Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 04, pp.68221-68228, April, 2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

SOFTWARE DEFINED OPTICAL NETWORKS TO EXPLORING MACHINE- LEARNING-BASED CONTROL PLANE INTRUSION DETECTION TECHNIQUES

***Priti Khaire**

Department of Computer Science and Technology, Shri Sant Gadge Baba College of Engineering and Technology, Bhusawal, Maharashtra Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra, India

ARTICLE INFO

Article History:
Received 28th January, 2018
Received in revised form
06th February, 2018
Accepted 14th March, 2018
Published online 30th April, 2018

Key words:

Optical networks, Control plane, Intrusion detection, Machine learning, cloud learning.

ABSTRACT

In this paper software defined optical networks (SDON), the centralized control plane may encounter numerous intrusion threatens which compromise the security level of provisioned services. In this current research paper, the issue of control plane security is studied and two machine-learning-based control plane intrusion detection techniques are proposed for SDON with properly selected features such as bandwidth, route length, In this paper, with the coordination of SDON and cloud platform, a multi-domain SDON architecture based on cloud control plane has been proposed, which is composed of data centers with database (DB), path computation element (PCE), SDON controller and orchestrator. In addition, the structure of the multidomain SDON orchestrator and Open Flow-enabled optical node are proposed to realize the combination of centralized and distributed effective management and control platform. As the focus of network security, Intrusion Detection Systems (IDS) are usually deployed separately without collaboration. They are also unable to detect novel attacks with limited intelligent abilities, which are hard to meet the needs of software defined 5G.

Citation: Priti Khaire, 2018. "Software defined optical networks to exploring machine- learning-based control plane intrusion detection techniques", *International Journal of Current Research*, 10, (04), 68221-68228.

INTRODUCTION

Software Defined Optical Networks (SDON) is a network architecture functional network, applying the concepts and techniques of software defined networks (SDN) to optical transport networks (Huibin Zhang *et al.*, 2017). It gradually becomes the trend of future optical networks, as it provides fast and customizable service while achieving the goals of high resource utilization and flexible services supply. In control plane of SDON, the controller serves as the main components.
A Self-Organizing Network (SON) is an automation technology designed to make the planning, configuration, management, optimization and healing of mobile radio access networks simpler and faster. SON functionality and behavior has been defined and specified in generally accepted mobile industry recommendations produced by organizations such as 3GPP (3rd Generation Partnership Project) and the NGMN (Next Generation Mobile Networks).

SDON controller network: A common method used by network managers to detecting illegal intrusion in control plane is called security rule matching. It does initializing a security-rule list and comparing each security rule in the list with incoming service request to checking violations. The security-rule list can be further categorized into blacklist and whitelist based on the contents of the security rules. Blacklist including the behaviors and characteristics of all potential attacks and malfunctions. It resembles a collection of symptoms used to diagnose diseases. However, the downside is that the full knowledge of complex and continuously changing in attacks can be hard to obtain. Whitelist, as opposed to blacklist, includes the rules regarding normal systems behaviors and functions. Software-Defined Networking (SDN) is an emerging area that promises to change the way we design, build, and operate the networks. Shifting from the traditional network architecture of proprietary based to the open, simple, and programmable network architecture. Open networking foundation defines SDN as "an evolving architecture that is dynamic, manageable, cost-effective, and adaptable. An ideal for the high bandwidth requirement and dynamic nature of today's application. The architecture decouples the network control and forwarding functions. This is enabling the network control to become directly programmable, and allowing the underlying infrastructure to be abstracted for applications and network services" (Huibin Zhang *et al.*, 2017). Today network has become an essential part of public infrastructures with the inception of public and private cloud computing.

****Corresponding author:* Priti Khaire,**
Department of Computer Science and Technology, Shri Sant Gadge Baba College of Engineering and Technology, Bhusawal, Maharashtra Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra, India.

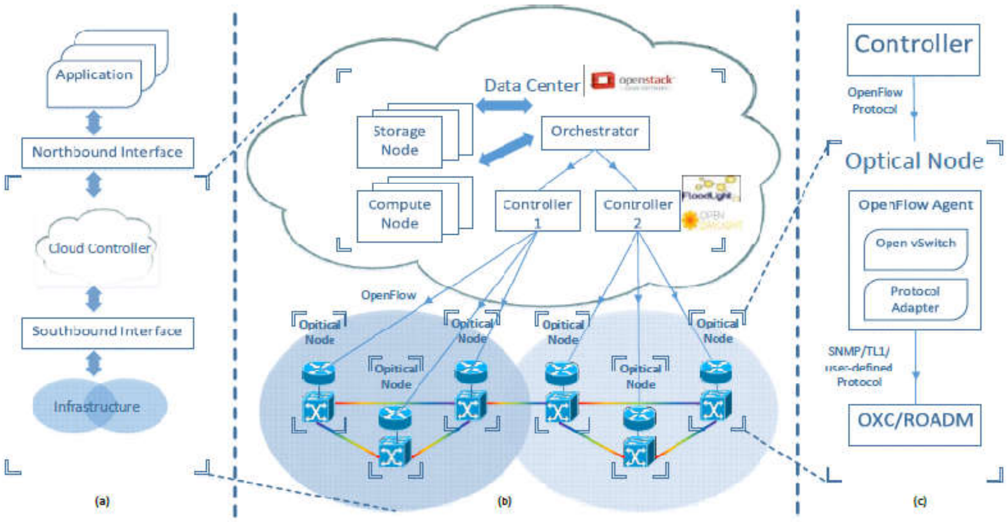

Fig.1Experimental network scenario (a) Abstract architecture. (b) Cloud Control Plane and Infrastructure Plane (c) Optical node structure[3]

The traditional networking approach has become too complex. This complexity has resulted in a barrier for creating new and innovative services within a single data center, difficulties in interconnecting data centers, interconnection within enterprises, and bigger barrier in the continued growth of the Internet in general. Furthermore, current network architecture has many limitations, which were resolved with the emergence of new SDN architecture. These include but are not limited to: inability to optimize network for WAN and Data Centre to generate more revenue and reduce expenses. With SDN more revenue can be generated by monitoring network devices and optimizing device utilization with a dynamic feature of SDN. The increase in capital and operational cost with SDN automation reduces human involvement in managing resources to a minimum which significantly reduces the cost. The SDN comprise three-tiered architecture that is designed to simplify network management (Atiku Abubakar and Bernardi Pranggono, 2017):

- The Application layer: contains application that delivers services.
- The SDN Controller: the main decision-making component separated originally from data plane which facilitates automated network management.
- The Infrastructure layer: a hardware layer that requires command line interface (CLI), but it does not need a programming language, unlike other layers.

SDON Control plane architecture

SDON migrates from the original distributed control architecture to centralized control architecture, thus dismissing a number of service routing protocols, and simplifying the network for that reason the path computing and path establishing can be completed in the controller. The main function of the controller is for manage the data forwarding of the transport plane through the programmable SBI and support applications who developing with NBI. It also allows multi-layer control for resource optimization in SDON. Also there is A Distributed Control Plane Architecture (DCP architecture) is a network architecture that makes it possible to allocate control protocol functions across multiple processor levels in the network system. The Internet uses a Distributed Control Plane Architecture.

The SDON controller is a software entity that over-sees transport plane resources and opens the network control ability through standard interfaces. The controller integrating a series of functions such as topology resource management, topology abstraction and virtualization, routing computation, service and connection control, etc, as shown in Fig. 1. With the assistance of the service layer adaptation functions, the controller obtains the resource information of the transport plane and achieves the connection control functions. Then it providing services for the application plane by taking advantages of the client layer adaptation function.

Topology management: obtaining the network topology information including node switching capability, link weight, shared risk link group (SRLG) information, link running status, maximum and available bandwidth, etc.

Abstraction and virtualization: abstracts some features of the network topology resources while hiding features that are independent of the exsting selecting standards.

Routing computation: computing end-to-end path for service connections in network.

Service/call control: supports service establishment, modification and release functions in network.

Connection control: establishing the required transport connection according to the service request, allocate resources, and complete the connection establishment, modification and release according to connection request parameters function.

Automatic link discovery: obtaining the link information between two nodes by running the automatic discovery protocol on them.

Policy control: provided appropriate business, security and survivability policies based on different management requirement and customer applications.

Notification processing: notified upper layer about network-status changes. Here, the client layer adaptation function can provides the APIs for the customers after abstracting and virtualizing the resource topology in the transport plane according to the customers' demands.

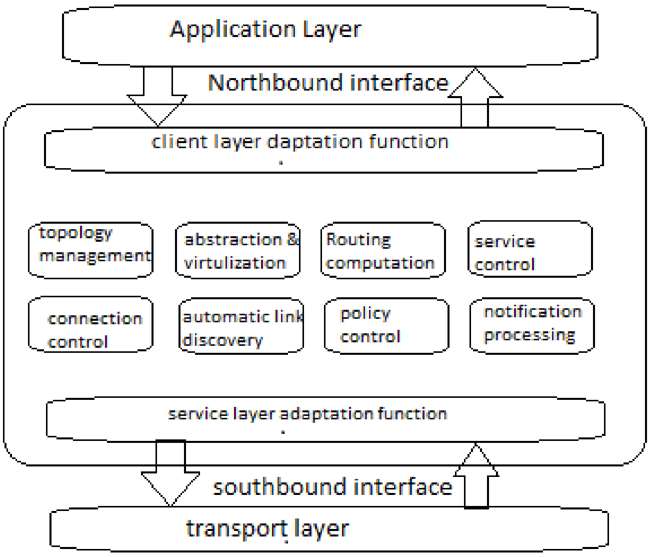

Fig. 1.1 Functions of SDON controller network [1].

Also, the client layer adaption function also has the responsibility to maintain the session with customers, as well as verify the identity of the customers. SDON controller manages network elements. The communication channels between the controller and transport plane switches is called control channel. The controller communicates with the transport plane elements overs the control channel by using the control protocol. Consequently, it is significant to establish and maintain the control channel between the controller and network elements, for the reason that if there exist a failure on it, the whole network will be down and out of control.

Potential intrusion threats

Control plane is a critical part in SDON architecture. Once it is under attack, most services can't be guaranteed. Here, we talk about some potential intrusion threats that the SDON control plane may encounter (Huibin Zhang *et al.*, 2017). The Potential Threat screen displays information about security risks to your clients and network. The Security Server gathers threat information by running Vulnerability Assessment and Cleanup Services to clean threats. Unlike the Current Threat screen that only displays information about a current threat, the Potential Threat screen displays information about all the threats to your clients and network that have not been resolved.

Unauthorized access

An attacker can get the access to control plane unauthorized by means of technical or nontechnical approaches, resulting in information leak and distortion. Control plane is connected to applications, network resources, etc. If the controller is impersonated, the attacker will gain access to network resources and will operate the network. Besides, if there is an unauthorized application trying to access the control plane with northbound API, the control plane is also under the intrusion threat.

Data leakage

In the southbound of SDN, Open Flow switches process different category of signaling messages (including messages about cookies, flags, ports etc.), some of which are sent to the controller. An attacker can fake such packages after learning its patterns and features, such as changing the status flag in a signaling data package. These crafted packages form massive number of requests and take up large portion of network resources, thus causing Denial of Service (DoS) attack (a cyberattack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet).

Data modification

As mentioned previously, the controller can manage the traffic in transport plane by means of programming the network devices. If controller is hijacked, the whole network will be out of control. Then, attacker can modify the flow rules in network elements so that package forwarding strategy will change and cause a chaos in SDON.

Point-anomaly-based detection

An anomaly occurs when a data instance represented by a point is outside a common region of normal behavior. In our case, for dynamic optical networks, we assume that each customer has its network profile including average bandwidth usage, frequent source and destination nodes, average route length, and modulation formats. Typically, we assume that a customer's behavior will match to certain patterns and a radical change might indicate a network intrusion. Though the change may be operated by the customer, it is such a low possible event that can be tolerated by the system. This change could be for example, a sudden increase in bandwidth between a pair of nodes not frequently used by the given customer. In our proposed scheme, a statistical technique learns the probability distribution of normal network behaviors from a training dataset. Then, it calculates the probability of an instance in the testing data set given the learned distribution A reasonable threshold needs to be determined to judge whether a user behavior is an anomaly. An anomaly-based intrusion detection system, is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation.

This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created.

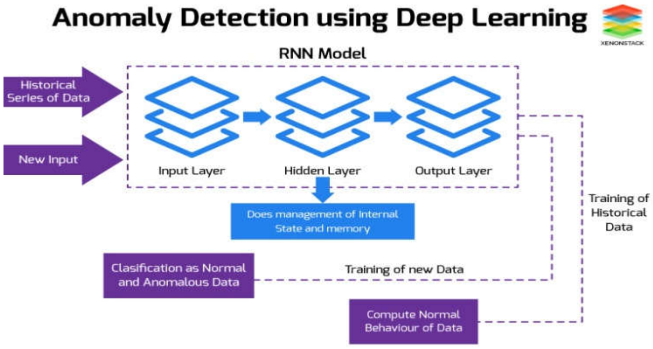
Anomaly Detection using Deep Learning
XENONSTACK
RNN Model
Historical Series of Data
New Input
Input Layer
Hidden Layer
Output Layer
Does management of Internal State and memory
Training of Historical Data
Clasification as Normal and Anomalous Data
Training of new Data
Compute Normal Behaviour of Data

Fig. 5. Anomaly detection using deep learning

Sequence-anomaly-based detection

In this scenario, individual data instances are not considered to be anomalies, but their occurrence together as a sequence are. For example, the intruder might perform malicious operations in a short period of time, such as light path creation, modification and deletion. While each network operation can be a normal behavior with normal parameters (e.g., connection bandwidth and route length), a sequence of continuous operations in a short time can be considered an intrusion. Fig. 4 shows an intuitive example where a red region is an anomaly because the low value lasts for a long time. In order to simplify the model and focus on the anomaly problem, we assume in optical networks, the request arrival can be described as Poisson process with number of arrivals in a finite interval of length t following a Poisson (λt) distribution $P\ \{n\} = (\lambda t)n\Delta\exp(-\lambda t)/n!$. We expect that the intruder's behavior will not align closely to the profile of normal network operations. As a result, we introduce the improved cumulative sum (CUSUM) approach (Ming *et al.*, 2016) to detect cumulative shifts in a stable process. With time going by, shifts will be accumulated. And the cumulative shifts, normally in a stable system, will wave in a fixed scope. Once the cumulative shifts go beyond the upper bound or the lower bound, then it can be considered as an anomaly.

Detection procedures can be summarized as

- Use normal training set to achieve upper and lower bounds of the model.
- Monitor CUSUM of the testing data and determine anomaly once CUSUM is over the limits.

Experiment design with virtual test

A virtual testbed is developed where various attacks are performed by means of simulation. Initially, different attacks techniques are implemented to observe the impact of DoS, Probe, U2R, and R2L attacks on SDN environment on both the servers and normal users accessing resources on the server. As signature-based IDS cannot be the solution to all type of attacks, it is necessary to provide alternative approaches that complement its seminar. A flow-based anomaly-based system is developed as an anomaly-based IDS. This is due to the nature OpenFlow protocol as the communication protocol between controller and infrastructure layer: it uses flow for identifying the network traffic, and also records its information by counters. The flow is a sequence of IP packets with common characteristics, going through monitoring point within a period of time. The seminar follows two approaches to provide a solution to this problem. The first is developing a virtual test bed that mimics the real scenario and provides a solution to signature-based attacks. The second method is designing the model that will provide anomaly-based detection. This would be integrated into signature-based architecture for detection of unknown attack undetected by signature-based IDS.

Virtual Test bed

Open Day Light controller (ODL) is installed and configured on Ubuntu Desktop 16.04 OS. ODL manages the Open Virtual Switches (OVS) based on Open Flow protocol through a remote connection to be established by Mininet simulator. The Mininet network simulator is also installed and configured to create host system, servers, and OVS on the same OS with ODL. The Metasploitable2 server is hosting four services that are left vulnerable intentionally for penetration testing purpose, while the Parrot security will be generating attack scenario on Metasploitable2.

Network Topology

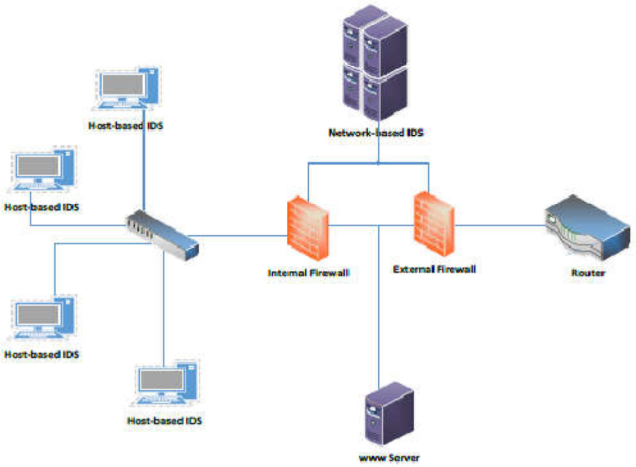

Fig. 7.1 Host based network [2]

The star topology is used for setting up laboratory network because it is easy to setup looking at the nature of the research and the combination of systems involved. Also, OVS-switch as a central hub is expected to provide optimal performance of the network traffic without overhead in providing centralize network monitoring. Therefore, failure of a single node will not affect the entire network. Inside Mininet, a network is created with fifteen VM hosts, five generating malicious traffic internally using manual attack procedure by attacking the server and other internal external server hosts. The ten hosts VMs generate normal or benign traffic between each other and the servers. All the hosts VM are connected to OVS-switch. PENTMENU penetration testing tool is installed on both Parrot Security and Mininet+ODL machine with aim of attacks demonstration using created hosts for internal attacks. The Wireshark services is on installed Mininet Simulator lunch, where the Wireshark will be monitoring the network traffic through the traffic filter any option. The purpose of using Wireshark is to observe MITM attacks on the controller. The connection between Open Flow ovs-switch with ODL controller is remote when creating the topology, a remote connection is specified with the loopback IP address of Ubuntu machine where ODL controller is installed. The Parrot Security, Metasploitable2 server, and Snort IDS are connected to Open Flow ovs-switch through the Mininet+ODL VM interface eth1, eth2 and eth3 respectively. Fig. 7.2 Signature-based Network Topology (Atiku Abubakar and Bernardi Pranggono, 2017)

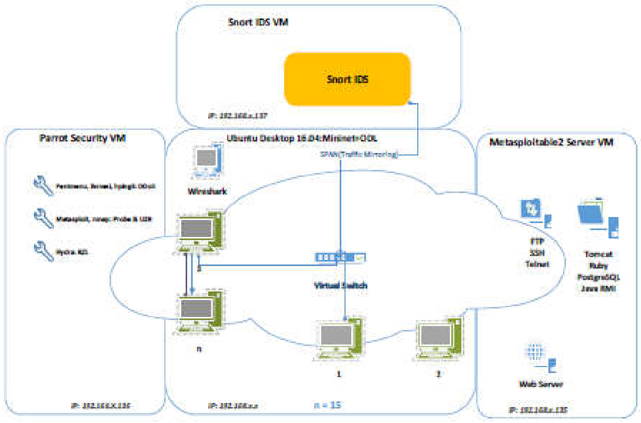

Fig. 7.2 Signature-based Network Topology [2]

Pattern Recognition of Neural Network

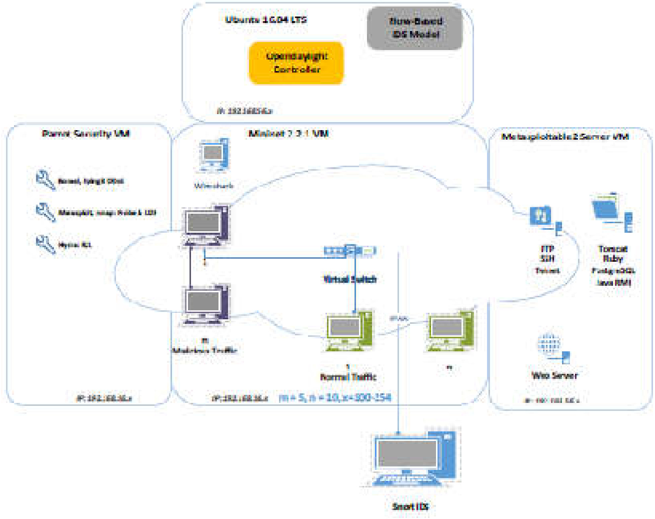

Fig. 7.3 Flow-based IDS Model Network Topology [2]

In addition to the existing signature-based IDS, a Neural Network-based model is designed to be integrated into the system. flow-based anomaly detection using machine learning approach to compliment the signature-based, since the signature-based cannot detect the unknown or zero-day attack. Furthermore, attack demonstration on the virtual test bed is limited to specific type of attacks under each category of attack. Therefore, a model that can detect a wide number of attacks is proposed. The flow-based IDS model will be implemented in the future, as a module using Restful API or Java and hosted over ODL controller. As an application layer model, the network policies of traffic flow is controlled by the application, in such a way that some rules will be imposed that will be responsible for attack detection. Typically the flow statistic request is sent to the switch by the controller over a certain time interval. When the statistics are available on the controller, the module will used it to detect anomaly behavior in the flow.

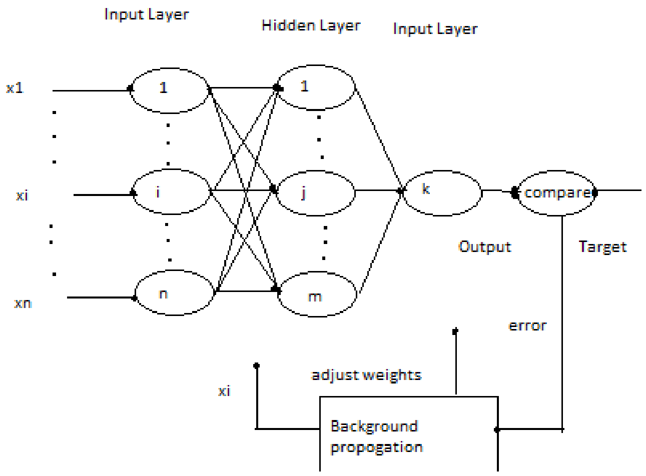

Fig. 7.3 flow based layer detection [2]

The detected anomaly traffic will be mitigated appropriately through flow modification, hence result in new network impose by the module IDS. Pattern recognition of neural network is implemented in this model. It usually classifies inputs into a set of target categories.

The network architecture consists of three layers

An input layer, hidden layer, and an output layer. Backpropagation algorithm is used to trained the network. Backpropagation algorithm is a training method used in classification by propagation and updating the weight of a network. When an input is received from the input layer, it is passed to the next layer, then to the output layer. The output is compared with the given targets or desired output, each output result of the neuron is calculated using a function and error value at the output layer. If the output matches the target or roughly closed, then it is presented as final output, otherwise an error is fired backwards from the output layer toward previous layers until desired output is obtained.

The SDON architecture b baasesedd o onn c lColuodu dc oCnotnrotrlo pl lPatlfaotfromrm (CCP) which is the coordination of traditional SDON and cloud platform. The model of SDON based on CCP is divided into three planes, namely, Infrastructure Plane, Cloud Control Plane and Application Plane. The difference with the traditional SDON structure is that the orchestrator and cloud services are added to the cloud control plane, and geographically distributed controllers are gathered in data centers of cloud service. The hierarchical structure of control plane and distributed peer-to-peer architecture of cloud service data centers are reserved to achieve highly integrated distribution and concentration as well as effective management and control. The concentrated orchestrator and controllers in data centers improve the efficiency of data processing and network management and control, while the distributed architecture of the cloud platform data centers also provides a great scalability for the network.

From the vertical perspective, the centralized management and control structure can achieve the local and global optimal control. And from the horizontal point of view, the distributed management and control can overcome the disadvantages of the heavy task, low efficiency, complicated management system and database, which is caused by the centralized management and control. The hierarchical centralized control is realized in the CCP architecture. When a local controller has an enough capability to handle the request effectively, the higher level controller or orchestrator will not interfere.

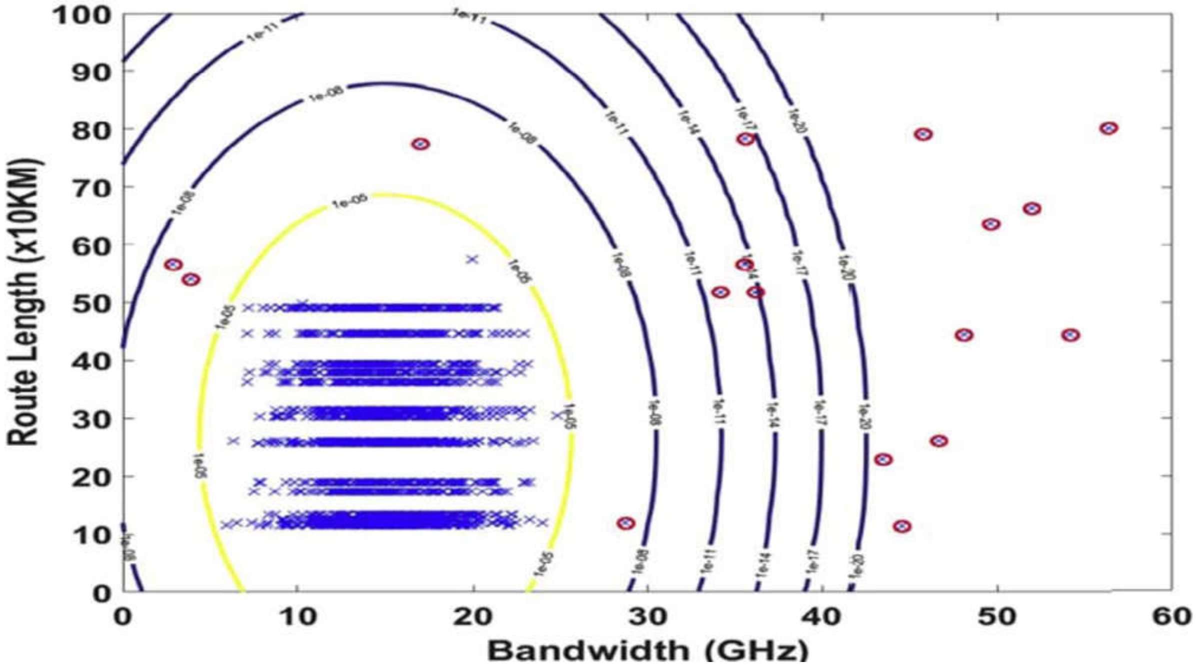

Fig.8.1 Contour diagram for testing data set with bandwidth and length[1].

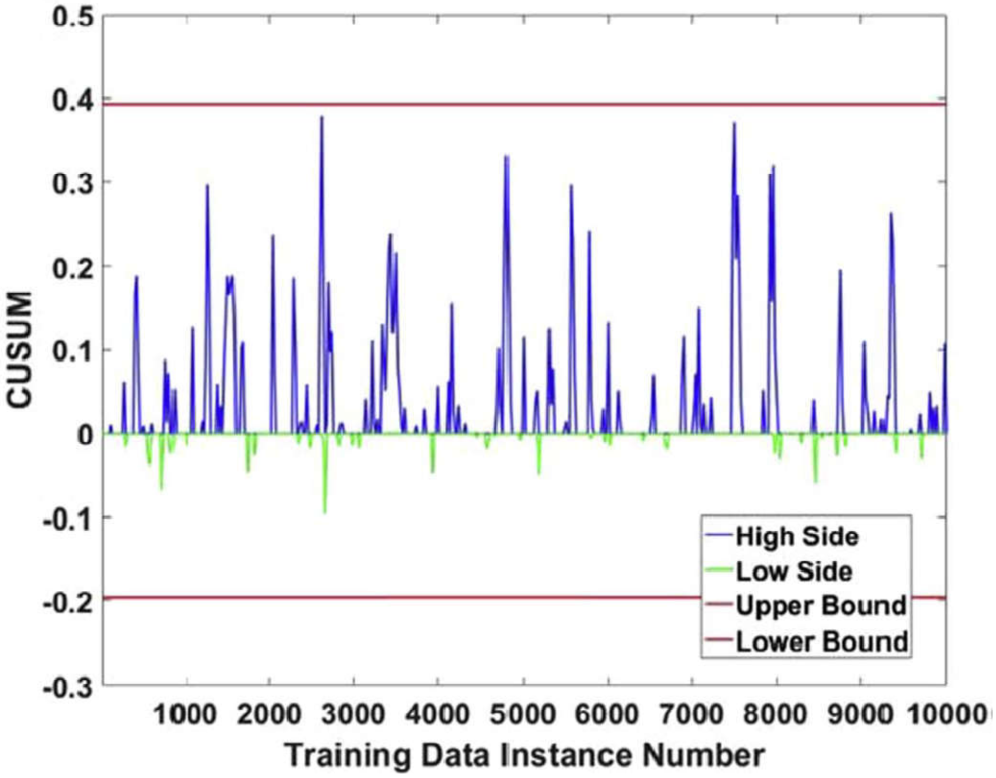

Fig. 8.2 CUSUM of training data set[1].

The higher level controller or orchestrator deal well with multi-domain requests only if the management and control task is not borne by a local controller. Meanwhile, hierarchical management systems play different roles to coordinate effectively. In this way, the scale of global management and control database, the time of enquiring and the amount of traffic management information are decreased significantly. These functions can be easily implemented by the efficient computing, management and storage of the cloud platform. This structure is suitable for a large scale, heterogeneous network interconnection, and geographically distributed network.

SIMULATION RESULTS

Fig. 7 illustrates the probability in contour diagram, where points on the same circle have the same probability. The inner circle in yellow indicates the threshold ε. Every blue point denotes an operation. Points in the red circle are declared as intrusion while points in region 1, as is shown in Fig. 2, are normal because the probabilities of these points are larger than ε. As a result, we detect 25 anomaly points (25/30), and the detection accuracy is 83%. To verify the sequence-anomaly-based detection, the training data set, which is generated with a

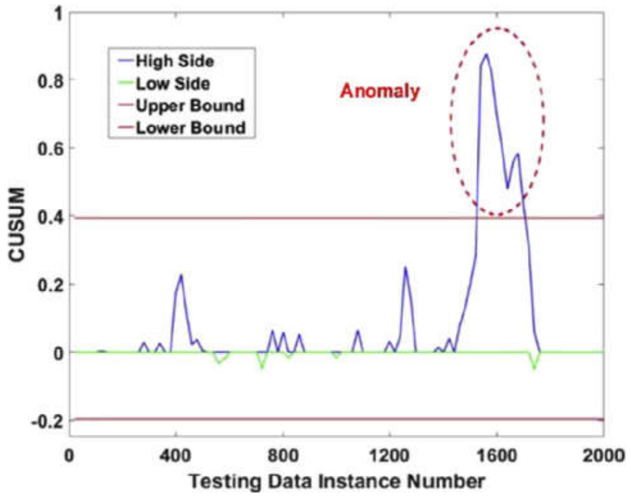

Fig. 8.3 CUSUM of testing data set[1].

Poisson process (λ = 0.4), includes 10,000 training data instances. We use normal training data to achieve bounds (−0.2, 0.4). Fig. 8.2 shows the CUSUM of the training data set. It is observed that the CUSUMs of normal data instances are within the bounds. Also, cumulative shifts are in the normal range for normal data set. Then, we generate 40 data instances for test with λ = 0.8 to simulate massive operations in a short period of time, then we randomly insert them into 1960 normal instances of testing data. Fig. 8.3 shows the detection of an anomaly when the CUSUM exceeds the upper bound with an abnormal number of network operation requests in a short period of time. We complete more than 100 tests with this scheme by obtaining an average detection accuracy over 85%. In the actual networks, point anomalies and sequence anomalies may occur at the same time. And the methods of network attack can also vary a lot, according to different network scenarios. The two anomaly detection techniques mentioned above do not conflict with each other. On the contrary, the detection accuracy can be improved by using both point-anomaly-based detection and sequence-anomalybased detection.

Machine learning based intrusion detection system for software defined networks

Software-Defined Networks (SDN) is an emerging area that promises to change the way we design, build, and operate network architecture. It tends to shift from traditional network architecture of proprietary based to open and programmable network architecture. However, this new innovative and improved technology also brings another security burden into the network architecture, with existing and emerging security threats. The network vulnerability has become more open to intruders: the focus is now shifted to a single point of failure where the central controller is a prime target. Therefore, integration of intrusion detection system (IDS) into the SDN architecture is essential to provide a network with attack countermeasure. The seminar designed and developed a virtual test bed that simulates the processes of the real network environment, where a star topology is created with hosts and servers connected to the Open Flow OVS-switch. Signature-based Snort IDS is deployed for traffic monitoring and attack detection, by mirroring the traffic destine to the servers (Atiku Abubakar and Bernardi Pranggono, 2017). The vulnerability assessment shows possible attacks threat exist in the network architecture and effectively contain by Snort IDS except for the few which the suggestion is made for possible mitigation. In order to provide scalable threat detection in the architecture, a flow-based IDS model is developed. A flow-based anomaly detection is implemented with machine learning to overcome the limitation of signature-based IDS. The results show positive improvement for detection of almost all the possible attacks in SDN environment with our pattern recognition of neural network for machine learning using our trained model with over 97% accuracy.

Keywords: Software-defined Network; Intrusion Detection System; Open Flow; Machine Learning; Neural Network;

Conclusion

In this seminar, we introduce the SDON architecture and the implementation of the control plane and control channel. We enumerate Potential intrusion threats in control plane in detail. We apply machine learning techniques for the intrusion detection in the control plane of software defined optical networks. Simulation results show that the accuracy of intrusion detection schemes can achieve over 83%. This accuracy can be enhanced in future seminar, by considering more features and generating more training data instances. Software Defined Networks as an emerging technology bring innovation into the networking, with decoupling of control plane and the data plane, removing proprietary in the network architecture to open and programmable network. Due to the numerous advantage of this architecture, many companies are shifting from the traditional network architecture to new SDN architecture. However, SDN as a new technology has arising issues that pose a challenge to the futuret of the technology. Security is one of the main issue that threatens the future of SDN technology. The seminar present machine learning (Neural Network) based intrusion detection for SDN. The model IDS are built on the existing signature-based IDS architecture as flow-based IDS to detect anomaly-based attacks in the SDN environment. The Pattern Recognition is used in this seminar due to its performance accuracy rate as compared with the other type of neural network model.

Acknowledgment

I feel great pleasure in submitting this review paper on “Software defined optical networks to Exploring machine-learning-based control plane intrusion detection techniques”. I wish to express true sense of gratitude towards my Prof. Yogesh S. Patil who at very discrete step in study of this paper contributed her valuable guidance and help me to solve every problem that arose. I would wish to thank our H.O.D., Prof. Dinesh D. Patil for opening the doors of the knowledge towards the realization of the paper. Most likely I would like to express my sincere gratitude towards my family for always being there when I needed them the most. With all gratitude and respect, I would like to thank all the people teachers, who helped me directly or indirectly. I owe my all success to them, and special thanks to all authors writers by whose this paper is referred by me.

REFERENCES

Atiku Abubakar and Bernardi Pranggono 2017. Department of Engineering and Mathematics, Sheffield Hallam University, Sheffield, S1 1WB, U.K. “Machine Learning

Based Intrusion Detection System for Software Defined Networks" in.

Huibin Zhang, Yuqiao Wang, Haoran Chen, Yongli Zhao and Jie Zhang, 2017." Exploring machine-learning-based control plane intrusion detection techniques in software defined optical networks" in.

Jiaqi, Li., Zhifeng Zhao and Rongpeng, Li. 2015. "A Machine Learning Based Intrusion Detection System for Software Defined 5G Network", in.

Ming, Li *et al.,* 2016 *J. Phys.: Conf. Ser.* 679 012022 "Design of Control Plane Architecture Based on Cloud Platform and Experimental Network Demonstration for Multi-domain SDON".

****