Detection as a Service: An SDN Application

Mehrnoosh Monshizadeh*†, Vikramajeet Khatri*, Raimo Kantola†

**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.com*, raimo.kantola@aalto.fi†

***Abstract*— In a cloud computing environment, future networks will most probably utilize network functions virtualization (NFV) which is a network architecture concept that proposes virtualizing network node functions into "building blocks" or entities that may be operationally connected or linked together to provide services. However, applying these mechanisms brings security challenges. Due to the programmability of software defined networking (SDN), if attackers gain access to an SDN controller, then the whole network may be exploited by the attackers. The attackers may change forwarding paths and pass malicious traffic to infect the SDN enabled network. To detect the security attacks and malicious traffic early enough and to protect the network, centralized monitoring and intrusion detection system (IDS) monitoring may be used for enhancing SDN, NFV and OpenFlow security. If the network traffic is analysed and the anomalies are detected, the SDN controller may be used to block such traffic from passing through the network by flow control, i.e. forwarding paths in a switch. IDS and intrusion prevention system (IPS) may be deployed at the gateway node to detect a security intrusion. Thus, the data traffic originated from a subscriber passes through each network element until the traffic reaches the gateway node. Such traffic may attack the network elements and may also cause a denial of service (DoS) attack in the network. IDS devices are designed to handle network traffic in real time, yet the cost and high processing time is a challenge for handling the traffic load. Combining dynamicity and programmability of SDN together with traffic filtering of IDS, enables a scalable, redundant and reliable anomaly detection for mobile network operators. In this study, we propose an architecture that combines IDS with programmability features of SDN for detection and mitigation of malicious traffic. Mitigation will be performed by SDN controller using flow control techniques. The proposed architecture can be applied to an SDN enabled mobile network with two different approaches for improved performance in terms of computation power.**

***Keyword*—Anomaly Detection, Cloud, Controller, DaaS, IDS, OpenFlow, Security, SDN**

Mehrnoosh Monshizadeh is finalizing her PhD at Electrical School of Aalto University, Finland. She is working at Nokia Bell Labs as security research specialist. Her research interests include cloud security, mobile network security, IoT security and data analytics.

Vikramajeet Khatri has M.Sc degree in information technology from Tampere University of Technology, Finland. He is working as research security specialist at Nokia Bell Labs. His research interests include intrusion detection, malware detection, IoT security and cloud security.

Raimo Kantola has a D.Tech degree in computer science from Helsinki University of Technology, Finland. He is a professor in networking technology at department of Comnet, Aalto University, Finland. His research interests include SDN, customer edge switching, trust in networks and cloud security.