Machine Learning in Software Defined Network

Jiamei Liu
College of Computer Science and Technology
Inner Mongolia Normal University
Hohhot, China
1124928309@qq.com

Qiaozhi Xu*
College of Computer Science and Technology
Inner Mongolia Normal University
Hohhot, China
ciecxqz@imnu.edu.cn (*Corresponding author)

***Abstract*—As a new network architecture, software defined network (SDN) separates the control plane from the forwarding plane which enables administrators to define and control the network through the method of software programming, provides a new research direction for the next generation of network architecture. At the same time, the machine learning technology has been developed rapidly in recent years and some studies have begun to introduce machine learning methods into SDN to improve the efficiency of network management and conformity, or to solve problems that cannot be solved easily by traditional methods. The paper analyses, summarizes and introduces these researches which used the supervised learning, unsupervised learning or semi-supervised learning methods to solve some specific problems on SDN, and it will help later researchers understand the filed more quickly and promote the development of the machine learning technology in SDN.**

Keywords—Machine Learning, Software Defined Network, SDN

I. INTRODUCTION

The machine learning is an important branch of artificial intelligence research area, and various machine learning algorithms such as Support Vector Machine (SVM) [1], K-Nearest Neighbor (KNN) [2], Logistic Regression (Logistic Regression) [3], Boosting [4], etc. have been widely used to solve complex problems in engineering and science fields. The emergences of big data and GPU technology provide more powerful support for the development of machine learning technology. The deep learning [5] proposed by Geoffrey Hinton et al. in 2006 pushed the machine learning to a new climax, and made machine learning rapidly develop into an independent area and be applied to various fields, such as pattern recognition, data mining, bioinformatics and autonomous driving, etc.

Clark proposed a network architecture of "A Knowledge Plane for the Internet" in 2003, which relies on machine learning and cognitive technology to manipulate the network [6]. The knowledge plane (KP) would bring many benefits to the network and change the way we operate, optimize and troubleshoot the network. But the distributed network architecture results in that each node (i.e., switches, routers) only has a partial view of the entire system, which makes it a huge challenge to apply machine learning to the network. Logical centralized control will alleviate the complexity of learning in a distributed environment. software defined network (SDN) [7] is a new network architecture that has developed rapidly in recent years. It decouples the control function from the network devices, can provide an overall network view in the logical centralized control plane, and greatly reduces the complexity of applying machine learning to the network, thus has made SDN be one of the application fields of machine learning technology, and also be a hotspot in the network research area.

To enable researchers quickly understand the application and research status of machine learning in the SDN, the paper organizes and summarizes related researches, and introduces situations of using supervised learning, unsupervised learning and semi-supervised learning methods to solve some specific problems in SDN, so as to help researchers to accelerate their research progress.

The remainder of this paper has organized as follows: section 2 introduces related technologies. Section 3 classifies and introduces machine learning mechanisms for SDN security. In section 4, researches of machine learning in traffic classification are discussed. Section 5 concludes the paper with future works.

II. RELATED WORK

A. Software Defined Network

In 2006, the Clean Slate team of the Stanford University proposed the concept of Openflow and tried to deploy it to the campus network [8]. In 2007, Ethane [9], a project led by Martin Casado introduced a centralized controller that made it easier for network administrators to define network security control policies. In 2008, McKeown Nick firstly introduced the Openflow protocol in detail, and later, the SDN (software defined network) architecture was proposed.

SDN separates the control function of a network device from the forwarding function, uses standardized protocols (such as Openflow) to exchange data between the forwarding plane and control plane, implements the programmability to network devices, simplifies network management, facilitates application deployment, and improves the maximum utilization of the underlying devices.

ONF (Open Networking Foundation) [10] divided the architecture of SDN into infrastructure layer, control layer and application layer. The infrastructure layer consisted of SDN switches which was responsible for data forwarding. The control layer was the core of SDN and consisted of one or more

978-1-5386-6243-4/19/$31.00 ©2019 IEEE

controllers. The application layer contained various APPs and provided users a flexible way to deploy application and services.

SDN has been applied in many network scenarios [11-13] to meet the requirements of centralized automatic management, multi-path forwarding, green energy saving and network load balancing. However, there are still many problems that are difficult to solve by traditional methods, therefore some researches introduce machine learning methods into SDN to solve some problems and achieve good results. Section 3 and section 4 will introduce and summarize these studies.

B. Machine learning technology

The name machine learning was coined in 1959 by Arthur Samuel [14]. Tom M. Mitchell provided a widely quoted, more formal definition of the algorithms studied in the machine learning field: "A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P if its performance at tasks in T, as measured by P, improves with experience E" [15].

The types of machine learning algorithms differ in their approach, and we divide them into three types according to the type of data they input and output, and the type of task or problem that they are intended to solve: Supervised Learning (SL), Semi-Supervised Learning (SSL) and Unsupervised Learning (USL).

1) Supervised Learning

Supervised learning is the machine learning task of learning a function that maps an input to an output based on example input-output pairs[16]. It infers a function from labeled training data consisting of a set of training examples[17]. In supervised learning, each example is a pair consisting of an input object (typically a vector) and a desired output value (also called the supervisory signal). A supervised learning algorithm analyzes the training data and produces an inferred function, which can be used for mapping new examples. An optimal scenario will allow for the algorithm to correctly determine the class labels for unseen instances.

The most widely used learning algorithms are Linear Regression, Logistic Regression (LR), Support Vector Machine (SVM), Back Propagation Neural Network (BPNN), K-Nearest Neighbor (KNN) and decision tree , etc.

2) Unsupervised Learning

Unsupervised learning is a branch of machine learning that learns from test data that has not been labeled, classified or categorized. Instead of responding to feedback, unsupervised learning identifies commonalities in the data and reacts based on the presence or absence of such commonalities in each new piece of data, and a central application of unsupervised learning is in the field of density estimation in statistics [18]. Compared to supervised learning where training data is labeled with the appropriate classifications, models using unsupervised learning must learn relationships between elements in a data set and classify the raw data without "help." This hunt for relationships can take many different algorithmic forms, but all models have the same goal of mimicking human logic by searching for indirect hidden structures, patterns or features to analyze new data [19].

Some of the most common algorithms used in unsupervised learning include: K-means, Apriori [20], self-organizing maps (SOM) [21], principal component analysis (PCA), etc. Among them, PCA is an algorithm for accelerating unsupervised learning [22], and many researchers used PCA for feature selection before applying classification [23]; Clustering algorithms such as K-means and other distance-based learning algorithms are often used for anomaly detection; the self-organizing mapping algorithm is an artificial neural network algorithm used to reduce the payload in network intrusion detection.

3) Semi-Supervised Learning

Semi-supervised learning is a class of machine learning tasks and techniques that also make use of unlabeled data for training-typically a small amount of labeled data with a large amount of unlabeled data. Semi-supervised learning falls between unsupervised learning and supervised learning. Many machine-learning researchers have found that unlabeled data, when used in conjunction with a small amount of labeled data, can produce considerable improvement in learning accuracy over unsupervised learning, but without the time and costs needed for supervised learning [24]. There are two steps are generally in a Semi-supervised learning algorithm, firstly, the general rule is analyzed using the labeled data, and then the rule is used to infer unmarked data. At present, the performance of semi-supervised learning is still unstable and needs to be improved.

C. Knowledge Defined Network (KDN)[25]

KDN was an architecture proposed by Cabellos for applying machine learning methods to SDN. In the KDN, the knowledge plane [26] and the management plane were added to the SDN architecture, as shown in figure 1. The data plane was composed of forwarding devices and responsible for storing, forwarding, and processing data flow according to the flow rules sent by the control plane. The control plane was composed of one or more SDN controllers, and sends the flow rule to the data plane through the southbound interface; The management plane was perpendicular to the control plane and data plane, define the network topology, collect and processes the information provided by the network device, monitor and analyze the network; The knowledge plane used machine learning methods to process the information collected by the management plane, then generated specific network control decisions and delivered them to the control plane and data plane.

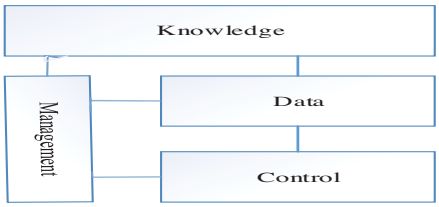

Fig. 1. Architecture of KDN in [26].

With the development of machine learning technologies, it is becoming one of the important choices to better solve some specific problems in SDN. At present, related researches mainly focused on SDN security and traffic classification, and we classify them according to the machine learning methods they used and introduce them in section 3 and section 4.

III. Machine Learning for SDN Security

The malicious flow existed in a data center will cause bad network performance, terrible user experience and even huge economic losses. IDS (Intrusion detection system) is one of the commonly used methods to protect network security, and how to distinguish malicious stream from normal is always the challenge of IDS faced. In SDN, the control plane has a global view of the network, and the security of a data center will be improved effectively if the suspicious stream can be identified and isolated based on the global information. The successes of machine learning technologies in classification create a new direction for researchers to protect the network security.

Currently, there are many datasets such as KDD Cup 1999 [27], NSL-KDD [28], ISCX [29], CIC DOS [30], ADFA-LD12 [31], UNSWNB15 [32], and WSN-DS [33] be widely used in related researches.

A. Detect attacks using supervised learning methods

Supervised learning can predict the type of unknown network flow by marking and learning from known network flow[34]. The SDN can collect a large amount of streams, so supervised learning methods can be used to detect, migrate, and isolate the suspicious streams.

In [35], the authors designed a model that firstly extracted flow from SDN switches, then used the SVM classifier to classify the flow and achieve the purpose of detecting intrusion. The model used the KDD dataset, three behavior-based SVCs, and the ID3 decision tree to perform behavioral feature analysis on the network stream to reduce features and ensure the accuracy of behavior-based SVC. The threat analysis process consisted of three steps:

a) Data collection. In the infrastructure layer, the model incorporated the Open vSwitch, Ryu controller and sFlow-RT and constructed a SDN-based SMP (Shredding-Mixing-Pumping) for traffic statistics and detection to suspicious behavior.

b) Intrusion detection using SVC. AIDS must guarantee low classification errors caused by maximizing the generalization ability of learning on the absence of the complete network data. Firstly, the SVC was trained to detect some specific attacks from the behavioral patterns of collected data and associate them with known malicious threats, and then identified the threatening behavior from the normal connections more accurately. Secondly, the model assessed the accuracy of the SVM in detecting known network attacks and improved the ability to detect unknown threats. Finally, the SVC was combined with SVM to determine whether a intrusion occurs by comparing the behavioral profiles of legitimate network connections and abnormal connections.

c) Migrating network attacks. Finally, the malicious streams would be filtered.

In [36], the authors used a SVM classifier to detect and analyze DDoS attacks in SDN based on the DARPA 2000 [37] dataset and the process was as shown in figure 2.

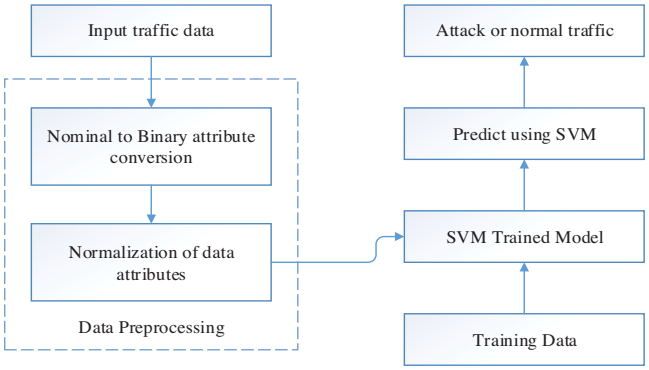

Fig. 2. Processes of Network Threat Detection in [36].

The normal access may be denied if controllers suffer a DDoS attack, therefore, it is better to detect DDoS attacks earlier. The authors compared the classification results of various classifiers and found that SVMs had lower false rate and higher classification accuracy than other classifiers, however, it needed more time for SVMs to train and generate inspection models, and they were very sensitive to parameter adjustments.

Wang used a PCA (principal component analysis) algorithm to remove redundant and uncorrelated features firstly, and then based on SVM to improve the recognition accuracy [38]. Niyaz used the soft-max regression as a classifier and increased the accuracy of training data to 92.48% based on NSL-KDD data set [23]. Coates compared the feature selection methods of various network intrusion detection, and analyzed their shortcomings [39]. In [40-41], the authors conducted active researches on feature selection to improve the accuracy of detection, such as main feature analysis, feature selection method based on double-layer behavior and random forest method.

B. Detect attacks using unsupervised learning methods

Unsupervised learning algorithms need to learn structure and knowledge representation in unmarked input data, so as to predict unknown data by simulating the basic structure or distribution of data [42]. It is often used for feature reduction, such as principal component analysis (PCA), self-organizing map (SOM), and clustering algorithms.

Sultana proposed the use of ML methods in IDS based on SDN and showed many advantages in security implementation, virtual management and quality of service (QoS) [43]. Syed adopted TRW-CB anomaly detection algorithm, rate limiting algorithm, maximum entropy detector algorithm and NETAD algorithm to solve the anomaly problem in SOHO network [44]. Rodrigo used self-organizing maps to construct an unsupervised artificial neural network that could detect DDoS attacks without installing any flow rules effectively [45].

Uamar used an auto encoder to detect DDoS attacks, but when the network was large, the controller would become the bottleneck [46]. Damian used self-organizing maps and learning vector quantization for intrusion detection [47].

Deep learning (DL) is a new field in machine learning, it belongs to unsupervised learning and can find correlations among data automatically. Therefore, some studies tried to apply deep learning in the NIDS, for example, Tuan used deep learning for flow-based anomaly detection, and provided an alternative solution for signature-based IDS [48].

The main challenge of IDS faced is how to detect unknown network attacks and the characteristics of unsupervised learning algorithms make them possibly the best choice for implementation of the NIDS.

C. Detect attacks using semi-supervised learning methods

Semi-supervised learning methods can make use of the information contained in the unlabeled training samples, and achieve a better compromise between the correctness of the classification and the training samples with fewer marks. In order to solve the difficulty of accessing to tagged data in network stream, some studies introduced semi-supervised learning methods into intrusion detection. The semi-supervised learning methods were used to mine the unmarked information, expanded the number of labeled samples and realized the detection of the malicious stream effectively.

In [49], an intrusion detection algorithm based on Semi-Supervised Fuzzy Clustering (SFC) [50] was proposed based on the fuzzy clustering method of objective function. The algorithm introduced competition clustering firstly, and then improved the clustering result by adding a balance term to the objective function. The experimental results showed that its detection rate was closed with fuzzy C-means (FCM). However, due to the supervision of the tag data, the false detection rate of the SFC is low, but there exists a large number of unknown intrusions in the real network, and the network traffic increases continuously, which may lead to errors in the detection of unknown intrusion.

In [51], the characteristics of the network stream were firstly trained by semi-supervised learning method, and then combined with Rocchio [51] and LIBLINEAR [52], so the performance was optimized. Firstly, the feature extraction was performed on the flow, and then the trained model was used for detection, so as to classify the normal flow from abnormal flow.

The experiment randomly selected 10,000 abnormal network data from the KDD99 dataset as the positive sample training set, used the Rocchio method to identify 10,000 normal data as the negative sample data from the remaining samples in the KDD99, and used LIBLINEAR for model training. Then randomly selected 6,000 samples from the KDD99 test set as the test set, including 1,550 positive sample data. The experimental results showed that the model can effectively detect the abnormal flow and improve the detection rate of unknown threats, but there were only positive sample data and no negative sample data in the experiment, and the processing for different data sets needed to be improved.

The semi-supervised learning methods can obtain results similar to those of supervised learning methods based on a small amount of marked data, and save a lot of markup workload. At the same time, since the semi-supervised learning methods are evolved from unsupervised learning, they also have the advantages of unsupervised learning, for example, there is no need to mark and strictly filter the training data, and a better detection effect on the unknown intrusion can be obtained.

With the deployment of SDN, each component in SDN may become the target of network attack such as forged traffic flow, vulnerable switches and centralized controllers are all potential threats, which may result in a destructive impact on the whole network. Therefore, it is significantly for data centers to utilize machine learning methods to improve the accuracy of NIDS based on the global view of the control plane in SDN.

IV. MACHINE LEARNING FOR TRAFFIC CLASSIFICATION

The identification and classification for the network flow is an important basis for understanding, managing and optimizing various network resources. Presently, traditional stream classification technologies based on port number are poor to identify stream generated by new applications and deep packet inspection (DPI) technology [53] becomes the primary choice to classify network stream. However, DPI consumes too much resources and cannot detect encrypted flow, therefore, the classification based on machine learning becomes the new direction.

A. Classify traffic using supervised learning

In [54], the authors proposed a comprehensive architecture to collect and analyze large-scale network data, studied the relationship between KPI (key performance indicators) and traffic patterns, and conducted traffic prediction, which consisted of three steps:

(1) Collecting traffic and other data from all sources in the network.

(2) Using ML algorithms to theoretically study the relationship between KPI and future traffic, and developing an optimization model through statistical modeling in order to understand the value of each parameter for traffic prediction and determine the key performance indicators;

(3) Applying the model to the system and analyzing the network performance to detect if it met the requirements. It would use the new network parameters if the network behavior reached the expected performance, otherwise, identify the problem and relearn.

A model was also built using Naive Bayes to analyze the relationship of the next-hour GSM traffic of a cell with the observed KPIs. It showed that the role of each KPI for traffic forecasting was different, and it depended not only on the types of traffic but also the time period. The model improved the performance and ensured that only important parameters were used for traffic prediction and redundant or irrelevant attributes were removed. By randomly selecting 100,000 samples from

different datasets as the training sets, the experimental results showed that when the same ML algorithm was applied, KPI model has better accuracy than time series model, especially when the traffic changed rapidly and irregularly, the performance of KPI model were improved, which could effectively perform data mining and machine learning tasks and had a high accuracy in predicting future traffic.

Pedro proposed a traffic classification architecture for SDN based on supervised learning methods, which could collect traffic in SDN network and traditional network [55]. The experimental results showed that it got a higher precision, but the stream types that could be collected and identified were limited, and it was not suitable for the complex and differentiated real network environment.

Thomas proposed a machine-defined network application-aware multi-path packet forwarding framework based on machine learning [56]. The system used the C4.5 decision tree to evaluate the characteristics of different flow, classified and prioritized each flow, and then selected the forwarding path according to the flow priority. The system will benefit large-scale multipath environments with QoS requirements, including data center networks, telecom/data networks, and campus networks.

Qazi proposed a framework Atlas that integrated application perception into the software-defined network. Atlas adopted the traffic classification technology based on machine learning to support fine-grained, accurate and extensible application classification in SDN [57]. Marc proposed a multi-path communication mechanism among cross-domain switches based on the fat tree algorithm, but the multi-path forwarding was random and QoS was not considered [58].

Supervised learning methods are widely being applied to traffic classification to achieve good results, however, the traffic in networks is huge and complex, which makes the marking of datasets very difficult, therefore, traffic classification using unsupervised or semi-supervised methods will become the focus in the future.

B. Classify traffic using unsupervised learning

The advantage of unsupervised learning methods is that the classes in the data set can be found automatically through clustering, so as to find the unknown relationship in the data and the similarity pattern among the observed objects, rather than having to mark the training samples, so as to discover new network applications.

The first unsupervised learning method was the auto class algorithm based on EM (Expectation Maximization Algorithm) proposed by Zander in 2005 [59]. The algorithm used EM method for maximum likelihood estimation, which was used to select samples and cluster, and obtained an average accuracy of 86.5% and improved the efficiency and accuracy of previous algorithms to some extent. However, the clusters obtained were not one-to-one corresponding to application categories, and the algorithm didn't specify how to determine the mapping relationship between clustering clusters and application types. Ideally, the number of clusters should be equal to the number of application categories and each application category corresponds to a unique cluster but in the actual situation, the number of clusters is often more than the number of application categories, which would lead to insufficient accuracy of data labels in the training set, thus affecting the accuracy of predicting unknown sample types.

Erman proposed a method for classifying streams using one-way flow information [60]. This method used the K-means algorithm to develop and validate an algorithm that could track and estimate the missing information from one-way packets. The experimental results showed that the traffic statistics feature of the server-to-client direction based on the TCP connection could provide more than 95% classification accuracy. However, it was necessary to manually mark the application types of clustering clusters. When processing large-scale samples, the clustering time was usually long, which would consume large computing and storage resources.

Lian synthesized k-means and DBSCAN algorithm, used the t-neighborhood density of the object in the density algorithm as the condition for the selection of the initial clustering center point, selected the better initial center point, and proposed the improved k-means algorithm [61]. The experimental results showed that the algorithm had some advantages in feasibility, accuracy and misjudgment rate, but it could not be run in the real network, and its consumption of resources needed to be further tested.

Compared with supervised learning methods, unsupervised learning does not require a training set, but the accuracy is lower. At present, researches on unsupervised learning are not comprehensive, and with the increasing of network applications, unsupervised learning will be more and more important and be one of the focus of future researches.

C. Classify traffic using semi-supervised learning

Semi-supervised methods use a small amount of tag data to assist the clustering process, so as to determine the mapping relationship between clusters and flow types and realize flow classification, and it can discover unknown new application types, improve detection accuracy, and reduce the workload for marking data.

Lu proposed a framework for QoS-aware flow classification for SDN, and traffic was divided into different QoS categories [62]. The QoS classifier used a semi-supervised learning method to process unknown application flows. The experimental results showed that the Laplace SVM was better than the K-means algorithm but the QoS classifier needed to be retrained each time.

Liu proposed an application layer traffic classification method STC based on the entropy function combined feature selection method [63]. Firstly, the STC used a small amount of tagged data to determine the initial center of Kmeans, then established a mapping relationships between the application types and clusters, and finally found an unknown application. For clusters that could not be marked, the STC used the fast KNN [64] to search for the k-th data closest to it, and used the majority votes to determine its flag. If the data was still not tagged, the data was determined to be a new type. STC used the Andew Moore dataset [65] as the original dataset and

divided the application into 6 categories. Firstly, the apparently unrelated features were manually eliminated, and then the entropy values of the remaining 108 features were calculated separately, and finally the Naive Bayesian classifier and the Sequential Backward Selection search method were used. The redundancy between features was removed, and finally 5 features were retained as the optimal feature subset of the STC algorithm. In the experimental evaluation, the detection accuracy reached 92.2%, which was higher than the Kmeans clustering algorithm.

The premise of pre-marking with supervised learning methods and the hope of using machine learning methods to classify traffic to get rid of the traditional traffic classification method are contradictory. Unsupervised learning methods only have advantages in new applications. The semi-supervised learning approach allows datasets including both labeled and unlabeled samples, and mining more useful information from unlabeled samples is the advantage of this approach.

The classification of network flow or the identification of network applications based on machine learning methods is a research hotspot in recent years. Instead of relying on the protocol port or parsing protocol content to identify the network application, they use the a priori features of the "stream" extracted from the transmitted traffic data or calculate the statistics of the flow to achieve the purpose of distinguishing the network applications. With the rapid development of network applications, the flow attributes change constantly, and new problems of traffic classification will face more and more challenges, so it will be a hot topic to use machine learning methods to classify data streams more accurately.

V. CONCLUSIONS

In June 2017, Cisco introduced the concept of "Intent-Based Networking (IBN)" [66], that is, using machine learning technology to intelligently control the network, and it will be the desired state of the network managed and the main development direction of future network. The SDN architecture and the development of machine learning methods are laying a technical foundation for the realization of IBN, and it will make IBN a reality as soon as possible to discuss and mine the machine learning methods under SDN architecture. The paper recognizes and analyzes the related researches which can help researchers to understand and enter the field quickly.

ACKNOWLEDGMENT

This work was supported by the Inner Mongolia Autonomous Region Higher Education Institutions Scientific Research Project (Grant No. NJZY18023), the Inner Mongolia Autonomous Region Natural Science Foundation (Grant No.2012MS0930), and the Inner Mongolia Autonomous Region Higher Education Institutions Scientific Research Project (Grant No. NJZY12032).

REFERENCES

[1] Cortes, Corinna, Vladimir Vapnik. "Support-vector networks." Machine learning 20.3, pp. 273-297, 1995.

[2] Altman N S. An introduction to kernel and nearest-neighbor nonparametric regression[J]. The American Statistician, 46(3), pp. 175-185, 1992.

[3] Hosmer D W, Lemeshow S. Introduction to the logistic regression model[M].2nd ed. Applied Logistic Regression, pp. 1-30, 2000.

[4] Schapire R E. The boosting approach to machine learning: An overview[M]. Nonlinear estimation and classification. Springer New York,2003:149-171.

[5] Hinton G E, Salakhutdinov R R. Reducing the dimensionality of data with neural networks[J]. Science,313(5786), pp. 504-507, 2006.

[6] Clark D D, Partridge C, Ramming J C, et al. A knowledge plane for the internet[C]//Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. ACM, pp. 3-10, 2003.

[7] Kreutz, Diego, et al. "Software-defined networking: A comprehensive survey." Proceedings of the IEEE 103.1 pp. 14-76, 2015.

[8] Stanford University Clean slate program, 2006. http://cleanslate.stanford.edu/

[9] Casado M, Freedman M J, Pettit J, et al. Ethane: taking control of the enterprise[C]//Acm Sigcomm Conference on Applications. ACM, pp.1-12, 2007.

[10] Foundation O N. Software-Defined Networking: The New Norm for Networks[J], 2012.

[11] Jain S, Kumar A, Mandal S, et al. B4: experience with a globally-deployed software defined wan[C]//ACM SIGCOMM 2013 Conference on SIGCOMM.ACM, pp. 3-14, 2013.

[12] Hong C Y, Kandula S, Mahajan R, et al. Achieving High Utilization with Software-Driven WAN[J]. Computer Communication Review, 43(4), pp. 15-26, 2013.

[13] Handigol N, Seetharaman S, Flajslik M, et al. Plug-n-Server: load-balacing Web traffic using Open Flow[C]//In ACM Sigcomm Demo, pp. 268-270, 2009.

[14] Samuel, Arthur, "Some Studies in Machine Learning Using the Game of Checkers." IBM Journal of Research and Development. 3 (3), pp. 210–229, 1959.

[15] Mitchell, T. Machine Learning. McGraw Hill. p. 2. ISBN 978-0-07-042807-2, 1997.

[16] Tao Xinmin, Song Shaoyu, Liu Furong, Cao Pandong, Bearings fault detection based on semi-supervised SVM Laplacian regularization, Control Conference (CCC), 2011 30th Chinese.

[17] Stuart J. Russell, Peter Norvig Artificial Intelligence: A Modern Approach, Third Edition, Prentice Hall ISBN 9780136042594, 2010.

[18] Barbara D.,Wu N., & Jajodia S, "Detecting novel network intrusions using Bayes estimators", In Paper presented at the first SIAM conference on data mining, Chicago, 2001

[19] https://en.wikipedia.org/wiki/Supervised_learning.

[20] M. Koerner and O. Kao. Evaluating sdn based rack-to-rack multipath switching for data-center networks. Procedia Computer Science, 34, pp. 118–125, 2014.

[21] Zanero S, Savaresi SM Unsupervised learning techniques for an intrusion detection system. In: Proceedings of the ACM symposium on applied computing, pp. 412–419, 2004.

[22] Eid HFA, Darwish A, Hassanien AE, Abraham A Principal components analysis and support vector machine based intrusion detection system. International conference intelligent systems design and applications(ISDA), 2010.

[23] Niyaz Q, Sun W, Javaid AY, Alam M A deep learning approach for network intrusion detection system. International conference wireless networks and mobile communications(WINCOM), 2016.

[24] https://en.wikipedia.org/wiki/Semi-supervised_learning , Retrieved 2018-12-3.

[25] Cabellos A, Cabellos A, Cabellos A, et al. Knowledge-Defined Networking[J]. Acm Sigcomm Computer Communication Review,47(3), pp. 2-10, 2017.

[26] Clark D, A knowledge plane for the internet[C]//Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. ACM, pp. 3-10, 2003.

[27] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[28] Gogoil P, Bhuyan MH Packet and flow-based network intrusion dataset. International conference on contemporary computing IC3, pp. 322–334, 2012.

[29] Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Comput Secur 31(3), pp. 357–374, 2012.

[30] University of New Brunswick (2017) [Online] available http://www.unb.ca/cic/research/datasets/dos-dataset.html. Accesses 22 June 2017

[31] Creech G, Hu J Generation of a new IDS test dataset: time to retire the KDD collection. Wirel Commun Netw Conf(WCNC).https://doi.org/10.1109/WCNC.2013.6555301, 2013.

[32] Nour M, Slay J The evaluation of network anomaly detection systems: statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Inf Secur J: A Glob Perspec, pp. 1–14, 2016.

[33] Almomani I, Al-Kasasbeh B, Al-Akhras M WSN-DS: a dataset for intrusion detection systems in wireless sensor networks. JSens16p, 2016.

[34] https://en.wikipedia.org/wiki/Support_vector_machine

[35] Ping Wang, Hsiao-Chung, Lin, Wen-Hui Lin, Kuo-Ming Chao, Chi-Chun Lo, An Efficient Flow Control Approach for SDN-based Network Threat Detection and Migration Using Support Vector Machine, 2016 IEEE International Conference on e-Business Engineering.

[36] RT Kokila, ST Selvi, K Govindarajan, DDoS Detection and Analysis in SDN-based Environment Using Support Vector Machine Classifier, International Conference on Advanced Computing, pp. 205-210, 2015.

[37] DARPA 2000 Scenario Specific dataset available from: http://www.ll.mit.edulmissionicommunications/cyber/CSTcorporalid eval/datal2000/LLS DDOS 1.0.html

[38] Wang L, Jones Big data analytics for network intrusion detection: a survey. Int J Netw Commun. https://doi.org/10.5923/j.ijnc.20170701.03, 2017.

[39] Coates A, Lee H, Ng Andrew Y An analysis of single-layer networks in unsupervised feature learning. In: Proceedings of the fourteenth international conference on artificial intelligence and statistics, PMLR 15, pp. 215–223, 2011.

[40] Lu Y, Cohen I, Zhou XS, Tian QFeature selection using principal feature analysis. Pattern Recogn Lett 49, pp. 33–39, 2014.

[41] Eid HF, Salama MA, Hassanien AE, Kim TH Bi-layer behavioral based feature selection approach for network intrusion classification.Commun Comput Inf Sci Book Ser 259, pp. 195–203, 2011.

[42] Supervised and unsupervised machine learning algorithms http://machinelearning mastery.com/supervised-and-unsupervised machine learning-algorithms/.Accessed 20 June 2017.

[43] N Sultana, N Chilamkurti, W Peng, R Alhadad, Survey on SDN based network intrusion detection system using machine learning approaches, Peer-to-Peer Networking and Applications, pp. 1-9, 2018.

[44] Mehdi SA, Khalid J, Khaiyam SA(2011)Revisiting traffic anomaly detection using software defined networking. In: Sommer R, Balzarotti D, Maier G(eds)Recent Advances in Intrusion Detection. RAID 2011. Lecture Notes in Computer Science, vol 6961.Springer, Berlin, Heidelberg.

[45] Braga R, Mota E, Passito A Lightweight DDoS flooding attack detection using NOX/OpenFlow.35th Annual IEEE conference on local computer networks, Denver, Colorado, 2010.

[46] Niyaz Q, Sun W, Javaid AY A deep learning based DDoS detection system in software defined networking(SDN). CoRR abs/1611.07400. https://doi.org/10.4108/eai.28-12-2017.153515, 2016.

[47] Jankowski D, Amanowwicz M on efficiency of selected machine learning algorithms for intrusion detection in software defined networks.Int J Electron Telecommun,62(3), pp. 247–252, 2016.

[48] Tuan TA, Mhamdi L, Mclernon D, Zaidi SAR, Ghogho M Deep learning approach for network intrusion detection in software defined networking. Int Conf Wirel Netw Mob Commun. https://doi.org/10.1109/WINCOM.2016.7777224, 2016.

[49] Rushan Wang, Yongzhong Li, Research on Intrusion Detection Algorithm Based on Semi-supervised Learning, Microelectronics and Computer, 26(10), pp. 25-28, 2009. (. in china)

[50] Pong Shao, Luming Yang, Image multi-threshold feature fusion and its application in face detection[J]. Mini-micro Systems, 29(10), pp.1878-1884, 2008. (. in china)

[51] Songqing Zhang, Zhiguo Liu, Industrial control network intrusion detection method based on semi-supervised learning, Information Technology and Network Security, 2018(1) (. in china)

[52] Fan Rongen, Chang Kaiwei, HSIEH C J, et al. LIBLINEAR: a library for large iinear classification[J]. Journal of Machine Learning R esearch, 9(12), pp. 1871-1874, 2010.

[53] Ubik S, Zejdl P. Evaluating application-layer classification using a Machine Learning technique over different high speed networks[C]//Systems and Networks Communications(ICSNC),2010 Fifth International Conference on. IEEE, pp. 387-391, 2010.

[54] Luong-Vy Le, Do Sinh, Li-Ping Tung, Bao-Shuh Paul Lin, A Practical Model for Traffic Forecasting based on Big Data, Machine-learning, and Network KPIs, 2018 15th IEEE Annual Consumer Communications & Networking Conference(CCNC)

[55] Pedro Amaral, Joao Dinis, Paulo Pinto, Machine Learning in Software Defined Networks: Data Collection and Traffic Classification, 2016 IEEE 24th International Conference on Network Protocols(ICNP)Workshop on Machine Learning in Computer Networks (Network ML 2016)

[56] Thomas Valerrian Pasca S, Siva Sairam Prasad,Kotaro Kataoka, AMPF: Application-aware Multipath Packet Forwarding using Machine Learning and SDN, arXiv:1606.05743v2[cs.NI]26 Jun 2016

[57] Z.A.Qazi, J.Lee, T.Jin, G.Bellala, M.Arndt, and G.Noubir. Application-awareness in sdn. In Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM, ACM, pp. 487–488, 2013.

[58] M. Koerner and O. Kao. Evaluating sdn based rack-to-rack multipath switching for data-center networks. Procedia Computer Science, 34, pp. 118–125, 2014.

[59] Zander S, Nguyen T, Armitage G. Automated traffic classification and application identification using machine learning[C]//Local Computer Networks,2005.30th Anniversary. The IEEE Conference on. IEEE, pp. 250-257, 2005.

[60] Erman J, Arlitt M, Mahanti A. Traffic classification using clustering algorithms[C]//Proceedings of the 2006 SIGCOMM workshop on Mining network data.ACM, pp. 281-286, 2006.

[61] Lian Yan, Research on P2P traffic identification technology based on unsupervised learning, Master's thesis of Xihua University, 2014 (. in china)

[62] Lu He, Chen Xu, Yan Luo, vTC: Machine Learning Based Traffic Classification as a Virtual Network Function

[63] Bin Liu, Zhitang Li, Hao Tu, Application layer traffic classification based on semi-supervised learning, MICROELECTRONICS & COMPUTER, 2008.10 (. in china)

[64] Yan Yu, Hao Huang, A semi-clustering anomaly intrusion detection algorithm[J]. computing Application,26(7), pp. 64-66, 2006. (. in china)

[65] Moore A W, Zuev D. Discriminators for use in flow based classif ication [R]. Cambridge: Intel Research, 2005.

[66] Bob Laliberte, ESG Senior Analyst. The Journey to Intent-based Networking (white pape). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-09-esg-analyst-report-cte-en.pdf, 2018.1.