SURVEY ON SDN BASED NETWORK INTRUSION DETECTION SYSTEM USING MACHINE LEARNING FRAMEWORK

Shivam Tiwari[1], Vanshika Pandita[2], Samarth Sharma[3], Vishal Dhande[4], Shailesh Bendale[5]

[1,2,3,4,5]B.E Student, Dept. of Computer Engineering, NBN Sinhgad School of Engineering, Ambegaon, Pune-411041, Maharashtra, India

---***---

ABSTRACT - Software Defined Network Technology gives us a way to possibly identify and record problems regarding network security. It ensures that our system is secure from possible attack. Machine learning techniques are used to monitor traffic from all the devices on the network. Network Intrusion Detection System is used to safeguard the network and helps to prevail over network security issues. Deep learning which comes under advance machine learning techniques is also used in SDN based environment. In this survey paper, we have referred some works done on machine learning techniques that support SDN based environment to apply NIDS. In this survey, we learned some equipment's that will help us to establish model of NIDS. For implementation we are try to increase the accuracy of network intrusion detection using the two algorithms stated in this paper.

2. Introduction

2.1 SDN

SDN is developed on centralized network topology which provides management of network resources and their intelligent control. With this kind of centralized and intelligent control factors like bandwidth management, security, repairing and policies can be highly refined by SDN Environment. SDN architecture consists of two planes, control plane and data plane which are separated and makes the packet transmitting simpler. Software Defined Network is a set of principles which aims to create a flexible, adaptable and effective network through software based configuration. In SDN environment the controller brings out the network information from the hardware devices and also provides the view of the network to the SDN applications. In SDN Architecture southbound APIs are used for the communication between SDN controller, router and switches. A northbound interface allows communication between a particular component and higher level components of the network.

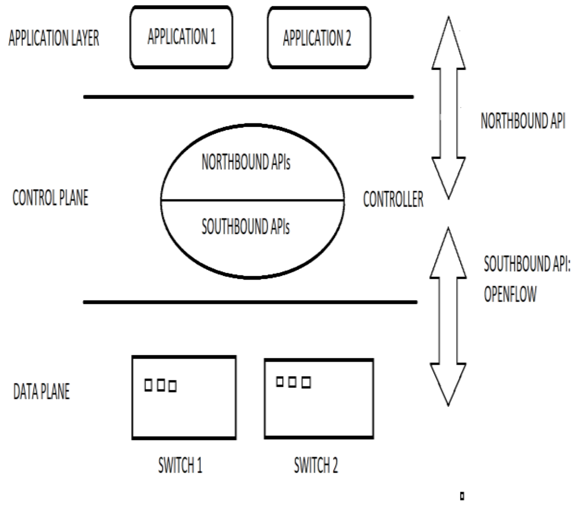

Fig.1 SDN Architecture

2.2 SDWN

The growth in daily use of mobile phones, tablet and laptops is resulting in the growing demand for high powered services from wireless networks. These growing demands endup requiring upgradation in the network architecture. For these requirements software defined wireless network has been an efficient solution. SDWN makes the network management simpler by decoupling the control plane and data plane. By using centralized controller or multiple controllers distributed in the network, the control plane can be centralized and implemented. SDWN can be efficiently used to overcome the limitations in the current architecture of spectrum management. From the hardware implementation the logic of traditional networks is absorbed into a higher level defined software. The controller in SDWN communicates with the intrinsic forwarding plane devices and organize their forwarding decisions .By decoupling the control and data plane, SDWN brings out the functions that are deeply hidden in the network to higher level. SDWN is different from SDN as wireless networks have different functions and lower layer protocol which should be identified carefully while implementing SDWN architecture .SDWN is self-configuring network as it do not need to understand the processing of signals and when to use lower layer protocols. SDWN is fully compatible because without changing the existing protocol stack, it is integrated into existing infrastructure.[8-12]

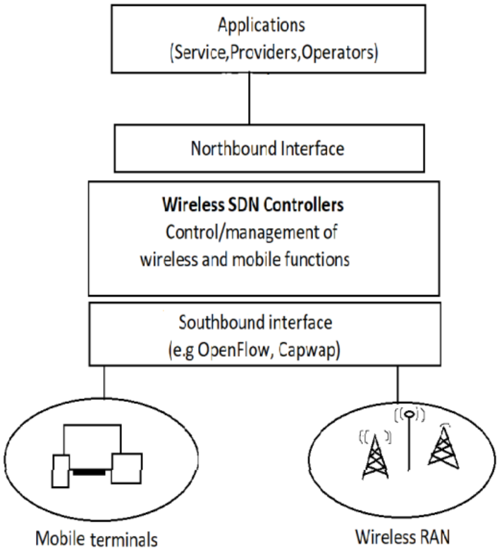

Fig.2 SDWN architecture

3. DDos Attack

DDos stands for distributed denial of service attack. It is an ill-natured attempt to distort the normal traffic of a targeted server, service or network by makes the target or the infrastructure surrounding it with a flood of Internet traffic. The machines that are exploited include computers and other resources of network such as IOT devices. In DDos attack, the attacker gets control over the network of online machines for carrying out the attack. Machines and computers are contaminated by malware turning each one of them into a bot. The attacker then remotely controls the group of bots. Once a botnet is created, attacker is able to direct the machines by sending instructions to each bot using the remote control. Once the IP address of the target is noted by the botnet. Each botnet responds when it sends message to the target, which causes the potential target server to overflow capacity which results in the denial of the service for the normal traffic. It caused because every bot is legitimate internet device which makes separation of normal attack from attack traffic very difficult.

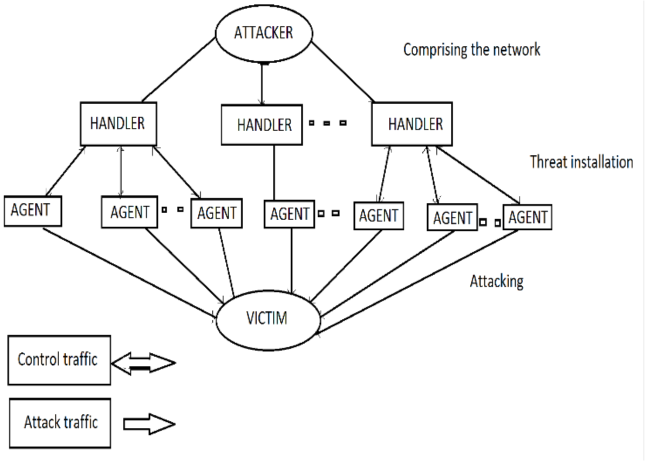

Fig 3. DDoS Architecture

4. Literature survey

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

The authors Nasrin Sultana, Naveen Chilamkurti, Wei Peng and Rabeialhadad [1] have discussed the ongoing challenges in implementing NIDS using machine learning and deep learning approaches. Further more, it discusses about the techniques of deep learning in developing SDN based NIDS and the tools that can be used to develop NIDS model in SDN environment that would help to detect network related issues. Overall, it provides an overview of programmable networks and explore the field of Software Defined Network.

The authors Gang Wang, Jinxing Hao, Jian Ma and Lihua Huang [2] have discussed a new approach called FC-ANN based on ANN and Fuzzy Clustering to achieve high detection rate, less false positive rate and stronger stability. The limitations which are present in ANN based IDS are overcome by proposing FC-ANN .It reduces the complexity of the training dataset and increases the detection performance.

The authors Lindinkosi L. Zulu, Kingsley A. Ogudo and Patrice O. Umenne [3] have discussed the use of Mininet to simulate SDN to illustrate the abilities of Mininet Wifi to be used as the Software Defined Network equivalent which can also be integrated to the existing network using a network virtualized function. This paper throws light upon the integration of Mininet research with other technologies. They have also discussed the benefits of emulator for wireless network providers with virtualize network functions.

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

The author Fernando M.V. Ramos, Diego Kreutz, Paulo Esteves Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky and Steve Uhlig have discussed the use of SDN paradigm which breaks the vertical integration and separates the network control logic from 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.

Sydney Mabwe Kasongo and Yanxia Sun [7] outlines the Deep Long Short Term Memory based classifier for Wireless Intrusion Detection System. As compared to traditional ML as well as Feed Forward DL method, the system proposed in this paper yielded an increased performance.

5. LSTM

Long Short Term Memory is an artificial recurrent neural network architecture used in the field of deep learning .Unlike standard Feed Forward Neural Networks, LSTM has feedback connections. Not only it processes single data points but also the entire sequence of data. LSTM comprises of cell, input gate, output gate and a forget gate. These three gates coordinate the information flow into and out of the cell and the cell remembers value over arbitrary intervals of time. LSTM networks are used for predictions, classification and processing based on data of time series. LSTM deals with the Vanishing Gradient problem that can be seen while training the traditional RNNs.

6. ANN

Artificial Neural Networks is based upon the collection of small computational units called artificial neurons which are connected in a complex structure. An artificial neuron processes the received signals and also it can signal neurons that are connected to it. ANN helps us to know the effect of increasing and decreasing the dataset horizontally and vertically on computational time. It helps us to understand best situations and best cases where the model fits the best way. It is completely related to the human nervous system. ANN is very rarely used when it comes to predicting model. ANN is used in cases where what has happened in the past can be used and repeated in the exact way

LSTM differs from ANN as it is a recurrent network architecture training with a suitable gradient based learning algorithm while ANN is a computational algorithm.

LSTM is designed to overcome error back flow problems, it can also learn to bridge the time intervals in excess of 1000 steps while ANN are computational models inspired by an animal nervous system and is also capable of pattern recognition and machine learning.

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]M.A. Patil, M.P. Jain, M.R. Ram, M.V. Vayachal and S.P. Bendale"Software defined network DDos attack detection".

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

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