International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

AN INITIATIVE WORK ON SDN BASED NETWORK INTRUSION DETECTION SYSTEM USING MACHINE LEARNING.

Shivam Tiwari, Vanshika Pandita, Samarth Sharma, Vishal Dhande, Shailesh Bendale

[1-4]*B.E student, Dept. of Computer Engineering, NBN Sinhgad School of Engineering, Maharashtra, India*
[5]*Professor, Dept. of Computer Engineering, NBN Sinhgad School of Engineering, Maharashtra, India*

Abstract - *Software Defined Network Technology gave us the best way possible to identify and record several problems which regards network security. SDN ensures that our system is secure from every possible attack. Various ML techniques are used for monitoring traffics from all the devices present on the network. NIDS is use to safeguard the various networks and helps us to prevail over network security issues. Deep learning which comes under the advance machine learning techniques is also used in SDN based environment. In this survey paper, we have made reference to some of the works done on the topic of machine learning techniques which support Software Define Network based environment to apply Network intrusion detection system. In this survey, we have learn various equipment which will help us to achieve an established model of Network Intrusion Detection System. For implementation purposes we will try to increase the accuracies of network intrusion detection using the two algorithms mentioned in this paper.*

Key Words: NIDS, SDN, SDWN, DDoS, ML, LSTM, ANN etc.

1. INTRODUCTION

1.1 Software Defined Network

Software Defined Network is developed through a centralize network topology which provides us the management of network resources and there intelligence control. By the help of these kind of centralize and intelligent control factors which include bandwidth managements, Cyber securities, repairing and policies can be highly refined through Software Defined Network Environment. SDN architecture has two planes which are control planes and data planes which are separated from each other and make the packet transmitting far simpler. SDN has some set of principles which aim to create an adaptable, more flexible and highly effective network via software based configuration**.** Inside Software Defined Network Architecture southbound APIs are use as the communication tool b/w Software Defined Network controllers, routers and switches. A northbound interface allows us to communicate b/w a particular component and higher level of components in the network.

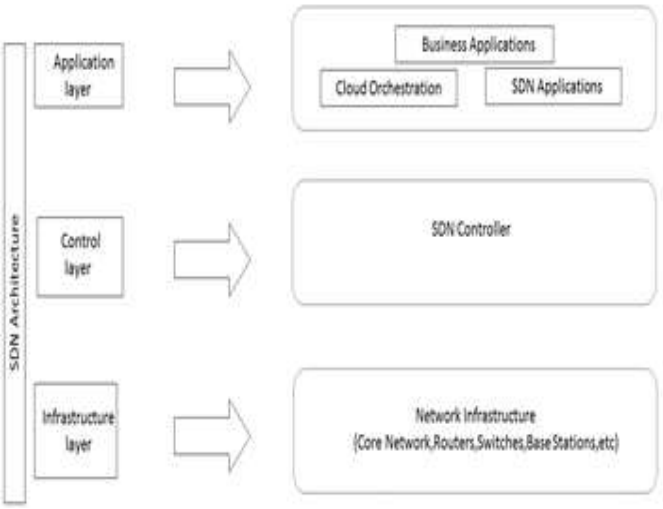

Fig. 1 SDN Architecture

1.2 Software Defined Wireless Network

The expansion in the use of mobiles, computers and other services results in the rise in requirement for effective services. These requirements generate new demands for the architecture of current network like resilience in managing and configuring the network architecture, versatility and the independence of the dealer. For meeting these demands and requirements, software defined wireless network is an adequate solution. With the use of SDWN, we can build a platform delivering services to the users according to their requirements. Software defined wireless network architecture can also be used in coming years which will help to resolve issues like excessive subscribers, continual mobility. This architecture intends to bring the advantages of logical composition. It provides the access of internet services even when there is a lot of data traffic on the network and also under the use of excess applications. To use the advantages of software defined network in networks that are wireless, software defined wireless network is given a thought.

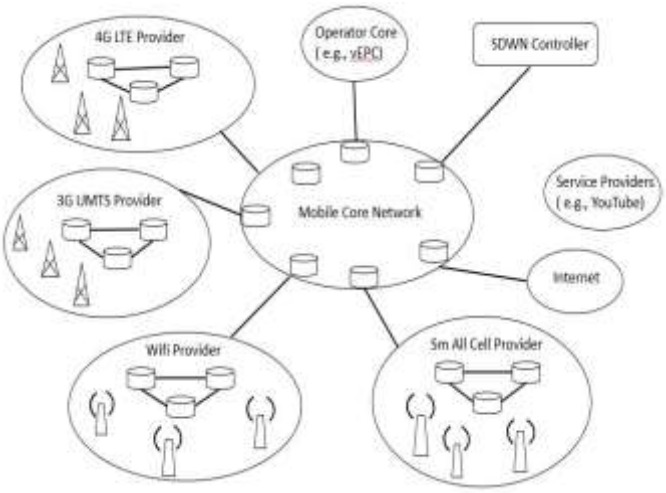

Fig. 2 SDWN Architecture

2. DDoS ATTACK

DDoS is an ill-natured effort to distort the usual traffic for an aimed server or network which makes the target and the infrastructure around it accompanied by large amount of internet traffic. The machines which are exploited include all the computers and other resources of networks which include IOT devices. In this attack, the attacker gets full command over the mesh of online machines to implement the attacks. Machines are contaminated with the virus converting each machine into a bot. The invader then remotely controls a huge number of bots. Once a botnet is created, then the attacker will be able to control the systems by giving commands to each bot by using remote control. Once the network identity number of the acquired target is noted by the running bots. Each botnet responds when it sends message to the target, which causes the potential target server to spill capacity which results in the refuses to provide the service to the general traffic. It is caused as every bot is reasonable internet device which makes separation of normal attack and attack traffic very difficult.

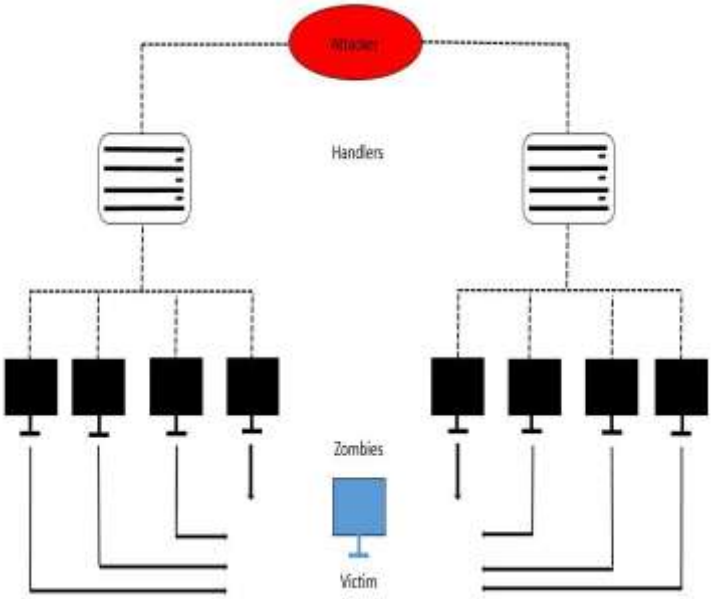

Fig 3. DDoS Architecture

3. LITERATURE SURVEY

Some of the papers that we have studied are discussed are shown below:

The authors Nasrin Sultana, Naveen Chilamkurti, Wei Peng and Rabeialhadad have discussed the various challenge which happen during implementation of NIDS using many ML and DL practices. Also, we can see that it tells us about the techniques of DL in making Software Defined Network based Network intrusion detection system and the tools which can be used to develop network intrusion detection system model in SDN environment that will help to detect various network related problems. Overall, it provides us a summary of programmable networks and explore the field of SDN.

The three authors Gang Wang, Jinxing Hao, Jian Ma and Lihua Huang [2] have discussed a type of technique known as FC-ANN based on Artificial neural network and Fuzzy Clustering to get very less detection time, stronger stable model and less false positive detection rate .FC-ANN is proposed to overcome various limitations which are present in ANN based IDS. It reduces the difficulties of the training dataset and increases the detection performance measure.

The authors Lindinkosi L. Zulu, Kingsley A. Ogudo and Patrice O. Umenne [3] have discussed the importance of Mininet to acquire SDN to illustrate the various abilities of Mininet Wifi to be used as the Software defined network equal and then it can also be linked to a network virtualized

function. This paper throws light upon the Mininet research integration with other technologies.

Wei Wang, Yinjie Chen, Qian Zhang and Tao Jiang [4] have discussed the benefits and advantages of Software Defined Wireless Network while keeping the features of small grained channelization. This paper throws light upon the principles and challenges for the realization of SDWN enabled spectrum management architecture. They have discussed a general architecture by keeping these challenges and principles in mind.

The author Fernando M.V. Ramos, Diego Kreutz, Paulo Esteves Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky and Steve Uhlig have discussed the use of Software Defined Network paradigm which breaks the process vertical integration and separates the network control logic with the router and switches that results in the reduction of complexity and easy management of networks. This paper gives the overview of SDN with its pros and cons.

Ramon Fantes, Samira Afzal, Mateus Augusto Silva Santos and Christian Esteve Rothenberg [6] have discussed the use of mininet wifi tool to emulate Wireless SDN scenarios. This paper gives an overview of the applications, benefits and limitations of Mininet Wifi.

4. LONG SHORT TERM MEMORY

LSTM networks are recurrent neural networks capable of predicting sequence problems. Long short term memory are a very complex area in the field of deep learning. Not only does it processes many individual data points but it also processes the entire sequence of data. Long Short-Term Memory (LSTM) can solve numerous tasks not solvable by previous learning algorithms for recurrent neural networks (RNNs*)*. These 3 gates coordinate the information flow in and out of the cells and the cells remember value over the arbitrary intervals of the time. LSTM networks are used with the purposes of predictions, classifications and also processing dependent on data of time series. LSTM deals with Vanishing Gradient problem which can be seen when we are training the traditional RNNs.

5. ARTIFICIAL NEURAL NETWORK

ANN is dependent on the collection of various small computational units which are known as artificial neurons. These neurons are connected in a very complex structure. An artificial neuron processes the signals received and also can signal neurons which are connected to it. Artificial Neural Network helps us to know the effects from increasing and decreasing the dataset horizontally as well as vertically on computational time. It helps us to understand best situations and also best cases in which the model fits in the best possible way. It is completely related and similar to the human nervous system. . Artificial Neural Network is used very rarely when it comes to predicting the model. ANN is used in such cases where things happened in the past can be used and repeated in the exact similar way.

6. RESULT

Predicted Class	P	N
Actual Class: P	TP 4676	FN 324
Actual Class: N	FP 668	TN 4332

Fig 4. Confusion matrix for LSTM

		Predicted Class: P	Predicted Class: N
Actual Class	P	TP 4352	FN 648
	N	FP 666	TN 4334

Fig 5. Confusion matrix for ANN

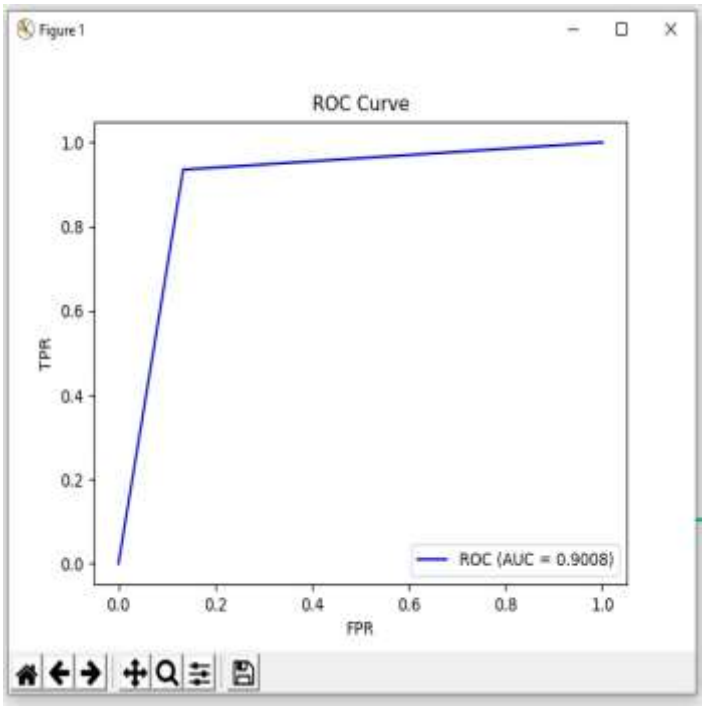

Chart -1: Receiver operating characteristic curve

```
Python 3.5.2 Shell
File Edit Shell Debug Options Window Help
Python 3.5.2 (v3.5.2:4def2a2901a5, Jun 25 2016, 22:18:55) [MSC v.1900 64 bit (AM
D64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
==== RESTART: J:\4_D Projects\2019_20\BE_IPG_NBN_IDS\RES\RESULTCODE_P2.py ====
------------------- LSTM ---------------------------------
population: 10000
P: 5000
N: 5000
PositiveTest: 5344
NegativeTest: 4656
TP: 4676
TN: 4332
FP: 668
FN: 324
TPR: 0.9352
TNR: 0.8664
PPV: 0.875
NPV: 0.9304123711340206
FPR: 0.1336
FDR: 0.125
FNR: 0.0648
ACC: 0.9008
F1_score: 0.9040989945862336
MCC: 0.8035039245087923
informedness: 0.8016000000000001
markedness: 0.8054123711340206
prevalence: 0.5
LRP: 7.0
LRN: 0.07479224376731301
DOR: 93.5925925925926
FOR: 0.06958762886597938
col_0     0     1
row_0
0.0    4332   668
1.0     324  4676
```

```
Python 3.5.2 Shell
File Edit Shell Debug Options Window Help
FOR: 0.06958762886597938
col_0     0     1
row_0
0.0    4332   668
1.0     324  4676

------------------- ANN ---------------------------------
population: 10000
P: 5000
N: 5000
PositiveTest: 5018
NegativeTest: 4982
TP: 4352
TN: 4334
FP: 666
FN: 648
TPR: 0.8704
TNR: 0.8668
PPV: 0.8672777999202871
NPV: 0.8699317543155359
FPR: 0.1332
FDR: 0.13272220007971303
FNR: 0.1296
ACC: 0.8686
F1_score: 0.8688360950289479
MCC: 0.7372047771024335
informedness: 0.7372000000000001
markedness: 0.737209554235823
prevalence: 0.5
LRP: 6.534534534534534
LRN: 0.1495154591601292
DOR: 43.70474177881585
FOR: 0.13006824568446407
col_0     0     1
row_0
0.0    4334   666
1.0     648  4352

----------------------------------------------------------
```

7. CONCLUSION

Hence, we studied about the SDN based Intrusion Detection system which will be used to detect the network security issues whenever an intrusion takes place in the network. In addition to this we have discussed the two efficient algorithms. For implementation we are trying to increase the accuracy of network intrusion detection using the two algorithms stated in this paper

8. REFERENCES

[1] Nasrin Sultana, Naveen Chilamkurti, Wei Peng and Rabeialhadad ,"Survey on SDN based network intrusion detection system using machine learning approaches", Research gate,2018.

[2] Gang Wang, Jinxing Hao, Jian Ma and Lihua Huang," a new approach to intrusion detection using ANN and Fuzzy clustering", ESWA, 2010.

[3] Lindinkosi L. Zulu, Kingsley A. Ogudo and Patrice O. Umenne, "Simulating software defined networking using mininet to optimize host communication in a realistic programmable network", IEEE, 2018.

[4] Wei Wang, Yinjie Chen, Qian Zhang and Tao Jiang,"A software defined wireless network enabled spectrum management architecture" IEEE, 2015.

[5] Fernando M.V. Ramos, Diego Kreutz, Paulo Esteves Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky and Steve Uhlig, "Software defined networking : A Comprehensive Survey".

[6] Ramon Fantes, Samira Afzal, Mateus Augusto Silva Santos and Christian Esteve Rothenberg, "Mininet Wifi emulating software defined wireless networks", Research gate,2015.

[7] Sydney Mabwe Kasongo and Yanxia Sun,"A deep long short term memory based classifier for wireless intrusion detection system", ICTE, 2019.

[8] S.P. Bendale and J. R. Prasad,"Security threats and challenges in future mobile wireless networks", (GCWCN) 2018.

[9] A. S. Patil, P.S. Jain, R.G. Ram, V.N. Vayachal and S.P. Bendale, "Detection of distributed denial of service attack on SDN",(IRJET) 2018.

[10] Siddhant Shah , Shailesh Bendale, "An Intuitive study: Intrusion Detection system and anomalies, how AI can be used as a tool to enable the majority, in 5G era, ICCUBEA, 2019.

[11] Chinmay Dharmadhikari, Salil Kulkarni, Swarali Temkar, Shailesh Bendale ," A Study of DDoS Attacks in Software Defined Networks" (IRJET) 2019.

[12] Shailesh P Bendale, Jayashree R Prasad,"Security Threats and Challenges in Future Mobile Wireless Networks", - 2018 IEEE Global Conference on Wireless Computing Network (GCWCN), 2018.

[13] Siddhant Shah and Shailesh Bendale, "An Intuitive Study: Intrusion Detection Systems and
Anomalies, How AI can be used as a tool to enable the majority, in 5G era." IEEE ICCUBEA (2019).

[14] Shailesh P. Bendale; Girish V. Chowdhary," Stable path selection and safe backup routing for Optical Border Gateway Protocol (OBGP) and Extended Optical Border Gateway Protocol (OBGP+)", IEEE ICCICT , 2012.

[15] Shailesh P. Bendale, Jayashree Rajesh Prasad, "Challenges in Design of Intelligent and Secure SDN", SITSFIST 2020.

[16] A. S. Patil, P. S. Jain, R. G. Ram, V. N. Vayachal, S P Bendale," Detection of Distributed Denial-of-Service (DDoS) Attack on Software Defined Network (SDN)", - IRJET 2018

[17] A. S. Patil, P S Jain, R G Ram, V N Vayachal, S P Bendale, "Software Defined Network: DDoS Attack Detection", — IRJET 2019

[18] Chinmay Dharmadhikari, Salil Kulkarni, Swarali Temkar, Shailesh Bendale," A Study of DDoS Attacks in Software Defined Networks", - - IRJET 2019.

[19] Shivam Tiwari, Vanshika Pandita, Samarth Sharma, Vishal Dhande, Shailesh Bendale, "SURVEY ON SDN BASED NETWORK INTRUSION DETECTION SYSTEM USING MACHINE LEARNING FRAMEWORK", IRJET 2019.

[20] Siddhant Shah, Aditi Thopte, Prabhdeep Singh Gandhi, Vrushali Ghodnadikar, Shailesh Bendale,"A Study of Generative Adversarial Networks in 3D Modelling", IRJET 2019.