A SURVEY ON SECURITY THREATS AND SOLUTIONS FOR SDN USING MACHINE LEARNING APPROACH

M. JANAT VINNARASI
M.Phil Research Scholar,
janetvino@gmail.com
Bishop Appasamy College of Arts and Science, Coimbatore
Bharathiar University, Coimbatore, Tamil Nadu, India.

Dr. N. SUDHA
Associate Professor, Department of Computer Science,
Bishop Appasamy College of Arts and Science, Coimbatore
Bharathiar University, Coimbatore, Tamil Nadu, India.

Abstract:
Software Defined Networks (SDN), a new buzz word, provides more versatility than any other traditional networks. It has seized a fair of attention as a new It is favored because it is overcoming the limitations of traditional networks. 7 layers of OSI network model of 7 layers are reduced to three layers. It is programmable, low cost and gives better performance when compared to traditional networks. SDN is exhaustively recognized by enterprises, that uses ranging from private sector to workgroup like small or medium scale workgroup network and corporate large-scale networks. Holding SDN in this modern network which provide more agility and visibility to adapt and organize the network solutions. But from the view of security regards attack prediction and risk mitigation attacks will happens such as DDoS. For this analysis this paper presents a comprehensive survey of the research relating to security in software-defined networking and provides solution using machine learning approach.

Keywords: SDN, Security Threats, DDoS and Machine Learning technique.

I. INTRODUCTION

Software defined networking (SDN) is a networking paradigm which promotes the split-up of network data-plane from the network control-plane. Works of the data-plane is to be being forward the data through the network, example packet and hardware were forward it, such as switches. And another one control-plane characterizes all logic information and devices which is accountable for defining how and where to the data is to be sent in the data-plane are defined in this network. In conventional network, it combines both planes in the same devices, concentrate on each device to make its own decisions for forwarding based on distributed routing protocols [1]. While SDN, it allows for the control-plane to provide a comprehensive view of the network for consider all the network state.
Software-Defined Networking (SDN) is a developing systems administration worldview that offers would like to change the impediments of current system frameworks. SDN is being circled to various systems administration framework. It is the capacity to program organize execution in open way utilizing dialects, frameworks, PCs that are common. Systems administration is being change into programming discipline. Indeed, even in the significant ramifications organizing is turning into the piece of processing. To upgrade the execution and for better activity administration SDN can be connected on the mist gadgets. SDN is the rising model that makes deportment of vehicular switches programmable and permitted to be controlled by focal component known as controller [2]. SDN worldview presents a concentrated and programmable method for planning systems and was intended to confront the inadequacies of customary systems, for example, manual design and upkeep of each gadget in the system, high inactivity in way recuperation because of appropriated approach, and so on [3]. SDN isolates the information plane from the control plane, enhancing the programmability of the system by outside applications. SDN is the main innovation to deal with the immense systems. The essential thought behind SDN is the partition of the system control plane from the information plane. By SDN separation, forwarding decisions of networking elements like switches, and access points from the data plane, it is uncomplicated for network administration and management hence the control plane were only concentrating with the information regards the routing of traffic, logical network topology, etc. In the view of data plane, it constitutes the network traffic holding with the conventional configuration in the control plane. In SDN, network policies were dictated through the controller by means of control operations were centralized [4].

Distributed Denial of Services (DDoS) attacks is one of dangerous threats to the present network that always provide and progresses in line with the advance of the network itself. This network has entered as a SDN era which provide centralized control and programmability network by separate the network control and data plane. From that, it results on us a dynamic, cost-effective, manageable and agile platform. On the issue have arisen that, this centralized stage can bring new security risk such as DDoS attacks on the central organizer which could concern the complete network [5]. Although the features of SDN provide a great effect on security, it is bare new threats that are central controller attack which force effect to all the system accessibility.

Availability is related to the accessibility of information when needed. Unavailability of system or information can make an organization/corporation lost their business revenue and user’s satisfaction. Availability is one of CIA (Confidentiality, Integrity, and Availability). While confidentiality refers to privacy, integrity is equivalent to the trustworthiness of data. These two aspects are very common safety aspect for security, meanwhile, availability is not priority one. By making an online service/server become inaccessible by transfer serious number and size of fake data from multiple sources is representing of DDoS attacks [6, 7]. This kind of security attacks is easy to establish but hard to discard and very effective to exhaust the network. This paper presents a survey of the current research work of SDN security particularly to overcome the DDoS attacks. Also present a short summary of the SDN and its technologies used for the SDN security was presented.

The organization of this paper is as follows, In Section 2, contains the review of several recent works in SDN security and how these specific works relate to different aspects of SDNs, in Section 3 discussed about overview of SDN, in Section 4 security threats of SDN was provided, in Section 5 improving security in SDN was discussed and Section 6 contains solution for security issues in SDN, and finally Section 7 contains the a conclusion about this paper.

II. LITERATURE REVIEW

Chemodanov [8] discover the occasion of characteristic or man-made fiascos, giving quick situational mindfulness through video/picture information gathered at remarkable episode scenes is frequently basic to the people on call. Notwithstanding, PC vision procedures that can procedure the media-rich and information concentrated substance acquired from nonmilitary personnel cell phones or reconnaissance cameras require a lot of computational assets or subordinate information sources that may not be accessible at the geological area of the episode. In this paper, we propose an occurrence supporting visual distributed computing arrangement by characterizing a gathering, calculation, and utilization (3C) engineering supporting haze processing at the system edge near the accumulation/utilization locales, which is combined with cloud offloading to a center calculation, using programming characterized organizing (SDN).

Yan, Qiao, et al [9] consider the Distributed Denial of Service (DDoS) assaults in distributed computing conditions are becoming because of the basic attributes of distributed computing. With ongoing advances in programming
characterized organizing (SDN), SDN-based cloud conveys us new opportunities to crush DDoS assaults in distributed computing conditions. By the by, there is an opposing connection among SDN and DDoS assaults. On one hand, the abilities of SDN, including programming-based movement investigation, brought together control, worldwide viewpoint of the system, dynamic stimulating of sending rules, make it less demanding to distinguish and respond to DDoS assaults. Then again, the security of SDN itself stays to be tended to, and potential DDoS vulnerabilities exist crosswise over SDN stages. In this paper, we talk about the new patterns and qualities of DDoS assaults in distributed computing and give a complete review of guard instruments against DDoS assaults utilizing SDN. This work can see how to make full utilization of SDN's focal points to vanquish DDoS assaults in distributed computing conditions and how to keep SDN itself from turning into a casualty of DDoS assaults, which are vital for the smooth advancement of SDN-based cloud without the diversion of DDoS assaults.

Bruno Astuto [10] infer the prospect of programmable systems has as of late auto increased important force because of the progress of the Software-Defined Networking (SDN) worldview. SDN, frequently referred to as an "essential new thought in systems management", guarantees to radically streamline establishing administration and empower advancement through system programmability. This exploration overviews the cutting edge in programmable systems with an accentuation on SDN. We give a notable viewpoint of programmable systems from early plans to late improvements. At that point author present the SDN design and the OpenFlow standard especially, they talk about flow choices for performance and testing of SDN-based resolutions and administrations, look at momentum and future SDN applications, and examine promising examination headings dependent on the SDN worldview.

Tryfon Theodorou [11], analyze the recent recommendations improves Wireless Sensor Networks (WSNs) with Software Defined Networking (SDN) works on, presenting new inventive system control procedures and conventions dependent on a focal control rationale, i.e., empowering WSNs as essential offices for the Internet of Things (IoT). Toward this path, we show CORAL-SDN, an SDN answer for WSNs which: (I) utilizes canny concentrated control components to modify powerfully the convention functionalities; (ii) bolsters versatility to the testing necessities of the WSNs; (iii) keeps up an adaptable design; and (iv) displays enhanced system administration and task as far as execution and asset usage. With this demo we give a reasonable domain to hands-on experimentation, including the CORAL-SDN convention task in genuine proving grounds and featuring the upgrades that SDN conveys to IoT.

Hai Huang [12] analyze the evolving technology of the Internet of Things (IoT) which requires global connectivity to billions of heterogeneous devices such as sensors, cameras, RFID devices, etc. However, due to the diverse of devices and accessing protocols, IoT networks are fetching enormous and more complex, which makes the management totally difficult. Based on Machine-to-Machine (M2M) technology and the programming feature of the network, taken by the Software Defined Network (SDN), devices in a network can be act as objects, thus separating the control plane from the data plane. In this paper, author proposed a framework for handling the devices and organizing the network actively based on SDN. Finally, they get a successful result.

### III. SDN OVERVIEW

In the internetworking, Software Defined Networking (SDN) is one of the emerging technologies nowadays. It is an open network architecture to solve some of the key faults of traditional networks. SDN explains that the control logic of the network and network functions were two different concept and be separated in different layers. In SDN, it presents the concepts of Control plane and data plane: The centralized control plane (also called as controller) it handles the network logic, control traffic direct from the data plane (also called as switches) it does the job of forwarding the packets among the networks [13]. So, here the SDN can be consider as a physically circulated switching with a sensibly centralized control. SDN is planned for provisioning extremely dynamic arrangement and quality of service/security strategies.

![Figure 1: View of SDN](image-url)
Along with SDN associated security applications and routing applications and mechanisms, contemporary networks expect plenty other functionalities and strategies ranging from traffic determining to network virtualization and custom packet processing to quality of service (QoS). Though the programmability of SDN, it allows for fast prototyping, modifying network functions, implementing range of QoS and high flexibility to configure strategies for different situations, at the same time it also unlocks new vectors for susceptibility, attacks and risks.

IV. SECURITY THREATS OF SDN

This section categorizes the threat and attack in SDN architecture. While having a centralized controller allows improving the policy-deciding process, issuing the strategy execution process over the switches introduces new issues and security threats about information discovery. In inheritance networks, the whole network functions are transferred to the specific network devices for executing them independently, thus providing autonomous control over configuration and access. In SDN based networks, only the policy-rule implementation part of the network functions is spread/replace throughout the data plane switches (OpenFlow) [14]. Thus, network strategies, traffic shaping, security, QoS functionalities like Intrusion detection and prevention systems, network virtualization, bandwidth organization and access control, are required by the switches (OpenFlow), through the flow rules connected by the controller, programmed by explicit SDN applications running in application plane. Inappropriately, this dynamic programmable behavior can significantly extend the attack exterior of the whole SDN based network. Threats to SDN can be classified into three main categories:

A) Behavior Characteristics

B) Based on Resources

C) Key Functional Components

The most common methods of attacks can be:

1. Spoofing: In this, an attacker seems to be a unpretentious user of the network resource. This can be done by counterfeiting fake IP or MAC address. Attackers fake the Address Resolution Protocol (ARP) packets and make the system to trust that they are the genuine users from genuine network resource.

2. Man, in the Middle attack: This is the ability of the attacker to attack the system by assigning himself as the genuine system and takes control over the controller in SDN. Secure Socket Layer (SSL) makes this task as a difficult task by providing highly secured way of protection.

3. Tampering: In this type of attack, the attackers grabs the systems data and change it to another form. The original form is completely changed into another form. This could be done by attaining the controller to apply flow rules offered to alter or bogus data packets or flow counters

4. Repudiation: Denial attacks are those the packets where the origins are not traceable. Here an attacker fakes packet source address, and sends packets to a wanted destination. In doing so, the receiving system cannot precisely determine the source of the established packets.

5. Information Disclosure: Being in ownership of information you are not permitted to have is usually mentioned to as information disclosure. In the context of SDN, this could suggest side networks attacks intended to disclose extended material about the open flow system.

6. Denial of Service - Flooding/Saturating Attacks: DOS attacks are considered to edge the system’s skill to communicate and received data in a usual and expectable manner. This is attained via the use of techniques considered to reduce bandwidth and system resources. This is where open flow is most susceptible presenting its largest exterior to attack ratio. The necessity of SDN that packets must be sent to the controller on a regular basis, offerings potential occasions for denial of service attacks. An attacker can attack the SDN fundamentals or an attacker can attack the control plane of SDN.

Top security problems include:

- It Capture and alteration of SDN control plane packets. By the SDN controller it can efforts to alter configurations of network items.
- Irregulate the network element firmware with modified software (malicious software).
- Reduce the network element firmware to an old version (eg: out-of-date version).
- At the outer or gateway (Network Edge Device NED) - Is the NED reliable? e.g., is the base software (OS, software switch, etc.) the one predictable.
- Are only the user itemized Security Application consecutively in the NED and examining the traffic? Can the user be certain that no other requests are managing the data?

V. IMPROVING SECURITY IN SDN

SDN provides an API interface. Le Application Programming Interface, it allows the network’s data plane to be modified by external applications. It reveals the two-sided with admiration to security because it permits both new security aspects and new threats. First SDN provides a susceptible network security functions by strategy [15]. It is thus the belief of this paper that a thoughtful focus on security is vital if SDN is to take its place as the network architecture in future. So, various security working sets have been set up for this reason.

a. Enhancing Configuration

In network management, configuration is one of the most important functions. Specifically, when new equipment is added into an existing network, proper configurations are required to achieve coherent network operation. However, owed to the heterogeneity between network device producers and configuration boundaries, current network configuration naturally involves a confident level of manual privilege. This manual privilege procedure is dull and error prone. At the same time, significant effort is also required to troubleshoot a network with configuration errors. It is generally accepted that, with the current network design, automatic and dynamic reconfiguration of a network remains a big challenge. SDN will help to remedy such a situation in network management. In SDN, union of the control plane is all over the network devices, including switches firewalls, Network Address Translators (NATs), routers, and load balancers, reduces it possible to configure network devices from a single point, repeatedly via software controlling. As such, a whole network can be programmatically configured and enthusiastically enhanced based on network position [16].

b. Improving Performance

Increasing the network infrastructure is a key objective for the network operations. Hence, due to the synchronization of various technologies and backers in a single network for improving performance will be difficult. Presently most of the approaches concentrate on performance of a subset of networks or quality of experience based on user in some network services. These methods based without involvement of local information which offer suboptimal performance, if not inconsistent of network operations. The SDN offers introduce the offers, that a chance to improve network performance globally. Mainly SDN allows for a centralized control with a global network view. And also exchange the information between different layers in the network architecture. As such, many challenging performance optimization problems would become manageable with properly designed centralized algorithms. It follows that new solutions for classical problems, such as data traffic scheduling, end-to-end congestion control load balanced packet routing, energy efficient operation, and Quality of Service (QoS) support can be developed and easily deployed to verify their effectiveness in improving network performance.

c. Encouraging Innovation

In the presence of continuing evolution of network applications, future network should encourage innovation rather than attempt to precisely predict and perfectly meet requirements of future applications. In existing network new idea and design were face immediate issues in implementation and in deployment stage. In conventional network components issues arise from used exclusive hardware for prevent changes for the experiment. Also, when experimentations are likely often conducted in a discrete simplified testbed. These results do not give sufficient assurance for industrial reworking of these new ideas or network designs. The innovation community efforts like Planet Lab and GENI have enabled the high assurance result. By comparing the SDN innovation it offers a programmable network platform to implement and deploy new ideas for earning services conveniently and flexibly. Progressive deployment of new ideas can be performed through a seamless transition from an experimental phase to an operational phase [17].

VI. PROVIDING SOLUTION USING MACHINE LEARNING

a. Neural networks

This replicates the systems used by biological nervous system that process information. A collection of elements are processed to transform a set of input to another set of output. This type of classification is done through neural networks. These are classified as attack pattern, attack type and the
usual network performance. Neural networks provide resourceful output after a period of training.

b. Support vector machines

The most common machine learning method to classify machine learning tasks is Support Vector Machine (SVM). This technique involves the use of a set of marked categories of training examples. Technique specific algorithms are used to construct a model that could determine if a new example falls within any of the previously marked categories of examples. The classification algorithm involves: - Determine an input attribute space X for each network connection. - Select n attribute characteristics. Let the network connection be described using the vector x (one-dimensional) as x = { x1, x2, ... , xn}, where i = 1, 2, ... , n, denote the attribute characteristic of the sample x. Let denote Y = (+1,-1) where +1 represents normal and -1 represents abnormal connections. A support vector machine approach is a better choice in intrusion detection, because of its hopeful results in the eradication of small samples.

c. Genetic algorithms

Genetic algorithm network features such as; flags, service, login status and super user efforts to individual chromosomes in genes. This technique includes search procedures that provide estimated solution to an optimization problem. A profile is created for a normal and suitable behavior. Creating profile, the genetic algorithm automatically makes the choice of which behavior of network is normal or doubtful. This technique executes in more efficiently with known attack patterns but is less prevalent with new and evolving attack patterns.

d. Fuzzy logic

Because of the unpredictability of the anomalous detection of likely network intrusions, the idea of fuzzy logic is well appropriate for proposal of intrusion detection logic in network security [18]. Fuzzy logic permits an object to suitable into different classes at the identical time. Although security requests that implements fuzzy logic have enumerated satisfactory degree of success, it's leaning to consume wide network resources and the lengthy time needed for training, are main disadvantages in the application of fuzzy logic designs in SDN security.

e. Bayesian networks

The Bayesian network system is made based on the naïve Bayesian algorithm that is used mainly for learning purpose, here the where training set with target class is offered. The goal is to categorize an unknown strategy whose class is unidentified.

f. Decision trees (DT)

Decision trees uses algorithm based logical implication and predictive modeling techniques to evaluate target functions that provide discrete values. Intrusion detection system in SDN is a main problem meanwhile networks or users, needs to be recognized either as a valid or ordinary connection, user or as one of the secret attack types. DT is commonly used in the areas of data mining, machine learning, and statistics to solve classification-based problems. DT ideas easily interpretable models that assist network security operators to examine and edit network records and reports [18].

VII. CONCLUSION

SDN has been a popular research area in recent years, especially in relation to traffic engineering, network orchestration, QoS and Security. SDN provides a new paradigm to solve DDoS problem in traditional networks by introducing separate layers for routing and data forwarding. SDN DDoS threat has become an open research field for researchers. In this article, we presented a comprehensive study of the vulnerabilities, threats and risks in the SDN architecture and discussed the solution for those security issues using machine-learning techniques. And in our future work, we will apply machine-learning techniques for accurate detection of behavioral patterns, fingerprinting, attack flows and anomalies in the SDN based networks. We believe that advanced machine learning methods can be successfully applied to detect and classify the baseline and anomalous behaviors in the communication channel in the SDN architecture.

REFERENCES


[7]. Ricardo Macedo, Rafael de Castro, “SelfOrganized SDN Controller Cluster Conformations against DDoS Attacks Effects”, Global Communications Conference (GLOBECOM), 2016 IEEE.


[9]. Yan, Qiao, et al. "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges."


