Security Requirements Modelling for Virtualized 5G Small Cell Networks

Vassilios G. Vassilakis*, Haralambos Mouratidis†, Emmanouil Panaousis†,
Ioannis D. Moscholios‡, Michael D. Logothetis§
* Dept. of Computer Science, University of York, York YO10 5GH, United Kingdom
† Secure and Dependable Software Systems Research Cluster, School of Computing, Engineering, and Mathematics, University of Brighton, Brighton BN2 4AT, United Kingdom
‡ Dept. of Informatics & Telecommunications, University of Peloponnese, Tripolis 221 00, Greece
§ Dept. of Electrical & Computer Engineering, University of Patras, Patras 265 04, Greece

***Abstract*—It is well acknowledged that one of the key enabling factors for the realization of future 5G networks will be the small cell (SC) technology. Furthermore, recent advances in the fields of network functions virtualization (NFV) and software-defined networking (SDN) open up the possibility of deploying advanced services at the network edge. In the context of mobile/cellular networks this is referred to as mobile edge computing (MEC). Within the scope of the EU-funded research project SESAME we perform a comprehensive security modelling of MEC-assisted quality-of-experience (QoE) enhancement of fast moving users in a virtualized SC wireless network, and demonstrate it through a representative scenario toward 5G. Our modelling and analysis is based on a formal security requirements engineering methodology called Secure Tropos which has been extended to support MEC-based SC networks. In the proposed model, critical resources which need protection, and potential security threats are identified. Furthermore, we identify appropriate security constraints and suitable security mechanisms for 5G networks. Thus, we reveal that existing security mechanisms need adaptation to face emerging security threats in 5G networks.**

***Keywords*—Security modelling; small cells; mobile edge computing; virtualization.**

I. Introduction

The widespread of end user devices with advanced capabilities, such as smartphones and tablet computers, has led to the appearance of a wide rage of mobile applications. At the same time, novel services are being introduced by mobile network operators (MNOs). This situation imposes very strict requirements on the existing infrastructure and communication technologies. The challenge becomes greater as devices are also expected to actively communicate with a multiplicity of equipment (sensors, smart meters, etc.) within a fully converged framework of heterogeneous network (HetNet) infrastructure [1].

Hence, in the recent years the evolution of mobile networks has more demanding requirements in terms of capacity, quality-of-experience (QoE), energy efficiency, and cost reduction. Research efforts towards next-generation 5G networks explore a number of emerging technologies, such as the small cell (SC) technology [2], wireless network virtualization [3], network functions virtualization (NFV) [4], software-defined networking (SDN) [5], and self-organizing networks (SON) [6]. The expected benefits, among others, include an increasing throughput and network capacity on demand, support for localized services, and energy-efficient operation of base stations (BSs).

A number of government and industry-funded R&D projects are working towards defining and developing 5G architectures, solutions, and technologies. For example, the EU-funded SESAME project [7], [8] targets innovations in the area of virtual small cells (VSCs) and the support of advanced services at the network edge by embracing the concept of mobile edge computing (MEC) [9]. The project also proposes a SDN/NFV-enabled architecture for MEC services in 5G SC networks. Recent studies indicate that the use of VSCs can be a good alternative to classical HetNets concept [10]. The main advantage of the VSC concept, in addition to the new BS deployment cost reduction, is that the cellular network coverage and capacity can be adjusted in real time in response to dynamics of user demand and changing network conditions. Many novel architectures and solutions that exploit the technologies of SDN, NFV, SON, and MEC, have been recently proposed [11]–[15]. No doubt that the evolution towards 5G will require the addition of new security features to protect against emerging threats. However, there are not many studies of tackling the 5G security issues, especially at the intersection of different 5G technologies.

A recently started EU-funded 5G-ENSURE project [16] aims at defining a 5G security architecture and developing usable security enablers for 5G. A limited number of existing works (e.g., [17]–[19]) mainly perform a high-level analysis of emerging security challenges and threats. For example, in [19] the prominent threats and vulnerabilities MEC-enabled SC networks have been identified and classified. The aforementioned works, however, do not propose formal methods or techniques for a secure design of 5G networks and its components. Our current work tries to fill in this gap for virtualized 5G SC networks. We perform security modelling and analysis of the main components of the SESAME architecture. In particular, we consider a realistic and representative 5G scenario: enhancing the QoE of fast moving users using MEC. To this end, we adopt a methodology for security requirements engineering, known as Secure Tropos [20], and extend it to enable security modelling and analysis of the main elements of the SESAME architecture. The proposed methodology has been implemented using the SecTro - a computer-aided software engineering (CASE) tool. Our methodology and the developed tool enable

TABLE I. LIST OF ABBREVIATIONS

BS	Base Station
CASE	Computer-Aided Software Engineering
CESC	Cloud Enabled Small Cell
CESCM	CESC Manager
DC	Data Center
DoS	Denial of Service
EMS	Element Management System
EPC	Evolved Packet Core
EU	End User
HetNet	Heterogeneous Network
MCN	Mobile Core Network
MEC	Mobile Edge Computing
MNO	Mobile Network Operator
MOCN	Multi-Operator Core Network
NFV	Network Functions Virtualization
QoE	Quality of Experience
RAN	Radio Access Network
SC	Small Cell
SDN	Software-Defined Networking
SLA	Service Level Agreement
SON	Self-Organizing Network
SP	Service Provider
UE	User Equipment
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
VNF	Virtual Network Function
VSC	Virtual Small Cell

formal specification of components and resources to be protected, identification of security constrains, and enforcement of appropriate security mechanisms. One of the big advantages of the developed tool is that the validation of conformance to specified security constraints can be performed very quickly and in real time. Although in this work we mainly focus on the radio access network (RAN), VSCs, and MEC servers, the methodology has the potential to be extended in other domains, too.

The rest of the paper is structured as follows. Section II briefly presents the existing works on 5G security. Section III describes the SESAME architecture for virtualized 5G SC networks. Section IV describes our considered 5G scenario and presents our security modelling approach. We conclude and discuss our future work in Section V. Besides, in Table I we present the list of abbreviations used in this paper.

II. RELATED WORK

In this section we briefly discuss some recent and representative works on 5G network security. In [17], a wide range of possible threats and attacks against the main 5G components have been investigated. The main focus is on security issues related to the user equipment (UE) and access networks. Different types of attacks, such as denial of service (DoS), tampering, and eavesdropping, have been studied and analyzed. Finally, potential mitigation techniques and future solutions have been discussed. In [18], a high level security architecture for 5G networks has been proposed. The introduced security framework enables 5G infrastructure and component protection. In particular, the framework integrates the following modules: authentication, encryption, unified access and unified security. The main focus of [18] is on threats originating from wireless local networks and UE. The proposed approach, however, does not take into consideration the peculiarities of emerging SDN, NFV, and MEC technologies, and their impact on 5G systems. In [21], the security aspects of SDN-enabled 5G networks have been addressed. A number of potential threats and attack vectors, such as DoS, privacy violation attacks, location spoofing attacks, and physical tampering attacks, have been studied and analyzed. Also, the problems of security policies management and secure tunneling have been discussed. The proposed security architecture includes a security gateway and a cluster of SDN controllers that are responsible for user authentication and firewalling. In [22], the security handover authentication and privacy protection in 5G is discussed. The focus is on 5G SCs and HetNets protection using SDN technology. The fact that a SDN controller has a global view of the network enables fast network reconfigurability and adaptation to changing network conditions. It also helps reducing redundant authentication across HetNets. Matlab-based simulations show low authentication delays and high network utilization of the proposed SDN-assisted authentication scheme. Finally, in [23], the multi-tenant MEC services have been modeled and analyzed from the security viewpoint using the Secure Tropos methodology.

III. THE SESAME FUNCTIONAL ARCHITECTURE

In this section we present the cellular network architecture developed in the context of the EC 5G-PPP SESAME project [7]. Herein, we only describe the elements relevant to our security requirements modelling that will follow. More details on the SESAME architecture and the considered scenarios can be found in [8], [13].

One of the key elements of this architecture is the incorporation of MEC concepts at the RAN level, by enhancing the VSCs with MEC servers. Another notable characteristic is the multi-tenancy support. This has been achieved by SDN and NFV technologies. The basic SESAME components are: (i) *MEC server*: Specialised hardware that is placed inside the SC and provides processing power, memory and storage capabilities, and networking resources; (ii) *cloud enabled small cell (CESC)*: A SC that has been enhanced with a MEC server; (iii) *CESC cluster*: A group of collocated and coordinated CESCs; (iv) *virtual infrastructure manager (VIM)*: An entity responsible for the management of the virtual hardware (i.e., virtual machines (VMs)) and networking resources of a single MEC server. The VIM is responsible for the lifecycle, provision, placement, and operation of VMs. The VIM is also responsible for the allocation of virtual network functions (VNFs) and for the control of virtual networks and storage resources across VNF instances. Finally, the VIM also manages the interaction of a VNF with the compute, storage, and network resources; (v) *CESC manager (CESCM)*: An entity responsible for managing and orchestrating the cloud environment of CESCs. It can manage at the same time multiple clusters, a single cluster, or a single CESC. The CESCM orchestrates services and consequently manages the VIM to compose them with virtual resources. The CESCM also manages the radio access and SONs self-x functionalities, e.g., self-optimising, self-healing, self-configuring of the SCs contained in each CESC cluster.

One important feature of the SESAME architecture is the formation of a light data center (DC) at the network edge. This is achieved via a distributed and logically grouped set of MEC servers, which are parts of the CESC cluster. The clusters are able to communicate with each other as well as with the

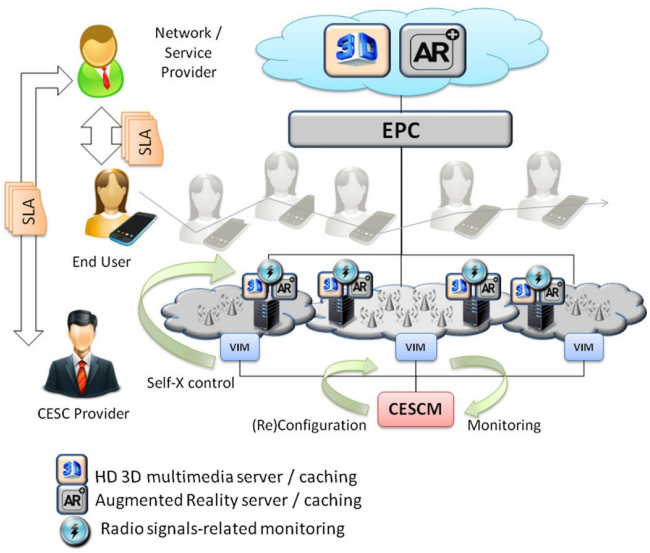

Fig. 1. 5G scenario: Enhancing QoE of fast moving users [13].

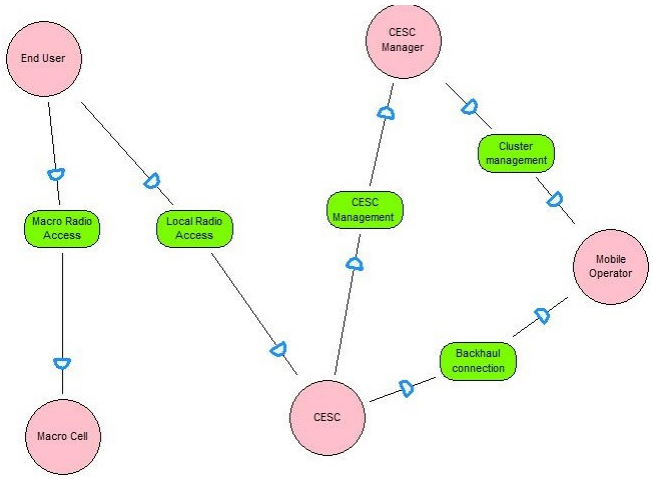

Fig. 2. SecTro: Actors and their dependencies.

evolved packet core (EPC). In addition to providing radio coverage and orchestration of multi-tenancy, a CESC provides a platform for MEC to support low latency and compute intensive applications and services. Hence, the end users (EUs) benefit from fast and cost-effective access to a wide range of innovative services and applications. At the CESC cluster level, the virtualization layer decouples the VNF software from the underlying hardware. The element management system (EMS) performs management of one or more VNFs (e.g, local gateways or multi-operator core network (MOCN) functions).

A cluster of CESCs is managed by the CESCM that constitutes: a VNF orchestrator, a VNF manager, and an EMS virtualization. The VNF manager is responsible for the VNF lifecycle management. Typical operations of the VNF manager include: i) instantiation of VNFs, ii) scaling of VNFs, iii) updating and/or upgrading VNFs, and iv) termination of VNFs. By leveraging on the monitoring mechanisms, the VNF manager is able to apply policies for network service level rescaling and reconfiguration to achieve high resource utilization. The VNF orchestrator is in charge of the orchestration and management of the NFV infrastructure. It is also responsible for the allocation of software resources and for realizing the network services. In particular, the VNF orchestrator has the ability to coordinate, authorize, release, and engage NFV infrastructure resources independently of any specific VIM. Finally, the VNF orchestrator composes service chains (constituted by two or more VNFs located either in one or several CESCs) and manages the deployment of VNFs over the light DC.

IV. Security modelling: Enhancing the QoE of fast moving users using MEC

A. Scenario Description

In our considered scenario, shown in Fig. 1, a CESC Provider manages a number of distributed CESC clusters, with each one covering a geographically contiguous area. We consider a single service provider (SP) that supports a number of EUs via the CESC infrastructure. Service level agreements (SLAs) regulate the interaction of CESC Provider, SP, and EUs. A reference EU moves between different CESC clusters and requires service continuity and appropriate QoE. We assume that the EU moves at a high speed and consumes a high-definition real-time content that has tight delay requirements. This scenario exploits the particular advantages of MEC, since MEC servers are deployed at the network edge and, hence, are able to provide low latency, location awareness, and improved QoE for real-time high-demand applications. In this scenario, it is crucial to enable smooth service execution and to preserve adequate QoE levels when the EU moves both between CESCs and between clusters.

The application of the MEC paradigm allows for an efficient monitoring of the user location and its related radio conditions, with real-time reporting and fast coordination. Also, the adoption of MEC servers at the CESC clusters ensures smooth handover between cells and clusters. The enhanced support for the EU mobility has been realized by implementing appropriate SON's self-x control functions at the macro cell level. These functions take advantage of edge monitoring capabilities to seamlessly manage the handover process across neighboring cells. Finally, the deployment of low-latency edge caches at the MEC servers allows fast and efficient access to the cached content [24]. When the mobility pattern of the EU is known or can be predicted (e.g., if monitored through signal inspection), the caches can help offloading EU's data storage tasks to the CESC.

B. Security Requirements Modelling

In Figs. 2 and 3 we present the Secure Tropos modelling for the considered scenario using the developed SecTro CASE tool. Figure 2 presents the actors and their dependencies. We identify five major actors, namely CESC, CESCM, Mobile Operator, Macro Cell (i.e., macro BS), and EU. The EU requires macro cell radio access and local radio access via CESC. The CESC depends on the CESCM for management purposes and on the Mobile Operator for backhaul connectivity. The Mobile Operator may also require cluster management functionality that is provided by the CESCM.

Figure 3 shows the security components view for the CESCM, who is one of the main actors in the considered

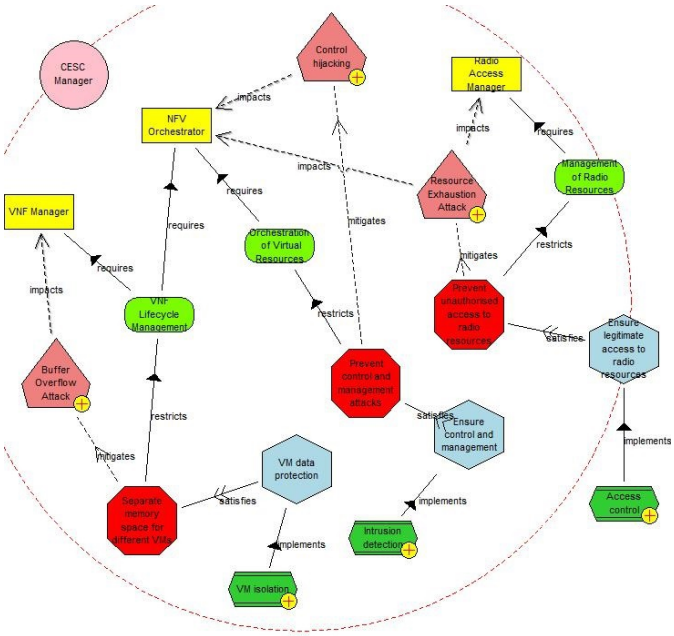

Fig. 3. SecTro: Security components view for the CESCM.

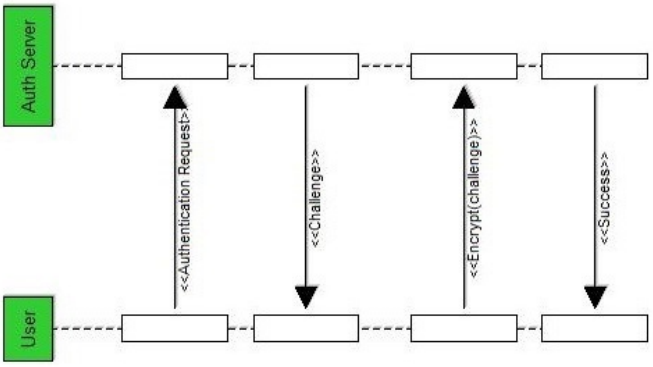

Fig. 4. SecTro: Modelling the Authentication mechanism.

scenario. The following three critical resources have been identified and will need protection: *VNF Manager*, *NFV Orchestrator*, and *Radio Access Manager*. In this example, the CESCM's primary goals, which depend on the aforementioned critical resources, are: *VNF lifecycle management*, *Orchestration of virtual resources*, and *Management of radio resources*. According to the Secure Tropos methodology, an actor's goal may be restricted by one or more security constraints. In this example, the constraints for the aforementioned goals are: *Separate memory space for different VMs*, *Prevent control and management attacks*, and *Prevent unauthorized access to radio resources*. The security constraints have to be satisfied by the following three security objectives: *VM data protection*, *Ensure control and management protection*, and *Ensure legitimate access to radio resources*. The corresponding security mechanisms to implement these objectives are *VM isolation*, *Intrusion detection*, and *Access control*. We also consider the following security threats on the critical resources: *Buffer overflow attack*, *Resource exhaustion attack*, and *Control hijacking*. The *Buffer overflow attack* threat can be mitigated by the *Separate memory space for different VMs* security constraint. The *Resource exhaustion attack* can be mitigated by the *Prevent unauthorized access to radio resources* security constraint. Finally, the *Control hijacking* can be mitigated by the *Prevent control and management attacks* security constraint.

The SecTro tool also allows us to model the details of a specific security mechanism in use. For example, the *Authentication mechanism* could be implemented using a challenge-response protocol, as shown in Fig. 4. This approach requires that each EU shares a secret key with the Authentication Server. When the Authentication Server receives a service request from the EU, it will generate and send back a unique *challenge*. The EU will send back the *encrypted challenge*. The encryption will be done using the shared secret key. The Authentication Server will decrypt the received message and if the result matches the *challenge*, this proves that the EU has a valid key and hence has been authenticated. Note, that this is a single-factor authentication. That is, possessing a valid secret key is a sufficient condition for the EU to get authenticated. For interactions that require high levels of security or in cases of emergency situations, such as natural disasters or cyber attacks, multi-factor authentication would be more appropriate [25].

C. Security Considerations

Particular attention must be paid on protecting user's data and confidentiality. Some data or code, including various configuration settings and security policies, can be altered. This is a particularly important issue in a virtualised multi-tenant environment [26]. It must be taken into account that some tenants could be malicious. Hence, adequate data and VM isolation for different tenants must be ensured. This could be done, for example at the database level or at the hardware level. Also, in some cases, sensitive information of a tenant may be leaked and made available to the adversary or to a malicious tenant.

Another important security threat is the unauthorized access to SC radio resources (physical or virtual) and MEC resources. Given the increasing trend of outsourcing data and applications, an adequate security solution must ensure that only authorized entities gain access. Also, the insider threat should be considered and appropriate mechanisms must be put in place for preventing service providers from misusing tenants' data.

Particular attention must also be paid on appropriate encryption methods. Weaknesses or improper use of cryptographic mechanisms may lead to security breaches in authentication processes and data confidentiality. Also, the generation of cryptographic keys shouldn't rely on weak random number generators. Other security problems may arise due to communication protocols that use weak cryptographic primitives. Hence, it should be ensured that the cryptographic security controls are in place. To ensure appropriate levels of protection, new multi-domain and multi-service trust models need to be considered. Also, encrypted communications and authentication of edge devices (such as MEC servers) will play an important role due to incorporation of MEC services.

Control hijacking attacks are expected to be a serious threat in SDN-based 5G networks. By exploiting the SDN controller implementation weaknesses, the adversary may try to divert the control flows to a controlled device. Then the captured messages can be discarded preventing the data plane entities from proper operation. In a more advanced case, the captured messages may be manipulated with a special purpose code and sent into the network.

Another serious type of attacks is the DoS leading to switched off or malfunctioning SC, or unavailable MEC servers. Also, a DoS attack against the hypervisor can cause service disruption and data loss. Yet, in a multi-tenant environment, security implications that may arise due weak isolation between tenants may allow adversaries to compromise more than one tenants upon compromising one of the other tenants. Furthermore, it has been shown that a DoS attack may be launched from within the SC [27].

V. Conclusion

Having facilitated by the advances of the EU-funded SESAME project, we study the security of virtualized small cell networks enhanced with MEC capabilities. We have modelled a representative 5G scenario using the Secure Tropos methodology. The proposed model has been implemented using a CASE tool, called SecTro. The tool enables security modeling and analysis of the involved actors. In particular, initially we identify the critical resources to be protected and potential security threats. Next, we identify appropriate security constraints and suitable security mechanisms. It is evident that the existing security mechanisms need to be adapted to address the emerging security threats in 5G networks. On the other hand, the incorporation of SDN and NFV technologies into 5G networks, and the introduction of intelligent network edge devices, as facilitated by MEC, enable the development of novel security concepts and mechanisms. In our future work, we intend to study a wider range of different 5G scenarios from the security viewpoint. We will also focus on the appropriate selection of mitigation mechanisms by taking into account the emerging threats to 5G networks.

VI. Acknowledgement

This research work is based upon the concept of the European research project SESAME (Small cEllS coordinAtion for Multi-tenancy and Edge services), and it has received funding under Grant Agreement No.671596 funded by the European Commission under the 5G-PPP framework, within the H2020 initiative.

References

[1] J. G. Andrews, "Seven ways that HetNets are a cellular paradigm shift," IEEE Communications Magazine, vol. 51, no. 3, 2013, pp. 136-144.

[2] M. Wildemeersch, T. Q. Quek, C. H. Slump, A. Rabbachin, "Cognitive small cell networks: Energy efficiency and trade-offs," IEEE Transactions on Communications, vol. 61, no. 9, 2014, pp. 4016-4029.

[3] E. Datsika, A. Antonopoulos, N. Zorba, C. Verikoukis, "Matching game based virtualization in shared LTE-A networks," IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, Dec. 2016, pp. 1-6.

[4] G. Xilouris, *et al.*, "T-NOVA: A marketplace for virtualized network functions," European Conference on Networks and Communications (EuCNC), Bologna, Italy, June 2014, pp. 1-5.

[5] K. Pentikousis, Y. Wang, W. Hu, "Mobileflow: Toward software-defined mobile networks," IEEE Communications Magazine, vol. 51, no. 7, 2013, pp. 44-53.

[6] T. Alsedairy, Y. Qi, A. Imran, M. A. Imran, B. Evans. "Self organising cloud cells: A resource efficient network densification strategy," Transactions on Emerging Telecommunication Technologies, vol. 26, no. 8, 2015, pp. 1096-1107.

[7] EC H2020 SESAME. https://5g-ppp.eu/sesame/ [April 2017].

[8] I. Giannoulakis, *et al.*, "System architecture and aspects of SESAME: Small cEllS coordinAtion for Multi-tenancy and Edge services," 2nd IEEE Conference on Network Softwarization (NetSoft), Workshop on Software Defined 5G Networks (Soft5G), Seoul, Korea, June 2016.

[9] ETSI, Mobile-Edge Computing, Introductory Technical White Paper, Sept. 2014.

[10] A. Galindo-Serrano, S. M. Lopez, A. De Ronzi, A. Gati. "Virtual small cells using large antenna arrays as an alternative to classical HetNets," IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, Scotland, May 2015, pp. 1-6.

[11] 5G PPP Architecture Working Group, View on 5G Architecture, July 2016.

[12] P. Rost, *et al.*, "Mobile network architecture evolution toward 5G," IEEE Communications Magazine, vol. 54, no. 5, 2016, pp. 84-91.

[13] J. O. Fajardo, *et al.*, "Introducing mobile edge computing capabilities through distributed 5G cloud enabled small cells," Mobile Networks and Applications, vol. 21, no. 4, Aug. 2016, pp. 564-574.

[14] V. Vassilakis, I. Moscholios, B. Alzahrani, M. Logothetis, "A software-defined architecture for next-generation cellular networks," IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, May 2016.

[15] H. Wang, S. Chen, H. Xu, M. Ai, Y. Shi, "SoftNet: A software defined decentralized mobile network architecture toward 5G," IEEE Network, vol. 29, no. 2, 2015, pp. 16-22.

[16] EC H2020 5G-ENSURE, https://5g-ppp.eu/5g-ensure/ [April 2017].

[17] G. Mantas, *et al.*, "Security for 5G communications," Fundamentals of 5G Mobile Networks, John Wiley & Sons, Ltd, 2015.

[18] Q. Fang, Z. Weijie, W. Guojun, F. Hui, "Unified security architecture research for 5G wireless system," 11th Web Information System and Application Conference, Tianjin, China, Sept. 2014.

[19] V. Vassilakis, E. Panaousis, H. Mouratidis, "Security challenges of small cell as a service in virtualized mobile edge computing environments," 10th IFIP International Conference on Information Security Theory and Practice, Heraklion, Greece, Sept. 2016, pp. 70-84.

[20] H. Mouratidis and P. Giorgini, "Secure tropos: A security-oriented extension of the tropos methodology," Int. Journal of Software Engineering and Knowledge Engineering, vol. 17, no. 2, 2007, pp. 285-309.

[21] V. Vassilakis, I. Moscholios, B. Alzahrani, M. Logothetis, "On the security of software-defined next-generation cellular networks," IEICE Information and Communication Technology Forum (ICTF), Patras, Greece, July 2016.

[22] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G HetNets using software-defined networking," IEEE Communications Magazine, vol. 53, no. 4, 2015, pp. 28-35.

[23] V. Vassilakis, *et al.*, "Security analysis of mobile edge computing in virtualized small cell networks," IFIP International Conference on Artificial Intelligence Applications and Innovations, Thessaloniki, Greece, Sept. 2016, pp. 653-665.

[24] K. Poularakis, G. Iosifidis, V. Sourlas, L. Tassiulas. "Exploiting caching and multicast for 5G wireless networks," IEEE Transactions on Wireless Communications, vol. 15, no. 4, 2016, pp. 2995-3007.

[25] X. Huang, Y. Xiang, E. Bertino, J. Zhou, L. Xu, "Robust multi-factor authentication for fragile communications," IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 6, 2014, pp. 568-581.

[26] B. Alohali and V. Vassilakis, "Protecting data confidentiality in the cloud of things," International Journal of Hyperconnectivity and the Internet of Things, vol. 1, no. 1, 2017, pp. 29-46.

[27] R. Roman, J. Lopez, M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Generation Computer Systems, in press, available online Nov. 2016.