Software Defined Monitoring For 5G Mobile Backhaul Networks

Priyanka R
R&D Engineer
Department of Research & Development

Darshan Kumar P,
Lecturer
Department of Electronics & Communication,
SRSRPT, Tiptur

Shreelakshmi C M,
Assistant Professor,
Department of Computer Science & Engineering,
GSSSIETW, Mysuru.

Khateeja Ambareen
Assistant Professor,
Department of Computer Science & Engineering,
GSSSIETW, Mysuru.

***Abstract*—Software Defined Network (SDN) is an advanced approach to designing dynamic, manageable, cost-effective, and adaptable network architectures. SDN will play a key role as an enabler for 5G and future networks. Transferring network monitoring functions to a software entity working in conjunction with configurable hardware accelerators through a scheme called Software Defined Monitoring (SDM) is one promising way to attain the dynamism necessary for the monitoring of the next generation-networks. In this paper, we propose a novel SDM architecture for future mobile backhaul networks. As an SDN solution, the proposed architecture provides more granular and dynamic network management functions through its programmable interface, centralized control, and virtualized abstractions. At the same time, the SDM framework intuitively seem prone to various challenges that come with the separation of the control and data planes of middle boxes. This paper collects specific opportunities, vulnerabilities as well as challenges related to SDM. It also highlights how SDM can be used to solve the current limitations in legacy monitoring systems. The feasibility of the proposed SDM architecture is verified by using a testbed implementation.**

Keywords—5G, Monitoring, Network Security, Software Defined Networking, Network Function Virtualization

I. INTRODUCTION

Network monitoring system is a crucial network management instrument in telecommunication networks which gathers network statistics and granularities to evaluate the status of the network. Such monitoring data is useful for different management tasks such as network maintenance, anomaly detection, network forensics, load balancing, traffic engineering, enforcing Service Level Agreements (SLA) and ensuring Quality of Service (QoS)/Quality of Experience (QoE). Traditionally, network monitoring systems are deployed at mobile network boundaries and they rely on physical interfaces. However, mobile data traffic is rapidly increasing due to Internet of Things (IoT), High Definition (HD) video streaming, online gaming, augmented reality, and tactile Internet. Hence, these monitoring systems would find several application areas in 5G networks. Future 5G mobile network will be designed as Software Defined Mobile Networks (SDMN) by integrating Software formatter will need to create these components, incorporating the applicable criteria that follow. Defined Networking (SDN) and Network Function Virtualization (NFV) concepts [1], [2]. These concepts can also be used to overcome the limitations of the legacy monitoring systems.

In this paper, we highlight the limitations of legacy monitoring systems in present mobile backhual networks. Then, we propose a novel Software Defined Monitoring (SDM) architecture to overcome these limitations in 5G networks. We propose necessary modifications to Software Defined Mobile Network (SDMN) architecture to implement the SDM framework. We also present specific opportunities, vulnerabilities as well as challenges related to SDM. Finally, we implement the proposed SDM architecture on a testbed to verify its feasibility. The rest of this paper is organized as follows, Section II discusses the limitations of legacy monitoring techniques and how SDN/NFV features can be used to solve these limitations. Section III presents the proposed SDM architecture and its key components. The experiment results and the expected advantages of SDM are discussed in Sections IV and V respectively. Section VI describes different challenges of SDM while Section VII concludes the article.

II.LIMITATIONS OF CURRENT MONITORING TECHNIQUES

The legacy monitoring systems have a number of limitations, such as high complexity which makes them difficult to deploy and maintain, high provisioning and operational costs due to the distributed infrastructure. The currently used vendor-specific monitoring systems come with hardwired operational logic in their firmwares, this means that changes in such legacy monitoring system either require complex configurations or changes in the firmware. As a result, these systems lack flexibility and cannot cope with the dynamic changes in network conditions [3], [4].

Traditional networks comprise many autonomous chunks of networked systems where a change in some parameters can induce undesirable effects on the overall network state. Moreover, there is no global visibility of the network state in current networks. This leads to localized decision-making at multiple points in the network. Hence, synchronizing a huge number of monitoring decisions is a daunting task for both network management and monitoring systems. Autonomous perimeter-based security policies further complicate

deploying. coherent network-wide security policies and inter policy and intra policy conflicts [5].

With heavy dependence on physical resources, it is extremely demanding to adapt the monitoring policies of existing monitoring systems to all possible network conditions. With the level of dynamism expected in 5G networks, such limitation becomes a major issue of concern for network administrators. Moreover, present-day monitoring solutions are over-provisioned to meet the peak hour traffic demands, hence causing prolonged underutilization of available resources [4].

In contrast to the physical control devices in legacy mobile networks, beyond 5G mobile networks will have virtualized control devices [1], [2]. However, present monitoring techniques are not designed to monitor virtualized components. [6]. Present mobile networks lack end-to-end visibility due to closed network equipment and distributed security mechanisms. Lack of interoperability and vendor specific network monitoring devices/systems constitutes another limitation to existing monitoring systems. As a result, operators have to implement a large number of network probes to monitor traffic in each sector which will ultimately lead to high monitoring overhead in terms of network bandwidth and operational cost. Moreover, beyond 5G networks will connect billions of devices and transport huge amount of backhual traffic. Then, the cost and control traffic of legacy monitoring systems will exponentially increase and drastically reduce the scalability of monitoring system due to the above reasons. These limitations can be addressed by applying SDN paradigm to the monitoring system. Table I shows how SDM features can be used to overcome the limitations in legacy monitoring techniques [1], [6]–[8].

III. SOFTWARE DEFINED MONITORING FRAMEWORK

SDM framework is designed to perform monitoring functions in SDN/NFV-based 5G mobile network architectures [9]. It is able to monitor both virtualized and physical network environments in an economical and efficient way. Initially, the proposed SDM architecture is used only to monitor 5G backhual network. Figure 1 illustrates how SDM framework is implemented on 5G SDMN architecture. The key components of the proposed SDM architecture are SDM controller, SDM control interface, monitoring probes, network probe manager, network monitoring management module and network monitoring dashboard.

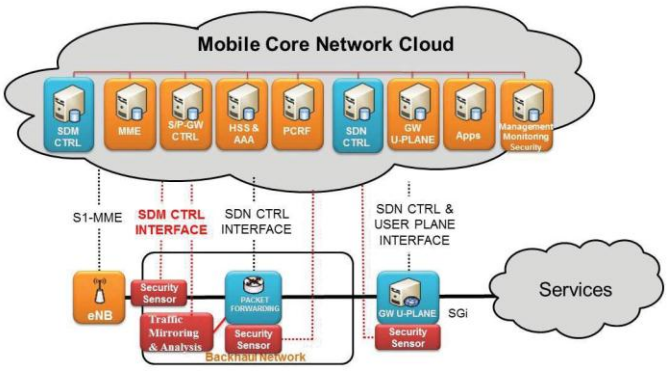

Fig. 1: Proposed network monitoring framework for SDMN.

Figure 2 shows how the components of the proposed architecture map to the three-layer mobile SDN architecture proposed by Open Network Foundation (ONF) [10]. Figure 3 further shows how SDM architecture is mapped to the NFV architecture proposed by European Telecommunications Standards Institute (ETSI) [11].

A. Key Components of SDM Framework

1) SDM Controller:

This component is an extension of the SDN controller. SDN controller allows the extraction of certain information from the routers using, for instance, the OpenFlow interface. However, OpenFlow is primarily designed for routing applications and deals with flows rather than individual packets. It is used for notifying events (e.g. changes in the link

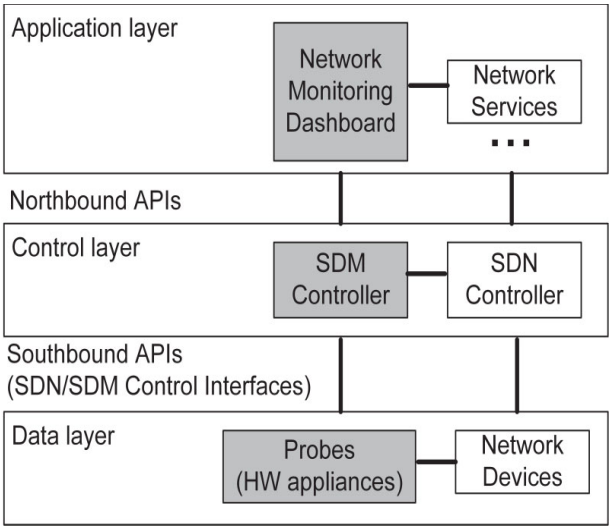

Fig. 2: SDM framework in three layer SDN architecture.

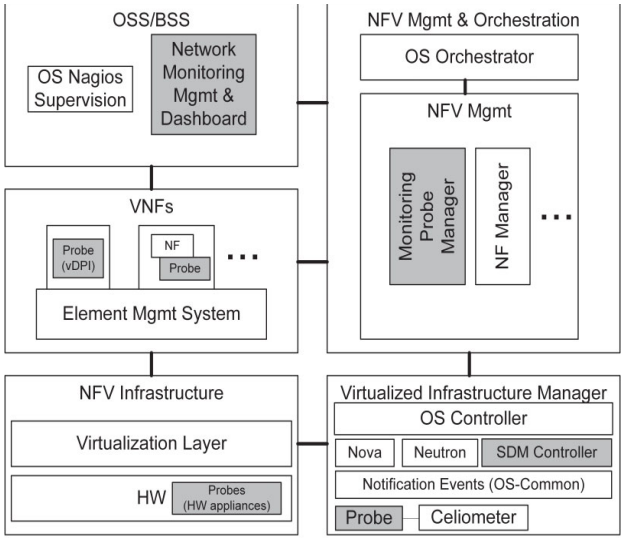

Fig. 3: SDM framework in high level NFV management architecture.

state, the arrival of new flow, e.t.c), flow statistics and *packetin messages* containing part of certain packets related to error conditions, mismatches or explicit requests [12]. Making all packets available to the controller using *packet-in messages* would be inefficient. Thus, the SDN controller has been extended by an SDM controller to enable better packet sampling, packet/flow metadata extraction and packet/flow redirection.To address the requirements of security and traffic analysis applications, it allows the controlling of monitoring functions (e.g., management of network monitoring appliances, traffic mirroring, traffic load balancing and aggregation) and accepts requests from network functions and applications. It optimizes packet and flow analysis according to the needs of the operators and different network functions. SDM controller can be implemented as distributed controllers following either a peer-to-peer or hierarchical model. They interact with the management-monitoring security functions and act as distributed analysis or decision points for enforcing the defined service and security policies.

2) SDM Control Interface:

This interface is an extension of the SDN control interface. The SDN control interface (e.g., OpenFlow) is designed mainly for routing. Thus, new SDM Control Interface is designed to support the monitoring functions. It also delivers the monitoring related control messages from SDM controller to monitoring probes.

3) Monitoring Probes:

Probes are needed for obtaining performance, security or behavior related information. There are two types of probes, i.e. passive (performing only analysis without disturbing the traffic) and active (carry out prevention, mitigation or corrective actions). Moreover, these probes are deployed in both actual and virtual environments. Hardware based physical probes are deployed in the physical data plane (i.e., hardware appliances) and virtual probes are deployed in the virtualized control plane (e.g., virtualized Deep Packet Inspection-vDPI) as a standalone network function or collocated with other network functions to address different needs. They also complement the basic monitoring functions (e.g., OpenStack's Celiometer [13]) of the virtualized infrastructure manager.

4) Network Monitoring Management:

This component is part of the OSS/BSS (Operations and Business Support Sy tem) that performs the standard management of monitoring functions such as network inventory, service provisioning, network configuration and fault management. It recuperates the information from the different probes and presents a more holistic view of the state of the network to the operator. This component displays near real time statistics (of both performance and security) of the situation of the network, its links, the different network elements, and the protocol and applications being used. It allows generating alerts that can be addressed either manually by the operator or automatically following the mitigation policies previously defined.

5) Network Probe Manager:

This component is part of the NFV management and orchestration for specifically deploying and dynamically configuring the probes in the virtual machines. The flexibility for SDM architecture is introduced by the virtualization of the network and its functions. The main objective of this component is to determine where the probes need to be deployed in the continuously changing environment, and if they should be stand-alone virtual machines or inside the network functions' virtual machines (e.g., soft switches).

6) Network Monitoring Dashboard:

This component is a centralized application that acts as a decision point and provides a dashboard for managing the distributed monitoring probes. This is a software application which provides a user friendly interface to define the objectives of the monitoring system (following the defined security and performance policies). Moreover, it provides a visual control for the deployment of the probes.

IV. EXPERIMENT RESULTS

We implemented a Proof-o-Concept (PoC) of the proposed SDM architecture in a testbed. The main objective of the experiment was to verify the ability of proposed SDM architecture to automatically detect and mitigate an ongoing attack in the network. The experiment testbed is presented in Figure 4. We used Mininet v2.2.1 the network emulation environment and OpenvSwitch v2.3.1 for the deployment of SDN switches. Floodlight v1.1 is used as the SDN controller. The network monitoring dashboard has been implemented within the SDM controller as a server side application. S1, S2, and S3 are virtual switches which are implemented with OpenvSwitch. RO (Route Optimizer) deals with a virtualized element for routing purposes.

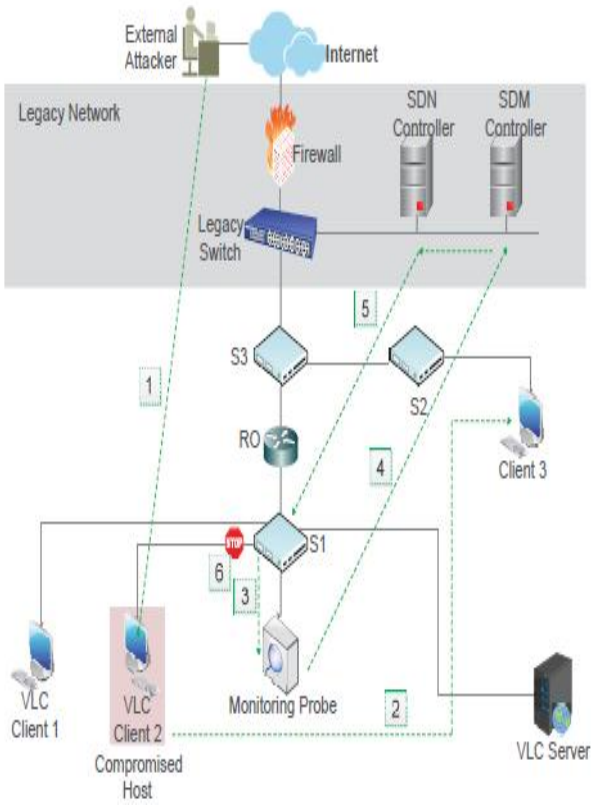

Fig. 4: The layout of the experimental testbed

In this experiment setup, a security use case has been defined as a proof of concept for how the proposed SDM architecture automatically detects and mitigates threats based on pre-defined security polices. A security policy was defined to isolate insecure network devices, before they can negatively affect the rest of the network. Upon discovering a potential threat, the SDM controller identifies the problem and automatically performs the previously considered or planned reactions to mitigate it, by interacting with the Northbound API of the SDN controller. After the threat has been resolved the SDM controller allows the affected devices to rejoin the network.

In this experiment, a VLC server had streamed video in the server LAN and several VLC clients were consuming this video. The test experiment was carried out using the following steps.

1) An external attacker compromised the VLC Client 2 by simulating a botnet.

2) The compromised host launched a network discovery process over the networks to identify the possible clients to extend the attack. It tried to take the control of another host in the network.

3) The suspicious traffic of the network discovery was detected by the security monitoring probe that wassniffing all the traffic crossing the virtual switch S1.

4) The probe reported this security event to the SDM controller.

5) The SDM controller processed this event matching against a predefined security policy that tells it to immediately block the connections to the host in S1.

6) The SDM controller forwarded this information to the SDN controller and the SDN Controller sent a flow table update to the S1 via Open Flow interface to drop all the traffic related to the compromised host. Afterwards, once the VLC Client 2 had recovered from its security issues, a new flow was injected into the S1 that reallowed it to send the traffic from the host to the network. Here, SDM system performed a cyber-attack detection by considering a unique source of information from the probe. Figure 5 represents the delay between when the attacker began to carry out the attack and the time that the attack was blocked

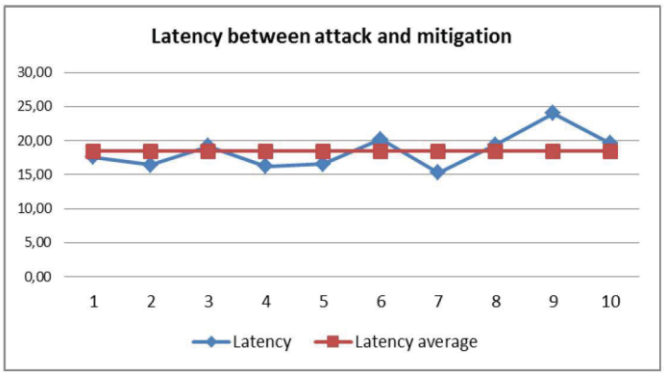

Fig. 5: Latency between attack and mitigation

We ran the experiment ten times and the proposed SDM architecture were able to work as a standalone system not only to detect attack but also mitigate the threat automatically based on pre-defined security polices. Thus, the experiment results had verified the feasibility of proposed SDM architecture. In this experiment, the expected delay is about 18.5 s.

V. EXPECTED ADVANTAGES OF SDM

The introduction of software defined monitoring can offer several advantages, which includes:

• *Abstraction:* SDN approach abstracts the monitorin functions away from the physical constructs of the network, for instance, the stateful firewalls and wire sniffers, and replace them by a set of flexible controls in the form of policy envelopes blanketing the virtualized (or physical) assets. With this level of abstraction, it is possible to establish common monitoring mechanisms that can easily be replicated across the network without recourse to the actual capabilities of the underlying physical hardware
[3], [4].

• *Automation:* Using SDN, each deployed monitoring device automatically inherits the predefined security policies. This way, it is easier to mitigate or eliminate inadvertent operator error and ensure that no monitoring system is deployed without being automatically attached to a security trust zone. With role based controls, only properly privileged administrators can make modifications to policies. On events of anomalous security threat, SDM automation reacts at a wire speed to send instant alerts and perform quarantining operations as predefined in the control policy [14]. Unlike the traditional monitoring systems that heavily depends on manual detection, action, and administration during such anomalies.

• *Scalability and Flexibility:* In SDM framework, overdependence on physical hardware is eliminated. This means that monitoring functions can be implemented on a case by case basis depending on what is considered appropriate for each network scenario, growing in scope that commensurate with the business needs. In other words, given that the monitoring functions are implemented on software, they are more flexible and can easily be scaled up across a cluster or a network segment. This also implies that monitoring resources and mechanism get implemented on-demand basis [15].

• *Centralized Control and Orchestration:* SDM integrates multiple network security controls into a single coordinated engine for intelligent analysis and actions. This includes intrusion detection and prevention, vulnerability management, network segmentation, and monitoring tools. Hence, unlimited amount of security input can be channeled into a policy-driven orchestration framework. This will improve the accuracy of the collected data and the effectiveness of the corresponding actions [16]. Such orchestration is also crucial to ensure compliance with designed policies since all major compliance standards dictate a variety of controls as parts of the specifications.

• *Portability:* Leveraging NFV, the SDM framework can be relocated from data centers to any network perimeter due to the portable nature of software modules of SDM and programmable network architecture of SDN.

• *Economically viable:* With virtualization, SDM security functions are dynamically deployed on already existing network infrastructure with minimum CAPEX costs. This also leads to a more flexible management schemes such as dynamic configuration, and countermeasures which reduce OPEX costs [17]. With traditional security appliances, these features are difficult to implement and would come at much higher costs.

• *Easy deployment:* SDM is a new model of flow monitoring which supports the easy deployment of advanced monitoring and security applications on the networks [8]. Since the monitoring functions are implemented as software applications in a mobile cloud, it is much easier to deploy and update than legacy hardware based monitoring systems.

VI. CHALLENGES OF SDM

Based on different studies and analysis [1], [7], [15], [16], SDM possesses series of desirable features that can spur its large scale adoption in network monitoring of the next generation networks. However, some potential challenges exist in the following main areas:

• *Compatibility with Traditional Monitoring Systems:* To facilitate the legacy mobile operators' smooth transitioning to novel softwarizated cloud based mobile networks, SDM frameworks should be compatibility with traditional monitoring systems. SDM should also be able to analyze the different control and user plane traffic flows over the network domains and new interfaces between the SDN and existing networks. It should also be able to identify related flows in different network domains.

• *Adapting Traditional Monitoring Techniques to SDN:* SDM should retain the basic functionalities of traditional monitoring techniques such as the Deep Packet Inspection (DPI) engines as well as the Intrusion Detection System (IDS). These include the classification of traffic, metadata extraction, data correlation, and identification ofmalicious or unwanted traffic. There are concerns on how DPI and IDS will have to effectively handle SDN, mobile networks, Virtualized Networks (VN), and Virtualized Network Function (VNF) [6].

• *Placement of Controller:* SDM architecture consists of a centralized controller which control all the monitoring functionalities. Thus, the proper deployment of controlleris important to achieving the expected scalability in SDM systems. In most mobile networks, the use a single controller is not feasible due to the latency in the control channel. Thus, multiple or distributed controller architectures are required for larger mobile backhual networks.On one hand, such solutions will lead to new challenges such as convergence and countless control instances to configure and manage. Moreover, SDM architecture should be able to solve the conflicts when multiple controllers are available for a single data plane device. On the other hand, it is also challenging to find the optimum number of controllers and the best location for each controller.

• *Information Extraction:* Since SDM relies heavily on virtualization, there is a need to understand how this affects the way traffic flow information, profiles, and properties are obtained using extracted protocol metadata, measurements, data mining, and machine learning techniques[1].

• *Complex Monitoring Applications:* It is challenging to design general purpose SDM applications which are fit into multiple dynamic network monitoring cases. Especially when considering the different level of scalability each application needs. In addition, hardware acceleration and packet preprocessing technologies need to be integrated and controlled by applications and functions to obtain highly optimized solutions.

• *Scalability and Performance Challenges:* This originates from the initial decoupling of control and data plan in SDN, since transferring traditionally local control functionalities to a remote controller can present some bottlenecks and increase signaling overheads. Different approaches have been defined to designing SDN controllers and switches to ensure scalability and robustness, and also to address security challenges. In [18], several of such approaches were analyzed, most of which are aimed at mitigating flow set-up delays, allowing more efficient access to counters, and minimizing controller overheads. However, other studies such as in [19] also reveal that such scalability concerns are not unique to SDN-based solutions, hence solutions built on SDN are mostly designed with scalability trade-offs, leaving no inherent bottlenecks to its scalability.

VII. CONCLUSION

The techniques and mechanisms of current monitoring systems rare their ability to support the inevitably high monitoring demands of 5G mobile networks both in terms of traffic flow and highly dynamic network environments. Software Defined Monitoring (SDM) possesses series of promising features that can well address the limitations of current monitoring solutions. SDM is proposing to transfer network monitoring operations to a software working in conjunction with configurable hardware accelerators. However, SDM also inherits some of the vulnerabilities of traditional software based solutions and cloud systems.

In this article, we discussed the limitations of current monitoring techniques, these include lack of interoperability, vendor specific network monitoring infrastructures, distributed

and uncoordinated monitoring systems, high dependence on physical resources, rigid monitoring policies, distributed infrastructures, and unautomated mitigation actions. We proposed a novel SDM architecture for future 5G Software Defined Mobile Network (SDMN) backhaul networks to overcome these limitations. The proposed modifications will enable a smooth implementation of SDM architecture on on 5G backhaul network. We also mapped the proposed SDM architecture for both SDN and NFV reference models to support the standardization of proposed SDM framework. We further discussed how various features of SDM set to address each of these limitations. For instance, the logically centralized control feature of SDM simplifies network management and maintenance, eliminates the need for distributed infrastructures and vendor specific mechanisms, enables more coordination in monitoring and dynamically adjusts mechanisms to meet existing network demands. The programmability feature automates monitoring functions, reduces dependence on physical resources, and makes adaptation easy. Overall, the use of software application to replace physical resources reduces the CapEx and OpEx of network monitoring. On the other hand, SDM is prone to challenges such as development of simple monitoring applications fit for multiple monitoring and network scenarios, adapting traditional monitoring techniques to SDN, the development of effective methods monitor virtual devices and handle virtualized content. It is therefore required that SDM addresses these limitations so as to be an effective monitoring solution for future telecommunication networks. Our future works will be focused on addressing these issues.

REFERENCES

[1] M. Liyanage, A. Gurtov, and M. Ylianttila, Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture. John Wiley & Sons, 2015.

[2] M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Vasilakos, "Software- Defined and Virtualized Future Mobile and Wireless Networks: A Survey," Mobile Networks and Applications, vol. 20, no. 1, pp. 4–18, 2015.

[3] M. Liyanage, I. Ahmad, M. Ylianttila, J. L. Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, E. M. de Oca, A. Valtierra, and C. Jimenez, "Security for Future Software Defined Mobile Networks," in Next Generation Mobile Applications Services and Technologies (NGMAST),9th International Conference on. IEEE, 2015, pp. 1–9.

[4] M. Liyanage, A. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security Perspective," IEEE Security and Privacy Magazine, 2015.

[5] H. Hamed and E. Al-Shaer, "Taxonomy of Conflicts in Network Security Policies," IEEE Communications Magazine, vol. 44, no. 3, pp. 134–141,2006.

[6] A. TaheriMonfared and C. Rong, "Multi-tenant Network Monitoring Based on Software Defined Networking," in On the Move to Meaningful Internet Systems: OTM 2013 Conferences. Springer, 2013, pp. 327–341.

[7] L. Kekely, V. Pus, and J. Korenek, "Software Defined Monitoring of Application Protocols," in INFOCOM, 2014 Proceedings IEEE. IEEE, 2014, pp. 1725–1733.

[8] Cisco, "Cisco Extensible Network Controller. Scalable and Cost-Effective Solution for Network Traffic Visibility Solution Overview." Cisco.

[9] J. Costa-Requena, J. L. Santos, V. F. Guasch, K. Ahokas, G. Premsankar,S. Luukkainen, I. Ahmed, M. Liyanage, M. Ylianttila, O. L. Prez, M. U. Itzazelaia, and E. M. de Oca, "SDN and NFV Integration in Generalized Mobile Network Architecture," in European Conference on Networks and Communications (EUCNC). IEEE, 2015, pp. 1–5.

[10] A. Lara, A. Kolasani, and B. Ramamurthy, "Network Innovation using Openflow: A Survey," Communications Surveys & Tutorials, IEEE, vol. 16, no. 1, pp. 493–512, 2014.

[11] "Network Functions Virtualisation (NFV): Architectural Framework," European Telecommunications Standards Institute (ETSI) Group Specification (GS) NFV, vol. 2, p. V1, 2013.

[12] "OpenFlow Switch Specification, Version 1.4.0 (Wire Protocol 0x05),"pp. 1–206, 2013.

[13] R. Kumar, N. Gupta, S. Charu, K. Jain, and S. K. Jangir, "Open Source Solution for Cloud Computing Platform Using OpenStack," International Journal of Computer Science and Mobile Computing, vol. 3, no. 5, pp. 89–98, 2014.

[14] D. Bercovich, L. M. Contreras, Y. Haddad, A. Adam, and C. J. Bernardos, "Software-Defined Wireless Transport Networks for Flexible Mobile Backhaul in 5G Systems," Springer Journal on Mobile Networks and Applications, vol. 20, no. 6, pp. 793–801, 2015.

[15] J. R. Ballard, I. Rae, and A. Akella, "Extensible and Scalable Network Monitoring using OpenSafe," Proc. 7th USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2010.

[16] N. L. Van Adrichem, C. Doerr, F. Kuipers et al., "Opennetmon: Network Monitoring in Openflow Software-Defined Networks," in Network Operations and Management Symposium (NOMS), 2014. IEEE, 2014, pp. 1–8.

[17] L. M. Contreras, P. Doolan, H. Lønsethagen, and D. R. L´opez, "Operational, Organizational and Business Challenges for Network Operators in the Context of SDN and NFV," Elsevier Journal on Computer Networks, 2015.

[18] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1617–1634, 2014.

[19] S. Yeganeh, A. Tootoonchian, and Y. Ganjali, "On Scalability of Software-Defined Networking," IEEE Communications Magazine, vol. 2, no. 51, pp. 136–141, 2013.