Design Principles for 5G Security

Chapter · January 2018

DOI: 10.1002/9781119293071.ch4

5 authors, including:

Ijaz Ahmad
University of Oulu
37 PUBLICATIONS **517** CITATIONS
SEE PROFILE

Madhusanka Liyanage
University College Dublin
93 PUBLICATIONS **643** CITATIONS
SEE PROFILE

Shahriar Shahabuddin
Nokia
18 PUBLICATIONS **55** CITATIONS
SEE PROFILE

Mika Ylianttila
University of Oulu
203 PUBLICATIONS **2,875** CITATIONS
SEE PROFILE

4

Design Principles for 5G Security

Ijaz Ahmad[1], Madhusanka Liyanage[1], Shahriar Shahabuddin[1], Mika Ylianttila[1], and Andrei Gurtov[2]

[1] *Centre for Wireless Communications (CWC), University of Oulu, Finland*
[2] *Department of Computer and Information Science, Linköping University, Linköping, Sweden*

4.1 Introduction

The vision of the 5G wireless networks lies in providing very high data rates, higher coverage through dense base station deployment with increased capacity, significantly better Quality of Service (QoS), and extremely low latency [1]. 5G is considered to provide broadband access everywhere, entertain higher user mobility, enable connectivity of a massive number of devices (e.g. IoT), and the connectivity will be ultra-reliable and affordable [2]. The development towards an all-IP-based communication, for example in 4G, has already helped develop new business opportunities, provide new online services and connect industrial machines, home appliances and business units. However, with this development, the security challenges and threat vectors have also increased.

Wireless communication systems were prone to security vulnerabilities from the very beginning. In the first generation (1G) wireless networks, mobile phones and wireless channels were targeted for illegal cloning and masquerading. In the second generation (2G) of wireless networks, message spamming became common, not only by pervasive attacks but also by injecting false information or broadcasting unwanted marketing information. In the third generation (3G) wireless networks, IP-based communication enabled the migration of Internet security vulnerabilities and challenges in the wireless domains. With the increased necessity of IP-based communication, the fourth Generation (4G) wireless networks enabled the proliferation of smart devices, multimedia traffic, and new services into the mobile domain. This development lead to a more complicated and dynamic threat landscape. With the advent of the fifth generation (5G) wireless networks, the security threat vectors will be bigger than even before, with greater concerns for privacy [3].

One haunting fact that has always stayed alive during the development towards the 5G is that the IP-based communication not only increased the variety of services and network traffic but opened new doors to develop new cracking and hacking mechanisms for wireless networks and mobile devices. Wireless networks and user equipment, however, had difficulty in keeping up the pace with the increasing security

A Comprehensive Guide to 5G Security, First Edition. Edited by Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, and Mika Ylianttila.

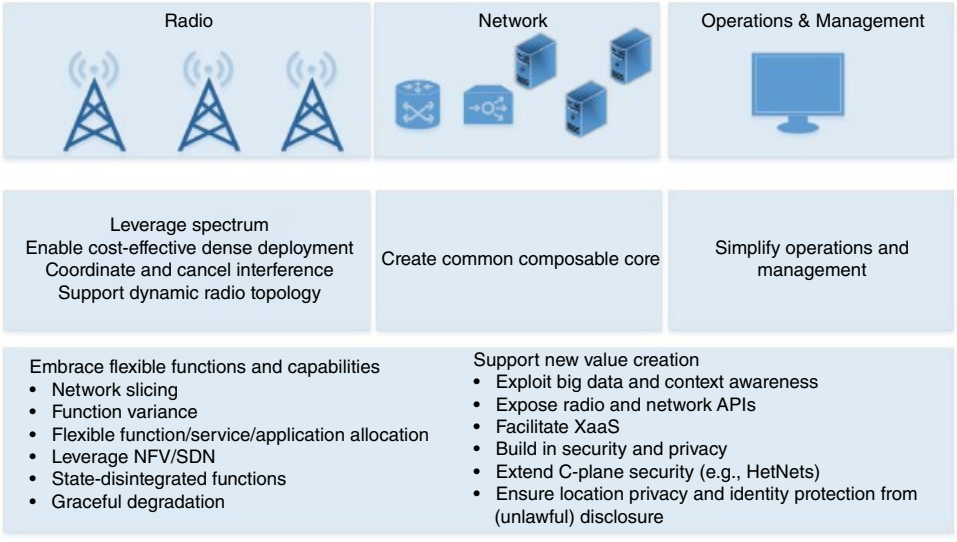

Figure 4.1 5G design principles.

challenges surfacing due to IP connectivity. Hence, new solutions and technologies have always been sought to protect the network, user traffic and services. In this chapter, we will provide an overview of the new types of security threats, and then present the solutions proposed for those threats.

5G will connect a critical infrastructure that will require more security to ensure safety of not only the critical infrastructure but safety of society as a whole. For example, a security breach in the power supply systems can be catastrophic for all the electrical and electronic systems on which the society depends upon. Similarly, data is critical in decision making and the data will be carried by the 5G network. Hence, adequate measures are required to safeguard the data. Similarly, it is envisioned that public safety systems will also be connected through 5G networks, hence it is more critical to develop proper measures to secure not only the network but also the services using 5G networks as a communication medium. Therefore, it is suggested by the Next Generation Mobile Networks (NGMN) [4] that 5G should provide more than hop-by-hop and radio bearer security. The 5G design principles elaborated in Figure 4.1 outlines the need for highly elastic and robust systems. Such architectures must support the deployment and placement of security functions whenever required in any network perimeter.

4.2 Overviews of Security Recommendations and Challenges

The security threat vectors in 5G will be multi-dimensional, right from the physical interfaces up to the application interfaces, services in the clouds, and user information. 5G networks will connect critical infrastructures, interconnect societies and

industries, provide anything as-a-service, and integrate new models of service delivery. The 5G ecosystem cannot be fully visualized at this moment, due to the rapid development and integration of new devices and services. However, the main attractions of 5G beyond extended connectivity, higher data rates and lower latencies will be the easy placement and utilization of new services and functions. This will complicate the security landscape as well. To make the security landscape easy to comprehend, we provide a discussion on security in two domains. First, the security of access networks, for example Radio Access Networks (RAN) that can be a composite of multiple access technologies such as cellular networks RAN comprising small and large base stations and WiFi, etc. Second, the security of the core network in which the network control resides with operator and vendor specific services. The International Telecommunication Union's Telecommunication sector (ITU-T) has proposed dimensions of security for telecommunication networks that address all the aspects of security [6]. Hence, first we will provide a brief introduction to these recommendations and then we will discuss different security challenges in different areas of 5G networks.

4.2.1 Security Recommendations by ITU-T

Security dimensions are proposed by ITU-T in its security recommendation [6] to address almost all the aspects of network security. The security dimensions include a set of security measures that can be used to protect the users and network against all major security threats. These dimensions are:

- *Access Control*: security measures that ensure only authorized personnel or devices access the network resources.
- *Authentication*: security mechanisms that ensure identities of the communicating parties and that a user or device is not attempting a masquerade or unauthorized replay of previous communications.
- *Non-Repudiation*: ensure that a particular action has been performed by a specific user or device is non-repudiation. Proper identities are used to ensure that authentic user or device can access particular services and resources.
- *Data Confidentiality*: security mechanisms to protect the data from unauthorized access. Encryption, access control mechanisms and file permissions are used to ensure data confidentiality.
- *Communication Security*: ensure that the data flows between the authorized endpoints and is not diverted or intercepted in between.
- *Data Integrity*: ensures the correctness or accuracy of data in transmission and protects it from unauthorized modification, deletion, creation and replication.
- *Availability*: ensures that there is no denial of authorized access to network resources and applications. Events impacting the network, such as system failures or disasters, scalability and security compromise, must not limit access to authorized users and devices.
- *Privacy*: mechanisms that ensure protection of information, which might be derived from observing network activities.

4.2.2 Security Threats and Recommendations by NGMN

The Next Generation Mobile Networks (NGMN) [7] provides recommendations for 5G based on the current network architectures, and the lacking security measures that are either not implemented or available. The recommendation highlights the cautionary notes. These include the infancy of 5G with many uncertainties, lack of defined design concepts and the unknown end-to-end (E2E) and subsystem architectures. The recommendation highlights the limitations in the access networks and cyber-attacks against the network infrastructure. The details of the security limitations and recommendations can found in [7]. Below we highlight the key points in the recommendations:

- *Flash network traffic*: It is known that the number of end user devices will grow exponentially in 5G, thus the large-scale events may cause significant changes in the network traffic patterns that could be either accidental or malicious. Therefore, it is recommended that the 5G systems must minimize large swings in traffic usage and provide resilience whenever such surges occur, while maintaining an acceptable level of performance.
- *Security of radio interface keys*: In the previous generations, even in 4G, keys for the radio interface encryption are generated in the home network and sent to the visited network over unsecure links causing a clear point of exposure of the keys. It is recommended that the keys are either not sent over those links, such as SS7/Diameter, or properly secured.
- *User plane integrity*: 3G and 4G do not provide cryptographic integrity protection for the user data plane, though these provide protection to some signaling messages. It is recommended to provide the protection at the transport or application layer that terminates beyond the mobile network. The exception to this could be network level security for resource constrained IoT or latency sensitive 5G devices and services. Application level E2E security may involve too much overhead for data transmission in the packet headers and handshakes.
- *Mandated security in the network*: There are service-driven constraints on the security architecture leading to optional use of security measures. Unfortunately, these constraints undermine system-lever security assumptions and cannot be completely eliminated. The challenge increases in multi-operator scenarios where one operator suffers due to inadequate measures by other. Therefore it is highly recommended that some level, if not all, must be mandated in 5G after proper investigation to recognize the most critical security challenges.
- *Consistency in subscriber level security policies*: There is a need that the user-security parameters are not changed due to roaming from one operator network to the other. In the case of highly mobile users, it is highly possible that all the security services are not updated frequently and per-user basis as the user moves from place to place or from one operator network to another in the case of roaming. When a user from one operator moves to another and is using latency sensitive services, the services might be provided through the edge of the visited operator network such as in Mobile Edge Computing (MEC). So will the security or the security of the service being used be automatically offered or configured at the new location? This needs security policy sharing among network operators on a much faster scale to secure user traffic with roaming. The recommendation discusses the possibility of using virtualization

techniques in such situations that can enable per-user slice configuration to keep the security policies and services intact whenever and wherever the user moves.

- *DoS attacks on the Infrastructure*: DoS and Distributed DoS (DDoS) attacks might circumvent the operation of devices controlling the critical infrastructure such as energy, health, transportation, and telecommunications, causing life threatening consequences with tremendous human and capital losses. DoS attacks are designed such that they exhaust the physical and logical resources of the targeted devices. The challenge will be more threatening due to the possibility of attacks from machines that are geographically dispersed in locations and in huge numbers. The network must be capable of servicing the increasing number of connections caused by the increasing proliferation of connected devices (e.g. IoT) with different operating capabilities and limitations.

4.2.3 Other Security Challenges

We can classify the security challenges on a high level into three domains, that is, security challenges in the access network, DoS Attacks, and security challenges in the core network. Below we briefly describe each of them.

4.2.3.1 Security Challenges in the Access Network

Network access security provides secure access to the network and services with protection from vulnerabilities in the radio. For example, the user must be ensured security from malicious network activities and the network must be secured from malicious access. 5G will utilize a variety of access technologies and integrate different types of access networks for extended coverage, higher throughput and lower latencies. To keep the network working, 5G must improve the system robustness against jamming attacks of the radio signals and channels. Furthermore, the security of small cell nodes must be improved due to their geographical distribution and ease of access.

One of the key challenges in 5G will be the excessive nodes sending data and receiving data simultaneously, practically jamming the radio interfaces. The challenge can be exacerbated by malicious nodes sending excessive signaling traffic, causing availability challenges or, in other words, leading to Denial of Service (DoS) attacks. Such signaling traffic or attacks must be recognized early and stopped before the jamming the network. 3G and 4G provided cryptographic integrity protection of some signaling messages but the user data plane was still not protected.

From 2G to 4G, the radio interface encryption keys are computed in the home core network and are transmitted to the visited radio network over SS7 or Diameter signaling links. These keys can be leaked, thus creating a clear point of exposure in the network [7]. Therefore, well designed key management protocols should be in place for 5G to reduce the threats. The basic techniques include improving the SS7 and Diameter security by introducing firewalls [7]. However, other approaches can be applied, such as using different secure control channels for distributing the keys. Some of these approaches are described in Chapter 10. Security of the physical layer is described in Chapter 6.

4.2.3.2 DoS Attacks

DoS and DDoS attacks originating from large sets of connected devices will very likely pose a real threat to 5G networks. These attacks can be either against the network infrastructure or the end user devices. Attacks against the infrastructure are designed to

deplete the resources of the network operator infrastructure that serves the users and devices. Though the original target is the operator network, the subscribers are indirectly affected. Attacks against users/devices are designed to deplete the resources of the users and devices. In this case, the subscribers and devices are directly targeted, but this impacts the network operator indirectly. Compromised user devices can also be used to cause the attacks against the network infrastructure.

DoS attacks on 5G network infrastructure would likely target the resources that are related to connectivity and bandwidth at promised levels of service. Hence, the focus can be against the following areas:

1) the signaling plane needed for authentication, connectivity and bandwidth assignment, and mobility of 5G users;
2) user plane needed to support two-way communication of devices;
3) management plane that supports the configuration of network elements that support signaling and user planes;
4) support systems that performs user/devices billing;
5) radio resources providing access to user devices; and
6) physical and logical resources supporting network clouds.

DoS attacks against the user devices will target the physical resources of the user devices such as memory, battery, processing units, radios, and sensors, etc. These attacks can also target the logical resources such as operating systems, applications, configuration data, and user data, etc.

4.2.3.3 Security Challenges in the Control Layer or Core Network

The massive penetration of IP protocols in the control and user planes in all network functions make the 5G core network highly vulnerable. Hence the network must be capable of ensuring availability with improved resilience against signaling-based threats. Specific security features must be incorporated for latency sensitive applications and use cases. The network must also incorporate the security requirements defined by the 3GPP. Furthermore, 5G networks should ensure communication in emergency situations such as when part of the network is either inaccessible or destroyed.

Overloading the signaling plane with huge number of infected IoT or M2M devices, either as an attempt of DoS attack or to gain access to the network, will be another pressing challenge in 5G networks [7]. IoT devices, in billions [46], will be resource constrained, thus making two kinds of requests. First, due to limited capabilities, these devices will require the resources in the clouds to perform processing, storing or sharing of information. Second, also due to their limited capabilities, these will be an easy target to masquerade or operate in a compromised environment for attacks on the network in the form of DoS attacks. Hence, the increasing number of connected devices will be a huge challenge for the signaling plane or core network of 5G networks. An example of this is the authentication and authorization requests to the HSS, which can potentially make the HSS inaccessible to legitimate users, in other words, compromise the centralized entity through a DoS attack or saturation attack [48].

The increasing range of communication services and devices leads to high traffic volumes for signaling purposes, such as authentication and bearer activation. Such traffic bursts bring about a signaling storm and may crash the core network [1]. Similarly, the signaling procedures occur at the NAS layer of 3GPP protocols that

include attach/detach, bearer activation, location update, and authentication. These form the NAS signaling storms [1]. This can be more challenging in 5G, where billions of devices will be connected to the same core network. Nokia Seimens Networks published [15] that signaling traffic is increasing 50% faster than the data traffic. Small cells with a vast number of connected devices being mobile will increase mobility handovers, thus increasing the signaling traffic. This will not only increase the signaling load on Mobility Management Entity (MME), but on other control entities such as HSS, public data network gateway (P-GW) and Serving Gateways (S-GW), to maintain the Quality of Service (QoS). Furthermore, the NAS layer of 3GPP protocols for UE attach or detach functions, bearer activation, location update, and authentication can cause signaling storms [16]. 3GPP recommends the use of IPSec encryption for LTE interfaces, such as X2, S1-MME, S5 and S6, etc. Thus, each eNB is required to support hundreds of IPSec tunnels, while the backhaul has to support thousands of tunnels. Such a massive tunnel establishment not only complicates the security establishment but massively increases the signaling load in the network. Furthermore, the tunnel establishment is static in nature and predefined by the administrator that further complicates the process of ensuring security of the control traffic. The tunnels, statically established, might not be in use but still sending periodic control information also increases the signaling load.

Therefore, using the currently deployed security architectures in 5G will cause major scalability and availability challenges, thus paving the way for DoS and DDoS attacks. Novel security architectures are needed for 5G to ensure the security of users and protect the network from malicious attacks.

4.3 Novel Technologies for 5G Security

Since 5G is not an incremental improvement in 4G, security systems should also be re-designed according to the design and architectural requirements of 5G. The vision for secure 5G systems outlined by NGMN is based on three principles:

1) Flexible security mechanisms;
2) Supreme built-in security; and
3) Automation.

The vision is that 5G should provide highly robust security systems against cyber-attacks, with enhanced privacy and security assurance. The security mechanisms must be flexible to incorporate novel technologies, for example for authentication and identification. The flexibility should enable the option of using encryption for the user plane and per network slice security parameters adjustment. The security systems must also be able to be automated to adjust and adapt itself intelligently according to the environment, threats or security controls. A holistic security orchestration and management will be highly required [4].

Since 5G has higher flexibility and agility, the two concepts that are most prominent to play a vital role in 5G are virtual network functions (VNFs) and software-based network control. These features are foreseen to be enabled by Network Functions Virtualization (NFV) and Software Defined Networking (SDN). NFV enables vendors to implement network function in software called VNFs and deploy them on high-end servers or cloud

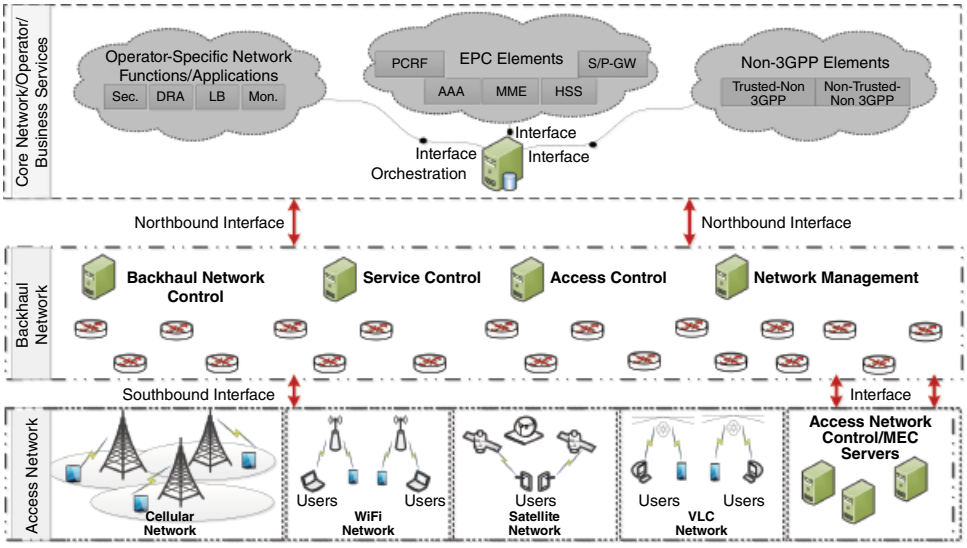

Figure 4.2 High-Level 5G architecture integrating multiple access technologies.

platforms instead of specialized function-specific hardware. SDN, on the other hand, separates the network control plane from the data forwarding plane to enable innovation in network control systems. Therefore, NFV and SDN will be vital in providing foolproof security in 5G systems. The basic diagram of the 5G network that provides connectivity to all devices at all times, covering almost every aspect of the society, is presented in Figure 4.2. The high level architectural diagram presented in the figure leverages the concepts of NFV and SDN to dynamically provide security in various network parameters, as the need arises. Below we describe the security challenges existing in both technologies and how these technologies can be used to increase the overall network security.

4.3.1 5G Security Leveraging NFV

Virtualization is used to decouple a system's service model from its physical realization and has been used in networking, for example for creating virtual links (tunnels) and broadcast domains (VLANs). Through virtualization, logical instances of a physical hardware can be used for different tasks, where the physical and logical instances are mapped through a network hypervisor [8]. The concept has led to the development of Mobile Virtual Network Operators (MVNOs). To minimize the investment in the infrastructure, MVNOs lease virtual resources including network resources from Mobile Network Operators (MNOs), thus a physical mobile network can host several MVNOs. MVNOs have their own operating and support systems and can offer independent services from the MNO. Therefore, NFV has a vital role, not only in the MVNO and MNO ecosystem, but also in the overall networking ecosystem to utilize the hardware resources in the most efficient manner possible.

NFV will enable function placement in different network perimeters without requiring function specific hardware but based on the need of the function or service at that location and time. Telecom networks will expose Application Programming Interfaces (APIs) on their hardware platform to users and third-party software providers to deploy their

services on the same hardware to reduce costs. However, decoupling the software and hardware will require new security models for the whole system, since the platform-specific security will not suffice for a shared hardware platform. There will be a demand for strong isolation mechanisms to secure each service running on the same hardware.

Virtualization enables multiple tenants or network users to share the same physical network resources that can create security vulnerabilities. A literature study on security implications of virtualization [9] shows that it has a positive effect on availability but has threatening security challenges related to confidentiality, integrity, authenticity and non-repudiation. Virtual machines can be created, deleted and moved around a network easily, hence tracking a malicious virtual machine would be much more complex. Similarly, if a hypervisor is hijacked, the whole system can be compromised [10]. Another major security challenge of NFV is to ensure trust among new elements such as hypervisors, virtual machines and management modules [54]. For instance, VNFs can store and fetch executable code from any server anywhere in the world. Therefore, a trusted mechanism is needed between the operator and cloud provider to ensure that the code is safe and correct.

On the other hand, NFV can highly improve network and user security. For example, secured network slicing can separate the communication of different parties, thus alienating malicious traffic from the remainder. Similarly, distributed can be deployed to resolve DoS and DDoS attacks, and with further intelligence, these VNFs can substantially improve self-protection of 5G networks [14]. Network hypervisor, a program that provides an abstraction layer for the network hardware, enables network engineers to create virtual networks that are completely decoupled from the network hardware. In this section, we outlined the importance of NFV and its security implications at a high level to show its importance for future networks. More detailed analysis of the security threat vectors and counter measures for VNFs and MVNOs is presented in Chapters 14 and 15.

4.3.2 Network Security Leveraging SDN

SDN separates the network control from the forwarding hardware and centralizes the network control into software-based controller platforms. The software-based control function will be centralized in high-end servers. This will accelerate novelty in network feature development, enhancement and rapid deployment. Therefore, the SDN-based wireless network has been a hot research topic and there are many proposals for SDN-based wireless networks [5]. The SDN architecture is vertically separated into three functional layers with interfaces between the layers, as shown in Figure 4.3. OpenFlow is the first viable implementation of SDN and also follows the three-tier architecture of SDN with OpenFlow applications, OpenFlow controller and OpenFlow switches.

The three logical planes are described as:

1) *Application plane*: consists of applications for various network functionalities such as network management, QoS management and security services, etc.
2) *Control plane*: is the logically centralized network control platform running the Network Operating System (NOS), having a global view of the network resources and stats, and provides hardware abstractions to the applications in the application plane.
3) *Infrastructure plane*: also called the data plane that consists the data forwarding elements that act on the instructions of the control plane for dealing with the data packets or traffic flows.

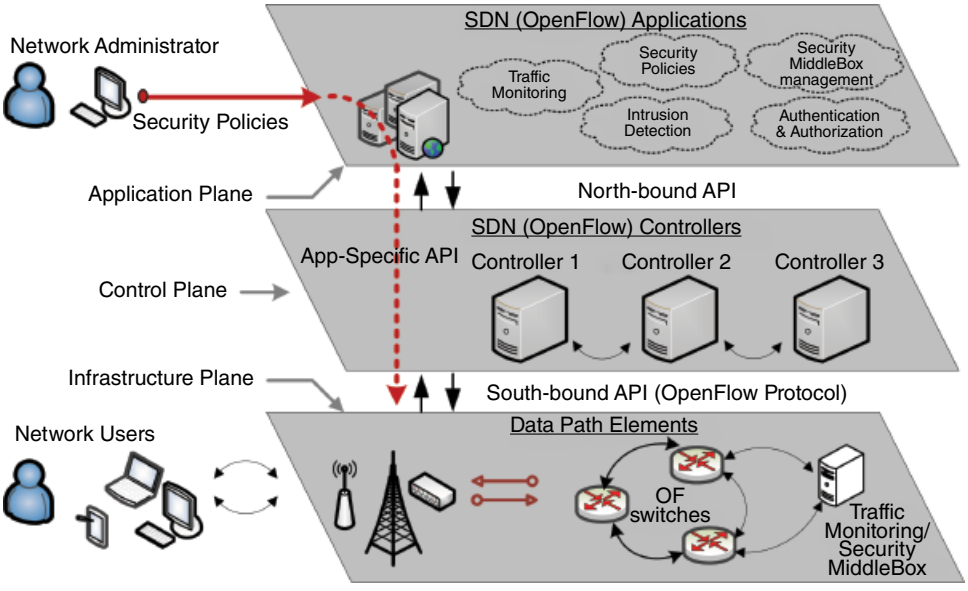

Figure 4.3 An overview of the SDN architecture.

In SDN, network security functions can be implemented as applications deployed in the SDN application plane. The applications gather traffic or network stats information through the control plane from the data forwarding plane using the north-bound interface (applications-control plane API). For example a security application, such as an intrusion detection application, can gather packet samples to perform analysis and then direct the data forwarding plane through the control plane to either drop the packets or forward the packets to a specific port. The port can be either towards the end user or a security middle box for further analysis. This makes the security systems highly flexible. When coupled with NFV, SDN would enable run-time network security function placement at any network perimeter as the need arises. The other main benefit is the decoupling of the network security functions from vendor-specific hardware. This decoupling would allow the network operators to change the security functions whenever deemed necessary, irrespective of the hardware specifications, or changes in the firmware of various hardware used for security purposes.

However, centralizing the network control and softwarizing network function opens new security challenges. For example, the centralized control will be a favorable choice for Denial of Service (DoS) attacks, and exposing the critical APIs to unintended software can render the whole network down. Some of the main threats are highlighted in Table 4.1. Therefore, SDN-based networks need novel security architectures right from the beginning. Below, we highlight the main security threats in SDN-based networks.

4.3.3 Security Challenges in SDN

4.3.3.1 Application Layer

SDN has two principle properties which form the foundation of networking innovation on one hand and the basis of security challenges on the other. First, the ability to control a network by software, and second, centralization of network intelligence in

Table 4.1 Security challenges in SDN.

SDN Layer	Type of Threat	Threat Description
Application	Lack of authentication and authorization	There are no compelling mechanisms for authentication and authorization of applications, and is more threatening in the case of a large number of third-party applications
	Fraudulent rules insertion	Malicious applications can generate false flow rules
	Lack of access control and accountability	A problem for the management plane and for illegal usage of network resources
Control	DoS, DDoS attack	Due to the visible nature of the control plane
	Unauthorized controller access	No compelling mechanisms to obligate access control for applications
	Scalability or availability	Centralizing intelligence in one entity will most likely present scalability and availability challenges
Data Plane	Fraudulent flow rules	Data plane is dumb and hence more susceptible to fraudulent flow rules
	Flooding attacks	Flow tables of OpenFlow switches can store a finite or limited number of flow rules
	Controller hijacking or compromise	Data Plane is dependent on the control plane, making its security dependent on controller security
Ctrl-Data Int.	TCP-Level attacks	TLS is vulnerable to TCP-level attacks
	Man-in-the middle attack	Optional use of TLS and complex configuration of TLS

network controllers [13]. Since most of the network functions can be implemented as SDN applications, malicious applications, if not stopped early enough, can spread havoc across a network. The main security challenges that applications can pose to the network will be due to the availability of open APIs in network equipment, trust relationship between the controller and the applications (mainly third-party applications) and authentication and authorization of applications to change or modify the network behavior [13]. In 5G most of the functionalities will be implemented as applications due to the ease in modifications, making updates, and deployment. NFV will be the key enabler of application-based services and will take application-based services into the networking domains. Therefore, securing the network from anomalies generated by applications will be highly important.

4.3.3.2 Controller Layer

In SDN the control plane (e.g. OpenFlow controller) is a centralized decision-making entity. Hence, the controller can be highly targeted for compromising the network or carrying out malicious activities in the network due to its pivotal role. The same reason is valid for DoS and DDoS attacks. Furthermore, malicious applications can acquire network information from the controller if there are no compelling authentication and authorization mechanisms in place in the controller. The visible nature of the controller

makes it a favorite choice for DoS attacks. Since the SDN controller modifies flow rules in the data path, the controller traffic can be easily identified, thus making the controller a visible entity in the network. Scalability of the controller is another challenge that can be targeted to make the controller a bottleneck for the whole network. If the number of controllers is less or the controller capabilities are not good enough to respond to the queries of the data path elements, the controller can easily become a bottleneck [17].

4.3.3.3 Infrastructure Layer

The SDN switches have flow tables used by the controller to install flow rules for each flow. If the number of flows increases in the switch, there is a high chance that the flow tables will be exhausted. Thus, malicious users can send flows with different field headers making the flow tables to exhaust to cause saturation attacks. In this case, legitimate flows will be discarded due to the limited capability of the switch to buffer legitimate TCP/UDP flows. Since the switches are dumb by taking intelligence to the control plane, it will not be possible for the switches to differentiate genuine flows from the malicious ones. Therefore, the switch can be used for attacks against other switches and the controller. Furthermore, the data plane is dependent on the security of the control plane. If the security of the controller is compromised so that it does not provide instructions for the incoming flows, the data plane will be practically offline. This also makes the controller-data plane link a favorable choice for attacks. Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) are specified for the controller-switch communication. However, the use of TLS and DTLS are left optional mainly due to its configuration complexity. This leaves the controller-switch communication open to attacks, thus increasing the vulnerability of the data and control planes.

4.3.4 Security Solutions for SDN

The logically centralized control plane of SDN provides a global view of the network and enables run-time configuration of the network elements. As a result, the SDN architecture supports highly reactive and proactive security monitoring, traffic analysis and response systems to facilitate network forensics, alteration of security policies and security service insertion [18]. SDN facilitates quick threat identification through a cycle of harvesting intelligence from the network resources, states and flows. The SDN architecture supports traffic redirection through flow-tables modification to analyze the data, update the policy, and reprogram the network accordingly. The programmability achieved by SDNs facilitates dynamic security policy alteration without the need of individual hardware configuration. The automation, thus achieved, would reduce the chances of misconfiguration and policy conflicts across different networks. Consistent network security policies can be deployed across the network due to the global network visibility, whereas security services such as firewalls and Intrusion Detection Systems (IDS) can be deployed on specified traffic according to globally defined security policies.

Below, we define the security of each plane or layer of SDN.

4.3.4.1 Application Plane Security

The SDN control plane works between the network hardware and applications to hide the network complexity from applications. Hence, the centralized control architecture makes it easy to use applications by providing them with the network statistics and

packet characteristics to implement new security services. Therefore, various solutions are proposed to enable the applications work in its functional boundaries with controlled access to network resources. The PermOF is a fine-grained permission system that provides controlled access of data and control planes to the SDN applications. The design of PermOF provides read, notification, write and system permissions to various applications to enforce permission control.

The NGMN security recommendation advises application level data integrity protection for battery constrained IoT devices or low latency 5G devices for user plane data integrity. This will enable data protection beyond the mobile network, thus minimizing the chances of vulnerability of data due to compromises in the network. Thus, SDN enables such applications to implement end-to-end security for constrained devices beyond the security implications of the network.

4.3.4.2 Control Plane Security

Since the security of the control plane is pivotal to the whole network, there have been many proposals and approaches for securing the control plane. The Security-Enhanced (SE) Floodlight controller [19] is an extended and secure version of the original floodlight controller [20]. By securing the SDN control layer, the SE-Floodlight controller provides mechanisms for privilege separation by adding a secure programmable northbound API to the controller and operates as a mediator between the application and data planes. It verifies flow rules generated by applications and attempts to resolve flow rules conflicts between applications.

To mitigate the risks of controller failure due to scalability, or the chances of DoS attacks due to its centralized role, controller resilience strategies have been proposed. The strategies include controller resilience through redundancy, maximizing its storage and processing capabilities, and distributing controller functionalities among multiple control points in the network. The OpenFlow variant of SDN supports wildcard rules so that the controller sends an aggregate of client requests to server replicas. By default, microflow requests are handled by the controller that can create potential scalability challenges and increase the chances of failures due to DoS attacks. Normally reactive controllers are used that act on a flow request when it arrives at the controller. Proactive controllers would install the flow rules in advance, thus minimizing the flow request queue in the controller. Similarly, various load balancing techniques are suggested that will balance the load among multiple controllers in a network.

4.3.4.3 Data Plane Security Solutions

The data plane that transports the actual packets also requires proper security mechanisms. The data plane must be secured from unauthorized applications. Applications can install, change or modify flow rules in the data plane, therefore security mechanisms such as authentication and authorization are used for applications that can change the flow rules in the data plane. FortNox [21] enables the controller to check contradictions in flow rules generated by applications. FlowCchecker [22] identifies inconsistencies in the flow rules in the data plane switches. Multiple controllers proposed for the controller resilience also help the data plane elements work if one controller fails to provide flow rules for newly arrived traffic flows.

4.4 Security in SDN-based Mobile Networks

The current version of SDN, that is the OpenFlow, operates on traffic flows. A flow can be a number of packets with the same characteristics, for example same TCP connection, or packets with a particular MAC or IP address. Operating on flows has been shown to be much more feasible in terms of control and granularity. The basic operation on flows is such that OpenFlow has three main entities as explained for the concept of SDN. These are:

1) *OpenFlow applications*: SDN application plane;
2) *OpenFlow controllers*: the SDN control plane; and
3) *OpenFlow Switches*: the SDN data plane.

The OpenFlow switches are dumb data path elements that forward packets between ports based on the instructions installed in their flow tables by the controller. The OpenFlow switch has three basic elements:

1) a flow table with actions associated with each flow;
2) a secure channel to the controller; using
3) an OpenFlow protocol that provides an open and standard mechanism for the controller to communicate with the switch [22,23].

When a new flow arrives, the switch checks its flow table for a matching entry. If there is no matching entry, the switch forwards it to the controller. The controller installs a matching entry in the switch flow table. Henceforth, when flows arrive at the switch, the switch checks its flow tables and acts accordingly. The flow tables have basically three types of actions for the packets. First, forward the flow to a given port as enlisted in the matching flow entry in the table. Second, encapsulate and forward the flow to the controller. Third, drop the flow's packets. This makes security services rather simple in SDN and forms the basis of security in future technologies:

- *Flow sampling*: is the selection of packets or packet header fields through various algorithms for analysis. Selected samples can be sent to security applications or systems to analyze the content of the flow and verify security threats or vulnerabilities. Basic analysis targets can be the content of the flow packets or header fields, frequency of particular types of packets, and inter-arrival times of packets with different characteristics. In SDNs, flow sampling can be as easy as changing the output port numbers and counters in the flow tables of the switch. The destination on that port can be a security system and the counter can show the number of packets to be sent to that destination.

In the following sections, we elaborate how the concepts of SDN can be used to provide robust security for mobile networks.

4.4.1 Data Link Security

Data link security is necessary to ensure that the data flows between the authorized endpoints and is not diverted or intercepted while in transit. The previous generations, that is, 3G and 4G, did not provide cryptographic integrity to user plane communication. In 5G, it will be a major security concern and will expose private communication not only

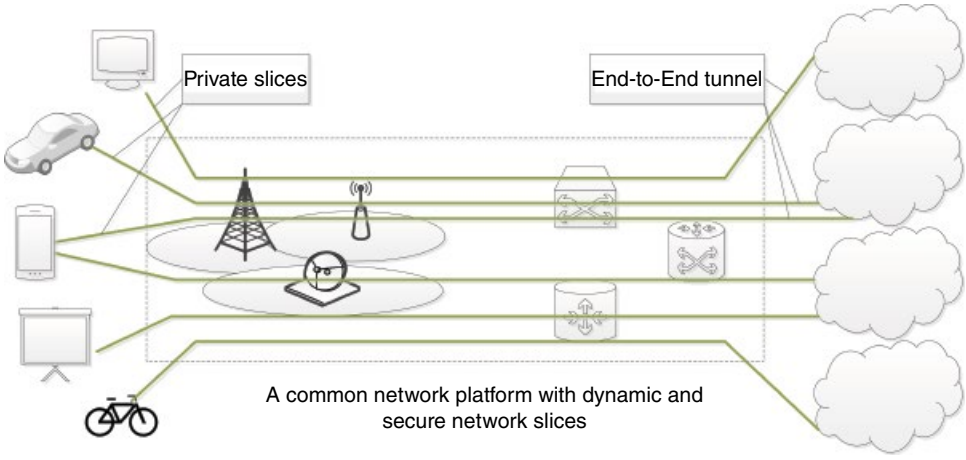

Figure 4.4 Secure network slices for different services.

between users but between devices carrying sensitive information such as data of health care systems and other critical infrastructures. Therefore, new mechanisms are needed to secure the data communication between users and devices. The OpenFlow protocol supports Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). TLS is used to provide privacy and data integrity for the communication between users. DTLS is used to secure data between communicating applications, mainly UDP traffic. These technologies use symmetric cryptography for data encryption. The TLS protocol is composed of two layers, that is, the TLS record protocol and the TLS handshake protocol. The Record Protocol guarantees connection privacy and reliability by means of data encryption. The TLS Handshake protocol authenticates the communicating parties with each other and negotiates the encryption algorithm and cryptographic keys before transmitting the first packet of an application.

Besides the use of TLS and DTLS, virtual networking or network slicing can be used to provide private communication channels for both data and control information, as shown in Figure 4.4. Slicing can also provide isolation-based data integrity and privacy. Slices of individual users can be separated by a networking hypervisor such as the FlowVisor [11]. Traffic isolation can be used to protect one type of traffic from another to strengthen the confidentiality and integrity of user traffic [43]. Hence, the Open vSwitch platform provides isolation in multi-tenant environments and during mobility across multiple subnets [44]. The OpenFlow Random Host Mutation (OF-RHM) [45] technique is proposed to avoid scanning attacks on end-hosts. Using the moving target defense (MTD) technique, the OF-RHM mutates IP addresses of end-hosts to avoid scanning attacks. The VAVE [14] platform validates the source addresses of all incoming packets to prevent data from being spoofed or forged through the OpenFlow interface attached to legacy devices.

4.4.2 Control Channels Security

Control channels carry the important control information between user and network, and among network entities.

Mutual authentication and key agreement between the UE and the network is important in many aspects, the most important being the identity insurance of the UE. In LTE, the UE and the network, or its entities such as the Mobility Management Entity (MME), perform mutual authentication through the Evolved Packet System (EPS) Authentication and Key Agreement (AKA), known as the EPS AKA. The EPS AKA is secure enough and has no visible vulnerabilities demonstrated so far [47]. When a UE connects to the EPC through the non-3GPP access network, the UE is authenticated through the AAA server. For trusted non-3GGP access networks, the UE and AAA server use Extensible Authentication Protocol-AKA (EAP-AKA) or improved EAP-AKA for authentication. For mistrusted non-3GPP access networks, the UE uses the evolved packet data gateway (ePDG) IPsec tunnel establishment to connect to the EPC [49]. Such control channels, besides being secure, have the following benefits [47]:

- The messages are short compared to other authentication protocols.
- It requires only one handshake between the UE and serving network, and between the serving and home networks.
- The HSS is updated through the serving network, thus is capable of handling many requests.
- The symmetric-key-based protocol makes the computations required in the authentication center (part of the HSS), and in the USIM (Universal Subscriber Identity Module) very efficient compared to public-key-based mechanisms. However, the advantages of the use of public-key based authentication and key agreement schemes could include that the home network does not need to be contacted for each authentication.

It is expected that in 5G there will be multiple control points in a network, which will require security of the control channels among those control points. For example, the concepts of SDN will be used for the benefits described in the previous sections. Thus, multiple controllers will be used for higher availability and scalability. Therefore, the control channels among the controllers must be secured. Similarly, the control channel between SDN controller and SDN switches must also be secured. The OpenFlow variant of SDN uses TLS, in which identification certificates are properly checked in either direction and allow encrypting the control channel in order to secure it and prevent it from eavesdropping. Furthermore, multiple control channels (associations) between switches and controllers are suggested to avoid the chances of services outages due to connection failures. The latest OpenFlow specifications support multiple connections between switches and controllers to improve network resilience in case of link failures. Therefore, fast link restoration mechanisms and backup entries with different priorities in the OpenFlow switches have been proposed and demonstrated in [49]. The backup links are computed by the controller and the traffic is switched to the backup link upon failure of the existing link. Similarly, flow entry migration techniques are proposed in [51] to reinstate a flow within 36 ms. This mechanism fulfills the carrier grade recovery requirement of 50 ms. Furthermore, HIP-based [52] secure control channels between the switches and the controllers are also proposed [53].

Moreover, IPsec is the most commonly used security protocol to secure the communication channels in current telecommunication networks such as 4G-LTE [55]. Thus, novel IPsec-based communication architectures were designed to secure control and data channels of 5G [56]. The proposed architecture use distributed Security

Gateways (SecGWs) to secure the controller and IPsec Encapsulating Security Payload (ESP) Bounded-End-to-End-Tunnel (BEET) mode tunnels to secure the control and data channels communication. Moreover, the Identity-Based Cryptography (IBC) protocol-based security mechanism is also proposed to secure the inter-controller and control channel traffic in a general multi-controller SDN networks [58].

4.4.3 Traffic Monitoring

Traffic monitoring can be used to detect intrusions and prevent them. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) observe network traffic according to different security policies, find vulnerabilities, threats and attacks, and use countermeasures to secure the network. In traditional networks, the control planes of network elements are loosely coupled with limited communication between their control planes. Hence, IDS and IPS technologies in each network domain are independently configured to deal with the challenges in its domain. This makes the current systems hard to update with newly identified types of attacks and threat vectors. SDN takes a different path by enabling applications to retrieve switch statistics or extract samples of packets from flows for security analysis. After security analysis, the applications can direct the controller to either drop the packets or forward them to security systems or middle boxes for further investigation. Therefore, SDN makes traffic monitoring rather simple by enabling global visibility of the network traffic behavior and network programmability.

4.4.4 Access Control

Traditional access control mechanisms use firewalls deployed on network boundaries to examine the incoming or outgoing packets to prevent attacks and unauthorized access. Therefore, insiders are considered as trusted partners. This can lead to serious security breaches, since in-zone users could launch attacks or circumvent the security mechanisms. Furthermore, the changes in network policies and traffic conditions require complex configuration of the firewalls, that make it further complex to keep the security in place. SDN enables automation through programmability and centralizes the network control that achieves global visibility of the network traffic behavior. Thus, traffic coming from the outside and traffic originated inside the network can be easily monitored. For example, the network ingress ports in OpenFlow switches can be dynamically configured from the controller to forward packets to a firewall in a separate middle box or an SDN firewall application. Similarly, traffic originating within the network can also be easily checked by updating the flow tables of the switch, in the same way as traffic coming from outside of the network. A number of firewall applications are already developed for SDNs, such as FLOWGUARD [24] and OpenFlow firewall [25].

4.4.5 Network Resilience

Network resilience mechanisms help the network to operate in the presence of diverse challenges, such as cyber-attacks, wrong configurations, operational overload, or equipment failures. The network must be capable to provide services to users when such challenges occur. Basic resilience strategies include Defend, Detect,

Remediate, Recover, Diagnose and Refine (D^2R^2 +DR) [26]. Through global visibility and a cycle of harvesting intelligence from the underlying network, the SDN control plane stays updated of the network situation. With programmable APIs in network equipment, fast reaction to failures in network equipment and miss-configuration is achieved. SDN-based resilience frameworks are developed that provide policy-controlled management with policy-based network configuration according to resilience strategies. An OpenFlow application is presented in [27] to enable interaction between multiple resilience mechanisms. The framework described in [27] also enables translation of high-level policies to device level configuration to act promptly to various failures. Other approaches include using multiple controllers to increase resilience of the SDNs.

4.4.6 Security Systems and Firewalls

To explain the possibilities of anomalies due to applications, consider the already existing example. Cellular network applications and middleboxes are independently managed by cellular operators and application developers. Application developers are unaware of the middlebox policies enforced by the operators. The operators have less knowledge of the application behavior and requirements. Such a mismatch or lack of understanding can create potential security challenges. For example, an operator can set an aggressive timeout value to quickly release the resources occupied by inactive TCP connections in the firewall. This could cause frequent disruptions in important application sessions [28].

Normally traffic is routed to various middleboxes to perform network security evaluation or check the traffic behavior and legality. However, the traditional middleboxes have a number of challenges regarding its placement, scalability and security policy alteration. These challenges mostly occur due to complex manual configurations, the need of path-specific middlebox placement, and non-flexibility of the existing network architectures [29]. SDN makes the deployment of middleboxes simple and elegant through network programmability and centralized network control. In [30], it is proposed to integrate the processing of middleboxes into the network itself, by using the concepts of SDN for policy consistency and higher visibility of the behavior of middleboxes through a centralized control. The simplicity of deploying and managing diverse and complex middleboxes, due to the above-mentioned characteristics of SDN, is presented in [31].

4.4.7 Network Security Automation

Automation is the process of minimizing human-machine interaction by delegating complex control functions to machines for reliability and accuracy. The main purpose of machine execution of complex functions, called automation, is accuracy and reliability through:

i) information acquisition;
ii) information analysis;
iii) decision and action selection; and
iv) action implementation [37].

However, automation has been used in a limited variety of networks even though human errors cause many network security and traffic management problems [35]. In today's multi-vendor networks, 62% of network downtime comes from human errors and 80% of corporations' IT budget is spent on maintenance and operations [36]. Stable and robust security policy deployment requires global analysis of policy configuration of all the networked elements to avoid conflicts and inconsistency in the security procedures and to diminish the chances of serious security breaches and network vulnerabilities [33]. As a security concern, a small oversight can lead to a global security problem such as placing a significant functionality on an unreliable system [34]. Therefore, automation of network and user security is highly important to avoid these challenges.

However, there are many challenges that make it difficult to automate and deploy automated security systems in today's communication networks. For example, most of the network systems used today are hardwired with specific control logic that require manual configuration of individual boxes. Such independent control systems in communication networks make it difficult to deploy consistent network-wide security policies throughout large networks that comprise a mix and match of control systems for different functionalities. Therefore, there are many proposals for the redesign of the communication systems and architectures.

Network security is an important and integral part of the network management that must be considered from planning to the deployment and use of the network [32]. Similarly, consistent policies over the network are highly important to avoid policy collusion that lead to security lapses. Among the proposals for such networks, SDN enables consistent network-wide policies through global visibility of the overall network systems and the policies implemented in each. By enabling programmability, and abstracting away the low-level configurations from individual boxes, SDN provides designing languages and network controllers that are capable of automatically reacting to the changing network state [38,39]. By abolishing the need of individual node configuration, taking the intelligence out of the networking components used to forward data and abstracting the control from the networking nodes, SDN paves the way for network security automation [40]. SDN enhances the automation of many processes and procedures, including physical and virtual network management and reconfiguration, and introduces the possibility of deploying new automated services. As a result, there are already several proposals for network automation using the concepts of SDN.

Procera [41] is a network control framework for operators, which implements flexible policies based on the network view. Procera maps high-level event driven policies to low-level network configuration driven policies, thus abolishing the need for manual configurations. The OpenFlow Management Infrastructure (OMNI) [42] simplifies OpenFlow management and provides mechanisms for a responsive autonomic control platform. Among the set of tools provided by OMNI, a web interface for the tools and a multi-agent system to autonomously control the network, OMNI tools for collecting statistics of flows and another that probes the network to obtain the physical topology, can be used for synchronizing the network traffic with the network security policies. The flows can be migrated to different physical paths according to the QoS and security requirement and without packet loss or security compromises. Using new technologies such as mentioned above, security systems can be automated in 5G.

Since the number of devices connected in 5G will be huge (the latency requirements will be strict that will require quick threat detection and faster response) security automation will be the need. Global visibility of the entire network behavior will enable quick threat detection and network programmability will enable faster threat mitigation. Since these features will be brought about by SDN, SDN-based automation will be highly valuable in 5G networks.

4.5 Conclusions and Future Directions

5G should be designed to provide more options of security beyond the currently used node-by-node security systems. It must provide more security than 4G and enable specific security designs for use cases that have specific requirements such as low latency, small cell sizes, and radio constraints. Sound security technologies and solutions must be built into the architecture of 5G from the beginning. This requires proper analysis of existing and future security threats to develop futuristic security solutions for 5G. New technologies will be integrated into the 5G ecosystem that requires new solutions for security as well. Flexible and agile technologies should be the core of network designs that enable adaptation not only to the service requirements but its security also.

The architectural limitations of current networks must not propagate to the future networks. The main limitation is the inflexibility of current networks due to its proprietary and closed nature. Such limitations make it difficult to deploy and use novel mechanisms and technologies when the need arises. These needs may be due to changes in user or business requirements, new service models or the limitations in the technology itself growing beyond its meaningful use. The concepts of SDN and NFV enable quick network updates, smoothen deployment of new technologies and services, and enable parallel deployment of old and new technologies and services. Being programmable in nature, these technologies also open the networking arena for innovation. This is the reason that new security systems and services are already developed by the industry, academia, and individuals working on open source projects.

However, enabling programmability of networking components is not entirely risk free in environments such as envisioned by 5G. For example, the critical infrastructure connected by 5G networks must be secured from malicious programs and access to programmable APIs in critical infrastructure for users or third-party developers must be constrained.

Network security has been rarely researched in parallel to network load balancing. It is extremely important in SDN-based mobile networks to develop load balancing architectures that work according to network security policies and vice-versa. For example, load balancing technologies can be used to avoid the saturation attacks. Similarly, security lapses of the controller can introduce delays in setting flow rules in the switches, leading to congestion in switches with unsolicited traffic flows. Therefore, it is necessary to consider network security in parallel with network traffic load balancing technologies in SDN-based mobile networks.

Most of the IoT devices will be constrained by capacity. Therefore, various types of wireless networking technologies are proposed having different cell sizes, differing architectures and heterogeneous infrastructures to perform functions on behalf of

constrained IoT devices. However, these devices can also easily become potential weak points for the networks. It is important to keep this limitation in mind while integrating networks of vulnerable IoT devices to the mainstream cellular or communication networks. Since these devices can easily be compromised to launch a DoS attack, it is necessary to either segregate them or use virtualization technologies so that they do not induce security vulnerabilities into the main network.

4.6 Acknowledgement

This work has been carried out under the projects SECURE-Connect (Secure Connectivity of Future Cyber-Physical Systems) and the Naked Approach Project (The Naked Approach Nordic perspective to gadget-free hyper connected environments).

References

1 Agiwal, M., Roy, A. and Saxena, N. (2016) Next generation 5G wireless networks: A comprehensive survey. In: *IEEE Communications Surveys & Tutorials*, 18(3), 1617–1655.
2 Kutscher, D. (2016) I's the network: Towards better security and transport performance in 5G. *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, San Francisco, CA, pp. 656–661.
3 Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M. and Gurtov, A. (2017) 5G security: Analysis of threats and solutions. *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, Helsinki, pp. 193–199.
4 Alliance, N.G.M.N. (2015) 5G white paper. *Next Generation Mobile Networks*.
5 Liyanage, M., Ylianttila, M. and Gurtov, A. (eds) (2015) *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*. John Wiley & Sons, USA.
6 ITU Telecommunication *Standardization Sector (*2003*) Security Architecture for Systems Providing End-to-end Communications*. Geneva, Switzerland.
7 Alliance, N.G.M.N. (2016) 5G security recommendations Package, White paper.
8 Casado, M., Koponen, T., Ramanathan, R. and Shenker, S. (2010) Virtualizing the network forwarding plane. *Proceedings of the Workshop Programme*. Routers Extensible Serv. Tomorrow, p. 8.
9 van Cleeff, A., Pieters, W. and Wieringa, R. (2009) Security implications of virtualization: A literature study. *Proceedings of the International Conference CSE*, 3, 353–358.
10 Vaughan-Nichols, S. (2008) Virtualization sparks security concerns. *Computer*, 41(8), pp. 13–15.
11 Sherwood, R. *et al*. (2009) Flowvisor: A network virtualization layer. *OpenFlow Switch Consortium*, Technical Report OPENFLOW-TR-2009-1, Stanford University, Stanford, CA.
12 Chung, C.-J., Khatkar, P., Xing, T., Lee, J. and Huang, D. (2013) NICE: Network intrusion detection and countermeasure selection in virtual network systems. *IEEE Trans. Dependable Secure Computing*, 10(4), 198–211.
13 Kreutz, D., Ramos, F. and Verissimo, P. (2013) Towards secure and dependable software-defined networks. *Proceedings of the 2nd ACM SIGCOMM Workshop. Hot Topics Software Defined Networks*, pp. 55–60.

14 Iwamura, M. (2015) NGMN view on 5G architecture. In: *Vehicular Technology Conference (VTC Spring)*, 81st Proceedings of the IEEE, pp. 1–5.

15 Nokia (2016) Signaling is growing 50% faster than data traffic [Online]. Available at: https://blog.networks.nokia.com/mobile-networks/2012/12/05/a-signaling-storm-is-gathering-is-your-packet-core-ready/ [accessed June 2017]. Published December 2012.

16 Zhou, X., Zhao, Z., Li, R. *et al*. (2014) Toward 5G: When explosive bursts meet soft cloud. *Network, IEEE*, 28(6), 12–17.

17 Ahmad, I., Namal, S., Ylianttila, M. and Gurtov, A. (2015) Security in software defined networks: a survey. *IEEE Communications Surveys & Tutorials*, 17(4), 2317–2346.

18 Sezer, S. *et al*. (2013) Are we ready for SDN? Implementation challenges for software-defined networks. *IEEE Communications Magazine*, 51(7), pp. 36–43.

19 Security-Enhanced Floodlight (2013) SDx Central, Sunnyvale, CA. [Online]. Available at: http://www.sdncentral.com/education/towardsecure-sdn-control-layer/2013/10/

20 Switch, B. (2012) Developing floodlight modules. Floodlight OpenFlow controller. [Online]. Available at: http://www.projectfloodlight.org/ floodlight/

21 Porras, P, Shin, S., Yegneswaran, V., Fong, M., Tyson, M. and Gu, G. (2012) A security enforcement kernel for OpenFlow networks. *Proceedings of the 1st ACM Workshop on Hot Topics in Software Defined Networks*, pp. 121–126.

22 Al-Shaer, E. and Al-Haj, S. (2010) FlowChecker: Configuration analysis and verification of federated OpenFlow infrastructures. *Proceedings of the 3rd ACM Workshop on Safe Configuration*, pp. 37–44.

23 McKeown, N, Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L. *et al*. (2008) OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 38(2), 69–74.

24 Hu, H., Han, W., Ahn, G.J. and Zhao, Z. (2014) FLOWGUARD: building robust firewalls for software-defined networks. *Proceedings of the 3rd ACM Workshop on Hot Topics in Software Defined Networking*, pp. 97–102.

25 OpenFlow Firewall: A Floodlight Module. [Online]. Available at: http:// www.open flowhub.org/display/floodlightcontroller

26 Sterbenz. J.P. *et al*. (2010) Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8), 1245–1265.

27 Smith, P., Schaeffer-Filho, A., Hutchison, D. and Mauthe, A. (2014) Management patterns: SDN-enabled network resilience management. *Proceedings of the IEEE NOMS*, pp. 1–9.

28 Wang, Z., Qian, Z., Xu, Q., Mao, Z. and Zhang. M, (2011) An untold story of middleboxes in cellular networks. *Proceedings of the ACM SIGCOMM Conference (SIGCOMM 2011)*. ACM, New York, pp. 374–385.

29 Joseph, D.A., Tavakoli, A. and Stoica, I. (2008) A policy-aware switching layer for data centers. *Proceedings of the ACM SIGCOMM*, New York, pp. 51–62.

30 Lee, J., Tourrilhes, J., Sharma, P. and Banerjee, S. (2010) No more middlebox: Integrate processing into network. *ACM SIGCOMM Computer Communication Review*, 40(4), 459–460.

31 Gember, A., Prabhu, P., Ghadiyali, Z. and Akella, A (2012) Toward software-defined middlebox networking. *Proceedings of the 11th ACM Workshop HotNets-XI*, pp. 7–12.

32 Casado, M., Freedman, M.J., Pettit, J., Luo, J., McKeown, N. and Shenker, S. (2007) Ethane: Taking control of the enterprise. *ACM SIGCOMM Computer Communication Review*, 37(4), 1–12.

33 Hamed, H. and Al-Shaer, E. (2006) Taxonomy of conflicts in network security policies. *IEEE Communications Magazine*, 44(3), 134–141.

34 Creery, A. and Byres, E. (2005) Industrial cybersecurity for power system and SCADA networks. *Petroleum and Chemical Industry Conference. Proceedings of the IEEE 52nd Annual Industry Applications Society*, pp. 303–309.

35 Luo, J, Pettit, J., Casado, M., Lockwood, J. and McKeown, N. (2007) Prototyping fast, simple, secure switches for ethane. *Proceedings of the 15th Annual IEEE Symposium on High-Performance Interconnects HOTI*, pp. 73–82.

36 Casado, M., Freedman, M.J., Pettit, J., Luo, J., Gude, N. *et al*. (2009) Rethinking enterprise network control. *IEEE/ACM Transactions on Networking (TON)*, 17(4), 1270–1283.

37 Parasuraman, R., Sheridan, T.B. and Wickens, C.D. (2000) A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 30(3), 286–297.

38 Kim, H. and Feamster, N. (2013) Improving network management with software defined networking. *IEEE Communications Magazine*, 51(2), 114–119.

39 Shenker, S. *et al*. (2011) The future of networking, and the past of protocols. *Open Networking Summit*.

40 Ortiz Jr., S. (2013) Software-defined networking: On the verge of a breakthrough? *Computer*, 46(7), 10–12.

41 Voellmy, A., Kim, H. and Feamster, N. (2012) Procera: a language for high-level reactive network control. *Proceedings of the ACM 1st Workshop on Hot Topics in Software Defined Networks*, pp. 43–48.

42 Mattos, D.M., Fernandes, N.C., da Costa, V.T., Cardoso, L.P., Campista, M E.M. *et al*. (2011) Omni: OpenFlow management infrastructure. *International Conference of the IEEE on Network of the Future (NOF)*, pp. 52–56.

43 Gutz, S., Story, A., Schlesinger, C. and Foster, N. (2012) Splendid isolation: A slice abstraction for software-defined networks. *Proceedings of the 1st Workshop HotSDN*, pp. 79–84.

44 Pfaff, B, Pettit, J., Amidon, K., Casado, M., Koponen, T. and Shenker, S. (2009) Extending networking into the virtualization layer. *Proceedings of Hotnets*, pp. 1–6.

45 Jafarian, J.H., Al-Shaer, E. and Duan, Q. (2012) OpenFlow random host mutation: transparent moving target defense using software defined networking. *Proceedings of the 1st Workshop Hot Topics Software Defined Networks*, pp. 127–132.

46 Wang, C.X., Haider, X. Gao, A., You, X.H., Yang, E. *et al*. (2014) Cellular architecture and key technologies for 5g wireless communication networks. *IEEE Communications Magazine*, 52(2), 122–130.

47 Schneider, P. and Horn, G. (2015) Towards 5G Security. *IEEE Trustcom/BigDataSE/ISPA*, Helsinki, pp. 1165–1170.

48 Piqueras Jover, R. (2013) Security attacks against the availability of LTE mobility networks: Overview and research directions. *Proceedings of the 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*. Atlantic City, NJ, pp. 1–9.

49 Cao, J., Ma, M., Li, H., Zhang, Y. and Luo, Z. (2014) A survey on security aspects for LTE and LTE-A Networks. *IEEE Communications Surveys & Tutorials*, 16(1), 283–302.

50 Sgambelluri, A., Giorgetti, A., Cugini, F., Paolucci, F. and Castoldi, P. (2013) Effective flow protection in OpenFlow rings. *Proceedings of the OFC/NFOEC*, pp. 1–3.

51 Li, J., Hyun, J., Yoo, J.-H., Baik, S. and Hong, J.-K. (2014) Scalable failover method for data center networks using OpenFlow. *Proceedings of the IEEE NOMS*, pp. 1–6.

52 Nikander, P., Gurtov, A. and Henderson, T (2010) Host Identity Protocol (HIP): Connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks. *IEEE Communications Surveys & Tutorials*, 12(2), 186–204.

53 Namal, S., Ahmad, I., Gurtov, A. and Ylianttila, Y. (2013) Enabling secure mobility with OpenFlow. *IEEE SDN for Future Networks and Services (SDN4FNS)*, Trento, pp. 1–5.

54 Liyanage, M., Abro, A.B., Ylianttila, M. and Gurtov, A. (2016) Opportunities and challenges of software-defined mobile networks in network security perspective. *IEEE Security and Privacy*, 14(4), 34–44.

55 Bikos, A.N. and Sklavos, N. (2013) LTE/SAE security issues on 4G wireless networks. *IEEE Security and Privacy*, 11(2), 55–62.

56 Liyanage, M., Braeken, A., Jurcut, A.D., Ylianttila, M. and Gurtov, A. (2017) Secure communication channel architecture for software defined mobile networks. *Elsevier Journal on Computer Networks (COMNET)*, 114, 32–50. Available at: http://dx.doi.org/10.1016/j.comnet.2017.01.007. (http://www.sciencedirect.com/science/article/pii/S1389128617300075)

57 Liyanage, M., Ylianttila, M. and Gurtov, A. (2014) Securing the control channel of software-defined mobile networks. *Proceedings of the IEEE 15th International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Sydney, Australia.

58 Lam, J-H., *et al*. (2015) Securing distributed SDN with IBC. *Seventh International Conference on Ubiquitous and Future Networks*. IEEE