International Journal of Future Generation Communication and Networking
Vol. 12, No. 3, (2019), pp. 70–79

# Software Defined Networks with Intrusion Detection Scheme

Santosh A. Darade,
*Research Scholar GITAM School of Technology*
*Hyderabad, India darade.santosh@gmail.com*

Dr M. Akkalakshmi,
*Research Guide*
*GITAM School of Technology*
*Hyderabad, India*
*lakshmi.muddana@gitam.edu*

Yogita S. Hande
*Research Scholar*
*GITAM School of Technology*
*Hyderabad, India*
*yhande18@gmail.com*

***Abstract***

*With the explosion of cloud server deployment, the response to a single user request is generated from a sequence of distributed API call(s). Such a distributed environment inherently creates a high-bandwidth of machine-to-machine interaction. Today's networks reconfiguration are performed relatively in a static way to avoid the risk of service interruption. In case of addition & deletion of network devices like routers & switches it is very difficult to network administrator to recognize the networks & manage it to earlier constraints. It is also very difficult to apply a consistent set of access, security, quality of service (QoS), and other policies. So we need a network which is scalable, high-performance, flexible, supportive & programmable. The new network called Software Define Networking (SDN) provides open interfaces that enable network administrator to develop a software that can control the connectivity provided by a set of network resources and the flow of network traffic through all these resources along with possible monitoring and modification of traffic that may be performed in the network. It is necessary to keep track or protect the traffic which is transferred from one machine to another, protection from unauthorized users and information must be available to authorized users when it is indeed. The solution called as Intrusion Detection Scheme, to monitor multiple types of networks traffic sharing the same physical infrastructure and protection to programmability offered by Software Defined Networks (SDN). This paper gives insight into threats detection such as Denial of service; Distributed Denial of service attacks using SDN based Intrusion Detection Scheme (IDS) using genetic algorithm.*

***Keywords—*** *Software Defined Networking; Denial of Service; Distributed Denial of Service attack; Intrusion Detection Scheme.*

## I. INTRODUCTION

The Internet is ever growing and we are truly graveled in a vast ocean of information. When it comes to the Internet there are millions and millions of users logging on and off on a daily basis. The fact is that about 30 – 40% of all users are aware of the things happening on their computers. Today



ISSN: 2233-7857 IJFGCN

Internet-based services such as cloud computing and social networking changed networking demands & requirements (e.g., bandwidth, network topologies, and routing information) dynamically. Traditional networks, have limited ability to change the scope of current requirements because of their static nature. To address these issues, Software Defined Networking (SDN) gives a horizon through new network architecture which allows more flexibility through software-enabled network controller [1]. In SDN architecture, the control and data planes are detached, with logically centralized intelligence controller (SDN Control software) & the underlying network infrastructure is abstracted from the applications as shown in Figure 1 [2][3].

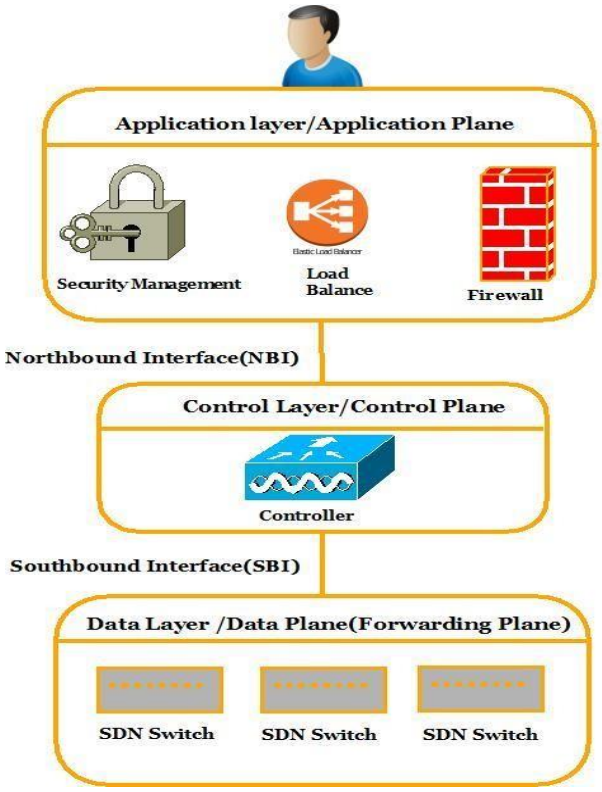


Fig. 1 SDN Architecture

As SDN is supporting many network applications such as programming flexibility at controller & switch level, addition of number devices & policies, among one the security has become an important aspect which was not yet highlighted in SDN architecture. Researcher [4] [5] shown that various security attacks can be conducted against SDN through different network components. As SDN controller was designed & implemented from different software's so it may exploit vulnerability due to continuous update from network administrator or operator [6]. Ultimately it crates impact on SDN security because of the code used to design SDN

may get vulnerable to attacks. Now it's an opportunity to provide a security to the SDN controller which we are thinking to cope up. Such implementations enable more flexible security controls in the dynamic & logical networking environment.

## II. TRADITIONAL NETWORKS CHALLENGES

Since traditional network unable to handle dynamic changing traffic patterns & high bandwidth requirements, there are several factors that give strength to SDN as an alternative to traditional networks. [1][2][7].



ISSN: 2233-7857 IJFGCN

*A. Changing traffic patterns:* If user wants to access their applications from any device, anywhere, anytime & from any networks whether it is wired or wireless which results additional data traffic across wide area network. This shows we need a computational model or underlying networks architecture to carry large amounts of traffic, and to deploy a number of distinct, dynamic applications & service which will handle all these traffic through programmable software.

*B. Need for more bandwidth:* As mentioned earlier because of increased traffic requires parallel processing on thousands of inter-connected servers. Data center also need to be scaling to very large size, while maintaining end-end-end connectivity. With the higher media/content traffic increases, requirement of more bandwidth increases.

*C. Need of flexible access to IT resources:* Users want to access the applications from any devices, anywhere, anytime & from any networks whether it is wired or wireless, which results additional data traffic across wide area network. It is mandatory to protect these devices also while protecting corporate data.

*D. Insecure Connectivity:* The success of the Internet is openness and connectivity (end to end) must be secure. However, few investors are limiting these fantastic features and generating revenue by exploiting security features.

*E. Static nature of network:* Network reconfigurations are performed relatively in static way to avoid the risk of service interruption. In case of addition & deletion of network devices like routers & switches it very difficult to network administrator to recognize the networks & manage it to earlier constraints. It is also very difficult to apply a consistent set of access, security, quality of service (QoS), and other policies.

*F. Scalability issue:* We need a new network which is scalable, high-performance; low-cost connectivity among many physical servers, flexible, supportive & programmable, it must give better differentiated service to users with different applications and needs.

*G. Security, Authentication, Trust:* 12% of IT business technologist stated that SDN has security challenges, and 31% were undecided whether SDN is a less secure or a more secure network paradigm than others [3]. A great concern to businesses, public administration and citizens are security and authentication. They are not addressed efficiently in the current Internet. So it is very important to increase trust without compromising openness.

*H. Volume:* The biggest task in internet in coming time is to handle 4 billion mobile users worldwide.

*I. Privacy and Confidentiality:* A machine to machine communication is also growing these days. The new application must obey user's right to privacy and confidentiality.

## III. RELATED WORK ON SDN SECURITY ISSUES

If Software Define Networking popularity is increasing, then the security in SDN must be an important agenda. The gap that still exists & not yet highlighted by different authors regarding security issues in SDN.

In [4] Nick McKeown et.al brief on how to add OpenFlow to their switch products for deployment in schools, college campuses, & universities as a backbones and wiring closets. Its good paper for beginners towards implementing OpenFlow table to their switch but here no specific method & protocol mentioned to detect intrusion. An experimental result shows that implemented methodology doesn't detect network level attacks such as spoofing, IP spoofing.

The proposed architecture of scalable intrusion detection scheme implemented on virtual Software Defined Networks environment [5] using a virtualization (kernel based virtual machine) focuses on distributed traffic sampling at network switches for malicious traffic inspection. In case of new malicious packets arrives in the network then detection of that packet is not possible by using Suricata



ISSN: 2233-7857 IJFGCN

IDS because provision of signature updating is not reflecting into the architecture. In case of increase in traffic flows the Suricata IDS is not scalable for future SDN based technology.

The Learning-IDS (L-IDS) is an intrusion detection Scheme for networks used to communicate with embedded mobile devices. The system was implemented on mobile device with in institutional boundaries without modification to the embedded device. Richard Skowyra, et.al. [8] Technique proposed is anomaly (Packets' sent, position, time passed, size, etc) based detection, so chances of generating false alarms are more. Such IDS required lot of historical data to test in an offline environment. There is no provision made for false positive alarm detection in L-based IDS.

Antonio Gonzalez et.al [9] offers programmability for the detection and prevention of intrusion in SDN, such as on path and off path in two ways. They preferred off path intrusion detection system to increase the network performance but have not defined the IDS functionality as well as position of IDS in SDN networks.

In [10] the author has made a comparative survey related to security in SDN by introducing different framework, a set of conclusions & proposals for future research directions are presented. All security techniques such as SANE, Ethane, ProtoGENI, STRIDE threat analysis discussed shows some security loop falls at their end.

The author in [11] has proposed a concept of new open flow switch which has inbuilt Intrusion Detection System. An IDS uses the database for IP verification and packet verification. Basis of IP verification techniques has not given,

such type of IDS implementation may be complex and it degrades the network performance.

Diego Kreutz et.al [12] argues on building secure & SDNs by design. Authors described seven potential threat vectors that may enable the exploit of SDN vulnerabilities. Several threat vector identification mechanisms discussed at SDN control level such as replication, diversity **(**e.g., software bugs or vulnerabilities). The general ideas about threat identification along with detection have been explained in this paper & trigger the discussions in SDN community around security issues. This paper triggers new ideas for those who want to do the research the field of Security in Software Defined Networking.

In [13] presented measurement method which allows collecting network traffic parameters, generated by virtual SDN environment. Soft computing approach such as artificial network, fuzzy logic is applied on dataset collected to detect suspicious activities in SDN environment.. It's very difficult for proposed methods to detect real time attacks because system was not tested on standard dataset & the matching of dataset with flow table degrade the performance of networks.

## IV. SDN SECURITY THREATS OR COUNTERMEASURES

Many researcher working hard for successful deployment & interoperate of SDN's over existing traditional networks but there has been limited push towards research in the field of security aspect of SDN from industry as well as from academics [8]. The hard work carried out by these researcher towards successful deployment of SDN's in the absence of proper security and intrusion detection mechanisms has no meaning because every layer of SDN exploits the vulnerability by attacker [14]. For example attacker can attacks on switches flow table which has information about; network management, switching, routing & access control. Attacker can also attacks on controller because it is central part of SDN. The communication between the SDN controller & switches is another major target of attacker. Following are the possible attacks which can affect on functionality of SDN resources [1].

### *A. Spoofing*

In Spoofing the attacker forged the networks information such as IP, MAC, ARP packets using faked IP address. Attacker may use fake IP address to gain access of network resources. An aim of spoofing is to flood the network & creates large number of attacks such as SYN flooding, Smurf etc. Spoofing denies



ISSN: 2233-7857 IJFGCN

the use of network resources to authorized users which create Denial of Service attacks, Distributed Denial of service attacks. Currently measure threat in SDN is because of IP spoofing & Address resolution protocol spoofing.

*B. IP Spoofing*

IP spoofing is usually open the doors of all other security attacks such as DNS modification/ tampering. Attacker can manipulate the DNS directory & reroute the traffic of legitimate websites which can be a part of large flooding or worm spreading attacks. IP spoofing methods always tries to redirect the traffic to illegitimate hosts which leads to man in the middle attacks. In SDN we required a properauthentication mechanism to avoid unauthorized intrusions or use of these resources.

*C. Denial of Service Attack*

DoS attacks are a series threat in the networking environment that affect the network performance, increase the latency, & drop the legal packets. DoS attack interrupting in the network connection between the users or making some services unavailable for user or disrupts the entire network by overloading with unwanted messages, so that network becomes slow and unavailable for users. Because of DoS attacks, attacker can overload the SDN controller & switch (flow table) memory to interrupt the normal activities.

*D. Modification*

Modification also called as tampering or destruction of network information, such as topology, flows in flow tables, policies, and access lists. For example, an attacker may try to send the unwanted rules into the network which will cause network misbehavior. Because of these unwanted rules entry into the flow table or firewall rules that will denies use of network resources to authorized users or allows unauthorized users. Attackers aim to capture the traffic & modify the traffic rules to flood the flow table with wrong rules. SDN controller communicates with southbound & northbound API, the reason it is very important to secure this communication from being tampered.

*E. Repudiation*

In case of repudiation the sender can't denial one of the entities involved in a communication or having participation in all part of communication. Principle of non-repudiation states that if sender sends some information and later on he denied that he never sends that information. Non-repudiation tries to make sure that such denial does not occur. In SDN non-repudiation helps to prove the identity of the sender who always tries to send illegal information on controller & switch.

## V. SDN WITH INTRUSION DETECTION SCHEME

Popularity of Software Define Networking is increasing then security in SDN must be an important agenda. The principles of a secure communications are confidentiality, integrity, availability of resource to authorized users, authentication and non-repudiation. The success ration of Internet is reduced because of network security threats, denial of service attacks, malicious software & the internal as well as outside attacks. Security professionals must take an initiative to secure the data & network assets (e.g. devices). Here we are trying to design a programmable software design networks & checking its scalability as well as complexity at high priority.

As shown in Fig 2, the network traffic is receiving at switch level & from switch it communicates to SDN controller for their route. SDN controller is configured to install the rule to send the packet to its destination and to the Intrusion Detection Scheme & also responsible for authentication of hosts and policy enforcement.

Outside network traffic received by SDN switches are sampled through packet counter method to identify the



ISSN: 2233-7857 IJFGCN

suspicious flow and forwarded towards IDS for intrusion detection.

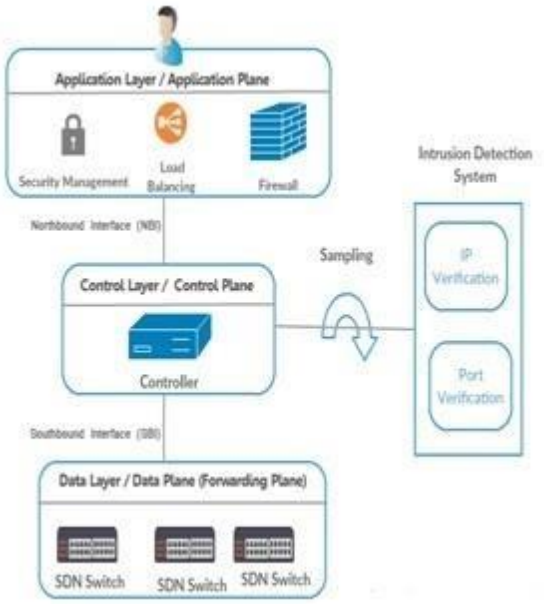


Fig. 2 Intrusion Detection Scheme for SDN

Packets counter method – This mechanism is comparing the number packet coming in particular time period with defined threshold value to catch suspicious flow. Identified suspicious flow accelerated towards IDS.

The Intrusion Detection Scheme (IDS) contains set of database (rules) patterns; based on these rules IDS notify intrusion. IDS having databases for IP address verification and port address verification. Suspicious flow packet details are match with IP address and Port address for intrusion detection.

IP address verification: IDS with IP address database consists of intrusion IP address that frequently performed attack on network (For Example if packet is coming from same source again & again the IDS will check the number of packets coming from same source within the specific time duration having same IP address, port number, protocol used). Malicious flow packet address verify with IP address database to detect intrusion.

Port address verification: IDS with port address database consists of mostly occurring port number for attack. Malicious flow packet details are again verified with port address database for intrusion detection.

The Intrusion Detection Scheme identifies intrusion and generates an alert which will send to the controller. When the controller is notified by the IDS, it lists all the flows installed in the OpenFlow switches and set a drop action to all the flows that matches the malicious one. As per the IDS results, the malicious packets get block at switch level itself.

Genetic Algorithm based approach selected to generate/define set of rules because of the simple representation of rules and



ISSN: 2233-7857 IJFGCN

the effective fitness function, the proposed method is easier to implement, while providing the flexibility to either generally detect network intrusions or precisely classify the types of attacks.

The following rule shows that, it classifies a network connection as the denial-of-service attacks *neptune*.

***if*** *(duration="0:0:2" and protocol="arp" and source_port=*1022 *and destination_port=513 and source_ip="9.9.9.9" and destination_ip="10.0.0.2")*

***then*** *(attack_name="neptune")*

The above rule expresses that if a network packet is originated from IP address 9.9.9.9 and port 1022, and sent to IP address
and port 513 using the protocol *arp*, and the connection duration is 2 second, then most likely it is a network attack of type *neptune* that may eventually cause the destination host out of service.

The system implementation divided in two parts: an offline training system for defining rules from historical data set especially (DARPA), and an online detection system that uses the generated rules to classify incoming network connections in real-time environment.

## VI SDN BASED IDS USING GENETIC ALGORITHM

**Algorithm:**

1. Received packets
2. Identify suspicious flow
   Apply sampling technique
   Packet counter method
   IP Address & Port address verification
3. Send suspicious flow to IDS
4. Identify attacks

Apply Genetic Algorithms to identify DoS attacks

5. Block attacks

Algorithms shows how SDN based IDS helps to detect DoS & DDoS attacks using genetic algorithm.

## VII IMPLEMENTATTION AND RESULTS

Using python programming language we can write our own POX controller components to program the SDN network or to control the flow of SDN network. Putty software tool is basically used to represent the flow of network in the graphical way. For example, we can represent host nodes, switches and controller using putty tool. Xming - software tool is generally used to support functionalities of putty tool in windows OS environment Following are the different steps which shows our implementation and results.



ISSN: 2233-7857 IJFGCN

1. Controller is up and there is network traffic between hosts.
2. Miniedit is used to virtually represent configuration of network
3. Ping command is used in root terminal to initiate the traffic between hosts
4. Python program is executed using POX controller
5. Final output showing Neptune attack detected as shown in figure 3.

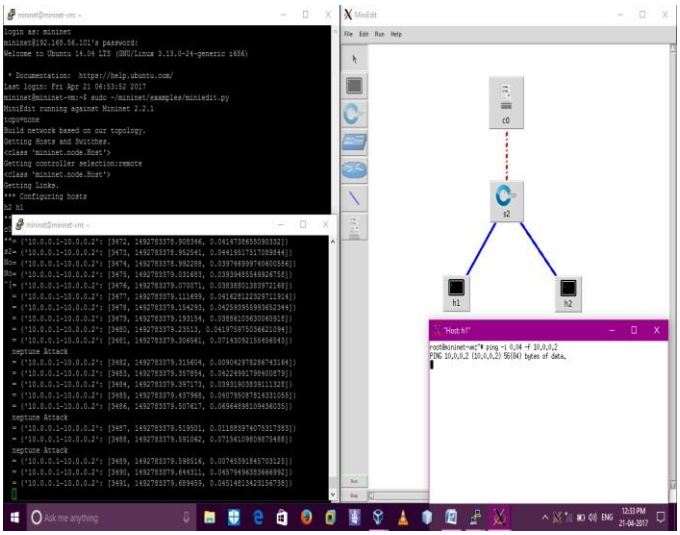

Fig. 3 SDN based IDS to detect DoS & DDoS attacks

## VIII BENEFITS OF IMPLEMENTING SND WITH IDS

Intrusion Detection Scheme is the most important tools that analyze & protect networks from inside as well as outside attacks, it monitors network behavior or patterns which look suspicious & detect them as an intrusion [15].

- SDNs lower operating expenses: - Implementing SDN with IDS requires less expense to design a SDN networks which avoid all burdens of network developing team.

- Flexible**:** - The development tools available make it easy to reconfigure the network very smoothly & it depends on user, how they want their own networks to be.

- Provides virtual management for computing & storage resources so that resellers can also plan IT strategies more effectively for their customers & apply security policies to the given networks.

- The biggest advantage of SDN network is infrastructure savings, because of separation of control & data plane reduces hardware prices as routers and switches must compete on price-performance features.



ISSN: 2233-7857 IJFGCN

## IX CONCULTION AND FUTURE WORK

Software Defined Network with Intrusion Detection Scheme is useful tool which will block the malicious flow of the network traffic specially the Denial of Service & Distributed Denial of Attacks & notifies to controller. The implemented IDS tested using mininet on controller level. We are also going to check the possibility of programming on switch level. Our future work is applying lightweight intrusion detection algorithm, to monitor the network traffic & also allowing multiple IDS virtual machines running in the same network.

Will further study the attack pattern, characteristics of various malwares, finding out malware detection techniques and explore the possibilities of employing them in the context of SDN with IDS. In addition to that we want to take better advantage of infrastructure and test our Scheme at a larger scale in order to give good optimization & scalability to our designed scheme. We want to keep this SDN based Intrusion Detection System running along with possible rule updating after some time interval in order to detect real time traffic & networks attacks.

## ACKNOWLEDGMENT

Special thanks to our Research guide Dr M. Akkalakshmi for her consistent guidance & support. We are also thankful to Mr. Nimit Shishodia, CEO of Ecode Networks Ltd. UK for guiding us on SDN concepts.

## REFERENCES

[1] Izzat Alsmadi, Dianxiang Xu "Security of Software Defined Networks: A Survey," Elsevier Science Direct 21 May 2015.

[2] ONF White Paper "Software-Defined Networking: The New Norm for Networks" April 13, 2012.

[3] Open Networking Foundation "SDN architecture" Issue 1 June, 2014.

[4] Nick Mckeown, Tom Anderson, et.al., "OpenFlow: Enabling Innovation in Computer Networks, 2008.

[5] Chiwook Jeong, Taejin Ha, et.al., **"**Scalable Network Intrusion Detection on Virtual SDN Environment,**"** IEEE third International conference on cloud networking, 2014.

[6] Angle, V. C., Lorena, B. L., Luise, C. V.: "Evolution and challenges of software Defined networking", IEEE on SDN Future Network and Services (SDN4 FNS), pp. 1-7, Nov 2013.

[7] Hrishikesh Arun Deshpande **"**Software Defined Networks:Challenges, Opportunities and Trends," IJSR, ISSN (Online): 2319-7064. Volume 4 Issue 9, September 2015.

[8] Richard Skowyra et.al., "Software-Defined IDS for Securing Embedded Mobile Devices," IEEE 2013.

[9] Antonio Gonzalez Pastana Lobato et.al., "An Architecture for Intrusion Prevention using Software Defined Networks" Universidade Federal do Rio de Janeiro - GTA/COPPE - Rio de Janeiro, Brazil.

[10] S. Scott-Hayward et.al., "SDN Security: - A Survey," IEEE on SDN Future Network and Services (SDN4 FNS), pp. 1-7, Nov 2013

[11] S. Kumar, T. Kumar, G. Singh, M. Nehra," Open Flow switch with Intrusion Detection System," International Journal of Scientific Research Engineering & Technology,Vol 1, Issue 7, pp 001 – 004, Oct 2012,ISSN 2278-0882.



ISSN: 2233-7857 IJFGCN

[12] Diego Kreutz et.al., "Towards Secure and Dependable Software-Defined Networks," *HotSDN'13,* August 16, 2013, Hong Kong, China.

[13] Damian Jankowski et.al., "Intrusion Detection in Software Defined Networks with Self-organized Maps," Journal of telecommunications & information technology 4, 2015.

[14] S. Sezer, S., Scott-Hayward, P. Chouhan, "Are we ready for SDN?- Implementation Challenges for Software- Defined Networks", White Paper.

[15] Santosh A. Darade, Dr M.Akkalaksmi, Yogita S. Hande "Security Techniques in Software Defined Networks with 5G Network," Volume: 05 Special Issue: 05, ICIAC – 2016, May- 2016.

[16] Yogita Hande, Akkalashmi Muddana, Santosh Darade "Software-Defined Network-Based Intrusion Detection System" H.S. Saini et al. (eds.), Innovations in Electronics and Communication Engineering, Lecture Notes in Networks and Systems 7, 23 https://doi.org/10.1007/978-981-10-3812-9_55.



ISSN: 2233-7857 IJFGCN