SECURING
SMART
CITIES

5G Security and Privacy for Smart Cities

22 Nov 2019

Authors:

Amin Hasbini, *Head of research center, META, Kaspersky*

David Jordan, *VP of Cyber Services and Smart Cities, Mission Secure Inc.*

Alan Seow, *Cybersecurity Practitioner*

Contributors:

Cesar Cerrudo, CTO, IOActive

1. Introduction and foundation

Wireless telecommunications technology has undergone a tremendous evolution in the last few decades, from making simple phone calls (1G) and sending text messages (2G), to connecting to high-speed internet (3G) and providing multimedia and entertainment services (4G). Futuristic technologies such as remote robotics and virtual reality are emerging quickly and are likely to see mass adoption, while 4G cellular networks have reached capacity limits and are incapable of supporting the uninterrupted operations of these services.

It is estimated that data will reach 175 zettabytes worldwide by 2025, up from 1.2 zettabytes in 2010, when 4G was first being deployed globally. 5G therefore provides a much-needed mobile bandwidth infrastructure for a world of connected objects and smarter cities. It is expected to be as much as 100 times faster than the present 4G systems, with up to 25 times lower latency or lag time and as many as one million devices supported within one square kilometer; this is 1000 times more dense than is currently possible. It is expected to be the core architecture of autonomous driving, virtual reality, the Internet of Things (IoT) and numerous other connected devices and services.

5G is known as the fifth-generation cellular network technology. 5G networks are digital cellular networks in which the service area covered by providers is divided into small geographical areas called cells. Analog signals representing sounds and images are digitized in the phone, converted by an analog to digital converter and transmitted as a stream of bits. Cells communicate through radio waves via local antenna and low power automated transceiver. The local antennas are connected with the telephone network and the internet via a high-bandwidth optical fiber. It therefore functions like our existing cell phone technology where a user crosses from one cell to another – his/her mobile device is automatically “handed-over” to the antenna of the new cell seamlessly.

The foundation of 5G can be summarized in five technologies:

1. Millimeter waves: 5G will be based on millimeter waves to open access to wider ranges of frequencies (up to 300 GHZ), to host and allow more devices and data. These frequencies have a short range and are therefore bound to be obstructed by buildings, trees, weather (rain/snow), etc.

2. Small cell networks: facing obstructions, low power small-scale base stations are deployed to serve as relays around obstacles, best applicable for cities where obstructions are ubiquitous; think every building at every corner as a potential repeater antenna possibility, if attachment rights can be had!

3. Massive MIMO (multiple input multiple output): used to improve spectral efficiency, ramping up network capacity. The technology was added for 4G LTE and is organic to 5G.

4. Beamforming: sending out signals as highly focused beams deliver a stronger radio signal with a higher data throughput for greater distances and preventing interference. This technology works as a traffic signaling service for massive MIMO so that more traffic can be managed simultaneously.

5. Bytes full duplex: another method for enhancing network capacity, based on the principle of data traffic reciprocity – incoming and outgoing signals do not collide when data is being transmitted on the same frequencies at the same time.

1.1. Importance of 5G

There is a need for smart cities to maintain a competitive edge in connectivity especially around digital infrastructure capabilities. A smart city will eventually face an economy transitioning to an absolute digital economy. In the digital economy streaming services, e-commerce and cloud computing are built on the assumption of uninterrupted access to the internet. The loss of connectivity can have potentially catastrophic business consequences, so we need to ensure the digital infrastructure is able to support the growing digital economy.

The adoption of 5G is inevitable especially for advanced services in healthcare, industry and entertainment. It is capable of hosting a massive number of devices, fulfilling the needs of the IoT and the IoE (Internet of Everything).

Examples of services that are enabled include:

- Smart city critical Infrastructure: management and monitoring of numerous remote systems for traffic, energy and water facilities;
- Smart city transport systems, orchestrating traffic and vehicle flows, while collecting data from numerous sensors distributed around the city.
- Smart city post and delivery services, highly dependent on communication schemes and remote communications
- Smart city financial services, where all payment machines are connected and require not only high speed connected services but also secure communications for transactions
- Surveillance and traffic cameras, vehicle to infrastructure communications, smart devices/services backhaul communications.
- Smart surgical operations, where surgeons can remotely perform surgeries, whether via pre-planned scheduled ones or remote ‘on the spot’ interventions in the case of emergencies or accidents using advanced drones
- Smart city government complex operations, monitoring borders, coastal safety, safeguarding protests…
- Day-to-day services such as 8k streaming, real-time mobile gaming into augmented/virtual reality experiences
- Smart city emergency interventions: services for saving lives greatly benefit from 5G installations; drones can quickly reach and live broadcast an incident location, could be used for delivering first aid and equipment or even to transport a victim to the closest medical center.

2. [5G] risks and challenges

Managing security is a continuous and dynamic process. With the dramatic increase in the number of connected devices comes a natural expansion of the attack surface and intensity of the threats. As 5G technologies become widely deployed the weaknesses and inherent security flaws of 5G will be identified and hopefully quickly patched.

The following are the key anticipated risks to be elaborated upon in the subsequent sections:

- Protocol weaknesses and large-scale vulnerability exploitation
- Severe DDoS attacks
- BYOD threats
- Data security and privacy
- State-funded terrorism, espionage or corporate sabotage
- Critical infrastructure/public safety

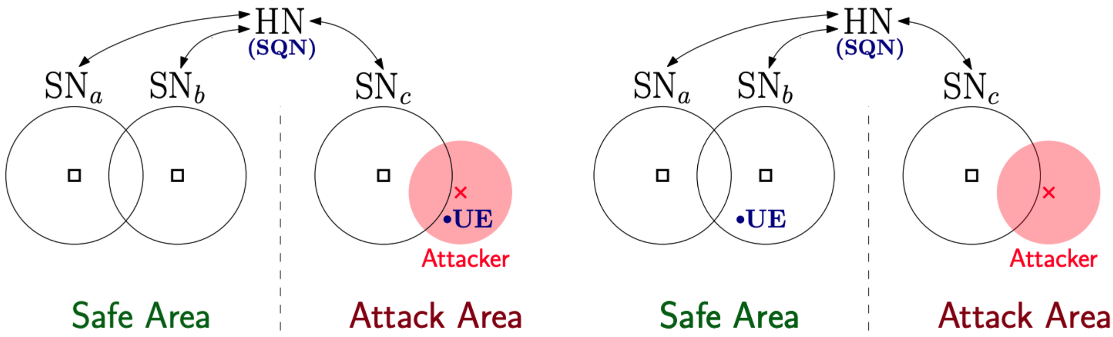
The dangers are profound, smart cities cannot survive without stable and secure communications, much danger could elevate and many could be at risk:

- Critical infrastructure could be at risk, misbehavior can stop water or power from reaching certain regions, or at the other side overflow other regions with water or damage power facilities, causing different sorts of disruptions and dangers
- Smart city transportation would be very serious if malfunctions arise and vehicles stop working or malfunction in the middle of the streets
- Smart city delivery and post services could be at risk, drones can fail, misbehave or fall down on the streets risking lives
- Smart city financial services could be affected if citizens are not able to complete transactions for their needs such as food and merchandise
- Smart city safety could be compromised if surveillance systems were taken down or fail, such would allow criminals to exert their offences without limits
- Smart city citizens and country safety could be at risk if medical drones are not able to reach emergency scenes or if borders are not controlled.

2.1. AKA protocol weaknesses

AKA stands for authentication and key agreement – a challenge-response mechanism for authenticating systems on the 5G network. It works by negotiating and generating keys for encrypting communications paths between a device and the cellular network. AKA protocols have been in use since 3G and 4G networks. After successful authentication a secure connection is established between the client device (e.g. a mobile phone) and the cellular network. AKA is vulnerable to IMSI (international mobile subscriber identity) catchers. This is a classic MITM (man-in-the-middle) attack allowing an attacker to pose as a fake base station and intercept traffic. More sophisticated attacks can downgrade the client device's network connection network to previous networks protocols and connection scenarios that allow for interception and manipulation of the traffic. It is a known practice by law enforcement agencies and authorities to intercept mobile phone traffic metadata and track mobile phone locations, etc.

While the AKA protocol was redesigned and enhanced for 5G security, a recent study indicates vulnerabilities remain (study by Borgaonkar, R., Hirschi, L., Park, S., & Shaik, A. (2019). New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. Proceedings on Privacy Enhancing Technologies, 2019(3), 108-127). The study disclosed a subtle vulnerability in the 3G, 4G and 5G AKA protocol implementations that could allow a low-cost attack to leak private data about the subscribers. The target device stepping in or out of the attack area, implemented with a fake base station with reference to its activities can reveal much about the device's user and its relations with other devices. Attackers might be able to keep track of users even when they move away from the "fake" base station (IMSI-catcher device) and later briefly return into the station's coverage. The diagrams (a) and (b) below, taken from this study, illustrate the attack approach of existing IMSI catchers and a new approach suggested by the researchers (HN=Home Network, SN=Serving Network, UE=User Equipment):



(a) When the *UE* is in the attack area, it was known that it may be subject to tracking, location attack, and monitoring attacks.

(b) *UEs* were supposed to be safe when outside of attack areas. This is no longer the case due to our attack as *UEs*' activities in that area will partially leak when they re-enter an attack area.

Source: Borgaonkar et al., 2019 study on 5G privacy threats

The researchers state that high profile targets such as embassy officials or journalists could be exposed to greater privacy risks. Installing a fake base station near an embassy would not only help the attacker in profiling personnel activities during the day but also at night or while on business travel (think corporate espionage). The attacker could find out if the target switched SIM cards, get to know their agenda or even specific target behavioral patterns when there is a sudden increase in calls/texts made in a sensitive timeframe (think blackmail or pre-crime prevention).

2.2. DDoS

Distributed denial of service (DDoS) attacks are not new with the first being used back in the year 2000. They are low cost and highly effective due to their simplicity. A DDoS attack relies on the abuse of computation and processing resources and the emulation of a large network of client machines via large numbers of infected systems, sometimes called botnets or zombie machines. DDoS attacks have been used to disable the online services of banks and e-commerce platforms, but also to jam countries out of the internet, as in the case of the Mirai botnet and Liberia. Critical infrastructure is also a target for DDoS attacks, such as in the 2014 case of Boston Children's Hospital where the medical staff were unable to use medical devices putting patients' lives in danger and causing damages totaling est. US$600,000.

The radio network is also affected by DDoS attacks. An attacker overwhelming 5G data channels with random data or noise can affect the connectivity of clients around the corresponding base station. 5G is also expected to connect critical infrastructure equipment and facilities which will need to develop adequate work-around for the potential loss of connectivity, possibly by employing alternative communication channels (most likely with much less capacity for video and other new century first responder communications technology such as head-up displays, monitoring by incident command of deployed 1st responder vital health statistics, team member locations, etc.). A similar impact can also be achieved if the attacker is capable of hijacking a large number of devices and controlling them to send large amounts of traffic at the same time with the intent of overwhelming the computation and processing resources thus preventing legitimate devices from establishing needed new network connections. Last, but not least, unanticipated natural disasters might cause anomalies in the functioning of these devices and therefore cause situations where a 'flash crowd' consumes all radio resources. 5G networks inevitably open up more dimensions for DDoS attacks.

2.3. BYOD infections

Bring your own device (BYOD) refers to the use of personal smart devices in a work/professional context. These devices are permitted to connect to enterprises' internal networks and resources as well as access and retrieve information. Access is controlled and each user will have their own profile to log-in. Today's workforce is evolving with technology; people work in less fixed environments and perform their roles in a more nomadic manner, anywhere and from any device. This work style is becoming the dominant work culture.

It could be argued that BYOD encourages employees to stay connected, reducing hardware requirements and commutes; resulting in higher productivity and lower costs for the company and the employee. However, problems arise when companies attempt to manage the privacy of the corporate data on employees' multi-purpose devices, especially when those devices belong to different brands and run different software. In a 5G environment with even more brands and applications for user devices, controlling data flows, data privacy and storage becomes highly complex and it's likely that more than one device will be hijacked and then remotely manipulated to steal sensitive enterprise data. In addition, the increase in the number of systems and devices used by each user will unquestionably increase the attack surface and the percentage of vulnerable devices that an attacker can target. Cross-platform attacks that allow cybercriminals to attack other devices from compromised ones (think compromised IT servers and routers used to deliver DDoS attacks via the Internet), will also become more feasible and relevant. Another risk that is expected to grow is DDoS, the bigger the number of inherently insecure devices, the larger the number of devices that will be remotely controlled specifically for DDoS attacks. Attackers can then send massive amounts of data from a large number of devices overwhelming and paralyzing the 5G network's bandwidth and channels. In other words BYOD threats and mobile management risks are grow with available bandwidth and the 5G-connected world is the next evolution of cyber risk/threat. 5G is the conduit that increases risk in both IT, OT and Critical Infrastructure services!

2.4. Espionage

In the political world and before it even reached technical discussions 5G triggered vicious debates around supply-chain security and 5G product vendor countries and affiliations. The U.S. government has initiated a sustained campaign against the Chinese technology giant Huawei, accusing it of selling telecom products with backdoors; making statements that the company has potential connections with the Chinese army, etc.(think high potential for political manipulation for better trade agreements having negative impacts on 5G technology deployments). Huawei meanwhile, claims it is the leading 5G technology developer and is at least 18 months ahead of any other 5G gear manufacturer in the world. As large Chinese companies provide more widely needed hardware such as electronic chips and batteries it is understandable that governments need to take exceptional precautions when it comes to their network gear suppliers. Such precautions are particularly relevant in cases where the 5G gear manufacturer can remotely shut down the equipment with a master switch or code. Imagine for example that a company who falls under the control of its hose government would be forced to use its technology to capture, collect data packets or reconfigure devices remotely in ways that could compromise some states' control and visibility over their own systems or have negative effects on that country's constituents causing unrest or even chaos.

3. Public privacy, safety and critical infrastructure

The aforementioned attack methods and ongoing political debates are reflected in the pessimistic public mood when it comes to the protection of critical infrastructure. 5G will help cover more areas than is the case with today's telecommunications equipment and will provide previously non-networkable devices with connectivity and centralized management. Connected services and infrastructure is a double-edged sword that helps provide better visibility, efficiency and performance, but is making non-critical infrastructure critical and therefore exposing more of the population to unaffordable risks. The general public is being 'lulled' into welcoming the convenience and continuous visibility provided by 5G, though in the event of a disruption, public order could be at stake. A current example of this type of human dependency (addiction) can be seen in during power outages in urban areas where traffic signals are powered by portable generators and an observer can see gaggles of constituents who have plugged extension cords into the generators to charge their wireless devices. Buildings code today do not require even a single power outlet in each apartment to be connected to a whole building emergency generator that would allow occupants to remain in their apartments and charge devices and perhaps run refrigerators, etc.

In the near future, remote surgeries could be a major service offering for patients in hospitals all around the world, especially in isolated locations. An attack on such services using DDoS or something similar could endanger the lives of many. Another potential hazard is that of automated vehicles that will require live feeds of data on road services, facilities and traffic conditions. The disruption of such services could easily block roads and transportation networks and with such vehicles unlikely to have manual driving capabilities, complicating things even further. In a 5G-connected world the conventional definition of critical infrastructure will expand far beyond the traditional areas of water supply, energy grid, military facilities, and financial institutions to unprecedented areas such as traffic control systems, oil and natural gas production and delivery, etc.

On the privacy side, matters become more complex. The advent of 5G with its short range will definitely mean more cell communication towers or building antenna attachments being deployed in dense urban centers. For example, in the United State roughly 80% of its 350M population live in urban regions of the country, according to the U.S. Census Bureau. The concern multiplies when other countries are analyzed such as India or China. With the right toolset, someone could collect and track the precise location of users. Another issue is that 5G service providers will have extensive access to large amounts of data being sent by user devices which could show exactly what is happening inside a user's home and at the very least describe via metadata their living environment, in-house sensors and parameters. Such data could be manipulated and misused in some cases, or service providers may consider selling this data to other service companies such as advertisers in an attempt to open up new revenue streams.

4. [5G] security solutions

4.1. Hybrid authentication

Traditionally, authentication from 2G to 4G is a unilateral process between the telco networks and service providers on one side and the client device on the other side. Multiple authentication models exist in the 5G ecosystem and that would support business and user communication schemes.

Network authentication is only offered by network providers and is considered expensive for service providers. Network authentication liberates the user from having to authenticate for every service they need access to – a single network authentication is sufficient. Service authentication only, on the other hand, can also be provided by service providers, lowering costs and relying on proven solutions.

One recommendation for secure authentication relies on network-based authentication. In special circumstances, service providers can choose to exempt network authentication for trusted devices using their own capabilities to lower the network authentication costs. In this case, 5G network security will require flexibility for organizations to manage multiple unknown devices with various levels of security. The security requirement for lightweight IoT/M2M communication and remote surgery might be very different. Therefore, a unified hybrid framework is needed to coordinate different security methods for each security layer. Security as a service will possibly offer the basic framework to fulfill the needs of connected devices and users.

4.2. Anomaly detection

Connected devices in 5G networks will have diverse configurations and firmware software owned and developed by third parties and not traditional cellular operators. Manufacturers would probably prefer to adopt bulk configurations to ensure fast updates and patches, opening the door to compatibility problems with other devices in the network, wide-scale vulnerabilities and service interruptions. Be it massive scale misconfiguration, patch updates or DDoS, the solution is to continuously observe the behavior of connected devices.

The network administrator can establish security principles to apply on the connected devices, by class of software, role and criticality. The scale of surveillance can then be limited by employing anomaly detection tools to monitor those devices not conforming to the defined rules. In normal circumstances, the performance of IOT/M2M devices would be stable and have well-defined resource utilization patterns, common network configuration and a particular network communication scheme, meaning they would be positively perceived by other devices in the network. In addition, user population and general usage data would have traffic and communication patterns for the network administrator to model and to create thresholds. Using these attributes to set up anomaly detection parameters would help easily identify problem devices and isolate them in time.

The methodology described above could also be useful in BYOD environments, with more unknown and untrusted devices on the network. System administrators can, for example, enforce know-your-user (KYU) procedures before giving devices access to the network. Any unknown device has to be authorized to enter the network with a user ID so that the network administrator can identify a problematic user and mitigate threats in case of a security breach.

4.3. [5G] gear audit

Debates around the political affiliations of network gear manufacturers are now more heated than ever and adopting the products of a foreign country for critical infrastructure is not an easy decision. The risks to a government of partnering with an unreliable supplier are very high, while it is also unwise to ignore 5G technology in today's highly connected, globalized and competitive economy.

Under such circumstances, the UK strategy might provide a possible solution. The UK relied on a scientific approach that translated into a thorough audit of network gears and source code developed by Huawei in early 2019. The National Cyber Security Centre (NCSC) has examined Huawei's products and concluded there is no evidence of a threat to national security. Even where their products have security concerns and require improvement, it is all within the boundaries of manageable risk. This method provides a scientific and technical basis for both technology adopters and providers, avoiding political prejudice. The manufacturer can refer to the technical experts' findings to enhance their products so that they match the technical standard. Simply put our new century requires 5G deployment to embrace ‘Security by Design’ and that drum beat should be echoed by device manufacturers as well. While the planet is migrating away from fossil fuels, it at the same time should migrate away from the ideas that cyber security can simple be bolted-on when needed. Both are mid-century approaches that have failed and will continue to fail.

4.4. Regulations and regulators

Governmental and industrial regulation will be the foundation of 5G security. On the one hand, 5G network gear manufacturers must comply with industry standards and convince their customers with secure products and services. On the other hand, the situation may get complicated when it comes to the background of the 5G technology manufacturer. The methodology of the U.S. Department of Defense (DOD) approach with regards to China's dominance in 5G technology is worth noting. The authority issued a publication in early 2019 suggesting a zero-trust model. It indicates that all network infrastructures must be presumed vulnerable to cyberattacks from the encryption and resiliency perspective.

5G needs the government for its governance, though 5G will not be seen as under total government control. At the basic level, many countries will need to free up the radio spectrum that is currently used for other things such as satellite and radar systems. The spectrum allocation will hence give birth to a regulatory framework coupled with associated policy issues.

As for 5G disrupting government agencies and private company operations such as the mass use of augmented reality or artificial intelligence, regulation will be required to set rules on what decisions can be delegated to machines and when humans will need to be in control of the decision-making process. In the area of healthcare services, detection of serious conditions through remote analysis of vital signs collected by body-worn devices would require regulation on how such information is used or distributed. For autonomous vehicles, 5G is capable of enabling rapid communications among self-driving cars. However, in emergency situations, there is not much time for human involvement. Self-driving vehicles will likely have to choose between different possible outcomes, such as whether to prioritize the safety of in-vehicle passengers or the people outside of the self-driven vehicle. It will therefore be up to the government to set the ethical rules and conditions for machines to follow.

Industry 4.0 is most likely to be seen as particularly dependent on safe environments. The manufacturing arena may see an increase in the usage of customer data but with tighter data security laws such as the General Data Protection Regulation (GDPR), which could mean data breaches leading to large fines and reputational damage. Additional commercial laws can also be applied to 5G technology trading and transfer. After all, the technology is a commodity and it can be subject to quality control and the trading record of the manufacturer. A reward and penalty system could be introduced to 5G network gear manufacturers based on their security capabilities and success. Executing meaningful regulation would ensure secure products and services for a country. While 5G holds huge potential for a range of industries, government-led industry-specific regulations are still very much needed to ensure devices and networks are well secured.

5. Conclusion

The 5G telecommunications revolution is imminent. It is the next generation of cellular network using the existing 4G LTE in addition to opening up the millimeter wave band. 5G will be able to welcome more network-connected devices and increase speeds considerably for users. It will serve as the foundation for many futuristic technologies such as self-driving vehicles, remote and electronic healthcare services, energy efficiency systems, etc. Smart cities, intelligent power grids and defense facilities will be built based on all these new technologies.

However, the security concerns of 5G are inescapable. It is an evolving and developing technology built on top of the previous infrastructure, from which it will inevitably inherit vulnerabilities and misconfigurations. Large-scale DDoS attacks will likely be amplified; the massive increase in the volume of connected devices, with all the uncertainties about their quality and security in the network will be a challenging task for telco administrators. Furthermore, the communication trust model will not be identical to previous cellular generations. IoT and M2M devices are expected to occupy a greater portion of the network capacity. The interaction of all these devices in the 5G network will likely trigger unprecedented issues in product design and device behavior. In an environment plagued by such fears and the attendant political challenges, encouraging a zero-trust network model and strict product quality compliance would help build trust between the technology adopters and providers.

Government and industry leaders should join efforts to promote secure and safe 5G technology projects to enhance the services and quality of life for citizens of smart cities.

Moreover, in today's connected society, 5G will become an indispensable part of our everyday lives. It opens up opportunities that in the past would not have been possible, as we have described in this paper. There is, however, a need to manage 5G deployment risk, hence vendor diversity is crucial when it comes to 5G ecosystem offerings in order to avoid a single point of failure.

5G will be a more complex environment compared to its predecessors. In a global supply chain setting, bans based on the nationality of a provider offer little assurance especially to countries that have adopted a "banned provider" as part of its vendor diversification process. As such, a moderate approach offers a potential way forward. It is important that we do not confuse 5G cybersecurity with international trade policies driven by political sophistry.