6G TECHNOLOGIES SECURITY REQUIREMENTS AND CHALLENGES

Dr.M.SAKTHI ASSOCIATE PROFESSOR, NGM college, Pollachi
R.SRIVIDHYA PG Computer Science, NGM college, Pollachi.
Srividhya0614@gmail.com

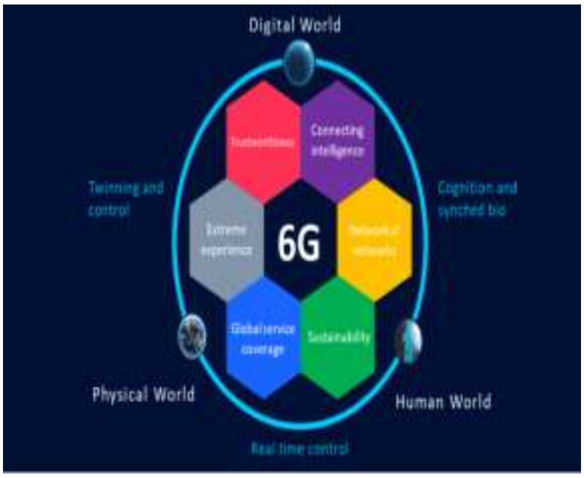
Abstract:

6G is anticipated to be enforced around the time 2030. It'll offer a significant experience for everyone by enabling hyperactive- connectivity between people and everything. In addition, it's anticipated to extend mobile communication possibilities where earlier generations couldn't have developed. These include forthcoming and current technologies similar aspost-quantum cryptography, artificial intelligence(AI), machine literacy(ML), enhanced edge computing, molecular communication, THz, visible light communication(VLC), and distributed tally(DL) technologies similar as blockchain. This paper provides perceptivity into the critical problems and difficulties related to the security, sequestration, and trust issues of 6G networks. also, the standard technologies and security challenges per each technology are clarified. This paper introduces the 6G security armature and advancements over the 5G armature. We also introduce the security issues and challenges of the 6G physical layer.

Keywords: *6G security, privacy, new challenges, security architecture, security threats, physical layer security, AI/ML security*

INTRODUCTION:

Sixth generation(6G) wireless network technology is predicted to offer advanced content, lower energy consumption, comprehensive spectral, and cost- effectiveness with advanced security(1). 6G networks will meet these conditions by planting new technologies analogous as multiple accesses, waveform design, channel rendering schemes, network slicing, numerous antenna technologies, and pall edge computing. 6G affects four significant future changes(2). First, it offers an integrated air – ground – space – ocean communication network by planting terrestrial and non-terrestrial networks(3). Second, new radio bands will meliorate network business capacity and data speed, including millimeter- swell(mm- swell),sub-6 GHz, terahertz(THz), and optical dispatches. Third, 6G will enable a new generation of intelligent operations and services using artificial intelligence(AI) and big data technologies in response to the massive datasets generated by eclectic networks with different communication scripts, wide bandwidths, a advanced number of antennas, and new 6G operations ' conditions(4). Fourth, network security and insulation must be strengthened and enhanced for 6G technologies and operations(5). This paper presents the 6G security trends and challenges of other forthcoming technologies and operations. Data processing, trouble discovery, business analysis, and data encryption are considered the most critical issues in 6G networks. The security issues due to massive business processing can be answered using decentralized security systems, in which the business can be handled roundly and locally. 6G use cases put stricter security conditions than 5G use cases,(6). The Internet of Everything(IoE), with a wide variety of capabilities and services, will make it more challenging to operate and install distributed AI, insulation, and security results. The high mobility conditions of the new connected bias make them change their connected networks and bear services from other networks, performing in security complications and insulation problems. For the Enhanced Ultra- Reliable and Low quiescence Communication(ERLLC) services, the end to end quiescence in 6G should be dropped to a numerous µs. also, 6G will need a ten- time increase in network energy effectiveness over 5G and a hundred- time increase over 4G(7). It's predicted to allow truly low- power transmissions for limited resource bias. Advanced and active operation technologies for high mobility will enable rapid-fire- fire movement at 1000 km per hour. To guarantee the quality of the service for ERLLC, the quiescence effect of security processes will be estimated. also, high conditions need largely effective security results that ensure service and resource vacuity. The IoE provides difficulties in planting and operating the new distributed intelligent AI and ML security ways. A critical element is figuring out how to incorporate new security enablers into resource- constrained bias(8). Figure 1 summarizes the comparison between 5G and 6G in data rates, responsibility, quiescence, and localization delicacy. Figure 1 The 5G and 6G features comparison. A comprehensive check on security and insulation enterprises with 6G networks is stressed in this study. We curtly introduce the security development of the former mobile radio generations(1G to 5G), fastening on the security shortcomings mentioned in being results. The 6G security problems in different critical fields are excavated. also, the study presents the 6G technologies and operations ' security issues and conditions. also, we propose results for the arising 6G operations. This paper considers one of the first studies that includes an extensive check for the 6G new technology security implicit results(9). We epitomize the paper contributions as follows Introducing the security issues in the earlier heritage mobile networks. Presenting the 5G security architecture advancements and their effect on the new architecture of 6G. Presenting the trending 6G technologies and studying the security conditions of each technology. Studying the 6G operations and services conditions. Presenting the 6G operations security problems and proposed results. The rest of this paper is organized as follows. Section 2 shows the security issues and architecture development of heritage mobile networks. Section 3 introduces the 6G network vision and essential disquisition systems. Section 4 introduces the security conditions of the proposed 6G architecture. 6G technologies ' security issues and possible results are presented in Section 5. Section 6 provides future security challenges and problems of 6G operations. The study is concluded in Section 7.



2. Security elaboration of Mobile Cellular Networks

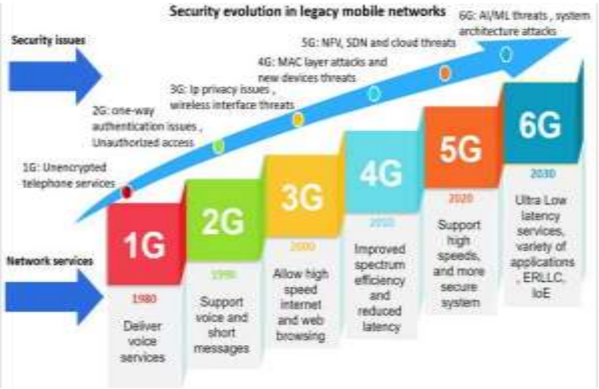
This section discusses different cellular network generations ' security pitfalls and sequestration enterprises. The early mobile generations encountered grueling security enterprises, involving wiretapping attacks, encryption issues, physical attacks, and authentication problems. therefore, the trouble geography has grown with further complex attacks and further competent attackers.

2.1. Security Issues in 1G, 2G, and 3G

In the 1980s, the 1G network was created specifically to deliver voice dispatches services. It uses analog modulation ways to transfer data. This generation has several issues, involving handover problems, no guarantees on security, and numerous transmission enterprises. In addition, due to the unencrypted nature of telephone services, data transmission can not be guaranteed to be secure or private. The 2G authentication fashion is grounded on a challenges and responses approach. obscurity is achieved via anonymous identifiers that make it insolvable to trace their factual individualities. Encryption protects stoner data and signaling, while the SIM creates the encryption keys. druggies save their sequestration using Temporary Mobile Subscriber Identity(TMSI) and radio path encryption(10). Unfortunately, despite considerable security advancements over the former generation, there's still important vulnerability in 2G security. The Third Generation Partnership Project(3GPP) establishes a complete access control security system, including air interface security and stoner authentication. The security of the air interface is used to cover dispatches over wireless links and druggies. At the same time, it provides a two- way authentication process that can authenticate druggies and the network on both sides (sender and receiver) for further trustability (11). The communication channel attacks between the end bias and their home networks also introduce 3G network pitfalls.

2.2 . Security Issues in 4G and 5G

In 2009, 4G networks offered up to 1 Gbit per second for downlink transmission and 500 Mbit per second for uplink communication(12). 4G networks also give high diapason effectiveness and lower quiescence, enabling 4G networks to handle complex operations similar as High- description TV(HD television) and Digital Video Broadcasting(DVB). 4G systems include IP core networks, backbone, access networks, and a diversity of intelligent mobile outstations. The 4G primary security problems are related to pitfalls of wireless radio communication, tampering, wiretapping, data revision, and network authentication. Due to the increased circular commerce between druggies and mobile outstations, the 4G network is more vulnerable to security issues than former mobile radio networks. As the 5G network approaches commercialization, we may anticipate increased data pets using complex systems and high- security infrastructures(13). 5G networks ’ novelty is their capacity to connect the growing number of bias while delivering advanced quality services to all network realities. The most straightforward approach to classify security and sequestration issues in 5G networks is to examine the network armature.


Security evolution in legacy mobile networks
Security issues
6G: AI/ML threats , system architecture attacks
5G: NFV, SDN and cloud threats
4G: MAC layer attacks and new devices threats
3G: Ip privacy issues , wireless interface threats
2G: one-way authentication issues , Unauthorized access
1G: Unencrypted telephone services
Network services
1G
1980
Deliver voice services
2G
1990
Support voice and short messages
3G
2000
Allow high speed internet and web browsing
4G
2010
Improved spectrum efficiency and reduced latency
5G
2020
Support high speeds, and more secure system
6G
2030
Ultra Low latency services, variety of applications , ERLLC, IoE

2.3. 5G Security Improements

5G improves security armature and authentication styles while addressing numerous 4G excrescencies. 5G is the first standard to use unified authentication. WiFi, string, and 3GPP networks are each supported. A 3GPP- authenticated UE may dislocate to anon-3GPP network without reauthenticating(14). This point increases network security. It also helps authorize interceptions. Drivers may block exchanges for sanctioned law enforcement agents when a judge issues a process to probe a crime. still, the communication format and reality part are different.

2.4. Conclusions of Mobile Networks Security

Every network generation has excrescencies. Although colorful measures to reduce exploitation live, the difficulty of upgrading introductory protocols leaves important vulnerability.The supported services, functions, and known security issues in the earlier generation security infrastructures. Attacks against 6G security armature and operations include signaling DoS(denial of service), DDoS(dispersed denial of service) against authentication waiters, energy reduction attacks, and stoner shadowing. For illustration, poor authentication and resource restrictions affect all network generations and are delicate to perfect.

3. 6G Network Vision and Essential Research systems

This section discusses the network vision about the security armature of 6G and the 6G original supported systems ’ conditions.

3.1 . 6G Network Vision

5G technologies, includingMulti-access Edge Computing(MEC), SDN, NFV, and network slicing, are still applicable to 6G networks. thus, their associated security matters will stay. For illustration, the most severe security enterprises connected with SDN include vulnerabilities on the SDN regulator, interfaces, and SDN operations platforms. Security obstacles associated with NFV include attacks on virtual machines, hypervisors, and virtual network function(VNF) directors. Eventually, MEC is vulnerable to physical pitfalls, DDoS, and the tremendously distributed structure of 6G systems. In 6G, a hierarchical security medium that differentiates communication security at thesub-network position fromsub-network to comprehensive area network security would be preferable. Confluence of the RAN and core functions centralizes the upper layer RAN services, coinciding with scattered core functions similar as stoner Aeroplane Micro Services(UPMS) and Control Aeroplane Micro Services(CPMS). 6G networks include zero- touch networking and Service Management(ZSM) armature to allow rapid-fire services, low operating costs, and lower mortal error. Complete robotization combined with tone- literacy enables attacks to grow in unrestricted-circle systems. Data sequestration protection is challenging in zero- touch networks due to critical robotization conditions with little mortal involvement.

4. 6G Security Conditions and Proposed Security Architecture

This section discusses the 6G security conditions and the security armature.

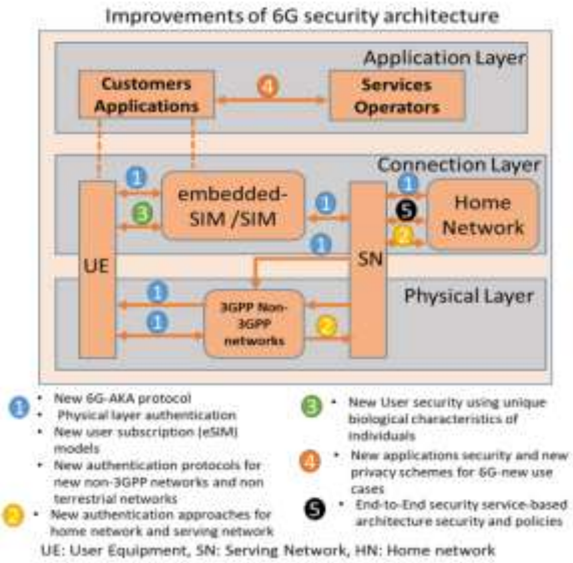
4.1. 6G Security Architecture Conditions

The 6G system security armature has been designed for openness. Because 6G is intended to be a more open network than 5G, the line between inside and outside the network will come precipitously blurred. As a result, current network security measures, similar as IPsec and firewalls, won't be important enough to cover the network from outside interferers. The 6G security armature should support the introductory security conception of zero trust(ZT) in the mobile communication network to palliate this issue. ZT is a security paradigm that emphasizes the protection of system coffers above everything differently. ZT presupposes that an bushwhacker may live within the network and that the network armature is accessible or untrustworthy from the outside. Such an assessment must be made regularly, and conduct must be taken to reduce the threat of internal asset loss. Zero trust armature(ZTA) is a security armature that uses the ZT conception and comprises connections between network realities(NEs), protocol processes, and access rules. thus, ZTA should be the foundation of 6G security armature. Some security conditions can be managed to support secure 6G networks using the ZT conception.

4.2 Proposed Security Architecture of 6G

This section presents a description of 6G’s current disquisition. It also addresses an explanation of new variations to 6G enabling technologies in the three situations(physical, connection/ network caste, and service/ operation caste).

6G network design will differ significantly from 5G in various ways. First, 6G may negotiate network automation and Network as a Service(NaaS). NaaS enables subscribers to customize networks. pivotal technologies include intent- predicated networking, end to end software, cloudization, and deep slicing/ function virtualization. Second, the fast handover of pall- predicated networks and open source software for core/ RAN network factors predicts the “ full openness ” future of 6G. 6G may be the first entirely AI- enabled cellular system. This vision would transfigure 5G’s “ connected effects ” into 6G’s “ connected intelligence, ” with AI ultimately controlling most network operations and bumps(16). According to(17), Deterministic Networking(DetNet) or Time-Sensitive Networking(TSN) may help 6G to achieveultra-Reliable and Low quiescence Dispatches(uRLLC).


Improvements of 6G security architecture
Application Layer
Customers Applications
4
Services Operators
Connection Layer
1
3
embedded-SIM /SIM
1
1
1
5
2
Home Network
UE
SN
Physical Layer
1
1
3GPP Non-3GPP networks
2
1 • New 6G-AKA protocol
• Physical layer authentication
• New user subscription (eSIM) models
• New authentication protocols for new non-3GPP networks and non terrestrial networks
2 • New authentication approaches for home network and serving network
3 • New User security using unique biological characteristics of individuals
4 • New applications security and new privacy schemes for 6G-new use cases
5 • End-to-End security service-based architecture security and policies
UE: User Equipment, SN: Serving Network, HN: Home network

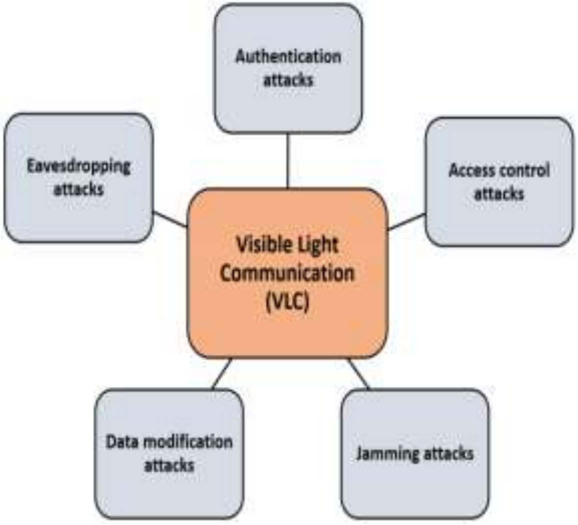
5. 6G Promising Technologies Security Challenges and Possible Attacks

Some significant technologies have formerly been proven to be effective in important essential sectors of the 6G networks. They give high security, low quiescence trustability, and effective communication services to 6G networks. still, utmost new 6G technologies have advanced security and sequestration pitfalls.

5.1 6G Physical Layer Technologies

The proposed styles for securing the physical layer depend on the arbitrary physical characteristics and the noise girding wireless networks. still, the inflexibility of PLS mechanisms, particularly in resource- constrained conditions, with the possibilities of disruptive 6G technologies, may pave the way for a new period of PLS in the 6G period(18).They will be basically used to communicate with idle holographic dispatches, small- scale dispatches,ultra-high-capacity data, and short- range transmission withultra-high-speed are only a many of the operation openings. situating with high delicacy and seeing with excellent resolution using THz communication signals are other demanding operations.

Figure 4 shows the most common attacks in 6G visible light communication technologies.



5.2 AI/ ML Technology

AI and ML have been marked as necessary factors of the network armature of all 6G networks technologies. As a result, artificial intelligence entered important attention in the 6G networking. AI/ ML in the 5G networks is enforced in locales with vast training data and effective computing cores. still, AI/ ML has come a significant reality of the 6G networks. AI and ML are used to secure colorful frames of 6G's security defense and protection. The use of AI and ML in security makes the security results more independent and more accurate with prophetic capabilities for security analytics. Thissub-section addresses some of the challenges associated with AI/ ML in the 6G system (19).

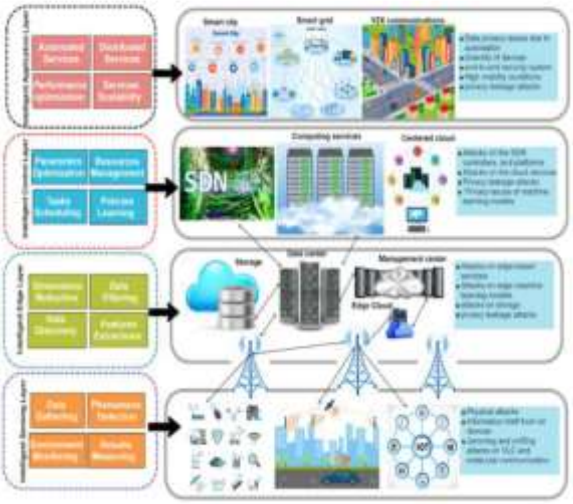
Trustworthiness **:** responsibility The trustability of machine literacy models and factors becomes important when AI handles network security.

Visibility : Monitoring security functions grounded on AI and ML in real time to insure control and credibility. Ethical and Legal Aspects Optimization ways grounded on AI can limit some guests or operations. AI- powered security results are invariant in their protection of all druggies or not; who's responsible for security services ’ failure controlled by AI.

Extensibility and viability : Secure data transfers are necessary to insure the sequestration of allied learners. Scalability of the needed computing, communication, and storehouse coffers is a challenge for AI/ ML.

Controlled security tasks : important outflow may affect when AI/ ML security results are associated with significant data processes.

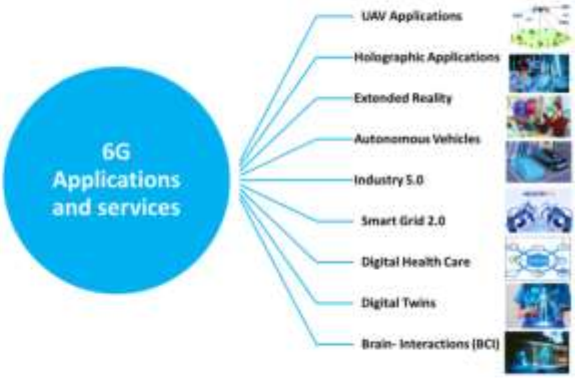
The 6G secured architecture-based AI/ML is shown in Figure 5 and summarized as follows.



6. 6G operations’ Security Challenges

Due to the high communication conditions and requirements of the 6G operations, numerous operations and services have veritably demanding performance and extraordinarily strict security conditions. The commerce between general performance prospects and security needs to come decreasingly more complex as largely competent, ubiquitous bushwhackers and vicious exertion come more current.

Figure 8 The most essential 6G operations in different technologies.



6.1 Connected Autonomous Vehicles:

6G networks will be vast, offer the stylish experience, and be applicable in a wide range of scripts, allowing connectivity to be available anywhere. The access network design must be reduced and made sufficiently elastic to give the essential capabilities to minimize processing quiescence. In addition, the exploration might concentrate on intelligent control mechanisms driven by conditions and radio resource operation, showing the necessity of a software- grounded, service- acquainted approach to design.

6.2 Industry 5.0

mortal collaboration with robots and intelligent technology has been linked as the coming artificial revolution advance in Industry 5.0(20). 6G is pivotal for the automated artificial terrain's advancement. Due to high- security pitfalls, Industry 5.0 apps must satisfy introductory security rudiments similar as integrity, vacuity, authentication, and auditing. For Industry 5.0 security styles, issues similar as lower functional costs, a further comprehensive range of bias, and lesser scalability must be considered.

6.3. Smart Grid2.0

Grid networks are getting more innovative as intelligent bias, and advanced data analytics styles are developed, moving from Smart grid 1.0 to Smart grid 2.0. Smart grid 2.0 introduces automated smart cadence data analysis, line loss analysis, intelligent dynamic pricing, and robotization and operation of grid distribution. Smart grid 2.0 has tone- mending and tone- organized capabilities.

6.4. Digital Healthcare

Digital healthcare is growing in new ways. Intelligence healthcare powered by AI'll be advanced through numerous new methodologies within the coming many times. In addition, the growing population may affect in a more significant focus on digital health than has preliminarily been honored. Body Area Networks(BANs) equipped with intelligent bedded systems advance personalized operation and health monitoring. These acclimatized BANs can gather health data from colorful detectors, partake it stoutly, and interact with network services(21). 6G will probably come the central communication platform for intelligent unborn healthcare services.

6.5. Brain – Computer relations (BCI)

The BCI process consists of four phases signs prisoner, birth of features, restatement of features, and final reporting. The primary operations of BCI are associated with the health care sector, substantially to allow impaired persons to manage the probative outfit. BCI communication is hovered by different types of attacks that limit the connection of these operations and may hang the case's life occasionally while using BCI in health operations. BCI attacks can be divided into brain signal generation attacks, data processing attacks, and data accession attacks.

7. Conclusions

This paper introduces an ferocious study on security challenges and conditions for the 6G network. It shows the elaboration of security in heritage wireless networks, starting from the 1G network to the forthcoming 6G network. In this paper, we proposed the 6G network vision and exploration directions in academia and industry. We also proposed a 6G security armature and the new anticipated security functions. We covered the different physical layer technologies in 6G networks by probing the possible attacks and proposed results. The anticipated innovative 6G system includes AI technologies to enhance security and increase network protection. therefore, the paper discusses the security armature of the 6G network grounded on AI/ ML technologies. The layers of security armature include the intelligent seeing layer, intelligent edge layer, intelligent control layer, and intelligent operation layer. Each layer supports colorful functions and introduces some attacks. Several security issues of the physical layer have been addressed, similar as molecular communication, THz communication, and VLC communication. utmost of the new 6G technologies pose significant security and sequestration pitfalls. These leading technologies have been stressed, clarifying their security challenges and attacks and security forestallment results. Every new generation of network technology introduces innovative and creative operations. 6G is snappily establishing itself as the network enabler for several other new operations that will unnaturally alter mortal civilization in the 2030s and beyond. numerous apps and services have largely demanding performance and incredibly severe specific security because of the high communication conditions and requirements of 6G operations. The paper presents different security challenges and musts for several 6G operations similar as unmanned ariel vehicles, holographic, extended reality, industry5.0, Smart grid2.0, health care, and brain- computer relations. Implicit 6G developments and difficulties for colorful 6G operations are also bandied. We intend to probe the different attacks on the 6G network with lesser depth in the future. Chancing a result for guarding 6G is a critical issue that will need to be delved in the future.

8. Reference

1. Parikh, J.; Basu, A. Technologies Assisting the Paradigm Shift from 4G to 5G. *Wirel. Pers. Commun.* **2020**, 1–22. [**Google Scholar**] [**CrossRef**]
2. Mallat, N.K.; Ishtiaq, M.; Rehman, A.U.; Iqbal, A. Millimeter-Wave in the Face of 5G Communication Potential Applications. *IETE J. Res.* **2020**, 1–9. [**Google Scholar**] [**CrossRef**]
3. Alsharif, M.H.; Kelechi, A.H.; Yahya, K.; Chaudhry, S.A. Machine Learning Algorithms for Smart Data Analysis in Internet of Things Environment: Taxonomies and Research Trends. *Symmetry* **2020**, *12*, 88. [**Google Scholar**] [**CrossRef**][**Green Version**]
4. Mobile World Live. Available online: **https://www.mobileworldlive.com/asia/asia-news/samsung-dominates-korea-5g-deployments/** (accessed on 28 March 2020).
5. Samsung "5G Launches in Korea". Available online: **https://images.samsung.com/is/content/samsung/p5/global/business/networks/insights/white-paper/5g-launches-in-korea-get-a-taste-of-the-future/5G-Launches-in-Korea-Get-a-taste-of-the-future.pdf** (accessed on 28 March 2020).
6. Ericsson Report "This Is 5G". Available online: **https://www.ericsson.com/49df43/assets/local/newsroom/media-kits/5g/doc/ericsson_this-is-5g_pdf_2019.pdf** (accessed on 28 March 2020).
7. Oyeleke, O.D.; Thomas, S.; Idowu-Bismark, O.; Nzerem, P.; Muhammad, I. Absorption, Diffraction and Free Space Path Losses Modeling for the Terahertz Band. *Int. J. Eng. Manuf.* **2020**, *10*, 54. [**Google Scholar**]
8. Saxena, S.; Manur, D.S.; Mansoor, N.; Ganguly, A. Scalable and energy efficient wireless inter chip interconnection fabrics using THz-band antennas. *J. Parallel Distrib. Comput.* **2020**, *139*, 148–160. [**Google Scholar**] [**CrossRef**]
9. Elmeadawy, S.; Shubair, R.M. Enabling Technologies for 6G Future Wireless Communications: Opportunities and Challenges. *arXiv* **2020**, arXiv:2002.06068

Dang, S.; Amin, O.; Shihada, B.; Alouini, M.-S. What should 6G be? *Nat. Electron.* **2020**, *3*, 20–29. [**Google Scholar**] [**CrossRef**][**Green Version**]

Liang, Y.-C.; Larsson, E.G.; Niyato, D.; Popovski, P. 6G Mobile Networks: Emerging Technologies and Applications. *China Commun.* **2020**, *17*, 1–6.

Chen, S.; Sun, S.; Xu, G.; Su, X.; Cai, Y. Beam-space Multiplexing: Practice, Theory, and Trends-From 4G TD-LTE, 5G, to 6G and Beyond. *arXiv* **2020**, arXiv:2001.05021. [**Google Scholar**] [**CrossRef**][**Green Version**]