International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

July- August-2020 Volume 7, Issue-4

Email: editor@ijermt.org www.ijermt.org

A STUDY OF 5G NETWORK SECURITY AND PRIVACY CHALLENGES IN MOBILE CLOUD NETWORK

Dr. Vikas Jain,

Assistant Professor, SCRIET-DCA,

Ch. Charan Singh University, Meerut, Uttar Pradesh, India

Abstract:

As 5G networks become more widespread, they will bring about new levels of speed, connectedness, and innovation across a wide range of businesses and in everyday life. Because of this technical breakthrough, new paradigms in networking and security have been introduced, which requires a reevaluation of the methodologies that have been traditionally used. Advanced technologies including as network slicing, edge computing, and enormous IoT (Internet of Things) are utilized by 5G networks. These technologies not only dramatically improve the capabilities of the network, but they also present new issues in terms of network security. This abstract investigates the distinctive qualities of 5G networks, focusing on their design, the technologies that are essential to their operation, and the security problems that are linked with them. This article addresses the effects that ultra-low latency, high bandwidth, and greater device density have on the security measures that are used for networks. Additionally, it investigates new security solutions and standards that are designed to protect 5G networks from the ever-evolving cyber threats that are now operating. In the end, developing an awareness of these difficulties and finding solutions to them is essential in order to fully realize the potential of 5G while also maintaining the security of networks that are strong and resilient.

Keywords: *Networking, 5g network, security, Mobile Cloud Network*

Introduction:

It is a momentous milestone in the field of telecommunications that the implementation of 5G networks will take place, since it promises to deliver unprecedented levels of speed, capacity, and connection. 5G is a revolutionary technology that features revolutionary technologies that enable varied applications. These applications range from ultra-reliable low-latency communications (URLLC) to massive machine-type communications (mMTC). These technologies are built upon the foundations of their predecessors. These innovations not only reimagine user experiences but also change industries such as healthcare, transportation, and manufacturing by enhancing the capabilities of the Internet of Things (IoT) and processing data in real time. Nevertheless, although these opportunities present themselves, they also present major obstacles, notably in the field of network security. A complex and dynamic network environment is created as a result of the architectural advancements of 5G, which include network slicing, edge computing, and virtualization. This environment necessitates the implementation of very effective security measures. The exponential development in data transmission and the proliferation of connected devices both magnify vulnerabilities, making it necessary to implement preventative techniques in order to reduce risks and protect critical information. Within the context of 5G networks, this introduction lays the groundwork for further investigation into the interaction of networking and security. The purpose of this paper is to give insights into the essential relevance of protecting 5G networks and the tactics that are necessary to create resilience in the face of current cyber attacks. This will be accomplished by evaluating the core architectural components, technical advancements, and increasing security concerns. It is vital to dive further into the architecture of 5G networks and the distinctive characteristics they possess in order to thoroughly address the security problems that are brought by these networks. The 5G architecture, in contrast to the architectures of previous generations, is developed using a service-based approach. It makes use of software-defined networking (SDN) and network function virtualization (NFV) to provide flexibility and scalability. Because of this architectural change, new attack surfaces and vulnerabilities have been introduced, which calls for a paradigm shift in the security techniques that are being implemented. One of the characteristics that distinguishes 5G from other generations is network slicing, which enables operators to construct virtualized, end-to-end networks that are customized to meet the requirements of certain applications or users. Despite the fact that network slicing improves resource efficiency and allows for greater service customization, it also raises security risks that are associated with the isolation, orchestration, and administration of various slices within a common infrastructure. Furthermore, the convergence of information technology and telecommunications technologies in 5G networks, which is made possible by edge computing and cloud-native architectures, brings computing resources closer to the end-users. Even though this reduces latency and makes the user experience better, it also creates new security concerns that are associated with maintaining data integrity, protecting users' privacy, and managing dispersed infrastructure. Furthermore, the large deployment of Internet of Things devices in 5G networks, which supports a wide range of applications ranging from smart cities to industrial automation, magnifies security threats owing to the heterogeneity and sheer volume of linked devices. The protection of these devices and the data that they produce is absolutely necessary in order to forestall cyberattacks and guarantee the dependability of life-sustaining services. Stakeholders in the 5G ecosystem, such as network operators, service providers, and regulatory authorities, are actively designing and implementing security frameworks, standards, and protocols in order to address the issues that have been presented. The purpose of these initiatives is to build complete security mechanisms that include authentication, encryption, access control, threat detection, and incident response that are suited to the specific characteristics of 5G networks.

It is of the utmost importance to acknowledge the multidimensional nature of the security problems that follow the advancement of this technology as the deployment of 5G networks continues to increase around the globe. Not only does the adoption of 5G have ramifications for the technical elements of architecture and connectivity, but it also has repercussions for the socio-economic aspects. Privacy issues, legal frameworks, and the potential influence on digital economies and global competitiveness are some of the ramifications that are associated with this. The huge amount of personal data that is created by connected devices is the source of privacy issues in 5G networks. Additionally, there is the possibility that this data may be accessed or misused by unwanted parties. The establishment of regulatory frameworks is very necessary in order to guarantee compliance with data protection laws and regulations, as well as to encourage openness and responsibility among network operators and service providers. Furthermore, the strategic implications of 5G in national security and geopolitical dynamics highlight the significance of protecting key infrastructure and communications networks from threats that are sponsored by states and those that are carried out by hostile actors. In a number of nations, the resilience of 5G networks against cyberattacks, espionage, and disruption is becoming an extremely important national concern. Research and development activities are now being directed toward the advancement of security technologies like as artificial intelligence-driven threat detection, blockchain-based authentication, and secure-by-design principles in network architecture. These efforts are being undertaken from a technological perspective. The purpose of these technologies is to improve the reliability and resiliency of 5G networks while simultaneously reducing the risks and vulnerabilities that they provide.

KEY SECURITY CHALLENGES IN 5G

As a result of the fact that 5G will connect important infrastructure, security measures will need to be increased in order to guarantee not just the safety of the critical infrastructure but also the safety of society as a whole. A security breach in the online power supply systems, for instance, has the potential to lead to disastrous consequences for all of the electrical and electronic systems that are essential to the functioning of civilization. Similarly, we are aware that data plays a significant role in the process of decision making; but, what would happen if essential data were to get damaged while it was being transferred via 5G networks? In light of this, it is of the utmost importance to research and bring attention to the significant security concerns that are associated with 5G networks, as well as to provide an overview of the various solutions that might result in safe 5G systems. The fundamental difficulties associated with 5G, which have been brought to light by Next Generation Mobile Networks (NGMN) and have been extensively explored in the literature, are as follows:

Flash network traffic: A large number of new products and gadgets for end users (Internet of products).

Security of radio interfaces: Encryption keys for radio interfaces conveyed across channels that are not secure.

User plane integrity: The user data plane does not have any protection against cryptographic integrity.

Mandated security in the network: There are limits on the security architecture that are dictated by the service, which result in the adoption of security measures being optional.

Roaming security: When traveling from one operator network to another, user-security settings are not updated, which results in security breaches resulting from roaming.

Denial of Service (DoS) attacks on the infrastructure: The nature of network control elements that are visible, as well as control channels that are not encrypted.

Signaling storms: Control systems that are distributed and require coordination, such as the Non-Access Stratum (NAS) layer of protocols developed by the Third Generation Partnership Project (3GPP).

DoS attacks on end-user devices: Neither the operating systems nor the apps nor the configuration data on user devices are protected by any security measures.

By actively participating in the process of identifying the security and privacy requirements, as well as describing the security architectures and protocols for 5G, the 3GPP working group known as SA WG3 makes significant contributions. With the goal of advancing the adoption of software-defined networking (SDN) and network function virtualization (NFV), the Open Networking Foundation (ONF) releases technical specifications, which include requirements for the security of the technologies. In addition to radio efficiency, the concepts of 5G architecture that have been defined by NGMN include the incorporation of a common composable core, as well as the simplification of operations and administration through the use of new computer and networking technologies. Consequently, we concentrated on the security of those technologies that would match the design principles described by NGMN, such as mobile clouds, software-defined networking (SDN), and network function virtualization (NFV), as well as the communication links that are utilized by or in between these technologies. We have also brought attention to the possible privacy difficulties that may arise as a result of the growing concerns around the privacy of users. Figure 1 depicts the issues that are associated with security, and Table 1 details these challenges. An overview of the many forms of security threats and assaults is presented in Table 1. The aspects or services in a network that are the focus of the attacks or threats are highlighted, and the technologies that are most susceptible to the attacks or threats are highlighted as well. A concise explanation of these security problems may be found in the sections that follow above.

Security Challenges in Mobile Clouds

It is possible for a user to distribute harmful traffic in order to bring the performance of the entire system down, use additional resources, or secretly access the resources of other users. This is because cloud computing platforms consist of a variety of resources that are shared among users. Interactions may also lead to conflicts in network setups in multi-tenant cloud networks, which are characterized by tenants operating their own control logic from their own devices. The notions of cloud computing are migrated into the ecosystems of 5G networks through the use of Mobile Cloud Computing (MCC). A variety of security flaws are introduced as a result of this, the most of them are associated with the architectural and infrastructure aspects.

alterations made to the 5G network. As a result, the open architecture of mobile cloud computing (MCC) and the adaptability of mobile terminals both provide weaknesses that attackers might use to launch attacks and violate privacy in mobile clouds. We classify mobile cloud computing (MCC) risks into front-end, back-end, and network-based mobile security threats in this study. These classifications are based on the targeted cloud segments. It is the client platform that makes up the front-end of the MCC architecture. This platform is comprised of the mobile terminal, which is where the applications and interfaces that are necessary to access the cloud facilities are executed. It is possible that the threat landscape on this segment may include both physical threats, in which the actual mobile device and other integrated hardware components are the primary targets, and application-based threats, in which malware, spyware, and other forms of malicious software are utilized by adversaries in order to disrupt user applications or gather sensitive user information. Cloud servers, data storage systems, virtual machines, hypervisors, and protocols are all components that make up the back-end platform. These components are necessary in order to provide cloud services. When it comes to this platform, the mobile cloud servers are the primary targets of security concerns. It is possible that the scope of these threats includes data replication as well as HTTP and XML denial of service assaults (HX-DoS). Radio Access Technologies (RATs), which are responsible for connecting mobile devices to the cloud, are the focus of network-based mobile security concerns.

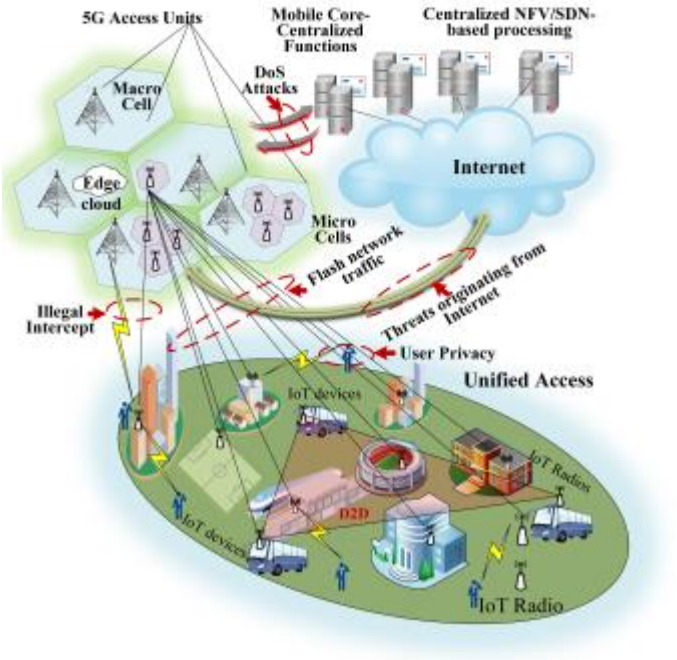

Figure 1. 5G network and the panorama of potential dangers

With 5G, this might refer to conventional Wi-Fi, 4G Long Term Evolution (LTE), or any number of other revolutionary radio access technologies (RATs). Wi-Fi snooping, denial of service attacks, address impersonation, and session hijacking are all examples of attacks that fall under this category. In the process of examining the security problems that are present in 5G mobile clouds, Cloud Radio Access Network (C-RAN) continues to be an important topic of focus. It is possible that C-RAN will be able to meet the capacity expansion requirements of the industry in order to achieve increased mobility in 5G mobile.

Table I : 5G Technologies Provide A Number Of Security Challenges

Security Threat	Target Point/Network Element	Effected Technology				Privacy
		SDN	NFV	Channels	Cloud	
DoS attack	Centralized control elements	C	C		C	
Hijacking attacks	SDN controller, hypervisor	C	C			
Signaling storms	5G core network elements			C	C	
Resource (slice) theft	Hypervisor, shared cloud resources		C		C	
Configuration attacks	SDN (virtual) switches, routers	C	C			
Saturation attacks	SDN controller and switches	C				

Penetration attacks	Virtual resources, clouds		C		C	
User identity theft	User information data bases				C	C
TCP level attacks	SDN controller-switch communication	C		C		
Man-in-the-middle attack	SDN controller-communication	C		C		C
Reset and IP spoofing	Control channels			C		
Scanning attacks	Open air interfaces			C		C
Security keys exposure	Unencrypted channels			C		
Semantic information attacks	Subscriber location			C		C
Timing attacks	Subscriber location				C	C
Boundary attacks	Subscriber location					C
IMSI catching attacks	Subscriber identity			C		C

the systems of communication C-RAN, on the other hand, is susceptible to the inherent security concerns that are associated with virtual systems and cloud computing technologies. For example, the centralized design of C-RAN is vulnerable to the risk of having a single point of failure. In addition, there are other risks that pose serious hazards to the system. These threats include intrusion assaults, which occur when attackers break into the virtual environment in order to monitor, change, or run software routines on the platform without being discovered.

Privacy Challenges in 5G

Some of the most significant privacy problems that might occur from the user's point of view are related to data, location, and identification. The vast majority of applications for smart phones demand the user to provide personal information before the installation may take place. The creators of the program or the organizations doing the development of the application rarely explain how the data is saved or what the reasons are that it will be utilized for. Threats that primarily target the geographic privacy of subscribers include semantic information attacks, timing attacks, and boundary attacks. Additional threats include boundary attacks. The access point selection algorithms used in 5G mobile networks have the potential to compromise users' privacy about their location at the physical layer level. An attack that catches the International Mobile Subscriber identify (IMSI) of a subscriber's User Equipment (UE) can be used to disclose the identify of a subscriber. This is accomplished by capturing the User Equipment (UE) of the subscriber. The establishment of a false base station that is seen as the preferred base station by the user equipment (UE) and may thus force subscribers to react with their IMSI is another method that can be used to launch such assaults. In addition, there are a variety of entities involved in 5G networks, including Virtual Mobile Network Operators (VMNOs), Communication Service suppliers (CSPs), and other suppliers of network infrastructure. Every single one of these actors has a unique set of goals when it comes to privacy and security. When it comes to the 5G network, one of the challenges that will be faced is the synchronization of mismatched privacy standards across different participants. Mobile operators have direct access to and control over all of the system components in the generations that came before this one before them. However, because they will be dependent on new players such as network service providers (CSPs), 5G mobile carriers would lose complete control of the systems. As a result, 5G operators will no longer have complete control over security and privacy controls. In shared environments, where the same infrastructure is shared by several players, such as virtual mobile network operators (VMNOs) and other such rivals, there is a significant risk to the privacy of users and their data. In addition, because 5G networks make use of cloud-based data storage and NFV capabilities, there are no physical limits when it comes to the network. Because of this, the operators of 5G networks do not have direct control over the location of the data storage in cloud environments. If user data is kept in a cloud that is located in a foreign nation, the privacy of the user is put in jeopardy. This is because various countries have varying levels of data privacy methods, which are determined by the context in which they wish to utilize them.

Security Solutions for Privacy in 5G

Privacy-by-design techniques, in which privacy is taken into consideration from the very beginning of the system, must be incorporated into 5G, and a large number of essential characteristics must be provided as built-in features. An method that is based on hybrid cloud computing is necessary, in which mobile operators are able to store and process data that is very sensitive locally, while also storing data that is less sensitive in public clouds. This will allow operators to have greater access to and control over the data, as well as the ability to select where it will be shared. In a similar vein, the implementation of service-oriented privacy in 5G will result in a more practical approach for protecting users' privacy. In order to provide accountability, data minimization, transparency, openness, and access control throughout the 5G network, improved methods will be required. For this reason, stringent privacy standards and legislation have to be taken into consideration during the process of standardizing 5G transmission. There are three distinct sorts of regulatory approaches that may be distinguished. A government-level regulation is the first type of regulation. This type of regulation is primarily responsible for the creation of country-specific privacy legislation, and it is implemented through multi-national organizations such as the United Nations (UN) and the European Union (EU). Second, there is the industry level, which is where a variety of industries and bodies, including as the ONF, ETSI, and 3GPP, work together to create the most effective principles and practices to safeguard individuals' privacy. In the third place, there are restrictions at the consumer level, which assure the required degree of privacy by taking into account the expectations of customers. In order to protect the privacy of the subscriber's location, it is necessary to use anonymity-based solutions, which allow the subscriber's true identity to be concealed and substituted with pseudonyms. Messages can be encrypted before being sent to a provider of location-based services (LBS), for example, which is another example of how encryption-based methods might be effective in this application. Obfuscation is another valuable technique that may be utilized to safeguard location privacy. This technique involves reducing the quality of location information in order to conceal its true nature. Furthermore, methods that are based on location cloaking are particularly effective for dealing with some of the most significant intrusions into location privacy, such as timing and boundary investigations.

Massive devices, different services, and different security levels.

The 5G network will be able to accommodate a wide variety of applications that have varying service needs. various players will be involved in the provision of these services, and they will require various security and privacy safeguards to be incorporated into the scope. Furthermore, sensitive information about users (such as bank passwords, medical records, and user-related data acquired from sensors) may be readily targeted due to the prevalence of non-identical access mechanisms, pervasive connection, and a huge number of devices. Taking transportation systems as an example, they require ubiquitous connection together with rapid and frequent authentication. On the other hand, smart-home gadgets, which are generally static, do not require fast and frequent authentication. The fact that a user may interface with gadgets in her house through her vehicle has resulted in the dissemination of user-related data to a variety of devices. (Table III presents a variety of use cases for 5G technology, along with their relative ranking in terms of the needs for security and privacy.) Because of this, the new security system needs to ensure that every component is protected and kept separate from the other components. This ensures that a compromised component does not influence or expose critical information about other components. As a result, plug-in-based security and privacy solutions will not be effective in the 5G network.

Attacks to/from small-cells

The deployment of small cells is advantageous in comparison to the deployment of a physical base station since it allows for quicker data rates, more efficient spectrum use, less energy consumption, and a significantly more cost-effective deployment. It is common for a SC, which is not installed by the trusted network, to cover many individuals in a public place. Because of this, SCs are more likely to be attacked. Intuitively, a hacked SC is capable of attacking many associated user equipment (UEs) as well as the core network. In addition, it is possible to deploy a malicious SC in order to corrupt and carry out a variety of attacks on the network and other devices. Consequently, it is necessary to have the knowledge to distinguish between trustworthy and malicious SCs, to understand how a device might trust a SC, and to understand how to ensure the safety of a trusted SC.

Conclusion

In conclusion, whereas 5G networks hold the promise of new prospects for innovation and economic growth, they also bring daunting security issues that need to be handled in a proactive and collaborative manner. Through a comprehensive knowledge of the complexities of 5G architecture, the identification of new threats, and the implementation of robust security measures, stakeholders are able to fully exploit the promise of 5G while simultaneously protecting the integrity of the network, the privacy of users, and the vital infrastructure. The purpose of this paper is to investigate these concerns in further detail, with the intention of providing insights into the changing environment of networking and security in the era of 5G. As a conclusion, the growth of networking and security in 5G networks reflects a landscape that is both complex and dynamic. This landscape is defined by technical innovation, regulatory obstacles, and strategic imperatives. Stakeholders can unleash the revolutionary potential of 5G by tackling these concerns in a comprehensive and collaborative manner. This will allow them to protect themselves against emerging threats and ensure the security, privacy, and dependability of future digital infrastructures.

REFERENCES

[1] N. Panwar et al., "A survey on 5G: The next generation of mobile communication," Physical Communication, vol. 18, pp. 64–84, 2016.

[2] "5G scenarios and security design," tech. rep., Huawei, 2016. Available at: http://www-file.huawei.com/~/media/CORPORATE/PDF/white%20paper/ 5g-scenarios-and-security-design.pdf.

[3] "5G PPP phase1 security landscape," tech. rep., 5GPPP, 2017. Available at: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP White-Paper Phase-1-Security-Landscape June-2017.pdf.

[4] "5G security recommendations package #2: Network slicing," tech. rep., NGMN Alliance, April, 2016. Available at: https://tinyurl.com/y6yrvnd3.

[5] F. Boccardi et al., "Five disruptive technology directions for 5G," IEEE Communications Magazine, vol. 52, no. 2, pp. 74–80, 2014.

[6] R. Ferrus´ et al., "SDN/NFV-enabled satellite communications networks: Opportunities, scenarios and challenges," Physical Communication, vol. 18, pp. 95–112, 2016.

[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] 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] 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] 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.