoing generation of fresh data sets. Although this data set includes a wide variety of attacks such as SSH brute force, DoS, or DDoS, the traffic traces containing these attacks were not used in this study because it disrupts the attack characteristics of the tcpreplay tool.

Table 3
Number of samples produced from flows collected over time

Day	Normal	Attack type	
		DoS	Portscan
11 June Friday	8640	0	0
12 June Saturday	8275	55	35
16 June Wednesday	8644	0	0
Total	25559	90	

These traffic track files were used in experiments to assess the accuracy and detection abilities of the OF approach. Replaying captured packet track data and injecting produced traffic onto a particular Ethernet port is accomplished using the tcpreplay [63] program, which is capable of replaying captured traffic at the rate at which it is captured. To perform the attack, hping3 [64], a programmable software tool, was used to allow sending packet strings with random protocol field values. This enables packets to be sent to a predefined destination IP address and port to perform a DoS attack. Finally, through the hping3 tool, the attack is performed by randomly selecting the source and destination ports with a specific source and destination IP address for the portscan scenario. The number of all flows collected from the generated traffic is shown in Table 2, and the number of samples containing features derived from the flows collected in a certain time interval (10 seconds) is shown in Table 3.

5.2. Anomaly detection and mitigation

The restricted clustering SSL strategy has been chosen as learning strategy because it requires less information, time and effort, and unlabeled data is easier to obtain for an intrusion detection system than labeled data [65]. Furthermore, this strategy is better suited to the detection methods' unsupervised training nature.

As can be seen in Figure 8, the data set is divided into two separate parts as training and test data set. To create a normal profile of the network traffic by applying SSL strategy, only the labeled data set containing normal flow characteristics is used in the training phase. The testing process makes use of an unlabeled data set containing both normal and attack flow characteristics. It's worth noting that in this analysis, the labels in the test data set are taken into consideration when calculating assessment metrics.

Since the techniques used in this analysis are parameterized, the models' performance should be calculated using the right parameters. Because abnormal data is not included in the training process, the cross-validation operation cannot be accomplished in the hyperparameter optimization [66]. Thus, the adjustment of the hyperparameters is done mostly taking into account the suggestions mentioned by Patterson and Gibson [67]. Following that, the RNN and EncDecAD hyperparameters are often set by trial and error.

Table 4
The evaluation results of RNN and EncDecAD

Method	Window Size	Bottleneck layer dimension	Accuracy	AUC
EncDecAD	6	32	0.993	0.933
EncDecAD	4	48	0.993	0.932
EncDecAD	10	8	0.992	0.931
EncDecAD	7	32	0.992	0.924
EncDecAD	8	32	0.993	0.920
EncDecAD	5	96	0.99	0.911
EncDecAD	9	8	0.992	0.911
EncDecAD	3	48	0.992	0.886
RNN	5	32	0.98	0.87
RNN	10	64	0.99	0.864
RNN	6	32	0.987	0.820
RNN	3	8	0.992	0.818
RNN	8	64	0.99	0.808
RNN	9	48	0.991	0.805
RNN	4	32	0.978	0.792
RNN	7	64	0.991	0.766

The experiments were carried out using a basic deep autoencoder architecture. The architectural diagram of the RNN and the architectural diagram of EncDecAD are shown in Figure 3 and Figure 4, respectively (when the window size is 3). Models were trained and developed using different dimensions such as 8, 16, 32, 48, 64, 80, 96 in the bottleneck layer of RNN and hidden layers of EncDecAD. The dimensions of the layers in the best performing RNN and EncDecAD models were established by trial and error while maintaining the layer count constant, that is, conforming to the given architectures. The following parameters are utilized in the RNN and EncDecAD neural network configurations: In training trials, learning rates (learning rates) such as [0.1, 0.01, 0.001] are employed. The optimal value for the learning rate is 0.001. Both neural networks were trained using the backpropagation technique and the conjugate gradient optimization approach, which is suggested for big data sets and outputs with real values [67]. The Adam updater [68] was chosen to avoid the local minimum and seek more efficient optimization alternatives. The following additional parameters are utilized in the EncDecAD configuration. In hidden layers, hyperbolic tangent function is utilized as the activation function. In the hyperparameters used to configure the RNN, which is commonly used and recommended in [46], the sigmoid activation function

was used in addition to the output layer, and the mean square error loss function, and the soft-max activation function were used in the output layer. Both RNN and EncDecAD models were implemented with the library [69] based on Pytorch [70] and trained for 50 epochs with 16 batch sizes. Reconstruction error was used as an anomaly score in both RNN and EncDecAD methods.

Initially, the normalization process was performed on the traffic traces by using the feature scaling method [71] to bring all values to the range [0,1]. To assess the algorithms' performance, distinct training and test data sets were used. The models were constructed by training the neural network exclusively on "Friday" and "Wednesday" normal flow data. This is because models are developed in an unsupervised manner, and the label for the final column in the dataset corresponds to the attack class that was not used during training. The testing procedure included both normal and attack traffic on alternate days. All attacks classified as "anomalies" during the testing procedure are those that are not "normal" or "benign." Metrics were computed for the performance evaluation of an attack class using only normal flow records and attack class-specific flow data, ignoring any other attack classes.

Performance evaluation of the methods is carried out using AUC and accuracy metrics. An assessment based on the AUC criterion is performed as it is the de facto standard for imbalanced anomaly detection and easy interpretation [72]. The AUC results of the methods are given in Table 4. When the results are examined, it is seen that the EncDecAD method gives better results than RNN in different time windows and bottleneck layers as can be seen in Figure 10 and Figure 11. It means that EncDecAD learns the relationship from the sequences better than RNN. The results shows that EncDecAD also gives better results compared to studies listed in Table 5 in terms of accuracy and AUC.

Table 5
The comparison of SAnDet with previous studies

Reference	Method	Number of features	Attack types	Controller	Dataset	Result
Niyaz et al. [31]	Stacked Autoencoder	TCP, UDP and ICMP flow features	DDoS	POX	Traffic dataset collected from different environmets	Accuracy % 95.65
Tang et al. [32]	Deep Neural Network	6 features	DoS, U2R, R2L, Probes	OF controller	KDD	Accuracy % 75.75
Tang et al. [73]	Recurrent Neural Network	6 features	DoS	POX	NSL-KDD	Accuracy %89
Braga et al. [38]	SOM	6 features	DDoS	NOX	KDD99	Accuracy % 98.57
Kokila et al. [22]	SVM	Flow statistics	DDoS	SDN controller	DARPA	% 95.11
Abubakar et al. [74]	Neural network	7 features	DoS, U2R, R2L and scan	OpenDaylight	NSLKDD	Accuracy %97
Wang et al. [75]	SVM	Feature reduction	DDoS	Ryu	KDD99	Accuracy % 99
The proposed approach (SAnDet)	EncDecAD (LSTM)	21 features	DoS and Portscan	Floodlight	ISCX2012 as normal traffic and attack with hping3	Accuracy % 99.3 AUC % 93.3

6. Conclusion

In this study, an intrusion detection and prevention architecture called SAnDet is proposed and implemented as a controller application. To put it more clearly, a statistics collection module using the OF protocol, an anomaly-based attack detection module that uses the EncDecAD method to detect attacks, and an intrusion prevention module that can prevent attacks via the OF protocol when an attack is detected is implemented as an SDN controller application. By employing a semi-supervised learning strategy, the attack detection capabilities of the RNN and EncDecAD algorithms for anomaly detection

were researched. The models were created using solely normal flow-based data. Besides, the tests of the models were carried out using a time series data set containing both normal and abnormal. Experimental results were obtained using ROC curves, AUC, and accuracy metrics. According to the results, it has been observed that EncDecAD has a higher rate of detecting attacks compared to other methods recommended in the literature.

As a future study, it is important to investigate how the method will perform by increasing the types of attacks in the data set. In addition, how the change in the time interval for statistics collection will affect system performance in terms of both controller load and attack detection rate is another future work.

Declarations

Declaration of Interest Statement

The authors declare that they have no conflict of interest.

References

1. Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network Anomaly Detection: Methods, Systems and Tools., " Commun Surv Tutorials, IEEE 16(1):303–336. doi: 10.1109/SURV.2013.052213.00046
2. McKeown N (2011) "How SDN will shape networking," *ONS2011*. https://www.youtube.com/watch?v=c9-K5O_qYgA (accessed Jan. 20, 2018)
3. Kim H, Feamster N (2013) Improving network management with software defined networking., " IEEE Commun Mag 51(2):114–119. doi: 10.1109/MCOM.2013.6461195
4. Scott-Hayward S, O'Callaghan G, Sezer S (2013) "SDN Security: A Survey," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, pp. 1–7, doi: 10.1109/SDN4FNS.2013.6702553
5. Scott-Hayward S, Natarajan S, Sezer S (2015) "A Survey of Security in Software Defined Networks," *Commun. Surv. Tutorials, IEEE*, vol. PP, no. 99, p. 1, doi: 10.1109/COMST.2015.2453114
6. Dotcenko S, Vladyko A, Letenko I (2014) "A fuzzy logic-based information security management for software-defined networks," in *Advanced Communication Technology (ICACT), 16th International Conference on*, 2014, pp. 167–171, doi: 10.1109/ICACT.2014.6778942
7. Jafarian T, Masdari M, Ghaffari A, Majidzadeh K (Sep. 2020) A survey and classification of the security anomaly detection mechanisms in software defined networks., " Cluster Comput 1–19. doi: 10.1007/s10586-020-03184-1
8. Hande Y, Muddana A (2020) A survey on intrusion detection system for software defined networks (SDN)., " Int J Bus Data Commun Netw 16(1):28–47. doi: 10.4018/IJBDCN.2020010103
9. Zhang Y (2013) "An adaptive flow counting method for anomaly detection in SDN," *Proceedings of the ninth ACM conference on Emerging networking experiments and technologies*. ACM, Santa Barbara, California, USA, pp. 25–30, doi: 10.1145/2535372.2535411

10. Ha T et al (2016) "Suspicious traffic sampling for intrusion detection in software-defined networks," *Comput. Networks*, vol. 109, Part, pp. 172–182, doi: <http://dx.doi.org/10.1016/j.comnet.2016.05.019>
11. Granby BR, Askwith B, Marnerides AK (2015) "SDN-PANDA: Software-Defined Network Platform for ANomaly Detection Applications," in *IEEE 23rd International Conference on Network Protocols (ICNP)*, 2015, pp. 463–466, doi: 10.1109/ICNP.2015.58
12. Hommes S, State R, Engel T (2014) Implications and detection of DoS attacks in OpenFlow-based networks., " 2014 IEEE Glob Commun Conf GLOBECOM 2014:537–543. doi: 10.1109/GLOCOM.2014.7036863
13. Carvalho LF, Fernandes G, Rodrigues JJPC, Mendes LS, Proenca ML (2017) A novel anomaly detection system to assist network management in SDN environment., " *IEEE Int Conf Commun.* doi: 10.1109/ICC.2017.7997214
14. He D, Chan S, Ni X, Guizani M (2017) "Software-Defined-Networking-Enabled Traffic Anomaly Detection and Mitigation," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1890–1898, Dec. doi: 10.1109/JIOT.2017.2694702
15. Carvalho LF, Abrão T, de Mendes L, Proença ML (Aug. 2018) An ecosystem for anomaly detection and mitigation in software-defined networking., " *Expert Syst Appl* 104:121–133. doi: 10.1016/J.ESWA.2018.03.027
16. Peng H, Sun Z, Zhao X, Tan S, Sun Z (2018) A Detection Method for Anomaly Flow in Software Defined Network., " *IEEE Access.* doi: 10.1109/ACCESS.2018.2839684
17. Mehdi SA, Khalid J, Khayam SA (2011) "Revisiting traffic anomaly detection using software defined networking," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6961 LNCS, pp. 161–180, doi: 10.1007/978-3-642-23644-0_9
18. Schechter SE, Jung J, Berger AW (2004) Fast detection of scanning worm infections., " *Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics)* 3224:59–81. doi: 10.1007/978-3-540-30143-1_4
19. Twycross J, Williamson MM (2003) "Implementing and Testing a Virus Throttle," in *Proceedings of the 12th Conference on USENIX Security Symposium - Volume 12*, p. 20
20. Williamson MM (2002) "Throttling viruses: Restricting propagation to defeat malicious mobile code," in *Proceedings - Annual Computer Security Applications Conference, ACSAC*, vol. 2002-January, pp. 61–68, doi: 10.1109/CSAC.2002.1176279
21. Mahoney MV (2003) "Network traffic anomaly detection based on packet bytes," in *Proceedings of the 2003 ACM symposium on Applied computing - SAC '03*, p. 346, doi: 10.1145/952532.952601
22. Kokila RT, Thamarai Selvi S, Govindarajan K (2015) "DDoS detection and analysis in SDN-based environment using support vector machine classifier," in *6th International Conference on Advanced Computing, ICoAC 2014*, Aug. pp. 205–210, doi: 10.1109/ICoAC.2014.7229711
23. Sathya R, Thangarajan R (2015) "Efficient anomaly detection and mitigation in software defined networking environment," in *Electronics and Communication Systems (ICECS), 2nd International*

- Conference on*, 2015, pp. 479–484, doi: 10.1109/ECS.2015.7124952
24. Yang C (Jul. 2019) Anomaly network traffic detection algorithm based on information entropy measurement under the cloud computing environment., " *Cluster Comput* 22(4):8309–8317. doi: 10.1007/s10586-018-1755-5
 25. Wang R, Jia Z, Ju L (2015) "An entropy-based distributed DDoS detection mechanism in software-defined networking," in *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom* Dec. 2015, vol. 1, pp. 310–317, doi: 10.1109/Trustcom.2015.389
 26. Giotis K, Argyropoulos C, Androulidakis G, Kalogeras D, Maglaris V (2014) Combining Open Flow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments., " *Comput Networks* 62:122–136. doi: 10.1016/j.bjp.2013.10.014
 27. Visible N, Packard H- (2003) "Traffic Monitoring using sFlow," *Analysis*, <http://www.sflow.org/sFlowOverview.pdf>
 28. Francois J, Festor O (2014) "Anomaly traceback using software defined networking," in *IEEE International Workshop on Information Forensics and Security (WIFS)*, 2014, pp. 203–208, doi: 10.1109/WIFS.2014.7084328
 29. Deng L, Yu D (2013) "Deep learning: Methods and applications. " *Foundations and Trends in Signal Processing*, vol 7. Now Publishers Inc, pp. 197–387,, pp 3–4. doi: 10.1561/20000000039.
 30. Dey SK, Rahman MM (2018) "Flow based anomaly detection in software defined networking: A deep learning approach with feature selection method," in *4th International Conference on Electrical Engineering and Information and Communication Technology, iCEEICT* Jan. 2019, pp. 630–635, doi: 10.1109/CEEICT.2018.8628069
 31. Niyaz Q, Sun W, Javaid AY (2016) "A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)," *arXiv Prepr. arXiv1611.07400*,
 32. Tang TA, Mhamdi L, McLernon D, Zaidi SAR, Ghogho M (2016) *International Conference on Wireless Networks and Mobile Communications, WINCOM 2016: Green Communications and Networking*, Dec. 2016, pp. 258–263, doi: 10.1109/WINCOM.2016.7777224
 33. Garg S, Kumar N, Rodrigues JJPC, Rodrigues JJPC (2019) "Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective," *IEEE Trans. Multimed.*, vol. 21, no. 3, pp. 566–578, Mar. doi: 10.1109/TMM.2019.2893549
 34. Li J, Zhao Z, Li R (2018) "Machine learning-based IDS for softwaredefined 5G network," *IET Networks*, vol. 7, no. 2, pp. 53–60, Mar. doi: 10.1049/iet-net.2017.0212
 35. Da Silva AS, Wickboldt JA, Granville LZ, Schaeffer-Filho A (2016) "ATLANTIC: A framework for anomaly traffic detection, classification, and mitigation in SDN," *Proc. NOMS - 2016 IEEE/IFIP Netw. Oper. Manag. Symp.*, no. Noms, pp. 27–35, 2016, doi: 10.1109/NOMS.2016.7502793
 36. Pang C, Jiang Y, Li Q (2016) Detecting forwarding anomaly in software-defined networks., " Jul. doi: 10.1109/ICC.2016.7510990

37. Cui Y (2016) SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks., " J Netw Comput Appl 68:65–79. doi: <http://dx.doi.org/10.1016/j.jnca.2016.04.005>
38. Braga R, Mota E, Passito A (2010) "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Proceedings - Conference on Local Computer Networks, LCN*, pp. 408–415, doi: 10.1109/LCN.2010.5735752
39. "Open Networking Foundation." <https://www.opennetworking.org/>
40. ONF, Foundation ON "Software-Defined Networking: The New Norm for Networks," 2012. doi: citeulike-article-id:12475417
41. Jarraya Y, Madi T, Debbabi M (2014) "A Survey and a Layered Taxonomy of Software-Defined Networking," *Commun. Surv. Tutorials, IEEE*, vol. PP, no. 99, p. 1, doi: 10.1109/COMST.2014.2320094
42. McKeown N et al (Mar. 2008) "OpenFlow: Enabling Innovation in Campus Networks," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, doi: 10.1145/1355734.1355746
43. Deng L, Yu D (2014) Deep learning: methods and applications., " *Found trends signal Process* 7:3–4, pp. 197–387,
44. Hecht-Nielsen R (1995) "Replicator neural networks for universal optimal source coding," *Science (80-.)*, vol. 269, no. 5232, pp. 1860–1863,
45. Hawkins S, He H, Williams G, Baxter R (2002) "Outlier detection using replicator neural networks," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2454 LNCS, pp. 170–180, doi: 10.1007/3-540-46145-0_17
46. Cordero CG, Hauke S, Muhlhauser M, Fischer M (2016) *14th Annual Conference on Privacy, Security and Trust, PST 2016*, 2016, pp. 317–324, doi: 10.1109/PST.2016.7906980
47. Dau HA, Ciesielski V, Song A (2014) "Anomaly detection using replicator neural networks trained on examples of one class," in *Asia-Pacific Conference on Simulated Evolution and Learning*, pp. 311–322
48. Srivastava N, Hinton G, Krizhevsky A, Sutskever I, Salakhutdinov R (2014) Dropout: A simple way to prevent neural networks from overfitting., " *J Mach Learn Res* 15(1):1929–1958
49. Tóth L, Gosztolya G (2004) "Replicator neural networks for outlier modeling in segmental speech recognition," in *International Symposium on Neural Networks*, pp. 996–1001
50. Hochreiter S, Schmidhuber J, Memory "LongShort-Term (1997) " *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. doi: 10.1162/neco.1997.9.8.1735
51. Malhotra P, Ramakrishnan A, Anand G, Vig L, Agarwal P, Shroff G "LSTM-based Encoder-Decoder for Multi-sensor Anomaly Detection." Accessed: May 04, 2019. [Online]. Available: <https://arxiv.org/pdf/1607.00148.pdf>
52. Gu O, Fogla P, Dagon D, Lee W, Škorić B (2006) "Measuring intrusion detection capability: An information-theoretic approach," in *Proceedings of the ACM Symposium on Information, Computer and Communications Security, ASIACCS '06*, 2006, vol. 2006, pp. 90–101, doi: 10.1145/1128817.1128834

53. Xin Y (2018) Machine Learning and Deep Learning Methods for Cybersecurity., " IEEE Access 1. doi: 10.1109/ACCESS.2018.2836950
54. Spackman KA, "SIGNAL DETECTION THEORY: VALUABLE TOOLS FOR EVALUATING INDUCTIVE LEARNING (1989)," in *Proceedings of the Sixth International Workshop on Machine Learning*, Elsevier, pp. 160–163
55. Fawcett T (2004) "ROC Graphs: Notes and Practical Considerations for Researchers," *HP Labs Tech Rep. HPL-2003-4*, pp. 1–38, doi: 10.1.1.10.9777
56. He H, Ma Y (2013) Imbalanced Learning: Foundations, Algorithms, and Applications. Wiley
57. Chowdhury SR, Bari MF, Ahmed R, Boutaba R (2014) "PayLess: A low cost network monitoring framework for Software Defined Networks," in *IEEE Network Operations and Management Symposium (NOMS)*, 2014, pp. 1–9, doi: 10.1109/NOMS.2014.6838227
58. Abuadlla Y, Kvascev G, Gajin S, Jovanović Z (2014) Flow-based anomaly intrusion detection system using two neural network stages., " *Comput Sci Inf Syst* 11(2):601–622. doi: 10.2298/CSIS130415035A
59. Floodlight "Floodlight OpenFlow Controller." <http://www.projectfloodlight.org/floodlight/>
60. "Open vSwitch." <http://openvswitch.org/>
61. Team M "Mininet: An Instant Virtual Network on your Laptop (or other PC) - Mininet." <http://mininet.org/>
62. Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA (2012) Toward developing a systematic approach to generate benchmark datasets for intrusion detection., " *Comput Secur* 31(3):357–374. doi: <http://dx.doi.org/10.1016/j.cose.2011.12.012>
63. "Tcpreplay." <http://tcpreplay.synfin.net/>
64. "Hping - Active Network Security Tool (accessed Nov. 16, 2020) " <http://www.hping.org/>
65. Zavrak S, Iskefiyeli M (2020) Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder., " *IEEE Access* 8:108346–108358. doi: 10.1109/ACCESS.2020.3001350
66. Cao VL, Nicolau M, McDermott J (2019) "Learning Neural Representations for Network Anomaly Detection," *IEEE Trans. Cybern.*, vol. 49, no. 8, pp. 3074–3087, Aug. doi: 10.1109/TCYB.2018.2838668
67. Patterson J, Gibson A (2017) Deep Learning: A Practitioner's Approach. O'Reilly Media
68. Sutskever I, Martens J, Dahl G, Hinton G (2013) "On the importance of initialization and momentum in deep learning," Accessed: Jan. 30, 2019. [Online]. Available: <http://www.cs.toronto.edu/~fritz/absps/momentum.pdf>
69. "KDD-OpenSource/DeepADoTS (2021) : Repository of the paper 'A Systematic Evaluation of Deep Anomaly Detection Methods for Time Series'." <https://github.com/KDD-OpenSource/DeepADoTS> (accessed Mar. 29,
70. "PyTorch (2020) " <https://pytorch.org/>(accessed Nov.16,

71. Aksoy S, Haralick RM (2001) Feature normalization and likelihood-based similarity measures for image retrieval., " Pattern Recognit Lett 22(5):563–582
72. Krzanowski WJ, Hand DJ (2009) ROC Curves for Continuous Data. CRC Press
73. Tang TA, Mhamdi L, McLernon D, Zaidi SAR, Ghogho M (2018) "Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks," in *4th IEEE Conference on Network Softwarization and Workshops, NetSoft 2018*, Sep. 2018, pp. 462–469, doi: 10.1109/NETSOFT.2018.8460090
74. Abubakar A, Pranggono B (2017) "Machine learning based intrusion detection system for software defined networks," in *Proceedings - 2017 7th International Conference on Emerging Security Technologies, EST 2017*, pp. 138–143, doi: 10.1109/EST.2017.8090413
75. Wang P, Chao KM, Lin HC, Lin WH, Lo CC (2016) "An Efficient Flow Control Approach for SDN-Based Network Threat Detection and Migration Using Support Vector Machine," in *IEEE 13th International Conference on e-Business Engineering (ICEBE)*, 2016, pp. 56–63, doi: 10.1109/ICEBE.2016.020

Figures

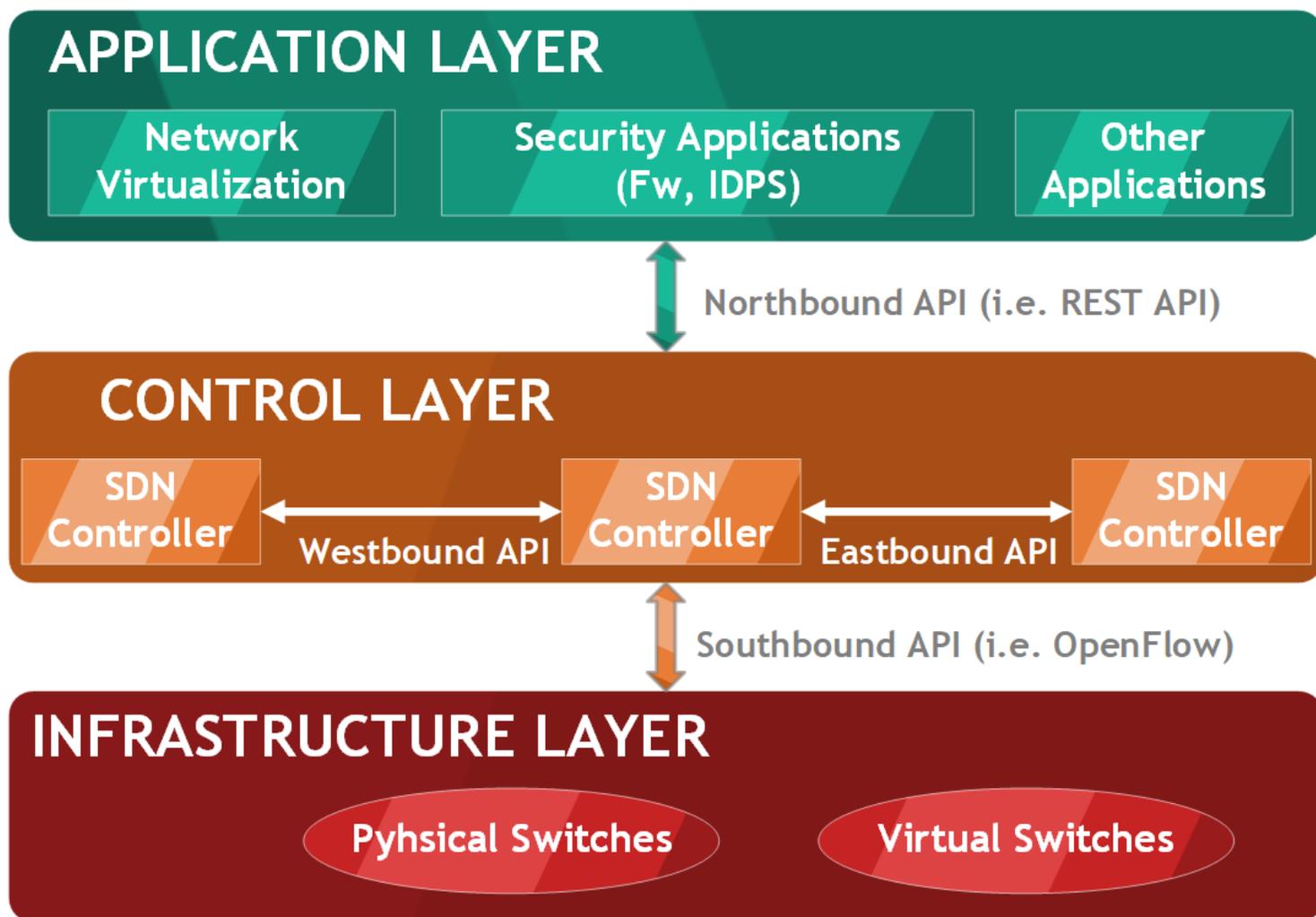


Figure 1

Figure 2

Flow Identification in OF [41]

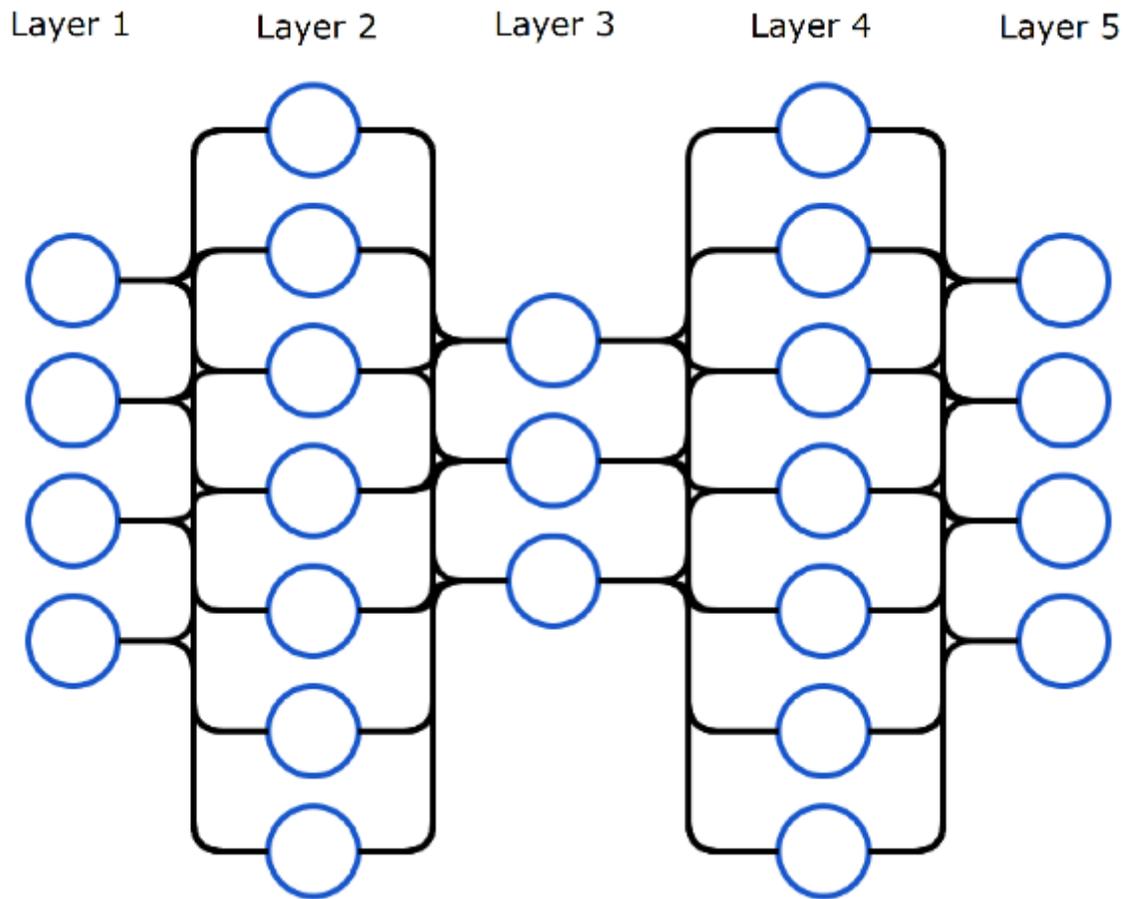


Figure 3

An example diagram of RNN [46]

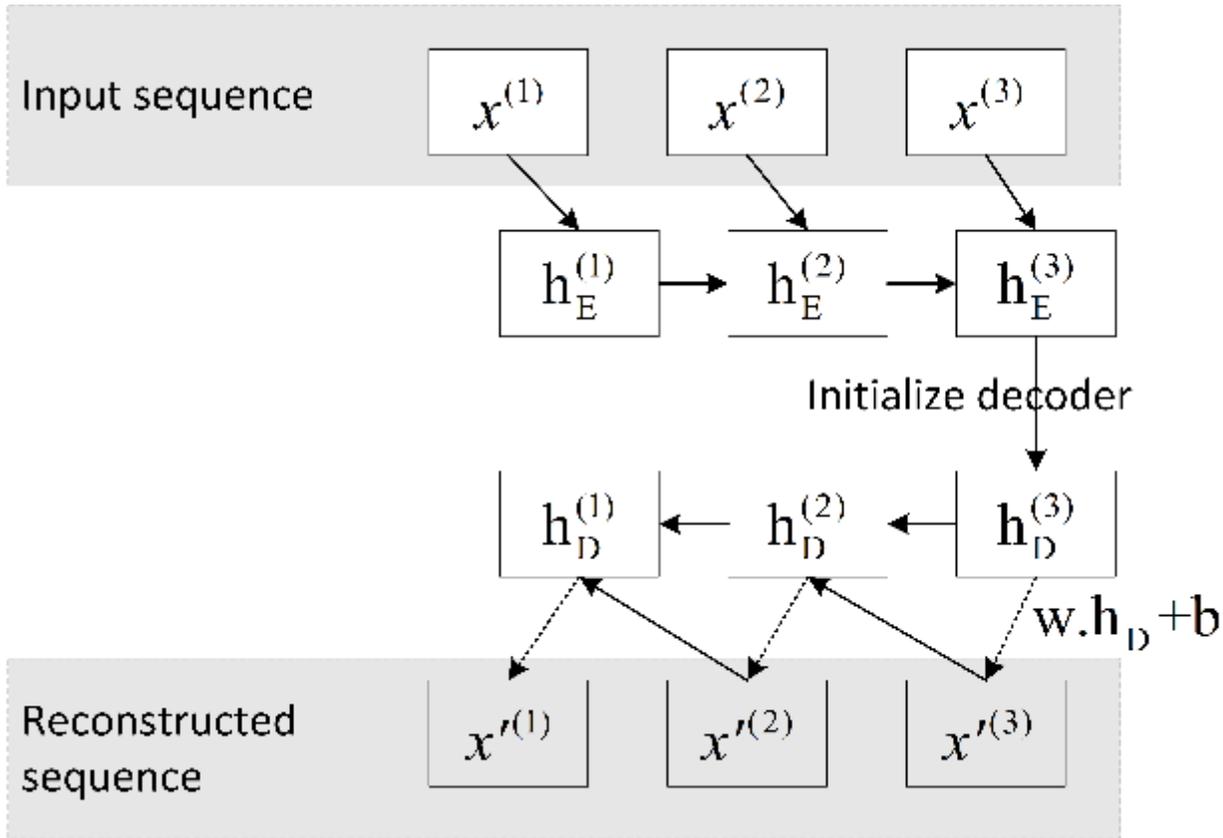


Figure 4

LSTM Encoder-Decoder inference steps



Figure 5

SAnDet architecture

```
active_flows # the active flows in specific time interval
t # time interval to query flow statistics
F # flow statistics table

if e is initialization event then
  active_flows <-  $\emptyset$ , U <-  $\emptyset$ 
end if

if e is PacketIn event then
  Statistics collection
```

Figure 6

The flow statistics collection algorithm

```

black_list # blacklist flows
detected_flows # identified flows

for all flows f in detected_flows do
  if black_list.contains(f) then
    do nothing # already in blacklist
  else
    # write drop rule to the switch for f
    create match m object
    m.srcIp = f.srcIp

```

Figure 7

Anomaly mitigation algorithm

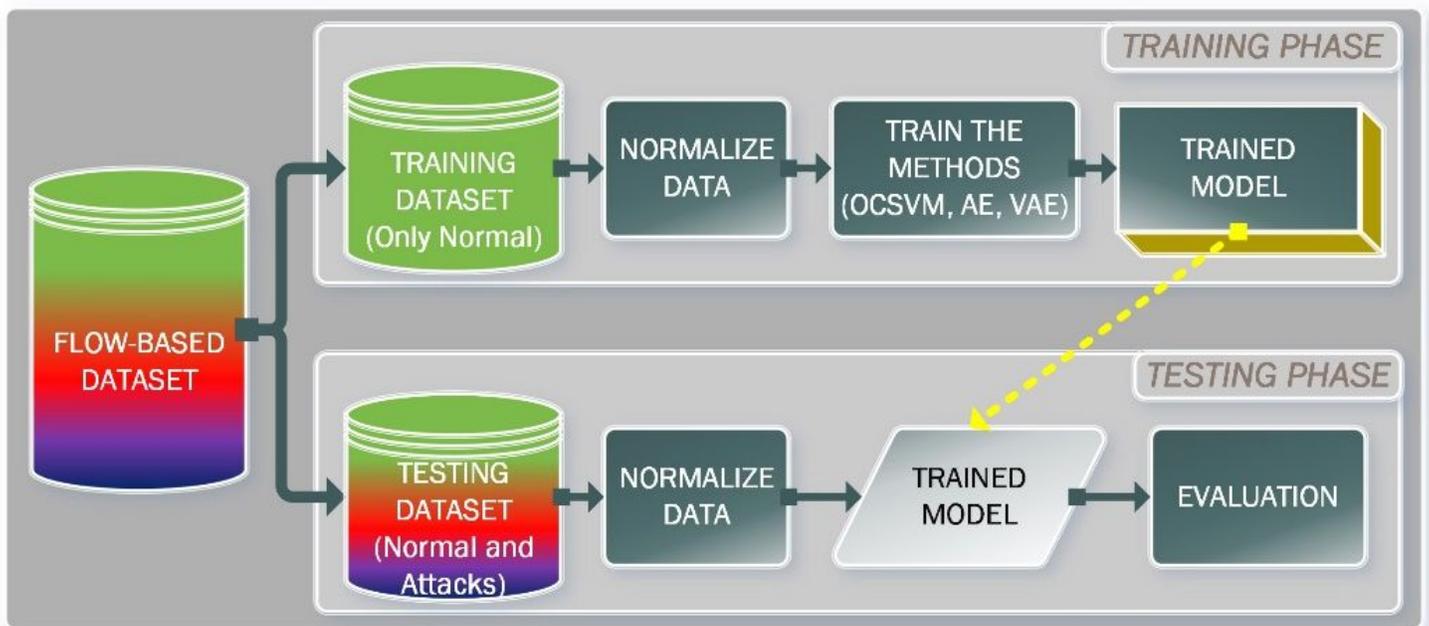


Figure 8

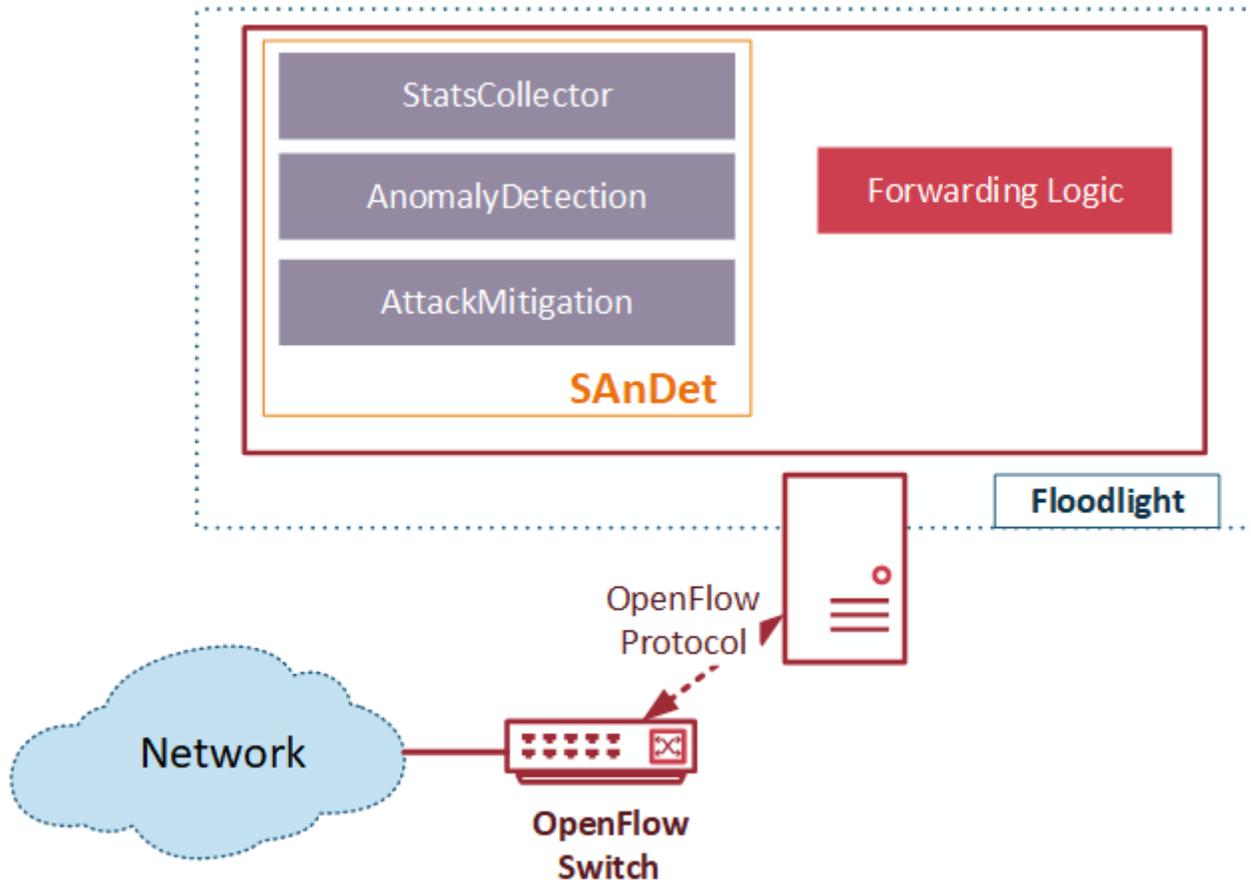


Figure 9

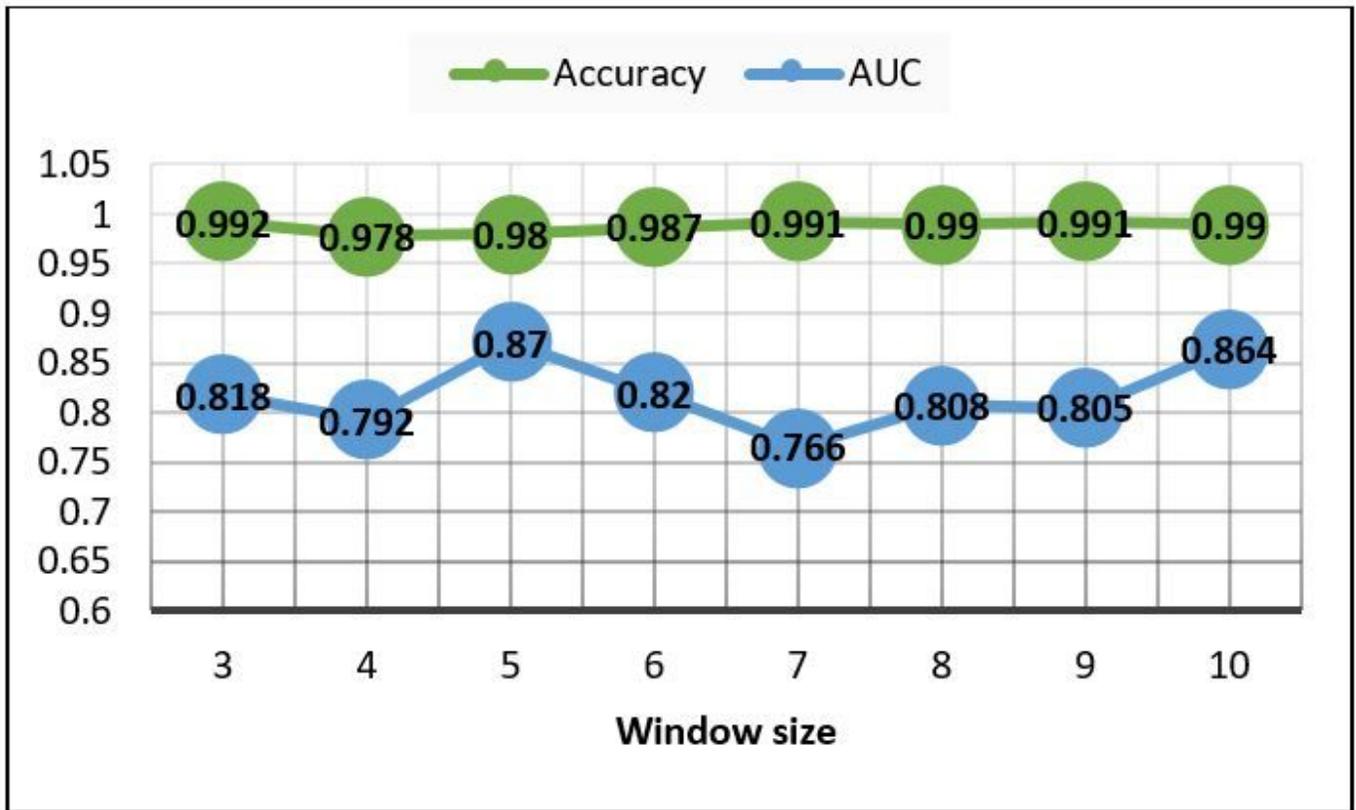


Figure 10

The plot of accuracy and AUC over time window in RNN

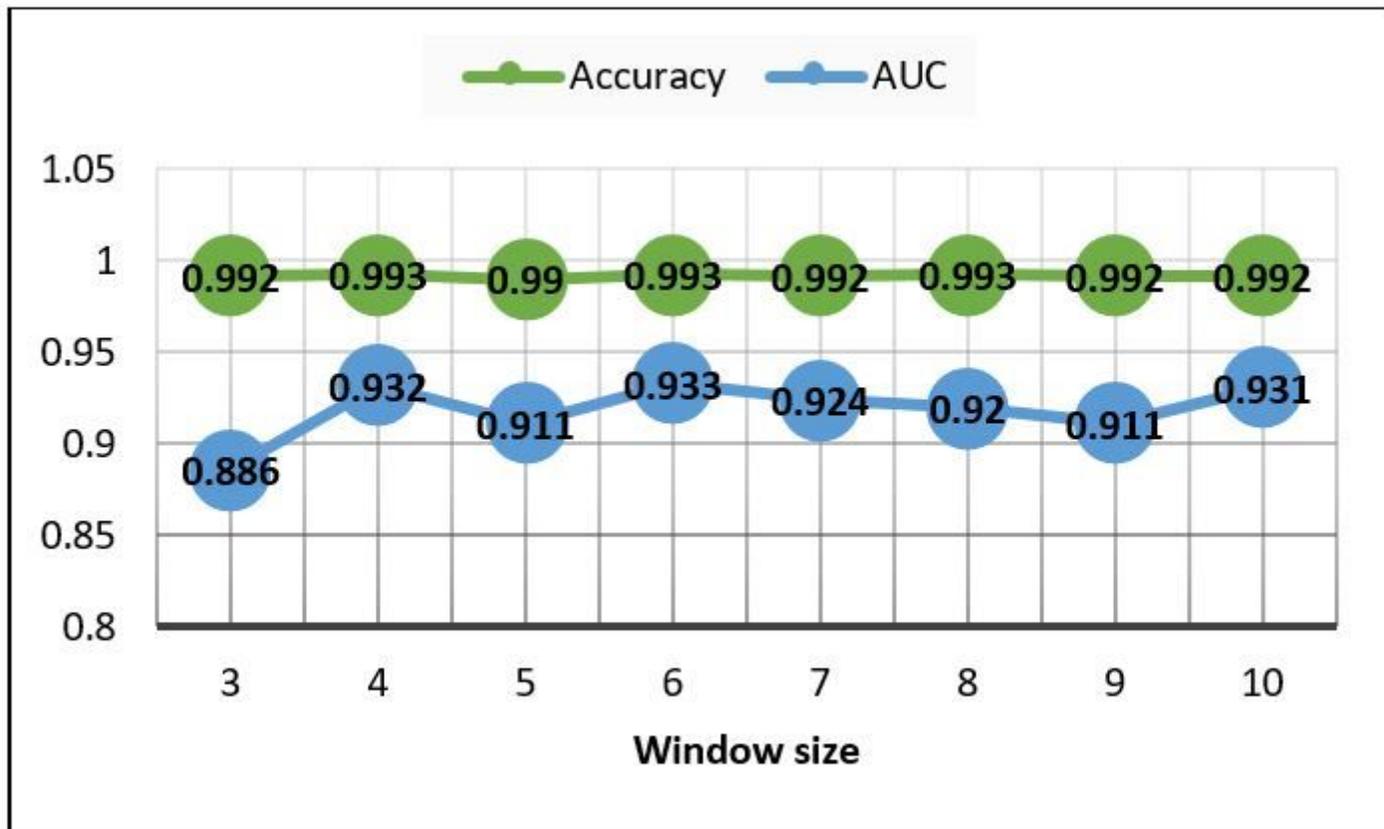


Figure 11

The plot of accuracy and AUC over time window in EncDecAD