Regular Paper

Communications of the CCISA
Vol. 29 No. 3 Aug. 2023

An Overview of 5G Technology Evolution with Cases on Drone, Smart Healthcare and Smart City

Rai Manu[1], Chit-Jie Chew[2], Ying-Chin Chen[3], Yun-Yi Fan[4], and Jung-San Lee[5]*
Department of Information Engineering and Computer Science, Feng-Chia University, Taichung, 40724, Taiwan
[1]rai.manu013@gmail.com, [2]ycchen.blythe@gmail.com, [3]p0933160@o365.fcu.edu.tw, [4]p1171237@o365.fcu.edu.tw, [5]leejs@fcu.edu.tw

Abstract

Since its inception in the late 1970s, the evolution of mobile wireless communication technology has exerted a profound influence on diverse industries, enterprises, and the quotidian lives of average consumers. The progression from 1G to 4G has witnessed remarkable technological leaps. With the maturation of 4G and the advent of 5G, our global landscape stands on the precipice of an era characterized by ceaseless and ubiquitous communication that interlinks virtually every conceivable device, thereby revolutionizing myriad facets of commerce and individual livelihoods. This article provides an exhaustive overview of the evolutionary trajectory of 5G technology, elucidating the developments in the domain, and elucidates three quintessential 5G applications: unmanned aerial vehicles (UAVs), intelligent healthcare systems, and smart urban environments. Each application is meticulously examined, thereby spotlighting potential security apprehensions that are intertwined with them. Additionally, we proffer strategic approaches for the amelioration of vulnerabilities in each scenario, offering invaluable insights for prospective research endeavors. In particular, future research endeavors ought to grapple with the escalating surge in cybercrimes, exemplified by burgeoning attack surfaces consequent to the burgeoning multitude of Internet-connected devices within the ambit of 5G wireless technology.

Keywords: 5G, drone, smart healthcare, smart city, cybersecurity

1. Introduction

The advent of 5G technology holds the promise of not only enhancing the convenience of living in the wireless communication realm, but also catalyzing global economic growth and revolutionizing the human experience. This innovative leap in wireless communication has engendered a ubiquitous tapestry of connections, ranging from device-to-device, device-to-cloud, and even encompassing human-device interactions, that has profoundly permeated every facet of businesses and lives. Since the emergence of mobile wireless technology in the late 1970s, research in this domain has steadfastly pursued the augmentation of both speed and robustness within wireless networks. However, the advent and implications of transformative technologies such as autonomous vehicles, smart cities, smart healthcare, and unmanned aerial vehicles, commonly known as drones, have stretched the capabilities of prevailing wireless networks to their limits [1]. Consequently, 5G wireless technology emerges as an imminent solution poised to satiate the burgeoning demand for ultra-low latency, unparalleled reliability, and rapid upload and download speeds, attributes essential for facilitating seamless interactions between users' devices and the vast expanse of the Internet, as well as among the intricate ecosystem of the Internet of Things (IoT). A distinguishing facet of the 5G architecture resides in its utilization of higher frequency spectrums in comparison to its precursors, thereby bolstering antenna performance and capacity. This paradigm shift yields a gamut of benefits encompassing flawless network roaming, the seamless integration of a prodigious multitude of devices, minimized power consumption, and an augmented battery lifespan for devices such as smartwatches, alongside a plethora of yet-to-be-explored advantages [2].

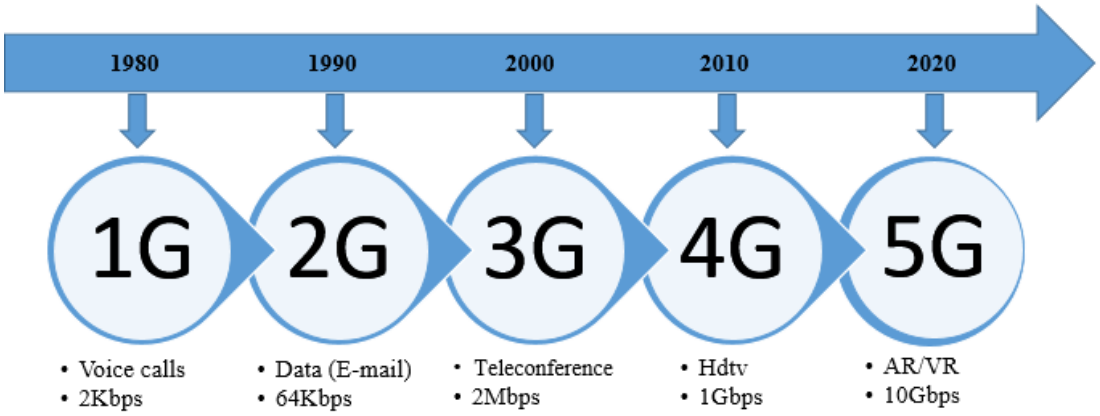

Fig. 1 Block diagram of mobile wireless communication evolution

Tracing back the history of cellular wireless communication, this technology has undergone transformations over the past decades, evolving from the initial 1st generation (1G) to the present early stages of 5G. The block diagram in Figure 1 above illustrates the

progression of mobile wireless communication. The diagram vividly demonstrates that nearly every decade witnessed the emergence of a new cellular technology generation. Furthermore, it is evident that these new innovations have consistently advanced in tandem with increasing data rates, leading to their adaptations across various usage scenarios. For example, consumers shifted from telephonic voice calls in the 1980s to teleconferencing and video calls in the 2000s. In the current 5G era, their preferences have extended to encompass the immersive realms of Augmented Reality (AR) and Virtual Reality (VR).

Since the emergence of wireless cellular communication in the late 1970s, voice communication became feasible during the analog era, often referred to as 1G. Nonetheless, this initial voice communication was fraught with unreliability, confined to short distances, and operated at low frequencies. Subsequently, the 1990s ushered in 2G, accompanied by digital technology, which introduced swifter data transfer speeds and marked the advent of short message services. As user demands surged, the 2000s witnessed the advent of 3G, incorporating wideband networks that bolstered its prowess in data-intensive services like video calls. Responding to the insatiable appetite for higher frequency capabilities, the 2010s introduced 4G, which substantially enhanced data rates, enabling the delivery of advanced services such as high-definition television channels and digital video broadcasting. Akin to this evolutionary trajectory, the growing appetite for artificial intelligence (AI) in augmented AR/VR and other multimedia applications catalyzed the deployment of 5G technology since 2019. As of now, 5G is in its preliminary rollout phase, designed to coexist with 4G LTE-A until it becomes an autonomous entity, fully unfurling its potential in the years to come. With an ambitious aspiration to operate at high bandwidths, offering data rates ranging from 10 to 50 Gbps, 5G is poised to revolutionize businesses, industries, and the broader public lifestyle due to its exceptional data transfer speeds, ultra-low latency, and unmatched reliability [1][2].

Together with the commonness of 5G, the 3rd Generation Partnership Project (3GPP) comprising seven standards organizations was established in 1998 in order to develop protocols and specifications for mobile telecommunications. Within 3GPP's purview, the deployment phases for 5G have been underscored in Release 15 and onwards, aligning with the prerequisites for the International Mobile Telecommunications - 2020 (IMT-2020) 5G system. The ongoing deployment of 3GPP's 5G Phase 1 leverages existing 4G infrastructure, known as the enhanced Mobile Broadband (eMBB), which confers high data rates in gigabytes per second. The culmination of 3GPP Phase 2 is anticipated to materialize when it seamlessly attains independence. This evolved 5G infrastructure is envisaged to encompass the realm of massive Machine Type Communications (mMTC), catering to IoT devices, and Ultra-reliable and Low Latency Communications (URLLC), catering to mission-critical applications within the domain of smart healthcare systems. Furthermore, 3GPP's dedication to 5G security is evident, outlining

specific security mechanisms to be implemented in both Non-standalone (NSA) mode, which amalgamates the existing 4G LTE radio infrastructure with the 5G New Radio (NR), and Standalone (SA) mode within the 5G NR radio infrastructure [3][4].

A seminal contribution to 5G security originates from a white paper authored by Bertino and Hussain, published by the Computing Community Consortium (CCC). This comprehensive work delves into a spectrum of technologies to be assimilated within the 5G infrastructure, encompassing millimeter waves (mmWaves), small cells, massive MIMO, beamforming, full duplex, and software-defined networks in conjunction with network functions virtualization. Additionally, the paper delves into the examination of protocols like LTEInspector in 4G and 5GReasoner in 5G, both aimed at enhancing security and privacy in cellular networks. The authors underscore countermeasures against common threats within base stations, side-channel vulnerabilities, identity exposure, and emergency alert systems. Furthermore, the paper illuminates the trajectory of future research directions pertaining to security solutions for 5G cellular networks [5].

Indeed, security concerns within cellular communication are far from novel; instead, they have evolved in tandem with the progression of infrastructure across successive generations, from the first generation onwards. The escalating complexity of cellular wireless communication's architecture has exposed vulnerabilities within its fabric, particularly within its constituent elements: the radio access network (RAN) and the core network (CN). Comparatively, wireless communication networks exhibit lower inherent security, rendering them susceptible to a myriad of potential attacks. Consequently, beginning from the 3G era, augmented security measures have been seamlessly woven into the architecture, encompassing network access security, network domain security, user domain security, application security, and the enhancement of visibility and security configuration.

The limitations inherent within cellular networks vis-à-vis security vulnerabilities have piqued the attention of numerous researchers. To illustrate, Gardezi has advanced security solutions, propounding protocols that govern and fortify cellular networks and WLAN communications against well-known cyber threats [6]. Similarly, in 2018, a white paper report by the worldwide mobile phone network Orange CEO identified and categorized seven primary threat vectors targeting mobile telecommunications networks while concurrently proposing countermeasures. Among the panoply of threats, safeguarding users' privacy and data has emerged as a paramount concern, given that sensitive information is increasingly disseminated across the vast expanse of the Internet and prominent social media platforms such as Facebook, Twitter, and Instagram. In light of this, the implementation of robust control measures and regulatory frameworks has become imperative to preserve privacy and data integrity [7].

With the ascendancy of 5G wireless communication technology as the quintessential

enabler across multifarious use cases, concerns relating to its security and privacy must be brought to the forefront. In consonance with this imperative, our discourse herein delves into three distinct use case scenarios empowered by 5G technology: the drone-based network system, the smart healthcare system, and the smart cities network system. Within this framework, we proffer salient solutions engineered to thwart the envisioned array of attacks. These solutions are meticulously crafted to engender the assurance of wireless network communications in diverse configurations, encompassing device-to-device, device-to-cloud, and human-device connections.

The subsequent sections of this paper are meticulously structured as follows: Section 2 introduces the preliminary foundations. In Section 3, we expound upon the proposed solutions tailored to the aforementioned scenarios, followed by a comprehensive threat analysis of these use cases in Section 4. Ultimately, our deliberations culminate in the conclusions presented in Section 5.

2. Related Work

The 5G wireless network use cases for drones, smart healthcare, and smart city are discussed. Possible attack types for each case are also mentioned in subsections 2.1, 2.2, and 2.3.

2.1 Drones

The utilization of drones has gained global prominence owing to its multifaceted applications since its inception in the early 1900s. Leveraging existing cellular wireless communication systems, drones have found manifold applications, encompassing fire monitoring, flood monitoring, border patrol, search and rescue operations, and recreational pursuits. As the realm of 5G technology and beyond unfolds, industries, businesses, and ordinary consumers are increasingly seeking the capabilities of drones. This growing interest has spurred researchers to explore the integration of drones into 5G wireless communication systems, scrutinizing their potential domains of application. Notably, the integration of Unmanned Aerial Vehicles (UAVs) or drone-based integrated networks within the space-air-ground framework to bolster communication has been under scrutiny, with these networks envisaged to facilitate inter-device connections, device-to-people interactions, and cloud-based technologies.

However, the employment of UAV-based cellular networks introduces tangible physical

risks and cybersecurity vulnerabilities, necessitating the meticulous consideration of countermeasures during attack mitigation. Consequently, numerous researchers have underscored the gamut of potential attacks that could imperil drones both physically and through cyber assaults. Ultimately, the drone is poised to assume a pivotal role in a plethora of applications within the landscape of 5G wireless communication technology [8][9]. Nevertheless, the surge in its popularity concurrently exacerbates the specter of physical and cyber threats.

2.1.1An attack scenario of drone-based 5G wireless network

In the realm of drone-based 5G wireless networks, adversaries could exploit vulnerabilities within the communication network connecting an autonomous vehicle via a drone to a small base station (SBS). In this scenario, the adversary could launch a distributed denial of service (DDoS) attack, targeting the autonomous car, the SBS, or the communication links. Such an assault could precipitate loss-of-control car crashes, thereby instigating potentially catastrophic casualties, particularly alarming when the car is operating at high speeds in real-time conditions. Figure 2 illustrates the mechanics of a DDoS attack within a drone-based 5G wireless network.

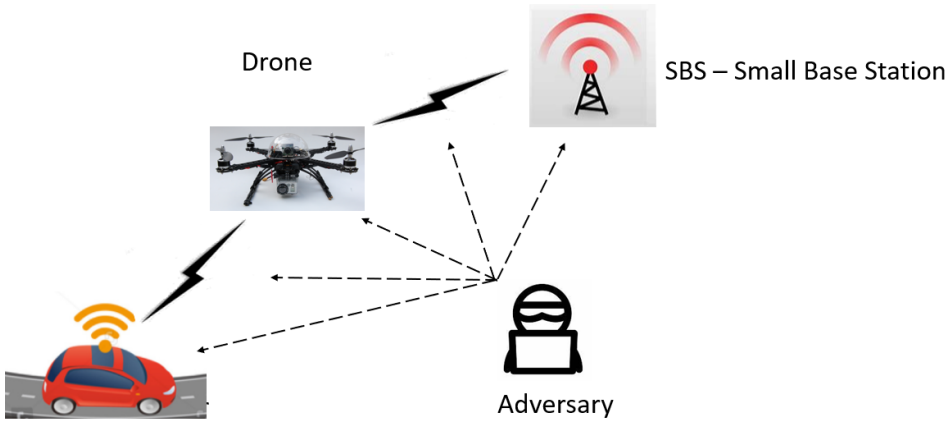

Fig. 2 DDoS attack in a drone-based 5G wireless network

DDoS attacks are a form of cyber onslaught aimed at inundating websites and online services with a deluge of Internet traffic, rendering them incapacitated and inaccessible. Hackers have long wielded DDoS attacks as a potent tool, and their prevalence remains persistent. The escalating growth of Internet-connected devices, predominantly within the Internet of Things (IoT) landscape, renders them prime targets for adversaries. Notably, IoT devices are frequently co-opted as integral components of botnets, facilitating the successful execution of DDoS attacks.

2.2 Smart Healthcare

The field of healthcare, having evolved over centuries, is currently undergoing rapid transformations. The prevailing cellular wireless communication networks, such as 3G and 4G LTE, coupled with heterogeneous networks like Bluetooth, Wi-Fi, and Wi-Max, have endowed healthcare with enhanced intelligence. In contemporary times, smart healthcare applications manifest in diverse manifestations. Notably, within domains like telemedicine and Body Area Networks (BAN), sensors embedded within wearable devices capture crucial data, ranging from heart rate and blood sugar levels to tracking behavioral shifts in the elderly population.

The advent of the 5G era, bolstered by the Internet of Things (IoT), propels smart healthcare into unprecedented dimensions by virtue of its ability to seamlessly connect an extensive array of devices. The dissemination of data across global hospitals, healthcare practitioners, and patients engenders outcomes characterized by elevated throughput and energy efficiency. Consequently, a burgeoning demand surfaces for smart healthcare systems capable of perpetually collecting and processing data in real-time, around the clock, all year long. Thus, the impediments faced by 3G and 4G technologies find resolution through 5G, poised to meet the exacting requisites of smart healthcare. This new paradigm of 5G offers augmented data rates, prolific connectivity, dense deployment, heightened reliability, minimal latency, exceptional energy efficiency, and expansive short- and long-range communication coverage, encompassing steadfast support for IoT-driven smart healthcare initiatives [10].

Beyond the acceleration of remote medical support facilitated by 5G technology, grave concerns arise within the ambit of security and privacy across global healthcare systems. Notably, as healthcare facilities transition to electronic or cloud-based medical records, the personal data of patients, including birthdates, addresses, social security numbers, and credit card information, lurk as tantalizing targets for cyber adversaries seeking data theft. Furthermore, the specter of mass connectivity looms large. Precisely, the advent of 5G wireless communication technology portends mass connectivity, underpinning the optimization of smart healthcare systems to enable feats such as remote surgery and peer support among physicians. However, the proliferation of connected devices within heterogeneous or cloud-based networks engenders a corresponding augmentation in potential attack surfaces. These vexing quandaries remain unresolved challenges necessitating meticulous exploration in forthcoming research endeavors [10][11].

2.2.1 An attack scenario of smart healthcare in 5G wireless network

With 5G network, smart healthcare system can adopt Device-to-Device (D2D) link to

monitor a patient's blood sugar level via electronic health record (EHR) application. In this scenario, the adversary can attack the devices such the smart watch, the smart phone, the base station, or the communication links between them through the Man-in-The-Middle (MiTM) attack as shown in Figure 3.

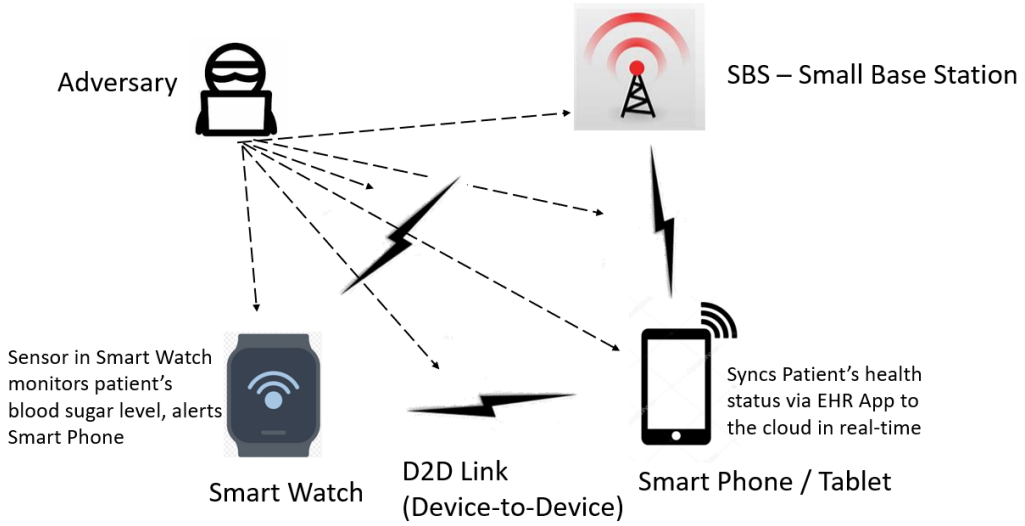

Fig. 3 Man-in-the-middle attack in smart healthcare system in 5G wireless network

The MiTM attack is a cyber-attack that allows attackers to secretly impede communications between two parties either to passively listen or modify traffic transmission between them. The aim of MiTM attack might be to steal login credentials or personal information, spy out the victim or corrupt the transmitted data or information between the two parties by taking advantage of an unsecured or misconfigured network or device.

2.3 Smart Cities

A pivotal milestone in the trajectory of wireless network evolution is the emergence of smart urban centers, often referred to as smart cities, engendering transformative shifts across diverse facets of urban life. Presently, numerous global metropolises have embraced the smart city paradigm, harnessing the capabilities of contemporary wireless communication technologies, most notably, 4G LTE. According to research projections [12], it is anticipated that by 2030, over half of the world's population will be concentrated within urban locales. Consequently, a burgeoning challenge looms, necessitating collaborative endeavors by city administrators and corporate leaders, to devise solutions addressing urban quandaries encompassing traffic congestion, pollution, resource scarcity, public healthcare, and communal safety. Notwithstanding the notable strides catalyzed by current 4G LTE in fostering urban development, these achievements have yet to fully satiate the soaring expectations of industries,

governmental entities, and inhabitants. This is attributed to the constricted bandwidth capacity of the frequency spectrum in which 4G LTE operates, impeding the transmission of copious data. The imperative to deliver more data is at the forefront. In this context, 5G wireless technology is poised to abrogate these constraints on prevailing urban infrastructures, culminating in the realization of smart city attributes encompassing intelligent traffic management, home automation, smart healthcare, and seamless public communication [8].

However, to unlock the full potential of smart cities underpinned by 5G as the underpinning technology, stringent security measures must be accorded paramount importance right from the outset. Notably, an anticipation of prospective physical and cyber assaults is imperative, necessitating the implementation, validation, and accessibility of corresponding countermeasure protocols and procedures. This imperative of securing Information and Communication Technology (ICT) infrastructure acquires even greater significance given the current landscape, where malevolent actors persistently seek vulnerabilities within open-source third-party software applications, IoT devices, gateway routers, and network systems to undermine home networks, corporate networks, or urban public transportation systems. Furthermore, the susceptibility of IoT devices prevalent in smart homes, smart healthcare systems, and analogous realms to exploitation presents a palpable threat, rendering the lives of urban residents insecure. Hence, it mandates a synergistic endeavor on the part of city administrators, corporate leaders, and residents alike to collaboratively foster the advancement of safer and smarter urban environments [12][13].

2.3.1An attack scenario of smart city in 5G wireless network

While the amalgamation of smartphones with IoT devices augments the intelligence of homes and cities within the 5G wireless network, it concurrently renders them more susceptible to malicious attacks. In this scenario, a malicious actor could launch an assault on smart home devices, ranging from door locks and refrigerators to smartphones and their communication channels, by wielding hacking toolkits to identify exploitable vulnerabilities. Illustrated in Figure 4 is the portrayal of a hacking toolkit attack targeting smart home devices within a smart

city environment facilitated by the 5G wireless network.

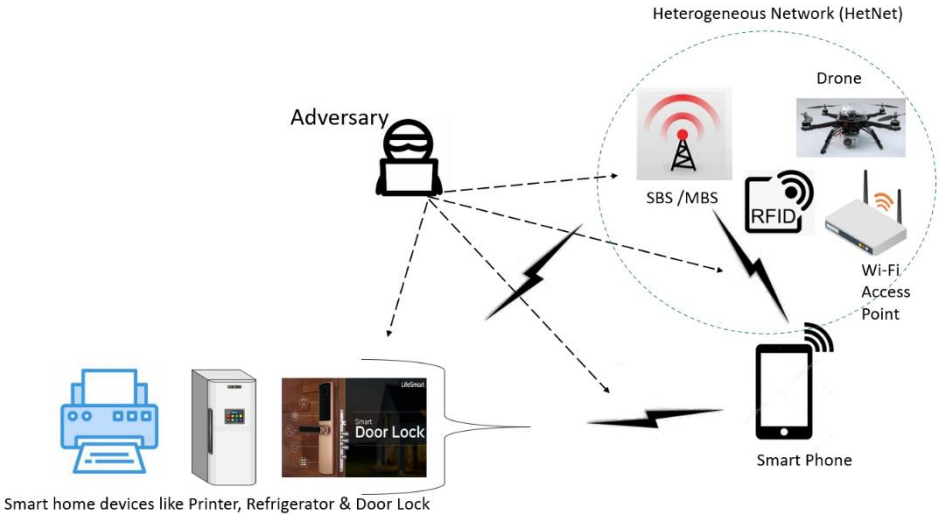

Fig. 4 Hacking toolkits attack in smart homes in a 5G smart city-based network

Hacking toolkits epitomize automated utilities empowering individuals to undertake both ethical and unethical hacking endeavors, unveiling shortcomings and vulnerabilities within computers, smart devices, sensor devices, IoT devices, and network systems. Cyber adversaries and hackers, ever entrenched within the labyrinth of the internet, perpetually engage in malicious incursions targeting networks and their interconnected systems. These transgressions disrupt normal operations, motivated by malevolent intentions such as pilfering personal information or tampering with pivotal clinical data.

3. Proposed Scheme

Threats either through cybercrime or physical tamper is unavoidable in cellular networks. These proposed solutions for the three use case scenarios are categorized into three sections. Firstly, in Section 3.1 we discuss the security protocols they use namely the public key infrastructure (PKI) and extensible authentication protocol – transport layer service (EAP-TLS). Secondly, the endpoint security solutions are discussed in Section 3.2, comprising the firewall, intrusion detection system/intrusion prevention system (IDS/IPS), and surveillance camera. Finally, in Section 3.3 we discuss the safeguard measures for smart devices, IoT devices and software applications used in these use case scenarios to avoid exploitations and attacks.

3.1 The security protocol solutions for the three scenarios in a 5G wireless network

3.1.1 Public key infrastructure (PKI)

The use of PKI is at most the best choice to guarantee a secure and mutual authentication between devices and servers in order to combat known cyber-threats like replay attacks. The PKI enables the establishment of binding relationship at the certificate authority (CA) server end during the time of registration. Thus, issuance of digital certificate is granted to users or nodes by CA with two-key pair of public and private keys, which are known as asymmetric encryption. This process enables a secure and mutual authentication between a device and server by establishing communication links between them. The PKI-based mutual authentication and encryption between two users is shown in Figure 5 below. In this diagram, if Alice decides to send a secret message to Bob, she requests the CA server that she trusts to obtain Bob's certificate, validates that the digital certificate really belongs to Bob with his particulars and public key on it. Alice then encrypts the message with the public key and sends it to Bob. Bob receives Alice's secret message and decrypts the message using his private key and reads it. If Bob wants to reply Alice's message, he has to follow the same procedure as Alice did.

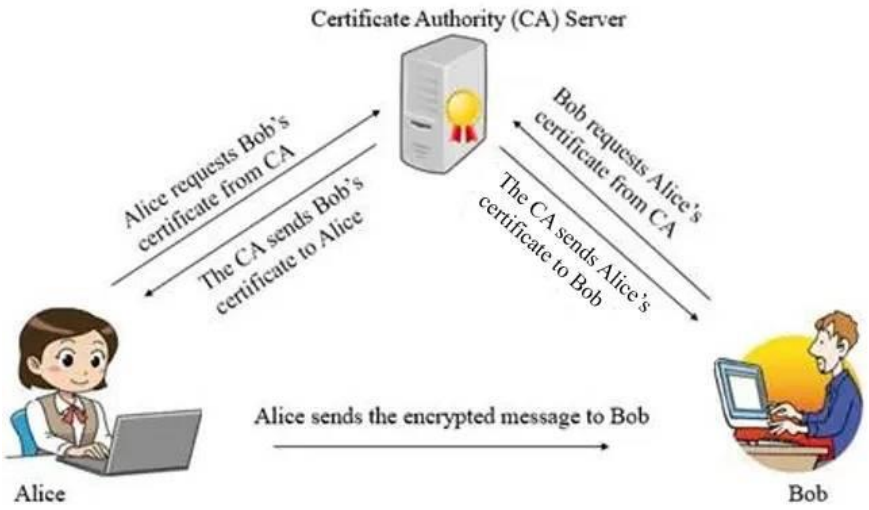

Fig. 5 PKI framework achieves mutual authentication and encryption between users

3.1.2 Extensible authentication protocol - transport layer service (EAP-TLS)

The EAP-TLS is an existing standard wireless local area network (WLAN) protocol that provides for certificate based and mutual authentication between a device and server in a

network, thus maintaining trust between them. Figure 6 illustrates a simplified scenario of EAP-TLS-based mutual authentication and encryption between a client and the server. In this diagram, both server and client must identify and verify each other with their certificates signed by the CA server which they both trust. The information or message is transferred through the authenticator (AP) until a communication link or session is established and they are able to encrypt/decrypt messages between them using the public and private keys stored in the certificates. If man-in-the-middle attack occurs on either the server or the client side, the attacker may have the public key but cannot know the private key they mutually hold, thus the attack seems to be impossible.

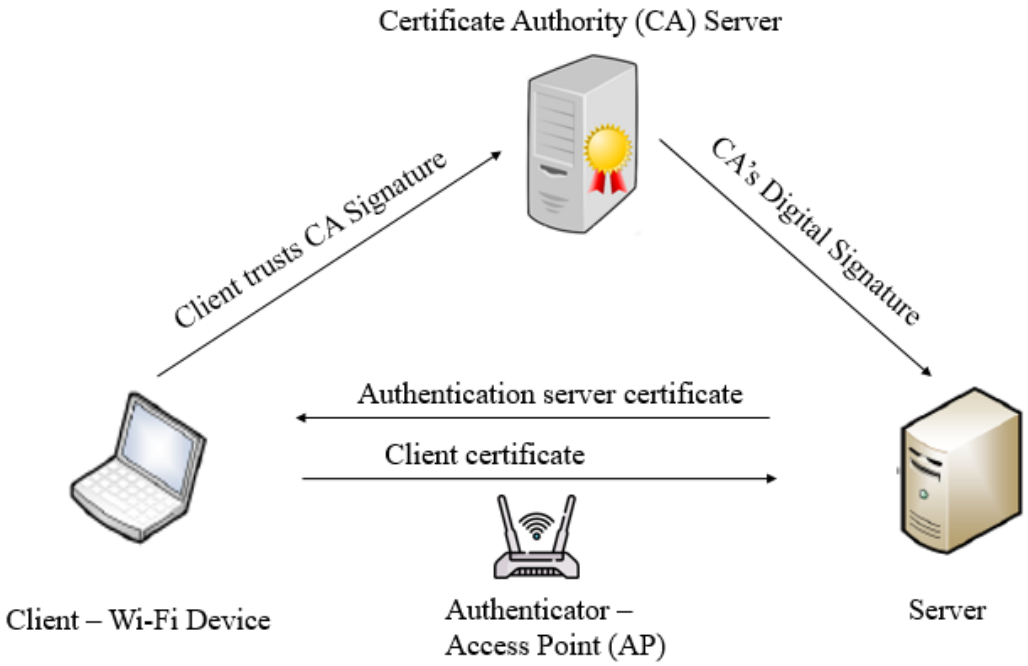

Fig. 6 EAP-TLS' secure mutual authentication and encryption framework between a client and server

3.2 The endpoint security solutions for the three scenarios in a 5G wireless network

3.2.1 Firewall

Another way to safeguard devices in a wireless network is the use of a firewall. Firewalls these days can be in the form of a hardware device or a web application. The firewall filters both the incoming and outgoing network traffic using pre-defined rules based on IP addresses and port numbers. By this mechanism, it can allow any traffic that meets the specific rules or

deny any traffic that does not meet the pre-defined rules.

3.2.2 Intrusion detection system / Intrusion prevention system (IDS/IPS)

An IDS can be a hardware device or software, which is used to monitor network traffic for anomaly activities/violations and provide immediate alerts on detection. Meanwhile, IPS, is a device that responds to a potential threat by attempting to stop it from happening. An IPS can be considered as an active defense compared with an IDS.

3.2.3 Surveillance camera

The use of surveillance camera these days is a good choice to prevent physical tamper or malicious behavior from happening. The deployment of surveillance cameras along the roads, buildings, and traffic light poles enables real-time capturing and monitoring images and videos at the control center. Accordingly, it guarantees fast response time in case there is an attack.

The Figure 7 below shows the holistic synthesis diagram of three scenarios' network systems. They can be independently monitored and be protected from any possible threats upon detection. Specifically, if a hacker from a public network (Internet) tries to invade a private network like a drone-based network system with DDoS, MiTM or hacking toolkit attacks, they are unable to get through the strong defense network system as they will be blocked upon detection.

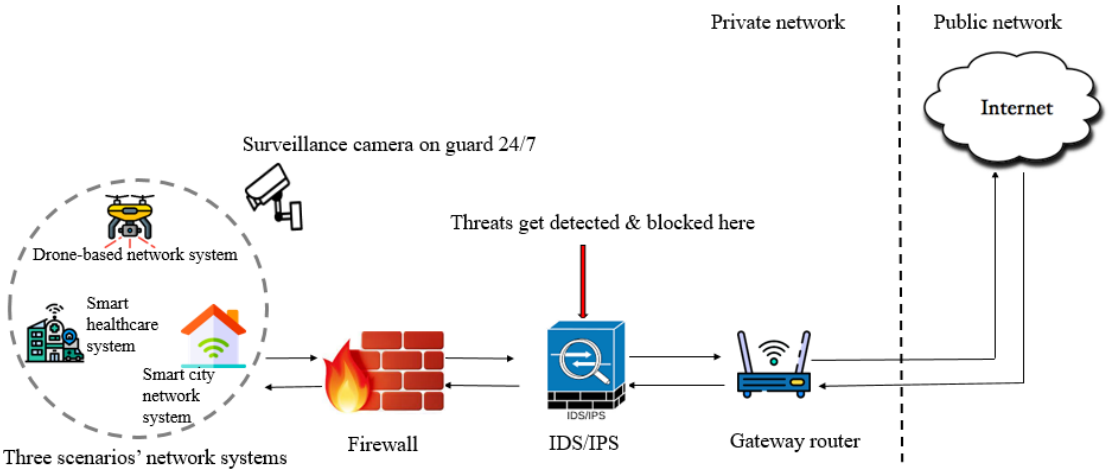

Fig. 7 A secure network system deploying firewall, IDS/IPS system, and surveillance camera solutions

3.3 The safeguard measures for smart devices, IoT device, and software applications for the three use case scenarios

In accordance with the aforementioned scenarios, several safeguard measures for smart devices, IoT devices, and software applications are suggested. Firstly, every firmware of devices needs to be upgraded to the latest version. Secondly, anti-malware should be installed and updated with latest virus definitions. Thirdly, any open ports on devices should be closed. Fourthly, all default manufacturer settings on devices, especially the username and password should be changed frequently. Finally, any legacy applications must be upgraded to latest version and an open third-party software application must be updated. In this way, we make sure that they are protected and less vulnerable to exploitations and attacks by hackers using hacking toolkits or other known malwares.

4. Threat comparison analysis

It is known that threats to cellular wireless networks come in various forms or types, either in cybercrime or physical tamper. They aim to do harm to privacy, data confidentiality, data integrity, authenticity and/or availability. Thus, scholars in the field have identified and discussed the existing threats and vulnerabilities with possible countermeasures for drones, smart healthcare and smart cities[9][11][13]. Some influential works are presented as follows.

Lee et al. attempted to achieve secure mutual authentication and data encryption between a user and an authentication server by using protocols like EAP-TLS adopted in PKI system. The authors recommended the lightweight secure roaming mechanism (LSRM) as a solution. LSRM offer anonymous roaming services that would avoid threats like MiTM attack or replay attack while users roam between cellular networks and WLANs. LSRM can successfully lower computational cost of the mobile device which was burdensome in Tseng's method where the mobile device needs to construct two symmetric en/decryptions and two asymmetric en/decryptions in order to complete roaming. LSRM mechanism is secure because of the Burrows-Abdi-Needham (BAN) authentication logic adoption. The BAN authentication logic is a significant and formal tool used to analyze the accuracy of an authentication procedure. BAN logic enables its users, with or without information exchanged, to be trusted or secured or both against attacks like eavesdropping [14].

Cheng et al. have proposed a scheme for mutual authentication like the smart IC-card-based remote authentication based on Wang et al.'s scheme [15]. This more recent scheme can fix the inability to counteract forgery attack in Wang et al.'s. Specifically, this newly proposed

scheme can protect against possible attacks that try to intercept login request to access the remote server by applying the timestamp mechanism. The security of this scheme adopts the public one-way hash function where it is hard to reverse the process [16].

In short, in 5G communication technology, security and privacy are the top most concerns these days. This is because of the ever-increasing number of Internet-connected devices, and the amount of data shared via 5G. They collectively pose greater threats than in the previous wireless cellular technologies like 2G, 3G or 4G. Accordingly, Section 3 of this paper has provided possible solutions that could mitigate the security concerns in terms of privacy, data integrity, authenticity, and availability, accompanied with some representative studies in the field in Section 4. In brief, to establish a well-protected network, a combination of firewall, IDS/IPS, and surveillance cameras must be collectively deployed. In addition, safeguarding the devices and software applications with regularly updated anti-malware can reduce the risk of attacks.

5. Conclusions

This article presents discussion on 5G wireless communication technology. In brief, 5G affords faster Internet speed with low latency, higher reliability, and larger geographical coverage. As such, it is efficient, cost-effective, and capable of activating multifaceted transformations in both business and human life. As discussed in this paper, there are more security and privacy concerns in 5G technology compared with previous cellular communication technologies as the complexity of 5G infrastructure will expand the attack surface. This necessitates an anticipation by investing in possible attack counter measures to prevent or minimize attack possibilities. The existing threats mentioned and the potential attack scenarios in 5G networks presented in this paper can raise awareness among industries, businesses, city managers, and the general public about security. As such, those involved parties may be better aware of security implementation and management to utilize the benefits of 5G technology-based applications and services, which are foreseen to be norm by 2030.

References

[1] U. B. Shukurillaevich, R. O. Sattorivich, and R. U. Amrillojonovich, “5G Technology Evolution,” 2019 International Conference on Information Science and Communications Technologies, Tashkent, Uzbekistan, 4-6 Nov. 2019.

[2] H. Ullah, N. G. Nair, A. Moore, C. Nugent, P. Muschamp, and M. Cuevas, "5G Communication: An Overview of Vehicle-to-Everything, Drones, and Healthcare Use-Cases," IEEE Access, vol. 7, pp. 37251-37268, Mar. 2019.

[3] 3rd Generation Partnership Project, "About 3GPP," Available Online: https://www.3gpp.org/about-3gpp.

[4] A. R. Prasad, A. Zugenmaier, A. Escott, and M. C. Soveri, "3GPP 5G Security," 3rd Generation Partnership Project, Aug. 2018.

[5] E. Bertino, S. R. Hussain, and O. Chowdhury "5G Security and Privacy: A Research Roadmap," White Paper of Computing Community Consortium, Mar. 2020.

[6] A. I. Gardezi, "Security in Wireless Cellular Networks," Technique Report of Washington University in Saint Louis, Available Online: https://www.cse.wustl.edu/~jain/cse574-06/cellular_security.htm, Apr. 2006.

[7] Groupe Speciale Mobile Association, "Mobile Telecommunications Security Landscape," Available Online:https://www.gsma.com/security/wp-content/uploads/2021/03/id_security_landscape_02_21.pdf, Mar. 2021.

[8] B. Li, Z.S. Fei, and Y. Zhang, "UAV Communications for 5G and Beyond: Recent Advances and Future Trends," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2241-2263, Apr. 2019.

[9] J. P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations," Internet of Things, vol. 11, pp. 1-39, Sep. 2020.

[10] A. Ahad, M. Tahir, and K.L. A. Yau, "5G-based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions," IEEE Access, vol. 7, pp. 100747-100762, Jul. 2019.

[11] H. Alemdar and C. Ersoy, "Wireless Sensor Networks for Healthcare: A survey," Computer Networks, vol. 54, no. 15, pp. 2688-2710, Oct. 2010.

[12] A. Phan and S. T. Qureshi, "5G Impact on Smart Cities," 5G Communications, pp. 1-13, Mar. 2017

[13] Rambus, "Smart Cities: Threat and Countermeasure," Available Online: https://www.rambus.com/iot/smart-cities/

[14] J.S. Lee, P.Y. Lin, and C.C. Chang, "Lightweight Secure Roaming Mechanism between GPRS/UMTS and Wireless LANs," Wireless Personal Communications, vol. 53, no. 4, pp. 569-580, Jun. 2010.

[15] C.T. Wang, C.C. Chang, C.H. Lin, "Using IC cards to remotely login passwords without verification tables," Proceedings of the 18th International Conference on Advanced Information Networking and Applications, Fukuoka, Japan, vol. 1, pp. 321-326, Mar.

2004.

[16] T.F. Cheng, J.S. Lee, and C.H. Chang, “Security Enhancement of an IC-Card-based Remote Login Mechanism,” Computer Networks, vol. 51, no. 9, pp. 2280-2287, Jun. 2007.