An Adaptive Detection and Prevention Architecture for Unsafe Traffic in SDN Enabled Mobile Networks

Mehrnoosh Monshizadeh
Nokia Bell Labs, Finland
Department of Comnet, Aalto University, Espoo, Finland
mehrnoosh.monshizadeh@nokia-bell-labs.com
mehrnoosh.monshizadeh@aalto.fi

Vikramajeet Khatri
Nokia Bell Labs, Finland
vikramajeet.khatri@nokia-bell-labs.com

Raimo Kantola
Department of Coment, Aalto University, Espoo, Finland
raimo.kantola@aalto.fi

***Abstract*— The forthcoming 5G cloud networks will utilize software defined networking (SDN) and network functions virtualization (NFV) to provide new services. However, applying these technologies introduce new threats to network. To detect the security attacks and malicious traffic both on end user and cloudified mobile network, we apply centralized monitoring and combine dynamicity and programmability of SDN, traffic filtering capabilities of IDS and clustering mechanisms for load balancing. We discuss and demonstrate an adaptive detection and prevention architecture for SDN enabled mobile networks.**

Keywords*— *Anomaly Detection; Cloud; Controller; Detection as a Service; IDS; SDN; Security

I. INTRODUCTION

While the traditional mobile networks are evolving to utilize cloud environment characteristics such as programmability and adaptively, the forthcoming 5G network will offer an increased data rate, a reduced end-to-end latency and an improved coverage. Cyber-attacks are growing rapidly and causing threats to the mobile networks. Traffic originated from mobile subscriber passes through all network elements till it reaches the gateway to the Internet and vice-versa. Such traffic may attack network elements and can also cause a denial of service (DoS) attack on the network.

In a mobile cloud environment, traffic will be separated into user plane (UP) and control plane (CP) using software defined networking (SDN) mechanism while mobile network functions will be executed over the cloud via network functions virtualization (NFV) technology. However, the programmability and openness of cloud network architecture increases attack surface and brings additional security challenges that must be addressed.

For a programmable SDN enabled network, if attacker gains unauthorized access to the SDN controller, the network can be exploited [1-2]. Attacker can distribute malicious traffic to the network, degrade or entirely bring down the network services. To detect such attacks early enough, centralized monitoring and intrusion detection systems (IDS) are recommended as detection solutions [3]. However, the cost and processing time to handle such a traffic load remains a challenge in IDS solutions. Therefore, we demonstrate a scalable, redundant and reliable architecture for anomaly detection and mitigation. This architecture combines dynamicity and programmability of SDN, traffic filtering capabilities of IDS and clustering mechanisms for load balancing.

II. SYSTEM ARCHITECTURE

This demo introduces a security architecture based on software level that comprises of an application layer, a management layer and a data layer. As it is shown in Figure 1, in an SDN enabled network, the application layer includes an SDN application and an application interface. The management layer constitutes of SDN controller and CP switches, whereas the data layer comprises UP switches, a clustering algorithm that clusters input traffic per its features and several detection as a service (DaaS) nodes to detect unsafe traffic. With our architecture, we aim to stop the malicious traffic from entering the network further and polluting its elements.

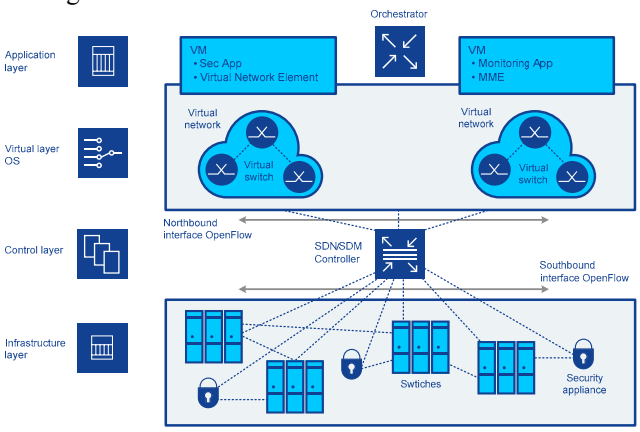

Fig. 1. SDN enabled network

DaaS will process network traffic to detect anomalies. The result of DaaS analysis will be reported to SDN application. The SDN application will serve as an orchestrator and process the output from multiple DaaS nodes, formulate flow(s) and send to SDN controller. In response, SDN controller delivers flow(s) to associated switch to carry out action(s) which include removing, modifying or installing flow; eventually such malicious traffic will be dropped at switch. The term 'flow' refers to forwarding rule in OpenFlow enabled switches, so the analysis would be done on packet level [4].

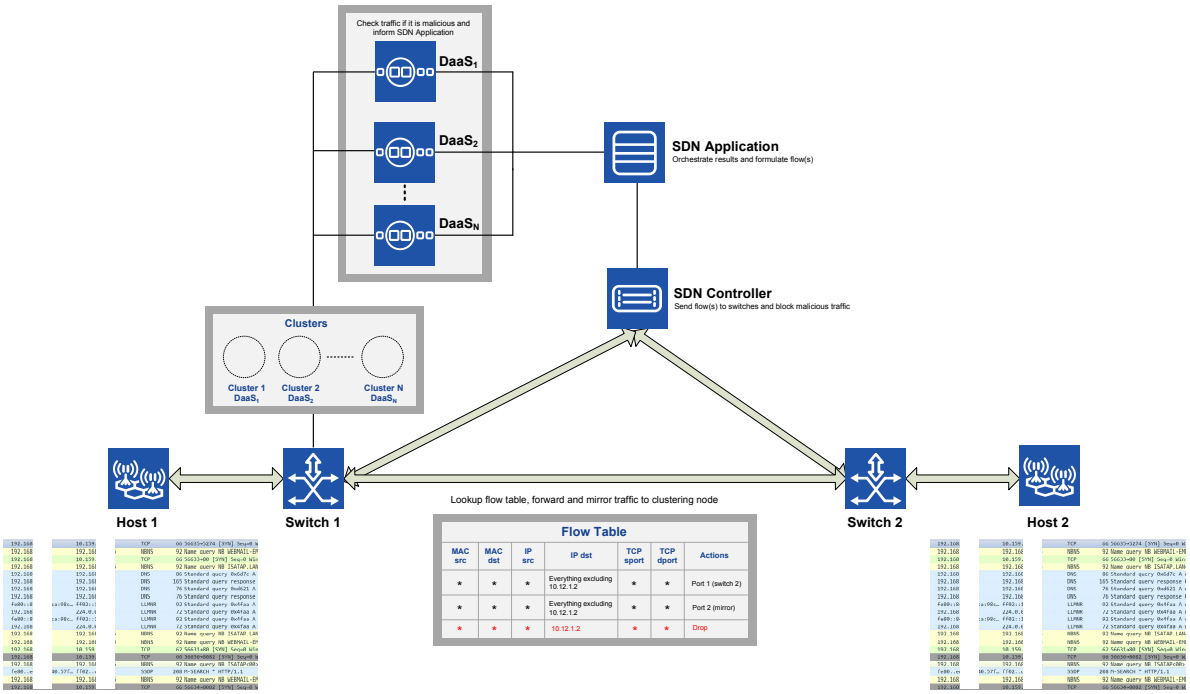

Fig. 2. SDN security monitoring

The security architecture can be seen in Figure 2. To process huge amount of traffic for attack detection and distribute load evenly, various DaaS instances should be utilized that brings scalability to architecture. Traffic clustering can be performed in two ways: clustering each packet or sampled traffic. An implementation with different types of attacks for both approaches is already ongoing by authors to evaluate the performance.

III. Demo Description

We demonstrate DaaS as an SDN network based anomaly detection and prevention system together with key features. As a proof of concept, DaaS will be simulated using demonstration data which contains safe and malicious traffic. The detection results and mitigation actions will be further demonstrated by blocking flows via programing SDN controlled switches. Demo utilizes OpenStack environment, OpenvSwitch, floodlight controller and relevant processes. Whether the input data contains every packet or only sampled traffic, two scenarios will be demonstrated. The general steps as shown in Figure 2 are as follow:

1. For every packet:
   - Clustering mechanism is applied at switch 1
   - User traffic is clustered and sent to corresponding DaaS node
2. For sampled traffic:
   - Data is sampled in switch 1 and sent to clustering node
   - Clustering node communicates with controller to send updated clusters to switch 1
   - Traffic is forwarded from switch 1 to corresponding DaaS node based on the clusters (load balancing)
3. Anomaly detection is applied in DaaS and results are sent to SDN Application
4. SDN Application communicates with controller:
   - Malicious flows will be removed
   - Normal traffic will be forwarded

IV. Conclusion

The malicious traffic should be detected and stopped as early as possible in a mobile network so it doesn't affect the network elements as well as other end-users. We demonstrate utilizing detection as a service (DaaS) in conjunction with software defined networking (SDN) controller in an SDN enabled network and mitigating malicious traffic using flow control techniques. The proposed architecture will protect SDN from being overloaded and from resource abuse attacks. In addition, applied load balancing mechanism together with clustering on the sampled traffic would reduce SDN controller load and computing resources and therefore computation cost and latency.

References

[1] Open Networking Foundation (ONF), "Threat Analysis for the SDN Architecture," Technical Report 530, v1.0, Jul. 2016.

[2] Anthony Lim, "Security Risks in SDN and Other New Software Issues," RSA Conference, Jul. 2015.

[3] M. Monshizadeh, Z. Yan, L. Hippeläinen and V. Khatri, "Cloudification and security implications of TaaS," *Computer Networks and Information Security (WSCNIS), 2015 World Symposium on,* Hammamet, 2015, pp. 1-8.

[4] M. Monshizadeh, V. Khatri and R. Kantola, "Detection as a Service: An SDN Application," *Advanced Communications Technology (ICACT), 19th IEEE International Conference on,* Pyeongchang, 2017 (Accepted).