Mitigation of Distributed Denial of Service (DDoS) Attacks over Software Defined Networks (SDN) using Machine Learning and Deep Learning Techniques

Ancy Sherin Jose, Latha R Nair, Varghese Paul

Abstract*: *Software Defined Networking (SDN) is an emerging networking paradigm which enables network control to be confined to a logically centralized controller. This enables global visibility of network and easier network management. The capability to program network through high level programming languages makes SDN a suitable network model to be extensively deployed in live environments. Still SDN is subject to several network attacks, among which DDoS - Distributed Denial of Service attack is the most prominent one. Controller which is the brain of SDN can be paralyzed by a high scale DDoS attack. Security of SDN is in immature state and considerable research is done in this area by both industry and academia. This paper focuses on the SDN DDoS mitigation techniques using Machine Learning (ML) and Deep Learning (DL) techniques. Network traffic features for determining DDoS are also surveyed in this work.

Index Terms*: *Software Defined Networking, SDN, Machine Learning - ML, Deep Learning - DL, DDoS attacks

I. INTRODUCTION

DDoS (Distributed Denial of Service) attack is a critical network security threat, which is a hot research area in the Network Security domain. The difficulty in identifying the attack pattern, the variety of free attack traffic generation tools available in market, difficulty to trace-back spoofed attack source address promote the launch of DDoS attacks even by novice attackers. The major aim of DDoS attack is to disrupt the services to legitimate users which in turn causes financial losses and reputational injuries to victim/target companies.

DDoS attacks can make use of protocol or application vulnerabilities to send malformed packets to the victim which is called a protocol attack. Ping of Death Attack is such a kind of attack. In the other kind of attack which is called DDoS Flooding attack, the victim gets overloaded with messages sent to it. The victim therefore, cannot provide services to the legitimate users [1]. By the usage of compromised hosts or botnets, large scale DDoS could be launched within minutes. Mirai and its variants [2] were disrupting the internet infrastructure and were used for launching DDoS in 2017. 2018 February marked the biggest DDoS attack which was targeted against GitHub, this was a memcached DDoS attack [3]. The size of DDoS attack is increasing and has crossed 100 Gbps in 2010 [4]. Therefore the development of defense frameworks against DDoS attack is today's necessity.

Traditional networks used middle boxes with integrated hardware and software, but the network configuration is rather complicated and vendor specific. Programmable interfaces offered by SDN helps to build network applications for defending DDoS attacks. The concept of centralized network control with global point of view, the promptness to add reactive/proactive flow rules within reasonable time limits helps SDN to be more defensive against DDoS attacks. The flow entries present in the flow table of switch decides the packet forwarding in SDN architecture. The flow entry in the SDN switch contains information like – duration, packet and byte count, protocol, source IP address, destination IP Address and ports [12]. Controller can collect the statistical messages from the switch, and can do necessary traffic analysis as needed. Whenever a packet reaches the network, dataplane devices or switches have to check its flow tables for the matching rules. The packets will be forwarded or dropped based on the actions associated with the matching rules [5]. In case of a table-miss, the packet will be directed to the controller. This happens during the incoming of a completely new type of packet. The controller – switch communication happens through a secure communication channel (TLS/SSL).

A group of bots can attack SDN, by sending the packets to unknown hosts for which flow rules does not exist in flow tables. In this case, the switches will have to pass the packet to the controller to get the rule to handle that packet. Many packets to unknown hosts or unknown destination IP address, will make numerous such requests to the controller, which will then get overloaded by processing. High volume of such packets can paralyze the controller. In effect, the legitimate traffic will suffer from severe network delays. Recently there are several works around to mitigate DDoS attack in SDN. They include architectural design considerations with redundancy of controllers, security

Revised Manuscript Received on December 22, 2018.

Ancy Sherin Jose, Department of Computer Science, Cochin University of Science and Technology Cochin, India.

Latha R Nair, Department of Computer Science, Cochin University of Science and Technology Cochin, India.

Varghese Paul, Department of Information Technology, Rajagiri School of Engineering and Technology, Kochi, India

network application development, network traffic analysis for pattern matching etc. Extensive works are done in Machine Learning and Deep Learning to detect the presence of DDoS attacks in SDN. This paper discusses about the ML and DL workarounds applied for DDoS detection and mitigation in SDN environment.

II. MACHINE LEARNING (ML) - AN OVERVIEW

Machine learning approaches are being implemented in SDN to overcome network security issues. ML algorithms are used to build implicit or explicit models from the given data [6]. The aim of ML is to build systems that can learn from data without being programmed. These kinds of systems help to find the hidden patterns and leads for better insights. The three categories of ML are Supervised, Unsupervised and Semi supervised Learning. Supervised Learning uses the labelled input data to acquire knowledge and uses this knowledge to classify unknown data [1]. Notable supervised algorithms are Decision Trees, SVM - Support Vector Machines, KNN - K-Nearest Neighbour , Random Forest etc. These algorithms are used for a variety of Classification, Prediction, and Regression problems. Unsupervised algorithms don't make use of labelled input data, instead these algorithms learn the underlying structure of the data to build models that predict/classify the unknown data. These algorithms mainly work either by computing distance or from similarity in the data. Clustering algorithms (K-means, K-medoids) and Principal Component Analysis (feature reduction technique) , SOM - Self Organizing Map are some examples [6]. Semi supervised algorithms use small amount of labeled and substantial amount of un-labeled data in the training phase. Semi supervised Support Vector Machine, Spectral Graph Transducer, Gaussian Fields approach are few examples. So ML focuses on a problem, centered on the properties or features it gained understanding from the training data [7]. Machine Learning algorithms gives a very high detection rate for Network Anomaly problems. The need for relevant information during training phase, the knowledge about the number of clusters required and resource consumption are the major drawbacks of these algorithms.[1]

III. DEEP LEARNING (DL) - AN OVERVIEW

Deep Learning (DL) also stated as Deep Feature / Representation Learning is a branch of ML that includes smaller subset of Machine Learning techniques [8] that exploit the abundant and affordable computation [6]. DL resembles human neuron's learning process which organizes ideas in hierarchical fashion. Building a computational model with high level abstractions is accomplished with multiple layers of generalizations in a DL algorithm. Deep Learning gained high momentum with the launch of Greedy Layer wise Unsupervised training. DL is in fact a nonlinear multi neuron, multilayer neural network [8]. The same input data is subject to be learned by multiple neurons instantiated with different weights parallely. Multiple hidden layers of neurons process the input data to provide the classified / regressed output. The type of neurons and layers of neurons depends on function. The basic neuron is a sigmoid neuron, but other types can be implemented as activation functions. In each layer the previously learnt features undergo a transformation, and is served as input to next layer. DL is categorized into Supervised, Unsupervised and Reinforcement Learning. This categorization is based on the type of input data they work on. The supervised learning requires the input data to be fully labelled. Classification and Regression are the two main output tasks of Supervised Learning. Convolutional Neural Network (CNN) is an example of supervised learning technique. The dataset of an unsupervised learning is unlabelled. Dimensionality Reduction, Clustering, Density estimation are the main output tasks of the Unsupervised Learning. In Reinforcement learning, input dataset is not explicitly labelled. State transitions are optimized by giving rewards, in such a way that algorithm learns to take the best action at each state to achieve greater rewards [9].

The main difference between ML and DL techniques lies in the feature processing. ML needs a domain expert to extract the necessary features, but the DL works on automatically extracted features. ML performs well over small datasets, but DL algorithms are more suitable for large datasets. As DL includes multiple parallel matrix operations, GPU is largely used for optimized processing [10]. Deep Learning based approaches are found to outperform Machine Learning based techniques in several classification problems. The ability of DL to reduce/extract features from a high dimensional dataset in an unsupervised manner helps to achieve better accuracy without much domain knowledge. Machine learning and deep learning techniques are compared in Table 1.

Table I. Comparing Machine Learning & Deep Learning

Machine Learning	**Deep Learning**
a subset of Artificial Intelligence (AI) closely related to statistics	a subset of ML that uses models similar to human learning – Artificial Neural Networks
Hand picked features / Feature Engineering needed. [10]	Feature extraction is automatic. DL finds best features by itself. [10]
Single Layer training – No hidden layers. Training takes relatively small time. [8]	Layer by layer training. Training time is relatively high. [8]
ML algorithms perform well on small datasets. [10]	DL Algorithms needs large datasets to understand the data representations. [10]
Traditional ML algorithms work well on CPUs.	DL performs better on GPU as it has large number of matrix operations.
Learning from complex data representation is difficult for ML [9]	Better performance and accuracy achieved for complex data representations [9]

IV. BACKGROUND AND RELATED WORKS

This section reviews the latest research works in the context of detecting and mitigating DDoS over SDN using Statistical, Machine Learning and Deep Learning methods

A. *Use of statistical methods for detecting DDoS in SDN*

[11] makes use of statistical method entropy to detect the presence of DDoS attack. Entropy is a statistical property, which in general refers to randomness. This work prototypes a DNS Reflection Amplification attack. In order to reduce the controller load, this work makes use of network monitor (sflow) to inspect the network traffic and an orchestrator (a multi threaded server). Orchestrator periodically checks with network monitor for status and update messages about the network state and decides whether it needs more packets for detecting high resolution attacks. Entropy of the destination IP and Average Response Size are calculated by the orchestrator module. If the entropy is less than the predefined threshold and average Response size is greater than standard DNS Response size, the network is considered to be in attack state and Rate Limiting is applied by inserting rules. This work considers the flow shortening and flow reduction problems as well. In order to detect high resolution attacks, it considers full load of packets, while for low resolution attacks, it applies sampling.

[12] considers the entropy of the newly incoming packets to all the hosts in the network for a specific window size. In ideal case, all the hosts in the network should be having closely equal entropy. In case entropy decreases behind an experimentally fixed threshold, there is chance of attack. This work is carried out in a simulated environment with attack traffic generated using Scapy. Wang et al. [13] also calculates the entropy of incoming packets to a destination IP on the OpenFlow edge switch to detect the presence of DDoS attacks. This attempt brings some intelligence to the switches while it correctly discriminates between DDoS and flashcrowds. CAIDA DoS attack 2007 dataset is used in this work and D-ITG tool is used to create attack traffic. JESS [14] describes the need for considering other attributes for calculating entropy. This work calculates entropy not only based on destination IP but also Transport Layer attributes like port number. [15] calculates joint entropy for the features like duration, source IP, length of packet and port (destination) to detect DDoS attacks in SDN. This work tries to detect DDoS from spoofed and unspoofed source IP. Sahoo et al. [16] have used General Entropy and Generalized Information Distance (GID) on destination IP address to discriminate Flash Events from DDoS attacks.

B. *Machine Learning and DDoS Detection in SDN*

In [17] flow table status information is collected from the switch to extract the features which characterizes a DDoS attack. The controller periodically sends onpflowstats request message to the switch which responds with statistic values like packet count, byte count etc for the respective flow entries present in the switch. The controller collects six feature values to build the model which is based on SVM Classifier. This work was done on a Mininet simulated environment. TCP, UDP, ICMP Floods are created using HPing tool (traffic generator). Count of Source IP for unit time, Count of source port per unit time, Standard Deviation calculated for packets and bits count for a predetermined period, rate of flow entries per unit time, Percentage of pairwise flow entries are the 6 features / dimensions considered in this work. This work achieves detection accuracy of 95.24% with False Alarm Rate (FAR) noted as 1.26%. [18] uses two flow features which are packet number and duration of existence of a flow rule to detect DDoS attacks. The tendency to make DDoS attacks by sending large number of flows with a single flow containing high packet number is considered as Type 1 attack. The tendency to send packets from a variety of spoofed IP to pretend as a normal traffic is considered as the Type 2 attack. A Linear SVM is engaged as the classifier, which classifies the traffic as Normal, Type1 or Type 2. For Type 1 attack traffic, the flows are dropped by making the flow timeout value as zero. For Type 2 attack, the flows are deleted from the flow table. This work uses CAIDA Dataset for training the SVM classifier module. Kokila et al. [19] uses SVM classifier to perform multiclass classification. The classifier was trained with 2000 DARPA intrusion detection specific Dataset for attack data, and 1998 DARPA Dataset for normal traffic. This work achieved detection accuracy of 95.11% for SVM based DDoS classification. [20] adopts two stage classification of network traffic. First the traffic is classified with Naive Bayes Classifier, and the suspicious traffic is then again classified using SVM Classifier function. This two way classification helps to reduce the rate of false alarms.

In [5] flow packet average, and byte average are used as features and executes Rule Based Classification in the SDN controller. A table is maintained in the Controller which collects the information about the distinct IPs connected to a switch, the number of packets in each flow, payload size for the flow and duration of a flow entry in the flow table. Rules are made such that if the packet average and byte average for the flow is less than a predetermined threshold, the system is susceptible to DDoS attack and consequently flow rules are written to drop packets. The experiments are done using a simulated network with Mininet-Wifi. Braga et al. [21] uses SOM (Self Organizing Map) an artificial neural network which employs six tuple features to classify DDoS attack. The features include averages calculated for packets and bytes per flow, duration of a flow, Percentage of pair flows, rate of increase of single flows and ports. Some of these feature are cumulative over time. [22] uses trained SOM and KNN to classify DDoS and considers entropy of features like protocol, source IP Address, ports (source and destination), and packet size. [3] leverages WMA (Weighted Moving Average) with Pauta criterion in Gaussian distribution over traffic samples based on two features (Byte count/s, Packetcount/s) to predict a future value range. This is done by their flow monitoring algorithm in the dataplane device. If the current values fall within the predicted range then it estimates the current traffic as normal. In other case, fine grained Machine Learning algorithm which is a combined Autoencoder with softmax classifier is executed at control plane for attack classification based on real time extracted traffic features.

[2] combines NFV (Network Function Virtualization) along with ML algorithm to detect the presence of DDoS attacks in SDN. Data plane devices employ VNF (Virtual Network Functions) to detect network attacks and for monitoring traffic. One VNF is responsible for extracting feature information from the traffic and it sends them to the controller. Random Forest based attack model is built on controller, which detects the botnet attacks. This work attempts to collect real time network traffic information using Virtual Network Function other than relying on historical data. Wang et al. [23] leverages Renyi entropy of IPAddress (both source and destination) and combines it with Hidden Markov Model to get probabilistic representation to detect Low Rate Distributed Denial of Service attack (LDDoS). This work uses Euclidean distance for Renyi entropies and Viterbi algorithm for HMM-R decoding. [24] compares four different machine learning algorithms - K-nearest neighbour (KNN), Naive Bayes, K-Means, K-Medoids and lists the detection accuracy and processing time for each algorithm. Naive bayes achieves the high detection accuracy rate of 94%.

C. *DDoS Detection using Deep Learning*

[25] incorporates Stacked Autoencoder (SAE) based DL approach to detect DDoS attack in SDN environment. The sparsed encoders are stacked to each other for feature reduction and the output is fed to a softmax classifier to classify the traffic as normal or that of attack. The list of features relevant for TCP, UDP, ICMP traffics are collected through detailed literature survey and reduced in unsupervised manner using sparse encoder with the feature extractor module in their design. In order to reduce false alarms, this work relies on every packet. Li et al. [26] builds a deep learning defense model to completely clean the DDoS attack traffic. The model is built using Long Short Term Memory (LSTM), Recurrent Neural Network (RNN) and Convolutional Neural Network (CNN). This work is done on GPU and uses DeepLearning Framework Keras. Very little research has been done to detect DDoS in SDN environments using DL approaches. [27-31] are the DL based works done in SDN environment for Network Intrusion Detection.

DeepDefence [32] leverages Recurrent Neural Network (LSTM -Long Short-term Memory), CNN (Convolutional Neural Networks), GRU - Gated Recurrent Unit and builds model to detect DDoS attack over traditional network. They use UNB ISCX Intrusion Detection Evaluation 2012 Dataset which is a large dataset. Performance comparison of Recurrent Neural Network with Random Forest algorithm is also done in this work. [33] incorporates Stacked AutoEncoder deep learning architecture to detect Application Layer DDoS attacks. Web server logs are collected and features are extracted. Normalization of features to fit in the same range is done by Min-Max algorithm. Deep Learning Model is used to understand abstract features. Finally Logistic Regression is used to classify network traffic. [34] builds a DDoS detection model based on Gaussian-Bernoulli type Restricted Boltzmann Machine (RBM). Comparison between three deep learning algorithms (Bernouli-Bernouli, Gaussian-Bernouli, Deep Belief Network) and three machine learning models (Decision tree , SVM - Epsilon

Table II . DDoS Detection Traffic Features From Literature

Method	Technique / Algorithm	Features
Statistical	Entropy	Destination IP, Average Response Size [11]
		Newly incoming IPs [12][13]
		Destination IP, TCP Port Number [14]
		Source IP, Flow Duration, Packet Length, Destination Port [15]
	General Entropy and Generalized Information Distance (GID)	Destination IP [16]
Machine Learning	SVM	Count of flow entries per unit time, Count of distinct Source IP and Source Port for unit time, Ratio of pairwise flow entries to total entries , Standard Deviation calculated for count of packets and bits per period [17]
	Linear SVM	Packet number Duration of existence of a flow rule [18]
	Rule based Classification	Flow Packet Average, Byte Average [21]
	SOM	Averages :- duration for each flow entry bytes per flow packets per flow Percentage of pair flows Rate of increase in flows, ports [22]
	SOM & KNN	Entropy calculated for protocol, source IP Address, source and destination port packet size [23]
Deep Learning	Stacked Autoencoder (SAE) based and softmax classifier [25]	——
	RNN, CNN, LSTM [26]	——

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

SVR , Radial Basis) is also done in this work. The various DDoS detection techniques and the traffic features used for the detection are listed in Table II.

V.TOOLS

SDN is found to be simulated using Mininet [35] in the surveyed works. Scapy [36] is the commonly used tool for traffic generation. D-ITG (Distributed Internet Traffic Generator), Hping, Trafgen are other traffic generators. CTU-13 Datasets, CAIDA Datasets, 2000 DARPA Datasets, KDD Cup 99, NSL-KDD Datasets, UNB ISCX Intrusion Detection Evaluation 2012 Dataset are used in many works. POX, Floodlight, OpenDayLight, RYU controllers are the main SDN Controllers used in SDN research and industry. Scikit learn [37] and Matlab [38] are used for Machine Learning while TensorFlow engine [39], PyTorch [40] and Keras frameworks [41] are used for implementing Deep Learning algorithms.

VI. CONTRIBUTION

This work is mainly focused on surveying the DDoS detection and mitigation techniques using Machine Learning and Deep Learning. From the detailed survey done, it is clear that SDN openflowstats request feature can be effectively utilized for getting the required statistics which can be used as ML features. Amplification attacks which are capable of paralyzing the entire network can be efficiently detected by using the traffic features surveyed through this work. DNS Amplification attacks, NTP Amplification Attacks and Memcache attacks can be captured by applying the ML techniques over SDN. DL algorithms can be employed for automatic feature extraction for detecting these attacks, which will be the focus of our future work.

VII. CONCLUSION

The impact of DDoS attack is significant and can make the entire network down if not addressed properly. DDoS attacks are getting more and more sophisticated and they are capable of easily bypassing the traditional shielding techniques. Deep Learning techniques are becoming matured to form Knowledge Defined Networks. These algorithms are found to be more effective than their predecessor ML techniques in many classification problems. The exciting features of SDN can be augmented with the deep learning algorithms for intelligent mitigation of DDoS attacks.

REFERENCES

1. Jing, Xuyang, Zheng Yan, and Witold Pedrycz, Security Data Collection and Data Analytics in the Internet: A Survey. IEEE Communications Surveys Tutorials (2018)
2. Park, Younghee, Nikhil Vijayakumar Kengalahalli, and Sang -Yoon Chang, Distributed Security Network Functions against Botnet Attacks in Software-defined Networks
3. Famous DDoS attacks, https://www.cloudflare.com/learning/ddos/famous-ddos-attacks
4. Han, Biao, Xiangrui Yang, Zhigang Sun, Jinfeng Huang, and Jinshu Su. OverWatch: A Cross-Plane DDoS Attack Defense Framework with Col-laborative Intelligence in SDN. Security and Communication Networks 2018
5. Gkountis, Christos, et al., Lightweight algorithm for protecting SDN controller against DDoS attacks. Wireless and Mobile Networking Conference (WMNC), 2017 10th IFIP. IEEE, 2017.
6. Sultana, Nasrin, et al., Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications (2018): 1-9.
7. Buczak, Anna L., and Erhan Guven. , A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys Tutorials 18.2 (2016): 1153-1176.
8. Fadlullah, Zubair, et al. , State-of-the-art deep learning: Evolving machine intelligence toward tomorrows intelligent network traffic control systems. IEEE Communications Surveys Tutorials 19.4 (2017): 2432-2455.
9. Hatcher, William Grant, and Wei Yu. , A Survey of Deep Learning: Platforms, Applications and Emerging Research Trends. IEEE Access 6 (2018): 24411-24432.
10. Xin, Yang, et al. , Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access (2018).
11. Zaalouk, Adel, et al. , Orchsec: An orchestrator-based architecture for enhancing network-security using network monitoring and sdn control functions. Network Operations and Management Symposium (NOMS), 2014 IEEE. IEEE, 2014.
12. Mousavi, Seyed Mohammad, and Marc St-Hilaire. , Early detection of DDoS attacks against SDN controllers. Computing, Networking and Communications (ICNC), 2015 International Conference on. IEEE, 2015.
13. Wang, Rui, Zhiping Jia, and Lei Ju. , An entropy-based distributed DDoS detection mechanism in software-defined networking.Trust-com/BigDataSE/ISPA, 2015 IEEE. Vol. 1. IEEE, 2015.
14. Kalkan, Kbra, et al., JESS: Joint Entropy-Based DDoS Defense Scheme in SDN.IEEE Journal on Selected Areas in Communications 36.10 (2018): 2358-2372.
15. Mao, Jiewen, Weijun Deng, and Fuke Shen. , DDoS Flooding Attack Detection Based on Joint-Entropy with Multiple Traffic Features. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018.
16. Sahoo, Kshira Sagar, Mayank Tiwary, and Bibhudatta Sahoo. , Detection of high rate DDoS attack from flash events using information metrics in software defined networks. Communication Systems Networks (COMSNETS), 2018 10th International Conference on. IEEE,2018.
17. Ye, Jin, et al. , A DDoS Attack Detection Method Based on SVM in Software Defined Network. Security and Communication Networks 2018 (2018).
18. Phan, Trung V., et al. , OpenFlowSIA: An optimized protection scheme for software-defined networks from flooding attacks. Communications and Electronics (ICCE), 2016 IEEE Sixth International Conference on. IEEE, 2016.
19. Kokila, R. T., S. Thamarai Selvi, and Kannan Govindarajan. , DDoS detection and analysis in SDN-based environment using support vector machine classifier. Advanced Computing (ICoAC), 2014 Sixth International Conference on. IEEE, 2014.
20. Khemapatapan, Chaiyaporn. , 2-Stage Soft Defending Scheme Against DDoS Attack Over SDN Based on NB AND SVM.
21. Braga, Rodrigo, Edjard Mota, and Alexandre Passito. , Lightweight DDoS flooding attack detection using NOX/OpenFlow. Local Computer Networks (LCN), 2010 IEEE 35th Conference on. IEEE, 2010.
22. Nam, Tran Manh, et al. , Self-organizing map-based approaches in DDoS flooding detection using SDN. 2018 International Conference on Information Networking (ICOIN). IEEE, 2018.
23. Wang, Wentao, Xuan Ke, and Lingxia Wang , A HMM-R Approach to Detect L-DDoS Attack Adaptively on SDN Controller. Future Internet 10.9 (2018): 83
24. Barki, Lohit, et al. , Detection of distributed denial of service attacks in software defined networks. Advances in Computing, Communications and Informatics (ICACCI), 2016 International

Conference on. IEEE, 2016.
25. Niyaz, Quamar, Weiqing Sun, and Ahmad Y. Javaid. , A deep learning based DDoS detection system in software-defined networking (SDN). arXiv preprint arXiv:1611.07400 (2016).
26. Li, Chuanhuang, et al. , Detection and defense of DDoS attackbased on deep learning in OpenFlowbased SDN. International Journal of Communication Systems 31.5 (2018): e3497.
27. Tang, Tuan A., et al. , Deep learning approach for network intrusion detection in software defined networking.Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on.IEEE, 2016.
28. Wang, Wei, et al. , HAST-IDS: learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection IEEE Access 6 (2018): 1792-1806.
29. Ishitaki, Taro, et al. , Application of Deep Recurrent Neural Networks for Prediction of User Behavior in Tor Networks. Advanced Infor-mation Networking and Applications Workshops (WAINA), 2017 31st International Conference on. IEEE, 2017.
30. Javaid, Ahmad, et al. , A deep learning approach for network intrusion detection system. Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016.
31. Tang, Tuan A. , et al., Deep recurrent neural network for intrusion detection in sdn-based networks. 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft). IEEE, 2018.
32. Yuan, Xiaoyong, Chuanhuang Li, and Xiaolin Li. , DeepDefense: Identifying DDoS Attack via Deep Learning. 2017 IEEE International Conference on Smart Computing (SMARTCOMP). IEEE, 2017.
33. Yadav, Satyajit, and Selvakumar Subramanian. , Detection of Application Layer DDoS attack by feature learning using Stacked AutoEncoder. Computational Techniques in Information and Communication Technolo- gies (ICCTICT), 2016 International Conference on. IEEE, 2016.
34. Imamverdiyev, Yadigar, and Fargana Abdullayeva. , Deep Learning Method for Denial of Service Attack Detection Based on Restricted Boltzmann Machine. Big Data 6.2 (2018): 159-169.
35. About Mininet, http://mininet.org/ Accessed on 25/03/2019
36. About Scapy, https://scapy.net Accessed on 25/03/2019
37. About Scikit learn, https://scikit-learn.org/ Accessed on 25/03/2019
38. About Matlab, https://in.mathworks.com/products/matlab.html Accessed on 25/03/2019
39. About TensorFlow, https://www.tensorflow.org/ Accessed on 25/03/2019
40. About PyTorch, https://pytorch.org/ Accessed on 25/03/2019
41. About Keras, https://keras.io/ Accessed on 25/03/2019

AUTHORS PROFILE

Ancy Sherin Jose is doing research under division of Computer Science Engineering, Cochin University of Science And Technology. She is a B.Tech, M.Tech holder in Computer Science. Her research areas are SDN, Network Security, Machine Learning, Deep Learning and Big Data Analytics. She has published papers in the network security domain.

Latha R Nair is working as Associate Professor in the division of Computer Engineering, Cochin University of Science and Technology. She is a B.Tech, M.Tech and Ph.D. holder in Computer Science. She has published a number of papers in the areas of machine intelligence and natural language processing. She has done extensive research in Malayalam language computing. Her areas of interest are machine intelligence, natural language processing and image processing.

Varghese Paul is. working as Post Graduate Professor in Computer Science and Engineering Department, in Rajagiri School of Engineering and Technology. His research areas are Data security using Cryptography, Data Compression, Data Mining, Image Processing and E_Governance. He is the developer of TDMRC Coding System for character representation and encryption system using this coding system. He has got many research publications in international as well as national journals. He is a Certified Software Test Manager, Ministry of Information Technology, Government of India. Also, member of Information System Audit and Control Association, USA and Indian Society for Technical Education, India.