Deep Learning Based Traffic Classification In Software Defined Networking –A Survey

K. Tamil Selvi, Dr. R.Thamilselvan

Abstract : Real time analysis of network traffic is prime factor for network intrusion detection. The core element of intrusion detection is the traffic classification. The traditional network is distributed in nature and implementation of intelligence in the network is a complex task. Software Defined Networking (SDN) provides a way for including intelligence into the network. SDN can provide centralized controller, dynamic update of flow table and traffic analysis, global view of network topology and dynamic routing. With these characteristics, network intelligence can be easily integrated into SDN environment. Machine learning algorithms are implemented for traffic classification. But it cannot suit to dynamic nature of the network and also classification of new trends of traffic. Deep learning techniques are best needed solution for traffic classification. It exhibits dynamic feature selection from the input traffic and provides higher rate of traffic classification accuracy. This paper summarizes various traffic classification techniques based on deep learning applied to SDN.

Index Terms : Controller, deep learning, features, software defined networking, traffic classification

1 INTRODUCTION

Rapid development of Internet and networking technologies has provided exponential growth of network traffic. Distribution of traffic in an optimized way and managing large volume of heterogeneous devices is a complex task. Deployment of intelligence in network can solve the above issues. Knowledge plane [1] had been proposed to incorporate intelligence, automation and recommendation to the network through machine learning techniques. But distributed nature of traditional network systems had made the process complex [2]. To reduce the complexity of learning, Software Defined networking (SDN) paved a way for it. It is an innovative architecture which decouples control plane from data plane [1]. The centralized control plane is responsible for routing and management policies. Fig.2 depicts the architecture of SDN. The data plane forwards the packet only through protocols like OpenFlow. An intelligent task of categorizing network traffic into different classes is termed as traffic classification. It is widely used for managing network, measuring services, network monitoring, and network design and so on. Classification of network traffic accurately is beneficial for providing Quality of Service (QoS), access control and imposing other security parameters. Traffic classification is a network function which identified different flow types in a fine-grained manner for network management. Handling of network and resource allocation can be done effectively through traffic classification. Machine Learning (ML) enables logical mining of valuable information from the collected network traffic or discovers the correlation automatically. The heterogeneous network traffic generated from sources exhibit different format and complex correlation. Traditional ML tools find it difficult to solve the problem of interest. ML degrades in performance [3] when provided with more volume of network traffic and cannot handle high dimension data. Hierarchical feature extraction can be provided by Deep Learning (DL) with large volume of network traffic. Hence network analysis and management in timely manner can be facilitated by DL. The view of traffic classification using deep learning model is shown in Figure 1. The article reviews the state-of-art techniques of deep learning for traffic classification in software defined networking environment. High-level overview of Software Defined Networking is projected. Then Deep learning models are explored. Finally, an insight on traffic classification techniques is provided.

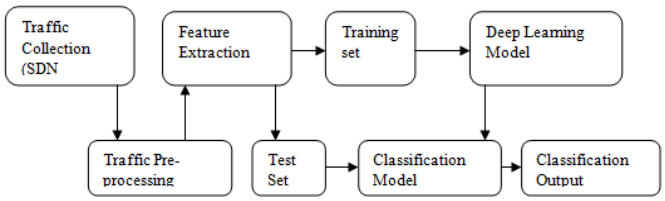

Figure 1 *Model of Traffic classification*

2 SOFTWARE DEFINED NETWORKING

In this section, brief background knowledge of SDN in terms of architecture and workflow is presented.

2.1 Architecture of SDN

SDN consists of three planes namely data plane, control plane and application plane. As per Open Networking Foundation (ONF), control plane is decoupled from data plane, network automation and intelligence are specified to centralized control plane and provides abstraction of network infrastructure to the application. The architecture component of each plane is shown in Figure 2.

2.2 Data Plane

Data plane is the lowest layer in SDN architecture. It consists of network forwarding elements like physical switches and logical switches (virtual). Software switches are virtual switches which run on common operating systems like Linux. Some of the virtual switch implementations are Indigo, Open vSwitch and Pantou [4]. The complete features of SDN protocol are supported by virtual switches whereas physical switches lack flexibility and feature completeness. The major responsibility of switches in data plane are forward, drop and modify packets based on flow rules received from the controller in the control plane. The communication protocol is OpenFlow.

- *K.Tamil Selvi, Assistant Professor, Department of CSE, Kongu Engineering College, Perundurai – 638060. E-mail: ktamilselvikec@gmail.com*
- *Dr.R.Thamilselvan, Professor, Department of IT, Kongu Engineering College, Perundurai - 638060 E-mail :rthamilselvan75@gmail.com*

Control Plane

The brain of the SDN architecture is the SDN controller present in the control plane. It is centralized controller provides the dynamic programming of network resources, updation of flow rules and make network administration flexible and agile. The information about network state of data plane is provided to application plane by the control plane. The application requirements are translated into policies and distributed to forwarding devices through control plane. The controller also provides functionalities like routing, network topology storage, device configuration, state information and so on. The various controllers available are NOX, POX, Ryu, OpenDayLight, FloodLight, Beacon, etc. Through OpenFlow protocol, the centralized control plane communicates with the network devices. Flow tables [5] which contain flow entries in the Open Flow switches provide the forwarding path for the flows. The fields of the flow table are match fields and associated actions. The native features of flow like source IP, Destination IP and header data. And also includes other statistical features like number of bytes, duration and so on. SDN realizes traffic classification and feature selection. The SDN controller provides the global view of the network through which classification of traffic can be performed. The effective matching of incoming packet is based on ruleset [6]. Effective bits are bits in rule set which partition ruleset at the best effort to find out highly related rules for each incoming packets.

2.3 Application Plane

The layer in the SDN architecture composed of business application is called application plane. The services in the application plane provide business management and optimization. The business services for applications are provided by the controller [7]. Some of the SDN applications are Traffic Engineering [7], security [8], Distributed Denial of services attack [9], Fault management [10] and so on. SDN has been deployed in many networks like transport network, optical network, wireless sensor network, Internet of Things, edge computing, Wide Area Network, cloud computing and Network Function Virtualization.

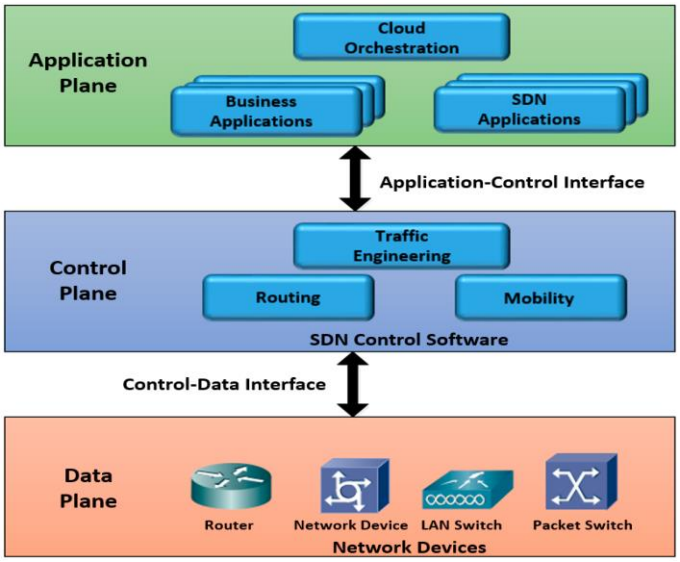

***Figure 2** SDN Architecture [11]*

3. DEEP LEARNING IN NETWORKING

In this section, a potential briefing on deep learning application in networking has presented. It also highlights the basic principles behind the deep learning algorithms and its advantages. The key principle behind the deep learning is to approximate complex functions by decomposing it into simple and predefined operations of neuron. The operations are performed by weighted combination of hidden layers with activation functions based on the structure of the model. Some of the available deep learning architectures are

- Recurrent Neural Networks (RNN)
- Long Short Term Memory and Gated Recurrent Units (LSTM-GRU)
- Convolution Neural Networks (CNN)
- Deep Belief Networks (DBN)

3.1 Recurrent Neural Networks

In RNN, output from the previous step is given as input to the next step. The feedback mechanism is provided by hidden layers, which remember some information about the sequences. Since RNN have memory, it remembers all the information calculated so far. It is less complex because it uses same parameters for each input or hidden layers to produce output. Accurately identifying various attacks in intrusion detection systems is the key in information security [12]. The data collected consist of 41 features and one class label. The label value is of four types namely Denial of Services (DoS), Root to Local attack (R2L), User to Root attack (U2R) and Probing attacks. RNN based intrusion detection provides higher accuracy than other classification techniques. Table 1 provides overview of SDN solutions for traffic classification based on deep learning. Convolution Neural Network provides higher accuracy rate compared to other neural network models. The SDN controller provides the complete view of the network and traffic collection. Thus the intelligence in traffic classification is performed by the centralized controller. Based on the application, the deep learning techniques may vary to meet the requirement of the network condition.

3.2 Long Short Term Memory and Gated Recurrent Units

LSTM contain memory cell which retains its information for long or short time based on the function of input value. It consists of three gates namely input gate, forget gate and output gate. The simplified form of LSTM is gated recurrent unit which lacks output gate. The two gates are update and reset gates. A GRU can model RNN by setting reset gate to 1 and the update gate to 0. GRU-RNNbased intrusion detection system has been proposed by [13]. With only six features, the system provided accuracy of 89%. Dynamic network routing based on LSTM [14] predict the Internet traffic with high accuracy. Estimating the future network traffic from the previous and achieved network data has been done using LSTM [15]. LSTM models long range dependencies more accurately than RNN. In order to identify time related characteristics of the traffic [16], LSTM is applied. It classifies the network traffic based on time features of the network traffic.

Table 1 *Deep Learning based Traffic classification in SDN*

Traffic collection	Traffic processing	Deep Learning techniques	Tool used	Parameters	Comments	Ref
Mobile Network Virtual Operators and SDN controller	In-Network and Computing	Deep reinforcement learning	Tensor Flow	Convergence rate	Faster convergence rate	[17]
NSL-KDD Dataset	Statistical based traffic classification	CNN	Tensor Flow	Accuracy	Improved Accuracy	[18]
SDN controller	Exploits non-regularities of network traffic	CNN	ONTS	Mean squared error	Long durability and fast forecast	[19]
SDN controller	Real time in IoT network	CNN and DBN	C++ WILL	Accuracy	Improved Accuracy	[20]
GEANT dataset	Predicting future traffic matrix	LSTM	Tensor Flow	Accuracy	Improved Accuracy	[21]
SDN Controller and GEANT dataset	Predicting future traffic matrix over time	LSTM	POX controller	Mean squared error	Improved Accuracy	[15]
SDN controller	Payload based traffic classification	LSTM	Tensor Flow	F1- score	Improved Accuracy	[22]

3.3 Convolution Neural Networks

CNN is a multilayer neural network which implements feature extraction and then applies classification. It consists of processing layer, convolution layer, pooling layer and classification layer. It uses multilayer perceptron to do computational tasks and uses filters for learning. The security in the SDN environment is implemented using CNN [23]. Automatic extraction of features from the network traffic and classification of traffic as malicious is done with [24] high accuracy rate using CNN characteristics. In Vehicular Adhoc Network, SDN controller is used to learn highest routing path trust value usingCNN. The trust based optimized routing is provided by CNN enabled SDN controller. Distributed Denial of Services (DDoS) attack is the major threat in the Internet. CNN provides classification of attacks with accuracy rate of 98.2%. The optimized feature selection is done using CNN algorithms [25]. One dimensional CNN [16] is used to find the features to classify the traffic from spatial range. To improve the performance of CNN, Capsule network [26] can be used. The activation function of this network is an instantiation parameter of a particular type of an entity.

3.4 Deep Belief Networks

DBN is a multilayer neural network with training algorithm. In DBN, each pair of hidden layer is a restricted Boltzmann machine (RBM). Hence DBN is represented as stack of RBMs. There are two phases of training namely unsupervised pretraining and supervised fine tuning. The output is the network classification. DDoS attack is identified through SDN controller [27] in the wireless sensor network. The attack prevention model is built using DBN. This model is implemented in multitenant cloud and IoT enabled architecture which shows high accuracy of classification. Large scale IoT deployments like smart cities needs high network resiliency and scalability [28]. DNB is used as dimensionality reduction tool for support vector machines. Short term traffic flow prediction [29] in Internet vehicular network using RBM provides better nonlinear fitting ability and prediction accuracy. DNB provides unsupervised feature learning [30] and multitask regression predicts the network traffic flows.

4 NETWORK TRAFFIC CLASSIFICATION

Classifying network traffic with the generated application is essential for traffic analysis. Traffic classification is an important network function for network operators to handle network resources effectively. The available network traffic classification techniques are

- Port based classification
- Payload based classification
- Statistical classification
- Behavioral classification

4.1 Port based classification

The header of the data packet contains TCP or UDP [31] port number which uniquely identifies the application. Earlier these port numbers are registered with Internet Assigned Numbers Authority (IANA). But peer to peer applications can take some random port number. Hence classification of network traffic results in increase of false negative classifier rate. So this method becomes obsolete [32]. Table 2

Table 2 *Traffic classification Techniques*

Category	Classification technique	Features used	Granularity	Processing overhead
Port based	Protocol Port	Protocol Port	High	Low
Payload based	Deep Packet Inspection	Payload inspection of first n packets	High	High
	Stochastic Packet inference	Statistical properties inherent in packet header and payload	High	High
Behavioral technique	End host	Behavioral pattern of end hosts	Low	Moderate
	Traffic accounting	Analysis of inspected packets and flows	High	High
Statistical technique	Packet based	packet duration, length of packet, packet inter-arrival time and flow idle time	High	Moderate
	Flow based	Duration, transmission rate, flow features	Low	Low

provides over all analysis of traffic classification techniques. To incorporate deep learning techniques for traffic classification, statistical classification is widely accepted.

4.2 Payload based classification

In order to overcome the flaws in port based classification, inspection goes beyond the header of the packet to the payload part of it. It works by examining the payload part of the packet and matching them with a set of stored patterns. Based on four degree of verification [33] namely signature-based, syntax, protocol conformance and semantic, a light weight traffic classifier has proposed. It achieved higher accuracy, completeness and convergence. [22] Proposed payload based traffic classification using multilayer LSTM in software defined network. The optimal hyper parameter tuning is performed with improved F1-score. Payload signature based traffic classification suffers from low processing speed [34]. To overcome this limitation, various design options has been proposed. To address the problem of unknown application, unsupervised clustering algorithms are used [35]. The proposed method uses bag of words model to represent the content of traffic clusters. To aggregate the similar traffic clusters, latent semantic analysis is applied. The model is trained using flow statistical properties and payload. Deep Packet Inspection (DPI) locates, examines, and classifies the data packet. A semi-supervised multi-classifier is used in SDN controller [36]. Dynamic flow table can be maintained through DPI. Dynamic nature of network application and network characteristics can be adapted using the classifier. In order to reduce the complexity of DPI process, SDN data planes are offloaded down to the network processing of filtering traffic to DPI [37]. DPI module in the SDN controller provides application aware traffic management [38]. This provides implementation of firewall and bandwidth manager. To detect elephant flows [39] in the data center network, DPI can be employed. A cost sensitive learning technique is used with DPI for classification of elephant or mice flows.

4.3 Statistical Classification

The network traffic is identified based on statistical characteristics of network traffic flow. The various statistical data of flow are packet duration, length of packet, packet inter-arrival time and flow idle time. These parameters are unique for each traffic that can distinguish applications from each other. The OpenFlow switch is incorporated with traffic classification [40]. Statistical classification is performed based on mean number of flows and coefficient of variation. With greater traffic intensity, the model behaves well with high classification accuracy. Packet bursts [41] are the characterized by HTTP and DNS traffic. SDN supports native flow features that do not describe intrinsic traffic profile. A sub optimal flow feature selection is enabled for classification of traffic with high accuracy. One of the applications of traffic classification is providing Quality of Services (QoS) [42]. The SDN controller is modelled with adaptive, real-time and accurate traffic classification mechanism. DPI and semi supervised algorithms are used for traffic classification with high accuracy.

4.4 Behavioral classification

In Behavioral classification, the whole traffic received by host or end point is observed for the examination of pattern. The main work of the classifier is to classify the application running in the hosts. NetFlow [43] records are exploited for traffic classification based on behavioral algorithm that uses number of packets and bytes. The supervised classifier provides 90% accuracy in worst case scenario. A CNN based traffic classification is proposed based on traffic data image [44]. Encrypted network traffic [45] can be classified using behavioral classification. CNN is used for feature extraction, feature selection and classification. The automatic non-linear relationship between the input and output is mapped based on the behavioral profile of the end hosts. The relationship between the flows [46] is used to classify the traffic. This reduces the number of packets used in classification of flows.

4.5 Other classification Models

The changing nature of network traffic [47] makes the classification task complex. For accurate classification of

network traffic, training and test dataset should have identical features. For different features, maximum entropy based model is used as base classifier in the transfer learning model. The stateless nature of User Datagram Protocol (UDP) [48] makes traffic classification hard. It analyses the statistical properties of UDP and Internet Control Message Protocol (ICMP) and uses vector machines for classification. The salient features hidden in the multimedia traffic [49] helps in the

accurately differentiation network traffic. The stacked encoder model is used to learn relevant features of multimedia traffic. Filter wrapper feature selection [56] selects robust features that represents minority classes resistant to concept drift. A self learning classifier [57], a unsupervised algorithm with adaptive seeding to automatically let classes of traffic emerge, being identified and labeled. It will automatically group flows into homogeneous clusters using simple statistical features. Correlation based flow classification [58] reduces sampling overhead with estimation of arrival time of elephant flows. The supervised learning algorithm classifies the flow and provides dynamic scheduling of elephant and mice flows. Flow level features of online traffic are classified using C4.5 decision tree classifier [59]. Entropy based minimum description length discretization algorithm achieves higher accuracy rate. Fingerprinting algorithm maps larger data items to smaller bit strings, its fingerprint which uniquely identifies the original data [60]. For single content addressable memory, it provides high efficient sampling for TCP flows. It can accommodate dynamic network conditions such as congestion, retransmission, varying network loads, delay, fragmentation and duplication. Hybrid deep learning model based on Bi-directional LSTM – LSTM provides higher classification accuracy than support vector machine [61]. CNN and Weight dropped LSTM hybrid deep learning model is used in big data networking environment [62]. Deep CNN is used to extract highly correlated features from big intrusion detection environment. To prevent overfitting of recurrent data, LSTM is is applied to retain long term dependencies among extracted features. To resolve imbalance in data, data gravitation based method is used [63]. The hybrid model of traffic classification is shown in Table 3.

Table 3 *Deep Learning based traffic classification Model (hybrid)*

Ref	Classification Model	Contributions
[47]	Transfer Learning Model	• Distinct features in training dataset and test dataset • Improved the learning ability of the prediction function • Transfer learning model will dynamically learn the traffic and classify the new kind of traffic
[48]	Hybrid classifier based on pattern of arrival – incremental learning	• Applied for connectionless traffic • Classify high and low rate attack traffics • Supervised classifier for detecting the attacks and unsupervised classifier for payload threats inspection
[50]	Efficient feature optimization approach using deep learning and feature selection technique	• Addresses multi-class imbalance problem • Uses DBN classifier • Handles the problem of drift of Internet traffic • Can handle high dimensionality traffic
[51]	Multimodal deep learning classifier	• Automatic extraction of features from multifaceted traffic • It is a multi-class traffic classification technique
[52]	Kernel based Extreme Machine learning	• Uses wavelet function as activation function • Optimized feature selection through genetic algorithm • Classification using Kernel based extreme learning classifier
[53]	Support Vector Machine classifier	• Extract multi fractal features from traffic flow using wavelet leaders multi fractal formalism • Optimized selection of features using principal component analysis • Classification using support vector machine
[54]	Datanet	• Multilayer Perceptron based classifier • Stacked autoencoder • CNN based classifier
[55]	Transfer Learning and One-shot learning	• Traffic classification based on multi-output deep neural network • Common knowledge from common layers

5 DISCUSSION

Traffic classification is a complex process due to influence of various parameters like traffic collection, classifier accuracy, learning algorithms and so on. From the related works of traffic classification using deep learning in SDN environment, the following issues has to solved with further research

- The traffic classifier must deal with big volume of data (Big Data) with increasing rate of traffic and traffic transmission rate
- The classifier algorithms are computational intensive. Light weight classifier algorithm is needed
- The growing needs of traffic encryption and protocol encapsulation pose a challenge on traffic classification
- New class of traffic being developed which is hard for the classification

6 SUMMARY

Cyber attacks and cyber crimes are providing challenges to identify the security hole. Traffic classification is the base for filtering the unwanted traffic by the security wall. This paper provides a cross field review on the traffic classification. IP traffic classifications based on deep learning architecture provides the way for handling Big data. SDN is enhancing the traffic classification through its inherent nature of programmability, global view of network and dynamic updation of flow table. The different DL architectures are reviewed and based on application, hybrid DL models can

be employed. Thus this discussion and exploration opened an avenue for development of SDN and implement of more intelligent network.

REFERENCES

[1] J. A. Wickboldt, W. P. De Jesus, P. H. Isolani, C. B. Both, J. Rochol, and L. Z. Granville, "Software-defined networking: management requirements and challenges," IEEE Communications Magazine, vol. 53, pp. 278-285, 2015.

[2] A. Mestres, A. Rodriguez-Natal, J. Carner, P. Barlet-Ros, E. Alarcón, M. Solé, et al., "Knowledge-defined networking," ACM SIGCOMM Computer Communication Review, vol. 47, pp. 2-10, 2017.

[3] I. Goodfellow, Y. Bengio, and A. Courville, Deep learning: MIT press, 2016.

[4] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, C. Wang, et al., "A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges," IEEE Communications Surveys & Tutorials, vol. 21, pp. 393-430, 2018.

[5] F. Hu, Q. Hao, and K. Bao, "A survey on software-defined network and openflow: From concept to implementation," IEEE Communications Surveys & Tutorials, vol. 16, pp. 2181-2206, 2014.

[6] C.-L. Hsieh, N. Weng, and W. Wei, "Scalable Many-Field Packet Classification for Traffic Steering in SDN Switches," IEEE Transactions on Network and Service Management, vol. 16, pp. 348-361, 2018.

[7] A. Mendiola, J. Astorga, E. Jacob, and M. Higuero, "A survey on the contributions of software-defined networking to traffic engineering," IEEE Communications Surveys & Tutorials, vol. 19, pp. 918-953, 2016.

[8] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," IEEE Communications Surveys & Tutorials, vol. 17, pp. 2317-2346, 2015.

[9] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," IEEE Communications Surveys & Tutorials, vol. 18, pp. 602-622, 2015.

[10] P. C. da Rocha Fonseca and E. S. Mota, "A survey on fault management in software-defined networks," IEEE Communications Surveys & Tutorials, vol. 19, pp. 2284-2321, 2017.

[11] Y. Sung, P. Sharma, E. Lopez, and J. Park, "FS-OpenSecurity: a taxonomic modeling of security threats in SDN for future sustainable computing," Sustainability, vol. 8, p. 919, 2016.

[12] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," Ieee Access, vol. 5, pp. 21954-21961, 2017.

[13] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep recurrent neural network for intrusion detection in sdn-based networks," in 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), 2018, pp. 202-206.

[14] A. Azzouni, R. Boutaba, and G. Pujolle, "NeuRoute: Predictive dynamic routing for software-defined networks," in 2017 13th International Conference on Network and Service Management (CNSM), 2017, pp. 1-6.

[15] A. Azzouni and G. Pujolle, "NeuTM: A neural network-based framework for traffic matrix prediction in SDN," in NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1-5.

[16] Y. Zeng, H. Gu, W. Wei, and Y. Guo, "$ Deep-Full-Range $: A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework," IEEE Access, vol. 7, pp. 45182-45190, 2019.

[17] Y. He, F. R. Yu, N. Zhao, V. C. Leung, and H. Yin, "Software-defined networks with mobile edge computing and caching for smart cities: A big data deep reinforcement learning approach," IEEE Communications Magazine, vol. 55, pp. 31-37, 2017.

[18] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), 2016, pp. 258-263.

[19] A. Mozo, B. Ordozgoiti, and S. Gomez-Canaval, "Forecasting short-term data center network traffic load with convolutional neural networks," PloS one, vol. 13, p. e0191939, 2018.

[20] F. Tang, Z. M. Fadlullah, B. Mao, and N. Kato, "An intelligent traffic load prediction-based adaptive channel assignment algorithm in SDN-IoT: A deep learning approach," IEEE Internet of Things Journal, vol. 5, pp. 5141-5154, 2018.

[21] R. Vinayakumar, K. Soman, and P. Poornachandran, "Applying deep learning approaches for network traffic prediction," in 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 2353-2358.

[22] H.-K. Lim, J.-B. Kim, K. Kim, Y.-G. Hong, and Y.-H. Han, "Payload-Based Traffic Classification Using Multi-Layer LSTM in Software Defined Networks," Applied Sciences, vol. 9, p. 2550, 2019.

[23] Y. Qin, J. Wei, and W. Yang, "Deep Learning Based Anomaly Detection Scheme in Software-Defined Networking," in 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2019, pp. 1-4.

[24] D. Zhang, F. R. Yu, and R. Yang, "A Machine Learning Approach for Software-Defined Vehicular Ad Hoc Networks with Trust Management," in 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1-6.

[25] D. Arivudainambi, V. K. KA, and S. S. Chakkaravarthy, "LION IDS: A meta-heuristics approach to detect DDoS attacks against Software-Defined Networks," Neural Computing and Applications, vol. 31, pp. 1491-1501, 2019.

[26] H. Yao, P. Gao, J. Wang, P. Zhang, C. Jiang, and Z. Han, "Capsule Network Assisted IoT Traffic Classification Mechanism for Smart Cities," IEEE Internet of Things Journal, 2019.

[27] P. K. Sharma, S. Singh, and J. H. Park, "OpCloudSec: open cloud software defined wireless network security for the Internet of Things," Computer Communications, vol. 122, pp. 1-8, 2018.

[28] A. Dawoud, S. Shahristani, and C. Raun, "Deep learning and software-defined networks: towards secure Iot architecture," Internet of Things, vol. 3, pp. 82-89, 2018.
[29] F. Kong, J. Li, B. Jiang, and H. Song, "Short-term traffic flow prediction in smart multimedia system for Internet of Vehicles based on deep belief network," Future Generation Computer Systems, vol. 93, pp. 460-472, 2019.
[30] W. Huang, G. Song, H. Hong, and K. Xie, "Deep architecture for traffic flow prediction: deep belief networks with multitask learning," IEEE Transactions on Intelligent Transportation Systems, vol. 15, pp. 2191-2201, 2014.
[31] N. Al Khater and R. E. Overill, "Network traffic classification techniques and challenges," in 2015 Tenth International Conference on Digital Information Management (ICDIM), 2015, pp. 43-48.
[32] T. Bakhshi and B. Ghita, "On internet traffic classification: A two-phased machine learning approach," Journal of Computer Networks and Communications, vol. 2016, 2016.
[33] F. Risso, M. Baldi, O. Morandi, A. Baldini, and P. Monclus, "Lightweight, payload-based traffic classification: An experimental evaluation," in 2008 IEEE International Conference on Communications, 2008, pp. 5869-5875.
[34] J.-S. Park, S.-H. Yoon, and M.-S. Kim, "Software architecture for a lightweight payload signature-based traffic classification system," in International Workshop on Traffic Monitoring and Analysis, 2011, pp. 136-149.
[35] J. Zhang, Y. Xiang, W. Zhou, and Y. Wang, "Unsupervised traffic classification using flow statistical properties and IP packet payload," Journal of Computer and System Sciences, vol. 79, pp. 573-585, 2013.
[36] C. Yu, J. Lan, J. Xie, and Y. Hu, "QoS-aware traffic classification architecture using machine learning and deep packet inspection in SDNs," Procedia computer science, vol. 131, pp. 1209-1216, 2018.
[37] D. Sanvito, D. Moro, and A. Capone, "Towards traffic classification offloading to stateful SDN data planes," in 2017 IEEE Conference on Network Softwarization (NetSoft), 2017, pp. 1-4.
[38] S. Jeong, D. Lee, J. Choi, J. Li, and J. W.-K. Hong, "Application-aware traffic management for OpenFlow networks," in 2016 18th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2016, pp. 1-5.
[39] P. Xiao, W. Qu, H. Qi, Y. Xu, and Z. Li, "An efficient elephant flow detection with cost-sensitive in SDN," in 2015 1st International Conference on Industrial Networks and Intelligent Systems (INISCom), 2015, pp. 24-28.
[40] S. Ogasawara and Y. Takahashi, "Performance analysis of traffic classification in an OpenFlow switch," in 2016 Cloudification of the Internet of Things (CIoT), 2016, pp. 1-6.
[41] A. S. Da Silva, C. C. Machado, R. V. Bisol, L. Z. Granville, and A. Schaeffer-Filho, "Identification and selection of flow features for accurate traffic classification in SDN," in 2015 IEEE 14th International Symposium on Network Computing and Applications, 2015, pp. 134-141.
[42] P. Wang, S.-C. Lin, and M. Luo, "A framework for QoS-aware traffic classification using semi-supervised machine learning in SDNs," in 2016 IEEE International Conference on Services Computing (SCC), 2016, pp. 760-765.
[43] D. Rossi and S. Valenti, "Fine-grained traffic classification with netflow data," in Proceedings of the 6th international wireless communications and mobile computing conference, 2010, pp. 479-483.
[44] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," in 2017 International Conference on Information Networking (ICOIN), 2017, pp. 712-717.
[45] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, "End-to-end encrypted traffic classification with one-dimensional convolution neural networks," in 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017, pp. 43-48.
[46] L. Ding, J. Liu, T. Qin, and H. Li, "Internet traffic classification based on expanding vector of flow," Computer Networks, vol. 129, pp. 178-192, 2017.
[47] G. Sun, L. Liang, T. Chen, F. Xiao, and F. Lang, "Network traffic classification based on transfer learning," Computers & electrical engineering, vol. 69, pp. 920-927, 2018.
[48] V. Punitha and C. Mala, "Traffic classification for connectionless services with incremental learning," Computer Communications, 2019.
[49] Z. Wang, S. Mao, and W. Yang, "Deep learning approach to multimedia traffic classification based on QoS characteristics," IET Networks, vol. 8, pp. 145-154, 2018.
[50] H. Shi, H. Li, D. Zhang, C. Cheng, and X. Cao, "An efficient feature generation approach based on deep learning and feature selection techniques for traffic classification," Computer Networks, vol. 132, pp. 81-98, 2018.
[51] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapè, "MIMETIC: Mobile encrypted traffic classification using multimodal deep learning," Computer Networks, vol. 165, p. 106944, 2019.
[52] F. Ertam and E. Avcı, "A new approach for internet traffic classification: GA-WK-ELM," Measurement, vol. 95, pp. 135-142, 2017.
[53] H. Shi, H. Li, D. Zhang, C. Cheng, and W. Wu, "Efficient and robust feature extraction and selection for traffic classification," Computer Networks, vol. 119, pp. 1-16, 2017.
[54] P. Wang, F. Ye, X. Chen, and Y. Qian, "Datanet: Deep learning based encrypted network traffic classification in sdn home gateway," IEEE Access, vol. 6, pp. 55380-55391, 2018.
[55] H. Sun, Y. Xiao, J. Wang, J. Wang, Q. Qi, J. Liao, et al., "Common Knowledge Based and One-Shot Learning Enabled Multi-Task Traffic Classification," IEEE Access, vol. 7, pp. 39485-39495, 2019.
[56] F. A. M. Zaki and T. S. Chin, "FWFS: Selecting Robust Features Towards Reliable and Stable Traffic Classifier in SDN," IEEE Access, vol. 7, pp. 166011-166020, 2019.
[57] L. Grimaudo, M. Mellia, E. Baralis, and R. Keralapura, "Select: Self-learning classifier for internet traffic," IEEE

Transactions on Network and Service Management, vol. 11, pp. 144-157, 2014.
[58] F. Tang, H. Zhang, L. T. Yang, and L. Chen, "Elephant Flow Detection and Differentiated Scheduling with Efficient Sampling and Classification," IEEE Transactions on Cloud Computing, 2019.
[59] D. Tong, Y. R. Qu, and V. K. Prasanna, "Accelerating decision tree based traffic classification on FPGA and multicore platforms," IEEE Transactions on Parallel and Distributed Systems, vol. 28, pp. 3046-3059, 2017.
[60] J. Kampeas, A. Cohen, and O. Gurewitz, "Traffic classification based on zero-length packets," IEEE Transactions on Network and Service Management, vol. 15, pp. 1049-1062, 2018.
[61] F. Ertam, "An efficient hybrid deep learning approach for internet security," Physica A: Statistical Mechanics and its Applications, vol. 535, p. 122492, 2019.
[62] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, "A Hybrid Deep Learning Model for Efficient Intrusion Detection in Big Data Environment," Information Sciences, 2019.
[63] L. Peng, H. Zhang, Y. Chen, and B. Yang, "Imbalanced traffic identification using an imbalanced data gravitation-based classification model," Computer Communications, vol. 102, pp. 177-189, 2017.