Cybersecurity Aspects of 5G Connectivity in Smart Cities Ecosystem via Connected and Autonomous Vehicles Use Cases

Athanasios Papadakis
Information Technologies Institute
Centre for Research and Technology Hellas, CERTH
Thessaloniki, Greece
papadakisa@iti.gr

Antonios Lalas
Information Technologies Institute
Centre for Research and Technology Hellas, CERTH
Thessaloniki, Greece
lalas@iti.gr

Konstantinos Votis
Information Technologies Institute
Centre for Research and Technology Hellas, CERTH
Thessaloniki, Greece
kvotis@iti.gr

Dimitrios Tzovaras
Information Technologies Institute
Centre for Research and Technology Hellas, CERTH
Thessaloniki, Greece
Dimitrios.Tzovaras@iti.gr

***Abstract*—This work presents the necessity of the implementation of mitigation techniques to counter the cybersecurity issues and threats that arise from the fifth generation (5G) embodiment in a smart city ecosystem. During the past few years, the popularity and growth of cellular technology has led the 5G networks to be considered as the emerging domain of future's communication architecture. Moreover, the connected and autonomous vehicles constitute an essential part of smart cities infrastructure, providing the answer for the city's mobility demands. With human safety being at stake, the security assurance is of the utmost importance. The requirement of ensuring a safe transportation system with complete trust to the smart city ecosystem is sufficiently described, while proper counter-measures within the scope of 5G connectivity are proposed.**

Keywords— Cybersecurity, 5G connected vehicles, Autonomous vehicles, Smart city, Mitigation techniques

I. INTRODUCTION

The rapid expansion of cities has concentrated more than half population of the world. This ever-growing urbanization is creating conditions demanding to find ways to preserve and optimize resources and organization. The aforementioned aspects have generated the formation of smart cities, which are defined by the ability to integrate multiple technological solutions, while securely managing the city's assets. The goal is to upgrade the quality of life by using technology to improve the efficiency of services [1]. One of the reasons that wireless and mobile networks have gone through so many changes over the past few years is to meet the ever-increasing needs of their users and satisfy the requirements of a smart city. The demand for service speed and reliability tends to grow over time, as the applications being used mandate more bandwidth. Thus, the new fifth generation mobile communications network (5G) promises to not only meet these requirements, but also radically change networking, as we know it. Smart cities in collaboration with the new 5G technology put a lot of emphasis on satisfying various quality necessities of the services provided to different application scenarios such as data transmission rate and delay. Where wide area coverage is required, 5G systems are capable of providing users with very high quality data transmission rates wherever they are, even if they are nearby the tips of the hives. In large cities where the density and volume wireless traffic is quite large, the demand for services increases especially at peak times [2].

In this context, the novel 5G's networks are able to provide excellent hot spot coverage with high capacity. An indicative application scenario is related to the sensors of connected or autonomous vehicles in a smart city, where a trusted connection between a large volume of low energy nodes is required. The 5G network can successfully deliver the connection of millions of devices covering the limitations of their low-power consumption sensors. However, one concern arising with the new era of 5G is related to the security aspects of connected or autonomous vehicles, as more people are using them and soon they will replace the outdated public transportation system. A characteristic example of a public application is the autonomous shuttle, which has been adopted in many cities all over the world [3] in a fully operative way. Since security is the cornerstone of creating a safe and viable transportation system, mitigation methods to tackle potential cybersecurity treats are of paramount importance. Specifically, the Internet of Vehicles (IoV) ecosystem, that is present in the automotive applications, is a combination of numerous networks such as vehicle-to-vehicle (V2V), vehicle to infrastructure (V2I), vehicle to pedestrian (V2P) and vehicle to

This work was supported by the European Union's Horizon 2020 Research and Innovation Programme Autonomous Vehicles to Evolve to a New Urban Experience (AVENUE) under Grant Agreement No 769033.

network (V2N). All these networks can efficiently operate under the 5G connectivity platform.

In this work, the necessity of counter-measures for cybersecurity threats in 5G networks operating in a smart city is introduced through the connected and autonomous vehicles paradigm. The information used to highlight the 5G security concerns is based on the challenges and attack vectors of previous network architecture technologies [4], but revisited to meet the high demands of smart city infrastructures. In section II, the need of 5G networks to connect with autonomous vehicles and smart city's infrastructure is adequately described, whereas the urgency to explore the security aspects of these connections is highlighted. Section III suggests some mitigation and prevention countermeasures, which can be implemented in this ecosystem.

II. Connected and Autonomous Transport in 5G-enabled Smart Cities

A definition for a smart city as it was given from Marsal-Llacuna et al. (2014) is: "Smart Cities initiatives try to improve urban performance by using data, information and information technologies (IT) to provide more efficient services to citizens, to monitor and optimize existing infrastructure, to increase collaboration among different economic actors, and to encourage innovative business models in both the private and public sectors" [5]. A person-centric adaptation of the Smart City Wheel [6] is depicted in Fig. 1, exhibiting the various aspects of a smart city and the technologies involved. Currently, some smart cities have been developed across the world, for instance Barcelona, Malta, and Singapore. The efficiency usage of energy and the reduction in both operational and capital cost are considered some indicative characteristics of them [7]. A notable example of utilizing these benefits is the connected or autonomous vehicle's ecosystem that exists in a smart city. Even though the technology required for such kind of applications already exists, the major drawback is the incapacity of the technology to operate in real time conditions across an interconnected network. The new 5G technology presents a solution for this problem while serving communication needs for billions of connected devices, with the right trade-offs between speed, latency, and cost. Speed is essential for data transfer, the response time of the connected component is translated in latency, and cost is related to the power consumption of the connected components, which answers the question if they will be able to operate for months or years without the need of human assistance. Some characteristics of the network's technology evolution are shown in Table 1 [8], which facilitates to understand the benefits of the novel wireless connectivity.

Some characteristic technologies that have being developed for 5G include Millimeter-Wave communications, which have opened up more spectrum range and provided the possibility of having much wider channel bandwidth. This alteration comes with some challenges in terms of technology and circuit design, while the main drawback of the mm-wave frequencies is that in practice they are absorbed completely from obstacles and consequently they do not travel far [9]. The

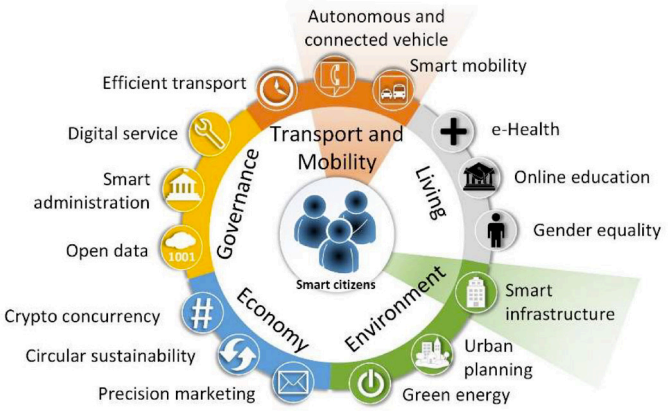

Fig. 1. Person-centric adaptation of the Smart City Wheel proposed by Cohen B [6].

cyclic prefix orthogonal frequency division multiplexing (CP-OFDM) is the main prospective for the new waveform adapted in 5G, as it provides excellent overall performance without being too heavy on the level of processing required, and comes to give the solution to some limitations of the orthogonal frequency division multiple access (OFDMA) 4G's technology [10]. An additional characteristic of 5G is massive multiple-input and multiple-output (MIMO) with beamsteering. Even though MIMO was used in many applications from LTE to Wi-Fi, the number of antennas were limited. However, the combination of numerous antennas provide enhanced performance giving excellent spectral efficiency and superior energy proficiency [11]. Furthermore, reducing the size of cells and deploying them with low transmission power and limited coverage provides more overall effective use of the available spectrum. Nevertheless, some issues need to be addressed in order to make the 5G architecture reliable [12].

Smart cities are constituted from six fundamental pillars; one of them is "effective mobility" or it can be found as "smart transport". This pillar is liable for improving the transportation of people inside the city, reducing the traffic accidents and utilizing the proper infrastructure for public transportation vehicles to operate more efficiently [13]. The person-centric adaptation of the Smart City Wheel [6] as shown in Fig. 1, denotes that connected vehicles are considered the key component of the smart transport pillar, either they are autonomous or not. Since the introduction of autonomous vehicles in 2010, their development and appeal has increased significantly. The link between smart city and smart transportation is undoubtedly the 5G network because vehicles are being fitted with sensory devices to derive input from external or internal environment for information processing, while the sharing of this sensitive information must be completed in real time. As a result, the successful operation of smart transportation system and its impact on society are solemnly depended on their management as well as the proper attention of privacy and cybersecurity issues [14].

III. Potential Attacks and Prevention Techniques

Autonomous vehicles have a built in plethora of cyber-connected components and multiple embedded sensors, in

TABLE 1. WIRELESS NETWORK TECHNOLOGY EVOLUTION DURING THE PAST FEW YEARS.

Technology	3G	4G	5G
Deployment	2004-2010	Now	5G Phase-1 (2018) 5G Phase-2 (2019)
Data Bandwidth	2Mbps	1Gbps	Bigger than 1Gbps
Key differentiator	Better internet experience, applications	Faster broadband internet, lower latency	Faster internet, wide range of applications, IoT
Technologies	WCDMA/HSPA+, CDMA2000/EV-DO, TD-SCDMA	LTE, LTE Advanced	Beam Division Multiple Access (BDMA) and Non- and quasi-orthogonal or Filter Bank multi carrier (FBMC) multiple access, not standardized yet
Services	Cohesive high class audio, video and data	Dynamic information access, wearable devices	Dynamic information access, wearable devices with AI capabilities
Core network	Packet N/W	Internet	Internet
Weakness	Failure of WAP for internet access, Real performance failed to match hype, Tied to legacy	Mobile explicit architecture and protocols	May exist after implementation

order to navigate freely and safely, exhibiting increased levels of connectivity. Since the 5G network is deemed as the central domain for future communication architecture, the associated potential attacks and threats, that arise, have to be thoroughly studied.

As observed in all networked computing devices, with connection mechanisms that support communication between the infrastructure and share data, the risk of attacks has been exponentially increased due to the multiple attack surfaces and vectors they employ. In order to create a robust defence, adequate understanding of the attack methods utilised for exploitation is required. Next, the attacks and the liabilities of the ecosystem are reported, taking into account the security challenges of 5G connectivity along with the wireless nature of mobile networks, but also the ones that exist in the potential technologies that are vastly important for 5G and suggest possible mitigation techniques.

A. Main security challenges in 5G

Software defined networking (SDN) is considered an indispensable part of the 5G networks. It is defined by the Open Networking Foundation (ONF) as "the physical separation of the network control plane from the forwarding plane, where the control plane controls several devices" [15]. Hence, it is used to control the switches in order to deliver network services wherever they are needed, regardless of the specific connections between a server and devices [16]. Unfortunately, it exhibits a variety of attack surfaces that can be targeted; some of the attacks are the following, as illustrated in Fig. 2. Denial-of-service (DoS) attacks, as well as distributed denial-of-service (DDoS) attacks, lead the user to lose control of the system. The main versions of these attacks are TCP/SYN flood, teardrop, smurf and ping of death. They overwhelm the recourses causing the inability of the system to respond. Respectively, DDoS attack the system's resources also, but they are launched from a large number of other host machines, which are infected from malicious software and/or controlled from the attacker. These kind of attacks do not provide direct benefits for the attackers but they can cause hazard depending on the infected target. Usually, the target point will be the centralized control elements for DoS attacks, and for the TCP attacks will be the SDN controller and switch communications. For example, it can be used on vehicular ad-hoc networks (VANETs) and general in V2X IoV ecosystem's communications, generating a traffic disturbance or even an accident [15].

Another, vulnerable element of SDN is the address resolution protocol (ARP) which is a communication protocol used for discovering the link layer address, such as MAC address, associated with a given internet layer address, typically an IPv4 address. It can been targeted by man in the middle attacks, which occur when a hacker intervenes between the communications of a client and a server, getting access to all the packets sent in the connection. Some versions of this kind of attack are session hijacking, IP spoofing and cache poisoning. When the connection is established and they have successfully implanted themselves between the two trusted parties, they exploit this trust and gather all the needed information. The magnitude of the hazard that follows this kind of attack depends on the attacker's intentions [18].

Moreover, SDN controllers can be targeted via traffic sniffing and repudiation attacks. With sniffing attacks, a malicious user is able to eavesdrop data from network or links and steal important information. The main condition for this is to have constant traffic in the network. In SDN, an attacker can take advantage of unencrypted communications to intercept traffic from and to a central controller. Repudiation is the act of refusing the authorisation of some transaction that occurred. The controller may experience this kind of attack from applications, or from upstream/downstream controllers when there are controller hierarchies. This attack is used to change the authorisation information of actions executed by an attacker and log whatsoever information he desires. Through this attack, general data could be manipulated in name of others, in a similar manner as spoofing mail messages function. If this attack takes place, the data stored on log files can be considered invalid or misleading [19].

All the application-programming interfaces (API) are exposed to some critical attacks, which target either to extract from the user information for their credentials or to guess them with various techniques. Usually, phishing and spear phishing attacks exploit the ignorance of some users and send emails that appear to be from trusted sources asking for personal information. There is a combination of social engineering and technical trickery in order to successful undertake this kind of attack. Spear phishing attacks are more personal and relevant to the user that is targeted [20], [21].

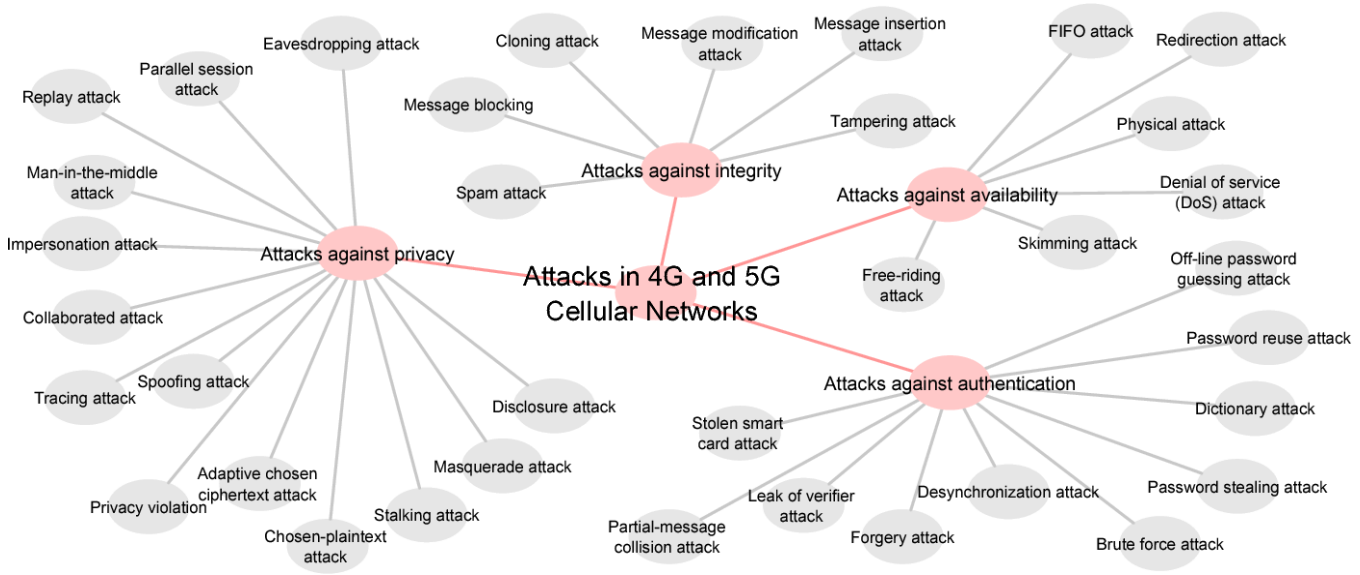

Fig. 2. Classification of attacks in 4G and 5G Cellular Networks

Regarding the login procedure, authorizations are susceptible to password attacks. These attacks target the passwords, as they are the most common way to authenticate users' information to a system. The malicious attackers are sniffing for information from the connected network to acquire unencrypted passwords with the assist of social engineering. There are two kinds of password attacks, the brute force and dictionary. The first employs random approach by trying different combinations of passwords and usernames, the second utilises the copied encrypted file that contains passwords, applies same encryption to a dictionary of frequently used passwords, and matches the results. As it happens with the phishing attacks, the potential problems that will be created are depended on the use of the sniffed credentials from the attacker, which can be used with several ways, as identity theft, personal data leakage, location privacy of subscribers, API exploitation, etc [22].

An alternative way to obtain credentials or confidential information that users send over the network is eavesdropping attacks, which occur through intercepting the network traffic. A vulnerable component on the 5G's architecture is the Orchestrator and/or the virtual network functions (VNF) manager. Eavesdropping methods in the specific occasion are used to exploit kernel-based virtual machine (KVM) live block migration when it does not properly create all expected files, allowing the attackers to obtain a snapshot of the root disk contents of other users via ephemeral storage. The ramifications are not visible right after the vulnerability exploitation, but it is up to the attacker how he will act with this information [19].

VNF are vulnerable to a special set of virtualization threats, such as side-channel attacks, flooding attacks, hypervisor hijacking [24], malware injection, and cloud-specific attacks [25]. Private deployments of network function virtualization (NFV) are weak to malicious insiders, who exploit the vulnerabilities of VNF's open source software. Usually, they are exposed to diverse security attacks and to possible leakage of security aspects or difficulties in communication. Also, attention is needed in completing flawlessly the updates on the system, without any suspension, which will give the attackers the ability to exploit any pre-updated backdoors. Thus, there should be a software validation for the authentication and integrity of the pre-loaded code, whereas it examines if any unauthorized personnel or operation has conducted modifications [26].

Additionally, VNF are based on virtual machines (VMs) architecture. Riddle and Chang [27] have presented that there are possible attacks able to steal resources from other VM(s). A potential attack for data theft occurs when the attackers infect the target VM with malicious malware, in order to use the memory bus or cache connection and steal data, e.g. cryptographic keys. Another method is the VM monitoring evasion, which happens with the exploitation of VM rollback process. If the VM is attacked with brute force for password cracking, it will probably alert the administrator and roll back in a previous snapshot. This provides the opportunity to the attackers to continue their attack, without being compromised. Indicative examples of attacks were executed in the Xen's hypervisor software by exploiting its credit scheduler [23].

B. Prevention techniques

Network security of 5G's architecture thus the smart city's ecosystem can be improved by implementing some vital mitigation techniques. An indicative example of a 5G network slice encompassing autonomous vehicle navigation [24] is depicted in Fig. 3. Various networks and components have to be taken into account in order to ensure a safe ecosystem. As it is more efficient to preclude the attack than to deal with the exploitation after the breach, some prevention techniques are proposed. Firstly, a network firewall is a critical defensive mechanism that inspects incoming and outgoing network traffic and permits it or blocks it, based on predefined rules. There may be multiple firewalls within the network and they must be placed at nodal locations. Firewalls may be employed as part of the existing 5G architecture or as a stand-alone device in accordance with the architectural smart city's needs.

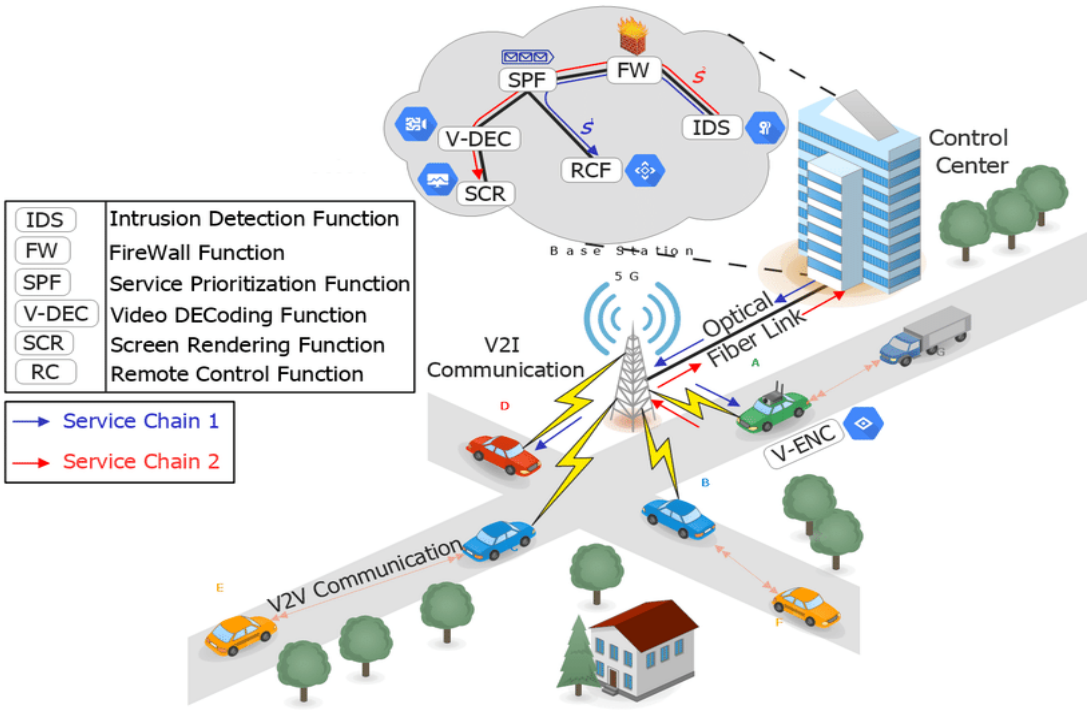

Fig. 3. Example of a 5G network slice encompassing autonomous vehicle navigation [28].

Access to the firewall must be restricted and require a unique password authentication for making changes in configuration or a change in rules. An additional approach is the security information and event management (SIEM), which is a software solution that aggregates and analyses the activity from many different resources across the infrastructure. SIEM collects security data, which are stored, normalized and fed to analytics processes, in order to discover trends, detect threats, and investigate alerts. For instance, malware information sharing program (MISP) is a sharing platform, which stores and distributes security indicators and discovered threats [29]. This software allows interaction with other similar programs, like intrusion detection systems (IDS). An IDS or intrusion detection and prevention system (IDPS) is an advanced network system that detects anomaly behaviour, while the IDPS prevents it from traversing across the network.

An IDS/IDPS is more powerful than a simple firewall, since it analyses behaviour based on previously seen data, timing, endpoints and not just a set of predefined rules at a set point in time. Two major approaches exist for creating the IDS/IDPS behaviour analysis: Using a predefined deterministic set of rules, or creating a dynamic set of rules based on machine learning. Each method has its advantages and disadvantages, but both share the overall benefits previously mentioned. The IDS/IDPS must be placed in similar fashion with firewall in order to maximize the amount of traffic that can be analysed. Another prevention technique that can be used is to keep logs, which must include any anomalies found in the system, attack attempts, failed login attempts, dropped messages, etc. Logs must either be encrypted or stored in a secure location to prevent an attacker from reading the log or tampering with it. Only specific and relevant processes shall have read/write/move access to their own logs in order to prevent an attacker from tampering with or learning from the log's content. Logs are useless if no one is looking at them, so there should be a mechanism to collect logs and send them back for inspection, such as the software reported earlier [30].

A drawback in some communication channels is the use of insecure and unencrypted protocols, which allows attackers to eavesdrop the traffic and data between the host and other communication party. An indicative example is the authentication keys, which may lead to authentication attacks in V2I networks. The attacker can extract valuable information about the vehicle stream, such as its trace by linking position data, and use it for own benefit. The presence of signatures in the beacon messages can worsen the situation, and allow the attackers to identify the participating vehicles in the cooperative adaptive cruise control stream. Eavesdropping is a type of passive attack, and hence is difficult to detect, especially in broadcast wireless communication [31]. However, it is possible to prevent the success of eavesdropping by using encryption to achieve data privacy or using anonymity techniques to ensure identity and location privacy. Anonymity is typically implemented using group signatures or short-term certificates (pseudonyms). In addition, another part of infrastructure, which requires authentication or encryption, is the key management. It must include methods for adding new entities and revoking existing entities that have expired or been compromised. The integrity of the key infrastructure must be assured i.e. devices that are part of the infrastructure should implement the appropriate

security mechanisms, such as hardware trust modules and secure boot, in order to prevent an attacker from extracting keys from a device [32].

IV. Conclusion

In this paper, the cybersecurity requirements of 5G-enabled smart cities have been introduced through the paradigm of smart mobility i.e. connected, autonomous or not, vehicles. During the next years, a more stable and complete 5G architecture will be available, thus enabling smart transportation to constitute the key piece of smart cities. In this context, vital attributes of 5G networks that have been modified in comparison to the previous 4G version, are examined. The main security challenges are analysed in terms of essential components that can threaten integrity in 5G implementations. Finally, a set of prevention techniques is provided to secure potential vulnerabilities for exploitation in the smart city ecosystem. The proposed approaches, whether considered during the design and deployment phases, are expected to minimize the potential security breach.

References

[1] Tao Han, Xiaohu Ge, Lijun Wang, Kyung Sup Kwak, Yujie Han, and Xiong Liu, "5G Converged cell-Less communications in smart cities," IEEE Communications Magazine, Vol. 55, No. 3, March 2017

[2] Panagiotis Demestichas, Andreas Georgakopoulos, Kostas Tsagkaris, and Serafim Kotrotsos, "Intelligent 5G networks: Managing 5G wireless mobile broadband," IEEE Vehicular Technology Magazine, Vol. 10, pp 41-50, Sept 2015

[3] NAVYA be fluid, Available online at: https://navya.tech/en/

[4] Simon Parkinson, Paul Ward, Kyle Wilson and Jonathan Miller, "Cyber threats facing autonomous and connected vehicles: future challenges," IEEE Transactions On intelligent Transportation Systems, Vol.18, pp 2898-2915, Nov 2017

[5] Vito Albino, Rosa Maria Dangelico and Umberto Berardi, "Smart cities: definitions, dimensions, performance, and initiatives," Journal of Urban Technology, Vol. 22, Issue 1, pp 3-21, February 2015

[6] José Manuel Lozano Domínguez and Tomás Jesús Mateo Sanguino, "Review on V2X, I2X, and P2X communications and their applications: A comprehensive analysis over time," Sensors 2019, Vol. 19, June 2019

[7] Mahmoud Al-Hader and Rodzi A., "The smart city infrastructure development & monitoring," Theoretical and Empirical Researches in Urban Management, Vol. 4, Issue 2, pp 87-94, May 2009

[8] Murtaza A.Siddiqi, Mohammad Khoso and Abdul Aziz, "Security issues in 5G network," International Conference on Computing and Mathematical Sciences, Feb 2017

[9] S. Rappaportet al., ''Millimeter wave mobile communications for 5G cellular: It will work!,'' IEEE Access, Vol. 1, pp. 335–349, May 2013

[10] Ali Fatih Demir, Mohamed Elkourdi, Mostafa Ibrahim and Huseyin Arslan, "Waveform design for 5G and beyond," 5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management, pp.51-76, Feb 2019

[11] Erik G. Larsson and Liesbet Van der Perre, "Massive MIMO for 5G," IEEE 5G Tech Focus: Vol. 1, , March 2017

[12] Akhil Gupta and Rakesh Kumar Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," IEEE Access, July 2015

[13] Anna Augustyn, "Smart Cities – brand cities of the future," The Business of Place: Critical, Practical and Pragmatic Perspectives, Jan 2013

[14] Hazel Si Min Lim and Araz Taeihagh, "Autonomous vehicles for smart and sustainable cities: an in-depth exploration of privacy and cybersecurity implications," Energies 2018, April 2018

[15] ONF (Open Networking Foundation), "Software-Defined Networking (SDN) Definition," https://www.opennetworking.org/sdn-resources/sdndefinition.

[16] Ghada Arfaoui, Jos´e Manuel Sanchez Vilchez and Jean-Philippe Wary, "Security and Resilience in 5G: Current Challenges and Future Directions," 2017 IEEE Trustcom/BigDataSE/ICESS, Aug 2017

[17] Sudhir K. Routray, and Sharmila. K. P., "Software defined networking for 5G," International Conference on Advanced Computing and Communication Systems 2017, Jan 2017

[18] Ijaz Ahmad, Tanesh Kumary, Madhusanka Liyanagez, Jude Okwuibex, Mika Ylianttila and Andrei Gurtov, "5G security: Analysis of threats and solutions," IEEE Conference on Standards for Communications and Networking (CSCN), Sept. 2017

[19] Ana Danping, Makan Pourzandi, Sandra Scott-Hayward, Haibin Song, Marcel Winandy and Dacheng Zhang, "Threat analysis for the SDN architecture," IEEE Conference on Standards for Communications and Networking (CSCN), July 2016

[20] Tom Jagatic, Nathaniel Johnson, Markus Jakobsson and Filippo Menczer, " Social Phishing," School of Informatics Indiana University, Bloomington December 12, 2005

[21] E. Conrad, S. Misenar and J. Feldman, CISSP Study Guide, 2010

[22] Aaron L.-F. Han, Derek F. Wong, Lidia S. Chao, Advances of Password Cracking and Countermeasures in Computer Security, https://arxiv.org/ftp/arxiv/papers/1411/1411.7803.pdf

[23] François Reynaud, François-Xavier Aguessy, Olivier Bettan, Mathieu Bouet and Vania Conan, "Attacks against network functions virtualization and software-defined networking: State-of-the-art," IEEE Conference on Network Softwarization, Nov 2016

[24] A. van Cleeff, W. Pieters, and R. J. Wieringa, "Security Implications of Virtualization: A Literature Study," 2009 Int'l. Conf. Computational Science and Engineering, vol. 3, pp. 353–58, Aug 2009

[25] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila and Andrei Gurtov, " Overview of 5G Security Challenges and Solutions, "IEEE Communications Standards Magazine, Vol. 2, pp. 36-43, April 2018

[26] Ahamed Aljuhani and Talal Alharbi, "Virtualized Network Functions Security Attacks and Vulnerabilities," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Jan 2017

[27] A. R. Riddle and S. M. Chung, "A Survey on the Security of Hypervisors in Cloud Computing," 2015 IEEE 35th International Conference on Distributed Computing Systems Workshops, 2015

[28] Long Qu, Chadi Assi and Maurice Jose Khabbaz, "Reliability-aware service chaining in carrier-grade softwarized networks," IEEE Journal on Selected Areas in Communications, March 2018

[29] Sandeep Bhatt, Pratyusa K. Manadhata and Loai Zomlot, "The operational role of security information and event management systems," IEEE Security & Privacy, Vol. 12, pp 25-41, Oct. 2014

[30] Ashutosh Dutta, "Security in SDN/NFV and 5G networks opportunities and challenges," IEEE Future Networks, June 2019

[31] Jonathan Petit and Steven E. Shladover, "Potential cyberattacks on automated vehicles", IEEE Transactions On intelligent Transportation Systems, Vol.16, pp 1-11, September 2014

[32] Arash Shaghaghi, Mohamed Ali Kaafa, Rajkumar Buyya and Sanjay Jha, "Software-Defined Network (SDN) data plane security: Issues, solutions and future directions," ArXiv 2018, April 2018.