# Software Defined Networking For Security Enhancement In Wireless Mobile Networks

**Mr. Najim Sheikh[1], Mr.Bharat Dhak[2]**
[1, 2]Assistant Professor,
[1, 2] Priyadarshini J.L College of Engineering

***Abstract-*** *Traffic volumes in mobile networks are rising and end-user needs are rapidly changing. Mobile network operators need more flexibility, lower network operating costs, faster service roll-out cycles, and new revenue sources. The 5th Generation (5G) and future networks aim to deliver ultra-fast and ultra-reliable network access capable of supporting the anticipated surge in data traffic and connected nodes in years to come. Several technologies have been developed to meet these emergent demands of future mobile networks, among these are software defined networking, network function virtualization, and cloud computing. In this paper, we discuss the security challenges these new technologies are prone to in the context of the new telecommunication paradigm. We present a multi-tier component-based security architecture to address these challenges and secure 5G software defined mobile network (SDMN), by handling security at different levels to protect the network and its users. The proposed architecture contains five components, i.e., secure communication, policy-based communication, security information and event management, security defined monitoring, and deep packet inspection components for elevated security in the control and the data planes of SDMNs. Finally, the proposed security mechanisms are validated using test bed experiments.*

***Keywords***- 5G, SDN, NFV, security, mobile networks, monitoring.

## I. INTRODUCTION

The evolution to 5G and future mobile telecommunication networks is characterized by a significant surge in demands in terms of performance, flexibility, portability, and energy efficiency across all network functions. Software Defined Mobile Network (SDMN) architecture integrates the prin- ciples of Software Defined Networking (SDN), Network Function Virtualization (NFV) and cloud computing to telecommunication networks. The SDMN architecture is designed to provide a suitable platform for novel network concepts that can meet the requirements of both evolving and future mobile networks.

The underlying principle of the SDN architecture is the decoupling of the network control and data planes. Using this principle, network control functions are logically centralized and the underlying network infrastructure is abstracted from the control functions. The introduction of NFV offers a new paradigm to design, deploy and manage networking services based on the decoupling of the network functions from pro- proletary hardware appliances, and providing such services on a software platform. However, the separation of control and data planes as well as the virtualization of network functions and programmability introduce a number of novel use cases and functions on the network. This will further usher in new stakeholders into the networking arena and hence will obviously alter the approach to security management in 5G and future telecommunication networks. Several proposals are available for securing general SDN networks [1]–[6] and SDMNs [7], [8]. However, none of these solutions pro- vide a unified solution to secure future 5G SDMN backhaul

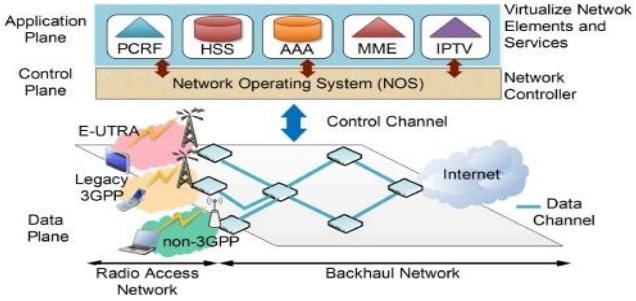


FIGURE 1. The consolidated SDMN architecture

### A. SDMN ARCHITECTURE

SDMN architecture integrates the core principles of SDN, cloud computing, and NFV into a design of programmable flow-centric mobile networks providing high flexibility. This modification is of significant improvement to the current LTE 3GPP (3rd Generation Partnership Project) networks. It offers benefits such as a uniform approach to Best Effort and Carrier Grade services, centralized control for functions that benefit from a network wide view, improvement in flexibility and more efficient segmentation. It also provides an enabling platform for automatic network management,

granular net- work control, elastic resource scaling and cost savings for backhaul devices. With SDMN, resource provisioning is done on-demand, hence allowing elastic resource scaling across the network [9].

B. SECURITY THREATS IN SDMN

As an ever-growing share of Internet use is over mobile networks [13], inherent Internet threats such as ease of Denial of Service (DoS) attacks, source address spoofing and distribution of malware apply to mobile networks as well. Similarly, SDN and NFV have their own security limitations as described in [12] and [14], and deploying these concepts in mobile networks without considering their inherent lim- itations will further elevate the security challenges. Hence, the separation of planes, aggregating the control functionality to a centralized system and running the control functions in the cloud as in SDN will open new security challenges for SDMNs.

## II. RELATED WORK

Since, SDN is considered to enable innovation in communi- cation networks, bring flexibility and simplify network man- agement, research efforts are going on for the deployment of its concepts in mobile networks. From security perspectives, SDN will enhance network security for two main reasons. First, it centralizes the network control plane that will provide global visibility of the network state and traffic behavior. Second, SDN brings programmability into communication networks through programmable APIs in the data forwarding elements.

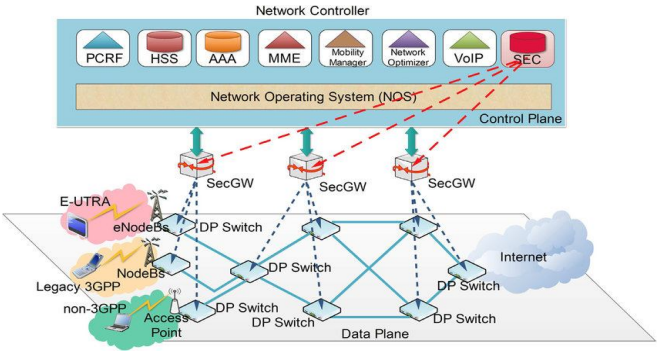


FIGURE 2. The proposed security architecture for SDMN.

## III. PROPOSED SECURITY ARCHITECTURE

Given that most of the requirement specific to telecom archi- textures are tightly coupled with the control and data planes than with the application plane [9], [12], hence, the proposed security architecture is geared towards securing the control plane, data plane and the Ctrl-Data interface (southbound interface). Figure 2 presents the proposed security architec- ture for SDMN networks.

The proposed SDMN security architecture is a multitier security approach with five components, namely;

1) Secure Communication (SC) Component.
2) Policy Based Communication (PBC) Component

A. SECURE COMMUNICATION (SC) COMPONENT

The SDMN architecture comprises of two main communica- tion channels, the data and control channels. The data channel handles the transportation of the user communication data while the control channel handles the movement of essen- tial control and signaling data between the data and control planes.The major security concerns in SDMN communication channels are the lack of IP-level security and weak authen- tication between backhaul devices as shown in Table 1. Existing SDMN communication channels are heavily reliant on higher layer security mechanisms like TLS (Transport Layer Security) /SSL (Secure Sockets Layer). A typical example is the widely used OpenFlow protocol which runs over a TLS/SSL based control channel [30].

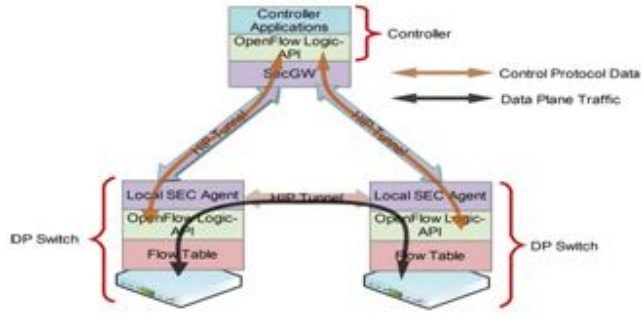


FIGURE 3. Secure communication channel.

Cooperation is a proven mechanism to effectively curb the antisocial behavior in a population [34]. We propose a two- tier cooperative approach to improve SDMN security and limit the extent of damage from Internet malpractices. The goal is to: 1) mitigate traditional attacks on SDMNs, i.e. DoS and source address spoofing; 2) encourage cooperation of all benevolent entities against the malicious source.3) tracing as well as containing all the resources used by the hacker in attacks. First tier is achieved by establishing the required level of edge-to-edge trust using Customer Edge Switching (CES). The second tier involves the ubiquitous collection and attribution of the attack evidences within a trust domain. CES nodes will then use the consolidated evidences to black and grey list remote entities.

For mobile networks, CES offers many advantages: (a) end users will benefit from a network firewall in the cloud, instead of relying only on host-based security solutions on The mobile device for blocking unwanted traffic and common attacks. This (b) saves computing resources of the device; and (c) contributes to battery lifetime of wireless device, by preventing unwanted traffic from reaching to device and disturbing its sleep cycle; besides preventing d) cluttering of air interface and network. CES does not require changes in end protocols, applications, or any explicit signaling from hosts to maintain their network connection: NAT bindings, or connection states. The policy-based communication facile-stated by CES means that all flows to the mobile hosts are admitted based on policy. Prior to admitting a flow, the remote node is a valid CES. The testing revealed that only flows from valid CES nodes are admitted into the network. A CES node based on its policies decides whether to accept an inbound flow or request the sender for additional details, which may result in another round of policy exchange. The negotiation of policies completes in either one or two round trips and results in either: a) success; or b) failure depending on policies. The subsequent connections from the sender

Having negotiated the CES policies, the subsequent flows from the sender only undergo one or two round trips of the host-to-host policy negotiation. A typical host-to-host user reutilize this validation result.

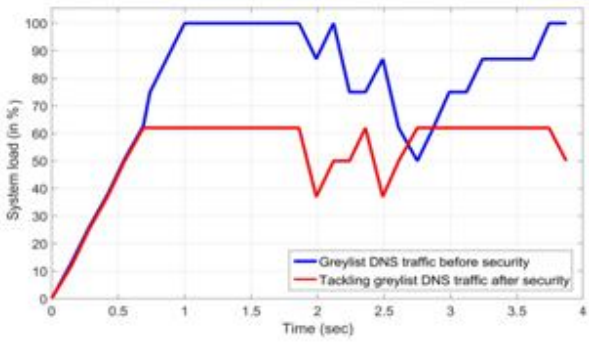


FIGURE 4. Delay induced by CETP policy negotiation on forwarding of the first packet of the user-data connection.

flow establishes after 80 msec or 145 msec delay incurred by 1-RTT or 2-RTTs of the host-policy negotiation, respectively. However, due to additional round of CES-policy exchange on the first inbound flow from the sender, the first host-to-host flow establishes in 220 msec for 1-RTT and 300 msec for 2-RTTs of the host-policy negotiation. Since we measured the connection setup on zero-latency links, one must add edge-to- edge latency of the real networks to get the actual connection setup delay. To account for network uncertainties, CES state machine can absorb any host retransmissions while the CETP process is still concluding.

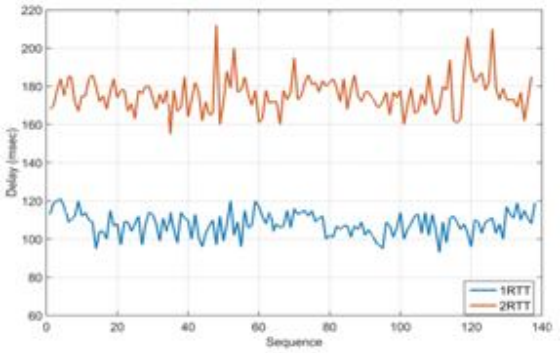


FIGURE 5. Delay induced by CETP policy negotiation on forwarding of the first packet of the user-data connection.

Figure 11 illustrates the connection setup delay of nearly 80 connections, using CETP host policies of varying com- plexity. The figure reveals that less complex policies are negotiated quicker than more complex policies that result in another round trip. Most of the presented delay in the figure is the due to slow control/data plane interaction, while the policy processing by CES is carried out in the order of milliseconds. In future, we aim to improve the CES-to-CES signaling by direct CES-to-CES control plane communicate and then synchronizing the negotiated user connection to the data-plane.

Figure shows the impact of resource allocation model on RGW on the event of a DNS flood. The model pre-vents the exhaustion of the address pool resources by rate limiting the DNS sources and by limiting the resources available to grey-listed DNS servers. By default, the servers that do not meet the SLA defined for trusted sources are relisted. This results in higher availability of address pool resources to legitimate DNS servers and clients, portico- larly under load conditions. Our testing of RGW revealed that TCP-Splicing completely eliminated spoofing, and no spoofed source could leak traffic into the private network or claim a user connection. A future version of the proto- type aims to employ SYN proxies instead of TCP-Splice, since they are optimized to handle millions of packets per second.

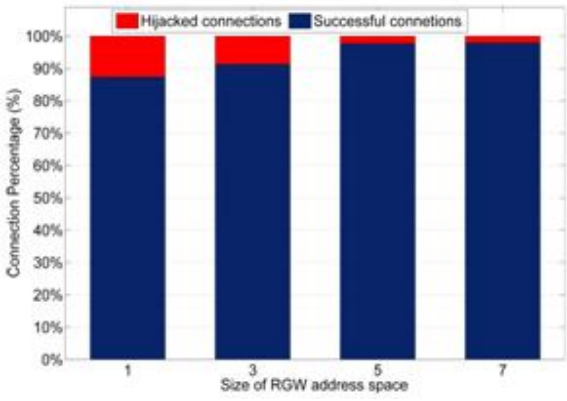


FIGURE 6. RGW security against non-spoofed floods.

Figure 13 presents an evaluation of the bot-detection algo- rithm which aims to filter floods from non-spoofed sources. The figure shows the impact of increasing the pool of inbound public IP addresses on RGW security. The figure shows that the security offered by the bot-detection algorithm is more effective if the attack surface for the hackers is larger.

In the third set of experiments, we validate the performance of SIEM and SMM components. The experiment testbed is presented in Figure 14. We used Mininet v2.2.1 the net- work emulation environment and OpenvSwitch v2.3.1 for the deployment of SDN switches. Floodlight v1.1 was used as the SDN controller. Security monitoring and management elements such as SDN adapted SIEM, security sensor and security server were connected via a legacy switch. S1,S2, and S3 were virtual SDN switch which were implemented as OpenvSwitches. RO (Route Optimizer) deals with a vir- tualized element for routing purposes. The test network had been segmented into four LANs depending on the nature of their services. These segments have different security require- ments. Tests were conducted with two users.

- DMZ LAN: It includes services exposed to Internet.
- Security LAN: It includes security services, such as the security sensor.
- Server LAN: It includes internal services.
- Client LAN: This is the end-user network.

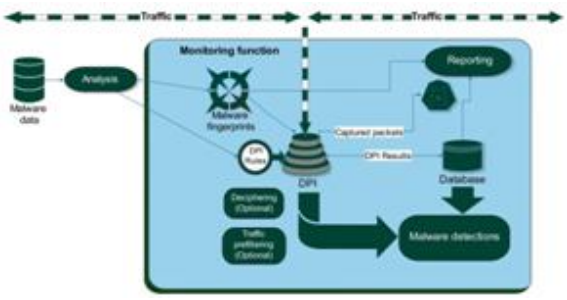


FIGURE 7. The layout of the experimental testbed for deep packet inspection (DPI) component.

In the fourth set of experiments, we validate the perfor- mance of DPI component. Figure 19 illustrates main com- ponentes of the developed monitoring prototype. The threat detection is based on malware fingerprints that are compared with monitored online traffic patterns as part of DPI analysis. Possible malware detections are then written to the local database with the other analysis data produced by the DPI component. Tests were conducted with a total of 10 simulated hosts.

In the evaluation environment about 5 percent of all data flows were interpreted as HTTP application flows by the DPI engine and therefore were compared with fingerprints (i.e., signature detection). In real time analysis we could not mea- sure any increase of CPU usage compared to the reference DPI analysis when the same number of metadata attributes were extracted. It has been found that the actual performance penalty should be measured at high data rates when packet drops may occur due to the additional processing. The average processing delay was defined as the measure of the delay from the time the flow starts to the time a packet is received that allows the first detection decision to be made. In the test bed environment, the average detection decision delay was 57 ms. The results of the validation show that it is possible to perform DPI in SDN scenarios by using the proposed DPI component.

## IV. DISCUSSION

Introducing SDN and NFV to networking will be a major game changer to the wireless networking arena. The costs, efficiency and network performance will be the main drivers of the change. There are two notable theories when it comes to network security. First is the idea of centralizing network control to minimize the fragmentation of security mecha- nisms. However, this inadvertently leads to higher risk of security lapses at a single point of failure, and this gives rise to the second theory which is using SDN to enhance network security by leveraging on its global network visibility feature as well as the centralized control functions. The proposed security gateways in this architecture.data plane element at trust domain boundaries because a standard OpenFlow switch does not have all the capabilities for packet filtering or rate limiting that are needed in a proper firewall. To improve performance, many of the security mechanisms we implemented in the proof-of-concept version of CES can be significantly improved. We are now work- ing on making substantial improvements. Moreover, there is also a need to investigate other identity-location separation architectures beside HIP, this will pave way for higher mobil- ity with security in future wireless networks.

## V. CONCLUSION AND FUTURE WORKS

This paper investigated the security vulnerabilities in SDMN (Software Defined Mobile Networks) and proposed novel security architectures to mitigate them. On the up side, SDMN concepts will improve network security leveraging on it global visibility of the network state in addition to its cen- tralized control and network function softwarization. On the down side, these same attributes also introduce new vulned- abilities that are inherent to software applications, Internet- based systems, and new technologies. This paper presented a comprehensive collection of the pros and cons related to SDMN as well as the state of the art for implementing security

architectures in SDMN. Based on the outcome of the experiments in this work, we maintain that security considerations are paramount when relying on SDN and NFV.

Various security methods have been implemented on the SDMN platform. In this work, we presented a multi-tier secu- rity architecture based on five key components: (1) secure communication channels leveraging on HIP. This is used to secure both control and data channels; (2) policy-based communications. This will serve to mitigate DoS attacks as well as source address spoofing, it will also allow net- work communications between end hosts only after a suc- casual negotiation of policy between edge nodes. This will effectively tackle the problem of unwanted traffic across the network and managing all flow admissions by policy;(3) security management and monitoring where the secu- rity mechanisms implemented are monitored on one hand while detected security threats are isolated using DPI and traffic monitoring techniques on the other hand; (4) Security Defined Monitoring (SDM) to orchestrate the monitoring activities related to security and finally 5) Deep Packet Inspection (DPI) component for improved security threat detection.

In this work, we analyzed the feasibility of implementing these components in a real-world using testbeds. The out- come of these experiments showed that the proposed security architecture can be implemented in real-world and would be able to prevent IP based attacks on SDMNs. The results of the validation also show that it is possible to automate mitigation and reaction actions in SDMNs by providing countermeasures and mitigation actions directly using REST- ful API in an SDN controller. The result of the validation shows that multiple sources of information can be com- bined to provide more accurate and rapid detection of cyber-attack.

Notwithstanding, certain elements of these system still needs to be examined in greater detail before integrating these new systems with the existing production environments.

We will extend this research to further analyze these requirements and define specific guidelines for the integration of the proposed security components into the SDMN architecture.

## VI. ACKNOWLEDGMENT

This work has been performed in the framework of the CELTIC project CP2012 SIGMONA and SECURE Connect (Secure Connectivity of Future Cyber-Physical Systems) Projects. The authors would like to acknowledge the contri- butions of their colleagues.

## REFERENCES

[1] S. Shin, P. A. Porras, V. Yegneswaran, M. W. Fong, G. Gu, and M. Tyson, ''FRESCO: Modular composable security services for software-defined networks,'' in *Proc. NDSS*, Apr. 2013, pp. 1–16.

[2] J. Kempf, E. Bellagamba, A. Kern, D. Jocha, and A. Takacs, and P. Sköldstrom, ''Scalable fault management for OpenFlow,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 6606–6610.

[3] K. Phemius, M. Bouet, and J. Leguay, ''DISCO: Distributed multi- domain SDN controllers,'' in *Proc. Netw. Oper. Manage. Symp. (NOMS)*, May 2014, pp. 1–4.

[4] Y. Zhang, N. Beheshti, and M. Tatipamula, ''On resilience of split-architecture networks,'' in *Proc. Global Telecommun. Conf. (GLOBECOM)*, Dec. 2011, pp. 1–6.

[5] A. K. Nayak, A. Reimers, N. Feamster, and R. Clark, ''Resonance: Dynamic access control for enterprise networks,'' in *Proc. 1st ACM Work- shop Res. Enterprise Netw.*, 2009, pp. 11–18.

[6] H. Hu, W. Han, G.-J. Ahn, and Z. Zhao, ''FLOWGUARD: Building robust firewalls for software-defined networks,'' in *Proc. 3rd Workshop Hot Topics Softw. Defined Netw.*, 2014, pp. 97–102.

[7] S. Luo, J. Wu, J. Li, L. Guo, and B. Pei, ''Toward vulnerability assessment for 5G mobile communication networks,'' in *Proc. IEEE Int. Conf. Smart City/SocialCom/SustainCom (SmartCity)*, Dec. 2015, pp. 72–76.

[8] X. Duan and X. Wang, ''Authentication handover and privacy protection in 5G HetNets using software-defined networking,'' *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 28–35, Apr. 2015.

[9] K. Pentikousis, Y. Wang, and W. Hu, ''Mobileflow: Toward software- defined mobile networks,'' *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 44–53, Jul. 2013.

[10] H. Hawilo, A. Shami, M. Mirahmadi, and R. Asal. (2014). ''NFV: State of the art, challenges and implementation in next generation mobile networks (vEPC).'' [Online]. Available: https://arxiv.org/abs/1409.4149

[11] M. Liyanage, M. Ylianttila, and A. Gurtov, *Software Defined Mobile Net- works (SDMN): Beyond LTE Network Architecture*. Hoboken, NJ, USA: Wiley, 2015.

[12] M. Liyanage, A. Abro, M. Ylianttila, and A. Gurtov, ''Opportu- nities and challenges of software-defined mobile networks in net- work security,'' *IEEE Security Privacy*, vol. 14, no. 4, pp. 34–44, Aug. 2016.

[13] ITU-T. (2016). *World Telecommunication/ICT Facts and Figures*. [Online]. Available: http://www.itu.int/en/ITU-

D/Statistics/Pages/stat/default.aspx

[14] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, ‘‘Security in software defined networks: A survey,’’ *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2317–2346, 4th Quart., 2015.

[15] A. Y. Ding, J. Crowcroft, S. Tarkoma, and H. Flinck, ‘‘Software defined networking for security enhancement in wireless mobile networks,’’ *Comput. Netw.*, vol. 66, pp. 94–101, Jun. 2014.

[16] T. Hinrichs, N. Gude, M. Casado, J. Mitchell, and S. Shenker, ‘‘Express- ing and enforcing flow-based network security policies,’’ Univ. Chicago, Chicago, IL, USA, Tech. Rep., 2008, vol. 9.

[17] S. Gutz, A. Story, C. Schlesinger, and N. Foster, ‘‘Splendid isolation: A slice abstraction for software-defined networks,’’ in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 79–84.

[18] R. Beckett, X. K. Zou, S. Zhang, S. Malik, J. Rexford, and D. Walker, ‘‘An assertion language for debugging SDN applications,’’ in *Proc. 3rd Workshop Hot Topics Softw. Defined Netw., Ser. HotSDN*, vol. 14. 2014, pp. 91–96.