A Survey on the Placement of Virtual Security Network Functions in Softwarised Networks

Godwin Thomas Samuel Chapanduka

Department of Electrical Engineering, Tshwane University of Technology, Private Bag X680 Pretoria 0001, South Africa

Abstract— *The introduction of an SDN-NFV ecosystem has created a general paradigm shift in telecommunications architecture from protocols to Application Programming Interfaces (APIs) and from 'boxes' to functions. This is delivering 'Softwarised Networks' targeted at lowering the cost of network and service operations and ultimately introducing higher flexibility. The collaborative use of SDN and NFV results in the virtualisation of network security functions and deployment of these as virtual security network functions (VSNFs) in commodity servers, thus reducing costs as well as enabling faster development and innovations. VSNFs such as IDS, firewall, DPI etc. can reside as applications in the SDN-NFV architecture. An important problem discussed in the literature is the issue of where to place these functions in the network. When placing these network security functions, objectives such as cost, delay, proficient use of network resources, network load, energy consumption, network security requirements etc, must be taken into account when placing the security functions, This paper presents a comprehensive survey of the placement of VSNFs in the SDN-NFV ecosystem by critically analysing the state-of-art solutions, identifying open research problems and making suggestions for insights to solve the identified placement problems*

Index Terms— **Software-Defined Networking (SDN), Network Function Virtualisation (NFV), Virtual Security Network Function (VSNF)**

1. INTRODUCTION

1.1 Background Information

According to an Ericsson Mobility report, approximately 3.5 billion 5G subscriptions are forecasted by the end of 2026 [1]. By the end of 2022, the Business To Business (B2B) IoT market will surpass US$500 billion, according to Bain and Company estimates [2] and the overall IoT spending is expected to reach US$726.5 billion at the end of 2022 based on data from IDC Forecasts Worldwide Technology [3]. The subsequent cost to organisation and economies is substantial and growing. The deployment of 5G network presents an opportunity for telecom operators to tap into the above mentioned new revenue streams emerging from the digitalisation of industries according to an Ericsson report. It is estimated that 24 billion devices will be interconnected by 2050 which means almost every object around us [1]. The data generated by these IoT devices are immensely high and will continue to rise on an unprecedented scale. This results in challenges in flow management, resource allocation and in particular security concerns. Organisations are investing immensely toward security capabilities that are failing to deliver the greatest efficiency and effectiveness. According to Accenture/Ponemon Institute report [4] (The Cost of Cybercrime) the average cost of cybercrime per organisation rose by more than $1m to reach $13m in the past three years. It is indeed clear that the current network security systems are not coping and will not cope with the future networks that are going to be softwarised and programmable. It therefore gives impetus to the need to research into new network security systems that will curtail revenue leakages.

1.2. Definitions of VSNFs and the Objectives of this Survey Paper

1.2.1 Software Networks

The expression "Softwarised Networks" refers to a paradigm shift in the telecommunications architecture from "boxes" to "functions", and also from "protocols" to "Application Programming Interfaces (APIs)". This shift is driving a convergence between IT infrastructure and telecommunications. This is consequently transforming several industries. The introduction of an SDN-NFV ecosystem is targeted at lowering the cost of network and service operations and ultimately introducing higher flexibility while reducing the time to market for new services. Through the collaborative use of SDN and NFV, delivery of on-demand network security services can be realised. Network security functions are virtualised and deployed as virtual security network functions (VSNFs) in commodity servers, thus reducing costs as well as enabling faster development and innovations.

1.2.2 VSNF Deployment

VSNFs can be removed, installed and migrated dynamically to suite the network resource requirements [5]. VSNFs are placed in a chain of a specific order in the substrate network forming a service function chain (SFC). Fig.1 shows an example of VSNFs deployment on substrate network. The top graph shows three VSNFs between source and destination nodes. The bottom graph is a substrate network with eight substrate nodes where SFC can be deployed.

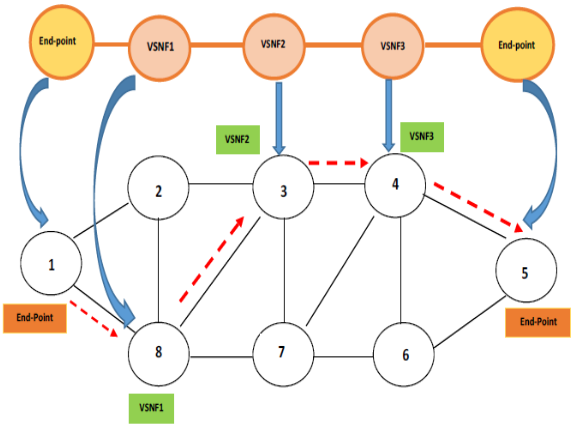


Fig. 1: An example of VSNFs deployment on substrate network

1.2.3 Contribution Summary

This paper presents a comprehensive survey of the placement of VSNFs in the SDN-NFV ecosystem by critically analysing the state-of-art solutions, identifying open research problems and making suggestions for insights to solve the identified placement problems

1.3 Organisation of the Paper

The rest of this paper is organised as follows: Section two (2) presents a brief description of NFV and SDN technologies and the relationship between them. The most common VSNFs in an SDN-NFV architecture is also reviewed. Section three (3) provides a comparison and examination of studies on the optimal placement of virtual security network functions. Finally, in Section four (4) open research challenges in this area of study are identified and ultimate suggestions of possible future directions that researchers can consider are made. It is hoped that this article will provide extensive guidelines for new researchers who would like to explore this avid area.

2. DESIGN CONSIDERATIONS AND RESEARCH CHALLENGES

2. Introduction

In this section, NFV and SDN technologies are briefly described; the relationship between them; review the most common VSNFs in an SDN-NFV architecture and state the research challenges.

2.1. SDN, NFV, SDN/NFV Ecosystem

2.1.1 Definition of SDN

SDN is an approach to network management in which network configuration are done programmatically. This result in improved network performance and monitoring [6]. As indicated in Fig. 2, SDN centralises network intelligence by separating the forward process of network from the routing process.

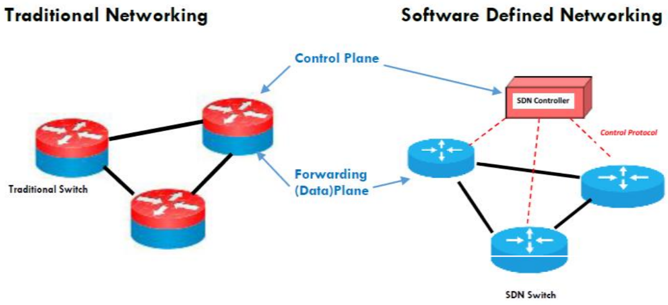


Fig. 2: Comparison of SDN and traditional networking

Figure. 2. Comparison of SDN and traditional networking

The SDN network intelligence in incorporated in the control panel which has one or more controllers. The SDN architecture consists mainly of three (3) planes (Fig. 3), namely, application plane, control plane and data plane, with their corresponding application programming interfaces (APIs). SDN architectures decouple network control and forwarding functions, enabling network control to become directly programmable [7].

The SDN architecture has the following attributes:

- *Direct programing:* The development of the forwarding function from the Network control ensures direct programming of the latter.
- *Agility:* Administrators can dynamically adjust the network-wide traffic flow to suite changing needs.
- *Central management:* Intelligence is centralised in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch.

- *Configuration Programmability:* SDN allows network managers configure, manage, secure, and optimise network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.

2.1.2 Definition of NFV

Network functions virtualisation (NFV) USES it virtualisation that can be connected or chained to form communication services. A VNF consists of one or more virtual machines running different software running different software processes. For example, a virtual session border controller could be deployed to protect a network without the typical cost and complexity of obtaining and installing physical network protection units. Other examples of NFV include virtualised load balancers, firewalls, intrusion detection devices and WAN accelerators [9].

NFV Framework: The NFV framework consists of three main components: [10]

(i) Virtualised network functions (VNFs) are software implementations deployed on a network functions virtualisation infrastructure (NFVI).

(ii) NFVI includes all software and hardware components that build the environment where VNFs are deployed. The NFV infrastructure can span several locations.

(iii) NFV-MANO: is the NFV management of orchestration architectural framework. It is a collection of functional blocks and data (storages) used by these blocks. It consists of NFVI managers and virtualisation software.

The following are the advantages of having NFV over traditional network architecture [11]:

- It cuts down the need to purchase new physical devices and hence the related cost.
- Improvises operational performance and efficiency.
- Improvises allocation of resources
- it reduces the consumption of energy
- faster and flexible deployment.

NFV is highly advantageous, but at the same time, it faces certain security threats which need to be handled. NFV definitely provides some of the unique advantages such as cost and energy saving, flexible deployment and scalability but it also faces major security challenges. The security attacks which revolve around VNFs in an NFVI can belong to three major categories: 1) Attack from within a VNF (Internal Weakness), 2) Attack from outside a VNF (External threat) and 3) Attack occurring between VNFs (Migration of an attack) [12].

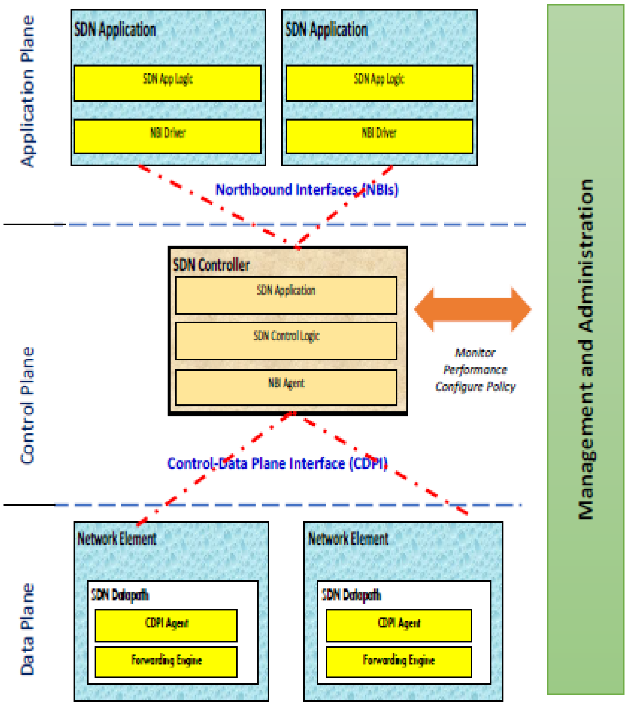


Fig. 3: Overview of Software Defined Networking Architecture

2.2 Overview Of SDN in The NFV Architectural Framework

SDN/NFV Relationship: Software Defined Networking (SDN) and Network Function Virtualisation (NFV) are the key pillars of future networks, including 5G and beyond that

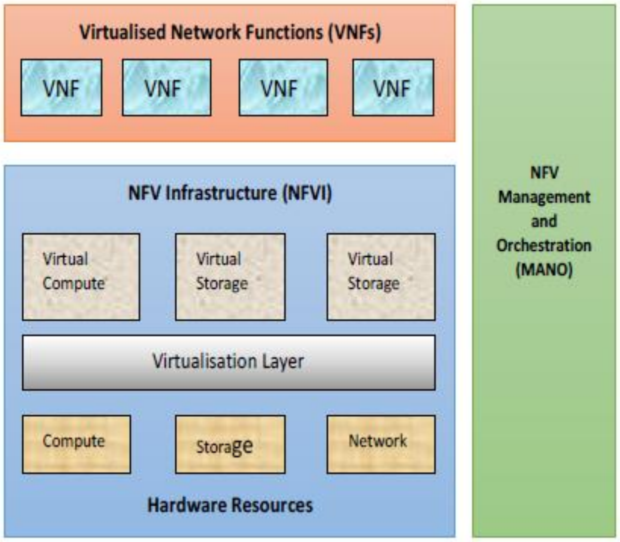


Fig. 4: NFV high-level architecture

In SDN and NFV technologies, software can finally be decoupled from the hardware, so that it is no longer constrained by the box that delivers it. This is the reason why SDN and NFV have become the key to building promise to support emerging applications such as enhanced mobile broadband, ultra-low latency, massive sensing type applications while providing the resiliency in the network. Service providers and other verticals (e.g., Connected IoT, Cars, eHealth) can leverage SDN/NFV to provide flexible and cost-effective service without compromising the end user quality of service (QoS).

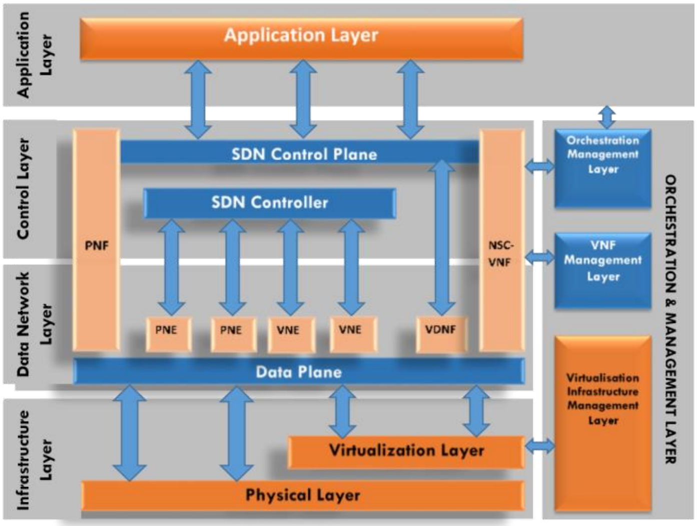


Fig. 5: Overall architecture of SDN/NFV integration &

networks that can: helping organisations to rapidly deploy new services, applications and infrastructure to quickly meet their changing requirements; enabling organisations to create new types of services applications and business models; create new revenue generating services; supporting automation and algorithm control through increased programmability of network elements to make it simple to design, deploy, manage and scale networks, allowing network functions to run on off the-shelf hardware. Fig 5: shows Overall architecture of SDN/NFV integration and management. Fig 6 shows an extended SDN/NFV architecture. and offers tools for the orchestration of complete network applications and its management. The *top layer* groups applications that use the application interface to orchestrate and deploy services in the platform. While

Some of the security challenges and opportunities introduced by SDN/NFV are:

- Hypervisor
- Virtual Network Functions (VNFs)
- SDN Controller
- Orchestrator
- Security function virtualisation

2.3 Summary of Section

Incorporate SDN and NFV in concerted ecosystems is advantageous (Fig 6). When SDN features drive an NFV network, the virtual overlay assists in provisioning and managing VNFs. In contrast to the hardware based networks of the past, the technology takes advantages of virtualisation and cloud systems. However this leaves the network more vulnerable to breaches if not properly secured.

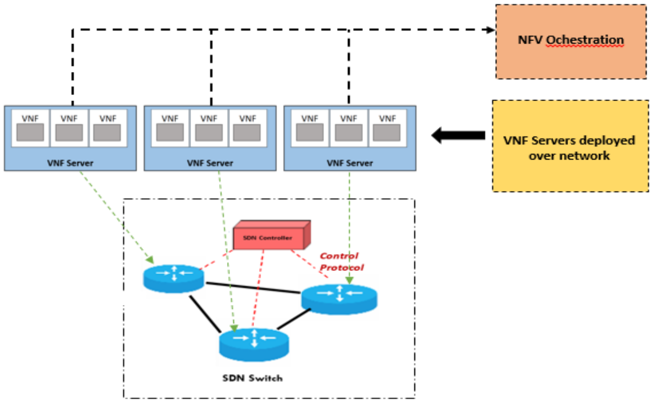


Fig. 6. SDNFV Architecture

3.0 STATE OF THE ART PLACEMENT METHODS

3.1 Introduction

In this section, the most common VSNFs in an SDN-NFV architecture and their uses in security is reviewed. A comparison and examination of studies on the optimal placement of virtual security network functions in an SDN-NFV ecosystem is also provided.

3.2 Virtual Security Functions in SDN-NFV Ecosystem

3.2.1 Security VNFs

In traditional networks, network security functions are implemented on vendor-specific appliances located at specific points [15]. However in an SDNFV architecture, these security functions are virtualised and placed in suitable virtual machines where they are executed [16,17]. Fig. 7 below shows typical security VNFs for an SDNFV architecture.

3.3 Classification of VSNFs

Virtualised security network functions are classified into three (3) categories, namely: *Detection, Prevention* and *Security Analytics.* The rest of this section gives an overview of the recent studies on the mentioned categories.

3.3.1 Detection Functions

Distributed denial of service (DDoS) detector: A target computer is overwhelmed by sending a high volume of fake requests in high volumes and consequently it cannot process real requests and will continue to be out of service. There are a variety of solutions to detect DDoS in traditional networks; but most of these solutions require analysing large numbers of packets. So while response time increases, their accuracy level decreases [18,19]. However, in SDN-NFV ecosystem, DDoS attacks can be detected more effectively with better response time since numerous switches can be directly controlled by the controller simultaneously [19].

Malware scanner: Malware scanners protect the local network from the malicious software such as viruses, worms, trojans etc [20] as malware analysis architecture by utilising the flexibility of SDN. The inspection module on top of the SDN controller analyses network flows by looking for pre-defined patterns. If malicious traffic is detected, the containment module prevents the malware from communicating with other elements, and the configuration manager modifies the network architecture dynamically according to the traffic characteristics [20]. Experimental results show that the proposed system detect more malware events than traditional solutions. *Intrusion detection system (IDS):* In traditional networks, Intrusion Detection Systems are the passive security functions that monitor the network, detect the malicious activities and policy violations to system administrators [21]. Also, performance is adversely affected as the network grows and complexity increases [23]. However in SDN, which is a software based architecture, collecting statistical data and routing the traffic is easier than the traditional networks. Authors in [24] developed an IDS named as OpenNetMon which detects the intrusions by evaluating the throughput, delay metrics and packet loss. The central view of the SDN controller enables access to a large amount of data to be analysed.

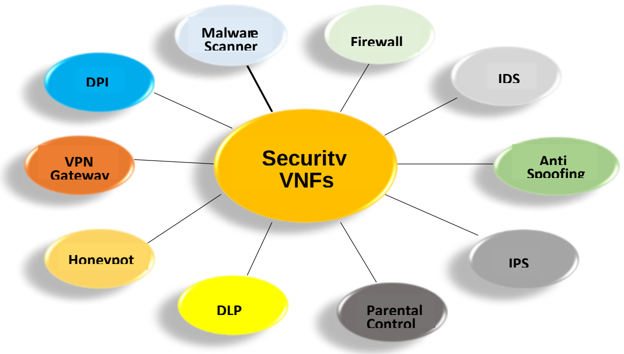


Fig. 7. Typical Security VNFs

3.3.1 Prevention Functions

Intrusion prevention system (IPS): Traditional IPSs are implemented on IDSs because they mainly need the attacks to be identified. Although many are open source software tools, different coding styles, development environments and interfaces make it difficult to deploy these systems. In addition, producing dynamic solutions to changing network states is quite difficult with the IPSs on traditional networks [22]. In SDN-NFV, on the other hand, IPSs detect and prevent intrusions in a dynamic manner, more agile and with lower cost. In the literature, the number of studies developing IPS for SDNNFV ecosystem is fewer than other security functions. The authors in [25] proposed an SDN based IPS and a load balancing function. Experimental results show that the proposed IPS model can detect attacks in shorter time and reduce latency with load balancing.

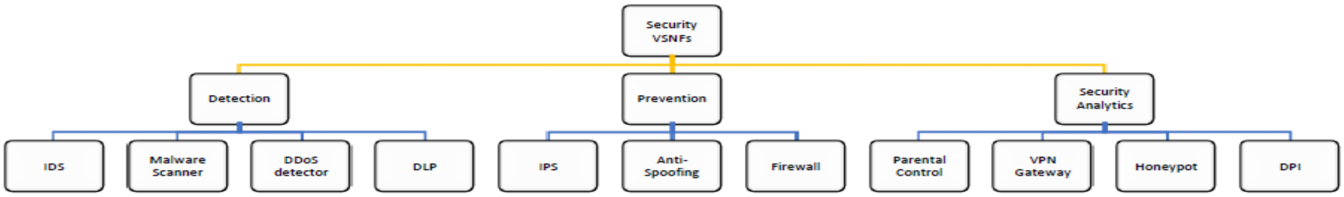
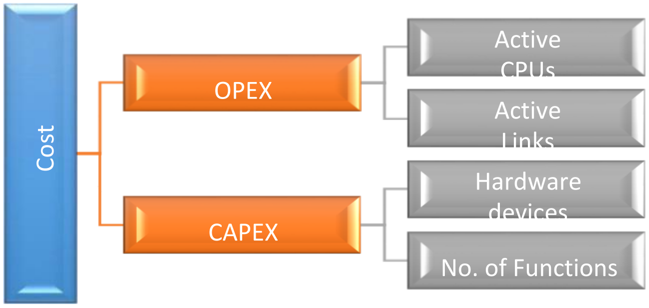


Fig. 7. Classification of VSNFs

Firewall: In traditional networks, due to the static firewall position, internal traffic cannot be seen and audited. With SDN, all internal traffic can be filtered because the firewall is implemented as a software function independent of physical location. Packet filtering is only one aspect of firewall design in SDN. Compliance with firewall rules and dynamic flow rules is also verified since configurations, network conditions, and flow rules can change dynamically. In addition, firewall placement architecture (distributed or central) and the exact places for this function should be determined carefully [26,27]. The authors in [26] developed a firewall solution called FlowGuard that can resolve policy violations automatically and in real-time when networks conditions change. In [28], the authors propose VNGuard framework for managing virtual firewalls with NFV. VNGuard involves a module for finding the optimum places for the policies defined by the virtual functions.

Anti-spoofing: Spoofing in different network protocols is a widespread technique utilised by adversaries to combat attack detection and mitigation. Proposals against IP spoofing generally involve the use of cryptographic primitives such as message authentication codes and filtering tables maintained by SDN controller applications [29,30]. Similarly, SDN application modules have been developed to prevent ARP spoofing by substituting the header fields of ARP request packets with safe dummy values to protect switches from cache poisoning [31] or performing validation in real time using dynamic MAC-IP association lists [32].



3.3.2 *Security Analytics Functions*

Honeypot: Honeypot is software with deliberately placed vulnerabilities to monitor intrusions and penetrations, detect new types of attacks and learn about attack methods. In SDN, the systems requiring dynamic routing and learning like honeypots attain better results than in traditional networks since the infrastructure is controlled by software [33]. In this regard, authors in [34] proposed a framework called FRESCO in which there are several security modules as well as honeypot. Fresco sends traffic to the honeypot when it detects a malicious connection request. Hence, the attackers think they are connected to the real target and cannot therefore penetrate the original system [34]. HoneyMix [35] is another honeypot-based system that utilises the programmability in SDN to exercise fine-grained control on network traffic and keep attackers occupied on the honeynet as long as possible to prevent them from threatening valuable targets.

Deep packet inspection (DPI): DPI is an advanced method for real-time detailed flows and user activities analysis. DPI engines examine the payload portion of a packet in terms of traffic type, malware content, packet headers and protocol compliance. In case of a suspicious event or an attack threat, DPI reroutes the packet to a different destination or reports it to another security tool [36]. Thus, it aims to protect the system from attacks, improve the performance, control the congestion, reduce bandwidth costs and enhance the quality of service [37]. In traditional networks, DPI engines which are implemented on hardware middleboxes are placed in specific locations on the network. However, with NFV and SDN, DPI tools are virtualised and dynamically deployed [36,38]. They argue that omitting the QoS causes performance degradation to latency-sensitive applications, in particle when traversing computationally-demanding security functions such as IDS/IPS. Although the literature reviewed addresses the placement of VSNFs, few solutions have been proposed with a focus on the network security constraints and requirements of the VSNF placement. In [61] the authors propose a heuristic algorithm and ILP formulation for efficiently composing chains of virtual security functions placement. In [61] the authors propose the model is aimed at preventing inefficient or incorrect placement of security functions, such as deployment of VPNs at the edges and an IDS at the core network.

3.4 Placement of VSNFs in an SDN-NFV Ecosystem

This section provides a comparison and examination of studies on the optimal placement of virtual security network functions in an SDN-NFV ecosystem.

3.4.1 OPEX and CAPEX

In an SDN-NFV ecosystem, security is provided by deploying virtual security functions such as intrusion detection/prevention systems (IDS/IPS), deep packet inspection (DPI), firewall etc. However, one of the important new challenges faced by network operators is where to deploy these virtualised functions. Hence, optimising the placement of virtual security functions for various objectives is an important research issue [40-42]. From the operational point of view, these functions must be placed with regards to possible conflicting objectives such as traffic management, load balancing, delay and energy consumption as well as meeting network security requirements [38,43,44]. Therefore, there is a need for virtual function placement solutions that simultaneously respond to the operational requirements of the network and do not compromise the security policies [16,45,46]. Generally, studies on virtual security function placement focus on finding the optimal solution in terms of cost efficiency. In this regard, the parameters used to define cost is classified in two categories (Fig. 9): OPEX (Operating expenses) and CAPEX (Capital expenditures). OPEX comprises network operational costs such as network planning, reconfiguration, provisioning, and the usage of network resources etc. [47]. CAPEX includes infrastructure costs such as installations, purchased hardware, software license fees etc.

OPEX Minimisation: An important factor affecting the network operating cost is energy consumption of the servers. To address this issue, in [48] an energy-aware virtual security function placement model is proposed which aims to place virtual security functions at optimum locations while minimizing server energy consumption. For this purpose, an integer linear programming (ILP) model is presented with strict security constraints. When placing multiple virtual security functions in NFV-SDN ecosystem, rules of these functions should not conflict with each other. Therefore, sequential order of them should also be taken into consideration. The authors in [49] studied placing virtual security functions in specific order while computing costs and minimizing latency. Their proposed model is aimed at routing traffic over less nodes in a short time. They tested their algorithm in OpenStack on OpenDaylight controller. The proposed algorithm produces better results than the current placement algorithm of OpenStack. The work in [50] consider the Quality of Service (QoS) and specific security requirements of each user application, and they aim to minimise total bandwidth used. Unlike other studies, they take security constraints into account instead of focusing on only cost optimisation constraints. An important advantage of this model is that it solves the placement problem for dynamic network scenarios where the service requests change over time.

CAPEX Minimisation: The SDN-NFV ecosystem approach reduces CAPEX by eliminating the need for single-purpose hardware appliances in networks, minimising the number of virtual functions, and thus the money spent for purchasing and deploying them on servers. Authors in [50] studied the placement of multiple virtual security functions with the objective of minimising the number of activated functions. Their optimisation model, which is based on genetic algorithm, allows specifying ordering constraints for functions. However, the work does not take into account the specific security requirements and resource consumption parameters of different types of functions. In [37], the authors stated that the deployment of DPI functions is costly in terms of license fees. Therefore there was a need to deploy DPI engines cost effectively inorder to meet network security constraints. For this purpose, the works proposed a genetic algorithm based approach that minimises the network load and number of engines at the same time. However, this approach is not scalable for larger networks. Therefore, the authors solved the same problem with integer linear programming [39] and reduced the complexity in [37] with their graph based greedy algorithm. The work in [16] proposed a framework named Ordered Cloud Defense Optimization (OCDO) that determines the proper order for security functions by calculating their priorities. The primary goal is to perform these tasks with minimum cost in a scalable fashion.

3.5 ANALYSIS

VSNFs Placement

There are a number of research works that consider specifically the placement of VSNFs. The authors in [51], focuses on searching optimal placement for VSNFs. The best hosts are the ones most capable of controlling the traffic. This is determined by the node centrality that represents the degree of connectivity between nodes The authors in [52],

propose a novel resource allocation scheme that deploys VSNFs optimally for cloud providers. The authors of [53]

TABLE 1 Studies On Placement Of Virtual Security Network Functions

VSNFs Placement Problem	Cost		Flow Management Strategy		Method Of Optimisation			Reference
	OPEX	CAP EX	Static	Dynamic	Genetic	ILP	Heuristic	
Minimise bandwidth consumption and maximum link utilisation	✓	✓		✓	✓	✓	✓	[76][36][38][49][50][66]
Minimise installation, transportation, reassignment, migration costs	✓			✓		✓		[75][16][38][40-44][45-50]
Minimise the number of used servers	✓	✓	✓	✓		✓	✓	[73][49][50]
Minimise flow rules and traffic between functions	✓		✓	✓		✓	✓	[74]16][28][36][38][48][49][50]
Minimise distance metric between clients and servers.	✓	✓		✓		✓	✓	[71][51][52][59]
Minimise end-to-end delay	✓			✓		✓	✓	[72][11][28][39][48]
Real-time placement	✓			✓		✓	✓	[17,67-70]

address problem of allocating VSNFs in cloud data centres by using the Best-Fit Decreasing (BFD) algorithm. In [58] the authors formulated the optimal placement problem as a travelling purchaser problem. The authors in [59], address the VSNFs placement problem by focusing on the proposing an ILP formulation whose objective is the minimisation of the energy consumption of servers though security constraints were not addressed. . This solution does not consider any security constraints. In [60] the authors proposed ILP formulation for placing VSNFs which takes into security constraints and quality of services (QoS). They argue that exclusion of QoS causes performance degradation. In [61] the authors propose a heuristic algorithm and ILP formulation for efficiently composing chains of virtual security functions. The ILP formulation includes a single security related constraint. The authors in [62], presented a model that takes into consideration deployment constraints. However the optimatisation algorithm does not scale well because it always computed for all flows in the networks. The network partitioning scheme is limited to fat-tree topologies. Lack of consideration of the end-to-end latency as one of the constraints of the proposed model, limits its application space. In [63], the authors consider network security defence patterns (NSDP) that selects deployment options and captures best security practices. In [64] a three stages model to solve the VSNFs mapping problem is presented. In stage 1 the requested security practices are translated into chained VSNFS. In stage two (2), to security of SFC mapping is presented as mixed ILP. Finally in stage 3 the MILP problem is solved. The proposed research work aims is to minimise the end-to-end communication delay by taking into consideration the security constraints (ie propagation, process delay) while keeping the overall deployment cost to minimum. In [65], the authors propose PESS (Progressive Embedding of Security Services), a VSNF provisioning model aimed at reduction in end-to-end latency of application traffic by deploying. In [66], the authors propose a Security Defense Patterns Aware Placement (SDPAP) approach that takes into account security and cost optimisation constraints. The model is aimed at preventing inefficient or incorrect placement of virtual security functions for example the deployment of an IDS at the core network.

3.6 Summary of Section

Virtual security functions are deployed on the network to provide security. Hence the optimisation the of virtual security functions placements is an important issue of research [40-42]. The placement of VSNFs must take into consideration factors such as load balancing delay energy consumption, traffic management and network security requirements [38,43,44] and must no compromise the security policies [16,45,46].

4. OPEN RESEARCH ISSUES AND POSSIBLE SOLUTIONS

4.1 Introduction
This section provides a comparison and examination of studies on the optimal placement of VSNFS functions in an SDN-NFV ecosystem.

4.2 Research Challenges and Possible Solutions

1. Placement of Different Types of Security Functions: As indicated in Fig. 6 there are several security functions. Apparently there is a lack of studies addressing the deployment of virtual IDSs. Consequently the optimal placement of different type of new security functions is a good line of future research.

2. Placement of Multiple Security Functions: Considering the placement of only one VSNF does not suffice. These studies focus on multiple VSNFs and are analysed in a general framework [16][48,49].

3. Optimal Placement For SDN-NFV ecosystem: The main objective of VSNFs placement solutions is finding the optimal solution taking into consideration cost, delay, performance, energy-aware, scalability etc [16,28,36,38,48,49,50] However there are yet to be studies on optimal placement of VSNFs in an SDN-NFV ecosystem optimising fault tolerance. Hence new models are needed that address objectives from the real world arena.

4. Real-time Placement Solutions: Realtime and dynamic placement are needed [17,67-70]. In order to achieve network security objectives since adding a new security function or changing deployment locations of the functions or may be of vital importance. Provision of uninterrupted service is an important issues that may must be addressed by developing algorithms for dynamic placement of VSNFs.

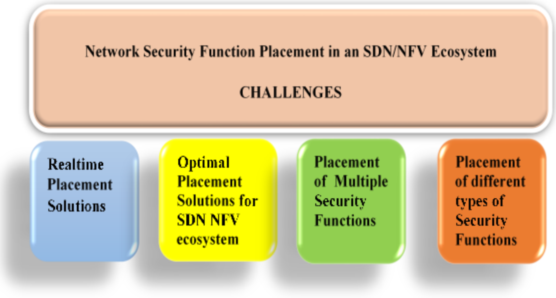

Network Security Function Placement in an SDN/NFV Ecosystem
CHALLENGES
Realtime Placement Solutions
Optimal Placement Solutions for SDN NFV ecosystem
Placement of Multiple Security Functions
Placement of different types of Security Functions

Fig.10. VSNF Placement Research Challenges

5. CONCLUSION AND FUTURE DIRECTIONS

The SDN-NFV ecosystem can deliver on-demand security services. Network security functions are virtualised and deployed as virtual security network functions (VSNFs) in commercial off-the-shelf (COTS) servers, thus reducing costs as well as enabling faster development and innovations. Inorder to deliver end-to-end network services in a virtual networking environment, traffic flow is processed using a service function chain (SFC), which is an ordered virtual network function (VNF) chain. Consequently, a challenging problem for an SFC is to determine where to deploy VNFs and how to route traffic between VNFs of an SFC on a substrate network.

This paper provides a critical survey on the placement of VSNFs in an SDN-NFV ecosystem and identifies open problems in this avid area of study. Description of NFV and SDN technologies, their relationship between them and a review of the most common VSNFs are given. A comparison and examination of studies on the optimal placement of VSNFs is also undertaken. Finally, several open research challenges in this area of study are identified and suggestions for potential future directions to be considered by researchers are made. There exist many open research issues in this fervent study. Study area include deployment of different types of VSNF ing the deployment of different types of security function, placement of multiple security functions, optimal placement of security functions, the interactions and dependencies among the security functions and real-time placement solutions in an SDN-NFV ecosystem are some of these areas.

REFERENCES

[1] Ericsson, “Ericsson Mobility Report”, (2020). [Online]. Available:www.ericsson.com/assets/local/mobilityreport/documents/2020.

[2] Bain And Company Estimates, “Choosing the right platform for the industrial IoT”, (2018). [Online]. Available:www.bain.com/insights/2018.

[3] International Data Corporation (IDC) – “Forecasts Worldwide Technology”; (2020). Available: https://www.idc.com.

[4] “Ponemon Institute Cyber Crime Study, 2017”. [Online]. Available:www.ponemon.org/library/2017cost-of-cyber-crime -study.

[5] J. Halpern, C. Pignataro, Service Function Chaining (SFC) Architecture; RFC 7665; IETF: Wilmington, DE, USA, 2015.

[6] K. Bensekki, A. El Fergougui; and E.A. Elbelrhiti (2016). "Software-defined networking (SDN): A survey". Security and Communication Networks. 9 (18): 5803–5833. doi:10.1002/sec.1737.

[7] A. F. Murillo, S. J. Rueda, L. V. Morales, and Á. A. Cardenas, “SDN and NFV Security: Challenges for Integrated Solutions, 2017”, Computer Communications and Networks, DOI 10.1007/978-3-319-64653-4_3

[8] D. B. Hoang, S. Farahmandian, “Security of SoftwareDefined Infrastructures with SDN, NFV, and Cloud Computing Technologies”, Comp. Comms and Net.,DOI 10.1007/978-3-319-64653-4_1

[9] http://www.etsi.org/technologiesclusters/technologies/nfv (2019).

[10] "Network Functions Virtualisation (NFV); Use NFV is present and SDN is future. Cases" (PDF). Accessed: July 2019.

[11] Network-Functions Virtualisation (NFV) Proofs of Concept; Framework, GS NFV-PER 002 v1.1.1 (2013-10).

[12] S. Lal, T. Taleb and A. Dutta, “NFV: Security Threats and Best Practices”, IEEE Communications Magazine, Vol 55, pp 211-216, May 2017.

[13] ONF, SDN architecture overview, available at https:// www.opennetworking.org/images/stories /downloads /sdn-resources/technical-reports/SDNarchitecture-overview-1.0.pdf.

[14] ETSI, GS NFV-EVE 005 (V1.1.1) - (12-2015), “Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework”, available at http://www.etsi.org/deliver/etsi_gs/NFV-EVE/001_099 /005/ 01.01.01_60 /gs_NFV-EVE005v010101p.pdf.

[15] H. Hu, G. Ahn, "Virtualizing and Utilizing Network Security Functions for Securing Software Defined Infrastructure", NSF Workshop on Software Defined Infrastructures and Software Defined Exchanges, Washington, D.C., USA, 70, (2016).

[16] Y. Jarraya, A. Shameli-Sendi, M. Poursandi, M. Cheriet, "Multistage OCDO: Scalable Security Provisioning Optimisation in SDN-Based Cloud", IEEE 8th International Conference on Cloud Computing, New York City, NY, USA 572–579, (2015).

[17] D. Krishnaswamy, R. Kothari, V. Gabale, "Latency and policy aware hierarchical partitioning for NFV systems",IEEE Conference on Network Function Virtualisation and Software Defined Network, San Francisco, CA, USA, 205 –211, (2016).

[18] G. Carl, G. Kesidis, R. R. Brooks, S. Rai, "Denial-of-services attack-detection techniques", IEEE Internet Computing, 10:82–89, (2006).

[19] R. Braga, E. Mota, A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow", IEEE 35th Conference on Local Computer Networks, Denver, CO, USA 408– 415, (2010).

[20] J.M. Ceron, C.B. Margi, L.Z. Granville, "MARS: "An SDN-based malware analysis solution", IEEE Symposium on Computers and Communication, Messina, Italy, 525–530, (2016).

[21] Internet: "What is an Intrusion Detection System?", http://techgenix.com/intrusion_detection_systems_ids_part_i__network_intrusions_attack_symptoms_ids_tasks_and_ids_architecture/ (accessed January 11, 2020).

[22] Z. Xiong, "An SDN-based IPS Development Framework in Cloud Networking Environment", (2014).

[23] Ballard, J.R., Rae, I., Akella, A. "Extensible and scalable network monitoring using opensafe", Internet Network. Management Workshop/Workshop on Research and Enterprise Networking, San Jose, CA, USA, (2008).

[24] N.L.M. Van Adrichem, C. Doerr, F.A. Kuipers, "OpenNetMon: Network monitoring in OpenFlow software-defined networks", IEEE Network Operations and Management Symposium, Krakow, Poland, 1–8, (2014).

[25] L. Zhang, G. Shou, Y. Hu, Guo, Z. "Deployment of Intrusion Prevention System based on Software Defined Networking", IEEE International Conference on Communication Technology, Guilin, China, 26–31, (2013).

[26] H. Hu, W. Han, G, Ahn, Z. Zhao, "FlowGuard: Building Robust Firewalls for SoftwareDefined Networks", Third workshop on Hot topics in software defined networking, Chicago, Illinois, USA, 97–102. (2014).

[27] M. Suh, S.H. Park, B. Lee, S. Yang, "Building firewall over the software-defined network controller", IEEE International Conference on Advanced Communication Technology, Pyeongchang, South Korea, 744–748, (2014).

[28] NFV/SDN combination framework for provisioning and managing virtual firewalls", IEEE Conference on Network Function Virtualisation and Software Defined Network, San Francisco, CA, USA, 107–114, (2016).

[29] J. Kwon, D. Seo, M. Kwon, H. Lee, A. Perrig, H. Kim, "An incrementally deployable antispoofing mechanism for software-defined networks", Computer Communications, 64:1–20, (2015).

[30] G. Yao, J. Bi, T. Feng, P. Xiao, D. Zhou, "Performing software defined route-based IP spoofing filtering with SEFA", 23th International Conference on Computer Communication and Networks, Shanghai, China, 1–8, (2014).

[31] T, Alharbi, D. Durando, F. Paksad, M. Portmann, "Securing ARP in Software Defined Networks", IEEE 41th Conference

on Local Computer Networks, Dubai, UAE, 523–526, (2016).

J.H. Cox, R.J. Clark, H,L. Owen, "Leveraging SDN for ARP security", IEEE SOUTHEASTCON, Norfolk VA, 1–8, (2016).

[32] S.T. Ali, V. Sivaraman, A. Radford, S. Jha, "A Survey of Securing Networks Using Software Defined Networking", IEEE Transctions on Reliability, 64:1086–1097, (2015).

[33] S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu, M. Tyson, A. Texas, C. Station, M. Park, "Fresco: Modular composable security services for software-defined networks", 20th Annual Network & Distributed System Security Symposium, San Diego, CA, USA, 1-16, (2013).

[34] W. Han, Z. Zhao, A. Doupé, G.-J Ahn, "HoneyMix: Toward SDN-based Intelligent Honeynet", ACM International Workshop on Security in Software Defined Networks & Network Function Virtualisation, New Orleans, Louisiana, USA, 1–6, (2016).

[35] M. Bouet, J. Leguay, V. Conan, "Cost-based placement of virtualised deep packet inspection functions in SDN", IEEE Military Communications Conference, San Diego, California, USA, 992– 997, (2013).

[36] Internet: "The Role of DPI in an SDN World", http://niwiit.org/wp-content/uploads/lteasia13 /6841Heavy_ Reading -Qosmos_DPI-SDN-WP_Dec-2012.pdf.

[37] M. Bouet, J. Leguay, T. Combe, V. Conan, "Cost-based placement of vDPI functions in NFV infrastructures", International Journal of Network Management, 25:490–506, (2015).

[38] W. Ma, B. Jonathan, Z. Pan, D. Pan, N. Pissinou, "SDNBased Traffic Aware Placement of NFV Middleboxes", IEEE Transactions on Network and Service Management, 14:528–542, (2017).

[39] X. Li, C. Qian, "The virtual network function placement problem", IEEE International Conference on Computer Communications Workshops, Hong Kong, China, 69–70, (2015).

[40] X. Li, C. Qian, "A survey of network function placement", 13th IEEE Annual Consumer Communications & Networking Conference, Las Vegas, NV, USA, 948–953, (2016).

[41] M.F. Bari, S.R. Chowdhury, R. Ahmed, R. Boutaba, "On orchestrating virtual network functions", 11th International Conference on Network and Service Management, Barcelona, Spain, 50–56, (2015).

[42] B. Addis, D. Belabed, M. Bouet, S. Secci, "Virtual network functions placement and routing optimisation", IEEE 4th International Conference on Cloud Networking, Niagara Falls, Canada, 171–177, (2015).

[43] M.C. Luiselli, L.B. Bays, L.S. Buriol, M.P. Barcellos, L.P. Gaspary, "Piecing together the NFV provisioning puzzle: Efficient placement and chaining of virtual network functions", IFIP/IEEE International Symposium on Integrated Network Management, Ottawa, ON, Canada, 98–106, (2015).

[44] D.B. Rawat, S.R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey", IEEE Communications Surveys & Tutorials, 19:325–346, (2017).

[45] C,M, Machuca, "Expenditures study for network operators", International Conference on Transparent Optical Networks, Nottingham, UK, 18–22, (2006).

[46] S. Demirci, M. Demirci, S. Sagiroglu, "Optimal Placement of Virtual Security Functions to Minimise Energy Consumption", International Symposium on Networks, Computers, and Communications, Rome, Italy, 1–6, (2018).

[47] A. Shameli-Sendi, Y. Jarraya, M. Fekih-Ahmed, M. Poursandi, C. Talhi, M. Cheriet, "Optimal placement of sequentially ordered virtual security appliances in the cloud", IFIP/IEEE International Symposium on Integrated Network Management, Ottawa, ON, Canada, 818–821, (2015).

[48] R. Doriguzzi-Corin, S. Scott-Hayward, D. Siracusa, M. Savi, E. Salvadori, "Dynamic and Application-Aware Provisioning of Chained Virtual Security Network Functions", https://arxiv.org/pdf/ 1901.01704.pdf, (2019).

[49] P. Murukan, P., D. Jamaluddine,"A Cost-based Placement Algorithm for Multiple Virtual Security Appliances in Cloud using SDN: MO-UFLP (MultiOrdered Uncapacitated Facility Location Problem)", http://arxiv.org/abs/1602.08155, 1–14, (2016).

[50] F. Bari et al., “Orchestrating Virtualised Network Functions,” IEEE TNSM, vol. 13, no. 4, pp. 725–739, 2016.

[51] S. Mehraghdam et al., “Specifying and Placing Chains of Virtual Network Functions,” in Proc. of IEEE CloudNet, 2014.

[52] P. Visarreta et al., “QoS-driven Function Placement Reducing Expenditures in NFV Deployments,” in Proc. of ICC, 2017.

[53] M. M. Tajiki et al., “Joint Energy Efficient and QoSaware Path Allocation and VNF Placement for Service Function Chaining,” IEEE TNSM, 2018.

[54] Y.Parket al., “Dynamic Defense Provision via Network Functions Virtualisation,” in Proc. of ACM SDN-NFV Sec., 2017.

[55] T. V. Phan et al., “Optimizing resource allocation for elastic security VNFs in the SDNFV-enabled cloud computing,” in Proc. of ICOIN, 2017.

[56] S. Demirci et al., “Optimal Placement of Virtual Security Functions to Minimise Energy Consumption,” in Proc. of the IEEE ISNCC, 2018.

[57] Q. Xu et al., “Low Latency Security Function Chain Embedding Across Multiple Domains,” IEEE Access, 2018.

[58] A. Shameli Sendiet al., “Efficient Provisioning of Security Service Function Chaining Using Network Security Defense Patterns,” IEEE Transactions on Services Computing, 2017.

[59] Y. Liu et al., “A Dynamic Composition Mechanism of Security Service Chaining Oriented to SDN/NFVEnabled Networks,” IEEE Access, vol. 6, pp. 53918– 53929, 2018.

[60] D. Huang et al., Software-Defined Networking and Security: From Theory to Practice. CRC Press, 2018.

[61] N. McKeown et al., "OpenFlow: enabling innovation in campus networks," ACM SIGCOMM Computer Communication Review, vol. 32, no. 2, pp. 69–74, April 2008.

[62] S. Gianvecchio et al., "Humans and Bots in Internet Chat: Measurement, Analysis, and Automated Classification," IEEE/ACM Trans. Netw., vol. 19, no. 5, pp. 1557–1571, Oct. 2011.

[63] J. Yan et al., "A Systematic Classification of Cheating in Online Games," in Proc. of ACM SIGCOMM NetGames, 2005.

[64] R. Doriguzzi-Corin, S. Scott-Hayward, D. Siracusa, M. Savi, E. Salvadori, "Dynamic and Application-Aware Provisioning of Chained Virtual Security Network Functions", IEEE Transactions on Network and Service Management 2019.

[65] Shameli Sendi, A., Jarraya, Y., Poursandi, M., Cheriet, M. "Efficient Provisioning of Security Service Function Chaining Using Network Security Defense Patterns", IEEE Transactions on Services Computing, 1–1, (2016).

[66] Wang, X., Wu, C., Le, F., Liu, A., Li, Z., Lau, F. "Online VNF scaling in datacenters", IEEE 9th International Conference on Cloud Computing, San Francisco, CA, USA, 140–147, (2017).

[67] Alleg, A., Kouah, R., Moussaoui, S., Ahmed, T. "Virtual Network Functions Placement and Chaining for real-time applications," IEEE 22th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, Lund, Sweden, 16, (2017).

[68] Cho, D., Taheri, J., Zomaya, A.Y., Bouvry, P. "RealTime Virtual Network Function (VNF) Migration toward Low Network Latency in Cloud Environments", IEEE 10th International Conference on Cloud Computing, Honolulu, CA, USA, 798–801, (2017).

[69] Kim, S., Han, Y., Park, S. "An energy-Aware service function chaining & reconfiguration algorithm in NFV", IEEE International Workshop on Foundations and Applications of Self Systems, Augsburg, Germany, 54– 59, (2016).

[70] Cohen, R., Eytan, L. and Naor, J. (2015). "Near optimal placement of virtual network functions", IEEE Conference on Computer Communications (INFOCOM).

[71] M. Luiselli, L. Bays and L. Buriol, "Piecing together the NFV provisioning puzzle: Efficient placement and chaining of virtual network functions", IFIP/IEEE International Symposium on Integrated Network Management (IM), 2015.

[72] H. Moens and F. Turck, "VNF-P: A model for efficient placement of virtualised network functions.", 10th International Conference on Network and Service Management (CNSM) and Workshop, 2014.

[73] A. Hirwe and K. Kataoka, "LightChain: A lightweight optimisation of VNF placement for service chaining in NFV", IEEE NetSoft Conference and Workshops (NetSoft), 2016.

[74] M. Ghaznavi, A. Khan and N. Shahriar, "Elastic virtual network function placement.", IEEE 4th International Conference on Cloud Networking (CloudNet), 2015.

[75] J. Cao, Y. Zhang and W. An, "VNF Placement in Hybrid NFV Environment: Modeling and Genetic Algorithms", IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS), 2016.

BIOGRAPHY

Godwin T.S. Chapanduka is currently studying for a Phd in Electrical Engineering at Tshwane University of Technology (TUT), Pretoria, South Africa. His research interests include 5G and Beyond Networks, network security, Internet of Things, design and performance evaluation of the next generation of wireless network architecture, high-speed networking, SDN, and NFV.