

On the Security of Software-Defined Next-Generation Cellular Networks

Vassilios G. Vassilakis*, Ioannis D. Moscholios[†], Bander A. Alzahrani[‡], Michael D. Logothetis[§]

* School of Computing & Engineering, University of West London, London, United Kingdom

[†] Dept. of Informatics & Telecommunications, University of Peloponnese, Tripolis, Greece

[‡] Information Systems Department, King Abdulaziz University, Jeddah, Saudi Arabia

[§] Dept. of Electrical & Computer Engineering, University of Patras, Patras, Greece

Abstract—In the recent years, mobile cellular networks are undergoing fundamental changes and many established concepts are being revisited. Future 5G network architectures will be designed to employ a wide range of new and emerging technologies such as Software Defined Networking (SDN) and Network Functions Virtualization (NFV). These create new virtual network elements each affecting the logic of the network management and operation, enabling the creation of new generation services with substantially higher data rates and lower delays. However, new security challenges and threats are also introduced. Current Long-Term Evolution (LTE) networks are not able to accommodate these new trends in a secure and reliable way. At the same time, novel 5G systems have proffered invaluable opportunities of developing novel solutions for attack prevention, management, and recovery. In this paper, first we discuss the main security threats and possible attack vectors in cellular networks. Second, driven by the emerging next-generation cellular networks, we discuss the architectural and functional requirements to enable appropriate levels of security.

Keywords—5G networks; security; software-defined networking; network function virtualization.

I. INTRODUCTION

In the recent years we are witnessing a widespread use of end user devices with advanced capabilities, such as smartphones and tablet computers, and the emergence of new services and communication technologies. Today, a large variety of Radio Access Technologies (RATs) and heterogeneous wireless networks have been successfully deployed and used. Also, the coverage of such wireless and cellular networks has increased substantially by deploying more Base Stations (BSs) and Access Points (APs).

It is evident that next-generation cellular networks will benefit from the recent advances in Software Defined Networking (SDN) [1], [2] and Network Function Virtualization (NFV) [3], [4]. Traditionally, SDN and NFV, although not dependent on each other, are seen as closely related and complementary concepts [5]. This integration enables good scalability in terms of supporting a large number of connections and 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], [7] as well as in the Mobile Core Network (MCN) [8].

The adoption of aforementioned technologies introduces new virtual network elements each affecting the logic of the network management and operation, enabling the creation of new generation services with substantially higher data rates and lower delays. However, new security challenges and threats are also introduced [9]. At the same time, novel next-generation systems have proffered invaluable opportunities of developing novel solutions for attack prevention, management and recovery. As security has always been a concern in the cellular industry and research communities, there is a consensus that the security of cellular systems, networks, and applications has to be studied and tackled adequately.

This paper is organized as follows. In Section II, we present the related work on SDN-based cellular architectures. In Section III, we describe our considered reference architecture for next-generation cellular networks, which is based on SDN and NFV. In Section IV, we discuss some of the main security threats in cellular networks and identify potential attack vectors. In Section V, we propose the architectural and functional enhancements to support security in next-generation cellular networks. In Section VI, as an example, we describe the realization of secure content delivery in a virtualized RAN. We conclude in Section VII. Finally, in Appendix A we present the list of abbreviations used in the paper.

II. RELATED WORK

In this section, we present the most important, recent works in the area of next-generation cellular networks security. In [10], potential security requirements and mechanisms for 5G networks are discussed. The focus is mainly on the security aspects of SDN and NFV, and on the differences compared to the security requirements of traditional Long-Term Evolution (LTE) networks, such as: confidentiality of user and device identity; location privacy; entity authentication; signalling data confidentiality; user data confidentiality; and platform security requirements.

In [11], the security of 5G wireless transmissions is studied. The technologies that have been analyzed are: Heterogeneous Networks (HetNets); Multiple-Input Multiple-Output (MIMO) systems, and millimeter wave wireless communications. In particular, the focus on physical layer security and the protection of data confidentiality by exploiting the intrinsic randomness of the wireless communications medium.

In [12], the security threats and their corresponding countermeasures with respect to the data layer, control layer,

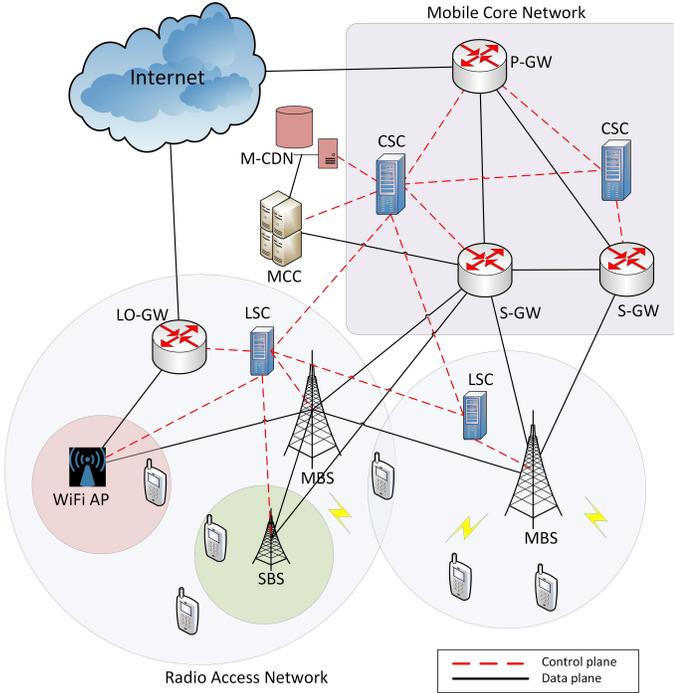


Fig. 1. A Software-Defined Cellular Network Architecture [13].

application layer, and communication protocols of SDN-based cellular network are explored. Various security threats are classified and the open security challenges are discussed in the context of SDN-based cellular networks.

The aforementioned works show that there is a need to consider the existing security threats as well as to prevent any new threats and risks that could arise. Our current work tries to contribute towards these efforts. In this paper, first we discuss the main security threats and possible attack vectors in cellular networks. Second, driven by the emerging next-generation cellular networks, we discuss the architectural and functional requirements to enable appropriate levels of security.

III. A SOFTWARE-DEFINED CELLULAR NETWORK ARCHITECTURE

In this section, we present our considered reference architecture for software-defined next-generation cellular networks [13]. This architecture has benefited from the recent advances in SDN and NFV technologies. Below, we describe the RAN and the MCN of the reference architecture (see also Fig. 1).

A. Radio Access Network (RAN)

The RAN consists of Small-cell BSs (SBSs), Macro-cell BSs (MBSs), WiFi APs, Local Offload Gateways (LO-GWs), and MUs. These are coordinated by the Local SDN Controller (LSC). The RAN is divided into clusters, with each cluster covering one or more macro cells and being controlled by a dedicated LSC. The notion of clusters is similar to the notion of Tracking Areas (TAs) in LTE networks. For simplicity, in Fig. 1 each one of the two LSCs controls a cluster covering only a single macro cell.

A LSC is responsible for receiving connection requests from its cluster and for allocating appropriate destination address. This is performed by the Local Request Resolution Function (LRRF). In particular, the LRRF will facilitate the connection establishment either with an in-cluster entity (MU, SBS, etc.) or will forward the request to the MCN. Hence, the LRRF is aware of the network topology within the cluster and of egress nodes connections towards the MCN and other clusters. The LRRF can also achieve load-balancing and other optimization objectives [14].

Other functions of a LSC include the Multi-RAT Coordination Function (MRCF) and the Local Content Caching Function (LCCF). The MRCF is responsible for allocating radio resources in geographical areas where more than one RAT is available. It can be seen as the Access Network Discovery and Selection Function (ANDSF) [15], enhanced with traffic offloading capabilities, using schemes such as the Selected IP Traffic Offload (SIPTO) or the Local IP Access (LIPA) [16].

The LCCF observes content requests from in-cluster MUs and keeps track of the localized content popularity. Based on that and on the knowledge of available storage resources in the cluster, the LCCF is responsible for caching decisions within the cluster. Most of caching solutions exploit the fact that the popularity distribution of content objects follows the Zipf-Mandelbrot distribution [17]. This means that even by allocating relatively small storage space, high cache hit ratio can be achieved [18]. This can greatly reduce the content access delay and the traffic going via the MCN [19].

Local routing decisions are performed by the Local Content Routing Function (LCRF). The LCRF receives requests from the LRRF to construct the content delivery path to a local source. Then it configures the Flow Tables at the data plane forwarding elements. A LSC is also responsible for steering the Device-to-Device (D2D) communication via the Device Control Function (DCF). This can be achieved using technologies such as LTE Direct [20], WiFi, or Bluetooth for data transfer between MUs, while the control channels to/from the BS may use licensed spectrum [21]. Furthermore, by co-designing the LCRF with the LCCF, joint optimisation of caching and routing logic can be achieved [22].

Finally, a LSC is handling the in-cluster mobility via the Local Mobility Management Function (LMMF). Hence, this information is not passed to the MCN, which greatly reduces the processing and signalling overhead, due to reduced paging messages [23]. This also enables native and elegant incorporation of distributed mobility management schemes [24]. Furthermore, SDN-assisted mobility management can efficiently support even fast moving users/vehicles assuring acceptable Quality-of-Experience (QoE) [25].

B. Mobile Core Network (MCN)

The MCN consists of a distributed set of Core SDN Controllers (CSCs), Mobile Cloud Computing (MCC) infrastructure, Mobile Content Delivery Network (M-CDN) servers, Packet Data Network Gateways (P-GWs), and Serving Gateways (S-GWs). A CSC is responsible for receiving and handling connection requests from a set of dedicated clusters, performed by the Core Content Resolution Function (CCRF),

and for carrying out the mobility management, via the Core Mobility Management Function (CMMF).

Management of storage (i.e., M-CDN or in-network caches), computing (i.e., MCC), spectrum, and energy resources, as well as QoE support, is performed by the Resource Management Function (RMF). RMF's decisions on the allocation of (both physical and virtualised) resources are based on a number of factors, such as current demand and consumption, monitored radio network conditions, MU density and mobility patterns. To support energy-efficient operation, the RMF is responsible for moving the virtualized resources away from heavily underutilized clusters and for switching some of the equipment off. This enables energy savings during off-peak hours. The role of a P-GW and a S-GW is similar to the role of homonymous entities in LTE networks, but is restricted to data plane only. The corresponding control plane functionality is performed by a CSC (in accordance with the SDN concept). In particular, a P-GW is used to access the external IP networks, whereas a S-GW is used to access the RAN.

IV. SECURITY THREATS AND ATTACK VECTORS

Below we discuss some of the main security threats in cellular networks and identify potential security attack vectors. In particular, we discuss the Denial of Service (DoS), Privacy Violation Attacks (PVA), Location Spoofing Attacks (LoSA), Operations, Administration and Management Traffic Spoofing Attacks (OAM-TSA), and Physical Tampering Attacks (PTA).

A. Denial of Service (DoS)

DoS attacks nowadays constitute a serious problem as more and more websites and companies are targets of such attacks. On the other hand, it is very hard to ensure appropriate levels of protection against them [26]. DoS is a significant threat mainly when the access to the MCN from BSs is done over untrusted networks (e.g., the Internet). Regarding the issue of DoS attacks that originate from the RAN side, this is generally considered as a low threat. The reason is that the traffic from BSs towards the MCN consists mainly of data traffic originating from MUs and management traffic originating from BSs. This traffic is generally considered very small to cause serious DoS.

B. Privacy Violation Attacks (PVA)

The privacy of MUs is a very important and sensitive topic. It has especially gained attention due to recently reported privacy violations and concerns from mobile network operators as well as the MUs. It is important to develop appropriate trust models and privacy policies to that the cellular infrastructure and communication channels can be trusted by the subscribers [27]. Regarding the radio communication part (channels between MUs and BSs), the interfaces according to 3GPP standards generally hide the MU identity information [28]. Also, to secure the backhaul (channels between BSs and MCN), IPsec tunneling is used to transfer the traffic. This aims, among others, at securing MU identities against eavesdroppers, contrary to what happens in open backhaul networks, such as the Internet.

C. Location Spoofing Attacks (LoSA)

Location verification is another important aspect that mainly concerns the SBSs. The aim is to ensure that the SBSs are deployed only in authorized locations, so that deployment of bogus SBSs is prevented. A LoSA tries to make the MCN believe that the SBS resides at locations different than its real physical locations. To address this issue, Global Positioning System (GPS) tracking and “sniffing” the cellular network environment can be used to verify and confirm the SBS location. However, even these measures are sometimes not sufficient and more sophisticated protection techniques need to be developed [29].

D. Operations, Administration and Management Traffic Spoofing Attacks (OAM-TSA)

An attacker may try to spoof the OAM traffic to disrupt the normal operation of the cellular network. To avoid this, OAM traffic from BSs must be encrypted and transported via an IPsec tunnel. This makes it harder for an attacker to spoof it from an untrusted backhaul network or from the BS itself. However, there could also be other threats. For example, there would be a possibility of insider attacks on the path from the S-GW to OAM [30].

E. Physical Tampering Attacks (PTA)

Although security is a critical aspect of any wireless communication system, the case of dense small cell deployments needs particular attention. SBSs can be easy targets of various security attacks if no adequate security measures are taken [31]. This is further complicated by the requirement for automated configuration of residential SBSs. That is, the customers expect they simply plug the SBS into their broadband connection and allow it to configure itself and join the cellular network. Hence, an important security requirement is the mutual authentication of the SBS and the rest of the cellular network. It is also expected that once the SBS joins the network it can be fully controlled by the network operator. Hence, to prevent a PTA by a malicious customer, the SBSs must be protected by a variety of mechanical and electronic techniques.

V. SECURITY ARCHITECTURE

Having identified the main security threats and potential security attack vectors in Section IV, in this section we propose the required architectural and functional enhancements for the reference architecture presented in Section III. In particular, we introduce the Security Gateway (SeGW), the IPsec tunnelling and the Security Policy Manager (SPM), and discuss the required security enhancements of the Home Subscriber Server (HSS) and the Element Management System (EMS).

A. Security Gateway (SeGW)

As suggested by the 3GPP, when the access to the MCN from BSs is done over untrusted networks (e.g., the Internet), the protection can be provided by a SeGW. A typical SeGW has mechanisms to protect against DoS attacks from the public Internet. A SeGW can be placed at the edge of the MCN to secure traffic to/from the RAN. The reason is that the backhaul

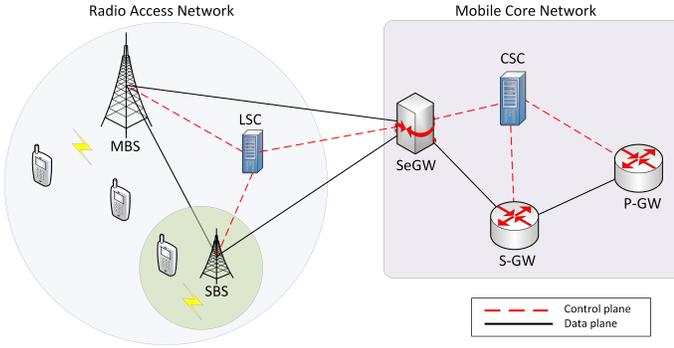


Fig. 2. Security Architecture.

network may be insecure. Hence, the SeGW will enable communication via secure tunnels to protect the information transmitted over the backhaul network. As shown in Fig. 2, SeGW participates both in the control plane and data plane. Before establishing the secure tunnel, the SeGW performs a mutual authentication with the LSC for control traffic and with the BS for data traffic. If and only if the authentication is successful, the incoming traffic will be allowed to the MCN. That is, to ensure secure operation, the SeGW must use certificates to perform mutual authentication with the LSC and the BS. The SeGW will filter out any received unauthenticated traffic.

B. IPsec Tunneling

For secure tunnelling between the MCN and the RAN, the IPsec protocol can be used [32]. To establish the IPsec tunnel, the Internet Key Exchange (IKE) v2 authentication protocol [33] may be used as specified in [34]. The IKEv2 configuration payload is used to provide the BS with an inner IP address, which is then used in IPsec tunnel mode operations for communication with the SeGW. The SeGW can check the status of the supplied certificate using a Certificate Revocation List (CRL) [35] or the Online Certificate Status Protocol (OSCP) [36]. Finally, to provide integrity, confidentiality, and replay protection for data in the IPsec tunnel, the Encapsulated Security Payload (ESP) protocol may be used [37].

C. Security Policy Manager (SPM)

To configure and enforce security policies, SPM has been introduced. This function, is part of a CSC and configures the RAN infrastructure according to specified policies, installs/upgrades the protection and performs location verification of untrusted equipment, such as a SBS. Since the SPM has been placed behind the SeGW, no transport layer security is required. Otherwise, this connection must be secured, e.g., via the Transport Layer Security (TLS) protocol [38].

D. Home Subscriber Server (HSS)

For holding the subscription data and authentication information for MUs, a HSS can be used. In addition to its usual functionality, the HSS can also be used for enforcing a more fine grained access control. For example, it may restrict MU access to specific parts of the cellular network or to specific insecure equipment.

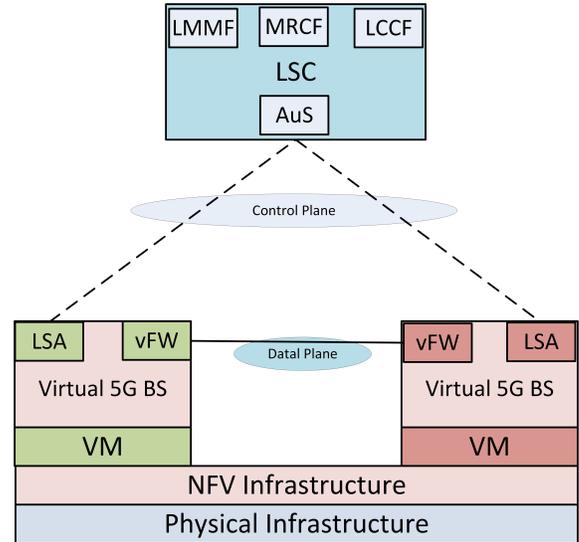


Fig. 3. Virtualized Radio Access Network.

E. Element Management System (EMS)

To secure the communication of the EMS with the BS via an untrusted network, certificate-based mutual authentication must be performed. For this purpose, the TLS protocol can be used. Alternatively, the EMS and the BS could communicate via the SeGW. In this case, the communication between the BS and the SeGW can be secured via the IPsec and the ESP.

VI. SECURE CONTENT DELIVERY IN VIRTUALISED RAN

In this section, we describe the realization of secure content delivery in a virtualised RAN. To enable efficient and smooth collaboration of LSCs within the RAN and with the MCN, NFV technology is used. NFV decouples the network functions from the underlying hardware, thus making these functions virtualized by allowing them to be migrated and instantiated on demand. This is realized via Virtual Machines (VMs), using tools like VMware [39] or VirtualBox [40]. Furthermore, low-cost and low-demand virtualization technologies, such as unikernels [41], enable migrating network functions and services even to MUs.

In Fig. 3, a model for a virtualized RAN using SDN and NFV is shown. A number of VMs, running on the same physical infrastructure, enable virtualized implementation of BSs via the available NFV Infrastructure (NFVI). As shown, LSC controls each virtual BS, within the corresponding cluster, via a dedicated Local SDN Agent (LSA). LSC has also been enhanced with the Authentication Server (AuS), which has the responsibility to authenticate all traffic coming from cluster BSs. Furthermore, each virtual BS is equipped with a Virtual Firewall (vFW) that can be used to control incoming and outgoing traffic according to specified security rules.

As an example, consider the virtualized content routing function that routes traffic between two BSs, as shown in Fig. 4. In this example, Bob wants to receive a *content object* from Alice. Let us assume that the request resolution has already taken place (via the LRRF) and the LSC knows that the content source is Alice. Let us also assume that Alice has been notified

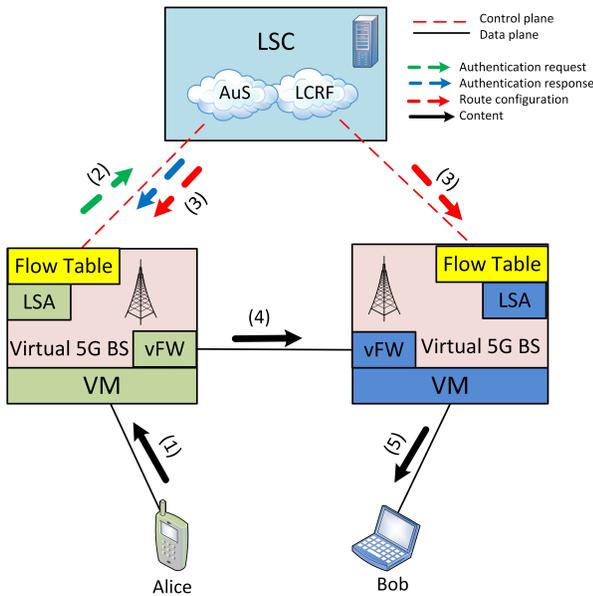


Fig. 4. Realization of Secure Local Content Routing Function.

about the content request. Initially, Alice will send the content to its attached BS. Next, the corresponding BS will send the *authentication request* message to the LSC. This message will be passed to the AuS. After that, the BS will receive the *authentication response* message. If the authentication attempt is successful, the LCRF will be informed to construct the delivery path and to configure the Flow Tables along the path by sending *route configuration* messages. After that, when the data plane forwarding entities (i.e., the two BSs) receive the requested content, they forward it to next hop according to the Flow Table.

Finally, to realize a secure inter-LSC communication, the IPsec protocol can be used. Neighboring LSCs may exchange information using X2 interfaces. In case the physical security of the involved LSCs is not assured, then the link can be secured using IPsec and ESP tunneling. The mutual authentication and authorization can be based on IKEv2. After that, a secured IPsec link is established between the two LSCs.

VII. CONCLUSION

In this paper, we first discuss the main security threats and potential attack vectors in a cellular network. Second, based on a reference software-defined cellular network architecture, we propose the required architectural and functional enhancements. In particular, we introduce the Security Gateway, the IPsec tunneling and the Security Policy Manager, and discuss the required security enhancements of the Home Subscriber Server and the Element Management System. Finally, we describe the realization of secure content delivery in a virtualized RAN. To achieve that, the Authentication Server and Virtual Firewalls have been introduced at the RAN level.

- ANDSF** Access Network Discovery and Selection Function
- AP** Access Point
- AuS** Authentication Server
- BS** Base Station
- CCRF** Core Content Resolution Function
- CMMF** Core Mobility Management Function
- CRL** Certificate Revocation List
- CSC** Core SDN Controller
- D2D** Device-to-Device
- DCF** Device Control Function
- DoS** Denial of Service
- EMS** Element Management System
- ESP** Encapsulated Security Payload
- GPS** Global Positioning System
- HetNet** Heterogeneous Network
- HSS** Home Subscriber Server
- IKE** Internet Key Exchange
- LCCF** Local Content Caching Function
- LCRF** Local Content Routing Function
- LIPA** Local IP Access
- LMMF** Local Mobility Management Function
- LO-GW** Local Offload Gateway
- LRRF** Local Request Resolution Function
- LSA** Local SDN Agent
- LoSA** Location Spoofing Attack
- LSC** Local SDN Controller
- LTE** Long-Term Evolution
- MBS** Macro-cell BS
- MCC** Mobile Cloud Computing
- M-CDN** Mobile Content Delivery Network
- MCN** Mobile Core Network
- MIMO** Multiple-Input Multiple-Output
- MRCF** Multi-RAT Coordination Function
- MU** Mobile User
- NFV** Network Function Virtualisation
- OAM** Operations, Administration and Management
- OCSP** Online Certificate Status Protocol
- P-GW** Packet Data Network Gateway
- PTA** Physical Tampering Attack
- PVA** Privacy Violation Attack
- QoE** Quality-of-Experience
- RAN** Radio Access Network
- RAT** Radio Access Technology
- RMF** Resource Management Function
- SBS** Small-cell BS
- SDN** Software-Defined Networking
- S-GW** Serving Gateway
- SeGW** Security Gateway

SIPTO Selected IP Traffic Offload
SPM Security Policy Manager
TA Tracking Area
TLS Transport Layer Security
TSA Traffic Spoofing Attack
vFW Virtual Firewall
VM Virtual Machine

REFERENCES

- [1] J. S. Thainesh, N. Wang, and R. Tafazolli, "A scalable architecture for handling control plane failures in heterogeneous networks," *IEEE Communications Magazine*, vol. 54, no. 4, April 2016, pp. 145-151.
- [2] X. Huang, R. Yu, J. Kang, N. Wang, S. Maharjan, and Y. Zhang, "Software defined networking with pseudonym systems for secure vehicular clouds," *IEEE Access* (in press), available online: April 2016, doi: 10.1109/ACCESS.2016.2560902.
- [3] I. Giannoulakis, E. Kafetzakis, G. Xylouris, G. Gardikis, and A. Kourtis, "On the applications of efficient NFV management towards 5G networking," *Proc. 1st International Conference on 5G for Ubiquitous Connectivity (5GU)*, Levi, Finland, Nov. 2014, pp. 1-5.
- [4] C. Liang, Chengchao, F. R. Yu, and X. Zhang, "Information-centric network function virtualization over 5G mobile wireless networks," *IEEE Network*, vol. 29, no. 3, May-June 2015, pp. 68-74.
- [5] E. Haleplidis, J. H. Salim, S. Denazis, and O. Koufopavlou, "Towards a network abstraction model for SDN," *Journal of Network and Systems Management*, vol. 23, no. 2, April 2015, pp. 309-327.
- [6] R. Shrivastava, S. Costanzo, K. Samdanis, D. Xenakis, D. Grace, and L. Merakos, "An SDN-based framework for elastic resource sharing in integrated FDD/TDD LTE-A HetNets," *Proc. IEEE International Conference on Cloud Networking (CloudNet)*, Luxembourg, Oct. 2014.
- [7] G. Tseliou, F. Adelantado, and C. Verikoukis, "Scalable RAN virtualization in multi-tenant LTE-A heterogeneous networks," *IEEE Transactions on Vehicular Technology* (in press), available online: Sept. 2015, doi: 10.1109/TVT.2015.2475641.
- [8] X. Jin, L. E. Li, L. Vanbever, and J. Rexford, "Softcell: Scalable and flexible cellular core network architecture," *Proc. 9th ACM Conference on Emerging Networking Experiments and Technologies (CoNEXT)*, Santa Barbara, California, USA, December 2013, pp. 163-174.
- [9] Huawei White Paper, "5G security: Forward thinking," Dec. 2015.
- [10] G. Horn and P. Schneider, "Towards 5G security," *Proc. 4th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Helsinki, Finland, August 2015.
- [11] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, 2015, pp. 20-27.
- [12] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-defined mobile networks security," *Mobile Networks and Applications*, January 2015, pp. 1-15.
- [13] V. G. Vassilakis, I. D. Moscholios, B. A. Alzahrani, and M. D. Logothetis, "A software-defined architecture for next-generation cellular networks," *Proc. IEEE International Conference on Communications (ICC)*, Kuala Lumpur, Malaysia, May 2016.
- [14] M. Glabowski, S. Hanczewski, and M. Stasiak, "Modelling load balancing mechanisms in self-optimising 4G mobile networks," *Proc. 21st Asia-Pacific Conference on Communications (APCC)*, Kyoto, Japan, October 2015, pp. 74-78.
- [15] D. Triantafyllopoulou, T. Guo, and K. Moessner, "Energy efficient ANDSF-assisted network discovery for non-3GPP access networks," *Proc. 17th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Barcelona, Spain, September 2012, pp. 297-301.
- [16] K. Samdanis, T. Taleb, and S. Schmid, "Traffic offload enhancements for eUTRAN," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 3, July 2012, pp. 884-896.
- [17] Z. Silagadze, "Citations and the Zipf-Mandelbrot's law," *Complex Systems*, vol. 11, 1997, pp. 487-499.
- [18] X. Zhang, N. Wang, V. G. Vassilakis, and M. P. Howarth, "A distributed in-network caching scheme for P2P-like content chunk delivery," *Computer Networks*, vol. 91, November 2015, pp. 577-592.
- [19] I. M. Stephanakis, I. P. Chochliourous, G. L. Lymperopoulos, and K. Berberidis, "Optimal video delivery in mobile networks using a cache-accelerated multi area eMBMS architecture," *Proc. Artificial Intelligence Applications and Innovations*, Springer, 2014, pp. 13-23.
- [20] B. Raghothaman, E. Deng, R. Pragada, G. Sternberg, T. Deng, and K. Vanganuru, "Architecture and protocols for LTE-based device to device communication," *Proc. IEEE International Conference on Computing, Networking and Communications (ICNC)*, San Diego, USA, January 2013, pp. 895-899.
- [21] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklós, Z. Turányi, "Design aspects of network assisted device-to-device communications," *IEEE Commun. Mag.*, vol. 50, no. 3, 2012, pp. 170-177.
- [22] V. G. Vassilakis, M. F. Al-Naday, M. J. Reed, B. Alzahrani, K. Yang, I. D. Moscholios, and M. D. Logothetis, "A cache-aware routing scheme for information-centric networks," *Proc. IEEE/IET 9th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)*, Manchester, U.K., July 2014, pp. 721-726.
- [23] D. Xenakis, N. Passas, L. Merakos, and C. Verikoukis, "Mobility management for femtocells in LTE-Advanced: Key aspects and survey of handover decision algorithms," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, February 2014, pp. 64-91.
- [24] F. Giust, L. Cominardi, and C. Bernardos, "Distributed mobility management for future 5G networks: Overview and analysis of existing approaches," *IEEE Commun. Mag.*, vol. 53, no. 1, 2015, pp. 142-149.
- [25] V. G. Vassilakis, I. D. Moscholios, A. Bontozoglou, and M. D. Logothetis, "Mobility-aware QoS assurance in software-defined radio access networks: An analytical study," *Proc. IEEE Workshop on Software-Defined 5G Networks (Soft5G)*, London, U.K., April 2015.
- [26] R. P. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," *Proc. 16th IEEE International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Atlantic City, New Jersey, USA, June 2013, pp. 1-9.
- [27] S. Taddei and B. Contena, "Privacy, trust and control: Which relationships with online self-disclosure?," *Computers in Human Behavior*, vol. 29, no. 3, May 2013, pp. 821-826.
- [28] 3GPP2 S.S0132-0, "Femtocell Security Framework 1.0", Jan. 2010.
- [29] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," *Proc. 18th ACM Conference on Computer and Communications Security (CCS)*, Chicago, USA, October 2011, pp. 75-86.
- [30] 3GPP TS 33.320 V12.0.0 (2013-09), "Security of Home Node B (HNB) / Home evolved Node B (HeNB)" (Release 12)
- [31] Small Cell Forum, "Security for Small Cells," June 2014.
- [32] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to protect mobile IPv6 signaling between mobile nodes and home agents," *RFC 3776*, June 2004.
- [33] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet key exchange protocol version 2 (IKEv2)," *RFC 5996*, Sept. 2010.
- [34] 3GPP TS 33.310, "Network Domain Security (NDS); Authentication Framework (AF)".
- [35] D. Cooper, "Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile," *RFC 5280*, May 2008.
- [36] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "Online certificate status protocol-OCSP," *RFC 6960*, June 2013.
- [37] S. Kent, "IP encapsulating security payload (ESP)," *RFC 4303*, December 2005.
- [38] T. Dierks, "The transport layer security (TLS) protocol version 1.2.," *RFC 5246*, August 2008.
- [39] VMware, <http://www.vmware.com/> [May 2016].
- [40] VirtualBox, <https://www.virtualbox.org/> [May 2016].
- [41] A. Madhavapeddy, D. J. Scott, J. Lango, M. Cavage, P. Helland, and D. Owens, "Unikernels: Rise of the virtual library operating system," *Communications of the ACM*, vol. 11, no. 11, January 2014.