Securing Cyberspace of Future Smart Cities with 5G Technologies

Adnan Akhunzada, Saif ul Islam, and Sherali Zeadally

Abstract

Future smart cities promise to dramatically improve the quality of life and have been attracting the attention of many researchers in recent years. The integration of IoT with their corresponding service delivery models to manage a city's asset securely remains a significant challenge. The deployment of diverse IoT technologies and several architectural components and novel entities of emerging ICT solutions opens up new security threats and vulnerabilities. Large-scale, seamless communication among multiple IoT technologies is highly dependent on the operations of the underlying wireless access technologies such as WSNs, SDR, CR and RFID. We present thematic layered taxonomies to highlight the potential security vulnerabilities, attacks, and challenges of key IoT enabling technologies which underpin the development of smart cities. We also identify potential requirements and key enablers that play a vital role in the development of secure smart cities. Finally, we discuss various open issues that need to be addressed to unlock the full potential of 5G for future smart cities.

Introduction

Smart cities have strong potential to improve the quality of life and they are no longer a futuristic promise but a reality. Several governments have started ambitious smart city projects around the world to address some of the challenges brought about by the rapidly evolving digital world and the fast growth of urbanization. Moreover, we have witnessed an increasing demand for Internet of Things (IoT) technologies and Information and Communications Technology (ICT) solutions. Today, many services are being delivered to IP-enabled smart mobile devices to mobile users. These technological trends are likely to attract a huge mass market and several key players within smart connected communities [1]. Among the many key players, the smart city concept has great potential to address the need for well-managed, reliable, flexible and improved quality of life [2]. Currently, the revolutionary smart city concept has leveraged mostly wired and wireless conventional networks. However, the development of future smart cities is increasingly being geared toward the provision of smart services. To implement the "smart" concept in a smart city, IoT technologies, ICT solutions and their corresponding service delivery models, and various underlying wireless access technologies, should all be seamlessly integrated [1, 3]. Despite all the hype about smart cities, academia and industry are still apprehensive about the security of future smart cities and many outstanding security challenges remain unsolved.

The advent of 5G wireless communications has brought about many benefits including the support of dynamic, high speed and reliable networks. 5G technology is a bold new initiative by diverse governments to keep pace with the rapidly evolving digital world and meet the needs of users and the connectivity requirements of billions of IoT devices in various sectors of smart connected communities [1]. 5G is leveraging multiple traditional and modern technologies to provide several gigabits per second data rates that are much higher than previous wireless technologies. Similarly, 5G can support ultra-low latency (less than one millisecond) which makes it very feasible to support various delay sensitive portable or mobile applications, robotics and virtual reality services, and cyberphysical systems [3]. Unlike LTE/4G, 5G is suitable for both automation systems and networked devices. 5G is expected to revolutionize the industry to meet the challenges of Industry 4.0. Consequently, it is essential to move beyond the smart services, products, and industries to unleash the full potential of 5G [3].

The smart city concept promises to improve the quality of life and provide substantial managerial benefits, security and integrity but these benefits remain unproven when it comes to the highly dynamic and heterogeneous environment of future smart cities. Moreover, the compromise of any integral entity in any way would certainly affect the entire connected smart city's network. Moreover, with the constantly evolving landscape of digital threats and cyberattacks, the abstraction of the underlying topologies, flows, software agents and hardware resources can significantly help in harvesting core intelligence that can be exploited to launch advanced and diverse attacks. In contrast, the programmability aspects of various applications and services are also vulnerable to numerous malicious code exploits that can subsequently be used to generate massive attacks. Moreover, the various communication Application Programming Interfaces (APIs) can also be targeted with diverse side-channel and Denial of Service (DoS) attacks [4, 5]. Several communication APIs involved are vulnerable to both active and passive eavesdropping [4]. Finally, the cyber-attacks launched through various smart city agents can also disrupt the future smart city's network.

Digital Object Identifier:
10.1109/MNET.001.1900559

Adnan Akhunzada is with Technical University of Denmark, and also with Comsats University Islamabad (CUI); Saif ul Islam is with KICSIT, Institute of Space Technology; Sherali Zeadally is with the University of Kentucky.

0890-8044/20/$25.00 © 2020 IEEE

Motivation: The IoT ecosystem comprises a layered architecture, where a security implication (i.e., a vulnerability exploit, a security incident, or cyber threat and attack) pertaining to any layer can severely affect the other layers. Furthermore, securing the highly dynamic and heterogeneous environment (i.e., IoT ecosystem and wide-ranging communication) that constitutes the cyberspace of a future smart city is crucial. In addition, the establishment of trust with novel architectural components and agents in a smart city remains a significant challenge.

Contributions of this Work

We summarize the main contributions of this article as follows:

- We discuss vulnerabilities and attacks of key IoT technologies which are used in the development of future smart cities. We also highlight outstanding security challenges that must be addressed for these technologies. We do so by developing thematic core layered taxonomies that present security aspects pertaining to each layer.
- We present open issues of 5G that need to be addressed to enable future smart cities to reap the benefits of 5G and ultimately improve the quality of life.

The remainder of this article is organized as follows. In the following section we present an overview of a smart city. Then we highlight the security vulnerabilities, attacks, and challenges of key IoT enabling technologies using a layered approach to identify the security needs of the future smart cities. Following that we discuss the requirements and key enablers of future smart cities. We then highlight open issues of 5G that, if addressed, could be beneficial for future smart cities. Finally, we present some concluding remarks.

Overview of Future Smart Cities

This section presents a brief introduction to future smart cities to better understand the cyberspace security concerns related to the integration of multiple IoT technologies into a smart city. Figure 1 depicts a simplified overview of a smart city. Rapid urbanization is a worldwide trend in the 21st century. Today, there is a significant increase in the number of inhabitants in urban areas in comparison to rural/countryside population, and this is expected to continue in coming years. The current Intergovernmental Panel on Climate Change (IPCC) reports on human settlements and infrastructures and found that the development of urban zones is growing at a pace almost twice as fast as the urban population development. Further, the IPCC reports also predict that in the first three decades of the 21st century, the anticipated urban development will be higher than the combined urban extension in all of mankind's history [6].

The utilization of smart ICT technologies in the development of modern communities is an emerging trend. These communities are getting smarter by automating routine processes in building infrastructures, traffic systems, energy networks, and communication systems. In many ways, such developments empower us to monitor, realize and plan the city to enhance productivity, value and personal satisfaction of its residents [1, 2]. The smart city concept started with the usage of easy to understand information and communication technologies created for urban spaces. Its significance has since been extended to address the needs of urban communities and their developments. Smart cities are creating modern, dynamic and adaptive societies to provide a higher quality of life. The concept of smart city not only links existing infrastructures, but also endorses social and technological innovations. Smart cities can be characterized by six characteristics, namely: smart economy, smart mobility, smart environment, smart people, smart living and smart governance [2].

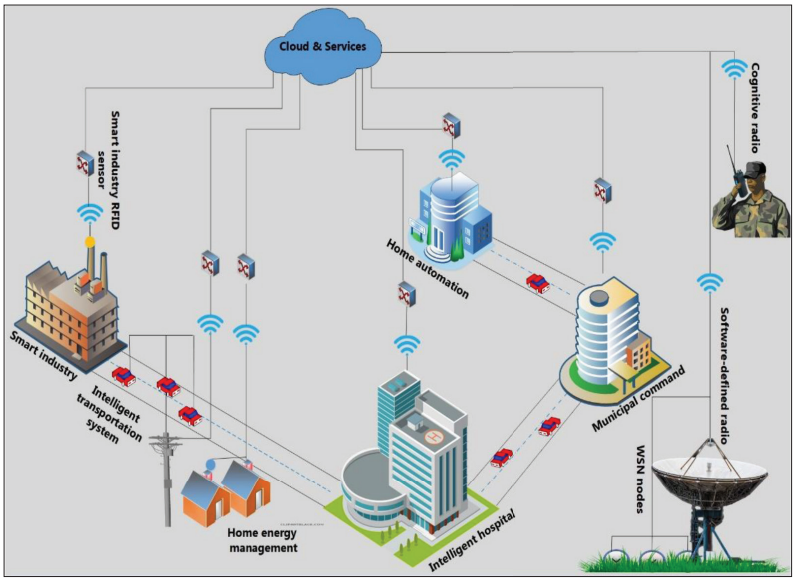

FIGURE 1. A simplified overview of the future smart city.

They leverage and integrate well-known energy sources, traffic and transport related sustainable and environment friendly ideas. Their emphasis is on new types of governance, administration and public contribution and participation. Each city can focus on any of the above-mentioned characteristics. A smart city is a community that is effective and efficient, practicable, sustainable and livable. The term 'smart city' has turned out to be increasingly prominent in the field of urban planning. Smart urban communities can act as a vehicle for managing quick urbanization and different issues brought about by the expanding urban population. The execution of smart technologies can increase the value of conventional cities. The smart city idea presents new practices and services that can affect policy decisions and planning. Hence, the smart city is a coordinated urban framework that includes the utilization of infrastructures such as smart grids together with different types of sustainable power sources (generation and distribution) and new systems of mobility based on an organized and distributed network. The development of the smart city is done by organizers, policymakers, officials, city divisions, designers, executive planners and industry.

Intelligent decisions need to be taken at the strategic level if urban communities need to have access to smart services. Currently, more than half of the world's population is living in urban areas and this will rise to two thirds by 2050 [7]. Clean water and disposable land are

constrained, as most of us know. Food, lodging and waste evacuation require crude materials and energy. To maintain a high standard of living in the long term, urban areas must diminish their environmental impact to minimize their biological footprint and explore alternative options to fossil fuel, for instance. Carbon dioxide (CO_2) emissions must be reduced in the decades to come, while measures should be taken to better manage global warming, floods and extended heat waves. Around the world, a large portion of greenhouse gases are due to urban living. Smart urban communities need to manage current worldwide and global issues such as climate change and scarcity of resources [6]. The present challenges confronting the smart city concept are globalization and the worldwide networking of the workforce. Institutions and information also have their impact on urban communities. Financial and social structures are constantly changing. Urban politics and legislative administration need to adapt their strategies to these emerging developments. The measures taken by smart city designers and developers should focus on a wide range of issues including social, financial, spatial and others [1, 2, 6].

New technologies and innovations must be evaluated in terms of their benefits for people. Before smart ideas are implemented and executed, we require a dynamic and active participation of the public. To reap the actual benefits from the smart city concept, some skills must be taught to the public by the government and the private sectors to cope with emerging tools and technologies, particularly for smart communications and data security. Eventually, collaborations and interactions must be developed across systems so that the objectives and solutions can be well-defined for smart cities to improve the daily lives of people. Some well-known attributes of a smart city include a well-planned friendly environment which provides cost-efficient services and sound technological services to improve the living standards of the residents [2].

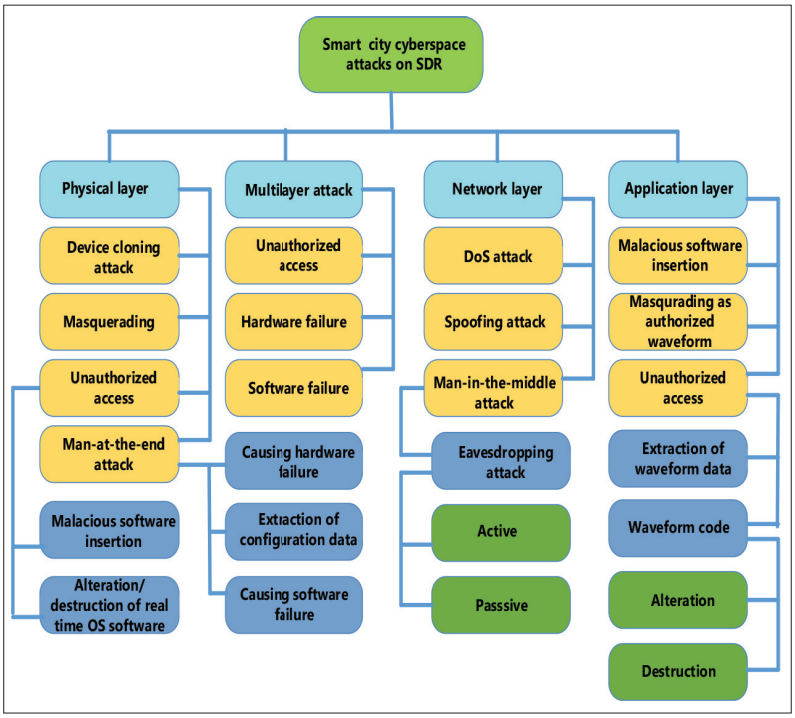

FIGURE 2. Taxonomy of SDR layered based security vulnerabilities, and attacks.

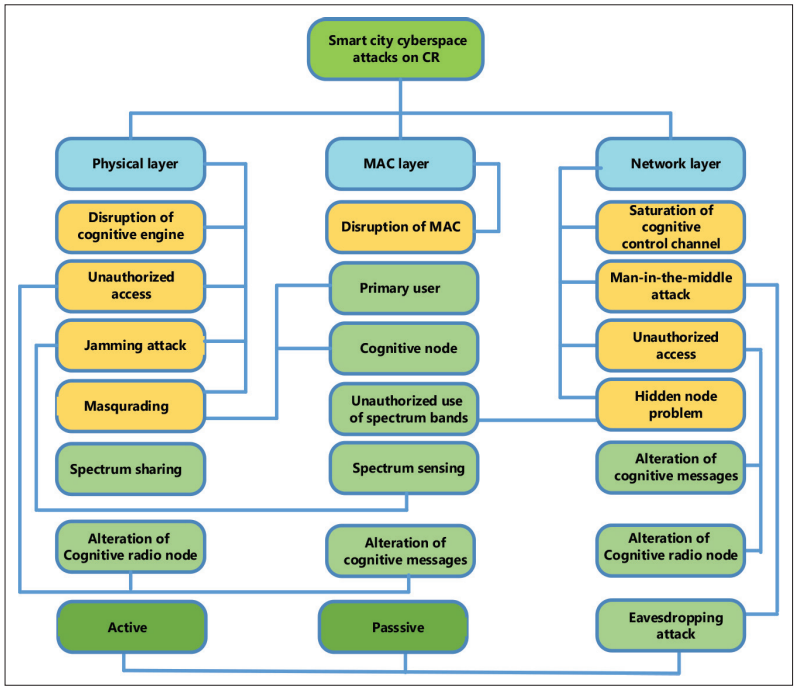

FIGURE 3. Taxonomy of CR layered based security vulnerabilities, and attacks.

A Top-Down Approach to Address Cybersecurity Vulnerabilities, Attacks and Challenges in Future Smart Cities

To smartly connect and enable ICT solutions with their corresponding service delivery, wireless access technologies must be integrated and employed. Several IoT enabling access technologies such as Radio Frequency Identification (RFID), Wireless Sensor Networks (WSNs), Software Defined Radio (SDR) and Cognitive Radio (CR) networks are vital for the intelligent gathering of information anywhere at any time in the highly dynamic heterogeneous environment of a future smart city. Consequently, we mainly focus on the security vulnerabilities, attacks, and challenges of these key IoT enabling technologies (i.e., RFID, WSNs, SDR, and CR) that constitute the smart city cyberspace using a top-down layered approach.

Security Vulnerabilities and Attacks of SDR and CR

CR and SDR wireless access technologies are used to enable interoperable communication to address the spectrum shortage problem. Both SDR and CR are vital to enable IoT and 5G communication. The cyberspace of a smart city communication network comprises diverse entities that opens up a new class of security threats and challenges. Considering the Dynamic Spectrum Access (DSA) of a smart city communication network, the authors of [8] systematically address security vulnerabilities and diverse sophisticated threats/attacks, and challenges associated with SDR and CR technologies. The DSA is an essential part of the emerging smart city communication networks [9]. To start with, the wide deployment of SDR requires an adequate level of physical

safety and security. SDR has reconfiguration capabilities which enable it to download various new radio applications and diverse communication links. Consequently, SDR is vulnerable to malicious modifications and injections due to its open communication without any integrity checks on the transmitted data.

Device cloning is a frequently used term in traditional wireless communications. It represents unauthorized access to diverse services offered by another SDR device. Device cloning is a major security threat to the emerging 5G communication networks. Irrespective of its architecture, design and framework, SDR heavily depends on end users and clients. Attacks such as Man-at-the-End (MATE, an adversary who has complete access to a software or hardware and can compromise it directly or through a remote connection) in general-purpose environments and settings are difficult to address [4]. Moreover, SDR devices and components are easily programmable and accessible in an open environment and are vulnerable to sophisticated MATE attacks. Such types of attacks may cause SDR devices to go completely offline, resulting in software or hardware failures and can also lead to unauthorized access [10]. Further, the Cognitive Control Channel (CCC) is also vulnerable to various denial of service attacks. Figure 2 presents a detailed taxonomy of vulnerabilities and attacks on SDR.

Cognitive radio (CR) also plays a vital role in the integration of multiple IoTs in a smart city ecosystem [8]. In a 5G dynamic spectrum, CR also requires an appropriate level of physical safety and security. The physical layer is vulnerable to sophisticated attacks such as unauthorized access, which subsequently leads to alteration of cognitive messages, and jamming attacks that severely affect spectrum sensing and sharing abilities. Moreover, the physical layer is also vulnerable to disruption of the cognitive engine as well as masquerading both as a primary user and a cognitive node. The network layer also experiences saturation attacks on the cognitive control channel and the hidden node problem that causes unauthorized use of spectrum bands. In addition, man-in-the-middle attacks can also cause active or passive eavesdropping. Furthermore, the MAC layer can experience severe Media Access Control (MAC) disruption such as DoS assaults and MAC address spoofing to disrupt network services. Figure 3 shows a detailed taxonomy of various possible attacks and vulnerabilities of CR.

Security Vulnerabilities and Attacks of RFID

RFID plays a significant role in the identification of a large number of connected devices in the smart city environment. RFID allows the integration of multiple IoT devices to perform location tracking, monitoring and transfers the processed information appropriately [11]. The major challenge associated with the wide deployment of RFIDs in future smart cities is ensuring an adequate level of security. The physical layer is vulnerable to various types of sophisticated attacks, including unauthorized access, which subsequently leads to RFID TAG modification and destruction, and jamming attacks which severely exhaust various resources. Moreover, the physical layer is also vulnerable to manipulation of various control messages

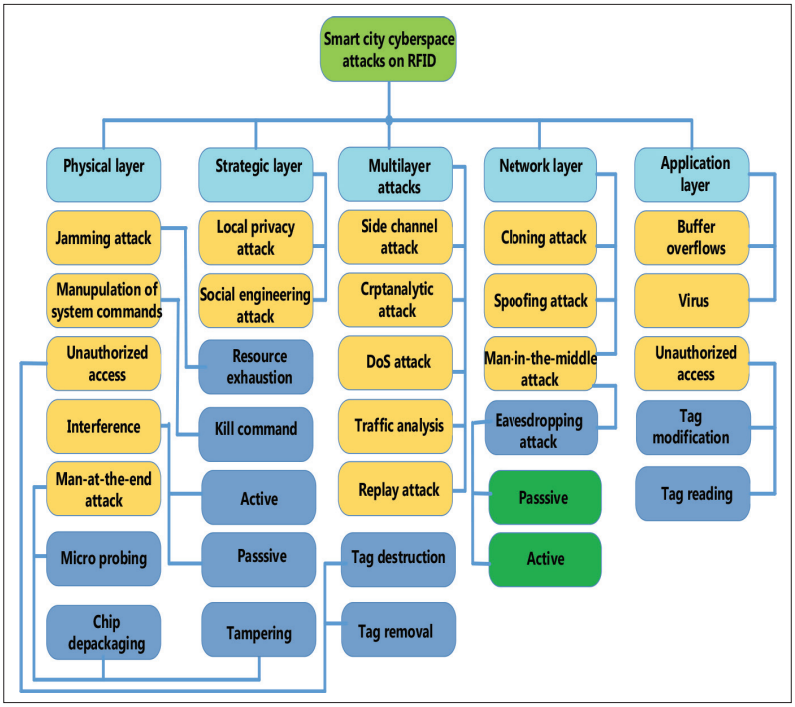

FIGURE 4. Taxonomy of RFID security vulnerabilities, and attacks.

and system commands. Additionally, Man-at-the-End attacks may further launch micro-probing, chip-de-packaging, and numerous tampering attacks. The physical layer is also vulnerable to channel interference. The network layer can also be targeted with spoofing, man-in-the-middle that may lead to eavesdropping (active and passive), and cloning attacks. The application layer is vulnerable to unauthorized access that can subsequently lead to RFID TAG reading, buffer overflow attack, and infection by various viruses. The strategic layer of RFID is vulnerable to location privacy attacks and social engineering attacks. RFIDs can also experience multilayer attacks, that is, side channel attacks, replay attacks, DoS attacks, traffic analysis and engineering, and cryptanalytic attacks. Figure 4 shows a detailed RFID taxonomy of attacks.

Security Vulnerabilities and Attacks of WSNs

WSNs play a crucial role in integrating multiple IoT devices and systems for future smart cities. Without sensor networks, IoT is seriously hindered and therefore, it is an integral part of future smart cities. Here we discuss generic WSNs attacks. However, it is applicable to any other sensor network such as Radio Sensor Networks (RSNs). A major challenge in the wide deployment of WSNs is the provision of an adequate level of security [12]. The physical layer is vulnerable to two sophisticated attacks (i.e., jamming attacks that severely contribute to resource exhaustion), and various tampering attacks. The network layer can also experience spoofing attacks, selective forwarding attacks, and is vulnerable to a variety of DoS attacks as shown in Fig. 5. However, a detailed description of these DoS attacks is beyond the scope of this article. The link layer is vulnerable to collision attack, neglect and greed attack, resource exhaustion attack, and unfairness attack (i.e., a DoS attack that continuously

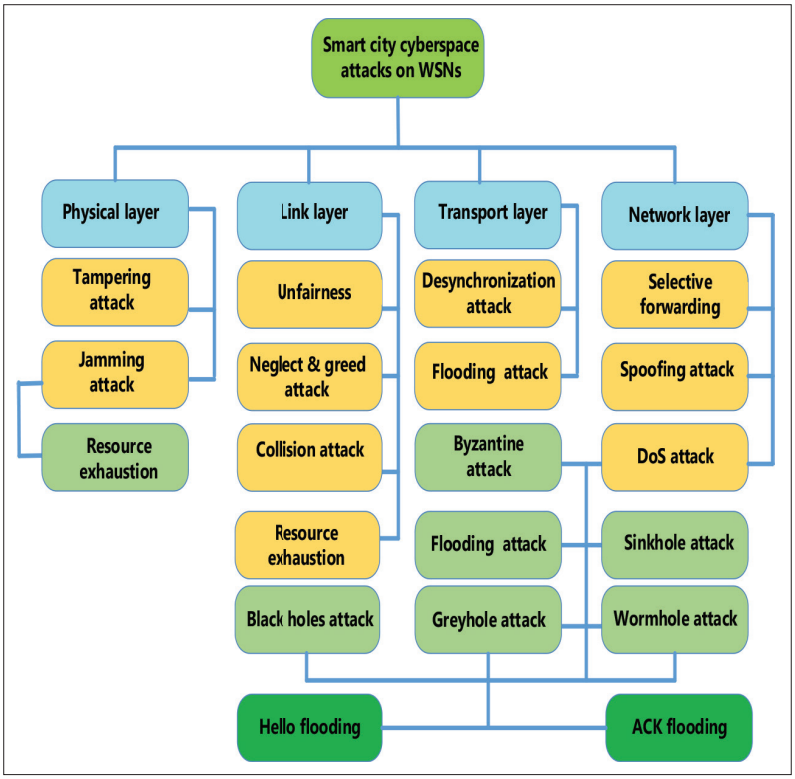

FIGURE 5. Taxonomy of WSNs' vulnerabilities, and attacks.

utilizes the connection layer for nothing). Moreover, the transport layer is vulnerable to various flooding attacks and de-synchronization attacks during high congestion periods. Figure 5 shows a detailed WSNs' taxonomy of attacks.

Requirements and Key Enablers for Smart City Security

Next, we discuss important security concerns and requirements that must be addressed before building and implementing a secure smart city environment.

Key elements and components of a smart city (i.e., dynamic spectrum, diverse communication, heterogeneous environment and the IoT ecosystem) can potentially be targeted with various threats and attacks. Neglecting the security of any potential element comprising the smart city environment can simply throw the entire smart city into chaos. In the open and prevalent environment of a smart city, we need robust protection solutions for various devices and technologies such as SDR, CR and others from both cyberattacks, physical attacks and their corresponding threats [8]. For instance, to ensure the availability of the SDR, the underlying operating system must be designed with features that do not allow backdoor accounts and patches with vulnerable open ports and services. To protect diverse smart city large-scale interactions, secure end-to-end communications must be ensured. Additionally, many SDR agents can be programmed in ways that make them vulnerable to attacks by skilled adversaries. Subsequently, every programmable device and Application Programming Interface (API) can be a potential target. Moreover, threat isolation, mitigation and identity management schemes must be ensured for key elements of a smart city such as SDR/CR and their corresponding agents. Table 1 presents the potential security threats which affect the corresponding functionalities along with security requirements and protection mechanisms. It is worth pointing out that the identified potential security threats, security requirements, and protection mechanisms are applicable to any essential element which has similar behavior and functionality.

Harnessing 5G Capabilities for Future Smart Cities

This section discusses open issues and challenges that need to be addressed to harness the full potential of 5G capabilities for future smart cities. We focus on 5G capabilities because it is an integral and indispensable part of future smart cities. Figure 6 depicts open issues and challenges associated with harnessing 5G capabilities for smart cities.

Reliability and Resiliency

The cyberspace of a future smart city constitutes a highly dynamic heterogeneous environment with diverse emerging ICT solutions to provide cybersecurity. The diverse information and heterogeneous communication security solutions which exist in the smart city environment is a major challenge. In particular, the heterogeneous environment of a smart city may face two types of serious conflicts, namely, inter-federated conformation and configuration conflicts. Additionally, the dynamic topology of the underlying communication networks due to high and random mobility of users and entities such as vehicles, and so on, may cause serious delay and performance issues that could ultimately affect the uninterrupted monitoring and security. Moreover, mobility and the large amounts of data produced make privacy and reliability even more challenging [13].

The intrinsic dynamic nature of wireless IoT ecosystems requires guaranteed system operation and availability even in harsh conditions. Apart from the efforts made to provide a capillary network coverage (enabled by multi-tier cellular architectures), an unexpected lack of infrastructure support caused by network node failures, wireless link issues and unavoidable congestion must be handled. These situations must not affect the proper functioning of IoT based services which typically rely on interoperation and cooperation among devices, especially in critical scenarios such as eHealth, e-energy management, transportation systems, and emergency management [1]. Hence, there must be an efficient recovery mechanism to identify and automatically address erroneous operations in 5G communication networks.

Standardization

The future smart city can properly respond and manage unexpected events and complex problems related to the programmability aspects of emerging ICT solutions. The increase in the digital landscape of a future smart city, and high prevalence of DDoS, malware, DoS, sophisticated phishing, spam and overhearing of active and passive attacks, will disrupt future smart city oper-

Potential security threats	Functionalities affected	Security requirements	Protection mechanisms
Operating system alteration	Application management	System integrity protection	Trusted computing
Channel jamming	Spectrum sharing, spectrum sensing	System integrity protection, robustness	Trusted computing
Software framework alteration	Application management	System integrity protection	Trusted computing
Masquerading primary user	Spectrum mobility, spectrum sharing	Identities verification, accountability	Deployment of secure administration module
Cognitive radio node failure	Spectrum mobility, spectrum sharing	System integrity protection, robustness	High assurance
Software failure	All functionalities	System integrity protection, robustness	High assurance
Hardware failure	All functionalities	System integrity protection, robustness	High assurance
Configuration data alteration	Resource management, application management.	Data integrity protection	Ensuring data integrity
Data extraction configuration	Data management	Protecting confidentiality	Assurance of data integrity
Unauthorized access	Entire functions	Verifying identities, integrity of system assurance	Deployment of secure administration
Eavesdropping	Spectrum sharing, spectrum sensing	Confidentiality protection	Data management
Saturation of cognitive control channel	Spectrum sharing, spectrum sensing	System integrity protection, robustness	High assurance
Unauthorized selfish use of spectrum bands	Spectrum sharing	Compliance	High assurance

TABLE 1. Potential security threats affecting corresponding functionalities with security requirements and protection mechanisms.

ations. The lack of standardization of emerging ICT solutions, particularly IoT technologies, and the prevalent open development environments of future smart cities make immense opportunities available to skilled adversaries who could launch severe attacks against various potential targets [4]. The 5G standardization process is in progress led by international bodies such as the 3rd Generation Partnership Project (3GPP) and the International Telecommunication Union (ITU). Consequently, 5G based large-scale commercial services are likely to emerge in the 2020s. However, pre-standard small-scale services have already been rolled out in 2019. Tremendous efforts are required to develop effective and proficient 5G communication network standards to be compatible with existing and upcoming technologies, many of which are vital in the development of smart cities [14].

Energy Efficiency

Energy efficiency during its harvesting, conservation, and consumption phases is one of the major issues characterizing the wireless ecosystem in future smart cities [15]. Achieving high-energy efficiency in communications is crucial to 5G communication networks. In this context, energy-efficient networking solutions are being investigated and introduced to address the stringent battery constraints of various sensors and actuators. Consequently, a Green 5G wireless communication network remains a major issue for future smart cities.

Scalability

Future smart cities comprise billions of interconnected smart devices [2]. Existing wireless networks could especially suffer from dynamic crowded IoT scenarios, where massive Machine-Type Communications (MTCs) need to be handled while providing and maintaining the required QoS. This aspect is particularly common in wireless telecommunication networks that deal with both MTCs and human-oriented communications in the same environment. 5G based IoT systems face the challenge of fully supporting MTCs. Hence, scalability is another challenge in the design and implementation of 5G enabled smart city solutions.

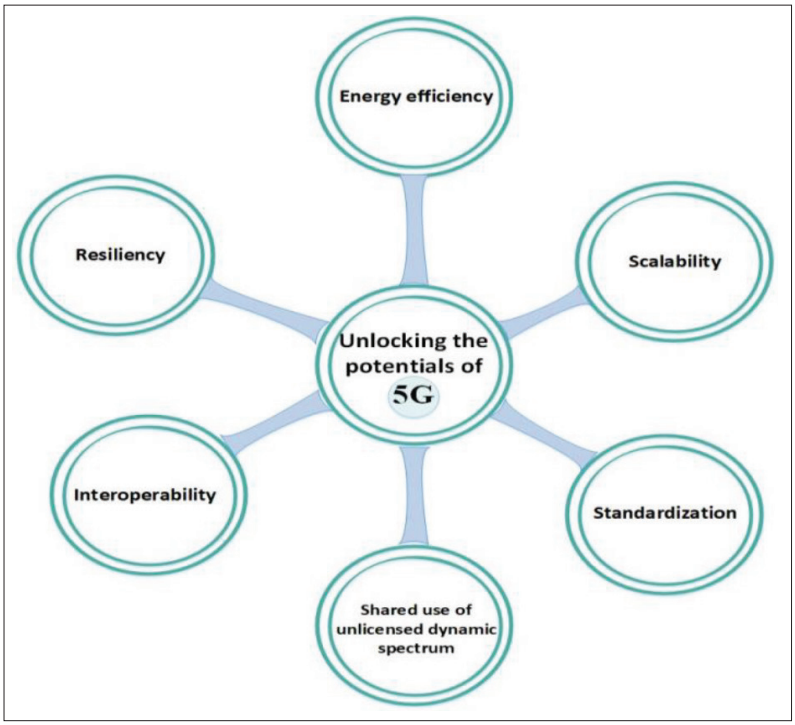

FIGURE 6. Harnessing 5G capabilities.

Interoperability

The smart city environment consists of a highly heterogeneous set of IoT objects, each one with its own specific hardware and software requirements and capabilities. One of the greatest chal-

lenges in such scenarios is to efficiently manage this intrinsic heterogeneity for providing transparent solutions to integrate various IoT devices, services and technologies in a forthcoming 5G and 6G communication network. Moreover, IoT heterogeneity should be able to efficiently manage the plethora of wireless technologies to support energy-constrained IoT devices [9]. However, to support a wide range of IoT application scenarios, 5G communication networks need efficient mechanisms to effectively support heterogeneous data handling capabilities and manage different radio technologies and integrated mobility management schemes.

Shared Use of Unlicensed Dynamic Spectrum

A promising solution to address the scarcity of the spectrum is to increase the utilization of available radio frequency bands by employing dynamic spectrum sharing in future smart cities [9]. The shared use of unlicensed frequency bands allows transmissions by anyone without any license. One approach for increasing the underlying transmission capacity for the required data traffic is to exploit the additional radio frequency bands and guarantee the access to unlicensed and licensed spectrum as much as possible. Therefore, 5G communication network researchers need to conduct more research on the development of effective spectrum management techniques.

Conclusion

Future smart cities are imposing new requirements of cybersecurity because of the newly deployed underlying infrastructural entities and architectural components that are part of them. IoT is a layered architecture where security implications pertaining to any layer can affect other layers and are heavily dependent on each other. To address the security issues, we have presented a systematic layered approach of key IoT enabling technologies which pave the way toward the development of secure future smart cities. We have presented thematic layered based taxonomies of attacks at each layer of a future smart city. We have also highlighted key requirements and enablers to secure future smart cities. Consequently, we discussed open research issues that need to be addressed in the future to harness 5G capabilities as 5G technologies are adopted by future smart cities. Finally, we argue that the critical areas at each layer of various wireless access technologies together with 5G and the emerging 6G must be further investigated to address the security needs of fast-growing smart cities and improve the quality of life.

References

[1] S. Musa, "Smart Cities — A Road Map for Development," *IEEE Potentials*, vol. 37, no. 2, Mar.-Apr. 2018, pp. 19–23.

[2] J. Santos *et al.*, "City of Things: Enabling Resource Provisioning in Smart Cities," *IEEE Commun. Mag.*, vol. 56, no. 7, July 2018, pp. 177–83.

[3] T. Taleb, I. Afolabi, and M. Bagaa, "Orchestrating 5G Network Slices to Support Industrial Internet and to Shape Next-Generation Smart Factories," *IEEE Network*, vol. 33, no. 4, July/Aug. 2019, pp. 146–54.

[4] A. Akhunzada *et al.*, "Securing Software Defined Networks: Taxonomy, Requirements, and Open Issues," *IEEE Commun. Mag.*, vol. 53, no. 4, Apr. 2015, pp. 36–44.

[5] F. Reynaud *et al.*, "Attacks Against Network Functions Virtualization and Software-Defined Networking: State-of-the-Art," *Proc. 2016 IEEE NetSoft Conf. Workshops (NetSoft)*, Seoul, June 2016, pp. 471–76.

[6] M. Andreas *et al.*, "Climate Change as Driver for Ecosystem Services Risk and Opportunities," *Atlas of Ecosystem Services*, Springer, Cham, 2019, pp. 173–78.

[7] M. Eremia, L. Toma, and M. Sanduleac. "The Smart City Concept in the 21st Century," *Procedia Engineering*, vol. 181, 2017, pp. 12–19.

[8] G. Baldini *et al.*, "Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and a Way Ahead," *IEEE Commun. Surveys & Tutorials*, vol. 14, no. 2, 2nd Qtr. 2012, pp. 355–79.

[9] A. A. Khan, M. H. Rehmani, and A. Rachedi, "Cognitive-Radio-Based Internet of Things: Applications, Architectures, Spectrum Related Functionalities, and Future Research Directions," *IEEE Wireless Commun.*, vol. 24, no. 3, June 2017, pp. 17–25.

[10] A. Akhunzada and M. K. Khan, "Toward Secure Software Defined Vehicular Networks: Taxonomy, Requirements, and Open Issues," *IEEE Commun. Mag.*, vol. 55, no. 7, July 2017, pp. 110–18.

[11] K. Fan *et al.*, "A Lightweight Authentication Scheme for Cloud-Based RFID Healthcare Systems," *IEEE Network*, vol. 33, no. 2, Mar./Apr. 2019, pp. 44–49.

[12] Y. Qu *et al.*, "Privacy of Things: Emerging Challenges and Opportunities in Wireless Internet of Things," *IEEE Wireless Commun.*, vol. 25, no. 6, Dec. 2018, pp. 91–97.

[13] M. Kountouris *et al.*, "Guest Editorial: Ultra-Reliable Low-Latency Communications in Wireless Networks," *IEEE JSAC*, vol. 37, no. 4, Apr. 2019, pp. 701–04.

[14] A. Al-Dulaimi, X. Wang, and C. L. I, "Standardization: The Road to 5G," *5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management*, Hoboken, NJ, USA: Wiley-IEEE Press, 2018, pp. 691–708.

[15] Y. Liu *et al.*, "Intelligent Edge Computing for IoT-Based Energy Management in Smart Cities," *IEEE Network*, vol. 33, no. 2, Mar./Apr. 2019, pp. 111–17.

Biographies

Adnan Akhunzada is an enthusiastic and dedicated professional with 12 years of R&D experience both in the ICT industry and academia, with a demonstrated history and a proven track record of high impact published research (i.e., patents, journals, transactions, commercial products, book chapters, reputable magazines, conferences and conference proceedings). His experience as an educator and researcher is diverse. It includes work as a lecturer, a senior lecturer, a tutor, occasional lecturer at other engineering departments, as an assistant professor at COMSATS University Islamabad (CUI), senior researcher at RISE SICs Vasteras AB, Sweden, as a research fellow and scientific lead at DTU Compute, The Technical University of Denmark (DTU), a visiting professor mentoring graduate students, and supervision of academic and R&D projects both at UG and PG level. He has also been involved in international accreditation such as with the Accreditation Board for Engineering and Technology (ABET), and curriculum development according to the guidelines of ACM/IEEE. He is currently involved in various EU and Swedish funded projects focused on cyber security. His main research capabilities and interest lies in the field of cyber security, machine learning, deep learning, reinforcement learning, artificial intelligence, Blockchain and data mining, information systems, large scale distributed systems (i.e., edge, fog, and cloud, SDNs), IoT, Industry 4.0, and Internet of Everything (IoE)). He is a member of the technical program committee of varied reputable conferences and editorial boards. He is presently serving as an associate editor of *IEEE Access*.

Saif ul Islam received his Ph.D. in computer science at the University Toulouse III Paul Sabatier, France in 2015. He is an assistant professor in the Department of Computer Science, KICSIT, Institute of Space Technology (IST), Islamabad, Pakistan. Previously, he served as an assistant professor for three years at COMSATS University, Islamabad, Pakistan. He has been part of European Union-funded research projects during his Ph.D. He was a focal person of a research team at COMSATS working on the O2 project in collaboration with CERN Switzerland. His research interests include resource and energy management in large-scale distributed systems (edge/fog, cloud, content distribution network (CDN)) and the Internet of Things (IoT).

Sherali Zeadally earned his bachelor's degree in computer science from the University of Cambridge, England. He also received a doctoral degree in computer science from the University of Buckingham, England. He is currently an associate professor in the College of Communication and Information, University of Kentucky. His research interests include cybersecurity, privacy, Internet of Things, computer networks, and energy-efficient networking. He is a Fellow of the British Computer Society and the Institution of Engineering Technology, England.