5G Security: Analysis of Threats and Solutions

Ijaz Ahmad*, Tanesh Kumar†, Madhusanka Liyanage‡, Jude Okwuibe§, Mika Ylianttila¶, Andrei Gurtov‖
*†‡§¶Centre for Wireless Communications, University of Oulu, Finland
‖ Department of Computer and Information Science, Linköping University, SE-581 83 Linköping, Sweden
Email: [*Ijaz.Ahmad,†Tanesh.Kumar‡Madhusanka.Liyanage§Jude.Okwuibe¶Mika.Ylianttila]@oulu.fi
‖gurtov@acm.org

***Abstract*—5G will provide broadband access everywhere, entertain higher user mobility, and enable connectivity of massive number of devices (e.g. Internet of Things (IoT)) in an ultra-reliable and affordable way. The main technological enablers such as cloud computing, Software Defined Networking (SDN) and Network Function Virtualization (NFV) are maturing towards their use in 5G. However, there are pressing security challenges in these technologies besides the growing concerns for user privacy. In this paper, we provide an overview of the security challenges in these technologies and the issues of privacy in 5G. Furthermore, we present security solutions to these challenges and future directions for secure 5G systems.**

***Index Terms*—Security; 5G Security; SDN; NFV; Cloud; Privacy; Communication Channels**

I. Introduction

The vision of 5G wireless networks lies in providing very high data rates and higher coverage through dense base station deployment with increased capacity, significantly better Quality of Service (QoS), and extremely low latency [1]. To provide the necessary services envisioned by 5G, novel networking, service deployment, storage and processing technologies will be required. Cloud computing provides an efficient way for operators to maintain data, services and applications without owning the infrastructure for these purposes. Therefore, mobile clouds using the same concepts will bring technologically distinct systems into a single domain on which multiple services can be deployed to achieve a higher degree of flexibility and availability with less Capital Expenditures (CapEx) and Operational Expenses (OpEx).

Softwarizing the network functions will enable easier portability and higher flexibility of networking systems and services. Software Defined Networking (SDN) enables network function softwarization by separating the network control and data forwarding planes. SDN brings innovation in networking through abstraction on one hand and simplifies the network management on the other hand. Network Function Virtualization (NFV) provides the basis for placing various network functions in different network perimeters on a need basis and eliminates the need for function or service-specific hardware. SDN and NFV, complementing each other, improve the network elasticity, simplify network control and management, break the barrier of vendor specific proprietary solutions, and thus are considered highly important for future networks. Yet with these novel technologies and concepts, network security and user privacy remain a big challenge for future networks.

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

Therefore, it is crucial to highlight the security challenges that are threatening not only due to the wireless nature of mobile networks, but exist in the potential technologies that are highly important for 5G. In this paper, we highlight the security challenges that are on the forefront of 5G and need prompt security measures. We further discuss the security solutions for the threats described in this paper. The rest of the paper is organized as follows: Section II describes the key security challenges followed by security solutions for the highlighted security challenges in Section III. The paper is concluded in Section IV.

II. Key Security Challenges in 5G

5G will connect critical infrastructure that will require more security to ensure safety of not only the critical infrastructure but safety of the society as a whole. For example, a security breach in the online power supply systems can be catastrophic for all the electrical and electronic systems that the society depends upon. Similarly, we know that data is critical in decision making, but what if the critical data is corrupted while being transmitted by the 5G networks? Therefore, it is highly important to investigate and highlight the important security challenges in 5G networks and overview the potential solutions that could lead to secure 5G systems. The basic challenges in 5G highlighted by Next Generation Mobile Networks (NGMN) [2] and highly discussed in the literature are as follows:

- **Flash network traffic:** High number of end-user devices and new things (IoT).
- **Security of radio interfaces:** Radio interface encryption keys sent over insecure channels.
- **User plane integrity:** No cryptographic integrity protection for the user data plane.
- **Mandated security in the network:** Service-driven constraints on the security architecture leading to the optional use of security measures.
- **Roaming security:** User-security parameters are not updated with roaming from one operator network to another, leading to security compromises with roaming.
- **Denial of Service (DoS) attacks on the infrastructure:** Visible nature of network control elements, and unencrypted control channels.
- **Signaling storms:** Distributed control systems requiring coordination, e.g. Non-Access Stratum (NAS) layer of Third Generation Partnership Project (3GPP) protocols.
- **DoS attacks on end-user devices:** No security measures for operating systems, applications, and configuration data on user devices.

The 3GPP working group i.e. SA WG3 [3] is actively involved in determining the security and privacy requirements, and specifying the security architectures and protocols for 5G. The Open Networking Foundation (ONF) [4] is dedicated to accelerating the adoption of SDN and NFV and publishes technical specifications including specifications for security of the technologies.

The 5G design principles outlined by NGMN beyond radio efficiency are: creating a common composable core and simplified operations and management by embracing new computing and networking technologies. Therefore, we focused on the security of those technologies that will fulfill the design principles outlined by NGMN i.e. mobile clouds, SDN and NFV and the communication links used by or in between these technologies. Due to the increasing concerns for user privacy, we have also highlighted the potential privacy challenges. The security challenges are pictured in Fig. 1 and presented in Table 1. Table 1 provides an overview of different types of security threats and attacks, the targeted elements or services in a network, and the technologies that are most prone to the attacks or threats are tick-marked. These security challenges are briefly described in the following sections.

A. Security Challenges in Mobile Clouds

Since cloud computing systems comprise various resources which are shared among users, it is possible that a user spread malicious traffic to tear down the performance of the whole system, consume more resources or stealthily access resource of other users. Similarly, in multi-tenant cloud networks where tenants run their own control logic, interactions can cause conflicts in network configurations. Mobile Cloud Computing (MCC) migrates the concepts of cloud computing into the 5G eco-systems. This creates a number of security vulnerabilities that mostly arise with the architectural and infrastructural

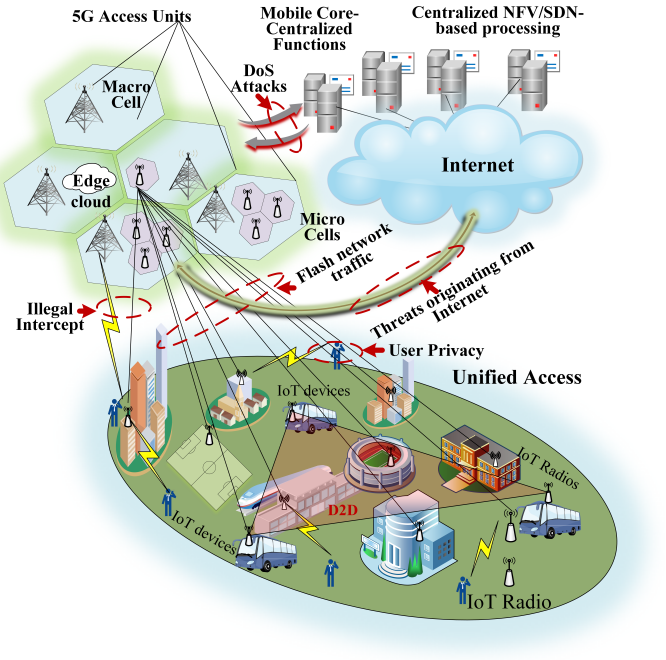

Figure 1. 5G network and the threat landscape.

modifications in 5G. Therefore, the open architecture of MCC and the versatility of mobile terminals create vulnerabilities through which adversaries could launch threats and breach privacy in mobile clouds [5].

In this work, we categorize MCC threats according to targeted cloud segments into front-end, back-end and network-based mobile security threats. The front-end of the MCC architecture is the client platform which consists of the mobile terminal on which applications and interfaces required to access the cloud facilities run. The threat landscape on this segment may range from physical threats; where the actual mobile device and other integrated hardware components are primary targets, to application-based threats; where malware, spyware, and other malignant software are used by adversaries to disrupt user applications or gather sensitive user information [6], [7]. The back-end platform consists of the cloud servers, data storage systems, virtual machines, hypervisor and protocols required to offer cloud services. On this platform, security threats are mainly targeted towards the mobile cloud servers. The scope of these threats may range from data-replication to HTTP and XML DoS (HX-DoS) attacks [8], [9].

Network-based mobile security threats are targeted towards the Radio Access Technologies (RATs) that interface mobile devices to the cloud. This may be traditional Wi-Fi, 4G Long Term Evolution (LTE) or other novel RATs that will come with 5G. Attacks in this category include Wi-Fi sniffing, DoS attacks, address impersonation, and session hijacking [6], [8]. Cloud Radio Access Network (C-RAN) is another key area of interest in analyzing the security challenges in 5G mobile clouds. C-RAN has the potential of addressing the industry's capacity growth needs for higher mobility in 5G mobile

Table I
SECURITY CHALLENGES IN 5G TECHNOLOGIES.

Security Threat	Target Point/Network Element	Effected Technology				Privacy
		SDN	NFV	Channels	Cloud	
DoS attack	Centralized control elements	✓	✓		✓	
Hijacking attacks	SDN controller, hypervisor	✓	✓			
Signaling storms	5G core network elements			✓	✓	
Resource (slice) theft	Hypervisor, shared cloud resources		✓		✓	
Configuration attacks	SDN (virtual) switches, routers	✓	✓			
Saturation attacks	SDN controller and switches	✓				
Penetration attacks	Virtual resources, clouds		✓		✓	
User identity theft	User information data bases				✓	✓
TCP level attacks	SDN controller-switch communication	✓		✓		
Man-in-the-middle attack	SDN controller-communication	✓		✓		✓
Reset and IP spoofing	Control channels			✓		
Scanning attacks	Open air interfaces			✓		✓
Security keys exposure	Unencrypted channels			✓		
Semantic information attacks	Subscriber location			✓		✓
Timing attacks	Subscriber location				✓	✓
Boundary attacks	Subscriber location					✓
IMSI catching attacks	Subscriber identity			✓		✓

communication systems [10]. C-RAN is however prone to inherent security challenges associated with virtual systems and cloud computing technology, for instance, the centralized architecture of C-RAN suffers the threat of single point of failure. Other threats like intrusion attacks where adversaries break into the virtual environment to monitor, modify, or run software routines on the platform while undetected also constitutes substantial threats to the system [10].

B. Security Challenges in SDN and NFV

SDN centralizes the network control platforms and enables programmability in communication networks. These two disruptive features, however, create opportunities for cracking and hacking the network. For example, the centralized control will be a favorable choice for DoS attacks, and exposing the critical Application Programming Interfaces (APIs) to unintended software can render the whole network down [11]. The SDN controller modifies flow rules in the data path, hence the controller traffic can be easily identified. This makes the controller a visible entity in the network rendering it a favorite choice for DoS attacks. The centralization of network control can also make the controller a bottleneck for the whole network due to saturation attacks as presented in [12], [13]. Since most network functions can be implemented as SDN applications, malicious applications if granted access can spread havoc across a network [14].

Even though NFV is highly important for future communication networks, it has basic security challenges such as confidentiality, integrity, authenticity and non-repudiation [15], [16]. From the point of view of its use in mobile networks, it is presented in [17], [18], that the current NFV platforms do not provide proper security and isolation to virtualized telecommunication services. One of the main challenges persistent to the use of NFV in mobile networks is the dynamic nature of Virtual Network Functions (VNFs) that leads to configuration errors and thus security lapses [19]. Further challenges are highlighted in Table 1, but the main challenge that need immediate attention is that the whole network can be compromised if the hypervisor is hijacked [15].

C. Security Challenges in Communication Channels

5G will have complex ecosystem involving drones and air traffic control, cloud driven virtual reality, connected vehicles, smart factories, cloud driven robots, transportation and e-health. Thus the applications need secure communication systems that support more frequent authentication and exchange of more sensitive data. Also, many new players such as public service providers, Mobile Network Operators (MNOs), and cloud operators will get involved with these services. In such an eco-system several layers of encapsulated authentications are required at both network access and service levels, and frequent authentication is required between actors.

Before 5G networks, mobile networks had dedicated communication channels based on GTP and IPsec tunnels. The communication interfaces, such as X2, S1, S6, S7, which are used only in mobile networks, require significant level of expertise to attack these interfaces. However, SDN-based 5G networks will not have such dedicated interfaces but rather common SDN interfaces. The openness of these interfaces will increase the possible set of attackers. The communication in SDN based 5G mobile networks can be categorized in to three communication channels i.e. data channel, control channel and inter-controller channel [20]. In current SDN system, these channels are protected by using TLS (Transport Layer Security)/ SSL (Secure Sockets Layer) sessions [21]. However, TLS/SSL sessions are highly vulnerable to IP layer attacks [22], SDN Scanner attacks [23] and lack strong authentication mechanisms [24].

D. Privacy Challenges in 5G

From the user's perspective, the major privacy concerns could arise from data, location and identity [25]. Most smart phone applications require details of subscriber's personal information before the installation. The application developers

or companies rarely mention that how the data is stored and for what purposes it is going to be used. Threats such as semantic information attacks, timing attacks, and boundary attacks mainly target the location privacy of subscribers [26]. At the physical layer level, location privacy can be leaked by access point selection algorithms in 5G mobile networks [27]. International Mobile Subscriber Identity (IMSI) catching attacks can be used to reveal the identity of a subscriber by catching the IMSI of the subscriber's User Equipment (UE). Such attacks can also be caused by setting up a fake base station which is considered as preferred base station by the UE and thus subscribers will respond with their IMSI.

Moreover, 5G networks have different actors such as Virtual MNOs (VMNOs), Communication Service Providers (CSPs) and network infrastructure providers. All of these actors have different priorities for security and privacy. The synchronization of mismatching privacy policies among these actors will be a challenge in 5G network [28]. In the previous generations, mobile operators had direct access and control of all the system components. However, 5G mobile operators are losing the full control of the systems as they will rely on new actors such CSPs. Thus, 5G operators will lose the full governance of security and privacy [29]. User and data privacy are seriously challenged in shared environments where the same infrastructure is shared among various actors, for instance VMNOs and other competitors. Moreover, there are no physical boundaries of 5G network as they use cloud based data storage and NFV features. Hence, the 5G operators have no direct control of the data storing place in cloud environments. As different countries have different level of data privacy mechanisms depending upon their preferred context, the privacy is challenged if the user data is stored in a cloud in a different country [30].

III. Potential Security Solutions

In this section, we highlight security solutions for the security challenges outlined in the previous section. The challenges of flash network traffic can be solved by either adding new resources or increasing the utility of existing systems with novel technologies. We believe that new technologies such as SDN and NFV can solve these challenges more cost effectively. SDN has the capability to enable run-time resource, e.g. bandwidth, assignment to particular parts of the network as the need arises [31]. In SDN, the controller can gather network stats through the south-bound API from network equipment to see if the traffic levels increase. Using NFV, services from the core network cloud can be transferred towards the edge to meet the user requirements. Similarly, virtual slices of the network can be dedicated only to areas with high density of UEs to cope with flash network traffic.

The security of the radio interface keys is still a challenge, that needs secure exchange of keys encrypted like the proposed Host Identity Protocol (HIP) based scheme in [32]. Similarly, the user plane integrity can be achieved by end-to-end encryption technologies suggested in [33], [24]. Roaming security and network-wide mandated security policies can be achieved using centralized systems that have global visibility of the users' activities and network traffic behavior e.g. SDN. The signaling storms will be more challenging due to the excessive connectivity of UEs, small base stations, and high user mobility. C-RAN and edge computing are the potential problem solvers for these challenges, but the design of these technologies must consider the increase in signaling traffic as an important aspect of the future networks as described by NGMN. Solutions for DoS attacks or saturation attacks on network control elements are presented in the following sections.

Due to space limitation and for brevity the security solutions for the threats in technologies described in the previous section are listed in Table II and the methodologies are described below.

A. Security Solutions for Mobile Clouds

Most proposed security measures in MCC revolve around the strategic use of virtualization technologies, the redesign of encryption methods and dynamic allocation of data processing points. Hence, virtualization comes as a natural option for securing cloud services since each end-node connects to a specific virtual instance in the cloud via a Virtual Machine (VM). This provides security through the isolation of each user's virtual connection from other users. Similarly, service-based restriction will also enable secure use of cloud computing technologies. For example, the authors in [51], proposed "Secure Sharing and Searching for Real-Time Video Data in Mobile Cloud", an infrastructure that leverages on cloud platform and 5G technology to secure cloud services and enable mobile users share real-time videos on 5G enabled clouds. Unlike existing solutions where users with shared links are able to access such online video feeds, this architecture restricts access to only authorized viewers. For specific security threats such as HX-DoS, specific solutions such as learning-based systems e.g. [9] are more useful than generic approaches. For example, the learning-based system [9] take a certain number of samples of packets and analyze them for various known attributes to detect and mitigate threats.

To secure the mobile terminals, the use of anti-malwares could well improve the overall resistance to malware attacks. Anti-malware solutions are installed on the mobile terminal or hosted and served directly from the cloud [7]. In MCC data and storage, the security framework will consist of energy efficient mechanisms for the integrity verification of data and storage services in conjunction with a public provable data possession scheme and some lightweight compromise resilient storage outsourcing. For application security, some proposed frameworks are based on securing elastic applications on mobile devices for cloud computing, lightweight dynamic credential generation mechanism for user identity protection, in-device spatial cloaking mechanism for privacy protection as well as MobiCloud which is a secure cloud framework for mobile computing and communication [50].

For Radio Access Network (RAN) security, a cloud based framework i.e. C-RAN is proposed for optimizing and provid-

Table II
SECURITY TECHNOLOGIES AND SOLUTIONS

Security Technology	Primary Focus	Target Technology				Privacy
		SDN	NFV	Channels	Cloud	
DoS, DDoS detection [34], [35]	Security of centralized control points	✓	✓			
Configuration verification [36], [37]	Flow rules verification in SDN switches	✓				
Access control [38], [39] [40]	Control access to SDN and core network elements	✓	✓		✓	
Traffic isolation [41]	Ensures isolation for VNFs and virtual slices		✓			
Link security [42], [24], [43]	Provide security to control channels	✓		✓		
Identity verification [44], [45], [46]	User identity verification for roaming and clouds services					✓
Identity security [47], [48]	Ensure identity security of users					✓
Location security [26], [27]	Ensure security of user location					✓
IMSI security [49]	Secure the subscriber identity through encryption					✓
Mobile terminal security [7]	Anti-maleware technologies to secure mobile terminals					✓
Integrity verification [50]	Security of data and storage systems in clouds				✓	
HX-DoS metigation [9]	Security for cloud web services				✓	
Service access Control [51]	Service-based access control security for clouds				✓	

ing safer RANs for 5G clouds. In [52], authors described how C-RAN can dynamically enhance the end-to-end performance of MCC services in next generations wireless networks. However, for C-RAN to meet this demand, it needs to provide a high level of reliability comparable to traditional optical networks like Synchronous Digital Hierarchy (SDH), and one way to achieve this is through the massive adoption of mechanisms like fiber ring network protection, which presently are mostly found in industrial and energy fields [53].

B. Security Solutions for SDN and NFV

Due to the logically centralized control plane with global network view and programmability, SDN facilitates quick threat identification through a cycle of harvesting intelligence from the network resources, states and flows. Therefore, the SDN architecture supports highly reactive and proactive security monitoring, traffic analysis and response systems to facilitate network forensics, the alteration of security policies and security service insertion [54]. Consistent network security policies can be deployed across the network due to global network visibility, whereas security systems such as firewalls and Intrusion Detection Systems (IDS) can be used for specific traffic by updating the flow tables of SDN switches.

The security of VNFs through a security orchestrator in correspondence with the ETSI NFV architecture is presented in [55]. The proposed architecture provides security not only to the virtual functions in a multi-tenant environment, but also to the physical entities of a telecommunication network. Using trusted computing, remote verification and integrity checking of virtual systems and hypervisors is proposed in [56] to provide hardware-based protection to private information and detect corrupt software in virtualized environments.

C. Security Solutions for Communication Channels

5G needs proper communication channels security not only to prevent the identified security threats but also to maintain the additional advantages of SDN such as centralized policy management, programmability and global network state visibility. IPsec is the most commonly used security protocol to secure the communication channels in present day telecommunication networks such as 4G-LTE[57]. It is possible to use IPsec tunneling to secure 5G communication channels with slight modifications as presented in [22] and [24]. Moreover, the security for LTE communications is provided by integrating various security algorithms, such as authentication, integrity and encryption. However, the main challenges in such existing security schemes are high resource consumption, high overhead and lack of coordination. Therefore, these solutions are not viable for critical infrastructure communication in 5G. Thus a higher level of security for critical communication is achievable by utilizing new security mechanisms such as physical layer security adopting Radio-Frequency (RF) fingerprinting [58], using asymmetric security schemes [59] and dynamically changing security parameters according to the situation [21]. Similarly, end-to-end user communication can be secured by using cryptographic protocols like HIP as presented in [60].

D. Security Solutions for Privacy in 5G

5G must embody privacy-by-design approaches where privacy is considered from the beginning in the system and many necessary features must be available built-in. A hybrid cloud based approach is required where mobile operators are able to store and process high sensitive data locally and less sensitive data in public clouds. In this way, operators will have more access and control over data and can decide where to share it. Similarly, service oriented privacy in 5G will lead to more viable solution for preserving privacy [61].

5G will require better mechanisms for accountability, data minimization, transparency, openness and access control [25]. Hence during the standardization of 5G, strong privacy regulations and legislation should be taken into account [29]. The regulatory approach can be classified into three types [62]. First is the government level regulation, where governments mainly make country-specific privacy regulations and through multi-national organizations such as the United Nations (UN) and European Union (EU). Second is the industry level, where various industries and groups such as 3GPP, ETSI, and ONF collaboratively draft the best principles and practices to protect

privacy. Third is the consumer level regulations where desired privacy is ensured by considering consumers requirements.

For location privacy, anonymity based techniques must be applied where the subscriber real identity could be hidden and replaced with pseudonyms [63]. Encryption based practices are also useful in this case, for instance message can be encrypted before sending to Location-Based Services (LBS) provider [64]. Techniques such as obfuscation are also useful, where the quality of location information is reduced in order to protect location privacy [65]. Moreover, location cloaking based algorithms are quite useful to handle some of major location privacy attacks such as timing and boundary attacks [26].

IV. Conclusion

5G will use mobile clouds, SDN and NFV to meet the challenges of massive connectivity, flexibility, and costs. With all the benefits, these technologies also have inherent security challenges. Therefore, in this paper we have highlighted the main security challenges that can become more threatening in 5G, unless properly addressed. We have also presented the security mechanisms and solutions for those challenges. However, due to the limited standalone and integrated deployment of these technologies in 5G, the security threat vectors cannot be fully realized at this time. Similarly, the communication security and privacy challenges will be more visible when more user devices e.g. IoT are connected and new diverse sets of services are offered in 5G. To sum it up, it is highly likely that new types of security threats and challenges will arise along with the deployment of novel 5G technologies and services. However, considering these challenges right from the initial design phases to the deployment will minimize the likelihood of potential security and privacy lapses.

Acknowledgment

This work was supported by TEKES Finland and Academy of Finland under projects: The Naked Approach, Towards Digital Paradise and SecureConnect. Andrei Gurtov was supported by the Center for Industrial Information Technology (CENIIT).

References

[1] M. Agiwal, A. Roy, and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.

[2] N. Alliance, "NGMN 5G white paper," *Next Generation Mobile Networks, White paper*, 2015.

[3] 3GPP. (2017, May) SA3-Security. The Third Generation Partnership Project (3GPP). [Online]. Available: http://www.3gpp.org/Specifications-groups/sa-plenary/54-sa3-security

[4] ONF. (2013) SDN Security Considerations in the Data Center. Open Networking Foundation. [Online]. Available: https://www.opennetworking.org/sdn-resources/sdn-library

[5] P. Kulkarni, R. Khanai, and G. Bindagi, "Security frameworks for mobile cloud computing: A survey," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, March 2016, pp. 2507–2511.

[6] S. S. Vikas, K. Pawan, A. K. Gurudatt, and G. Shyam, "Mobile cloud computing: Security threats," in *2014 International Conference on Electronics and Communication Systems (ICECS)*, Feb 2014, pp. 1–4.

[7] M. L. Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 446–471, First 2013.

[8] H. Suo, Z. Liu, J. Wan, and K. Zhou, "Security and privacy in mobile cloud computing," in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, July 2013, pp. 655–659.

[9] A. Chonka and J. Abawajy, "Detecting and Mitigating HX-DoS Attacks against Cloud Web Services," in *2012 15th International Conference on Network-Based Information Systems*, Sept 2012, pp. 429–434.

[10] V. Sucasas, G. Mantas, and J. Rodriguez, "Security Challenges for Cloud Radio Access Networks," *Backhauling/Fronthauling for Future Wireless Systems*, pp. 195–211, 2016.

[11] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in Software Defined Networks: A Survey," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2317–2346, Fourthquarter 2015.

[12] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-defined Networks," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 413–424. [Online]. Available: http://doi.acm.org/10.1145/2508859.2516684

[13] P. Fonseca, R. Bennesby, E. Mota, and A. Passito, "A replication component for resilient OpenFlow-based networking," in *2012 IEEE Network Operations and Management Symposium*, April 2012, pp. 933–939.

[14] D. Kreutz, F. M. Ramos, and P. Verissimo, "Towards Secure and Dependable Software-defined Networks," in *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, ser. HotSDN '13. New York, NY, USA: ACM, 2013, pp. 55–60. [Online]. Available: http://doi.acm.org/10.1145/2491185.2491199

[15] A. van Cleeff, W. Pieters, and R. J. Wieringa, "Security Implications of Virtualization: A Literature Study," in *2009 International Conference on Computational Science and Engineering*, vol. 3, Aug 2009, pp. 353–358.

[16] S. J. Vaughan-Nichols, "Virtualization sparks security concerns," *Computer*, vol. 41, no. 8, pp. 13–15, Aug 2008.

[17] M. Monshizadeh, V. Khatri, and A. Gurtov, "NFV security considerations for cloud-based mobile virtual network operators," in *2016 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Sept 2016, pp. 1–5.

[18] H. Hawilo, A. Shami, M. Mirahmadi, and R. Asal, "NFV: state of the art, challenges, and implementation in next generation mobile networks (vEPC)," *IEEE Network*, vol. 28, no. 6, pp. 18–26, Nov 2014.

[19] W. Yang and C. Fung, "A survey on security in network functions virtualization," in *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, June 2016, pp. 15–19.

[20] M. Liyanage, A. Gurtov, and M. Ylianttila, *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*. John Wiley & Sons, 2015.

[21] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security," *IEEE Security Privacy*, vol. 14, no. 4, pp. 34–44, July 2016.

[22] M. Liyanage, M. Ylianttila, and A. Gurtov, "Securing the control channel of software-defined mobile networks," in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, June 2014, pp. 1–6.

[23] S. Shin and G. Gu, "Attacking software-defined networks: A first feasibility study," in *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, ser. HotSDN '13. New York, NY, USA: ACM, 2013, pp. 165–166. [Online]. Available: http://doi.acm.org/10.1145/2491185.2491220

[24] M. Liyanage, A. Braeken, A. D. Jurcut, M. Ylianttila, and A. Gurtov, "Secure communication channel architecture for Software Defined Mobile Networks," *Computer Networks*, vol. 114, pp. 32 – 50, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128617300075

[25] T. Kumar and M. Liyanage and A. Braeken and I. Ahmad and M. Ylianttila, "From Gadget to Gadget-Free Hyperconnected World: Conceptual Analysis of User Privacy Challenges," in *2017 European Conference on Networks and Communications (EuCNC)*, June 2017, pp. 1–6.

[26] R. Yu, Z. Bai, L. Yang, P. Wang, O. A. Move, and Y. Liu, "A Location Cloaking Algorithm Based on Combinatorial Optimization for Location-Based Services in 5G Networks," *IEEE Access*, vol. 4, pp. 6515–6527, 2016.

[27] S. Farhang, Y. Hayel, and Q. Zhu, "PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks," in *2015 IEEE Conference on Communications and Network Security (CNS)*, Sept 2015, pp. 263–271.

[28] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Security and Communication Networks*, vol. 9, no. 16, pp. 3059–3069, 2016, sCN-14-0760.R1. [Online]. Available: http://dx.doi.org/10.1002/sec.1243

[29] L. T. Sorensen, S. Khajuria, and K. E. Skouby, "5G Visions of User Privacy," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, May 2015, pp. 1–4.

[30] F. Kemmer, C. Reich, M. Knahl, and N. Clarke, "Software defined privacy," in *2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW)*, April 2016, pp. 25–29.

[31] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Towards software defined cognitive networking," in *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)*, July 2015, pp. 1–5.

[32] M. Liyanage and A. Gurtov, "Secured VPN Models for LTE Backhaul Networks," in *2012 IEEE Vehicular Technology Conference (VTC Fall)*, Sept 2012, pp. 1–5.

[33] M. Liyanage, I. Ahmad, M. Ylianttila, A. Gurtov, A. B. Abro, and E. M. de Oca, "Leveraging LTE security with SDN and NFV," in *2015 IEEE 10th International Conference on Industrial and Information Systems (ICIIS)*, Dec 2015, pp. 220–225.

[34] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, Oct 2010, pp. 408–415.

[35] E. Maccherani, M. Femminella, J. W. Lee, R. Francescangeli, J. Janak, G. Reali, and H. Schulzrinne, "Extending the NetServ autonomic management capabilities using OpenFlow," in *2012 IEEE Network Operations and Management Symposium*, April 2012, pp. 582–585.

[36] E. Al-Shaer and S. Al-Haj, "FlowChecker: Configuration Analysis and Verification of Federated Openflow Infrastructures," in *Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration*, ser. SafeConfig '10. ACM, 2010, pp. 37–44.

[37] A. Khurshid, W. Zhou, M. Caesar, and P. B. Godfrey, "Veriflow: Verifying Network-wide Invariants in Real Time," *SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, pp. 467–472, Sep. 2012.

[38] S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu, and M. Tyson, "FRESCO: Modular composable security services for software-defined networks," in *Proceedings of Network and Distributed Security Symposium*, 2013.

[39] A. K. Nayak, A. Reimers, N. Feamster, and R. Clark, "Resonance: dynamic access control for enterprise networks," in *Proceedings of the 1st ACM workshop on Research on enterprise networking*. ACM, 2009, pp. 11–18.

[40] S. Namal, I. Ahmad, A. Gurtov, and M. Ylianttila, "SDN Based Inter-Technology Load Balancing Leveraged by Flow Admission Control," in *2013 IEEE SDN for Future Networks and Services (SDN4FNS)*, Nov 2013, pp. 1–5.

[41] C. Schlesinger, A. Story, S. Gutz, N. Foster, and D. Walker, "Splendid isolation: Language-based security for software-defined networks," 2012.

[42] T. Dierks, "The transport layer security (TLS) protocol version 1.2," 2008. [Online]. Available: http://tools.ietf.org/html/rfc5246

[43] J.-H. Lam, S.-G. Lee, H.-J. Lee, and Y. E. Oktian, "Securing distributed SDN with IBC," in *2015 Seventh International Conference on Ubiquitous and Future Networks*, July 2015, pp. 921–925.

[44] M. A. S. Santos, B. T. de Oliveira, C. B. Margi, B. A. A. Nunes, T. Turletti, and K. Obraczka, "Software-defined networking based capacity sharing in hybrid networks," pp. 1–6, Oct 2013.

[45] C. YuHunag, T. MinChi, C. YaoTing, C. YuChieh, and C. YanRen, "A novel design for future on-demand service and security," in *Communication Technology (ICCT), 2010 12th IEEE International Conference on*. IEEE, 2010, pp. 385–388.

[46] S. Namal, I. Ahmad, A. Gurtov, and M. Ylianttila, "Enabling Secure Mobility with OpenFlow," in *SDN for Future Networks and Services (SDN4FNS), 2013 IEEE*. IEEE, 2013, pp. 1–5.

[47] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "OpenFlow random host mutation: transparent moving target defense using software defined networking," in *Proceedings of the first workshop on Hot topics in software defined networks*. ACM, 2012, pp. 127–132.

[48] A. Gember, C. Dragga, and A. Akella, "ECOS: Leveraging Software-defined Networks to Support Mobile Application Offloading," in *Proceedings of the Eighth ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, ser. ANCS '12. ACM, 2012, pp. 199–210.

[49] K. Norrman, M. Näslund, and E. Dubrova, "Protecting IMSI and User Privacy in 5G Networks," in *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, ser. MobiMedia '16. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016, pp. 159–166. [Online]. Available: http://dl.acm.org/citation.cfm?id=3021385.3021415

[50] A. N. Khan, M. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," *Future Generation Computer Systems*, vol. 29, no. 5, pp. 1278 – 1299, 2013, special section: Hybrid Cloud Computing. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X12001598

[51] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, "Secure sharing and searching for real-time video data in mobile cloud," *IEEE Network*, vol. 29, no. 2, pp. 46–50, March 2015.

[52] Y. Cai, F. R. Yu, and S. Bu, "Dynamic Operations of Cloud Radio Access Networks (C-RAN) for Mobile Cloud Computing Systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1536–1548, March 2016.

[53] A. Checko, H. L. Christiansen, Y. Yan, L. Scolari, G. Kardaras, M. S. Berger, and L. Dittmann, "Cloud RAN for Mobile Networks x2014;A Technology Overview," *IEEE Communications Surveys Tutorials*, vol. 17, no. 1, pp. 405–426, Firstquarter 2015.

[54] S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 36–43, July 2013.

[55] B. Jaeger, "Security Orchestrator: Introducing a Security Orchestrator in the Context of the ETSI NFV Reference Architecture," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug 2015, pp. 1255–1260.

[56] H. Lauer and N. Kuntze, "Hypervisor-based attestation of virtual environments," in *2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, July 2016, pp. 333–340.

[57] A. N. Bikos and N. Sklavos, "LTE/SAE Security Issues on 4G Wireless Networks," *IEEE Security Privacy*, vol. 11, no. 2, pp. 55–62, March 2013.

[58] G. Baldini, R. Giuliani, and E. Cano Pons, "An Analysis of the Privacy Threat in Vehicular Ad Hoc Networks due to Radio Frequency Fingerprinting," *Mobile Information Systems*, vol. 2017, 2017.

[59] C. Zhao, L. Huang, Y. Zhao, and X. Du, "Secure Machine-Type Communications toward LTE Heterogeneous Networks," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 82–87, February 2017.

[60] I. Ahmad and M. Liyanage and M. Ylianttila and Andrei Gurtov, "Analysis of Deployment Challenges of Host Identity Protocol," in *2017 European Conference on Networks and Communications (EuCNC)*, June 2017, pp. 1–6.

[61] Huawei, "5G Security: Forward Thinking," Huawei, Tech. Rep., 2016. [Online]. Available: http://www.huawei.com/minisite/5g/img/5G_-Security_Whitepaper_en.pdf

[62] C. G. Panayiotou, G. Ellinas, E. Kyriakides, and M. M. Polycarpou, *Critical Information Infrastructures Security*. Springer, 2016.

[63] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: A game-theoretic analysis," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 324–337. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653702

[64] P. Xiao, X. Zhen, and M. Xiaofeng, "Survey of location privacy-preserving," *Journal of Frontiers of Computer Science and Technology*, vol. 1, no. 3, pp. 268–281, 2007.

[65] T. Xu and Y. Cai, "Location Anonymity in Continuous Location-based Services," in *Proceedings of the 15th Annual ACM International Symposium on Advances in Geographic Information Systems*, ser. GIS '07. New York, NY, USA: ACM, 2007, pp. 39:1–39:8. [Online]. Available: http://doi.acm.org/10.1145/1341012.1341062