ATARC 5G Executive Whitepaper

May 2020

Baseline Knowledge

5G denotes the 5th generation of mobile cellular technology and represents the largest increase in capabilities compared to previous generations. Going beyond traditional cell-phone use cases, 5G includes support for vehicle communications, internet of things (IOT), satellite communications, and more. While capable of being deployed in conjunction with 4G infrastructure or standalone, 5G offers the potential for lower latency, higher reliability, more connected devices, and endpoint to endpoint communications. The 5G standard is developed by an international body called 3GPP, which is composed of participants from multiple national telecom standards organizations and many of the world's most prominent technology companies including Ericsson, Samsung, Nokia, Apple, Intel, and Huawei. The 3GPP 5G standard is incrementally defined; Release 15 marked the 5G phase 1 standard in 2018, and Release 16 will mark the full 5G standard later in 2020.

One of the most significant changes in 5G is the addition of "millimeter wave" spectrum; the word "spectrum" is used to denote the radio frequencies used by a signal. Millimeter wave is higher in frequency than those used in 4G networks, closer to that of infra-red and visible light. While the higher frequency signals mean it can carry more data, it also means it cannot travel as far and has a harder time going through materials like walls and people, similar to infrared and visible light. This means to achieve the highest data throughput, millimeter wave must be used in conjunction with a denser deployment of access points and directional transmission to overcome many of the propagation drawbacks [1]. Even with the addition of millimeter wave, 5G will simultaneously use 4G-like and millimeter wave spectrum. More details on the Federal Communications Commission's spectrum approach can be found in [2].

Health issues associated with the deployment of 5G need to be understood and addressed. Public theories have surfaced that that 5G is unsafe, going so far as to result in the public destruction of 5G infrastructure in the United Kingdom [3]. Contrary to this, the FDA states in [4] that, "to date, there is no consistent or credible scientific evidence of health problems caused by the exposure to radio frequency energy emitted by cell phones." The FDA goes on to state that there will be, "no new implications for 5G" and that, "the conclusions reached based on the current body of scientific evidence covers [5G] frequencies."

Radiation like Gamma Rays and X-Rays can be dangerous because they pass through the body and directly damage DNA [5]; radiation from 5G is not known to behave this way. According to the International Commission on Non-Ionizing Radiation Protection (ICNIRP) in [6], "the only substantiated effect of [radiofrequency electromagnetic field] exposure relevant to human health and safety is heating of exposed tissue," in the millimeter wave spectrum. The ICNIRP goes on to state that, "a considerable amount of research has been conducted on the relationship between [radiofrequency electromagnetic field] and health outcomes such as headaches, concentration difficulty, sleep quality, cognitive function, cardiovascular effects, etc.…this research has not shown any such health effects."

Besides changes to spectrum, 5G changes its core infrastructure to leverage virtualization for network scalability, flexibility, and security. In 4G, we generally think of typical consumers as being equal on the same network, having the same quality of service, data throughput, and user experience. In a 5G network, carriers or private network architects can enable "network slicing," which essentially dedicates a virtual private network with different service characteristics (quality of service, throughput, latency, and security) to different types of devices [7]. For example, vehicles may need high priority- low latency service but not need much data throughput, while traditional personal mobile users may need high data throughput but be flexible on latency; in the 5G networks these different use cases can be segmented into their own slices to minimize impacts of one slice on another.   A technical comparison between 4G and 5G can be found in Table 1 of [8].

While 4G networks impacted consumer culture, creating successful American businesses like Uber, GrubHub, and Facebook, experts expect that 5G will impact a broader set of industries such as aviation, agriculture, manufacturing, and healthcare [9].

Current Capabilities

While many key pieces of the 5G standard are defined in 3GPP Release 15, as of April 2020, many of these capabilities have not yet materialized in consumer grade solutions. Existing consumer grade 5G is limited to "Enhanced Mobile Broadband" for traditional cell phones; commercial carriers report end user download speeds of over 4Gb/s in certain areas. While this marks a significant improvement over 4G speeds, we have yet to realize the full impact of the ubiquitous connectivity that 5G will enable.

Although 5G hasn't yet reached full maturity, the Department of Veteran's Affairs has been demonstrating what is possible with current 5G technology and standards. In a partnership with Microsoft, Verizon, and Mediviz, the Department of Veteran's Affairs has created the first 5G-enabled hospital. Implementing a private 5G network with specialized devices, the VA has been able to create the infrastructure to allow for live streaming of medical imagery in augmented reality to allow for remote patient diagnostics, real time clinical collaboration, and enhanced medical education. The VA is an exemplar of what is currently possible with 5G despite an incomplete standard.

While private 4G networks are somewhat rare, private 5G networks are likely to be common. The 3GPP 5G standard supports non-5G specific authentication protocols, which means that authentication and access to a private 5G network can occur through standardized enterprise methods. Many existing experimental implementations of 5G are considered private networks.

Planned Capabilities

This section discusses many of the features defined or planned in the 3GPP 5G standard, but not yet realized at the consumer or enterprise level. As discussed in the "Baseline Knowledge" section of this paper, network slicing is a core 5G capability that enhances security by providing virtual separation of devices requiring different performance and security levels. For example, 5G will enable large numbers of low power, low cost devices to be connected to the internet; this is known as the Internet of Things (IoT). Network slicing can be used to separate IoT devices from consumer devices to ensure both sets of devices realize specific security and network performance requirements while allowing both types of devices to physically communicate to the same radio infrastructure. [10] [11]

In addition to IoT, 5G supports vehicle communications; this is referred to as "Vehicle to Anything" (V2X). In this use case, vehicles communicate directly to each other, or through existing 5G/4G infrastructure. Departing from the needs of consumer devices and IoT, V2X 5G must have extremely low latency while supporting communications between vehicles (cars, unmanned aerial vehicles) traveling up to 310mph. Again, network slicing will ensure that V2X low-throughput low-latency communications are prioritized over less life-critical communications. [12]

5G allows for the possibility to enhance global communication. 3GPP Release 16 will define satellite access for 5G, enabling companies to launch low earth orbit satellite that can directly connect to smart devices, mobile assets (planes, ships, UAS), and fixed assets (buildings, bases). While these services may not be able to achieve the extremely low latency communications of terrestrial infrastructure (due to physics), it will represent a decrease in latency, increase in speed, and increase in coverage over existing satellite networks. [13]

Further innovations include 5G as a medium for broadcast TV service, support for critical medical applications, and enhancements for UAV communications [12] [11] [14].

Security

The 5G standard represents a significant enhancement to security over 4G. As discussed previously, 5G now incorporates standard enterprise authentication, virtualization, and stronger encryption than 4G, while also addressing security vulnerabilities from 4G. Despite these advancements in security, organizations should remain vigilant when implementing 5G; many of the security enhancements are *optional* and may not be supported by all equipment. Experts anticipate that 5G adoption will significantly increase the number of connected devices, thus increasing the attack surface for threat actors to exploit [15]. To mitigate against this potential threat, it is strongly recommended that 5G use cases be integrated into an organization's comprehensive Zero Trust Architecture[1] strategy as the foundation for addressing the breadth and scope of connected devices.

While the 5G standard is open and transparent, a significant number of contributions to the standard have been by Chinese companies [16], though many trusted 5G vendors such as Erikson, Nokia, and Samsung are heavily engaged in standards to secure all aspects of 5G. Internationally, one of the most prominent security concerns is supply chain and the secure production of 5G equipment. If a non-trustworthy company manufactures 5G equipment, that equipment may be subject to compromised confidentiality, integrity, or availability. Compounding this problem, Chinese companies may be required to deliver any gathered intelligence to the Chinese government [17].

The U.S. government has demonstrated its commitment to help secure 5G for itself and allies through the Secure 5G and Beyond Act of 2020 [18]. Enacted into law in early March 2020, this bill requires development of a Federal 5G Security Strategy, which was released shortly thereafter in late March 2020 [19]. Additionally, the federal government has taken steps to stop introduction of Chinese telecommunications and networking infrastructure in the U.S. through the recently enacted Secure and Trusted Communications Networks Act of 2019 [20].

Enterprise Considerations

5G has the potential to significantly change enterprise information technology. Due to enhanced connectivity for traditional endpoints (laptops, desktops, mobile devices), small to medium size enterprises may choose to eliminate on-premise networking infrastructure (routers, firewalls, cable) in favor of commercial 5G connectivity. To make this significant shift in network architecture, an enterprise must enhance its investment to protect endpoints, centralize computing services in the cloud or datacenters, and establish robust network tunneling solutions.

Should an enterprise choose to rely more on commercial 5G connectivity rather than their own infrastructure, enterprises should establish Service Level Agreements (SLAs) to ensure that the network quality and availability of service is sufficient for enterprise operations; requirements for communications access, resiliency, and contingencies must be mutually understood. Organizations choosing to implement their own private 5G infrastructure should be aware that 5G will require denser infrastructure than 4G (i.e. more base stations) and plan

[1] Per [21], Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move network defenses from static, network-based perimeters to focus on users, assets, and resources. A Zero Trust Architecture uses zero trust principles (e.g. no implicit trust granted based solely on network location, explicit authentication and authorization, network micro-segmentation, etc) to more effectively protect an organization's resources and data especially in the light of increased cloud, mobility, and 5G emphases.

for lifecycle costs associated with maintaining private 5G infrastructure as well as recurring 5G carrier access costs.

Security should always be a consideration in any organization's 5G adoption plan. As discussed previously, an organization should integrate 5G into their comprehensive Zero Trust Architecture including awareness aware of their 5G infrastructure's source, interoperability with their existing network infrastructure, ability to monitor and secure their endpoints, cloud, and datacenter environments [21].

With any new technology, public-private collaboration is essential to an organization's successful adoption. Technology leaders should be forward leaning, transparent, and innovative in their approach; 5G offers significantly more than an incremental network capability to smart phones, rather it has the potential to transform business operations in the same way network enabled apps transformed the consumer experience.

Credits

This paper was produced by the ATARC 5G Working Group. Specific contributors were as follows:

- ATARC 5G Working Group Government Lead: LT Kenneth Miltenberger, Co-Chair USCG Mobility Council, USCG
- ATARC 5G Working Group Industry Lead: Dr. D.J. Shyy, PhD, Mitre
- Allen Hill, Executive Director of Telecommunication Services, GSA
- Marc Wine, Director of Technical Integration Support and Industry Liaison, Department of Veteran's Affairs
- Russell Mohr, Engineering Director, MobileIron
- Kevin Robins, Analyst, GSA-FAS ITC
- Derek Lee, IT Specialist, U.S. Customs and Immigration Service
- Joshua Weaver, Naval Surface Warfare Center Dahlgren
- Viet Le, DISA Innovation & Systems Engineering Directorate
- Steve Vetter, Federal Strategist, Cisco Systems Inc.
- Ronald Davis, National Institute of Health
- Victor Florido, GSA
- William Butler, Capitol Technical University

References

[1] A. Nordrum, K. Clark and I. S. Staff, "5G Bytes: Beamforming Explained," IEEE, 15 July 2017. [Online]. Available: https://spectrum.ieee.org/video/telecom/wireless/5g-bytes-beamforming-explained.

[2] FCC, "FCC's 5G Fast Plan," FCC, [Online]. Available: https://docs.fcc.gov/public/attachments/DOC-354326A1.pdf.

[3] L. Kelion, "Mast fire probe amid 5G coronavirus claims," BBC, 04 April 2020. [Online]. Available: https://www.bbc.com/news/uk-england-52164358.

[4] Food and Drug Administration, "FDA.gov," 10 February 2020. [Online]. Available: https://www.fda.gov/radiation-emitting-products/cell-phones/scientific-evidence-cell-phone-safety.

[5] S. Behjati, G. Gundem, D. C. Wedge, N. D. Roberts, P. S. Tarpey, S. L. Cooke and H. Davies, "Mutational signatures of ionizing radiation in second malignancies," 12 September 2016. [Online]. Available: https://sci-hub.tw/10.1038/ncomms12605.

[6] International Commission on Non-Ionizing Radiation Protection, "RF EMFS 100kHz-300GHz," [Online]. Available: https://www.icnirp.org/en/frequencies/radiofrequency/index.html. [Accessed 30 April 2020].

[7] 3GPP, "3GPP Release 15," [Online]. Available: https://www.3gpp.org/release-15.

[8] ATARC, "Federal Mobile Technology Summit Whitepaper," 6 August 2019. [Online]. Available: https://atarc.org/wp-content/uploads/2019/11/Final-2019-Mobile-White-Paper-1.pdf.

[9] Intel Corporation, "Prepared Statement for the Record of Intel Corporation for the United States Senate Committee on Commerce, Science, and Transportation: Hearing on 5G Supply Chain Security: Threats and Solutions," 4 March 2020. [Online]. Available: https://www.commerce.senate.gov/services/files/FD5715C5-1C34-4B09-8A70-FD219F343016.

[10] 3GPP, "3GPP Release 13," [Online]. Available: https://www.3gpp.org/release-13.

[11] 3GPP, "3GPP Release 16," [Online]. Available: https://www.3gpp.org/release-16.

[12] 3GPP, "3GPP Release 14," [Online]. Available: https://www.3gpp.org/release-14.

[13] SaT5G Project, "Integrated SaT5G General Network Architecture," December 2019. [Online]. Available: https://www.sat5g-project.eu/wp-content/uploads/2020/02/761413_Deliverable_9_Integrated-SaT5G-General-Network-Architecture-.pdf.

[14] 3GPP, "3GPP Release 17," [Online]. Available: https://www.3gpp.org/release-17.

[15] "5G Supply Chain Security: Threats and Solutions," 4 March 2020. [Online]. Available: https://www.commerce.senate.gov/2020/3/5g-supply-chain-security-threats-and-solutions.

[16] 3GPP, "3GPP Work Plan and Past Contributions," [Online]. Available: https://www.3gpp.org/ftp/Information/WORK_PLAN/.

[17] A. Kharpal, "Huawei says it would never hand data to China’s government. Experts say it wouldn’t have a choice," CNBC, 4 March 2019. [Online]. Available: https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

[18] "Senate Bill 893: Secure 5G and Beyond Act of 2020," 23 March 2020. [Online]. Available: https://www.congress.gov/bill/116th-congress/senate-bill/893.

[19] United States of America, "National Strategy to Secure 5G," March 2020. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

[20] "House Bill 4998: Secure and Strusted Communications Networks Act of 2019," 12 March 2020. [Online]. Available: https://www.congress.gov/bill/116th-congress/house-bill/4998/text.

[21] NIST, "SP 800-207 (draft)," 13 March 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-207/draft.