An Overview of the Security Landscape of Virtual Mobile Networks

IJAZ AHMAD1, JARNO PINOLA1, ILKKA HARJULA1, JANI SUOMALAINEN1, ERKKI HARJULA2, JYRKI HUUSKO1, TANESH KUMAR2

1VTT Technical Research Center of Finland, Espoo, Finland (e-mail: firstname.lastname@vtt.fi)
2Centre for Wireless Communication, University of Oulu, Finland (e-mail: firstname.lastname@oulu.fi)

Corresponding author: Ijaz Ahmad (e-mail: ijaz.ahmad@vtt.fi).

This research work was supported by Academy of Finland, under the projects: DigiHealth and 6G Flagship Projects (grants 326291, 318927).

ABSTRACT 5G enables the use of different types of services over the same physical infrastructure through the concepts and technologies of virtualization, softwarization, network slicing and cloud computing. Mobile Virtual Network Operators (MVNOs), using these concepts, provide an opportunity to share the same physical infrastructure among multiple operators. Each MVNO can have its own distinct operating and support systems. However, the technologies used to enable such an environment have their own explicit security challenges and solutions. The integrated environment built upon these novel concepts and technologies, thus, will have complex security implications and requirements to be satisfied. In this vain, this article provides an overview of the security challenges and potential solutions for MVNOs.

INDEX TERMS Security; Virtual Mobile Networks (VMNs) Security; VMNs; NFV Security; Virtual Networks; 5G.

I. INTRODUCTION

With new technological developments in 5G, such as virtualization and network slicing, Virtual Mobile Networks (VMNs) provide an opportunity to share the same physical infrastructure among multiple operators. Each VMN operator, called Mobile Virtual Network Operator (MVNO), can have its own operating and support systems, service offering and user base. Being virtual in nature, the network can be easily scaled up and down as the need arises [1]. Due to the many benefits, since 2012 the European Telecommunications Standards Institute (ETSI) hosted the industry specification group for Network Function Virtualization (NFV) to apply the mainstream virtualization techniques to standardized network elements. Hence, access, backhaul and core networks, or parts of them, can be virtualized.

NFV makes it possible for telecom operators to use commercial off-the-shelf (COTS) general purpose network equipment to satisfy the needs of various types of applications with much less costs compared to the use of dedicated hardware [2]. This capability of NFV has brought the flexibility and agility of clouds to communication networks in terms of facilitating different services on network equipment [3]. Furthermore, NFV facilitates dynamic service creation and management in different network perimeters [4].

With the flexibility provided by programmable networks, mainly Software Defined Networking (SDN), Virtual Network Functions (VNFs) can be placed in different network perimeters [5], and thus, NFV and SDN have become highly complementary technologies. A VNF can be any function performed by a network node, implemented solely in software, to avail the benefits of cost-effective customization and changes. Hence, networking and service functions can be upgraded, chained, deployed, re-deployed or removed instantaneously. However, such elasticity must not cause security vulnerabilities. The technologies used to enable VMNs, have their own security challenges and solutions [6]. Therefore, the technologically integrated environment will have much complex security threat landscape, while security solutions are distinct, resulting a complicated operating environment. Although a lot of work has been done on security of each distinct technology, such as SDN, NFV and cloud platforms, very little attention has been paid to the security of the integrated VMN environment.

In this article, we discuss the possible security challenges and the potential solutions for integrated VMN environment. Since, the main enabler as whole for VMNs is 5G, we first provide a brief overview of the basics of 5G security, and
then move forward to the security of VMNs. This article is organized as follows: In section II, the background with security in 5G, as the main enabler of VMNs, is discussed on a high level. Section III discusses the security challenges and possible security solutions of VMNs along with relevant enabling technologies. Section IV discusses the security management VMNs along with trust, privacy and standardization efforts. Important future research directions are discussed in Section V, and the article is concluded in Section VI.

II. BACKGROUND

Virtualization has received high attention with the 5G research momentum [7]. Technologies that were not there before, such as NFV, SDN, and the concepts of cloud computing, has increased the potential and ease of deployment of virtual networks [5], [8]. Thus, the virtualization of different parts of the network from core [9] to Radio Access Network (RAN) [10], [11] has taken off, leading to new concepts such as light and mobile evolved packet core system [12] and Open RAN [13]. This has resulted in the possibility of new strain of communication networks, that are fully virtualized and even portable. Since the underlying infrastructure of such virtualized networks is based on the concepts and technologies of 5G, the security concerns, challenges, and solutions will be relevant in the case of VMNs. Therefore, below we provide a brief overview of the 5G security.

A. BRIEF OVERVIEW OF 5G SECURITY

5G security differs from the previous generations, i.e., from 1G to 4G, mainly due to the emergence of new services and technologies used in the communication infrastructure [14]. New services, such as vehicular communication or Unmanned Aerial Vehicles (UAVs), teledmedicine, smart homes, etc., will require different security approaches. Similarly, new software technologies, such as virtualization and multi-tenancy, in which different and possibly conflicting services share the same mobile network infrastructure, have emerged mainly after the previous generations [6], [14]. Therefore, the Next Generation Mobile Networks (NGMN) consortium suggests 5G to provide more than hop-by-hop or radio bearer security, which was common in 4G and prior generations of cellular networks [14]. Due to the inclusion of diverse services and technologies, the security threat landscape will be much more different and complex. The most important challenges, that are more threatening in the case of 5G, compared to previous generations [6], [14], are summarized in Table 1.

1) Brief Overview of 5G Security Challenges

Main reasons for the security challenges in 5G, as outlined in [14] and tabulate in Table 1, are as follows:

- **Flash network traffic:** Due to the exponential growth of connected devices, mainly Internet of Things (IoT).
- **Security of radio interfaces:** Radio interface encryption keys generated in home network and sent to visited network over insecure links.
- **User plane integrity:** Lack of cryptographic integrity protection to for the user data plane, specifically for low capability devices, where the traffic terminates beyond mobile networks.
- **Security assurance:** The lack of mandated security assurance in multi-operator environments.
- **Roaming security:** The lack of securely exchanging and maintaining subscriber level information including security policies during roaming.
- **Denial of Service (DoS) Attack:** Preventing and disturbing the availability of resources to end users and services.

| Security Challenge | Description |
|--------------------|-------------|
| Flash network traffic | Sudden arrival of large number of packets may cause service breaks and disturbances. |
| Security of interfaces | The loss or vulnerabilities of encryption keys weakens security of radio interfaces. |
| User plane integrity | Loss of integrity of user data specifically beyond the domain of mobile network. |
| Lack of assurance | Security lapses occurring due to lack of security assurance in multi-operator environments. |
| Roaming security | Possible conflicts among multiple operators, regarding subscriber security during roaming. |
| Denial of Service (DoS) Attack | Preventing and disturbing the availability of resources to end users and services. |

2) Brief Overview of Solution to the Challenges

The 5G security architecture defined by the third generation partnership project (3GPP) has the following main domains:

- **Network access security (I):** The set of security features that enable a UE to securely authenticate and access network services. Access security includes security of 3GPP and non-3GPP access technologies, and delivery of security context from serving network to the UE.
- **Network domain security (II):** A set of security features that enable network nodes to securely exchange signaling and user plane data.
- **User domain security (III):** Security features that enable the secure user access to UE.
I. Ahmad et al.: Virtual Mobile Networks: An Overview of Security

Figure 1: Potential security challenges in 5G.

- **Application domain security (IV):** Security features that enable applications (user and provider domains) to securely exchange messages.
- **Service Based Architecture (SBA) domain security (V):** Security features for network element registration, discovery, and authorization, as well as security for service-based interfaces.
- **Visibility and configurability of security (VI):** Security features that inform users whether security features are in operation or not.

5G will use new technologies such as SDN, VNFs, cloud computing and its local form, Multi-access Edge Computing (MEC). Each of these technologies will also bring their own security concerns [16], [17]. Thus, the solutions will also be first based on each technology, and then based on the overall architecture of 5G. Within each technology, the principle of security by-design must be adopted. From the overall architecture point of view, the solutions could also be defined on the basis of the 5G security architecture defined by 3GPP. These solutions, according to the 3GPP security architecture, are mapped to security challenges in Table 2.

5G will integrate diverse types of devices, such as different IoT devices, and services in the form of verticals.

| Security Type | Description (solution for challenges outlined in Table 1) |
|---------------|----------------------------------------------------------|
| Network access security | For secure authentication and access to network services. (User plane integrity) |
| Network domain security | For secure exchange of signaling and user plane data among network nodes. (Security of interfaces) |
| User domain security | For secure user access to a user equipment (UE). (User plane integrity) |
| Application domain security | Security features that enable user and provider domain applications to securely exchange messages. (User plane integrity, security assurance, roaming security) |
| Service-based architecture domain security | Security features for network element registration, discovery, authorization, and service-based interfaces. |
| Visibility & configurability | Security features that inform users of security features operations. (DoS, security assurance) |

Table 2: Solutions according to the security architecture defined by 3GPP

Therefore, the security vision is based on three main principles, which are: i) Supreme built-in-security following the principle of security-by-design for new emerging systems and services, ii) Flexible security mechanisms leveraging the principles of NFV and SDN for deploying dynamic security functions, and iii) Automation-leveraging AI for minimal human intervention. Therefore, from the network perspective, the technologies used within 5G, such as NFV and SDN, must also be first secured from their inherent security limitations. In relation to VMNs, these technologies
play pivotal role and, therefore, their security has direct implications on security of the overall network as described below.

The motives and use cases for virtualizing the network operations are diverse. Different types of MVNOs have different quality and security requirements for the shared network and can also provide differentiated security for their clients. For instance:

- Commercial service operators provide regular end-users alternative means to subscribe network services. They both compete the network operators (with custom user interface, differentiated service experience, or pricing) and cooperate by purchasing the access network services. MVNO’s requirements for hosting Mobile Network Operators (MNOs) include provisioning of the agreed service level or share of the capacity.
- Private industrial networks – for instance, factories, companies and other organizations – can rely on shared RANs but manage itself core network services as well as company critical services and user databases. They require geographically limited coverage, and may, in some cases, also require differentiated services from the access network operator. Traditionally, industrial networks have been closed and isolated environments. The use of common infrastructure for industrial applications requires strong isolation between public and industrial domains.
- Public safety networks – used by first response teams, fire and rescue personnel, law enforcement authorities, or border guards etc. – may be built in cooperation with the commercial networks operators. The utilization of shared commercial access network infrastructure enables public safety authorities to achieve wide and high-quality network coverage with better cost-effectiveness, when compared to a dedicated infrastructure. Typically, sensitive mission-critical application services, as well as user authentication and authorization databases, are managed by the authorities. For the shared infrastructure, the authorities may define additional requirements related to availability assurance, e.g., redundancy, prioritization of authority traffic flows in the case of congestion, and support for isolated operations if a backhaul fails, e.g., due to disaster or cyber-attacks.

III. VMN SECURITY CHALLENGES AND SOLUTIONS

VMNs will leverage the concept of cloud computing besides NFV and SDN to efficiently place network functions, scale up resource for different functions when needed, and provide unified platforms for network management, resulting in Telecommunication network as a Service (TaaS). As shown in Fig. 2, a slice, e.g., Vehicle to Everything (V2X) experiment slice, can be generated by leveraging networking and virtualization techniques to offer diverse services on the same shared infrastructure. Therefore, the security of VMNs will be dependent on security of SDN, cloud platforms, and most importantly, virtualization technologies and NFV. The security of each of these in this context is described below.

A. SECURITY OF NETWORK VIRTUALIZATION TECHNIQUES

Due to the capability to deploy diverse sets of services on the same physical infrastructure, the concepts of virtualization have been applied to communication networks. Virtualization enables common commodity systems to run one or several different VNFs. The concept of NFV, to implement networking functions in software to be deployed on commodity network equipment, led to the rise of VNFs. NFV then became a vital technology for 5G and beyond 5G networks. Soon novel verticals will span multiple operator environments to provide novel services such as ehealth, smart homes, and vehicle-to-vehicle communications, etc.

SDN is one of the main enabling technologies of VMNs for its ability to provide abstractions of the physical network infrastructure. SDN separates the network control from the data forwarding elements, introduces network programmability and logically centralizes the network control to manage the whole network from a central vantage point. These attributes make the network robust, simplifies network management, and minimize operational expenses. However, these attributes also open doors to new security vulnerabilities and challenges. SDN highly facilitates NFV in terms of deployment of VNFs besides providing the support in the network infrastructure, and thus, SDN and NFV are highly complementary to each other. Since all these technologies are highly relevant and interdependent, in this subsection we discuss the security challenges and their possible solutions.

1) Security Challenges in NFV

The security challenges of NFV in VMNs revolve around hypervisors, VMs, and VNFs. The concept of virtualized threats recently emerged that refers to attacks against availability, integrity and confidentiality of software and hardware in VMN. In VMNs, the hypervisor is a central entity that is responsible for creating virtual instances on the hardware. Furthermore, security threats can arise from the software implementations, VNF configurations, security weaknesses in hypervisors and cloud platforms, as well as direct attacks on VNFs such as side-channel attacks, flooding attacks, and malware injection. Due to the dynamic nature of VNFs, trust management is another serious concern since VNFs will be capable to move between multiple networks, and cloud platforms maintained by different owners and operators. The targets of such attacks include user traffic, VNF code and policy input, and state of VNFs. Such attacks can be materialized by exploiting inherent limitations in operating environments including its software and hardware. Furthermore, serious security challenges can arise from interfaces, mainly when standardized interfaces are not defined.
2) Security Solutions for NFV

Similar to centralized or core network elements, the hypervisor must be protected through proper authentication, authorization and accountability mechanisms. Similarly, security mechanisms for ensuring availability must be in place since unavailability of the hypervisor is crucial for all services. The VNF package security validation check is highly important to avoid introducing security vulnerabilities in the whole system. Therefore, there are several proposals for confidentiality check through proper authentication and integrity verification for VNF packages onboarding into NFV systems. There are also other proposals for ensuring security of systems from malicious VNFs. For example, authors in [28] propose and demonstrate a verification system for security attributes of different VNFs to protect NFV infrastructure (NFVI) using standard TOSCA [29] data models. ETSI has come moved forward to standardize interfaces and bring solutions for security management of VNFs and VMNs, as described in the following section.

3) Security Challenges in Network Slicing

Network slicing facilitates resource sharing in 5G networks, but simultaneously creates new challenges for security and privacy. Slicing is a new concept for mobile networks and, hence, prone to design and implementation errors similarly to SBA. During slice life-cycle management processes, the slice template, slice configuration Application Programming Interface (API) and user data handling are all possible targets for attacks. During slice run-time, the risks include DoS and performance attacks, as well as data exposure and privacy breaks. The possible attack points include the user devices, service interfaces, sub-slices, slice manager, network functions and network resources involved in network slicing. Possible inter-slice communication scenarios also introduce additional attack points to the network [30]. In addition, the new network functions involved in slice management, slice isolation, security differentiation between slices and interworking between the Evolved Packet Core (EPC) and 5G Core Network (5GC) during slicing are all new areas with potential security threats in mobile networks [31].

4) Security Solutions for Network Slicing

In order to provide consistent security for all 5G network slices in an efficient and scalable way, special attention should be put to the methods and techniques guaranteeing end-to-end slice security, slice isolation and slice resource management and orchestration. In addition, new trust models for different slicing scenarios are needed also at the technical level to facilitate resource sharing between actors and networks participating to the slices [30]. Moreover, strong isolation mechanisms will be required to minimize the effects of malicious slice on another one, and on the hypervisor [15]. Furthermore, active monitoring the network traffic, recognizing suspicious and malicious activities early on, and stopping in-bound traffic leveraging the concepts of SDN can improve security of different slices in a network. However, SDN has its own security challenges that must be
addressed, as discussed below.

5) Security Challenges in SDN

The separation of the data and control planes, centralized control and network programmability with programmable APIs on network equipment opens SDN to security challenges [32]. For example, the communication channels between isolated planes can be used to masquerade one plane to launch attack against the other. Moreover, the centralized controllers are favorable targets for DoS and resource exhaustion attacks. Fingerprinting the controllers, for example through time stamps of live packets in the network [33], or round-trip time [34] have been demonstrated. Thus, directing attacks towards the control points of the network has been rendered simple in SDN. Furthermore, SDN enables applications to program or change the behavior of the network. This gives rise to the possibility for malicious programs to stealthily manipulate the network resources, divert traffic to bots or hackers, or sniff on users’ traffic. In VMNs, the network is more software-based, thus, malicious software capable to manipulate the network will be threatening on a higher level due to the fact that finding the malicious software can be further challenging.

6) Security Solutions for SDN

The protection against attacks on SDN begins from overcoming the weaknesses of the architecture of traditional SDNs. For example, maintaining the control of the network in a logically centralized, but physically distributed manner can overcome the challenges of resource exhaustion attacks, as well as ensuring availability of network control points for the data plane [35]. Such resilience can be achieved through devolving the controller functions (e.g., local decision-making) [36], implementing hierarchical controllers [37], increasing resources and resource capabilities, and using intelligent security systems equipped with Machine Learning (ML) for proactive measures to be in place before attacks enter the weak points in a network [32].

SDN can be also used to improve the security of virtual networks [38]. Virtual Machine (VM) migration techniques using SDN can help to move resources to secure perimeters. For instance, live VM migration if the network is under a DoS attack can efficiently help in scalability through monitoring the load states (e.g. packet counter values from flow tables) in the SDN forwarding plane. Live VM migration in legacy networks has been difficult for two reasons. The first reason is network state unpredictability, and the second reason is that VM migration is limited to the Local Area Network (LAN) since Internet Protocol (IP) does not support VM mobility without session breakups. SDN solves these challenges by having the capability to program live network from a centralized control platform through programmable APIs in forwarding elements, and being independent from the layered IP stacks. Therefore, SDN can improve the security of VMNs through increased resilience [32].

B. SECURITY OF CLOUD PLATFORMS

Cloud computing [39] has become a central part of mobile networks for a number of benefits ranging from RAN to core networks [40]. Cloud computing concepts have been extended to meet latency requirements through edge computing [41], [42], MEC [43], and fog computing [44]. Virtualization of the cloud platforms for enabling novel services have many benefits of costs and efficiency. However, there are inherent security challenges in cloud platforms that are highly important when it comes to virtual systems on cloud platforms. For example, MEC suffers from latency during authentication, and the existing authorization, accounting and access control are not suitable for MEC, leaving space to threats, as discussed in [45]. Therefore, novel techniques for security [45] and privacy [46] in MEC platforms must be adopted, and novel lightweight techniques need to be designed for fog platforms when these technologies are used in VMNs.

The two main interjunction points of cloud and virtualization for wireless networks are cloud RAN (C-RAN) [47] and cloud-based core networks [4]. A survey on C-RAN security in [48] outlines the main challenges and potential solutions. The existing challenges include the lack of universal C-RAN security framework, secure sensing techniques, trust and privacy, and the infancy of physical layer security. The C-RAN service plane architecture is a cloud platform, which directly interacts with the users or service providers. The cloud provider should provide trust and privacy protection, and should ensure the confidentiality and integrity of the data by outsourcing security. Furthermore, C-RAN pools Baseband units from multiple base stations into a centralized pool for statistical multiplexing gain [47]. Such centralization would invite DoS and other resource exhaustion attacks. On the core network side, most of the security challenges are related to signaling storms, DoS attacks, and the security dependability on SDN and NFV [49]. In the following, we discuss the security challenges in cloud platforms from the core network to the edge of the network.

1) Security Challenges in Virtual EPC and 5GC

Unlike the previous mobile network generations that were initially designed for circuit-switched voice services, the core network architectures in 4G and 5G systems are designed for handling common IP-based packet data traffic. This means that, compared to the previous mobile network generations that were mostly based on proprietary hardware and protocols only used in mobile networks, there are a lot more readily available tools and resources for actors with malicious intent to attack 4G and 5G networks with minimal effort and knowledge of their target system. With native support for IP-based data and increased data rates in 4G and 5G, mobile networks have also managed to attract a more heterogeneous user and service base. Combined with the heterogeneity in the access network architecture, related to the large variety of supported Radio Access Technologies (RATs) and UE types, the complexity of the core network
components and interfaces related to 4G and 5G network access has increased as well. Consequently, due to their heterogeneous and IP-based architectures, 4G and 5G core networks have inherited all the security problems of the supported access technologies, and most of the IP-specific security vulnerabilities from computer networks. Flat IP-based architecture in EPC means more attack surface to the network infrastructure with common tools and more potential single points for failure, e.g., in the form of Mobility Management Entities (MME) managing multiple base stations in a given area [50]. The flat architecture also makes attacks against network availability possible with control plane flooding against the Home Subscriber Server (HSS), Serving Gateway (SGW) or other control plane network functions during UE attach/re-attach procedures [51]. Heterogeneous access networks are difficult to manage securely in high mobility scenarios [50]. In addition to vertical handovers, security in heterogeneous networks is difficult to guarantee during roaming [52].

5GC is even more complex and heterogeneous than EPC when it comes to the user devices, access networks, services and underlying enabling technologies. This will make some of the above-mentioned risks related to access and handover security more difficult to handle in 5GC, e.g., during frequent small cell handovers [53]. With the introduction of new more business-oriented use cases and services, new 5G-specific threats also include IoT, Device to Device (D2D) and V2X security [31]. In addition, there is a fundamental clash between zero latency and high-security requirements in 5GC [53], [52].

2) Security Solutions for Virtual EPC and 5GC
The potential solutions to identified threats include enhanced authentication schemes for initial access and handover procedures. In addition, enhancements to protocol security, key management, fast access and mutual authentication have been proposed in the literature [50]. Added to the enhanced authentication methods for 5GC [31], the potential solutions proposed in the literature include a variety of security- and latency-aware protocols that would able to balance the contradicting requirements between security and performance for different types of services [53]. In addition to the countermeasures to better secure the communications between 5GC network functions, additional end-to-end application level security enhancements would also be needed, e.g., in roaming scenarios [54].

The challenges of complexity due to overwhelming number of end-user devices, heterogeneity of access technologies and increase in traffic can be effectively solved by a combination of technologies such as SDN and the use of ML. SDN simplifies the networking by decoupling the complicated control systems from the data plane and render the data plane for simply forwarding packets on the directions of the control plane. This also helps solving the challenges arising from heterogeneity in access networks. Traffic redirection through sparsely used data plane through flow table updates, and monitoring the packet counters in the flow tables not only simplifies monitoring but also facilitates stopping malicious traffic from entering the core networks. ML-based techniques [55] coupled with SDN [56] can help deploy predictive protection techniques.

3) Security Challenges in Virtualized Edge
The virtualization at the edge networks is vital for ensuring the flexible, elastic and reliable services, and offers key features such as platform independence, resource abstraction, and isolation [57] [58]. However, the virtual infrastructure responsible for the deployment and allocation of virtual resources at the edge are prone to various security threats such as VM manipulation threats, i.e. by extraction and manipulation of sensitive information and misuse of various resources. Other well-known attacks to the virtual edge environment include: DoS attacks (a malware VM tries to exhaust the resources), VM escape (host vulnerabilities), and Privacy leakage (sensitive information can be fetched by malicious VM with unprotected APs) among others. Furthermore, the migration of VMs/services from one edge node to another node also provide adversaries to launch various attacks, e.g. man-in-the-middle attacks [59].

Recently, lightweight virtualization approaches, such as container virtualization, have gained immense popularity for enabling edge computing on resource-constrained local devices and IoT nodes. Since containers share a common OS kernel among themselves, unlike VMs, where each have separate kernel, the security requirements and challenges of containers will differ from conventional VMs. For example, security issues may arise in the context of container isolation, host hardening, image distribution and container control levels [60]. The authors in [61] discussed the container security challenges using four different cases, i) Protecting a container from applications inside IT (image vulnerabilities, image configuration defects, embedded malware), ii) inter-container protection (untrusted images, insecure container runtime), iii) protecting host from containers (Host OS attack surface, host file-systems tampering), and iv) protecting containers from the host.

4) Security Solutions for Virtualized Edge
To address the potential security attacks at the virtualized edge, various security solutions have been highlighted in the literature, e.g. isolation policies, hypervisor hardening, and separation of VM roles [59]. Furthermore, VM introspection (VMI) based approaches can be used as a potential solutions for virtualization threats at the edge networks [62]. To counter the container security attacks, both software and hardware protection mechanisms are needed [60], [61]. Software-based mechanisms are based on either Linux Security Features (LSFs) or Linux Security Modules (LSMs). These Linux kernel features include the solutions using the namespaces, Control Groups (cgroups),Capabilities Dropping and Computation Mode (Seccomp) [61], [63]. Hardware-based protection can be
performed using two approaches, i.e. Virtual Trusted Platform Modules (vTPMs) and Intel SGX. Distributed Ledger Technologies (DLT)/Blockchain can provide trusted security monitoring and management functionalities during the execution of various process/ phases at virtualized Edge networks, e.g., prediction and detection of potential anomalies at the edge [64].

C. SECURITY OF VIRTUALIZED RADIO ACCESS NETWORKS

Instead of the monolithic approach taken in the past generations of mobile networks, where all base station functionality is integrated into proprietary hardware at the cell site, the separation of the radio front-end and the baseband processing units in 4G has made it possible to split the base station functionality into several inter-connected network components. Taking advantage of this functional split virtualization has been extended to RAN, and new concepts related to virtual RAN have been emerging. For example, C-RAN pools baseband units from multiple base stations into a centralized pool for statistical multiplexing gain [47]. Virtualization would allow mobile network operators to share radio resources [65], even towards pooling virtual base stations, as presented in [66].

In the original C-RAN concept, the base station functionality is divided into two RAN elements, i.e., the Baseband Unit (BBU) and the Remote Radio Head (RRH). All functionality related to baseband processing as well as to the user and control plane protocols on the Physical Layer (PHY) and above is provided by the BBU. The RRH handles only the radio functionalities. As a more recent advance towards the wide spread adoption of virtual RANs, the 3GPP specifications for 5G also support the virtualization of the base stations with the Next Generation RAN (NG-RAN) architecture [67]. In NG-RAN, the base station functionality can be divided up into three distinct RAN elements, i.e., the Central Unit (CU), Distributed Unit (DU) and Radio Unit (RU). The functionality can be divided between them in different ways for added flexibility during deployment. In the Higher Layer Split option 2, the CU contains the Radio Resource Control (RRC), Packet Data Convergence Protocol (PDCP) and Service Data Application Protocol (SDAP) functionalities, whereas the DU contains the Radio Link Control (RLC), Medium Access Control (MAC) and PHY functionalities. The RU contains a combination of low PHY and radio functionalities in the Lower Layer Split (LLS) option 7 or only the radio functionalities in LLS option 8, which corresponds to the traditional C-RAN architecture [68].

Building on top of the NG-RAN architecture, open RAN aims to extend the virtual RAN concept with open standardized interfaces and open source software running on top of generic multi-purpose hardware platforms. In other words, open RAN aims to overcome the limitations caused by proprietary hardware, software and interfaces which all are seen to hinder the deployment potential of the virtualized RANs. As a result, mobile networks would benefit from the softwarization trend end-to-end as the ecosystem would open up for new agile players to increase supply chain versatility and security as well as accelerate innovation in the RAN. Industry associations and work groups, such as O-RAN Alliance, Telecom Infra Project’s OpenRAN and Open Network Foundation’s Software Defined RAN (SD-RAN), are the current forerunners investigating, implementing and validating open RAN technologies and preparing the specifications required for their interoperability. Especially the MNOs are interested in the technology as it would allow them more flexibility when planning architectures and choosing vendors for tailored network deployments which are built around use cases instead of a product portfolio of an individual vendor.

1) Security Challenges in Virtual RAN

The main differentiator of NG-RAN in 5G deployments from the previous generations is that the separation between RAN and core is not fixed, but can vary depending on the use case to be implemented [69]. For example, in deployments requiring ultra-low latency, the traditional core network functionality is brought as close to RAN as possible, or can even be co-located with the RAN. In practice this means, that in some deployments, the gNB is the end point for the encryption and integrity protection, and potentially, therefore accessible for anyone accessing the gNB or its implementation.

The threats towards C-RAN physical, control and service planes are discussed in [48], and similar vulnerabilities can be found in NG-RAN. In the physical plane, eavesdropping attacks, jamming attacks, impersonation attacks, primary user emulation attacks, and threats related to the wireless channel itself have been distinguished as the main security threats. In the control plane, threats related to network and MAC layer protocol attacks, common control channel attacks, radio spectrum resource attacks, and Spectrum Sensing Data Falsification (SSDF) attacks have been identified. In the service plane, transport and application layer attacks, threats related to cloud computing, virtualization threats, and privacy threats have been identified as security threats.

2) Security Solutions for Virtual RAN

Regarding the NG-RAN, the security solutions can be identified separately for non-standalone, standalone and possible future deployments [69]. For non-standalone deployment, the gNB is connected not to the 5GC but to an eNB in a 4G RAN. The eNB plays the role of a master base station, and the gNB plays the role of a serving base station. The serving gNB forwards the uplink user plane data to the master eNB, and user data is then decrypted in the RAN before being forwarded to the core network. This means that user data is available unencrypted in the eNB when this deployment is used. In a standalone deployment, the security in 5G networks is standardized in a hop-by-hop fashion, where user data is decrypted and
encrypted in different functions within the network. User data is encrypted in transit, but processed in cleartext in many functions. The air interface is encrypted between the device and the gNB. From the gNB over the backhaul network to the core network, the 3GPP defined Nework Domain Security (NDS) / IP security framework is used to protect the integrity and confidentiality of the user plane and control plane between the device, the gNB and the core network. In the future, these RAN functions can be placed in different physical sites in an actual deployment of RAN, depending on the use case. This allows a breakout of RAN functions to support low-latency use cases as well as flexible implementations. Consequently, the split between RAN and core may be clear in standards, but it becomes unclear when viewed in actual deployments. The initiatives such as distributed RAN, split RAN, O-RAN etc. aim to further fragment and distribute the RAN functions. This has severe security implications, as the all the options make it unclear how the functions will be distributed or co-located in the long run. In order to tackle this problem, it is proposed that the standardization will drive for the implementation of the secure solutions and not leave it for the market-driven deployments to decide, as they often target for cost-effective solutions.

In more concrete level, the security solutions proposed for the C-RAN in [48] can be applied in some extent also to NG-RAN. In the physical plane, random phase shift keying sequences or pre-agreed beamforming pilots can be used to detect eaves-dropping attacks. For defending against primary user emulation attacks, several methods have been identified based on spectrum sensing and investigation of signal source location, physical layer authentication using cryptographic signatures or authentication tags. Similarly, [48] proposes several solutions for the threats in C-RAN control plane. For overcoming the MAC layer protocol attacks, several novel MAC protocols were identified. A user-centric security resource allocation scheme and a corresponding algorithm based on user self-condition was proposed as a resolution for the radio spectrum resource attacks. A user-centric security resource allocation scheme and a corresponding algorithm based on user self-condition was identified as a tool to resist SSDF attacks. The shared cloud platform should ensure the security of resource allocation in a virtualized RAN environment. For defending against virtualization attacks, virtual machine-based intrusion detection, virtual machine-based kernel protection, virtual machine-based access control, and virtual machine-based trusted computing can be used.

3) Security Challenges in Open RAN

O-RAN architecture [70] specifies the new interfaces and RAN functions needed to realize the vision of an open, intelligent, disaggregated and cloud-native RAN. The architecture is based on 3GPP specifications and extends the functionality defined by 3GPP. In that sense, the introduction of new open management interfaces and components in the O-RAN architecture increases the network threat and attack surface. In addition, as the key concepts behind O-RAN are openness, intelligence, disaggregation and cloudification, it inherits many of the generic security threats already related to virtual RANs, NFV, SDN, cloud platforms and utilization of Artificial Intelligence (AI). Moreover, the shift to multi-vendor environments can lead to interoperability challenges, unexpected functionality and, hence, additional security threats [71].

From the security perspective, a key component in the O-RAN architecture is the RAN Intelligent Controller (RIC). It is logical RAN management function divided into a non-real time RIC and near-real time RIC part residing in the Service Management and Orchestration (SMO) framework and RAN, respectively. The near-real time RIC also hosts applications called xApps, which can consist of one or more microservices used to collect information and control RAN resources through APIs [72]. Similarly to an SDN controller in wired networks, the RIC is able to reconfigure RAN functionality and resources on the fly in an operational network. Hence, it is a potential centralized target for DoS and resource exhaustion attacks. In addition, as xApps running in the near-real time RIC can be provided by the RIC platform vendor or any 3rd party, the validation of the utilised hardware platform as well as software components running on top of it must be performed each time a new xApp is deployed in the architecture [73].

ML has been introduced into the O-RAN architecture to better handle the large amount of parameters and options in the configuration of the 5G protocol stack. There are three types of control loops where ML algorithms can be used in the O-RAN architecture. Those control loops are designed to operate in real time, near-real time and non-real time basis. The training of the ML models usually happens at the non-real time RIC, but for some ML algorithms, it can also be part of the near-RT RIC. The ML model inference can happen at the non-real time RIC, near-real time RIC or O-RAN Distributed Unit (O-DU), which is an O-RAN architecture equivalent for a 3GPP NG-RAN DU [74]. Depending on time scale at which the ML algorithms operate, they can be used to control and optimize resources related to key RAN functionalities, such as channel estimation, Radio Resource Management (RRM), user plane and control plane management and admission or policy control. Consequently, proper training and updating of the utilised ML models as well as orchestration and coordination of the control loops operating at different time scales must be guaranteed for optimal network performance. The impact of misbehaving ML models to RAN performance is high and attacks against the ML algorithms are possible, e.g., through adversarial learning [75]. If the hostile actors are able to find out enough information on what ML algorithms are utilised in the network and how they control the network resources, they will also able to tamper with the network behaviour in various ways [76].
4) Security Solutions for Open RAN

Despite the security challenges traditionally associated with the key concepts enabling the O-RAN architecture, the proponents of the technology see that the opportunities and benefits in the open RAN approach outweigh the threats. First of all, the new open and standardised interfaces guarantee better visibility into the implementation of RAN security, which in turn facilitates the deployment of automated security monitoring and management tools. Even though extensive utilization of open source code in the utilized network equipment increases the exposure to public exploits and information on the vulnerabilities of the open source libraries can be hard to track comprehensively, the code is always available for continuous review by the open source community, which improves code security through faster identification and fixing of bugs. In addition, the disaggregated O-RAN architecture enhances network resilience with improved modularity and reduced interdependencies, enabling more granular security fixes and less risky software updates in live production networks [73]. Finally, new deployment strategies on top of commercial cloud infrastructures bring more possibilities for the MNOs to directly enforce cloud security and adopt industry best practices on RAN security though resource isolation and containerization of network functions.

As the role of a RIC in O-RAN architecture resembles that of a SDN controller in wired networks, the potential solutions to secure RIC operations are similar to those discussed earlier for SDN. For example, in order to avoid single point of failure during attacks against the logically centralized RAN control entity, the RIC functionality must be deployed in a physically distributed manner. In addition, development efforts towards the zero-trust model should be taken in order to guarantee the required validation checks for both the hardware and software components in the O-RAN architecture [73]. As the O-RAN concept also proposes extensive utilization of ML algorithms for automated RAN management, utilisation of more advanced Cognitive Radios (CRs) at the future O-RAN Radio Units (O-RUs) and UEs could enable better identification and restraining of hostile actors performing adversarial learning in the network [75].

D. SUMMARY OF THE SECURITY LANDSCAPE

The summary of the security landscape of VMNs is presented in Table 3, with respect to the security dimensions provided by the International Telecommunications Union-Telecommunications (ITU-T) recommendations X.805 (10/03) [77]. The security dimensions provide a set of security measures designed to address a particular aspect of the network security. The ITU-T recommendation identifies eight such sets that protect against all major security threats, as presented in the Table 3 under the heading of security dimensions. The security dimensions are briefly described, followed by the relevant impact of each dimension on different technologies used in VMNs. In Table 3, the relevant impacts of the dimensions are listed in three levels: Low (L), Medium (M) and High (H).

The security impact, in terms of challenges or threats, is high when there are few resources with respect to the security implication. For example, access control is more threatening in SDN than traditional networks, since unauthorized access to the SDN controller can lead to a hijack of the whole network. Yet, the control platforms are not capable to host heavy security mechanisms due to scalability challenges, as compared to centralized cloud platforms. Therefore, access control will have higher security implications in SDN than cloud platforms. The challenges are labeled as low (L), when there is no direct implication of the particular challenge on the technology. For example, the availability of a VNF can be a security challenge, yet VNFs can be created and moved around different resources at runtime without compromising on running flows. Therefore, it is considered as a low-level (L) challenge, even though every challenge must be considered as important eventually. In the table a comparative analysis, to derive the most important future research challenges, is the main objective.

IV. SECURITY MANAGEMENT IN VMNS

Due to the dynamic nature of NFVI and VNFs, the security management is much more complex in virtualized environments. The complexity is mainly attributed to consistent maintenance and management of VNF configurations and seamless transfer of state information from one VNF to another [78]. Similarly, the elasticity of NFV brings forth challenges in decomposing services for data and control planes, enforcing policies, and managing and controlling the entire network where the control signals must go only through the trusted functional blocks such as VNF managers, Virtualized Infrastructure Manager (VIM), and NFV orchestrator [79].

The ETSI specification release 3 security management and monitoring specification [80], provides important insights into security management and monitoring problems. It is mentioned that traditional security systems will not scale for NFV. This may result in inconsistent security policies, inefficient processes and increase overall complexity. Monitoring in NFV deployments is much more complicated due to the possibility of concealed interfaces by consolidated verticals, functional silos, and collapsed stacks like shared memory and virtual sockets. In large-scale deployments, probing for security monitoring is complicated by the myriad of VNFs, vendor-proprietary implementations, and non-3GPP standardized interfaces, as well as automation and live migrations.

ETSI proposes a high-level security management framework [80], as shown in Fig. 3, to meet these requirements. From the top, the NFV Security Manager (NSM) copes with complexity, separation of domains, and consistency challenges for security management of network services. The Security Element Managers (SEMs) manage different security functions. Tailored security functions are imple-
Table 3: Security domain implications and challenge level in each technology

| Security Domain          | Description                                                                 | SDN | cloud | VMs | VNF | vDedge | vEPC | vRAN | ORAN |
|--------------------------|------------------------------------------------------------------------------|-----|-------|-----|-----|--------|------|------|------|
| Access Control           | Protects against unauthorized use of uMEC resources.                         | H   | M     | M   | M   | M      | M    | L    | M    |
| Authentication           | Confirms identities of communicating entities; ensures its validity.         | H   | H     | H   | H   | M      | M    | H    | H    |
| Non-Reputation           | Provides means for associating actions with entities.                        | M   | M     | L   | L   | L      | L    | M    | M    |
| Data Confidentiality     | Protects data from unauthorized disclosures.                                | L   | H     | L   | M   | L      | M    | H    | M    |
| Communication security   | Ensures that information flows only between authorized end points.          | H   | L     | L   | L   | L      | M    | H    | H    |
| Data integrity           | Ensures correctness of data, protects from unauthorized changes.            | L   | H     | L   | L   | L      | L    | H    | H    |
| Availability             | Ensures authorized access to resources, information, and services.          | H   | M     | L   | L   | L      | M    | L    | L    |
| Privacy                  | Protects information to be derived from observations of uMEC                | L   | H     | L   | L   | L      | H    | L    | H    |

Figure 3: High-level NFV security management framework.
the case when third-party entities require access. The fourth security requirements is to enable ML based security analytics mechanism which can able to analyze and predict the security threats. The fifth category is data protection that corresponds to the various technical mechanisms regulation/policies to preserve the data privacy.

In addition to providing security functions, the implementations of MANO functions (both security and non-security related) must be secure and trustworthy. The implementations should be high quality software where the amount of potential vulnerabilities is minimized. Review practises are needed to minimize backdoors and security bugs. However, software quality and security assurance can be challenges for smaller MANO projects. Also, some implementations have higher complexity or lower maturity [82] and are, hence, more susceptible for security vulnerabilities. The reputation and trustworthiness of the implementations depends on the contributing parties, origin, and acceptance. For instance, the ONAP project is hosted by the Linux Foundation and OSM is hosted by ETSI. Both are respected and trusted organizations. The ONAP project has been adopted by a larger group of global service providers [82], which can be indicate more thorough reviews and testing and thus also maturity of security, but it has also been criticized [82] on deployment complexity.

B. TRUST ESTABLISHMENT

Trust and privacy will be primary concerns in shared environments. Trust in communication networks is about the expected outcomes of communicating with remote entities. Trusted networking encompasses questions of losing data or assets, network resources, and privacy during communication [86]. In VMNs, trust establishment can be rather tricky, mainly because of sophisticated tools over the network used to hide identities. One of the basic approaches to ensure trust over the network is strong identity binding techniques starting from the locator/ID split of communicating devices [87]. Raimo Kantola in [87] described the potential pitfalls and possible mitigation principles and techniques with great detail. In VMNs, the case is same with the only exception that tracking in virtualized environment will be more challenging than the physical counterpart. Blockchain/DLTs can also be effective in establishing distributed and decentralized trust while sharing and managing the data/ virtual resources among various entities at virtualized edge networks [88], [89].

C. SECURITY ASSURANCE

Security assurance methods increase the confidence that implementations and practises provide the needed security level—and thus, minimize the MVNO’s need to trust—to systems and cooperation domains. The methods for verifying trustworthiness of network elements and cooperation organizations includes a) regulation and liabilities (breaking of trust implies legal or financial consequences), b) procedural and c) technical controls to assure trustworthiness of different elements or organizations. Different assurance methods are needed in the different phases of the life cycle of the domains or elements of VMNs.

Network element and solution time assurance is based on security testing and verification. Network device vendors utilize their own and third-party test laboratories, which are accredited by GSMA [90], for assuring trustworthiness and secure implementation of network elements. 3GPP has developed generic and product specific security assurance specifications as well as a generic process [91] for creating test specifications and for evaluating security compliance of product development and product life-cycle management.

Organizational requirements for information security management systems, such as ISO 27000 standards [80], NIST 800-53 [92] audit criteria, and requirements from Cloud Security Alliance [93], provide guidelines to define and measure security of MNO and MVNO organizations. These criteria identify and specify technical and procedural requirements for information security that protects critical assets. Operational time trustworthiness assurance approaches include trusted computing based mechanisms [94] to attest and enforce that devices and virtualized functions [95], [96] are running the expected software configuration and providing the needed security level.

D. PRIVACY

Any information or the identifiable attributes from a person must be kept private. Generally, virtual networks support privacy, since techniques of virtualization, such as slicing, for instance, create boundaries between groups of users or links and channels that keep them separate. Furthermore, techniques that create virtual users to enhance privacy of individuals over communication networks exist, as presented in [97]. However, in VMNs, the control of user over his information is very low compared to traditional networks. Furthermore, also operators in VMNs have lower control over the infrastructure. This results in lack of trust of users and transparency in ownership of user-data. One of the main challenges in this regard is related to user privacy in third-party cloud systems. There are a number of approaches that can be used to secure privacy in virtual systems in clouds such as described in [46], [98], [99]. Yet, more research is required on increasing user trust in VMNs and providing transparent handling of user data and information.

VMNs are comprised of various actors and service providers which may use common/single virtual edge infrastructure which are dedicated to provide various services/resources. Each of these stakeholders have their own/different commercial interests and hence the priorities for the user’s privacy protection may vary for each of these stakeholders [98]. For example, the privacy protection provided by one virtual service provider may not be necessarily considered/agreed by the another one. In addition, such multi-operator/stakeholder computing environment will be much more complex in terms of identifying the responsible as well liable entities if any of probable data breaches
occurs [100]. Therefore, the shared virtualized edge platform might be a relatively easy target for the adversaries and thus it requires collaborative privacy and trust mechanisms that should be acceptable by all relevant parties.

MEC is already an important component for enhancing data privacy protection by processing the sensitive data closer to the user/device [101]. Virtual infrastructures at the edge networks are also prone to various privacy breaches. For example, keeping transparency is among one of the major challenges for the VM at the edge networks, i.e. a malware VM can obtain critical user information in the case if the APIs at the virtual edge are not secured properly [59]. With respect to local edge computing scenarios, it is also good to note that the existing security approaches developed for cloud-based architectures are not well suited for the purpose due to lower available capacity for execution and deployment [102]). Therefore, lightweight cryptography-based protocols, efficient, adaptive and lightweight end-to-end security mechanisms are needed throughout the service processes [103].

### E. STANDARDIZATION EFFORTS

There are a number of organizations and associations working on security related efforts in terms of standardization. The 3GPP working group SA WG3 [104] is monitoring security of 5G, including virtualization and NFV, etc. ETSI is more focused on NFV and virtualization. Thus, the ETSI Industry Specification Group for NFV [105] is working on security with a dedicated group called the Industry Specification Group NFV Security group (ISG NFV Sec). The latest, 2019-2020 NFV release 4, covers the verification, and certification procedures and mechanisms. The ISG NFV Sec group has published several group specification documents related to security, such as access token specification for API access [106], VNF Package Security Specification [107], Security Specification for MANO Components and Reference points [108], report on NFV Remote Attestation Architecture [109], and security management and monitoring specification in release 3 [110]. Furthermore, there are several other reports related to e.g. privacy and regulations, trust guidance, cataloguing security features in management software, certificate management and other regulatory aspects.

Recently, International Telecommunication Union (ITU) in Recommendation ITU-T X.1044 [111] discussed the different security threats and requirements for the network virtualization at various layers, i.e. the physical resource layer, the virtual resource layer and the logically isolated network partition (LINP) layer. Furthermore, security guidelines for the MVNOs are presented in ITU-T X Suppl. 30 [112] that examines various key security characteristics, the potential security threats and requirements, and presents a security framework for MVNOs.

### V. FUTURE RESEARCH DIRECTIONS

In future networks, i.e., 6G, different microservices with distinct requirements will require the network infrastructure to respond to their needs. Dynamic network resource adjustment, for instance, will be one of the main needs of future services leveraging network softwarization and virtualization. Softwarization of functions that were previously performed by hardware paves the way for virtualization, and thus, enables elastic services to follow users through the network infrastructure. Therefore, VMNs will bring new opportunities in future networks, yet have distinct security requirements. However, more security concerns will arise as we move forward towards its practical use.

There exist many security challenges when the future of VMNs is visualized with respect to the current technological development in that direction. There are, for example, virtualization-specific challenges such as techniques for integrity verification of VNF packages, slice synchronization, consistent policy enforcement, and security monitoring among multi-operator environments. On the network side, the 5G utilizes a service oriented approach at the control plane with its Service-Based Architecture (SBA). With SBA, new network functions related to service discovery and exposure are introduced into the architecture together with a Representational State Transfer (REST)-based APIs and request-response communication model. Web technologies are extensively used in SBAs that bring with them new inherent vulnerabilities to mobile networks. Risks of using web technologies are mainly related to availability, confidentiality, integrity and control of the mobile network functions and signalling [54]. Therefore, new solutions for securing web-based systems, such as new SBAs, are required. Related to O-RAN, their ecosystems need to adopt the industry practices for software development and security testing, which is also prioritized by the O-RAN Alliance through its Security Task Group. However, the work on O-RAN implementations has only started so there is a lot of implementation, testing and validation to be done especially related to the interoperability, security and automation of O-RAN functionalities in large-scale deployments.

There are also new emerging concepts for efficiently utilizing VMNs which need further research to not only secure those services, but also the underlying VMNs from security threats arising with the use of such services. For example, network in a box (NIB), a personalized private network to provide services in mission critical situations, will be one of the main strengths of 6G [113]. Virtualization will be at the core of NIB to provide differentiated or isolated services, and the communication infrastructure to provide necessary dedicated resources and isolation from other services. However, the security of NIB will be a major challenge since the integration of NIBs into mainstream networks will require proper authorization and security-based service level agreements. On the flip side, NIB can help enabling the security-as-a-service model [114] and its integration into mainstream networks along with the capa-
bility of mobility. Secure virtual mobile small cells [115] is a similar concept, enabling users to create, operate, and maintain small cells. Leveraging SDN and NFV, end user devices, working in a stand alone cell fashion, will also have security concerns related to the integration into mainstream operator networks. Therefore, the security of these concepts must be investigated for future networks, since microservices and micro-operators will be common in future networks and these concepts will be highly important.

AI will play in important role in future networks, specifically in 6G, as discussed in [116]. However, there is limited research in utilizing AI within the domain of VMNs. An interesting future research in this direction includes the investigation of AI-assisted virtualization, where AI techniques take decisions in terms of i) identifying resources for virtualization, ii) defining the number or amount of virtual instances or shares to be created on a resource, and iii) the duration or life-cycle of the virtual resources. On the flip side, AI has its own security challenges, specifically when it comes to wireless networks as detailed in [76], [117]. Therefore, secure-by-design AI-based network virtualization makes important future research direction. Such work will require investigating the security of the AI techniques first, then the security of the virtualization techniques that leverage AI, and in the end security of the AI-based VMNs.

VI. CONCLUSIONS

With VMNs, many operators will be able to share the same physical infrastructure, including MNOs and MVNOs. As a consequence, the security environment will be complex and dependent on the security features of the enabling technologies and other operators. In this article, the security challenges and their potential solutions in VMNs and its enabling technologies are elaborated. The article discusses on how security is managed in VMNs with the standardized techniques along with the development of the standardization. Since VMNs are not yet widely deployed on commercial basis, the security landscape is still not very clear. Yet, there exist important future research directions that can ensure safe and secure operation of VMNs, which are discussed in the future research directions. The most important research direction is the security-by-design approach that leaves less room for security vulnerabilities.

References

[1] Y. Xiao, M. Krunz, and T. Shu, “Multi-operator network sharing for massive IoT,” IEEE Communications Magazine, vol. 57, no. 4, pp. 96–101, 2019.
[2] B. Yi, X. Wang, K. Li, S. K. Das, and M. Huang, “A comprehensive survey of network function virtualization,” Computer Networks, vol. 133, pp. 212 – 262, 2018.
[3] I. Cerrato, A. Palesandro, F. Risco, M. Suñé, V. Vercellone, and H. Woessner, “Toward dynamic virtualized network services in telecom operator networks,” Computer Networks, vol. 92, pp. 380 – 395, 2015, software Defined Networks and Virtualization.
[4] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, “Network function virtualization: Challenges and opportunities for innovations,” IEEE Communications Magazine, vol. 53, no. 2, pp. 90–97, Feb 2015.
[5] Costa-Requena, et al., “SDN and NFV integration in generalized mobile network architecture,” in Networks and Communications (EuCNC), 2015 European Conference on, June 2015, pp. 154–158.
[6] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, “Overview of 5G Security Challenges and Solutions,” IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36–43, 2018.
[7] N. M. K. Chowdhury and R. Boutaba, “A survey of network virtualization,” Computer Networks, vol. 54, no. 5, pp. 862–876, 2010.
[8] J. Ordóñez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, “Network slicing for 5g with sdn/nfv: Concepts, architectures, and challenges,” IEEE Communications Magazine, vol. 55, no. 5, pp. 80–87, 2017.
[9] A. Baumgartner, V. S. Reddy, and T. Bauschert, “Mobile core network virtualization: A model for combined virtual core network function placement and topology optimization,” in Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft), 2015, pp. 1–9.
[10] X. Costa-Perez, J. Swetina, T. Guo, R. Mahindra, and S. Rangarajan, “Radio access network virtualization for future mobile carrier networks,” IEEE Communications Magazine, vol. 51, no. 7, pp. 27–35, 2013.
[11] E. J. Kitindi, S. Fu, Y. Jia, A. Kabir, and Y. Wang, “Wireless network virtualization with sdn and c-ran for 5g networks: Requirements, opportunities, and challenges,” IEEE Access, vol. 5, pp. 19099–19115, 2017.
[12] V.-G. Nguyen, A. Brunstrom, K.-J. Grinnemo, and J. Taheri, “Sdn/nfv-based mobile packet core network architectures: A survey,” IEEE Communications Surveys Tutorials, vol. 19, no. 3, pp. 1567–1602, 2017.
[13] M. Yang, Y. Li, D. Jin, L. Su, S. Ma, and L. Zeng, “Openran: A software-defined ran architecture via virtualization,” SIGCOMM Comput. Commun. Rev., vol. 43, no. 4, p. 549–550, Aug. 2013. [Online]. Available: https://doi.org/10.1145/2533469.2491732
[14] I. Ahmad, M. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, “Security for 5G and Beyond,” IEEE Communications Surveys Tutorials, vol. 21, no. 4, pp. 3682–3722, Fourthquarter 2019.
[15] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, A Comprehensive Guide to 5G Security. John Wiley & Sons, 2018.
[16] M. Liyanage, I. Ahmad, M. Ylianttila, J. L. Santos, R. Kantola, O. L. Perez, M. U. Izzaelaia, E. Montes De Oca, A. Valtierra, and C. Jimenez, “Security for future software defined mobile networks,” in 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015, pp. 256–264.
[17] M. Liyanage, I. Ahmad, J. Okwuibe, M. Ylianttila, H. Kabir, J. L. Santos, R. Kantola, O. L. Perez, M. U. Izzaelaia, and E. M. De Oca, “Enhancing security of software defined mobile networks,” IEEE Access, vol. 5, pp. 9422–9438, 2017.
[18] N. B. Khalifa, A. Benhamiche, A. Simonian, and M. Bouillon, “Profit and strategic analysis for mno-mvn partnership,” in 2018 IFIP Networking Conference (IFIP Networking) and Workshops. IEEE, 2018, pp. 325–333.
[19] Y. Li, J. Zheng, Z. Li, Y. Liu, F. Qian, S. Bai, Y. Liu, and X. Xin, “Understanding the ecosystem and addressing the fundamental concerns of commercial mno,” IEEE/ACM Transactions on Networking, vol. 28, no. 3, pp. 1364–1377, 2020.
[20] A. Aijaz, “Private 5g: The future of industrial wireless,” IEEE Industrial Electronics Magazine, vol. 14, no. 4, pp. 136–145, 2020.
[21] T. Taleb, I. Afolabi, and M. Bagaa, “Orchestrating 5g network slices to support industrial internet and to shape next-generation smart factories,” IEEE Internet of Things Journal, vol. 33, no. 4, pp. 146–154, 2019.
[22] A. Jawar, A. Sabah, M. Ibnkahla, and O. Issa, “Lite-based public safety networks: A survey,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1165–1187, 2019.
[23] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider, “Nfv and sdn—key technology enablers for 5g networks,” IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2468–2478, 2017.
[24] G. Bizcok, M. Dramitinos, L. Toka, P. E. Heegaard, and H. Lonsethagen, “Manufactured by software: Sdn-enabled multi-operator composite services with the 5g exchange,” IEEE Communications Magazine, vol. 55, no. 4, pp. 80–86, 2017.
[25] J. Matias, J. Garay, N. Toledo, J. Unzilla, and E. Jacob, “Toward an SDN-enabled NFV architecture,” IEEE Communications Magazine, vol. 53, no. 4, pp. 187–193, 2015.
[26] E. Marku, G. Bizcok, and C. Boyd, “Towards protected vNf for multi-operator service delivery,” in 2019 IEEE Conference on Network Softwarization (NetSoft), 2019, pp. 19–23.
16

VOLUME 4, 2016

I. Ahmad et al.: Virtual Mobile Networks: An Overview of Security

[73] 5G Americas, “Security considerations for the 5G era,” Jul. 2020. [Online]. Available: https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Loosless.pdf

[74] O-RAN Alliance, “AI/ML workflow description and requirements - v1.3,” Jul. 2020.

[75] P. H. Masur and J. H. Reed, “Artificial intelligence in open radio access network,” arXiv:2104.09445 [cs.NI], Apr. 2021.

[76] J. Suomalainen, A. Juhola, S. Shahabuddin, A. Mammela, and I. Ahmad, “Machine Learning Threats 5G Security,” IEEE Access, vol. 8, pp. 190822–190842, 2020.

[77] ITU-T, “Security architecture for systems providing end-to-end communications,” 2003.

[78] J. Keeney, S. v. d. Meer, and L. Fallon, “Towards real-time management of virtualized telecommunication networks,” in 10th International Conference on Network and Service Management (CNSM) and Workshop, Nov 2014, pp. 388–393.

[79] R. Szabo, M. Kind, F. Westphal, H. Woesner, D. Jocha, and A. Csaszar, “Elastic network functions: opportunities and challenges,” IEEE Network, vol. 29, no. 3, pp. 15–21, May 2015.

[80] Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification. [Online]. Available: https://www.etsi.org

[81] G. M. Yilma, F. Z. Youssaf, V. Sciancalepore, and X. Costa-Perez, “On the challenges and kpis for openapi based telecom vnf managed clouds: Osm vs onap,” arXiv preprint arXiv:1904.10697, 2019.

[82] L. Mamashane, A. A. Lysoy, T. Mukute, M. Wamganga, and Z. Du Toit, “Overview of a open-source resource orchestrating ETSI MANO compliant implementations: A brief survey,” in 2019 IEEE 2nd Wireless Africa Conference (WAC). IEEE, 2019, pp. 1–7.

[83] A. La Marra, A. Lunardelli, F. Martinelli, P. Mori, A. Saracino, P. Catooldi, F. Martino, and B. Martin, “Enhancing security in etsi open source network end-to-end with usage capability control,” in 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2019, pp. 25–29.

[84] A. Reid, A. González, A. Armengol, G. de Blas, M. Xie, P. Grensund, P. Willis, P. Eardley, and F. Salgueiro, “Osm scope, functionality, operation and integration guidelines,” ETSI, White Paper, 2019.

[85] Ospaq security requirements. [Online]. Available: https://wiki.openup.org/display/DW/ONAP#Security-Requirements

[86] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucci, I. Oppermann, Z. Yan, T. H. Nguyen, F. Liu, T. Hewa, M. Ylianttila et al., “6G white paper: Research challenges for trust, Security and Privacy,” arXiv preprint arXiv:2004.11665, 2020.

[87] R. Kantola, “Trust Networking for Beyond 5G and 6G,” in 2020 2nd 6G Wireless Summit (6G SUMMIT), 2020, pp. 1–6.

[88] A. Celesti, M. Fazio, A. Galletta, L. Carnevale, J. Wan, and M. Villari, “Security assurance methodology (scas) for 3gpp network products,” 3GPP, 2020.

[89] A. Celesti, M. Fazio, A. Galletta, L. Carnevale, J. Wan, M. Villari, and M. Ylianttila, “User privacy, identity and trust in 5g,” A Comprehensive Guide to 5G Security, pp. 267–279, 2018.

[90] X. Liu, J. Lee, S. H. Kim, Q. Zheng, S. Xu, T. Suh, W. W. Ro, and W. Shi, “Architectural protection of application privacy against software and physical attacks in untrusted cloud environment,” IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 478–491, 2018.

[91] 5G and Data Privacy: An overview for policymakers. [Online]. Available: https://www.gsma.com/publicpolicy/wp-content/uploads/2020/07/GSMA_5G_Data_Privacy_July_20.pdf

[92] P. Zhang, M. Durreisi, and A. Durreisi, “Multi-access edge computing aided mobility for privacy protection in internet of things,” Computing, vol. 101, no. 7, pp. 729–742, 2019.

[93] A. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, “A light weight authentication protocol for iot-enabled devices in distributed cloud computing environment,” Future Generation Computer Systems, vol. 78, pp. 1005–1019, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X1630824X

[94] T. Kumar, A. Braeken, A. D. Jurcut, M. Liyanage, and M. Ylianttila, “Age: authentication in gadget-free healthcare environments,” Information Technology and Management, vol. 21, pp. 95–114, 2020.

[95] X. Zhang, A. Kunz, and S. Schröder, “Overview of 5G security in 3GPP,” in 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2017, pp. 181–186.

[96] Network Functions Virtualisation. European Telecommunications Standards Institute (ETSI). [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/ovpfa

[97] Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access. [Online]. Available: https://www.etsi.org

[98] Network Functions Virtualisation (NFV) Release 2; Security; VNF Package Security Specification. [Online]. Available: https://www.etsi.org

[99] Network Functions Virtualisation (NFV) Release 3; Security; Security Specification for MANO Components and Reference points. [Online]. Available: https://www.etsi.org

[100] Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture. [Online]. Available: https://www.etsi.org

[101] Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components. [Online]. Available: https://www.etsi.org

[102] X.1044 : Security requirements of network virtualization. [Online]. Available: https://www.itu.int/rec/T-REC-X.1044-201910-P/en

[103] Network Functions Virtualisation (NFV) : Supplement on security guidelines for mobile virtual operators. [Online]. Available: https://www.itu.int/rec/T-REC-X.1044-201910-P/en

[104] P. Pratim Ray, N. Kumar, and M. Guizani, “A Vision on 6G-Enabled NB: Requirements, Technologies, Deployments and Prospects,” IEEE Wireless Communications, pp. 1–8, 2021.

[105] V. Varadharan and U. Tupakula, “Security as a service model for cloud environment,” IEEE Transactions on Network and Service Management, vol. 11, no. 1, pp. 70–75, 2014.

[106] D. Shilo, “Method and system for securing user identities and creating virtual users to enhance privacy on a communication network,” Aug. 12 2008, US Patent 7,422,636.

[107] T. Kumar, M. Liyanage, I. Ahmad, A. Braeken, and M. Ylianttila, “User privacy, identity and trust in 5g,” A Comprehensive Guide to 5G Security, pp. 267–279, 2018.

[108] L. Xue, J. Lee, S. H. Kim, Q. Zheng, S. Xu, T. Suh, W. W. Ro, and W. Shi, “Architectural protection of application privacy against software and physical attacks in untrusted cloud environment,” IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 478–491, 2018.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3133319, IEEE Access

16
IJAZ AHMAD received his MSc. and PhD. in Wireless Communications from the University of Oulu, Finland in 2012 and 2018, respectively. Currently, he is working with VTT Technical Research Centre of Finland, and is an adjunct professor at the University of Oulu, Finland. He has been a post-doctoral fellow at the Centre for Wireless Communications (CWC), Oulu, Finland. Dr. Ijaz has visited several institutions as a visiting scientist, such as Technical University of Vienna, Austria (2019), and Aalto University Finland (2018). Dr. Ijaz has more than 45 publications including journals, conference papers, book chapters, a patent application, and published an edited book on the security of 5G, called “A comprehensive guide to 5G security” with Wiley. Inc. Dr. Ijaz is the recipient of several awards including the Nokia foundation, Tauno Töning and Jorma Ollila grant awards, and VTT Excellence award for 2020. Furthermore, Dr. Ijaz has received two best paper awards in IEEE conferences. His research interests include cybersecurity, security of 5G/6G, and the applications of machine learning in wireless networks.

JANO PINOLA received his M.Sc. degree in telecommunications from the University of Oulu in 2008. Working as a researcher at VTT, he has contributed to numerous national and international R&D projects which have studied and developed various wireless communication technologies, including 3G/UMTS, 4G/LTE, WiMAX, and WiFi. During the past few years, he has also been involved in the Finnish national 5G test networks through the 5G Test Network Finland (5GTNF) coordination action. His current research interests include mobile network architectures, performance evaluation, and testing of wireless communication technologies in the context of 5G and beyond systems.

ILKKA HARJULA is working as a senior scientist at the VTT Technical Research Centre of Finland. He has a long research experience in the domain of wireless networks and has been involved in several national and international research projects. His research interests include 5G and beyond, virtual networks, and RAN management.

JYRKI HUUSKO received his degree in theoretical physics with minor subjects in information technology and mathematics from the University of Oulu. He is working at the VTT Technical Research Centre of Finland as a research team leader. His current research topics include future autonomic networks and services, transport protocols and multimedia delivery optimization, cross-layer communication design in heterogeneous wireless and mobile networks, cross-layer communication aided network mobility and multi-access.

ERKKI HARJULA works as an Assistant Professor (tenure track) at the Centre for Wireless Communications - Networks and Systems (CWC-NS) research group, University of Oulu, Finland. He focuses on wireless system level architectures for future digital healthcare, where his key research topics are wrapped around intelligent trustworthy distributed IoT and edge computing. Dr. Harjula has background in the interface between computer science and wireless communications: mobile and IoT networks, distributed networks, cloud and edge computing and green computing. He has also long experience as a research project manager. He received his D.Sc. degree in 2016, and his M.Sc. degree in 2007 at University of Oulu. He has coauthored more than 70 international peer-reviewed articles. He is a Member of IEEE and associate editor in Springer Wireless Networks journal.

TANESH KUMAR is currently working as a Postdoctoral researcher at the Centre for Wireless Communications (CWC), University of Oulu, Finland. He received his D.Sc. degree in communications engineering from the University of Oulu, Finland, in 2016, the M.Sc. degree in computer science from South Asian University, New Delhi, India, in 2014 and the B.E. degree in computer engineering from the National University of Sciences and Technology (E&ME), Pakistan, in 2012. He has coauthored over 40 peer-reviewed scientific articles. His current research interests include security, privacy and trust in the IoT, 5G/6G edge computing, Blockchain and Medical ICT.