Security analysis of mobile edge computing in virtualized small cell networks

Security Analysis of Mobile Edge Computing in Virtualized Small Cell Networks

Vassilios Vassilakis[1], Ioannis P. Chochliouros[2], Anastasia S. Spiliopoulou[3], Evangelos Sfakianakis[2], Maria Belesioti[2], Nikolaos Bompetsis[2], Mick Wilson[4], Charles Turyagyenda[4] and Athanassios Dardamanis[5]

[1] School of Computing and Engineering,
University of West London, W5 5RF, London, UK
vasileios.vasilakis@uwl.ac.uk

[2] Research Programs Section Fixed
Hellenic Telecommunications Organization (OTE) S.A.,
1, Pelika & Spartis Street, GR-151 22, Athens, Greece
{ichochliouros, esfak, mbelesioti, nbompetsis}@oteresearch.gr

[3] Hellenic Telecommunications Organization (OTE) S.A.,
99 Kifissias Avenue, GR-151 24, Athens, Greece
aspiliopoul@ote.gr

[4] Fujitsu Laboratories of Europe Ltd.,
Hayes Park Central, Hayes End Road, Hayes, Middlesex, UB4 8FE, UK
{Mick.Wilson, Charles.Turyagyenda}@uk.fujitsu.com

[4] SmartNET S.A.,
2, Lakonias Street, GR-173 42, Agios Dimitrios, Attica, Greece
ADardamanis@smartnet.gr

Abstract. Based upon the context of Mobile Edge Computing (MEC) actual research and within the innovative scope of the *SESAME* EU-funded research project, we propose and assess a framework for security analysis applied in virtualised Small Cell Networks, with the aim of further extending MEC in the broader 5G environment. More specifically, by applying the fundamental concepts of the SESAME original architecture that aims at providing enhanced multi-tenant MEC services though Small Cells coordination and virtualization, we focus on a realistic 5G-*oriented* scenario enabling the provision of large multi-tenant enterprise services by using MEC. Then we evaluate several security issues by using a formal methodology, known as *Secure Tropos*.

Keywords: 5G, Mobile Edge Computing (MEC), Network Functions Virtualization (NFV), security, Software Defined Networking (SDN), Small Cell (SC), virtual network function (VNF).

1 Introduction

In the recent years we are witnessing a widespread use of end user devices with advanced capabilities, such as smart-phones and tablet computers, and the emergence of new services and communication technologies. Modern devices implicate for powerful multimedia capabilities and they are increasingly penetrating the global e-communications market, thus creating new demands on broadband (wireless or mobile) access. The challenge becomes greater as devices are also expected to actively communicate with a multiplicity of equipment (such as sensors, smart meters, actuators, etc.) within a fully converged framework of heterogeneous (underlying) network infrastructure(s). This results to the emergence of new data services and/or related applications that can drastically "reshape" the network usage and all associated demands; these are also "key success factors" in order to realize an effective mobile broadband experience for the benefit of our modern societies and economies. This new evolved ecosystem, *however*, imposes very strict requirements on the network architecture and its functionality. Enabling small end-to-end (E2E) latency and supporting a large number of connections at the fitting level, is not possible to be accomplished in current Long-Term Evolution (LTE) networks. In fact, the fundamental limitations of current approaches lie in their centralized mobility management and data forwarding, as well as in insufficient support for multiple co-existing Radio Access Technologies (RATs) [1] and for suitable adaptability to new architectural schemes.

Today, a large variety of RATs and heterogeneous wireless networks have been successfully deployed and used. However, under the current architectural framework, it is not easy to integrate -*or to "enable"*- a way of a suitable coordination of these technologies. Despite the fact that the coverage of such wireless and cellular networks has increased by deploying more Base Stations (BSs) and Access Points (APs), the Quality-of-Experience (QoE) of End-Users (EUs) does not increase, *accordingly*. For example, the current architectural approach does not enable a Mobile User (MU) selecting the "best available network" in a dynamic and efficient way. It also does not enable simultaneous and coordinated use of radio resources, from different RATs. This leads to highly inefficient use of hardware resources (wireless infrastructure) and spectrum, which is worsened even more with almost uncontrollable inter-RAT interference [2]. In this paper, we build on a novel architectural proposed for next-generation cellular networks. This architecture benefits from the recent advances in Software Defined Networking (SDN) [3] and Network Function Virtualization (NFV) [4], which are natively integrated into the new and novel architecture. Traditionally, SDN and NFV although not dependent on each other, are seen as "*closely related*" and as "complementary" concepts [5]. This integration enables good scalability in terms of supporting a large number of connections as well as heavy mobility scenarios. Also, the introduction of new services and applications becomes much easier. Decoupling control and data planes, and abstracting network functions from the underlying physical infrastructure, brings much greater flexibility to efficiently utilize radio and computing resources both in the Radio Access Network (RAN) [6] as well as in the Mobile Core Network (MCN). Furthermore, the new approach enables the incorporation of Mobile Edge Computing (MEC) services in an easy and straightforward way.

MEC, also known as "*Fog computing*", is a novel concept that extends the services, typically provided by the Cloud, to the network edge [7], [8]. In case of 5G wireless networks, by the term "edge" we usually mean the RAN and some part of the Cloud services is provided by cognitive BSs. The provided services may include storage, computing, data, and application services. The available MEC infrastructure allows applications to run closer to the end user. This is expected to reduce the E2E network latency and to reduce the backhaul capacity requirements. Moreover, it enables better QoE of fast moving EUs, facilitates highly-interactive real-time applications, and even the emergence of novel applications, such as the *Tactile Internet* [9]. In this work, we focus on Small Cell (SC) BSs, which include both physical BSs as well as BSs that are virtualized via NFV and SDN technologies. Our architectural assumptions are based upon the *SESAME architecture*, which derives from an ongoing European 5G-PPP funded research project that aims at providing enhanced multi-tenant MEC services though Small Cells coordination and virtualization [10]. However, our analysis can be easily extended to alternative network architectures and even in the cases of Macro-Cells or combinations of Macro- and Small-Cells. Thus, in the present work we perform an analysis the MEC when applied in a selective and realistic 5G scenario enabling large multi-tenant enterprise services, from the security and privacy viewpoint.

2 Previous Relevant Works

In this section we review the most important and recent works on security and privacy for MEC. The fact that MEC is still at its infancy explains the very limited number of relevant works. These works mainly just touch the security and privacy implications of MEC and no adequate solutions have been proposed to address all the challenges, especially when considering the interaction of MEC with other technologies, such as SDN, and NFV, within the 5G networks context.

In [11], a number of security and privacy challenges of MEC have been discussed. The considered security threats are mainly in the context of a cloud-enabled IoT (Internet of Things) environment. The study makes a classification of the available security technologies according to the involved network elements, such as technologies to secure a fog node (i.e., the MEC server) and an IoT node, as well as techniques to protect the communication. Next, two threats on the existing security mechanisms have been described, namely the *man-in-the-middle (MitM) attack* and *malicious fog node problem*. Finally, a number of high-level suggestions have been proposed to address the security concerns, such as intrusion detection; malicious node detection; data protection; and secure data management. In [12], the security issues of MEC have been discussed in the context of smart grids, smart traffic lights, wireless sensor networks, and SDN. The focus of this study is the MitM attack and, *in particular*, the stealthy features of this attack that could be addressed by examining the Customer Premises Unit (CPU) and memory consumption of the fog node. This work also addresses the assessment of authentication and authorization techniques for connecting the fog with the cloud. The applicability of existing techniques, such as signature-*based* and anomaly-*based* intrusion detection has been studied.

In [13], the challenges of MEC with respect to digital forensics have been discussed. This work mainly considers sensors and various types of smart objects that require connectivity to the cloud and to each other. The focus of this work is to study processes and events that would allow to reconstruct past activity for providing digital evidence. Various existing solutions, such as Virtual Machine (VM) introspection and Trusted Platform Module (TPM), have been discussed and analysed. This paper also makes a distinction between the techniques that can be applied in both fog and cloud, and between those that are only applicable in one of them. In [14], the existing data protection techniques have been studied with respect to their suitability in MEC. The conferred data theft attacks include both external intrusion as well as insider attacks. The paper has proposed a novel approach for data protection, using offensive decoy technology. According to this approach, the data access is initially monitored to detect any abnormal access patterns. Next, when unauthorized access in suspected, large amounts of decoy information is returned to the attacker. Experiments in realistic scenarios indicate that such kind of approach could provide sufficient levels of data protection in MEC environments. In [15], a number of research and security challenges towards realisation of MEC have been identified and analysed. One important conclusion drawn is that the MEC paradigm would need to develop security and privacy solutions to explicitly consider coexistence of trusted nodes with malicious ones in distributed edge settings. This will require the enforcement of secure and redundant routing, and trust topologies. Another implication of shifting the computation from the cloud to the edge is that the concentration of information is prevented in comparison to the centralised cloud computing approach. Hence, novel techniques are required to deal with fragmented information that is distributed over a potentially large and heterogeneous set of edge nodes.

We observe that the existing works on security analysis of MEC mainly consider M2M-like scenarios, while at the same time lacking a formal methodological analysis approach and a study of security and privacy in MEC in relation to other coexisting technologies. In this work, we are trying to "fill" this gap.

3 SESAME-based Essential Architecture

In this section, we describe the cellular network architecture developed in the context of the SESAME project [4]. In the following, this architecture is referred to as the "*SESAME architecture*". One of its key elements is the incorporation of MEC concepts at the RAN level, i.e. by enhancing the BSs with MEC servers. Other important characteristic of the architecture is the support of multi-tenancy feature through cellular infrastructure virtualization and NFV. Below we describe the involved actors and their inter-relations (as schematic representation is also given in Fig. 1); afterwards, we describe the functional architecture and its essential elements.

We distinguish the following essential definitions: **(i)** ***End User (EU)****:* It can be a mobile device (such as a smart-phone or a laptop) that consumes communication services via the cellular network; **(ii)** ***Infrastructure Owner (IO)****:* This is the owner of the cellular infrastructure, such as SCs and macro BS. An IO could be, *for example*, a *Venue Owner (VO)* (such as mall, stadium, enterprise or municipality) or the

traditional network operator; **(iii)** ***IT Equipment Vendor (ITEV)****:* It is a legal entity/company that develops, manufactures, and/or sells IT equipment, such as BSs and servers; **(iv)** ***Small Cell Network Operator (SCNO)****:* It is a legal entity/company that possesses the equipment so as to provide radio communications services and provides radio access to end users locally, by using SCs; **(v)** ***Virtual Small Cell Network Operator (VSCNO)****:* It is a legal entity/company that does not possess the equipment but lease it from another one, so as to provide radio communications services and deliver services to EUs; **(vi)** ***Macro- Cell Network Operator (MCNO)****:* It is a legal entity/company y that possesses the equipment so as to provide radio communications services and provides radio access to EUs in wide areas at the macro cell level; **(vii)** ***Backhaul Provider (BP)****:* A legal entity/company that provides the backhaul connection (either wired or wireless) of the Small Cells and Macro Cells. This could be an Internet Service Provider (ISP) or the traditional Mobile Network Operator; **(viii)** ***Service Provider (SP)****:* This is a legal entity/company that produces, controls and distributes services over the MNO/VMNO. *(This could include, for example, the traditional Over-the-Top (OTT) players)*; **(ix)** ***Virtual Function Provider (VFP)****:* This is a legal entity/company that supplies virtual network functions and other appliances, such as gateways, proxies, firewalls and transcoders. In this way, the need for the customer to acquire, install, and maintain specialised hardware is essentially eliminated, *and*; **(x)** ***Spectrum Owner (SO)***: This is a legal entity/company that owes a particular piece of spectrum in a given geographical area. Nowadays, the SO is essentially the MNO who leases the spectrum from the relevant national authority. However, it is envisioned that in the future an independent player may owe the spectrum and lease it to an operator (such as MCNO, SCNO, VSCNO).

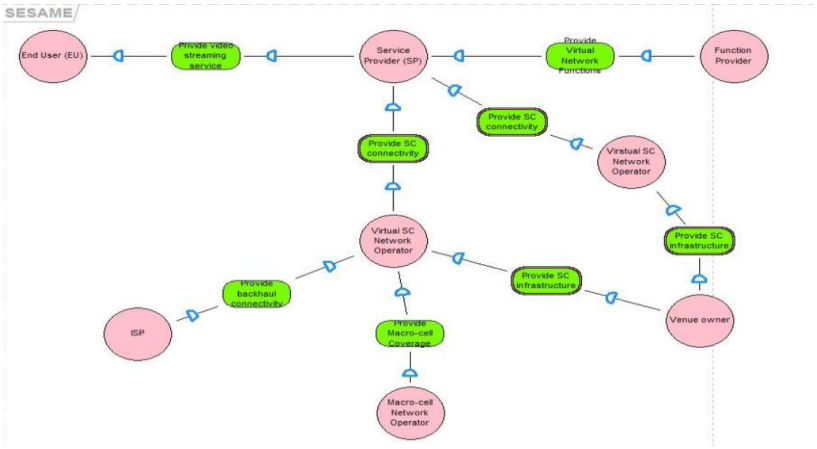

Fig. 1. Actors and their relationships

As shown in Fig.1, the EU is dependent on the SP for receiving one or more services (such as the video streaming service). To provide that, the SP depends on the SCNO or the VSCNO who provide the SC connectivity, and also on the VFP who provides the required (virtual) network functions. Both, SCNO and VSCNO are

dependent on the VO who owes the SC infrastructure. Finally, the VSCNO is also dependent on the BP (e.g., an ISP) who provides backhaul connectivity as well as on the MCNO who provides the macro-cell connectivity.

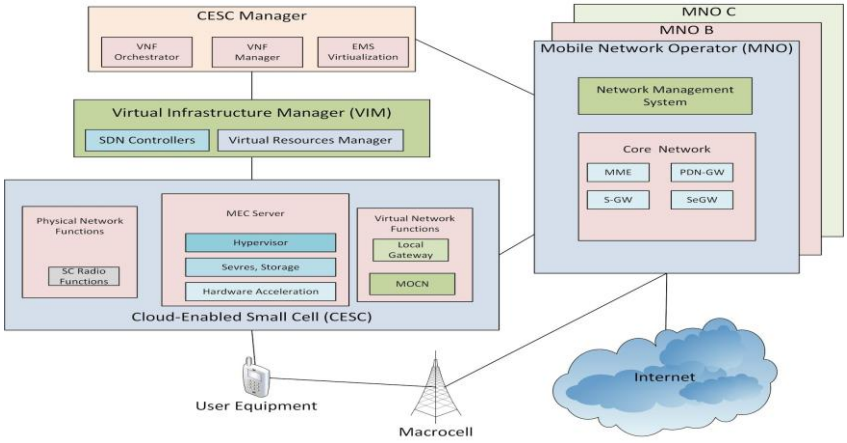

Fig. 2. SESAME functional architecture

We describe, *in brief*, the SESAME functional architecture, which is also illustrated in Fig. 2. Firstly, we provide the basic component definitions and afterwards we describe "*how these components interact with each other*". In fact, we identify the following fundamental components: **(i)** ***MEC server***: It is 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)****:* This is the SC device which has been enriched with a MEC server; **(iii)** ***CESC cluster****:* A group of CESCs that are collocated, able to exchange information and properly coordinated; as a trivial case, a CESC cluster could comprise one CESC; **(iv)** ***Light Data Center (Light DC)****:* It is a cluster of MEC servers. In particular, the Light DC is a logical entity consisting of a set of distributed MEC servers of the same CESC cluster; **(v)** ***Virtual Infrastructure Manager (VIM)****:* This is an entity responsible for management of the virtual hardware (i.e., Virtual Machines-VMs) and networking resources of a single Light DC; in particular, the VIM manages the lifecycle, provision, placement, and operation of VMs. The VIM is also responsible for the allocation of Virtual Network Functions (VNFs) over the hardware it manages and offers functionalities to control virtual networks across VNF instances and associate storage to them. The VIM offers an aggregated view of compute, network and storage resources of the Light DC; **(vi)** ***CESC Manager (CESCM)****:* The architectural component in charge of managing and orchestrating the cloud environment of the Light DC; it can simultaneously manage multiple clusters, a cluster or a single CESC. The CESC Manager also manages the radio access and "*self-x*" functionalities, e.g., self-optimising, self-healing and self-configuring of the Small Cells contained in each CESC cluster, in order to guarantee the service continuity and the required performance of services. The CESCM orchestrates

services and, *consequently*, manages the VIM to compose them with virtual resources. A CESCM is actually a functionality that will be "mapped" on to the distributed physical elements. As mentioned before, one important feature of this architecture is the distributed set of MEC servers which can logically "be grouped into clusters", thus effectively forming a Light DC at the network edge. Clusters are able to communicate with each other as well as with the mobile core network (i.e., Evolved Packet Core (EPC) in LTE terminology). The distributed deployment of MEC servers facilitates flexible and dynamic allocation of resources in cases of flash crowd events and fast EU mobility.

4 Security and Privacy Considerations

Network and system security is a very critical issue because the SESAME system is expected to support both customer enterprises and end users, who cannot tolerate financial losses or data privacy violations and, *therefore*, they seek the highest possible security guarantees. In the present section, the considered SESAME scenario and functional components are evaluated by using a formal methodology known as the *Secure Tropos (SecTro)* [16]. Our goal is to identify, model and analyse security issues from the early stages of system design and software development as well as to model and analyse threats and vulnerabilities in existing software and protocols that will be used in the SESAME system. We aim at preventing a wide range of attacks, such as control hijacking, reverse engineering, malware injection, eavesdropping, *just to name a few*. At the same time, the innovative SESAME concepts and technologies can provide invaluable opportunities of developing modern solutions for attack prevention, management and recovery.

First of all, the physical security of CESC infrastructure and hardware integrity has to be ensured. Hence, appropriate security controls (such as those in [17]) should be deployed by the CESC infrastructure owner, to prevent hardware tampering. Likewise, it is important to consider attacks that are initiated from the cloud side. This is particularly relevant in scenarios where multiple enterprises using private clouds are hosted. Especially in the multi-tenant environment of SESAME, the adversary *per se* could be a legitimate tenant interacting with network entities by using valid credentials and having privileged *access* to virtualised resources. Also, the emerging *Bring Your Own Device (BYOD)* trend [18] in many enterprises constitutes many conventional security solutions incapable of protecting the private network; for example, a Trojan horse, that infected an employee's device, can bypass the security of the corporate firewall. Hence, the cloud provider must ensure the physical security of the cloud infrastructure and of the data centres. This can be done, *e.g.*, by following the recommendations from the *Cloud Security Alliance* [19]. Moreover, the selection of suitable cloud provider can be based on formal methodologies to ensure that the security and privacy requirements are properly met [20]. This effectively means that services offered by cloud providers who do not meet the specified requirements and have not implemented the mandatory security controls, could so be restricted or even could be blocked. To ensure confidentiality and integrity of the User Equipment (UE) data, cryptographic security controls must be in place. This is to say that any adopted

Public-Key scheme that enables the encryption of the communications among CESC, UE and the cloud, must be sufficiently secure. Cryptographic and privacy protection techniques are particularly important in cases where an EU receives service from multiple service or network providers, due to mobility or QoE considerations.

An important category of attacks could potentially "target" the management system (for example, if initiated inside virtualised environments and aims at taking control of the Hypervisor shown in Fig. 2). Also, the NFV Orchestrator is an attractive "attack target" due to being in the "middle" of the system model architecture; the same can be for other components of the management layer, such as the VNF Manager. Also, impersonation by the adversary of one of the VNFs or the MEC server when communicating with the management layer could be a potential threat. Considering again the virtualised environment, both host and guest Operating Systems (OSs) may be targeted, and to alleviate the impact of such an attack, adequate isolation must be enforced between guest VMs, as well as between the host and guest VMs. The adversary could attempt to break the isolation by exploiting, *e.g.*, some flaws of the used virtualisation platform [12]. Therefore, appropriate choice of the virtualisation platform that meets security and privacy requirements is of major importance.

In some cases, to launch an attack against a component, the adversary requires that this component has specific exploitable configuration or runs specific software. For example, a precondition for a *Denial-of-Service (DoS) attack* can be specific configuration of the CESCM with regard to the allocation of resources to tenants. Yet, some flaws in the resource allocation algorithm can allow the adversary to prevent a tenant from accessing its portion of virtual resources. The introduction of the MEC paradigm has also implications on the E2E security in 5G networks. A potential solution for this problem is to facilitate the network slicing concept, according which each application or network flow get its own slide of the network. This allows the end-to-end security to be enforced within each slice by each application individually and any security breaches would not affect other applications. As security will be a fundamental enabling factor of future 5G networks, we are concerned with identifying and mitigating security threats and vulnerabilities against a broad range of targets at the intersection of MEC with *"Small Cells-as a-Service"* (SCaaS), SDN, and NFV. These will have crucial effect on legal and regulatory frameworks as well as on decisions of businesses, governments, and end users.

4.1 Scenario: *Enabling Large Multi-Tenant Enterprise Services by using MEC*

To further emphasize, we consider a Small Cell Network Operator (SCNO) who is providing a radio interface to a number of distinct mobile operators (MOs), virtual mobile network operators (VMNOs) and virtual small cell network operators (VSCNOs). The SCNO may transmit by using licensed or unlicensed spectrum over the air interface. In addition to the provision of radio coverage in the business centre and orchestration of multi-tenancy, the SCNO offers a platform for MEC for low latency and compute intensive applications/services. The MOs, VMNOs and VSCNOs provide both in-house and third party services from over-the-top (OTT) players or the service providers (SPs). The offered services can include *inter-alia*: multi-person real-time video-conferencing, virtual presence 360° video

communications with meetings using virtual presence glasses/devices, and assisted reality to actively inform users of ambient interests such as danger warnings to support people with disabilities and improve interactions with their surroundings.

The End Users (EUs) can benefit from fast and cost-effective access to a wide variety of innovative services from third party players. MOs, VMNOs and VSCNOs can benefit from extra market share. Venue owners (VOs) can benefit from having a single set of radio and IT equipment installed on the premises, instead of multiple installations from multiple network operators. The CESC is made up of: hardware resources, virtualisation layer, virtual network functions (VNFs), and an Element Management System (EMS). The virtualisation layer abstracts the hardware resources and decouples the VNF software from the underlying hardware. A VNF is a virtualisation of a network function in a legacy non-virtualised network. The EMS performs management of one or more VNFs. A cluster of CESCs is managed by the CESCM that constitutes of: virtualised infrastructure manager (VIM), VNF manager and the network functions virtualisation orchestrator (NFVO). The VIM manages the interaction of a VNF with the compute, storage and network resources under its specific authority. The VNF manager is responsible for VNF lifecycle management. The orchestrator is in charge of orchestration, of management NFV infrastructure and software resources and of realising network services.

In Fig. 3 we demonstrate *how this scenario can be supported by the specific SESAME system*. In particular, we see a CESC infrastructure provider who owns, deploys and maintains the network of CESCs inside the premises where different enterprises are hosted. The CESC provider has a *Service Level Agreement (SLA)* with each customer enterprise and SLAs are to enable enterprise users to a number of services offered by the CESC network; the SLA shall cover the target performance metrics for any service (or service category) required by each enterprise, supporting different tenants' requirements. Such sort of services can be categorised in data services and real-time services: these can include, *inter-alia*, Internet access for enterprise users, web browsing, file sharing, electronic mail service, voice communications and video conferencing. The deployment of MEC servers with high processing capabilities can enable close-to-zero latency and enhanced QoE of the enterprise users (i.e., an enhanced handling of the media flows and, *consequently*, an optimal QoE). In addition to the computing resources, MEC servers can provide storage resources and support content caching at the network edge. The reality is that different hosted enterprises may have different traffic patterns which may fluctuate greatly, depending on the time of the day or on special occasions, such as popular events. This leads to the requirement of a "flexible" system which can be scaled up and down, *on demand*. For example, most enterprises may need a higher capacity and higher quality of service (QoS) during the office hours, while a security firm providing security to the building would need a low capacity and the same service quality throughout the day. The main issues may arise from possible service disruptions and from the dynamicity of the enterprise activity. The service quality levels can be dynamic (time variant) as well. In some instants, the total capacity and the number of connected devices for a certain enterprise could rise significantly. This can be an event like an Annual General Meeting or a conference/exhibition organised by the enterprise. This extra capacity / connections may not need the same QoS and may not access the internal enterprise data, so may not need the same level of security. The main requirements are for the available capacity to be rapidly scaled up

and other virtual network(s) created mainly for open access. Also in some cases, certain enterprises may downsize their operations or move out of the premise, which requires scaling down. This kind of scalability and flexibility needs to be incorporated into the design of particular use cases for this representative scenario.

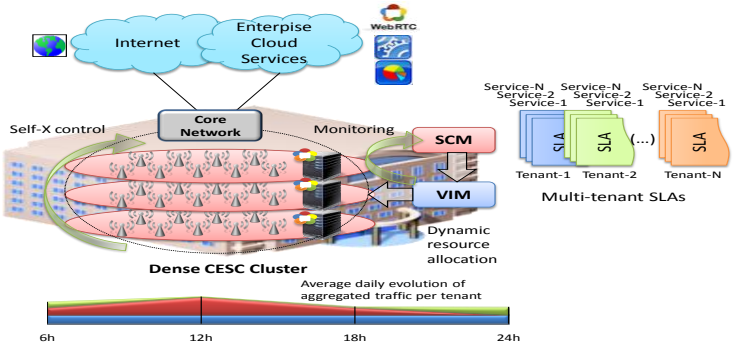

Fig. 3. Scenario: Enterprise services in multi-tenant large businesses

The enterprise scenario shown in Fig. 3 will leverage on SESAME features such as intrinsic support of multi-tenancy by enabling multiple SC operators since Small Cells operators to provide network services and connectivity over the network owned by a single CESC infrastructure provider. Furthermore, the SESAME system allows native incorporation of self-organizing network techniques, which can be adapted to network behaviour and can optimize service delivery to the enterprise users. In any case, the high level of network security as demanded by the enterprise customers will be an inherent feature of the respective SESAME solutions.

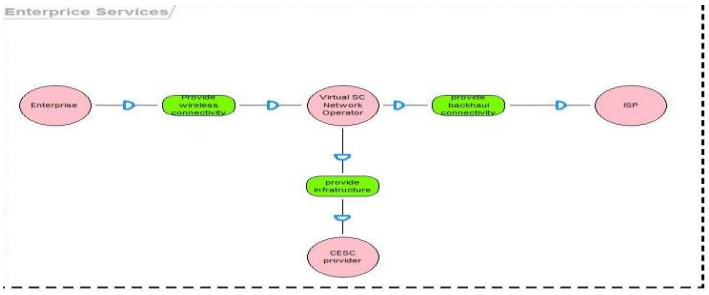

Fig. 4. Involved actors in the selected scenario

In Fig. 4, we present the actors involved in the scenario, their corresponding goals as well as their dependencies. We identify four major actors, namely CESC infrastructure provider, Virtual SCNO, ISP and enterprise. The enterprise depends on the SC operator which provides the wireless connectivity. The SC operator requires

backhaul connectivity and access to external networks, such as Internet. This can be provided by an ISP. Finally, the SC operator in order to provide its services to multiple enterprises depends on the CESC infrastructure which is owned and maintained by the CESC provider.

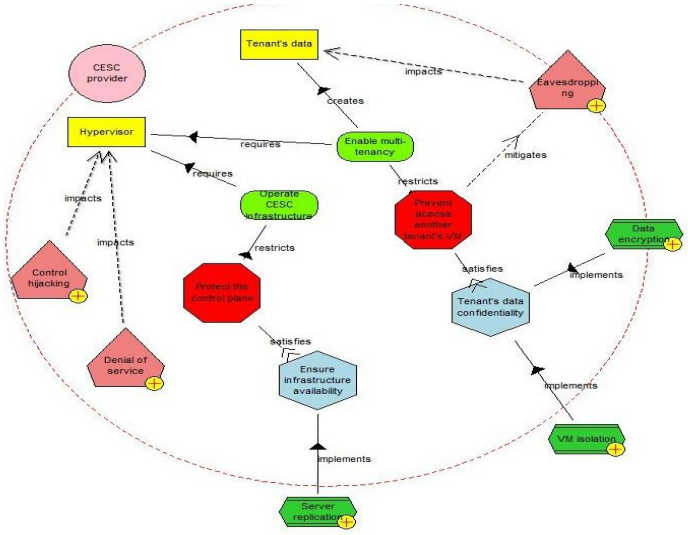

Fig. 5. Security components view for the CESC provider

In Figs. 5 and 6 we present the *Security Components View* for two main actors of this scenario: the *CESC provider* and the *virtual SCNO*. The security component view of the CESC provider, depicted in Fig. 5, contains two "resources" that need to be protected: the *Hypervisor* and the *Tenant's Data*. A resource in the *Secure Tropos terminology* could be a physical or an informational entity, and in the *SecTro* tool is depicted as a yellow, rectangular box. A resource is required to achieve a specific "goal" of an actor (the CESC provider in this example). A goal represents an actor's strategic interests. In this example, we consider two primary goals (depicted as green ovals): *operating the CESC infrastructure* and *enabling multi-tenancy*. Both these goals require the Hypervisor as a primary resource. Also, to enable multi-tenancy, the Tenant's Data resource has to be created. A goal could be restricted by a "security constraint" (depicted as a red octagon). In this example, the CESC infrastructure operation is restricted by the requirement to *protect the control plane*, whereas the multi-tenancy goal is restricted by the requirement to *prevent unauthorized access to another tenant's VM*. Various security constraints must satisfy a number of "security objectives" (depicted as blue hexagons). In this example, the security constraints are satisfied by the two objectives: *Protect the Control Plane* and *Prevent Access to another Tenant's VM*. These objectives are implemented by using a number of "security mechanisms" (green hexagons), such as VM isolation, Data Encryption, and Server Replication. We also consider a number of "threats" (depicted as pentagons) that impact some of the resources. In this example, the Hypervisor can be

impacted by the two threats: *Control Hijacking* and *Denial of Service*. The Tenant's Data resource can be impacted by the *Eavesdropping* threat.

The security component view of the Virtual SCNO, depicted in Fig. 6, contains three resources that need to be protected: the *Radio Resources*, the *Radio Spectrum* and the *Element Management System (EMS)*. In this example, the actor's primary goals (that require the above resources) are to provide wireless capacity and spectrum to the tenants. The corresponding security constraints that restrict these goals are to *protect the management plane*, to *prevent unauthorized access to the wireless spectrum* and to *protect user data.* These constraints must be satisfied by two security objectives: *Ensure service availability* and *ensure data confidentiality*. The corresponding security mechanisms to implement these objectives are using firewalls and access control mechanisms. Finally, a number of threats could impact the considered resources, such as *DoS, control hijacking* and *radio jamming attacks*.

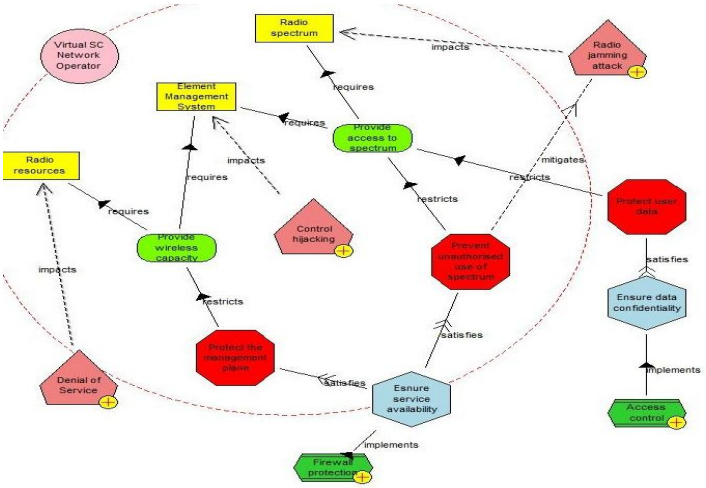

Fig. 6. Security components view for the virtual SC network operator (SCNO)

Acknowledgments. The present work has been performed in the scope of the *SESAME* ("*Small cEllS CoordinAtion for Multi-tenancy and Edge services*") European Research Project and has been supported by the Commission of the European Communities (*5G-PPP/H2020, Grant Agreement No.671596*).

References

1. Demestichas, P., Georgakopoulos, A., et *al.*: 5G on the Horizon: Key Challenges for the Radio-Access Network. IEEE Vehicular Technology Magazine 8(3), 47--53, (2013)
2. Andrews, J.G.: Seven Ways that HetNets are a Cellular Paradigm Shift. IEEE Communications Magazine, 51(3), 136--144, (2013)

3. Nunes, B.A.A., Mendonça, M., Ngyen, X.-N., Obraczka, K., Turletti, T.: A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. IEEE Communications Surveys and Tutorials, 16(3), 1--18, (2014)
4. Mosharaf, N.M., Chowdhury, K., and Boutaba, R.: A Survey of Network Virtualization. Computer Networks, 54(5), 862--876, (2010)
5. Haleplidis, E., Salim, J.H., Denazis, S., et *al.*: Towards a Network Abstraction Model for SDN. Journal of Network and Systems Management, 23(2), 309--327, (2015)
6. Shrivastava, R., Constanzo, S., Samdanis, K., Xenakis, D., Grace, D., Merakos, L.: An SDN-based Framework for Elastic Resource Sharing in Integrated FDD/TDD LTE-A HetNets. In: Proceedings of the 3rd IEEE International Conference on Cloud Networking (CloudNet), pp. 126--131. IEEE Press, New York (2014)
7. European Telecommunications Standards Institute (ETSI): Mobile-Edge Computing, Introductory Technical White Paper. ETSI, Sophia-Antipolis (2014)
8. Vaquero, L.M., Rodero-Merino, L.: Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing. ACM SIGCOMM Computer Communication Review, 44(5), 27--32, (2014)
9. Fetweiss, G.P.: The Tactile Internet: Applications and Challenges. IEEE Vehicular Technology Magazine, 9(1), 64--70, (2014)
10. SESAME H2020 5G-PPP Project (Grant Agreement No.671596), http://www.sesame-h2020-5g-ppp.eu/Home.aspx.
11. Lee, K., Kim, D., Ha, D., Rajput, U., Oh, H.: On Security and Privacy Issues of Fog Computing supported Internet of Things Environment. In: Proceedings of the 6th IEEE International Conference on the Network of the Future (NOF), pp. 1--3. IEEE (2015)
12. Stojmenovic, I., Wen, S., Huang, X., Luan, H.: An Overview of Fog Computing and its Security Issues. Concurrency and Computation: Practice and Experience (2015, April)
13. Wang, Y., Uehara, T., Sasaki, R.: Fog Computing: Issues and Challenges. In: Proceedings of the 39th IEEE Annual COMPSAC Conference, pp. 53--59. IEEE (2015)
14. Stolfo, S.J., Salem, M.B., Keromytis, A.D.: Fog Computing: Mitigating insider Data Theft attacks in the Cloud. In: Proceedings of the IEEE Symposium on Security and Privacy Workshops (SPW), pp. 125--128. IEEE (2012)
15. Lopez, P.G., Montresor, A., Epema, et *al.*: Edge-centric Computing: Vision and Challenges. ACM SIGCOMM Computer Communication Review, 45(5), 37--42, (2015)
16. Mouratidis, H., Giorgini, P.: Secure Tropos: A Security-Oriented Extension of the Tropos Methodology. International Journal of Software Engineering and Knowledge Engineering, 17(2), 285--309, (2007)
17. Skorobogatov, S.: Physical Attacks and Tamper Resistance. In: Introduction to Hardware Security and Trust, pp. 143-173. Springer, New York (2011)
18. Buetnner, R.: Towards a New Personal Information Technology Acceptance Model: Conceptualization and Empirical Evidence from a Bring Your Own Device Datataset. In: Proceedings of the 21st AMCIS. AIS, Fajardo, Puerto-Rico (2015)
19. Cloud Security Alliance (CSA): Security Guidance for Critical Areas of Focus in Cloud Computing v2.1. CSA (2009)
20. Mouratidis, H., Islam, S., Kalloniatis, C., Gritzalis, S.: A Framework to Support Selection of Cloud Providers based on Security and Privacy Requirements. Journal of Systems and Software, 86(9), 2276--2293, (2013)