Prevention of Service Denial in Collaborative Network

Gangotri Tamman
PG Student
Department of Computer Science and Engineering
PDA College of Engineering, Kalburgi

Prof. Patil Rekha
Assistant Professor
Department of Computer Science and Engineering
PDA College of Engineering, Kalburgi

Abstract

Software Defined Networking (SDN) is a developing innovation that pulls in noteworthy consideration from both industry and the scholarly community as of late. By decoupling the control rationale from the shut and restrictive executions of conventional system gadgets, it empowers analysts and specialists to outline new imaginative system capacities/conventions in a significantly more adaptable, intense, and simpler way. SDN gives new research chances to security, and it can incredibly affect organize security inquire about in a wide range of ways. In any case, till today, SDN has not been very much perceived by the security group yet. The new elements given by SDN can help improve organize security and data security prepare. By efficiently thinking the open doors acquainted by SDN with system security, new bits of knowledge for future research has been given in this essential region.
Keywords: User, Register, Password, Attacker, Administrator, UTM, SDN

I. INTRODUCTION

Software Defined Networking (SDN) has immediately risen as another promising technology for future systems. With the division of control plane from information plane along these lines empowering the simple expansion of new, inventive, capable system capacities/conventions, SDN has pulled in huge consideration from both academia and industry. In academia, since the production of OpenFlow, which is a key part to understand the SDN idea, many research thoughts in view of SDN/OpenFlow have been proposed (and still go on). In industry, SDN is broadly considered as the new worldview for future systems, and many organizations are sending or plan to convey such technology with a specific end goal to reinforce their system structures, lessen operational cost, and empower new system applications/capacities. The motivation behind why numerous analysts and experts have interests in SDN is for the most part in light of the fact that by decoupling the control logic from the shut, exclusive executions of conventional system switch framework, SDN empowers us to outline and disperse imaginative flow handling and system control calculations effortlessly, and it encourages us include a great deal more knowledge and adaptability to the control plane. With the assistance of SDN, we can dynamically control arrange flows and screen organize status effectively. For instance, by utilizing SDN, we can without much of a stretch executes a system stack adjusting capacity that is not effectively and inexpensively explained with existing methods. These effective and rich capacities from SDN empower individuals to make new and inventive system administrations or models.

II. RELATED WORK

In recent years we have seen a fast change in the networking industry: leading by the Software Defined Networking (SDN) paradigm that separates the control plane from the data plane to enable programmability and centralized control of the network infrastructure, the SDN design not only simplifies the network management but also accelerates the innovation speed of deploying advanced network applications. Meanwhile, the landscape of the wireless and mobile industry is changing dramatically as well. Given the advance of wireless technologies such as 4G and Wi-Fi offering a pervasive Internet access, the traffic growth from the smart phone-alike devices has placed an increasing strain on the mobile network infrastructure and infringed the profit. Since the demand is increasing together with the growth of mobile users, the incumbent legacy infrastructure is already calling for an upgrade to overcome its existing limitations in terms of network management and security. In this paper, we advocate that the way forward is to integrate SDN and fully utilize its feature to solve the problem. As the security issue has raise serious concern in the networking community recently, we focus on the security aspect and investigate how to enhance the security with SDN for the wireless mobile networks. Distributed denial-of-service (DDoS) attacks became one of the main Internet security problems over the last decade, threatening public web servers in particular. Although the DDoS mechanism is widely understood, its detection is a very hard task because of the similarities between normal traffic and useless packets, sent by compromised hosts to their victims. This work presents a lightweight method for DDoS attack detection based on traffic flow features, in which the extraction of such information is made with a very low overhead compared to traditional approaches. This is possible due to the use of the NOX platform which provides a programmatic interface to facilitate the handling of switch information. Other major contributions

Include the high rate of detection and very low rate of false alarms obtained by flow analysis using Self Organizing Maps. Software Defined Network (SDN) architecture is a new and novel way of network management. In SDN, switches don't process

the incoming packets. They match for the incoming packets in the forwarding tables and if there is none it will be sent to the controller for processing which is the operating system of the SDN. A Distributed Denial of Service (DDoS) attack is a biggest threat to cyber security in SDN network .The attack will occur at the network layer or the application layer of the compromised systems that are connected to the network. In this project we discuss the DDoS attacks from the traces of the traffic flow. We use different machine learning algorithms such as Naive Bayes, K-Nearest neighbor, K-means and K-medoids to classify the traffic as normal and abnormal. Then these algorithms are measured using parameters such as detection rate and efficiency. The algorithm having more accuracy is chosen to implement Signature IDS and results of it are then processed by Advanced IDS which detects anomalous behavior based on open connections and provides accurate results of the hosts specifying which hosts is involved in the DDOS attack. The Software Defined Networking (SDN) paradigm introduces separation of data and control planes for flow-switched networks and enables different approaches to network security than those existing in present IP networks. The centralized control plane, i.e. the SDN controller, can host new security services that profit from the global view of the network and from direct control of switches. Some security services can be deployed as external applications that communicate with the controller. Due to the fact that all unknown traffic must be transmitted for investigation to the controller, maliciously crafted traffic can lead to Denial Of Service (DoS) attack on it. In this work we analyses features of SDN in the context of security application. Additionally we point out some aspects of SDN networks that, if changed, could improve SDN network security capabilities. Moreover, the last section of the paper presents a detailed description of security application that detects a broad kind of malicious activity using key features of SDN architecture. Now days we have observed that the fast change in the cloud network by the Software Defined Networking (SDN) paradigm that differentiate the control plane from the data plane to give the flexibility for programmability and centralized control of the cloud networks, SDN networks not only provide simplification of cloud network management it also provides more security with SDN by implementing firewalls with in the SDNs. The demand of cloud increased day by day with the increasing of usage of cloud. The SDN is provided with OpenFlow network, cloud network states are dynamically updated and configurations are frequently changed. Open Flow accepts various Field actions that can dynamically change the packet headers. A firewall embedded in SDN can immediately enforce updated rules in the firewall policy to check security violations. Cloud computing allows all categories of users to use applications without installation and access their personal files at any system with internet access Supporting modern workers and learners requires a shift in attitude of IT managers worldwide. Movement to bring your own device with further resources on the cloud seems inevitable. However despite the trend toward mobility and flexibility in IT there is a significant requirement for BYOD users to re-evaluate their attitude toward the security of their own devices and the resources they utilize on the cloud. This work outlines an evaluation of business user's attitudes towards utilizing their own devices for business. The work also outlines the results of a survey of on business users attitudes towards resources stored on the cloud. Finally recommendations are made regarding the best practice in aiding the users comprehension of security risks in BYOD and the cloud. This work presents Flow NAC, a Flow-based Network Access Control solution that allows to grant users the rights to access the network depending on the target service requested. Each service, defined univocally as a set of flows, can be independently requested and multiple services can be authorized simultaneously. Building this proposal over SDN principles has several benefits: SDN adds the appropriate granularity (fine- or coarse-grained) depending on the target scenario and flexibility to dynamically identify the services at data plane as a set of flows to enforce the adequate policy. Flow NAC uses a modified version of IEEE 802.1X (novel EAPoL-in-EAPoL encapsulation) to authenticate the users (without the need of a captive portal) and service level access control based on proactive deployment of flows (instead of reactive). Explicit service request avoids misidentifying the target service, as it could happen by analyzing the traffic (e.g. private services). The proposal is evaluated in a challenging scenario (concurrent authentication and authorization processes) with promising results. Network management is challenging. To operate, maintain, and secure a communication network, network operators must grapple with low-level vendor-specific configuration to implement complex high-level network policies. Despite many previous proposals to make networks easier to manage, many solutions to network management problems amount to stop-gap solutions because of the difficulty of changing the underlying infrastructure. The rigidity of the underlying infrastructure presents few possibilities for innovation or improvement, since network devices have generally been closed, proprietary, and vertically integrated. A new paradigm in networking, software defined networking (SDN), advocates separating the data plane and the control plane, making network switches in the data plane simple packet forwarding devices and leaving a logically centralized software program to control the behavior of the entire network. SDN introduces new possibilities for network management and configuration methods. In this article, we identify problems with the current state-of-the-art network configuration and management mechanisms and introduce mechanisms to improve various aspects of network management. We focus on three problems in network management: enabling frequent changes to network conditions and state, providing support for network configuration in a high level language, and providing better visibility and control over tasks for performing network diagnosis and troubleshooting. The technologies we describe enable network operators to implement a wide range of network policies in a high-level policy language and easily determine sources of performance problems. In addition to the systems themselves, we describe various prototype deployments in campus and home networks that demonstrate how SDN can improve common network management tasks.

III. SYSTEM DESIGN

A. *Existing System:*

Network security is first priority of any organization. In today's fast network development the security threats are increasing day by day which leave all network appliances and internet services, insecure and unreliable. While growing industries day by day security measures works more importantly towards fulfilling the cutting edge demands. The need is also induced in to the areas like defense, where secure and authenticated access of resources are the key issues related to information security. Wi-Fi networks are very common in providing wireless network access to different resources and connecting various devices wirelessly. To handle Wi-Fi threats and network hacking attempts there are need of different challenges and Issues. Today's antivirus and security software less comply with the growing system complexity and fail to manage many malicious activities which are active anytime.

B. *Proposed System:*

The Proposed system provides more security than the existing system. This system blocks the corrupted data which are sent from sender to receiver by implementing SDN .It helps us to control the network flow dynamically, controlling network flows dynamically provides many new possibilities in network security functions. First, we can implement a dynamic access control function, which is commonly used to protect a network. Previously, we need to install an independent middle box (e.g., firewall) to achieve in-line access control. However, with the help of SDN, we do not need to set up additional middle boxes, but just use a network device (e.g., an OpenFlow switch/router) that supports SDN functions for access control.

1) Advantages of Proposed system

- Controlling network flows dynamically provides many new possibilities in network security functions. First, we can implement a dynamic access control function, which is commonly used to protect a network. Previously, we need to install an independent middle box (e.g., firewall) to achieve in-line access control. However, with the help of SDN, we do not need to set up additional middle boxes, but just use a network device (e.g., an OpenFlow switch/router) that supports SDN functions for access control. In addition, we can control network flows with diverse granularity (from 1 tuple to 12 tuples), and it enables us to control network flows more efficiently.
- Second, it enables us to separate malicious (or suspicious) network flows from benign ones dynamically. This ability is quite useful when we want to differentiate security services. Suppose we simply monitor network flows to detect malicious (or suspicious) flows with a network intrusion detection system (NIDS). At this time, if an NIDS detects some flows and we want to investigate more about the flows, we may use in-depth security services (e.g., honey pot) to do it. In this case, we usually apply a proxy server to reroute or capture network flows for deeper investigation. However, if we apply SDN, we can simply build this function by controlling network flows dynamically.

IV. SYSTEM ARCHITECTURE

Figure 1 shows the proposed architecture consists of Collaborative UTM which stores the details of the attacked file affected by that. These data can be view by the admin so that the admin can restore the data of the file.

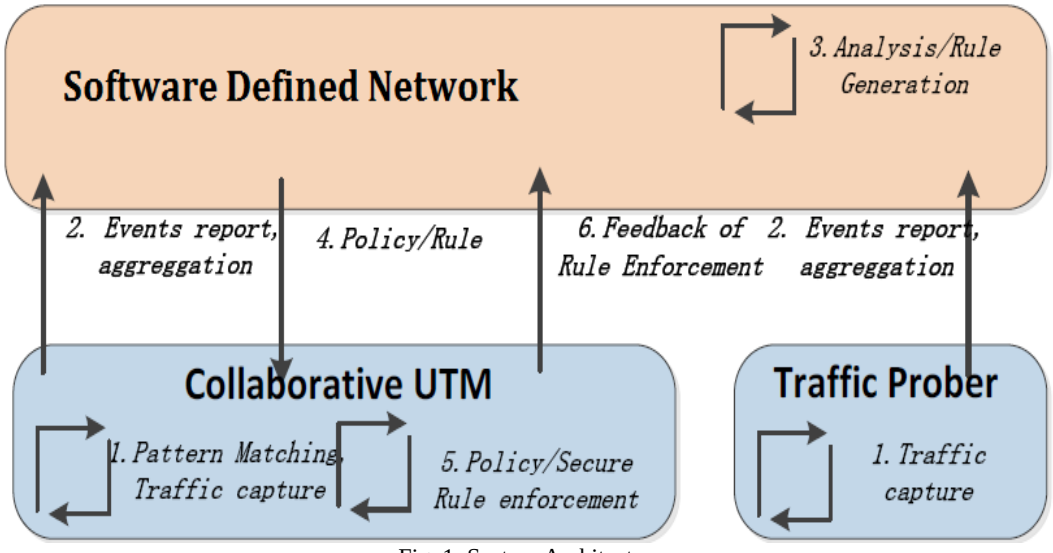

Fig. 1: System Architecture

The system contains the traffic prober which checks the file uploaded by the user, if the file contains any data retrieving code the system will block the file. SDN (software defined network) is software which monitors the network automatically. This will also help in recovering the file affected during the attack.

V. IMPLEMENTATION

User will register in register page and give the user name and password and login to include website pages in a folder which is made in extend folder. The user can upload the records (.jsp and .html only).This same strategy is rehash to the second user moreover. The administrator give the user name and password and logs into the site and can give the registered users and furthermore the records uploaded by the user. The administrator can give the unlawful uploaded of records in different users folder in the UTM (unified threat management).The attackers is likewise a registered a number get to he's document uploaded in server which can uncover the data of the nearness of other folder in a similar area. Presently the attackers can upload the documents in another user and can delete the record which can be recognized by the administrator. The administrator can give these data in the UTM and can delete those extra records uploaded by another attacker. The administrator can likewise recoup the deleted records from the reinforcement and place it in the deleted Document list.

Fig. 2: This fig shows the removed records are successfully recovered.

VI. RESULT AND DISCUSSION

The main goal of this project is to attract some sensible solutions to our main research question - can we (and how to) use the new elements given by SDN to enhance network security. In view of our genuine overviews and inside and out investigation of SDN highlights and their applications talked about in this project, we assert that SDN can unmistakably enhance network security functions in the accompanying focuses. In the first place, its capacity of controlling network streams powerfully can give more adaptable organizations of security functions on a network since it enables us to empower security functions on SDN-empowered network gadgets without introducing extra gadgets (e.g., center boxes). Second, its extensive perceive ability can understand far reaching observing as far as security. This capacity gives an all-encompassing perspective to us, and consequently we can appreciate network assaults broadly dispersed in the Internet (e.g., all-inclusive checking or DDoS) substantially more productively than heritage network observing frameworks. Third, its programmability encourages us grow more propelled network security functions. We can (generally) effortlessly execute a model security framework without putting much exertion. All things considered, SDN elements can be utilized in quickening the improvement of new and propelled network security functions.

VII. CONCLUSION AND FUTURE SCOPE

We introduce the SDN technology and systematically investigate its usage for security. Although many people have interests in this technology, until now, it is not yet well embraced by security researchers. We believe that SDN can, in time, prove to be one of the most impactful technologies to drive a variety of innovations in network security. We hope this study can not only provide a quick introduction and systematic survey but also give significant insights for using SDN for better security applications and stimulate more future research in this important area.

A. Future Scope

The Proposed system does not identity the attacker it only detects the attacked file so in the future scope

- We may detect the attacker
- And block the attacker with his Mac address

REFERENCES

[1] ACM. Acm sigcomm symposium on sdn research (sosr). http: //www.sigcomm.org/events/SOSR.
[2] Mohammad Al-Fares, Sivasankar Radhakrishnan, Barath Raghavan, Nelson Huang, and Amin Vahdat. Hedera: Dynamic Flow Scheduling for Data Center Networks. In Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation, 2010.
[3] Ali Al-Shabibi, Marc De Leenheer, Matteo Gerola, Ayaka Koshibe, Guru Parulkar, Elio Salvadori, and Bill Snow. OpenVirteX: Make Your Virtual SDNs Programmable. In HotSDN'14, 2014.
[4] Jeffrey R. Ballard, Ian Rae, and Aditya Akella. Extensible and Scalable Network Monitoring Using OpenSAFE. In Usenix INW/WREN, 2010.
[5] BigSwitch. Bigtap: Monitor traffic everywhere. http://www. bigswitch.com/products/big-tap-network-monitoring.
[6] R. S. Braga, E. Mota, and A. Passito. Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow. In Proceedings of the35thAnnualIEEEConferenceonLocalComputerNetworks, LCN, 2010.
[7] Kenneth L. Calvert, Rebecca E. Grinter, W. Keith Edwards, Ye Deng, Nick Feamster, and Xuzi Zhou. Instrumenting Home Networks. 2010.
[8] Cisco. Cisco ios security: Access control lists. http://www.cisco.com/en/US/docs/ios/12 2/security/ configuration/guide/scfacls.html.
[9] Andy Curtis, Jeff Mogul, Jean Tourrilhes, Praveen Yalagandula, Puneet Sharma, and Sujata Banerjee. DevoFlow: Scaling Flow Management for High-Performance Networks. In Proceedings of ACM SIGCOMM, 2011.
[10] Mohan Dhawan, Rishabh Poddar, Kshiteej Mahajan, and Vijay Mann. SPHINX: Detecting Security Attacks in SoftwareDefined Networks. In NDSS'15, 2015.
[11] D.A. Drutskoy. Software-defined network virtualization with flown. Master Thesis, 2012. ftp://ftp.cs.princeton.edu/ techreports/2012/929.pdf.
[12] Qi Duan, Ehab Al-Shaer, and Haadi Jafarian. Efficient Random Route Mutation considering flow and network constraints. In CNS'13, 2013.
[13] Seyed K. Fayaz, Yoshiaki Tobioka, Vyas Sekar, and Michael Bailey. Bohatei: Flexible and Elastic DDoS Defense. In Usenix Security'15, 2015. S.K.Fayazbakhsh, L.Chiang, V.Sekar, M.Yu, and J.C.Mogul. Enforcing network-wide policies in the presence of dynamic middlebox actions using FlowTags. In NSDI'14, 2014.