Mobile Netw Appl
DOI 10.1007/s11036-015-0665-5

Software-Defined Mobile Networks Security

Min Chen[1] · Yongfeng Qian[1] · Shiwen Mao[2] · Wan Tang[3] · Ximin Yang[3]

Abstract The future 5G wireless is triggered by the higher demand on wireless capacity. With Software Defined Network (SDN), the data layer can be separated from the control layer. The development of relevant studies about Network Function Virtualization (NFV) and cloud computing has the potential of offering a quicker and more reliable network access for growing data traffic. Under such circumstances, Software Defined Mobile Network (SDMN) is presented as a promising solution for meeting the wireless data demands. This paper provides a survey of SDMN and its related security problems. As SDMN integrates cloud computing, SDN, and NFV, and works on improving network functions, performance, flexibility, energy efficiency, and scalability, it is an important component of the next generation telecommunication networks. However, the SDMN concept also raises new security concerns. We explore relevant security threats and their corresponding countermeasures with respect to the data layer, control layer, application layer, and communication protocols. We also adopt the STRIDE method to classify various security threats to better reveal them in the context of SDMN. This survey is concluded with a list of open security challenges in SDMN.

Keywords Software defined mobile network (SDMN) · OpenFlow · Network function virtualization (NFV) · Security

1 Introduction

With the expected drastic increase in mobile traffic demand [1, 2], and the compelling needs for provisioning of elastic service, collaborative working capability [3, 4], transmission speed, and quality of service (QoS) [5, 6], as well as, the requirement for costly network upgrades [7, 8], Software Defined Mobile Network (SDMN) has been recognized as a solution to meet these challenges. SDMN is an integration of cloud computing, Network Function Virtualization (NFV), and Software Defined Network (SDN). In SDMN, emerging network technologies such as SDN and NFV are integrated into the mobile network architecture in order to meet its ever-changing demand. To be more specific, at the core of SDMN, the software control aims to enable dynamic traffic management and functional reconfiguration. Instead of conventional static IP based networking structure, the backbone network is abstracted through traffic-based NFV in SDMN. In a front haul connection, the network capability and QoS are improved through centralized management of wireless radio spectrum resources [9] and the implementation of Software-Defined

✉ Yongfeng Qian
yongfeng.hust@gmail.com

✉ Min Chen
minchen@ieee.org

Shiwen Mao
smao@ieee.org

Wan Tang
tangwan@scuec.edu.cn

Ximin Yang
yangximin@scuec.edu.cn

[1] Embedded and Pervasive Computing Lab, School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China

[2] Department of Electrical & Computer Engineering, Auburn University, 200 Broun Hall, Auburn, AL, 36849-5201, USA

[3] College of Computer Science, South-Central University for Nationalities, Wuhan 430074, China

Published online: 09 January 2016

Radio (SDR), Cognitive Radio (CR) for reconfigurable networks [10].

With the development of SDMN [11], the related network security issues have drawn considerable attention [12–15]. The Open Networking Foundation (ONF) Security Discussion Group is committed to security study and standardization for SDN. For example, report TR-511 proposes a set of core security principles with implementation strategies regarding SDN core protocol OpenFlow Switch Specification v1.3.4 [16]. In [17], a comprehensive survey of software-defined networking is provided, covering its context, rationale, main concepts, distinctive features, and future challenges. It also provides a detailed summary of SDN network security issues, including the point of attack, means of attack, and countermeasures. However, the security problems related to SDMN have not yet been well analyzed.

Moving from SDN to SDMN, the increased complexity, due to the hybrid infrastructure, leads to multiple security requirements that must be satisfied. To guarantee the collaborative work capability between different access technologies and SDN-enabled network nodes, pure reliance on progressive upgrading of existing 3GPP solutions cannot develop the logic part. Stringent QoS requirements that dynamic service matching should be based on light and stable basic data and protocol of cryptosystem, but security solutions currently proposed have yet to solve this problem. Even as a leading SDN technology, the application of OpenFlow in the next generation of mobile network is still a challenging problem [17].

To this end, a network security threat model is critical, as it can identify and isolate, in a systematic way, the existing drawbacks and potential attack vectors. Without such an abstraction, the improvement of safety design will become more difficult and its inherent complexity cannot be reduced. Therefore, The network security threat model has become a prerequisite for standardization and practical implementation of SDMN [18]. A preliminary attempt is made in this paper towards this direction by the proposal of a STRIDE-based network security threat model [19, 20].

Security in SDMN is a challenging issue due to the large amount of smart devices and terminals in the SDMN, which are proactive for content fetching. The main considerations of security research include the existing problems of mobile networks [21] and the security vulnerabilities of SDN. On the one hand, the virtualization mechanism is flexibly managed; on the other hand, harmful behaviors will result from an unethical malicious intent. Therefore, in addition to typical security problems of mobile networks, additional security problems caused by the introduction of SDN and NFV cannot be ignored.

Based on the above considerations of SDMN security, this paper is structured as follows. Section 2 presents the main framework of SDMN, the corresponding OpenFlow protocol, and the NFV structure based on this framework. Section 3 reviews security problems of SDMN. The inherent security problems of SDN are introduced first, including the SDN architecture, the security problems, and the corresponding security principles brought about by SDN features. And then, special security problems of SDMN are discussed; Section 4 introduces the attacks and corresponding countermeasures in SDMN, with the STRIDE-based classification and analysis, as well as the security challenges of SDMN. Section 5 concludes this paper.

2 SDMN architecture

2.1 SDMN introduction

SDMN is a programmable, flexible and flow-centric mobile network constructed by using a combination of SDN, NFV, and cloud computing. SDMN is the architecture of embodiment and application extension of the idea that the control layer in an SDN is separated from the forwarding layer in a wireless network. The traditional mobile network has distinctive differences from an SDMN. The core of the software-defined mobile packet forwarding involves the problems of matching the sending/control layer and mobile environment [22–25], the service logic of mobile communication, which is transmitted to the cloud [26] to guarantee the programmability [27] of LTC/EPC structure inside, and the combination of SDN and NFV [28]. SDMN has many advantages, such as centralized control, high flexibility, effective division, automatic network management, and reduction of the backhaul device operating cost [29, 30].

2.2 SDMN architecture

SDMN is put forward as an extension of SDN, by adding the special functions of a mobile network. The SDN architecture is different from existing mobile networks with the flow-centric models [31, 32], integration of inexpensive hardware, and a centralized logic controller. Like SDN, SDMN consists primarily of three parts: data plane, control plane, and application plane [33]. Furthermore, SDMN integrates SDN, cloud computing [34], and NFV. The SDMN architecture is illustrated in Fig. 1.

2.2.1 NFV

NFV involves decoupling the network function from the hardware application by means of IT virtualization technology, which is implemented in and operates in software.

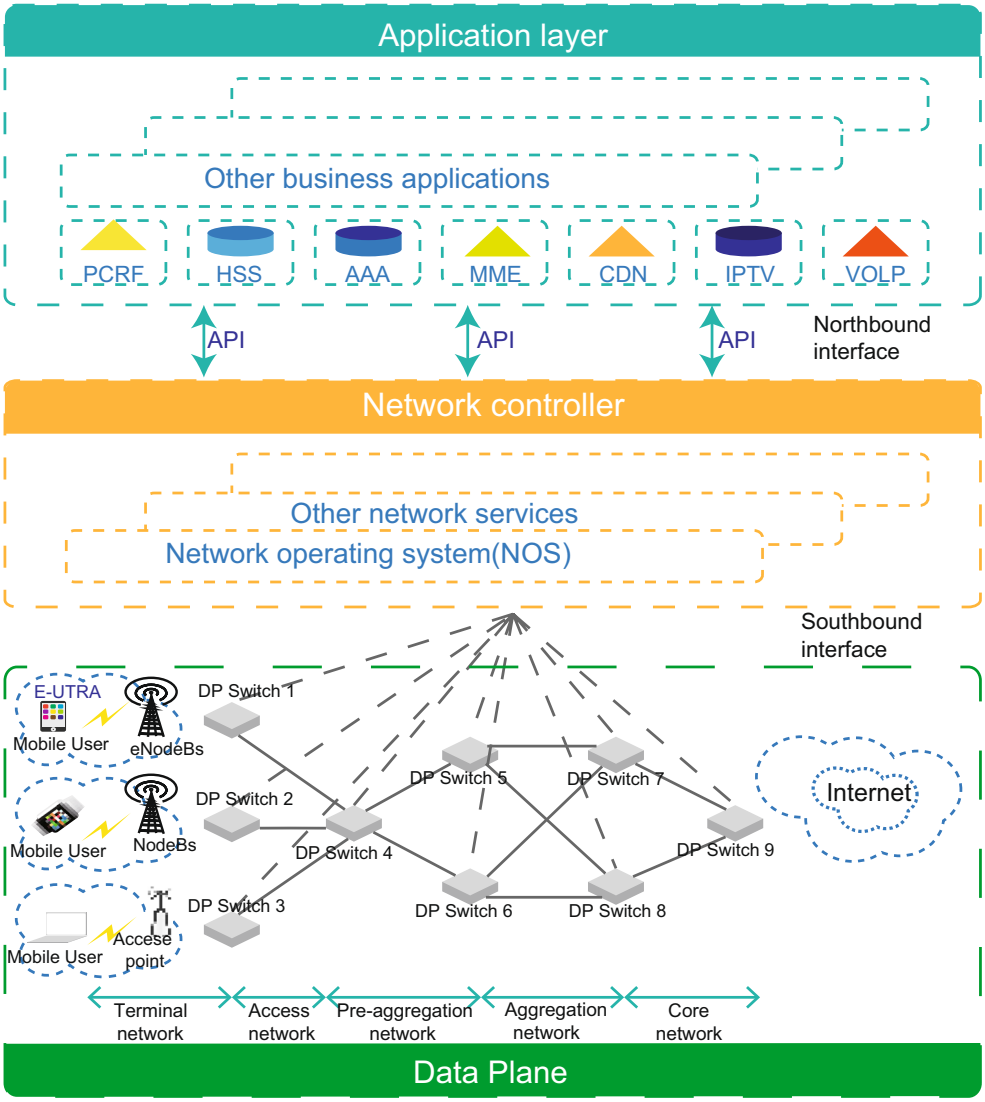

Fig. 1 Illustration of the SDMN architecture

This is an innovative method which is applied in the design and deployment [35] of the network management service. Network virtualization targets mainly the aggregation of distributed resources, utilizing a shared pool of configurable computing hardware resources to realize on-demand network access.

In accordance with the NFV-based LTE/EPC architecture as described by ETSI, Fig. 2 shows a reduced graph of NFV members [36]. In consideration of the complexity of the virtualization program segment, the threat model can further be subdivided into threats in relation to each NFV assembly/area, such as layout and Virtual Management Function (VMF)/Virtual Infrastructure Management (VIM), agency and resource management program, virtual network [37], service, transport layer, and telecommunication infrastructure areas. To be more specific, avoidance of original controller/traffic management logic, or disclosure of user control/data traffic is possible by attacking and concealing VMF/VIM/layout or other identities of VMF(MME,S/PG-W...) and tampering with virtual network communication traffic.

Malicious information and viruses are injected only through the ARP plane and a replay attack is implemented (a common vector of traditional IP environment); the malicious virtual machine (VM) mechanism can destroy normal service logic [37], on the condition that NFV communication traffic exits from a virtual line of defense [38, 39]. If VNF is operated on kernel-based VM, the threat of tampering with the integrity of the kernel will affect normal EPC status. Through kernel code and interface loopholes, the integrity of VNF will be damaged, causing DoS of potential NFVI assembly by loading LKM, rootkit malicious software without controlled data and by attacking resource depletion [40–42].

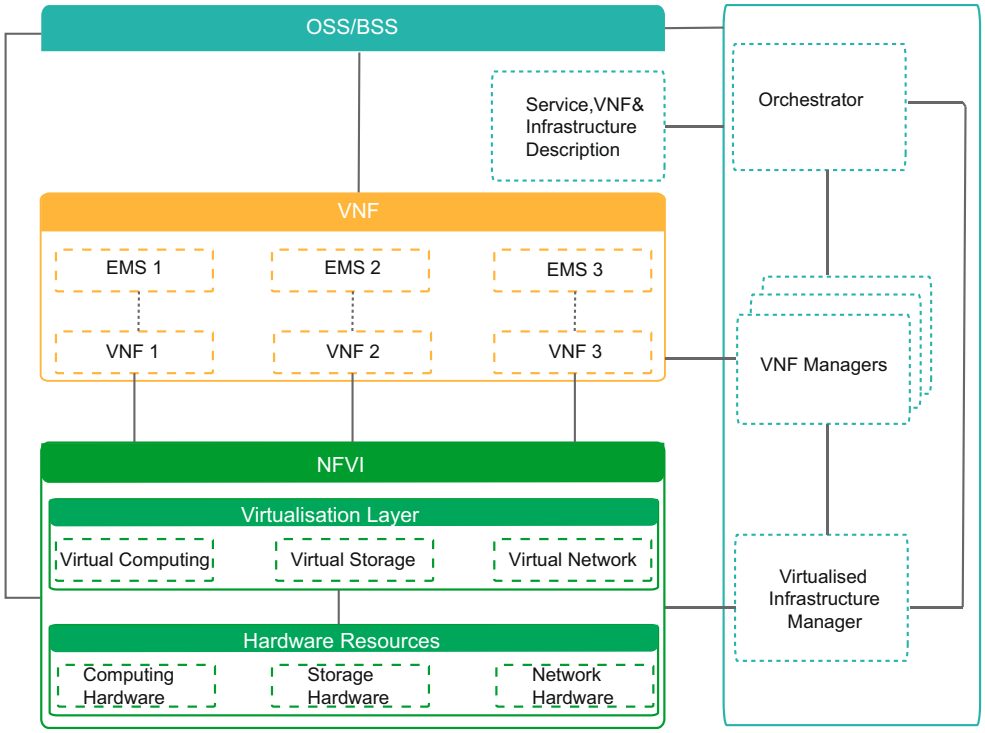

Fig. 2 Illustration of the NFV architecture

Because the IaaS user group shares the same address and cannot provide an ideal VM isolation, SDMN service transport in the IaaS region will enlarge the attack level, and may cause information disclosure, service denial and privilege escalation to occur [43]. Due to the malicious use of the VM's common address and the convergence of the same resources in the NFVI region, there will be a point where malicious software can form a brief existence or VM spread, causing the depletion of hardware resources and performance degradation of the EPC running in the NFVI region. It has been proven that a side channel VM attack can acquire plaintext passwords, keys and data memory [44, 45]. It may also be used for NFVI area fingerprint technology. The technology provides useful information for the launch of another SDMN target attack. For example, this may result in the service denial of physical infrastructure, causing the IaaS data center network to be usurped and attacked or to launch complex and continuous service denial attack [46, 47]. Similarly, VIM can be loaded into the module from an externally introduced transmission (E2E connect SDN controller) or service (NFVSDN controller) due to the presence of the host operating system (OS) simulation program weaknesses or cross the VM attack (e.g., escape and reflection attacks) attack, and there will be a threat of privilege escalation [48]. It should be pointed out that the NFV guidelines recommend using AAA and reliable communication solutions throughout the virtual area. However, it is not strictly controlled by the relevant mechanisms, and it will make the supplier adopt an incompatible security policy (which also refers to the key management procedures) in the specific configuration of the telephone communications and IaaS architecture. Also, in the case of OpenFlow, the convergence NFV program similar to the cloud computing concept of the IaaS model posts a technical threat, which is non-characteristic for the traditional mobile core environment.

NFV proposed a virtual firewall, traffic balance, and other L4–L7 network security applications. These applications are the virtualized network functions (VNF), which are used to meet the requirements of network communication and service management. In [49], the authors presented a framework of wireless network virtualization for 3GPP LTE mobile cellular networks, but there is no in-depth study of security issues. In [50] and [51], respectively, the authors proposed the 5G SDMN architecture which can effectively guarantee the E2E QoS and QoE, among which the NFV technology creates a variety of middle boxes, including the middle boxes providing security service in data encryption, firewalls and honeypots.

2.2.2 OPENFLOW

OpenFlow is a kind of open protocol, and it is proposed to standardize the communications between the data layer

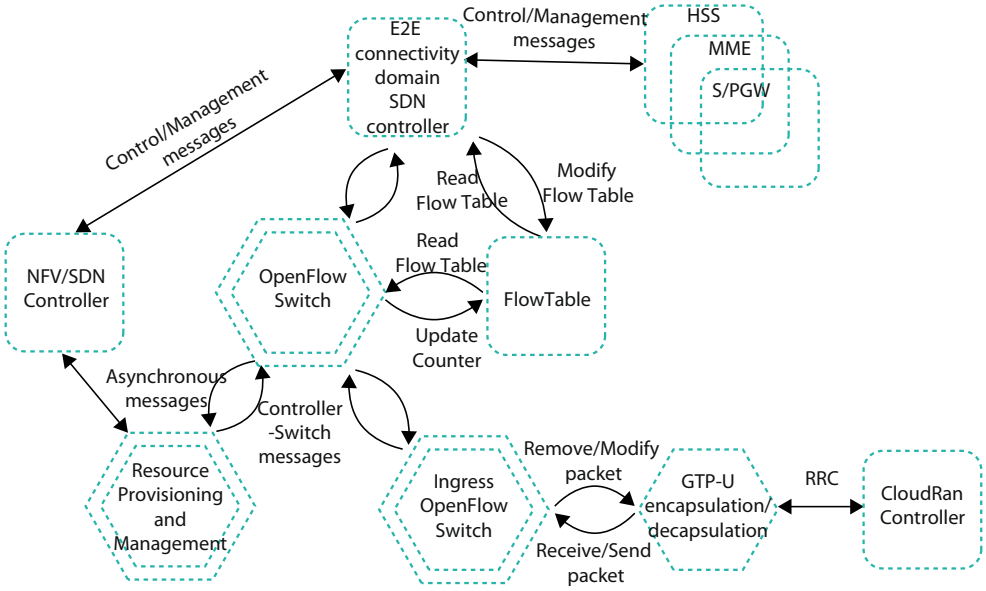

Fig. 3 Illustration of the OpenFlow architecture

and control layer. In accordance with the OpenFlow threat model described in [52], Fig. 3 shows partial, OpenFlow, simplified data flow diagrams in the SDMN architecture. In mobile networks, the assumption of using the TLS safety passage in the OpenFlow network and concrete cryptosecurity remains effective.

As far as threats and decoy attacks are concerned, the authors in [53] discussed the possibility of topological poison and attack or, in other words, a host address hijacking and link manufacturing attack. In consideration of the diversity of running operating servers in the NFV area of SDMN, HDS communication is made between the host hijacked SDN controller and the OpenFlow switch to provide the opportunity for the destroyed core server to hijack legitimate data and transfer information. Likewise, the LLDP protocol is used in a link manufacturing attack to inject forged internal links, and sensitive flow results in a deliberate weakening of the system processing QoS, or is used to launch attacks and cause server refusal.

Decoy attacks target the IP protocol address of the E2E/NFVSDN controller, resulting in a change/recognition of running traffic rules and avoidance of charge, safety or other mobile management policies. As network saturation and complete performance degradation is caused by the depletion of resources, the malicious host simply needs to disguise as acting SDN controller to cause partial traffic to circumvent overload control subsystem(OCS)/Policy and Charging Rules Function (PCRF), firewalls or other LTE/EPC control nodes, or copy/certain traffic of black holes, and thus, the legal interception mechanism may be destroyed.

The traffic unmatched to effective rules will lead to saturation of the OpenFlow plane and overflow of the transmission plane, and Distributed Denial of Service (DDoS) is detected in the real SDN controller as a result of the transmission mechanism's failure. Moreover, the malicious OpenFlow node may tamper counter and insert false communication to some users, circumventthe charge system and adopt incorrect rate/cost of the traffic [54]. Likewise, the entry of an OpenFlow router may become the target of the saturation attack so that the geological locations of some wireless mobile communication services can be shielded. Another tampering-related attack is a virus attack on the traffic platform or buffer memory in the controller status, which will keep the integrity of the SDMN OpenFlow topological structure.

For SDMN OpenFlow members, another information disclosure attack exists, in which the network fingerprint and controller data may be disclosed as a result of an XML external mechanism attack [55]. As mentioned above, the most convincible threat is denial of service (DoS) resulting from depletion of resources, link manufacturing, Hash collision attack, SDN controller overload and OpenFlow switch circuit disconnection, as shown in [52, 53, 55] and [56]. In general, some network security viewpoints indicate that security attributes in relation to OpenFlow technology and security problems of SDN [57] itself are the major security problems of SDMN.

3 SDMN security issues

Due to the unique characteristics, SDMN brings about many special secure issues. Ref. [16] describes the secure principles, which is supplemented and enhanced in this section.

3.1 SDN original security issues

Since SDMN is developed on the basis of SDN, we first introduce SDN and its related security problems before discussing SDMN security issues.

3.1.1 SDN architecture

The SDN architecture consists of the following key planes.

- Data plane (also known as the infrastructure layer): primarily consists of a data forwarding unit including physical switches and virtual switches for exchanging and forwarding data packets. We also categorize the physical mobile terminal as belonging in the data plane.
- Control plane: consists of a series of controllers providing centralized control. The Open API (application program interface) enables open switches data forwarding functions to realize the state collection and centralized control of the data plane.
- Application plane (also called application layer): provides various applications to end-users, such as mobile management, security application, network virtualization, etc. The mobile terminal applications are categorized into this plane.

3.1.2 Security problems due to several characteristics of SDN

The following security problems are inherit from SDN.

- Centralized control mode. Centralized management integrates the network configuration, network service access control, and service deployment at the control layer. Once the attacker controls the SDN successfully, it will cause the network service to be paralyzed, and therefore affect the entire network.
- Programmability. The programmability of SDN has brought about new security problems. The first is traffic and resource isolation. Due to this feature, there may be additional interaction to handle different SLAs and privacy issues. The second is the trust based on the third party applications and controller. Programmability is a double-edged sword. It brings about the convenience of implementation as well as the risk of malicious applications, so it is necessary to strengthen the authentication mechanism in the communications between the application and control layers to prevent controller exposure. The last issue involves the protection for the Application-Controller Plane Interface (A-CPI) and Intermediate-Controller Plane Interface (I-CPI).
- Integration with the existing protocols. When the existing protocols are applied to SDN, compatibility must be detected. At the same time, in the construction of the SDN architecture, the weakness of the existing architecture should not be repeated, or at least not inflated.
- Cross domain connection. SDN implementation requirements are infrastructures connected with different domains. This requires the establishment of trust relationship to guarantee secure channel setup.

3.1.3 Security principles

All the protocols, components, and interfaces in the SDN architecture should follow the following security Pprinciples [16].

- Clearly define security dependencies and trust boundaries. Security dependencies of different components should be described when these parts are constructed for the SDN network. Circular dependencies should be avoided. Based on privilege changes, information flow and data integrity and confidentiality through different domains cannot be verified. Trust boundaries of the data dependency relationship should be defined. Any external dependency should depict its trust boundary. Management of internal attacks should be considered to prevent an external environment attack.
- Assure robust identity. In order to establish effective authentication, authorization and accounting implementation, we must establish a strong identity framework. Robust identity should be able to distinguish its owner from other entities; and robust identity should be able to generated, updated, and revoked.
- Build security based on the open standard which gives priority to use the existing mechanisms, and provide the existing security mechanisms MD5 and SHA-1, which are not recommended.
- Protect the information security triad. We must consider the impact of safety control on the whole SDN architecture. Determining whether or not the effectiveness of the whole system may be reduced will be an effective method to evaluate the new control. This control should not introduce new vulnerabilities. The method which will reduce the effectiveness of core pillars should be certified or moderated. The establishment of security control should not cause an unnecessary decrease in system performance or increase in the complexity of the system. In practice, the security requirements, cost, etc. will affect the final solution of security control.

- Protect operational reference data. Incorrect information may result in the loss of confidentiality, integrity and availability of the system. However, the lack of specific sensitive data, such as the lack of a keyword, will breach the security control.
- Make systems secure by default. When the control is unable to meet the security requirements, such as deny by default, etc., we need to establish a different security level.
- Provide accountability and traceability. Based on log data, auditors can not only identify the action of the entity, but also find the correlation orders of the action.

In addition to the above seven safety guidelines, we also need to consider other control issues, such as the fact that security control must be able to be performed, maintained, and operated easily.

3.2 Special security issues in SDMN

Some security problems are brought about by the centralized control, resulting from the isolation between the data level and control level, and due to the specific architecture of SDMN under the cloud environment. Other than the characteristics of SDN, the combination of NFV and SDN has resulted in a series of security problems. Examples include OpenFlow, NFV, software defined fronthaul network security problems, and terminal problems, etc. For software defined fronthaul, a virtualized attack is a threat. In terms of Software-Defined Fronthaul (SDF) wireless programs, the threat to SDMN security is extended to the launch of the wireless medium and the recognition of attack surface [58]. Certain radio frequency interference, MAC tampering and malicious RF interference [59] can consistently adapt to the e-utran details and heterogeneous network environment, so that the radio program segment of the SDMN fronthaul can be regarded as the target of the attack [60, 61].

On the other hand, the software defined radio awareness [60] is associated with numerous STRIDE threats, as listed in [62, 63]. Considering the spectrum utilization method, the convergence of SDF program is vulnerable to be simulated by the primary user, Byzantine or spectrum sensing data operation/forgery and several DoS attacks [64–66]. Due to the development of collaborative malware attacks on smart mobile to LTERAN, the SDF program segment may provide stronghold for recursion/slow DDoS botnet attacks, considering that most of these attacks will tamper with the quality of service (QoS) scheduler, bandwidth requirements and the implementation process of the nano micro honeycomb base station [67–69].

Table 1 lists the main wireless network/SDN/SDMN, reviews the security issues involved, and provides the corresponding security criteria. In the table, "*" and "-" denote whether the domain specified in the column has been discussed in the survey or not. AL, CP, DP and CL represent the application layer, control plane, data plane, and communication layer, respectively.

4 SDMN security measures

In this section, we study the relationship between threat and security in the data layer, control layer, application layer and communication protocols.

4.1 Considering the security components of the SDMN architecture

In order to reduce SDMN attacks, there are a lot of solutions which attempt to protect the logic segment. An experiment involves SDN state processing and the use of the centralized virtualization management platform to integrate VNF and SDN logic program segments to provide a more comprehensive examination of the EPC/LTE network state, and to achieve cross domain anomaly monitoring and detection [75]. Similarly, cell-pot infrastructure coupled with intrusion / anomaly detection and protection solutions [76–79] can help to maintain real-time security of the SDMN control channel and to provide protection for the overall mobile target. In the background of strengthening the network defense cooperation and forensic tracking [80], the network edge can provide auxiliary shielding and prevent malicious software from launching an SDMN attack which would fail the solution [81–83].

As stated in [84], current SDN defense mechanisms can only provide limited SDMN security enhancements due to the lack of structural features associated with the movement. The same conclusion can also be applied to [85]. The SDMN virtualization of security, to a large extent, is still a design direction for the computer system structure, although the concept is in the experimental stage. The fundamental differences between service and infrastructure, whether in IaaS or in the RANaaS program, are the specific trust mechanism. Resource allocation, mobility management and the missing isolation scheme of the current virtual platform are necessary conditions. A good starting point for SDMN secure virtual direction is presented in [72], despite the fact that different schemes should be implemented to meet the different requirements of the core and fronthaul virtualization. In previous cases, the above mechanism may benefit from the guidance of safety and trust in the EPC/LTE core [84, 85], while in the later cases, it may benefit from the cloud operating security policy. The paper [70] defines the SDMN architecture, and the multitier method for SDMN is introduced. This method protects the network itself, as well as the user, based on the security question of different

Table 1 Feature table

Existing Work		Conventional Security Issues			SDN Security Issues				SDWN Security Issues		
		Firewall	IDS	IPS	AL	CP	DP	CL	Network Architecture	Communication Protocol	Mobile Terminal
2015	[70]	-	-	-	-	*	*	*	*	*	-
	[17]	-	-	-	*	*	*	*	-	-	-
	[6]	-	-	-	-	*	-	-	-	-	-
	[1]	-	-	-	-	*	-	-	-	-	-
	[71]	*	*	-	*	*	*	*	-	-	-
	[72]	*	*	-	*	*	*	*	-	-	-
2014	[13]	-	-	-	-	*	*	-	-	-	-
	[73]	-	*	-	*	*	*	*	-	-	-
	[74]	*	-	-	-	-	-	-	-	-	-

layers. In the paper [70], it is suggested to use HIP and IPSe tunneling to protect communication channels and to restrict the unwanted access by communication policy. Meanwhile, the backhaul devices are protected from the address spoofing source and DoS. Finally, SDM and data are collected to detect and prevent threats. The paper [50] establishes the 5G network based on SDN and NFV. It presents the specific architecture, but there is little description about the specific implementation of methods deployed in regards to security issues.

In order to introduce the research advances in SDMN security in detail, Table 2 provides a comparison of the architecture of SDMN security problems addressed in the prior works.

Table 2 SDMN security framework

Wor	Proposed Architecture	Basic Theory	Pros.	Cons.	OFN Security Principle
[51]	5G SDMN arhitecture	An end-to-end software defining architecture, which introduces a logically centralized control plane and dramatically simplifies the data-plane.	Give a solution to efficiently guarantee E2E QoS and QoE	No discussions on security issues	N/A
[70]	multitier security approach with four components: SC, PBC, SMM and Synch.	communication channel protection; limit unwanted access; threat detection by the use of SDM and data collection	Protect single point failure of controller by the use of distributed SecGWs	No consideration of terminal devices	Assure Robust Identity
[50]	SDN and NFV integration for 5G network	security issues exist from SDN controller to whole network	Analyze SDN, NFV and 5G network, and give principles	No discussions on security	N/A
[33]	Direct the mobile network to a flow-centric model that employs hardware and a logically centralized controller	the new security challenges of the control channel of SDMNs	Address security issues in control layer	No security consideration in data layer and application layer	Properties of Manageable Security Control.

4.2 Attacks and countermeasures at each level

SDMN's unique security problems have been widely recognized by researchers. Figure 4 shows the various security aspects in the SDMN.

The characteristics of SDN (i.e., separation of control plane and data plane, centralized management of the network through the controller, network programabiliy and flow analysis are implemented via applications) can effectively resist DDoS [47]. However, these features of SDMN are also a double-edged sword and bring a number of new vulnerabilities. In this section, we will focus on the analysis of the latter to provide better security, reliability, validity, and flexibility of the SDMN.

4.2.1 Data plane attack

Attacks Aiming at the OpenFlow-enable Switch

(i) Security threats

- Attacks southbound Application Programming Interface(API) via false and forged flow table entries due to the intelligent lacking of APIs.
- Flow table is a hardware structure of the OF switch, and the flow entry is its basic unit.. The storage capacity in the flow table is limited. A general flow table has only a few hundred flow entries [86]. The resource attack is studied in [87]. The attacker continuously sends data packets with slightly different head information to generate a disguised data stream, so that the flow table becomes overflow quickly, while the corresponding flow entry of the legitimate flows cannot be updated on time. In addition, this sharply increased number of flow entry requests also exhaust the computing power of the controller and its applications. A new type of inference attack has also been designed by exploit the Weakness of OpenFlow-based SDN networks. When the flow table is full, the frequent operations between the data plane and the control plane are employed to regrade network performance.
- The disguised control information modifies the flow table entries due to the lack of an information authentication mechanism. Similar to the controller under DDoS attack, when flow matching with no clear rules, will lead to the forwarding overflow [86].

(ii) Countermeasures

- Improve the maintenance mechanism to ensure the flow table does not overflow.
- Add a monitoring component. Install the local security agent (LSA) to each of switch to process the application functions related to the switch [70]. This is an insertion mechanism. The most basic control protocol and user platform for communication channels are not changed. Making the network device adopt the proactive forwarding mode rather than the reactive forwarding mode, the flow entries will have been designed and configured before the network devices running [87].
- Network security mechanism synchronizing with the flow traffic. The control plane receives the latest security status of network traffic through monitoring, generates the corresponding security rules, and empties them into the flow table of the OF switch in the data plane via the issuance of flow table entries.

Attacks Aiming at the Terminals (i.e., Client-end Devices)

(i) Security threats

- Insider threats for the mobile terminal includes misuse, downloading of application, etc. Moreover, Trojans and viruses are also the threats of the terminals. The security protection for the mobile terminal is also equipment-centered [83]. The terminal lacks effective tools, e.g., intrusion detection system, antivirus software, endpoint firewall, spam blocking, etc., which are very effective and common in other platforms [88], but still unworkable for mobile terminals [89].
- Due to physical access vulnerabilities, malicious code is written and injected.

(ii) Countermeasures

- Use traditional tools, but need to customize them for mobile devices and provide the security service through the cloud [21].
- Install and run lightweight safety procedures, and encrypt the data of mobile devices [90]. A user-centric model named SECURED is proposed in [83], changing the status that an Internet users must provide different security profile and policies for his/her increasing number of mobile ends, like mobile phone and iPad, to simplify the device security problem.
- Monitoring the access of key ports and core programs.

4.2.2 Control plane attack

(i) Security threats

- The limitations of the API will lead to the illegal controller access operation and counterfeit rules insertion. When a packet is not matched to the flow entries, it will be sent to the controller. As a result, an attacker detects the vulnerability of the controller by simply sending data [91].

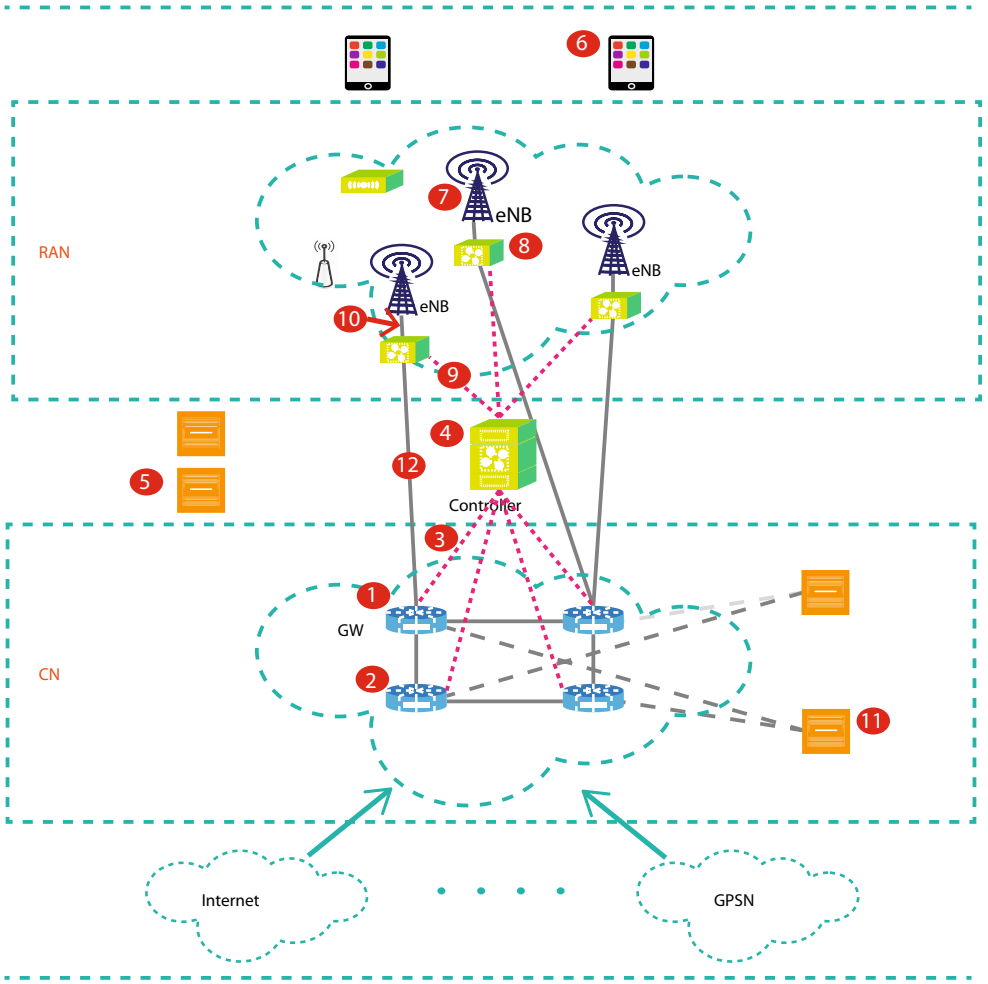

Fig. 4 Security aspects of SDMN

- Attacking the eastbound API can generate Interference policies by different applications to arouse the DDoS among controller [47].
- The controller will be hijacked and compromised while the controller being made public.
- The backhaul mobile device lacks unified control of the unauthorized access to the controller, which is a loophole that can be used by the forged information to modify the entities of flow tables without authorization.
- The security issue of all kinds of database. For instance, the Host Location Hijacking Attack and Link Fabrication Attack can exploit to poison the network topology information in OpenFlow networks. In addition, DOS attack and man-in-the-middle attack can lead to the false network routing and data packets forwarding by providing inaccurate topological information for the routing components in the controller [53].
- The controller is disguised and send harmful controlling information.
- The controller is controlled while its vulnerability is detected [91]. Recently, some vulnerabilities, which are not specific to SDN, have been practical discovered. Such as the XML eXternal Entity vulnerability in OpenDay light netconfi., DDoS when deserializing malformer packets in ONOS, and the tTopology spoofing via host tracking. A SDN network scanning tool, called the SDN scanner [92] can easily operate the existing mobile network scanning tools (e.g. ICMP scanning and TCP SYN scanning). For the SDN networks, which do not require high performance and high bandwidth devices, these attacks will greatly reduce the network performance [47].

(ii) Countermeasures

- Rule authentication. FortNOX provides an extension of the rule-based authentication and security constraint mechanism for the OpenFlow controller of NOX. The real-time monitoring of the flow rules applies the

role-based authentication to judge the legality of the rules generated by each OpenFlow application and prevent the controller from the attacks incurred by the counterfeit flow rules [93].
- Network behavior and message monitoring. As a component of the controller, SPHINX is used to detect attacks on network topology and data plane structure in SDN networks. When the behavior of the network control platform is changed, the new network behavior can be detected and a warning will be issued. It monitors and judges the legitimacy of the switches and routers. Thereby, only legitimate and harmless control messages are executed [85]. TopoGuard, a new security extension to the OpenFlow controllers provides automatic and real-time detection of Network Topology Poisoning Attacks [13].
- Carry out an omnidirectional monitor for detecting abnormal attacks. (1) The SMM module monitors the APP distributed in SDN and virtual environment through distributing virtual sensor nodes, including monitoring the network resources, network performance, flow, etc. SDM is used to manager these monitoring nodes. (2) Apply the intrusion detection system (IDS) in SDN [94]. Evolving defense mechanism (EDM), a bionics-based architecture, can configure the network variations, e.g., IP address, routing, host respond, encryption algorithm, and authentication scheme, to ensure the network safety [71].
- Implement attack prevention via firewall, single point failure recovery [70], IPS, and Authorization/authentication of valid rules and accessed objects.

4.2.3 Application plane attack

As the core equipment of the application plane, a mobile terminal is not only the source of attacks, but also the target of attacks. Therefore, the security of the mobile terminal data is even more important than that of data and control planes.
(i) Security threats [16]

- A large number of APPs lack authentication and authorization and can be accessed by an illegal controller.
- Misusing and abusing the controller is caused by the APP containing security vulnerabilities, alicious code, and bugs.
- The harmful APP generates faulty information flow and inject rules of deceptive rules.
- Attack the northbound APIs.

(ii) Countermeasures

- Strengthen the APP management via authentication mechanism, e.g., the user authentication and the third party certification [21].
- Assure the APP testing and debug to guarantee the correctness and reliability of APPs.
- Judge the APP unauthorized access according to the Constraints of APP and its installation.

4.2.4 Attack at the communication protocols

There are also attacks at protocols for the communications between base stations and controller, controller and application services, and switches and controller.
(i) Security threats

- The lacks of the underlying IP layer security and the authentication in the communication between backhaul devices result in IP spoofing.
- The TLS/SSL security protocol in High level is vulnerable to being attacked, For example, there exist some TCP layer attacks, such as SYN DoS and TCP reset attack [16].
- Randomness in use and complexity of configuration of TLS and communication interception [70], e.g., Man-in-the-Middle attack.

(ii) Countermeasures

- Improve the existing protocols. The HIP protocol and IPSec tunnelling are proposed to ensure the safety of the channel between the control and data planes [70]. Prevent the threat of user authentication and communication when the user connects LTE network in the first time and the handover process is run [77].
- Detect the incorrect protocol information via IDS.
- Take advantage of the controller to guarantee the communication security between the end nodes. (1) Install the Customer Edge Switching (CES) APP in the controller. The APP interacts with the data interaction path of the gateway and insert negotiated flow to ensure end-to-end user communication by applying the customer edge traversal protocol (CETP), and extends the realm gateway (RGW) function of traditional firewalls. Furthermore, the abusive, DoS, forged source addresses and other tools can also be detected and removed. (2) Introducing the TCP-Splicing mechanism to relay the user data from a host that has not been forged [50, 70].
- Employ the oligarchic trust models adopting the multiple trust-anchor certification authority, e.g. one per subdomain or per controller instance [12].
- Implement the optional support for encrypted TLS communication and a certificate exchange between the switches and the controller(s) proposed in OpenFlow 1.3.0 [8].

4.3 Category and analysis of STRIDE

The previous section analyzes the attacks and threats on the SDMN in accordance with the network architecture layers. This section will analyze the corresponding network attacks or vulnerabilities from the point of view of computer security systems. The STRIDE method makes logical separations within the complex system security, as shown in [19, 95]. STRIDE is a type of security threat method. With STRIDE, security threats are divided into six categories: Spoofing of user identity (S), Tampering (T), Repudiation (R), Information disclosure (I), e.g., privacy breach or data leak [96], Denial of service (DoS) (D), and Elevation of privilege (E).

Table 3 provides a study of SDMN related attacks based on the classifications of STRIDE. The state-of-the-art of the research on the attacks of SDMN is also presented in the table.

To summarize Table 3, a brief analysis is provided as follows.

- As shown in Table 3, some attacks are categorized into one layer, however, they actually may affect several layers. Therefore, corresponding strategies require the interaction and collaboration among multi-layers.
- Monitoring the network state and behavior in each layer is the common means. In addition to the traditional monitoring of network traffic, port access, and network state, one also needs to monitor the SDMN specific message and behavior between the OF switch and controller, among controllers, and between the application layer APP and controller. However the real-time monitoring and the corresponding information preservation have brought new problems to the network traffic delay, the normal mobile terminal application running, the controller operation efficiency, the storage space of each layer, etc.
- DDoS may occur in all the layers. Once it occurs, at present, there is no better way to prevent or solve this kind of attack except isolating the related network equipment and links. Therefore, based on the network behavior and characteristics existing prior to a DDoS attack, we conclude that early detection and prevention are the most feasible measures.

Table 3 STRIDE based classification

Location	Category	Existing Work
Data	S	[70]
Layer	T	[17]
	R	[62]
	I	[62, 81]
	D	[17, 47]
	E	[62]
Control	S	[17, 97]
Layer	T	[97]
	R	[17]
	I	[97]
	D	[47, 70, 97]
	E	[70]
Application	S	[70]
Layer	T	[97]
	R	[70]
	I	[81]
	D	[47]
	E	[70]
Communication	S	[17, 53, 98]
Protocol	T	[86, 87, 98]
Stack	R	[55, 98]
	I	[55, 98]
	D	[52, 85, 86]
	E	[17, 98]

4.4 SDMN security challenges

Although some advances are being made, there are many challenging problems in SDMN security that call for significant research efforts. Some SDMN security challenges are listed below.

- APP authorization and authentication mechanism.
- Security problems for multi-controller architectures [16].
- Security issues from multicast protocols.
- Redundant connections resulting from security guaranty mechanisms [16].
- Security measures of the communication with other networks.

5 Conclusion

This paper introduced the structure of SDMN, and its special security issues. The security measures of SDMN involve three layers. First, there is the data layer, which is associated with the security threats of OpenFlow switch and terminal, and the corresponding countermeasures. Second, there is the control layer, including the security of all databases. Specific security problems of SDMN in the control layer and the corresponding measures were reviewed and discussed. In addition, the STRIDE method was used to achieve a classification of SDMN attacks, as the data layer, control layer, application layer, and communication protocol attacks. Finally, a list of security challenges of SDMN was presented that call for significant research efforts.

Acknowledgments This work was supported by the Program of International S&T Cooperation of MOST (No.2013DFA11140, No. 2013CFA051), the National Natural Science Foundation of China (grant No.61210010, No.61300231, 61572220). Mao's work is supported in part by the US NSF (Grant CNS-0953513) and by the Wireless Engineering Research and Education Center at Auburn University.

References

1. Sama MR, Contreras LM, Kaippallimalil J, Akiyoshi I, Qian H, Ni H (2015) Software-defined control of the virtualized mobile packet core. IEEE Commun Mag 53(2):107–115
2. Ge X, Yang B, Ye J, Mao G, Wang C-X, Han T (2015) Spatial Spectrum and Energy Efficiency of Random Cellular Networks. IEEE Trans Commun 63(3):1019–1030
3. Bernardos C, La Oliva A, Serrano P, Banchs A, Contreras LM, Jin H, Zúñiga JC (2014) An architecture for software defined wireless networking. IEEE Wirel Commun 21(3):52–61
4. Ge X, Huang K, Wang C-X, Hong X, Yang X (2011) Capacity Analysis of a Multi-Cell Multi-Antenna Cooperative Cellular Network with Co-Channel Interference. IEEE Trans Wirel Commun 10(10):3298–3309
5. He J, Wen Y, Huang J, Wu D (2014) On the Cost–QoE Tradeoff for Cloud-Based Video Streaming Under Amazon EC2's Pricing Models. IEEE Transactions on Circuits and Systems for Video Technology 24(4):669–680
6. Chávez-Santiago R, Szydełko M, Kliks A, Foukalas F, Haddad Y, Nolan KE, Kelly MY, Masonta MT, Balasingham I (2015) 5G: The convergence of wireless communications. Wirel Pers Commun:1–26
7. Naudts B, Kind M, Westphal F-J, Verbrugge S, Colle D, Pickavet M (2012) Techno-economic analysis of software defined networking as architecture for the virtualization of a mobile network. In: 2012 European Workshop on Software Defined Networking (EWSDN). IEEE, pp 67–72
8. Nunes B, Mendonca M, Nguyen X-N, Obraczka K, Turletti T, et al. (2014) A survey of software-defined networking: past, present, and future of programmable networks. IEEE Communications Surveys & Tutorials 16(3):1617–1634
9. Checko A, Christiansen HL, Yan Y, Scolari L, Kardaras G, Berger MS, Dittmann L (2014) Cloud RAN for mobile networks – a technology overview. IEEE Communications Surveys & Tutorials 17(1):405–426
10. Xiao J, Hu R, Qian Y, Gong L, Wang B (2013) Expanding lte network spectrum with cognitive radios: From concept to implementation. IEEE Wirel Commun 20(2):12–19
11. Manzalini A, Saracco R, Buyukkoc C et al. (2014) Software-defined networks for future networks and services: main technical challenges and business implications, SDN4FNS. IEEE
12. Kreutz D, Ramos F, Verissimo P (2013) Towards secure and dependable software-defined networks. In: Proceedings of the second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. ACM, pp 55–60
13. Hakiri A, Gokhale A, Berthou P, Schmidt DC, Gayraud T (2014) Software-defined networking: Challenges and research opportunities for future internet. Comput Netw 75(24):453–471
14. Shin S, Porras PA, Yegneswaran V, Fong MW, Gu G, Tyson M (2013) Fresco: Modular composable security services for software-defined networks. In: NDSS
15. Kreutz D, Bessani A, Feitosa E, Cunha H (2014) Towards secure and dependable authentication and authorization infrastructures. In: 2014 IEEE 20th Pacific Rim International Symposium on Dependable Computing (PRDC). IEEE, pp 43–52
16. Principles and practices for securing software-defined networks, 2015. www.opennetworking.org
17. Kreutz D, Ramos FM, Esteves Verissimo P, Esteve Rothenberg C, Azodolmolky S, Uhlig S (2015) Software-defined networking: A comprehensive survey. proc IEEE 103(1):14–76
18. Yap K-K, Sherwood R, Kobayashi M, Huang T-Y, Chan M, Handigol N, McKeown N, Parulkar G (2010) Blueprint for introducing innovation into wireless mobile networks. In: Proceedings of the second ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures. ACM, pp 25–32
19. Hernan S, Lambert S, Ostwald T, Shostack A (2006) Uncover security design flaws using the stride approach msdn. microsoft. com
20. Wikipedia, Stride(security)–wikipedia, the free encyclopedia, 2015, [Online; accessed 20-July-2015]. [Online]. Available: https://en.wikipedia.org/wiki/STRIDE_(security)
21. Ali M, Khan SU, Vasilakos AV (2015) Security in cloud computing: Opportunities and challenges. Inf Sci 305(1):357–383
22. Yazıcı V, Kozat UC, Oguz Sunay M (2014) A new control plane for 5G network architecture with a case study on unified handoff, mobility, and routing management. IEEE Commun Mag 52(11):76–85
23. Yang M, Li Y, Hu L, Li B, Jin D, Chen S, Yan Z (2014) Cross-layer software-defined 5G network. Mobile Networks and Applications 20(3):1–10
24. Jin X, Li LE, Vanbever L, Rexford J (2013) Softcell: Scalable and flexible cellular core network architecture. In: Proceedings of the ninth ACM Conference on Emerging Networking Experiments and Technologies. ACM, pp 163–174
25. Costa-Requena J (2014) SDN integration in lte mobile backhaul networks. In: 2014 International Conference on Information Networking (ICOIN). IEEE, pp 264–269
26. Kempf J, Johansson B, Pettersson S, Lüning H, Nilsson T (2012) Moving the mobile evolved packet core to the cloud. In: 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, pp 784–791
27. Sama MR, Ben Hadj Said S, Guillouard K, Suciu L (2014) Enabling network programmability in lte/epc architecture using OpenFlow. In: 2014 12th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt). IEEE, pp 389–396
28. Nagy M, Kotuliak I (2014) Utilizing OpenFlow, SDN and NFV in GPRS core network, in Testbeds and Research Infrastructure: Development of Networks and Communities. Springer, pp 184–193
29. Ge X, Cheng H, Guizani M, Han T (2014) 5G Wireless Backhaul Networks: Challenges and Research Advances. IEEE Netw 28(6):6–11
30. He J, Xue Z, Wu D, Wu DO, Wen Y (2014) CBM: Online Strategies on Cost-aware Buffer Management for Mobile Video Streaming. IEEE Transactions on Multimedia 16(1): 242–252
31. Lei L, Zhong Z, Zheng K, Chen J, Meng H (2013) Challenges on Wireless Heterogeneous Networks for Mobile Cloud Computing. IEEE Wirel Commun 20(3):34–44
32. Zheng K, Wang Y, Wang W, Dohler M, Wang J (2011) Energy-efficient wireless in-home: the need for interference-controlled femtocells. IEEE Wirel Commun 18(6):36–44
33. Liyanage M, Ylianttila M, Gurtov A (2014) Securing the control channel of software-defined mobile networks. In: 2014 IEEE 15th International Symposium on A World of Wireless Mobile and Multimedia Networks (WoWMoM). IEEE, pp 1–6

34. Wu D, Xue Z, He J (2014) iCloudAccess: Cost-Effective Streaming of Video Games from the Cloud with Low Latency. IEEE Transactions on Circuits and Systems for Video Technology 24(8):1405–1416
35. He J, Wu D, Zeng Y, Hei X, Wen Y (2013) Toward Optimal Deployment of Cloud-Assisted Video Distribution Services. IEEE Transactions on Circuits and Systems for Video Technology 23(10):1717–1728
36. Network functions virtualisation (nfv), 2013. [Online]. Available: https://portal.etsi.org/nfv/nfv_white_paper2.pdf
37. Bays LR, Oliveira RR, Barcellos MP, Gaspary LP, Madeira ERM (2015) Virtual network security: Threats, countermeasures, and challenges. Journal of Internet Services and Applications 6(1):1–19
38. Wolinsky DI, Agrawal A, Boykin PO, Davis JR, Ganguly A, Paramygin V, Sheng YP, Figueiredo RJ (2006) On the design of virtual machine sandboxes for distributed computing in wide-area overlays of virtual workstations. In: 2006 First International Workshop on Virtualization Technology in Distributed Computing, 2006 VTDC. IEEE, pp 8–8
39. Wu H, Ding Y, Winer C, Yao L (2010) Network security for virtual machine in cloud computing. In: 2010 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT). IEEE, pp 18–21
40. de Oliveira DAS, Wu FS (2009) Protecting kernel code and data with a virtualization-aware collaborative operating system. In: 2009 Annual Computer Security Applications Conference, ACSAC'09. IEEE, pp 451–460
41. Zhang L, Shetty S, Liu P, Jing J (2014) Rootkitdet: Practical end-to-end defense against kernel rootkits in a cloud environment. In: Computer Security-ESORICS 2014. Springer, pp 475–493
42. Baliga A, Kamat P, Iftode L (2007) Lurking in the shadows: Identifying systemic threats to kernel data. In: IEEE Symposium on Security and Privacy, 2007. SP'07. IEEE, pp 246–251
43. Fernandes DA, Soares LF, Gomes JV, Freire MM, Inácio PR (2014) Security issues in cloud environments: A survey. Int J Inf Secur 13(2):113–170
44. Nguyen M-D, Chau N-T, Jung S, Jung S (2014) A demonstration of malicious insider attacks inside cloud iaas vendor. International journal of Information and Education Teachnology 4(6)
45. Rocha F, Correia M (2011) Lucy in the sky without diamonds: Stealing confidential data in the cloud. In: 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W). IEEE, pp 129–134
46. Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Futur Gener Comput Syst 28(3):583–592
47. Yan Q, Yu F (2015) Distributed denial of service attacks in software-defined networking with cloud computing. EEE Commun Mag 53(4):52–59
48. Szefer J, Keller E, Lee RB, Rexford J (2011) Eliminating the hypervisor attack surface for a more secure cloud. In: Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, pp 401–412
49. Liang C, Yu FR (2015) Wireless virtualization for next generation mobile cellular networks. IEEE Wirel Commun 22(1):61–69
50. Costa-Requena J, Santos JL, Guasch VF, Ahokas K, Premsankar G, Luukkainen S, Pérez OL, Itzazelaia MU, Ahmad I, Liyanage M, et al. (2015) SDN and NFV integration in generalized mobile network architecture. In: 2015 European Conference on Networks and Communications (EuCNC). IEEE, pp 154–158
51. Yang M, Li Y, Li B, Jin D, Chen S (2015) Service-oriented 5G network architecture: an end-to-end software defining approach. Int J Commun Syst
52. Kloti R, Kotronis V, Smith P (2013) OpenFlow: A security analysis. In: 2013 21st IEEE International Conference on Network Protocols (ICNP). IEEE, pp 1–6
53. Hong S, Xu L, Wang H, Gu G (2015) Poisoning network visibility in software-defined networks: New attacks and countermeasures. In: Network and Distributed System Security (NDSS) Symposium 2015. NDSS, pp 8–11
54. Benton K, Camp LJ, Small C (2013) OpenFlow vulnerability assessment. In: Proceedings of the second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. ACM, pp 151–152
55. Shin S, Gu G (2013) Attacking software-defined networks: A first feasibility study. In: Proceedings of the second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. ACM, pp 165–166
56. Shin S, Song Y, Lee T, Lee S, Chung J, Porras P, Yegneswaran V, Noh J, Kang BB (2014) Rosemary: A robust, secure, and high-performance network operating system. ACM
57. Schehlmann L, Abt S, Baier H (2014) Blessing or curse? revisiting security aspects of software-defined networking. In: 2014 10th International Conference on Network and Service Management (CNSM). IEEE, pp 382–387
58. Marinho J, Granjal J, Monteiro E (2015) A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. EURASIP Journal on Information Security 2015(1):1–14
59. Naseef M (2014) Vulnerabilities of LTE and LTE-Advanced Communication White Paper
60. Qi F, Sun S, Rong B, Hu RQ, Qian Y Cognitive radio based adaptive SON for LTE-a heterogeneous networks. In: 2014 IEEE Global Communications Conference (GLOBECOM), vol 2014. IEEE, pp 4412–4417
61. Lien S-Y, Chen K-C, Liang Y-C, Lin Y (2014) Cognitive radio resource management for future cellular networks. IEEE Wirel Commun 21(1):70–79
62. Baldini G, Sturman T, Biswas AR, Leschhorn R, Gódor G, Street M (2012) Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead. IEEE Communications Surveys & Tutorials 14(2):355–379
63. Park J-M, Reed JH, Beex A, Clancy TC, Kumar V, Bahrak B (2014) Security and enforcement in spectrum sharing. Proc IEEE 102(3):270–281
64. Sethi A, Brown TX (2008) Hammer model threat assessment of cognitive radio denial of service attacks. In: 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks 2008, DySPAN 2008. IEEE, pp 1–12
65. Hlavacek D, Chang JM (2014) A layered approach to cognitive radio network security: A survey. Comput Netw 75(24):414–436
66. Zhang L, Ding G, Wu Q, Zou Y, Han Z, Wang J (2015) Byzantine attack and defense in cognitive radio networks: A survey. IEEE Communication Surveys & Tutorials 17(3):1342–1363
67. Jermyn J, Salles-Loustau G, Zonouz S (2014) An analysis of dos attack strategies against the LTE RAN. Journal of Cyber Security 3(2):159–180
68. Golde N, Redon K, Borgaonkar R (2012) Weaponizing femtocells: The effect of rogue devices on mobile telecommunications. In: NDSS
69. Lichtman M, Reed JH, Clancy TC, Norton M (2013) Vulnerability of lte to hostile interference. In: 2013 IEEE Global Conference on Signal and Information Processing (GlobalSIP). IEEE, pp 285–288

70. Liyanage M, Ahmad I, Ylianttila M, Santos JL, Kantola R, Perez OL, Itzazelaia MU, de Oca EM, Valtierra A, Jimenez C (2015) Security for future software defined mobile networks. In: 9th International Conference on Next Generation Mobile Applications Services and Technologies (NGMAST). IEEE, pp 1–9
71. Zhou H, Wu C, Jiang M, Zhou B, Gao W, Pan T, Huang M (2015) Evolving defense mechanism for future network security. IEEE Commun Mag 53(4):45–51
72. Gonzales D, Kaplan J, Saltzman E, Winkelman Z, Woods D (2015) Cloud-trust-a security assessment model for infrastructure as a service (IaaS) clouds, IEEE Transactions on Cloud Computing
73. Hu F, Hao Q, Bao K (2014) A survey on software-defined network and OpenFlow: from concept to implementation. IEEE Communications Surveys & Tutorials 16(4):2181–2206
74. Hu H, Ahn G-J, Han W, Zhao Z (2014) Towards a reliable SDN firewall, Presented as part of the Open Networking Summit 2014 (ONS 2014)
75. Matias J, Garay J, Toledo N, Unzilla J, Jacob E (2015) Toward an SDN-enabled NFV architecture. IEEE Commun Mag 53(4):187–193
76. Alzahrani AJ, Ghorbani AA (2015) A multi-agent system for smartphone intrusion detection framework. In: Proceedings of the 18th Asia Pacific Symposium on Intelligent and Evolutionary Systems, Vol 1. Springer, pp 101–113
77. El-Gaml EF, ElAttar H, El-Badawy HM (2014) Evaluation of intrusion prevention technique in lte based network. Int J Sci Eng Res 5:1395–1400
78. Liebergeld S, Lange M, Borgaonkar R (2014) Cellpot: A concept for next generation cellular network honeypots. In: Workshop on Security Emergence Network Technology. NDSS
79. Yan Z, Zhang P, Vasilakos AV (2015) A security and trust framework for virtualized networks and software-defined networking. Security and Communication Networks
80. Franċois J, Festor O (2015) Anomaly traceback using software defined networking. In: 2015 National Conference on Parallel Computing Technologies (PARCOMPTECH). IEEE, pp 203–208
81. Duan X, Wang X (2015) Authentication handover and privacy protection in 5G hetnets using software-defined networking. IEEE Commun Mag 53(4):28–35
82. Yang N, Wang L, Geraci G, Elkashlan M, Yuan J, Renzo MD (2015) Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun Mag 53(4):20–27
83. Montero D, Yannuzzi M, Shaw A, Jacquin L, Pastor A, Serral-Gracia R, Lioy A, Risso F, Basile C, Sassu R et al (2015) Virtualized security at the network edge: A user-centric approach. IEEE Commun Mag 53(4):176–186
84. Ding AY, Crowcroft J, Tarkoma S, Flinck H (2014) Software defined networking for security enhancement in wireless mobile networks. Comput Netw 66:94–101
85. Dhawan M, Poddar R, Mahajan K, Mann V (2015) SPHINX: Detecting security attacks in software-defined networks. In: Proceedings of the 2015 Network and Distributed System Security (NDSS) Symposium
86. Leng J, Zhou Y, Zhang J, Hu C (2015) An inference attack model for flow table capacity and usage: Exploiting the vulnerability of flow table overflow in software-defined network, arXiv:1504.03095
87. Tri N, Hiep T, Kim K (2015) Assessing the impact of resource attack in software defined network. In: 2015 International Conference on Information Networking (ICOIN). IEEE, pp 420–425
88. Dinh HT, Lee C, Niyato D, Wang P (2013) A survey of mobile cloud computing: architecture, applications, and approaches. Wirel Commun Mob Comput 13(18):1587–1611
89. Mobile device security in the workplace: 6 key risks & challenges, 2015. [Online]. Available: http://focus.forsythe.com/articles/55/Mobile-Device-Security-in-the-Wor kplace-6-Key-Risks-and-Challenges
90. Khan AN, Kiah MM, Madani SA, Ali M et al (2013) Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing. J Supercomput 66(3):1687–1706
91. SDN and security, 2015. [Online]. Available: http://onosproject.org/2015/04/03/sdn-and-security-david-jorm/
92. Gudipati A, Perry D, Li LE, Katti S (2013) SoftRAN: Software defined radio access network. In: Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, pp 25–30
93. Porras P, Shin S, Yegneswaran V, Fong M, Tyson M, Gu G (2012) A security enforcement kernel for OpenFlow networks. In: Proceedings of the first workshop on Hot topics in software defined networks. ACM, pp 121–126
94. Giotis K, Argyropoulos C, Androulidakis G, Kalogeras D, Maglaris V (2014) Combining OpenFlow and sflow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Comput Netw 62:122–136
95. Yang M, Li Y, Jin D, Zeng L, Wu X, Vasilakos AV (2014) Software-defined and virtualized future mobile and wireless networks: a survey. Mobile Networks and Applications 20(1):4–18
96. Li G, Wu D, Shen J, Li T (2015) Deciphering Privacy Leakage in Microblogging Social Networks: A Measurement Study, Security and Communication Networks
97. Akhunzada A, Ahmed E, Gani A, Khan M, Imran M, Guizani S (2015) Securing software defined networks: taxonomy, requirements, and open issues. IEEE Commun Mag 53(4):36–44
98. Tasch M, Khondoker R, Marx R, Bayarou K (2014) Security analysis of security applications for software defined networks. In: Proceedings of the AINTEC 2014 on Asian Internet Engineering Conference. ACM, pp 23–30