International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7, Issue-6, March 2019

Advanced Defence Mechanisms for Future Network Security using SDN

Jisha S Najeem, Prabhakar Krishnan

Abstract*: Currently, the technology landscape is growing at a tremendous pace and new networking paradigms are emerging such as "Software-Defined-Network (SDN), Network-Function-Virtualization (NFV), Internet-of-Things (IoT), Industrial Internet (IIoT, SCADA), Industry 4.0, SDWAN, Software defined infrastructure (SDX), Internet Exchange Points (IXP), Software Defined Perimeter (SDP), M2M" and many more. Conventional network defence mechanisms are not sophisticated enough to overcome these challenges as they can detect only the rudimentary attacks, permitting attackers in exploiting the vulnerabilities in the modern network. In this paper, we proposed various novel secure and distributed SDN-based defence architectures for legacy networks, containing dedicated engines for traffic management, behavioural analysis and Anomaly detection. We have also conducted a comprehensive study of state-of-the-art defence mechanisms and frameworks that have evolved to resolve security problems of the future networks and our study compares the efficacy of our proposed defence mechanism.

Index Terms*: SDN, IoT, NFV, *Intrusion Detection Systems (IDS), Network Security, , Network defence, OpenFlow.

I. INTRODUCTION

Large enterprises and data centres have increasingly adopting Network Intrusion Detection Systems (IDS), for detecting and mitigating malware campaign and attacks. Network IDS/IPS are implemented as middle box systems, that do deep packet inspection, flow based and signature-based packet level analysis. Such centralized NIDS are not efficient for deployment in high-speed networks, as DPI takes more processing overhead.

Software Defined Networking (SDN) paradigm is a paradigm shift that happened to address these challenges, since it brings in centralized control for defining policies for traffic management & routing and distributed enforcement of these policies such as flow-control, forwarding logic, QoS of the network. In SDN infrastructure (Fig.1) the control layer is centralised, which is the root of the trust and certain level of trust of identifies are distributed across multiple SDN components. In the software defined/driven networks, the whole network domain appears to be a single virtual switch. In our systematic survey on SDN/NFV security, we investigate different frameworks provided by SDN/NFV to enhance network security and information security process. The security of SDN spans across multiple disciplines: physical application area – smart-grid/IoT/Embedded systems and cyber area- protocols, malware, DDOS detections etc. Distributed Denial of Service (DDoS) attack methods is popular to degrade availability of targeted service on the Internet. IDS techniques are used to protect the system from attackers, but such systems are not designed to mitigate all DDoS attacks. Researches have showed possible vulnerabilities, growing threats, expanding attack vectors and provide security solutions. The SDN infrastructures are backward compatible to interface with the sFlow protocols on legacy network switches/routers and use SDN specific protocol OpenFlow and this whole SDN deployment can be monitored and managed by a sophisticated software-based centralized controller. In Large scale network SDN systems can be deployed encompassing multiple network segments with one controller per domain and whole network orchestrated by a central console controlling multiple SDN controllers.

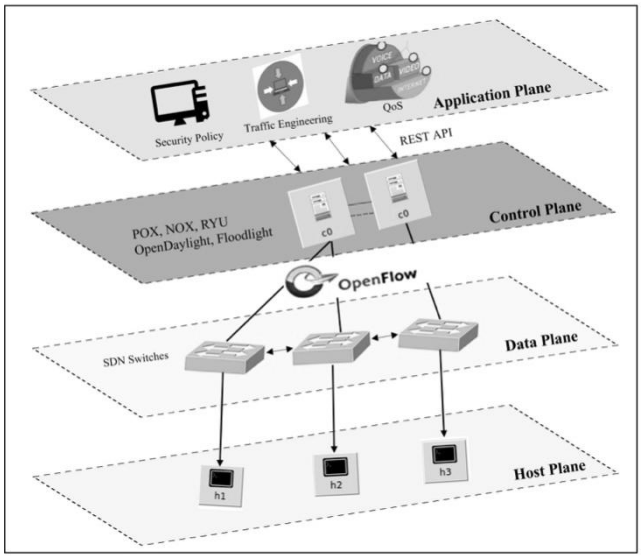

Fig 1. SDN Architecture

The rest of this paper is organized as follows: related works in Section II, our proposal of a suite of novel SDN based security and defence mechanisms in Section III, our experiences with the evaluation in Section IV, one use case of our security framework for IoT architecture in Section V and the paper concludes in Section VI.

Revised Manuscript Received on 30 March 2019.
***** Correspondence Author
Jisha S Najeem, Amrita Center for Cybersecurity Systems and Networks, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Amrita University, Amritapuri, India
Prabhakar Krishnan, Amrita Center for Cybersecurity Systems and Networks, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Amrita University, Amritapuri, India.

II. RELATED WORKS

Different mechanisms are being used by SDN/NFV technology such as OpenFlow, to improve the performance of DDoS mitigation. The methodology behind the OpenFlow mechanism is that OpenFlow enabled switches has the ability to modify the flow rules in OpenFlow table thereby, mitigating attacks by blocking malicious traffic. Even though there are multiple DDoS mechanisms, its detection is a hard task since it is difficult to distinguish between normal traffic and useless packets, sent by compromised hosts to their victim.

Cbench [1] proposed another modification into SDN networks with the introduction of fingerprinting mechanism. Enables feasibility by experimenting a realistic attack use case to an SDN network with real-world experimental data. But another potential vulnerability lies within the flow table capacity of the SDN switches. Due to frequent communications between the controller and the switches, an attacker can leverage the interactions thereby degrading the perceived performance of an SDN network.

SLICK [2] a network programming architecture decoupling central control plane responsible for initializing and migrating functions on to customized middle-boxes in the SDN network. Application directs SLICK controller for routing specific traffic through its middle-boxes. Using SLICK middle-boxes, a modular application is being created and trigger an asynchronous communication to the SDN that transverses the flows triggered during the communication.

On a survey of basics of security configurations using SDN in OVS-based (Open vSwitch) vProbe [3] capable of adding and processing monitoring metadata on the northbound offers a full control as well as a more limiting intent-based interface. vProbes integrated with orchestration layer assures end-to-end services delivered over the physical and virtual network and enables operationalization of virtual next-generation networks through dynamic control and operations automation.

Motivated by security in SDN environment, Delta is one among the first penetration testing tool. A new SDN framework that can automatically instantiate attack cases against SDN elements and can also assist in uncovering unknown security problems within an SDN deployment. A more simplified version has been contributed by Radware, inbuilt in the Opensource controller, OpenDaylight [4] project, DefenseFlow. This application measures bottleneck traffic flows collected by the SDN controller and monitors flow statistics pattern regardless of the type of attack.

III. PROPOSED DEFENSE MECHANISM USING SDN

In this section, we discuss integrating SDN into conventional network architecture. The logically centralized controller allows improving the policy-deciding process, distributing the policy- enforcement process across the switch(es). In legacy networks, the complete network functions get deployed in the form of standalone middleboxes or appliances and hence implemented independently. Hence, realizing autonomous control of configuration and access control policies in the network. In SDN based networks, only the policy-rule enforcement part of the network functions is distributed/delegated throughout the data plane switches. The control operations are executed at the control plane applications and flow-rules are installed to the data plane switches through the OpenFlow channel. Thus, network policies, traffic shaping, security, QoS functionalities such as IPS, IDS, virtualized network functions(VNFs), bandwidth management, ACLs are managed in the data plane OF switches. The control plane installs the flow-rule/match-action entries, programmed by specific SDN applications running in application plane.

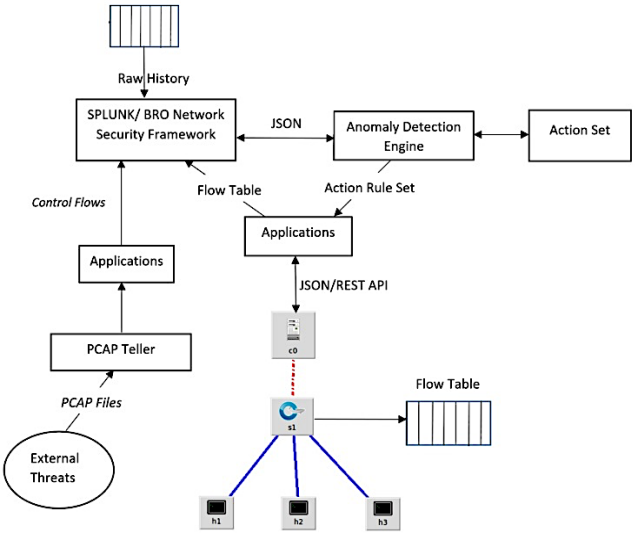

Fig 2. Proposed Defense Framework

We proposed a new secure and distributed novel conceptual SDN-based framework (Fig.2), that consists of a dedicated module for traffic management and Anomaly detection engine. OpenFlow enabled switches can create flow tables which are then matched up with the historical flow table using the anomaly detection engine. Using *Bro Network security framework* or network packet broker integrated with SNORT IDS system, this anomaly detection module can detect intrusion activities in real-time as well as offline.

The Bro Network security framework provides real-time threat mitigation as well as more general network traffic analysis, making it a powerful intrusion detection system (IDS). Bro architecture supports *libpcap* package, also a passive network tool thereby supporting network tap or using and a span sport in SDN Switches without being another node on the monitored network. Once Bro receives IP packet, Bro inspects the network traffic and its event engine is responsible for detecting malicious traffic and then converting them into events. It can also detect flows coming from packet broker and thereby can send shunting commands to the visibility network. The events are then forwarded to the policy script interpreter and then actions are being triggered out depending on the outputs. The logs from Bro can be visualized using the tool such as SPLUNK, Elastic Search, and Kafka.

IV. EVALUATION

For a comprehensive study of state of the art SDN systems and to investigate the efficacy of SDN based defence mechanisms,

we have built a network security research platform which is reconfigurable and provides extensible test beds. Through this platform, we were able to emulate network configuration & attacks in real world deployment and applications and also develop targeted defence mechanisms for different attacks. Our study included enumeration of various advanced attack scenarios and experiment the applicability of our SDN based defence mechanisms in each test bed.

The experimental platform was developed utilising a combination of hardware SDN switches and software emulated SDN switch such as Open vSwitch on a virtualised testing environment, OpenDaylight controller and mininet, a single console that allow users to manage and design virtual network topology. To evaluate the attack vectors, some experimental scenarios has been deployed on the SDN testbed using two virtual machines (VMs) connected on the same network. We used KVM for host virtualisation. We have also used different SDN controllers and developed custom defence mechanism and did comparative study around them. The controllers are deployed to be in a secure private network on a different machine running secure Ubuntu 14.04 operating system.

After running the attack tools in our experimental testbed, we will analyse the data logs of attacks, defence and monitoring mechanisms in SDN environment. We have developed a novel cooperative monitoring engine which monitors the entire network, with active probes deployed at each end point and network devices in the architecture under study. The deployed SDN Testbed covers OpenDaylight SDN controller using OpenFlow 1.3 protocol. According to the OpenFlow protocol, Discovery in SDN includes the discovery of the switches, links, and hosts to know the features of a controller, providing the intelligence of the network. And about the switches in its control domain and discovering the attach points of hosts. After the establishment of a connection between a switch and a controller, the controller periodically sends commands to switch to flood Link Layer Discovery Protocol (LLDP) for direct links and Broadcast Domain Discovery Protocol (BDDP) packets used in discovering the switches in the same broadcast domain through all its ports.

A discovery protocol packet typically contains the Data path ID (DPID) of the sender along with the port of the switch corresponding to the received message. The reserved set of destination MAC addresses and Ethernet types used by the discovery protocol packets lets the controller differentiate them with the other data packets. Combining LLDP and BDDP packets, the controller discovers the direct and indirect connections between the switches, and the liveliness of the connections regularly with periodical checks. Using these protocols, the controller can discover the attach points of each host that are connected to the switches.

Packets are being sent from multiple hosts to the controller creating flow entries. When all the possible entries are installed, verifying the flows installed in the OVS switch by dumping the flows in the mininet console. To test the firewalling rules in OVS switch, hping3 tool a network tool used to send custom TCP/IP packets. Act as a hide ping, useful when the host target is behind a firewall by dropping ICMP packets. Using *hping3* from one VM1 to another VM2, resulting in DoS attacks. This method involves saturating the host VM2 with external communication requests, by not responding to legitimate traffic due to server overload. Under advanced network attack and large-scale attack scenarios, we have measured and compared our architecture over two axes:

- Efficacy and accuracy of the defence
- Performance and processing overhead of our defence mechanism

As the number of devices on the Internet is growing at a rapid pace, with the proliferation of mobile and IoT devices, the volume of network traffic has phenomenally increased. Most critically, the crucial function of any IDS/Firewall is the response time to security attack and mitigation time required after the discovery of the attack and the malware on the network. We show our fast response (Fig.3) to mitigate the DoS attacks with SDN based security mechanism.

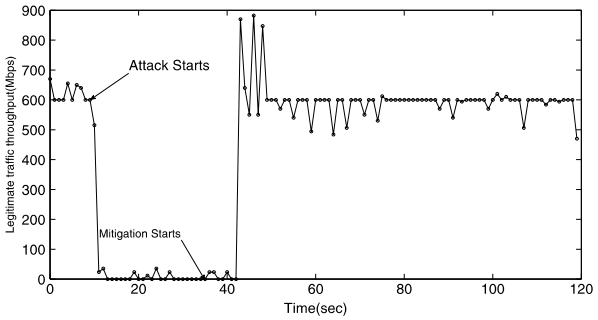

Fig 3. Response of SDN Defense Mechanism

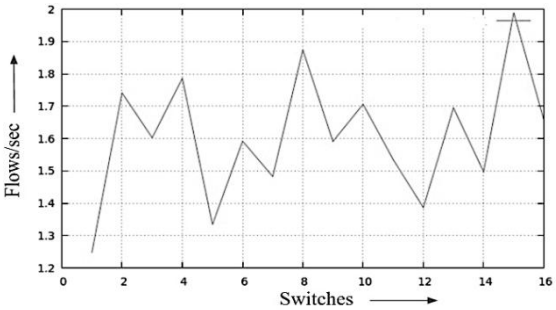

Fig 4. IDS Performance before Attack

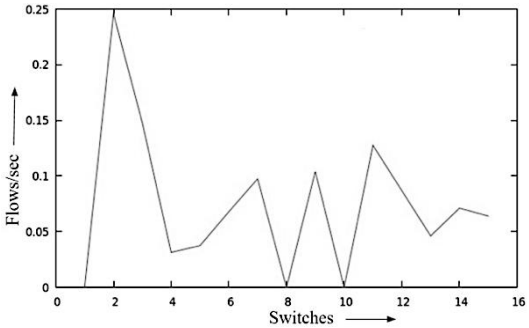

Fig 5. IDS performance after DoS attack

The traditional defence mechanisms today lack the required granularity and responsiveness in the large enterprise or public network. But our proposed defence architecture has the distributed presence and features for dynamically configure the security signatures and rules to detect or prevent attacks. To compare the two paradigms – legacy and our SDN, we conducted experiments with Linux IPTABLES, SNORT and also our SDN defence mechanism.

On large scale, simulated series of attacks which involved more than 1000 rules/filters after every attack, our results show (Fig.4) that the traditional firewall takes longer time to add new rules and at about 10,000 rules on the firewall the IDS simply becomes a bottleneck in the network. But with our SDN defence, we could rapidly add rules as high as 2000 at a time and there was no limit to saturate the SDN based IDS. The significant improvement (Fig.5) is that with SDN defence, the defence rules can be deployed in constant time at multiple points in the network just with a single protocol command from the controller and the latency is negligible in the ingress and egress networks.

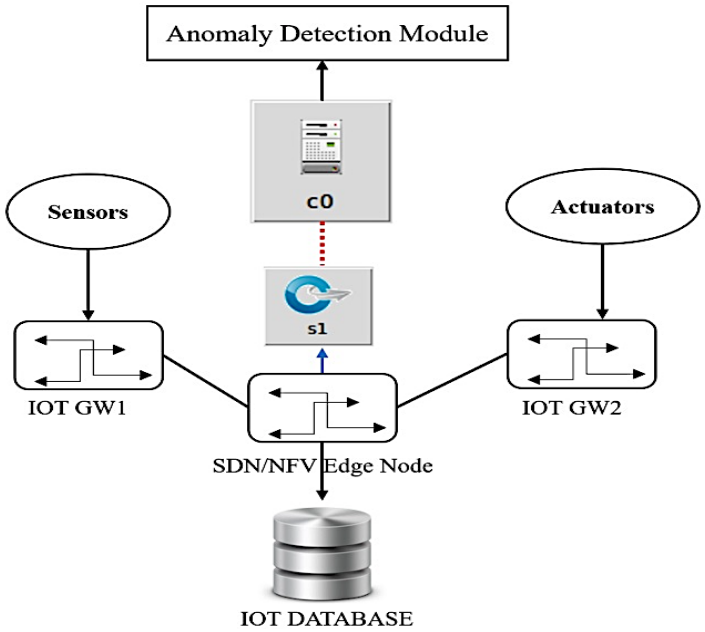

Fig 6. SDN enabled Secure IoT Architecture

V. USE CASES

Exploring the proposed architecture for coordinate responses in DDoS mitigation, Network level intrusion detections and security in Cyber-physical systems such as Internet of Things (IoT) and Industrial Networks ICS/IIoT/SCADA/Wireless Sensor Networks.

Security in IoT must be implemented at various layers (Fig.6) – the supply chain, the chip, Operating System, device, network and the system level. On top of this it needs to be adapted to the constraints presented by the devices that comprise the IoT network. IoT devices send out sensitive information that must be protected from unauthorized usage or disclosure. A key primitive to achieve this goal is to establish an immutable trust-base that cannot be tampered with. The designed architecture is used to establish secure communication between IoT devices and how flows can be routed between controllers. Having multiple controllers provides trustworthiness and fault tolerance.

A framework to improve the security in IoT based on the SDN architecture paradigms will be implemented and its security effectiveness will be measured under real IoT network and simulated with virtual IoT network for large scale IoT. Common attacks in the Cloud, inter-domain attacks (DoS, spoofing, MITM, fuzzing, scanning) would be simulated in the SDN-IoT testbed and the efficiency/resilience of the proposed framework would be computed. For large scale network, using Openstack Cloud or interconnected IoT clusters over WAN (simulated Cloud).

To secure a large farm of IoT device network in the cloud, we must enumerate all possible vulnerabilities and attack vectors and build a model that can predict the attacks. Programmable features of SDN for more processing at the "edge", more flexible reconfiguration of devices or removal of insecure devices. Security and admission control done at the edge/gateway before it gets into the network. Thereby, by improving security in adhoc and large-scale industrial networks. Further apply the proposed model to synthesize a set of potential real-life attacks adversaries could launch against SDN networks. Finally, we intend to provide security recommendations to address the threats.

For Industrial networks, such as Supervisory control and Data Acquisition (SCADA), we investigate the benefits of using SDN to assist in the deployment of next generation SCADA systems. Basically, only few Intrusion Detection systems (IDS) are currently available for industrial networks. Using the SDN paradigm to fingerprint the SCADA network, extract traffic patterns and enforce these traffic patterns, which allows us to detect and prevent various network attacks such ARP spoofing, replay attacks, detect malicious command forwarding behaviours, filter out flooded responses from control and field devices caused by spoofed requests. This anomaly detection approach through SDN framework relies on establishing behavioural models through observing & verifying the network behaviour of SCADA components.

VI. CONCLUSION

SDN is an evolving technology and new players are entering the market, where the security is largely undefined.
This paper has outlined a comprehensive study in discussing different defence mechanisms currently in SDN world in addition to the introduction of a new conceptual SDN architecture.

Fine-grained distributed network traffic monitoring using SDN is an important capability for effective network management and defence. The key research question we have attempted to answer in this work is whether the emerging SDN architecture can provide dependable defence mechanisms and be the next-generation firewall or IDS/IPS for the modern networks and large cloud networks. The long-term objective of this research is to produce an SDN/NFV based security monitoring and defence solution, develop reference defence modules for various network applications, design agile, scalable SDN architecture with highly responsible systems that can dynamically learn and adapt to attack patterns, network traffic and targeted security management.

REFERENCES

1. Tootoonchian, S. Gorbunov, Y. Ganjali, M. Casado, and R. Sher-wood, "On controller performance in software-defined networks." Hot-ICE, vol. 12, pp. 1–6, 2012
2. Anwer, T. Benson, N. Feamster, D. Levin, and J. Rexford, "A slick control plane for network middleboxes," in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013, pp. 147–148.
3. H. Mahkonen, R. Manghirmalani, M. Shirazipour, M. Xia and A.Tackas, "Elastic network monitoring with virtual probes," in Network Function Virtualization and Software Defined Network (NFV-SDN), 2015 IEEE Conference on. IEEE, 2015, pp. 1–3
4. J. Medved, R. Varga, A. Tkacik, and K. Gray, "Opendaylight: Towards a model-driven sdn controller architecture," in A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th Inter-national Symposium on. IEEE, 2014, pp. 1–6.
5. S. Shin, P. Porras, V. Yegneswaran, and G. Gu, "A framework for inte-grating security services into software-defined networks," Proceedings of the 2013 open networking summit (Research Track poster paper), ser. ONS, vol. 13, 2013.
6. Autenrieth, J.-P. Elbers, P. Kaczmarek, and P. Kostecki, "Cloud orchestration with sdn/openflow in carrier transport networks," in Trans-parent Optical Networks (ICTON), 2013 15th International Conference on. IEEE, 2013, pp. 1–4.
7. O. Flauzac, C. Gonzalez,´ A. Hachani, and F. Nolot, "Sdn based architecture for iot and improvement of the security," in Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on. IEEE, 2015, pp. 688–693.
8. Scott-Hayward, Sandra, Gemma O'Callaghan, and Sakir Sezer. "SDN security: A survey." Future Networks and Services (SDN4FNS), 2013 IEEE SDN For. IEEE, 2013.
9. Acharya and K. Arpitha, "An intrusion detection system against udp flood attack and ping of death attack (ddos) in manet."
10. M. G. B. A. Nair, Mol and Nair, "A mediator based dynamic server load balancing approach using sdn," in International Journal of Control Theory and Applications, 2016, pp. 6647–6652.