Is 5G Ready For The Social Internet Of Things World?

Terry Schorn

Abstract: A game changer in mobile communication is presently happening today concerning affordable gigabit cellular connectivity. Gigabit connection speeds for cellular users has been a natural progression from previous technological advances in this area. We have gone through a logical progression of 2G, 3G, 4G, and now the latest and fastest option 5G. This faster 5G option will open up many new, game-changing opportunities for the commercial and residential Internet of Things (IoT) applications that rely on “always on” internet connections. Advancement in this technology brings new security concerns that “always on” internet connections present. This document will explore how 5G cellular connections have evolved with a security focus in mind. Security concerns, both present and future, are presented to the reader for consideration. Key security concerns include transition to 5G, changes in Trust Models, IoT strategies, consumer acceptance, and 5G availability. Please continue to read further for more information on how 5G will impact your future IoT strategy and how to leverage IoT applications securely and economically.

Overview:

5G will spur new wireless security worries and drive new security trust models, new service delivery models, an advanced threat landscape and an amplified emphasis for privacy. 5G systems are the next phase in the progression of mobile communication. As a crucial element of persistent internet integration, 5G networks need to offer security solutions not only for existing voice and data communication but also for future needs, including the plethora of IoT devices and application options delivered to the general public. This paper presents solutions to these challenges and directions to secure 5G systems.

Problem Statement:

Is 5G ready for business and consumers? Below are a few critical questions one will need to address when considering using a 5G network.

1. The first thing to consider before implementing 5G is what to expect from the end-of-life cellular technologies? See Figure 3 below for a timeline identifying when legacy cellular products will be phased out. Note that support for 2G and 3G devices will be ending soon for major carriers such as AT&T and Verizon.

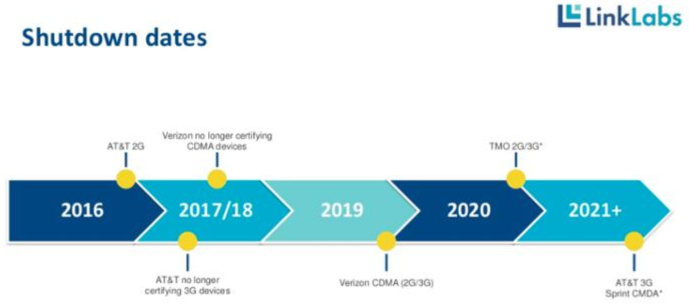


***Fig. 1** End of Life Timeline*

***Source**: (1)*

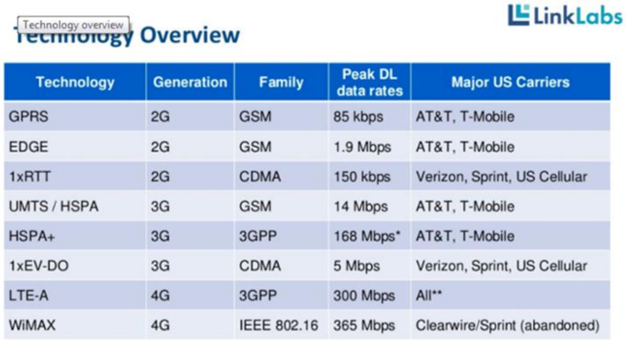
2. Another critical piece to consider is potential hardware constraints from vendors. Scrutinize all facets of your supply chain to ensure vendors continue to manufacture the hardware needed in the future. Deprecation must be considered because legacy network devices may not be available down the road as products are discontinued. Also, contact your carrier and find out if they plan to limit types of hardware that can be added to their network beyond a certain point.
3. Some devices will always need line power to perform their functions, like ATMs, electrical meters, and vending machines. Many devices that don't require line power could benefit from recent new battery-efficient technologies available today. The arrival of vanadium batteries could be a significant solution for long-term storage needed with access controls, tracking devices, and industrial monitoring devices.
4. Consideration must be addressed for device and service management as well. Many legacy devices used today were implemented close to 20 years ago. Much has changed since then regarding device and service management, requiring you to make backend modifications to support new devices such as smartphones and IIoT devices. It is paramount that folks consider modern architectural solutions as opposed to re-architecting your existing system to support new technologies. Choosing new options will provide added features and simplicity as well.
5. Trends in IoT uses and applications will require a shift in strategy on how to manage data. Innovative IoT opportunities will drive new data security paradigms. Use this time to strategize about your future IoT presence. Vendors offer similar interface modules across the various categories of LTE. For example, they're offering compatible components for Cat-1, LTE-M, and NB-IoT, so you may get a chance to consider even lower power devices than you were previously viewing.

Related Work:

Pragmatism is an important point to contemplate about 5G technology. 5G is going to require some critical re-engineering not just on the network hardware side, but also in devices. New modems and front-end radio designs will be costly and problematic to fit into current mobile form factors. These factors will most definitely hinder a quick deployment of 5G. 5G conversion requirements are in stark contrast to the Gigabit LTE conversion executed recently. Present Gigabit LTE is simple to implement, mostly scaling up existing networking LTE and Wi-Fi bands. (2). 5G is defined by 3GPP, and there are some base stations and silicon that support limited 5G features, consumer wireless routers for example. Commercial rollouts for 5G handsets are several years out. As 5G smartphones roll out, mass adoption for 5G IoT devices will evolve quickly. Transition away from legacy devices to 5G could be as far out as 2023. If gigabit capabilities are needed now, 4G LTE advanced pro may be a viable option in the interim. See Fig. 2 for transition detail.

Past Cellular Technology

Before any discussion can occur about 5G and the future of cellular technology, we must review past cellular use and technological progressions. As Fig. 2 below shows, there has been a steady progression of connection speeds from GPRS (2G) at 85 kbps to LTE (4G) at 300 Mbps. Recent LTE Advanced Pro offerings are scratching the 1 GB threshold as Fig. 3 illustrates.



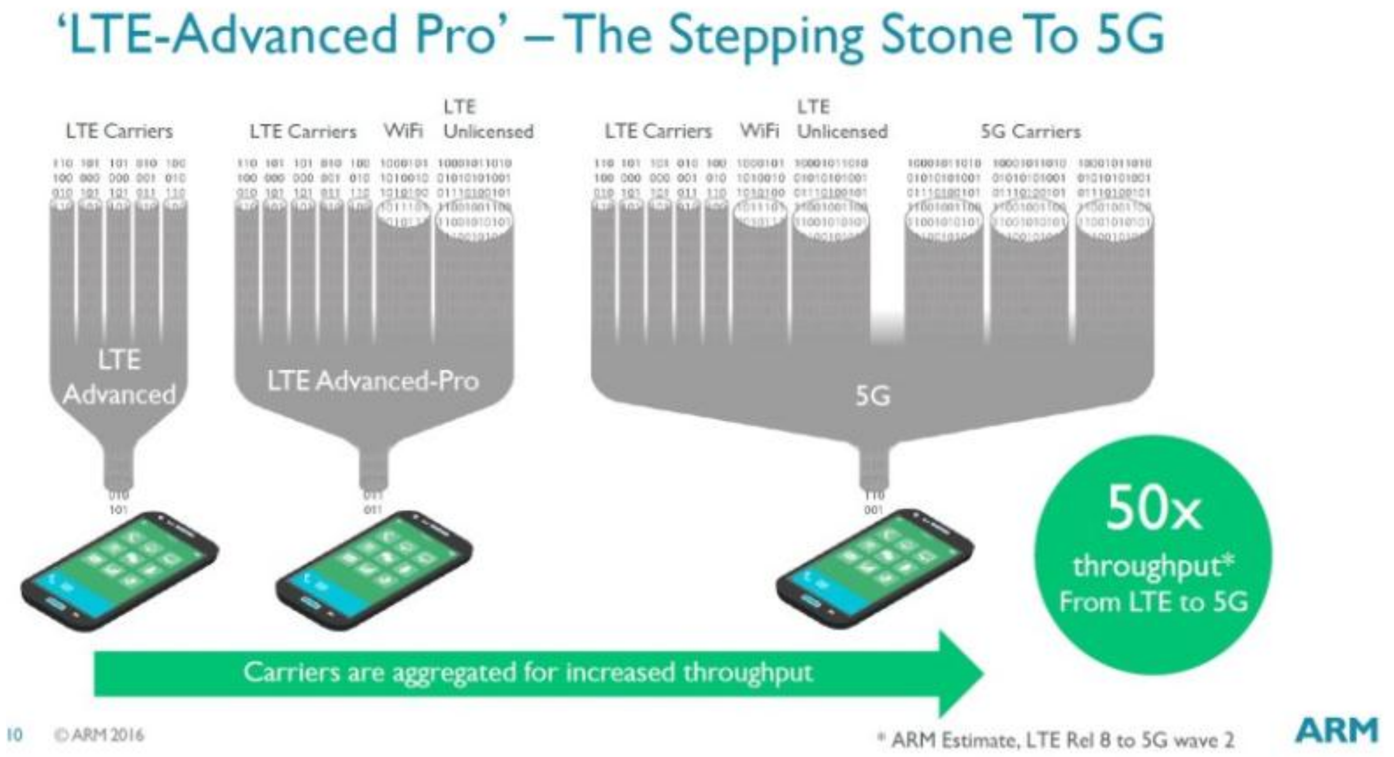
Technology overview

Technology Overview

Technology	Generation	Family	Peak DL data rates	Major US Carriers
GPRS	2G	GSM	85 kbps	AT&T, T-Mobile
EDGE	2G	GSM	1.9 Mbps	AT&T, T-Mobile
1xRTT	2G	CDMA	150 kbps	Verizon, Sprint, US Cellular
UMTS / HSPA	3G	GSM	14 Mbps	AT&T, T-Mobile
HSPA+	3G	3GPP	168 Mbps*	AT&T, T-Mobile
1xEV-DO	3G	CDMA	5 Mbps	Verizon, Sprint, US Cellular
LTE-A	4G	3GPP	300 Mbps	All**
WiMAX	4G	IEEE 802.16	365 Mbps	Clearwire/Sprint (abandoned)

Fig. 2 *Cellular Overview*

Source: *(1)*



'LTE-Advanced Pro' – The Stepping Stone To 5G

Fig. 3 *Future Cellular Options*

Source: *(3)*

Progression from 2G to 3G to LTE to 5G isn't the same as merely replacing a component. Numerous telco, ISP and security groups in the 1990s and 2000s were incredibly unique and on the cutting edge of machine learning (ML) communication. These businesses are poised well to integrate 5G technologies into their networks. Those companies that still use legacy devices in the field that have functioned well may struggle in the 5G era. It is tempting to switch out a component to keep your devices working for a short-term fix. Careful thought must be considered for a long-term product strategy. What will your business be doing for the next 10-15 years regarding IoT? Focusing on the future ensures you are positioned securely to function in an IoT world.

Present Cellular Technologies

Gigabit LTE rules the high-speed cellular space today. Present LTE will continue to provide abundant coverage and crucial services that supplement early 5G NR deployments. Fig. 4 identifies present LTE Gigabit enhancements. While these enhancements are substantial, they will only be a stop gap until 5G is fully implemented.

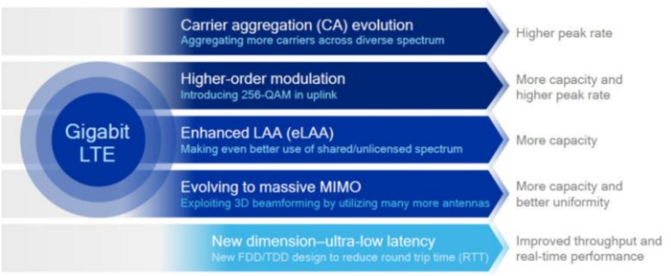

Gigabit LTE
Carrier aggregation (CA) evolution
Aggregating more carriers across diverse spectrum
Higher peak rate
Higher-order modulation
Introducing 256-QAM in uplink
More capacity and higher peak rate
Enhanced LAA (eLAA)
Making even better use of shared/unlicensed spectrum
More capacity
Evolving to massive MIMO
Exploiting 3D beamforming by utilizing many more antennas
More capacity and better uniformity
New dimension–ultra-low latency
New FDD/TDD design to reduce round trip time (RTT)
Improved throughput and real-time performance

Fig. 4 *LTE Gigabit*

Source: *(4)*

Future Cellular Technologies

The mobile industry is bustling about the next generation of high-speed wireless service termed 5G. Fig. 5 depicts how a typical 5G network might look. This could take a few years as the conversion to 5G will roll out slowly. Carriers have to upgrade their massive 4G infrastructure, which will take extensive time. 5G is about more than just transferring Gigabits of data to and from your smartphone more quickly. It's an information conduit built with the potential to link self-driving cars, VR headsets, delivery drones, and billions of IoT devices inside the home and small office. 5G performance and a rich feature set could spell the end for landline services and related devices. As Fig. 6 indicates, 5G NR mmWave can provide 10 GB connection speeds. IoT home devices (Appliances, energy-saving features, personal assistants, robots, etc.), will function adequately over a 5G network without the need for wired modems, switches and routers.

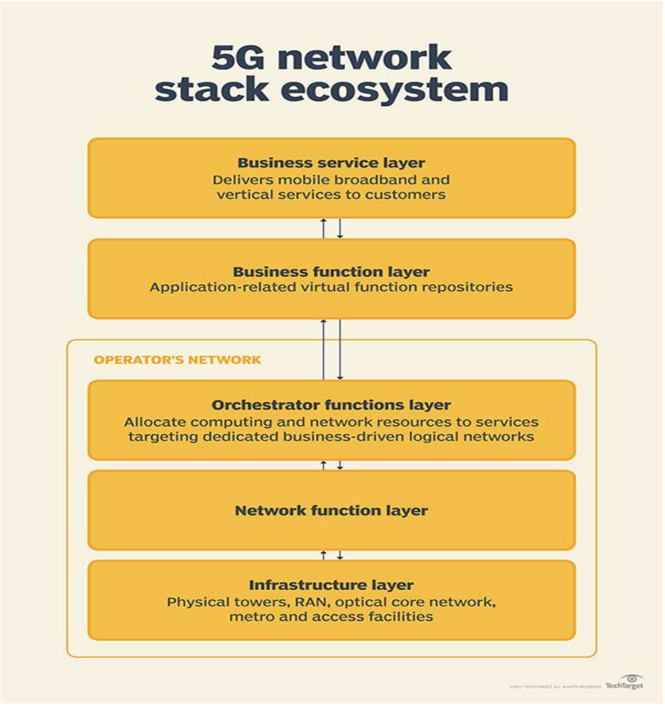

5G network stack ecosystem
Business service layer
Delivers mobile broadband and vertical services to customers
Business function layer
Application-related virtual function repositories
OPERATOR'S NETWORK
Orchestrator functions layer
Allocate computing and network resources to services targeting dedicated business-driven logical networks
Network function layer
Infrastructure layer
Physical towers, RAN, optical core network, metro and access facilities
TechTarget

Fig. 5 *5G what is it?*

Source: *TechTarget.com*

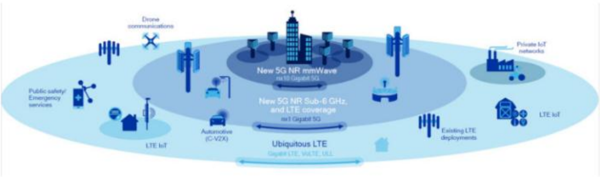


Fig. 6 *Gigabit 5G*

Source: *(4)*

Analysis

Trust Models

A solid framework for an IoT trust model should build transparency and individual choice into IoT security. (5) For IoT security to be effective, individuals must trust IoT device operations are secure, safe, and private. Consumers and employees will need to safely, and instinctively interact with a vast number of multifaceted, and associated IoT devices. 5G IoT at this massive level will bring an assortment of threats to individuals and society as a whole. Disorganized engineering of IoT systems that combine physical and digital worlds today must advance. We are poised to impose failed trust models onto the 5G IoT world unless new trust models are developed.

Attack Surfaces

As you can see in Fig. 7, mobile devices will constitute a much higher threat in 5G networks. Threats can originate from a variety of sources such as Edge Cloud, Macro and Micro Cells, Edge Devices, and Flash Networks. As high-speed 5G access, takes hold, folks will demand mobile apps to do more routine tasks such as banking, shopping, etc. Mobile apps are focused and targeted, and they have to complete requests quickly. Mobile device use will accelerate, especially with the addition of wearable technology. Endpoint security will be crucial to ensure secure communications. Most mobile apps today do not sufficiently guard against tampering. Applications incorporate platform-specific best practices but do not guard against attacks across the device, network, and application tiers. There has been a surge in the number of malware and phishing attacks on smartphones to steal valuable customer data. Banking information, for example, can be stored on smartphone payment apps. This type of malware enables hackers to steal login information by targeting apps using malware that spoofs the legitimate apps screen. (6)

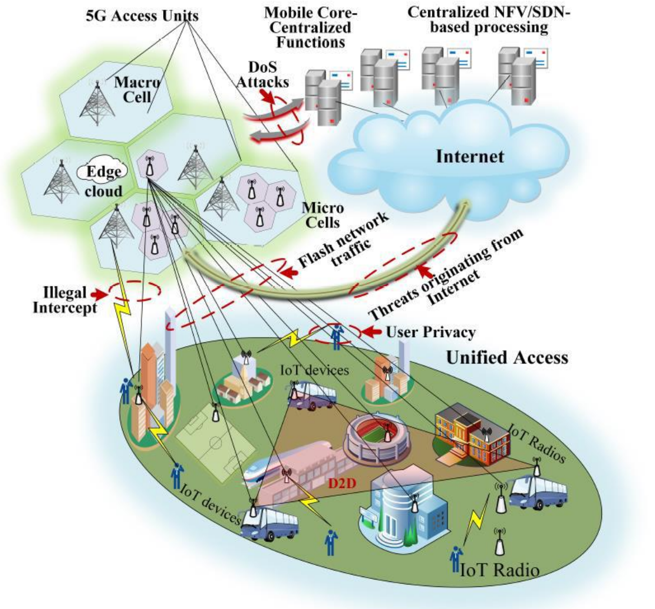


Fig. 7 *5G Mobile Attack Surfaces*

Trust-Based – Social Aware Solutions (User plane integrity)

A plane, relating to networking, is one of three essential mechanisms of a telecommunications structural design. Three plane elements include the data plane, the control plane, and the management plane. These planes can be thought of as diverse areas of processes. Each plane transmits a different type of data traffic and is hypothetically a communications network that runs autonomously on top of each other, still supported by its infrastructure. (7) See Fig. 8 for detail. [The data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) carries the network user traffic. The control plane carries signaling traffic. Control packets originate from or are destined for a router. The management plane, which carries administrative traffic, is considered a subset of the control plane. In conventional networking, all three planes are implemented in the firmware of routers and switches. Software-defined networking (SDN) decouples the data and control planes, removes the control plane from network hardware and implements it in software instead, which enables programmatic access and, as a result, makes network administration much more flexible. Moving the control plane to software allows dynamic access and administration. A network administrator can shape traffic from a centralized control console without having to touch individual switches. The administrator can change any network switch's rules when necessary -- prioritizing, de-prioritizing or even blocking specific types of packets with a very granular level of control.] (7) Fig. 8 shows the user plane protocol stack of a classic configuration. Notice how radio access uses protocols MAC, RLC, and PDCP. The user plane portion of the S1 interface is built on the GPRS Tunneling Protocol (GTP). GTP uses a tunneling process guaranteeing IP packets meant for a given UE are supplied to the eNodeB. GTP encapsulates the original IP packet into an outer IP packet addressed to the proper eNodeB. The S1 interface can be run over several Layer 1/Layer 2 technologies, e.g., fiber optic cables, leased (copper) lines or microwave links. Fig. 8 demonstrates how sample TCP/IP-based web browsing operates as well. The matching peer objects function in the UE and at the server hosting the web application. Peer protocol objects of the server are drawn in the Serving Gateway (S-GW) for simplicity.

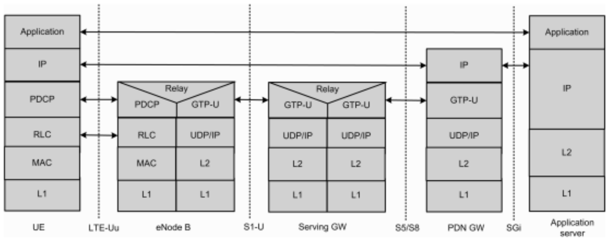


Fig. 8 *User Plane End to End Protocol*

Source: *(8)*

The control plane protocol function is to control the radio access bearers and the connection between the UE and the network, i.e., signaling between E-UTRAN and EPC (Fig. 8). The control plane consists of protocols for control and support of the user plane functions:

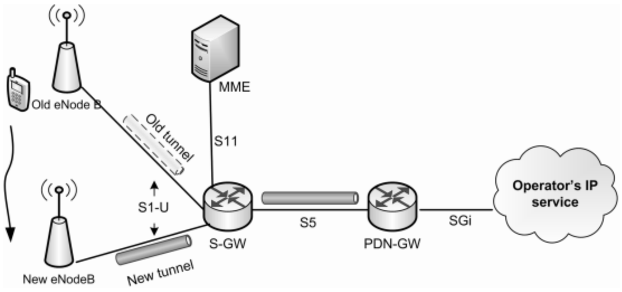


Fig. 9 *GTP Tunneling*

Source: *(8)*

2G security provides no integrity security of user plane data or control plane data. User plane data is encrypted delivering limited protection against a Man-In-The-Middle attack. Altering data in transit can occur since encryption is linear (a stream cipher) making checksums linear as well. 3G and 4G include partial cryptographic integrity security for signaling messages but not for user plane data. Data integrity is applied at the transport or application layer. This includes additional encryption options. [In special cases, bearer layer integrity (plus encryption) may represent a lower overhead solution, provided the security end-points are appropriately aligned with the service end-points. A bearer security API (supported on the device or within the network, or ideally both) might allow a service to request that a particular security configuration is used (e.g., request integrity is switched on, require a particular end-point), and also check what bearer security is in place.] (8) With 5G Device-to-Device (D2D), content uploading requires reliability and repudiation demonstrating the level of trust you would find in enterprise network environments. Taking a page from new Social Internet of Things (SIoT) modeling, social-awareness of a device must be acknowledged as a crucial factor to define the trustworthiness of a device.

Trust-based and social-aware solutions can assure higher upload gains and security for the devices using D2D-based content uploading. (9)

Mandated security in the network

5G will use novel technological models to meet the requirements of broadband access everywhere, high user and device mobility, and connectivity of massive numbers of IoT devices. 5G security models will include things such as Software Defined Networking (SDN), Network Function Virtualization (NFV) and Mobile Edge Computing, drawing on improvements in cloud computing. Securely using these technologies and providing user privacy will be a serious concern. Mandated security in a 5G environment can assist in satisfying reliability and repudiation. The new Social Internet of Things (SIoT) paradigm, social-awareness of the devices, is identified as a critical trust model to define 5G security. [The objectives being pursued by the Social Internet of Things (SIoT) paradigm are clear: to keep separate the two levels of people and things; to allow objects to have their own social networks; to allow humans to impose rules to protect their privacy and only access the result of autonomous inter-object interactions occurring on the objects' social network.] (10)

Trusted Machine Identities

There are more machines and devices online than people today, spurring increased demand for trusted machine identities. Businesses need to know how to use machine credentialing and manage demand securely. One existing foundational technology, public key infrastructures (PKIs) can provide the framework to manage digital certificates for people, machines, and device credentialing at a high volume. IoT demands solutions that will require careful planning and a chain and root of trust you can rely on. A few key things to consider to support machine credentialing should include:

- What is the role of PKIs in the new IoT environment
- How IoT proliferation increases demand on PKIs
- Why crucial orchestration and lifecycle control is vital
- Root of trust must be recognized to guarantee security

Consumer acceptance:

The advent of high speed and affordable 5G access will change the customer experience in varied ways. Customer Experience Management is one such paradigm change. Adobe® announced a novel customer experience construct called "customer experience system of record" that pulls in information, not just from Adobe tools, but wherever it lives. (11) This new construct will provide a positive user experience making it a front and center IoT marketing strategy. Salesforce®, with its cloud services for sales and marketing, is also working on a similar IoT marketing strategy. They are tapping the data integration layer to access client information from across the enterprise software stack, whether on-premise, in the cloud or inside or outside of Salesforce. This strategy will fit well with the “always on” mobile user needs of the future. (12) As 5G and IoT demands challenge traditional social network security models, it is imperative to experiment with alternatives. A great example of an alternative social network security model in use is a new startup called Arbtr®. It provides a social network that limits users to share a single thing at any given time, which cuts down on endless feeds filled with irrelevant information. (13) New types of customer experience systems such as this will path the way for security models of the future. Existing and future Smart Cities can take advantage of 5G networks as well. A Smart City is a city that integrates diverse kinds of data gathering sensors to stream information used to manage resources resourcefully. This could include data acquired from humans, devices, and other resources. The smart city model assimilates IoT info and various physical devices connected to the network, to enhance city functions. As you may realize, collecting data at this magnitude will require added security from the source. New York City is introducing cybersecurity app options to guard citizens against malicious online threats, particularly on mobile devices. (14) This strategy could be expanded to include all IoT data sources using a 5G network.

How 5G connectivity and new technology could pave the way for self-driving cars

As 5G matures and is widely available, Vehicle-to-everything (V2X) capabilities will be unlimited. [V2X communication is the passing of information from a vehicle to any entity that may affect the vehicle. It is generally referred to as "cellular V2X" (C-V2X) to differentiate itself from the 802.11p based V2X technology. C-V2X enables vehicles to communicate, which should reduce accidents and aid autonomous driving] (15).

Please see Fig. 10 for detail.

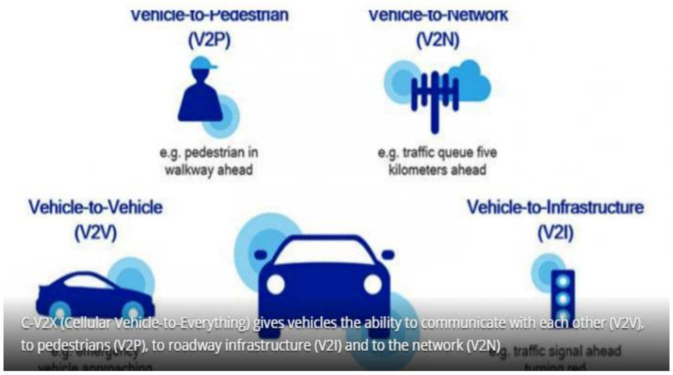

Vehicle-to-Pedestrian
(V2P)
e.g. pedestrian in walkway ahead
Vehicle-to-Network
(V2N)
e.g. traffic queue five kilometers ahead
Vehicle-to-Vehicle
(V2V)
Vehicle-to-Infrastructure
(V2I)
e.g. emergency vehicle approaching
e.g. traffic signal ahead turning red
C-V2X (Cellular Vehicle-to-Everything) gives vehicles the ability to communicate with each other (V2V), to pedestrians (V2P), to roadway infrastructure (V2I) and to the network (V2N)

Fig. 10 *V2X Options*

Source *(15)*

Cars could be safer and more efficient if they could, network with traffic lights, be alerted to walkers, or communicate with each other. C-V2X, a peer-to-peer wireless technology, can alert vehicles about potential items that cameras and radar might not catch, connecting them to their surroundings in a way that could eventually help them drive themselves. C-V2X is a likely beneficiary of 5G networking. Qualcomm, a leading player in C-V2X, publicized the first-ever U.S. deployment in cooperation with Ford® and Panasonic®. "Recent field test results show a significant range, reliability, and performance advantage of C-V2X direct communications, with more than twice the range and improved reliability compared to 802.11p radio technology," according to Qualcomm. (16) Using cellular networks, C-V2X can benefit on the continuous enhancements these operators make, 5G in particular. Under C-V2X, short-range communications between adjacent vehicles happen automatically, without relying on any cellular connection, but cars can also connect to adjoining mobile networks via 5G, enabling it to communicate with cars located farther away. (17). Recent C-V2X demos, which took place in Colorado on August 14, 2018, also coupled vehicles to traffic lights, enabling drivers to anticipate when stop lights would change color. Future enhancements include illuminated instruction turn lanes, route data between vehicles and bridges, toll booths, construction signs, and other shoulder infrastructure. Other applications that could benefit from 5G include drones such as Skydio® self-flying cameras. (18). Video surveillance cameras for security purposes can now be more mobile as well.

Industrial (IIoT)

As Industrial Internet of Things (IIoT) applications expand and become ubiquitous on shop floors and factories, issues with security become critical. Significant benefits can be gained from connecting systems and sensors on the factory floor to corporate networks, and multiple sites. IIoT applications bring cost savings and direct access to factory data. IIoT applications could jeopardize corporate networks due to weak or non-existent security controls, however. IIoT applications must be secured to prevent, intrusions, potentially negating the benefits. There are two areas of vulnerability. The first is a disruption of operations. The second is data loss. When implementing IIoT in industrial environments, standard solutions to protect infrastructure, as well as solutions that can be embedded in the protocol stack of the devices themselves, are required. (19)

Global Positioning System GPS

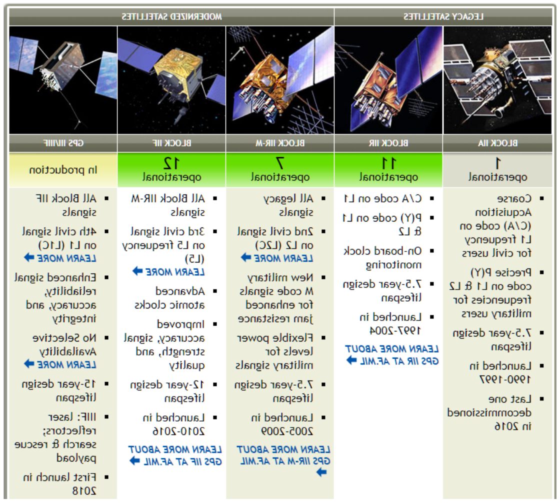
GPS stands for Global Positioning System. There were a total of 31 operational satellites in the GPS constellation, not including the mothballed, on-orbit standbys. The satellites communicate with specific receivers on the ground, providing the exact position of the receivers. It takes a minimum of 24 satellites to make a Global Positioning System. The Russians have one called GLONASS, the Europeans have one called Galileo, and the Chinese have one called BeiDou Navigation Satellite System (BDS). [Put in place by the US military starting in 1989, the GPS satellite constellation transmits a signal for its use and a separate signal that anyone with the technological wherewithal is free to access. Access to this signal has allowed manufacturers to integrate the technology into their products. GPS satellites are constantly transmitting a signal toward the Earth, which includes their exact position and the precise time as measured by an atomic clock. Receivers pick up these transmissions, calculate how long it took the signal to reach them, and measure that against their internal clock. By picking up a signal from at least three satellites, the device can then Fig. out exactly where it is using a process called trilateration: "If satellites are here, here, and here, I must be here." The only information that is transmitted by a GPS satellite is its trajectory, along with those of all the other satellites in use, and the exact time of the transmission. The receiver then uses this information to calculate its position in 3-dimensional space as a set of coordinates.] (20)

The Satellite Blocks, Current and Future

Currently, there are five types of functioning satellites in the GPS constellation, known as Blocks. There is one active IIA satellite in use (military), 11 IIR satellites (military, emergency response and commercial), 7 IIRM satellites (Military, commercial), 12 IIF satellites (military, commercial, emergency response), 1 GPS III/IIF (Military, Commercial). Please see Fig. 10 for detail. The orbiting IIR and IIF are the core of today's Global Positioning System. GPS III satellites are poised to take on the projected burden of IoT devices coming online in conjunction with the 5G rollout in 2019. The first GPS III satellite has been delivered to Florida for launch in December 2018 on a SpaceX rocket.

GPS embedded in everything – Basics to human implants

Though Global Positioning System (GPS) was only science fiction until just a decade ago, devices using GPS technology is all-encompassing today. GPS is used in cars, phones, social media, and computers. It is used to keep us safe, for loss prevention, increase productivity, and to keep time. Dreamers and Hollywood producers have provided a lot of misconceptions about GPS, and functions of global positioning overall. Trackers as small as a pea do not exist at this time of writing but stay tuned. The only portion absent to bring GPS to realization for embedded trackers/receivers is a reliable source of power. Though receivers can be as small as a grain of rice, the battery tech is not there. When all the pieces are in place, embedded GPS uses will explode, and 5G will be the preferred network platform to connect these devices.



LEGACY SATELLITES		MODERNIZED SATELLITES		
BLOCK IIA	BLOCK IIR	BLOCK IIR-M	BLOCK IIF	GPS III/IIIF
1 operational	11 operational	7 operational	12 operational	In production
▪ Coarse Acquisition (C/A) code on L1 frequency for civil users ▪ Precise P(Y) code on L1 & L2 frequencies for military users ▪ 7.5-year design lifespan ▪ Launched in 1990-1997 ▪ Last one decommissioned in 2016	▪ C/A code on L1 ▪ P(Y) code on L1 & L2 ▪ On-board clock monitoring ▪ 7.5-year design lifespan ▪ Launched in 1997-2004 LEARN MORE ABOUT GPS IIR AT AF.MIL ⬅	▪ All legacy signals ▪ 2nd civil signal on L2 (L2C) LEARN MORE ⬅ ▪ New military M code signals for enhanced jam resistance ▪ Flexible power levels for military signals ▪ 7.5-year design lifespan ▪ Launched in 2005-2009 LEARN MORE ABOUT GPS IIR-M AT AF.MIL ⬅	▪ All Block IIR-M signals ▪ 3rd civil signal on L5 frequency (L5) LEARN MORE ⬅ ▪ Advanced atomic clocks ▪ Improved accuracy, signal strength, and quality ▪ 12-year design lifespan ▪ Launched in 2010-2016 LEARN MORE ABOUT GPS IIF AT AF.MIL ⬅	▪ All Block IIF signals ▪ 4th civil signal on L1 (L1C) LEARN MORE ⬅ ▪ Enhanced signal reliability, accuracy, and integrity ▪ No Selective Availability LEARN MORE ⬅ ▪ 15-year design lifespan ▪ IIIF: laser reflectors; search & rescue payload ▪ First launch in 2018

__Fig. 11__ GPS Satellite Block List

Source: *(21)*

Practical Applications

The most common non-government use for GPS devices is in-vehicle navigation systems found in automobiles and agricultural equipment. These systems are sold as standalone devices and are frequently incorporated into cell phones, cars, trucks, and tractors. Coordinates will be accurate to within a few yards under optimal conditions. To date, GPS receivers are only provided coordinates by the satellite block. The navigation device itself converts coordinates into a readable address for the consumer to use. Modern devices, such as smartphones, will connect to a mapping system on the Internet, transmit the coordinates they receive to a mapping program, and get addresses back. Note that with the advent of 5G, internet mapping will be ubiquitous with downloaded maps being deprecated and obsolete. GPS tracking devices operate in the same manner; instead of displaying information, however, data is transmitted to a server via the Internet. Servers host a platform that users can access to view the device's current and past locations, and often other information, like speed. In the case of agriculture use, a grid map is saved to be reused as needed. Devices transmit their data using a local cellular network to mitigate costs, but some send out a satellite signal, allowing for use anywhere in the world. The advent of affordable 5G worldwide will minimize the need for direct satellite connections in all but extreme cases. As 5G becomes widely available, GPS usage will increase exponentially.

Where is This all Going?

Global Positioning Systems will be expanded and enhanced as time goes by. Integration with numerous satellite navigation systems will allow for quicker communications and more precise responses. The fundamental need for future systems will be making Global Positioning Systems more global. With the projected launch of the GPS III block, coverage over regions will bring more reliability and precision. Where we go beyond the GPS III block is still a mystery, but continued expanding of coverage worldwide will be the primary emphasis and 5G networks will be a critical delivery system for this technology. As for personal GPS use, no one predicted the extensiveness of activity trackers and the practical applications of cellular-based tracking and maps. Ten years ago the idea of billions of people monitoring their locations and movements in constant real time was doubtful. As this technology becomes more pervasive, with continued improvements in augmented and virtual realities, folks will be interacting with GPS in ways no one can fathom at this time. With this in mind, consumer communications, coupled with population growth, will drive advancement in our Global Positioning System's infrastructure. (20)

API Platform Development

New advances in social technologies put the consumer front and center of growth plans, creating the necessity to redefine business models. Consumers are now a potential piece to the distribution of product and play a key role in providing added value to products. What this means is, businesses using API platform development strategies are facilitating specific roles and transactions rather than owning the product. Think of Facebook®, Twitter®, and Snap Chat® for example. This new API model positions businesses well for the IoT “always on” environment 5G brings to the table. API platform development will excel at building applications where customer groups are stimulated to create, curate, and consume in an ecosystem of collaboration, open innovation, and non-linear transactions. (22)

Conclusion:

A decade ago phones weren't computers, and your home speakers only played sound. Life has become a little easier today with our beloved IoT devices such as Alexa™, Echo™, etc. All that ease comes at a price regarding security. All around us computers are executing everyday functions we never thought possible. They’ve become weathermen, cashiers, pilots, etc., eliminating work of humans. This paper identified how device connectivity, in addition to a fundamental gap between 5G technology and security, are driving significant cybersecurity challenges. New solutions to building resilience and evolving the way we approach automation with security in mind were presented. We as a society need to continue to develop technology that works in conjunction with humans that meet our needs securely and practically.

Bibliography

[1]. Link Labs. The CDMA Sunset & Its Impact On Your IoT Strategy. LinkLabs Home Blog. [Online] 2 18, 2018. https://www.link-labs.com/blog/cdma.

[2]. Gigabit LTE. Android Authority. [Online] March 2018. https://www.androidauthority.com/5g-vs-gigabit-lte-843341/.

[3]. Werdmuller, Neil. ARM Cortex-R8 paves way to LTE-Advanced Pro and 5G. https://community.arm.com. [Online] 2015. https://community.arm.com/processors/b/blog/posts/arm-cortex-r8-paves-way-to-lte-advanced-pro-and-5g?CommentId=ae27c3f9-6d59-4367-ab4c-bdf4808e242b.

[4]. Triggs, Rober. Gigabit LTE: The Diferences Explained. Android Authority. [Online] March 2018. https://www.androidauthority.com/5g-vs-gigabit-lte-843341/.

[5]. All, IoT For. How Do You Ensure Trust in IoT? IoTForAll. [Online] June 2017. https://medium.com/iotforall/human-centric-trust-model-for-iot-a98c04fceec1.

[6]. Singal, Nidhi. New attack vectors targeting mobile devices pose emerging risks:. Business Today. [Online] 3 19, 2018. https://www.businesstoday.in/latest/trends/new-attack-vectors-targeting-mobile-devices-pose-an-emerging-risk-manjunath-bhat-gartner/story/272979.html.

[7]. TechTarget. Plane In Networking. TechTarget WhatIs.com. [Online] 1 2013. https://whatis.techtarget.com/definition/plane-in-networking.

[8]. NGMN. 5G Security Recommendations. NGMN. [Online] May 2016.

https://www.ngmn.org/fileadmin/user_upload/160506_NGMN_5G_Security_Package_1_v1_0.pdf.

[9]. Militano, Leonardo. Trust-based and social-aware coalition formation game for multihop data uploading in 5G systems. Science Direct. [Online] August 2016. https://www.sciencedirect.com/science/article/pii/S1389128616302432.

[10]. ATZORI, LUIGI. Social Internet of Things. Social Internet of Things. [Online] 8 1, 2018. http://www.social-iot.org/.

[11]. Adobe. Adobe Insights. [Online] 2018. https://www.adobe.com/insights/experience-system-of-record.html.

[12]. Miller, Ron. IoT Devices Could be the Next Customer Data Fontier. Tech Crunch. [Online] March 2018. https://techcrunch.com/2018/03/30/iot-devices-could-be-next-customer-data-frontier/.

[13]. Coldewey, Devin. Arbtr wants to create an anti-feed where users can only share one thing at a time. Tech Crunch. [Online] March 2018. https://techcrunch.com/2018/03/31/arbtr-wants-to-create-an-anti-feed-where-users-can-only-share-one-thing-at-a-time/.

[14]. Hatmaker, Taylor. New York City is Launching Cyber Tools. Tech Crunch. [Online] March 2018. https://techcrunch.com/2018/03/29/nyc-secure-new-york-cybersecurity-app-de-blasio/.

[15]. Kinney, Shaun. RCR Wireless News. What is CV2X? [Online] https://www.rcrwireless.com/20180601/network-infrastructure/what-is-c-v2x-tag17-tag99.

[16]. Qualcomm. Panasonic, Qualcomm and Ford Join Forces on First U.S. Deployment for C-V2X Vehicle Communications in Colorado. Qualcomm. [Online] June 2018. https://www.qualcomm.com/news/releases/2018/06/01/panasonic-qualcomm-and-ford-join-forces-first-us-deployment-c-v2x-vehicle.

[17]. Woyke, Elizabeth. How 5G connectivity and new technology could pave the way for self-driving cars. MIT Tech Review. [Online] August 2018. https://www.technologyreview.com/s/611883/how-5g-connectivity-and-new-technology-could-pave-the-way-for-self-driving-cars/.

[18]. Trew, James. Skydio R1 review: The ultimate follow-me drone comes at a price. EnGadget. [Online] April 2018. https://www.engadget.com/2018/04/02/skydio-r1-review/.

[19]. Giokas, Louis. Industrial Internet of Things (IIOT). Design News. [Online] September 2018. https://www.designnews.com/continuing-education-center/security-industrial-internet-things-iiot.

[20]. Brickhouse Security. GPS is Ready for it's Closeup. Brickhouse Security. [Online] 2017. https://www.brickhousesecurity.com/gps-trackers/how-gps-works/?gclid=EAIaIQobChMI__e7gqnl3AIVRdbACh3lGgRxEAAYAiAAEgKxlPD_BwE.

[21]. Space Segment. GPS.gov. [Online] August 2018. https://www.gps.gov/systems/gps/space/.

[22]. FISHER, RHYS. What Exactly is an API Platform? A Competitive Edge That's What! Nordic APIS. [Online] 2014. https://nordicapis.com/what-exactly-is-an-api-platform-competitive-edge/.

[23]. Glen Shatz. 2G.3G,4G Sunsets. LinkLabs. [Online] 2018. https://www.link-labs.com/2g-3g-cdma-sunset-webinar.

[24]. ATZORI, LUIGI. When Things Get Smart The Internet of Things Gets Social. Social Internet of Things. [Online] http://www.social-iot.org/.

[25]. Schreiner, Erin. Effects of Mobile Phones on Students. Sciencing. [Online] April 2018. https://sciencing.com/effects-mobile-phones-students-5977357.html..

[26]. Yu, Jonny. City buses use Cloudian storage for video data. TechTarget. [Online] https://searchstorage.techtarget.com/news/252450229/City-buses-use-Cloudian-storage-for-video-data?track=NL-1822&ad=923518&src=923518&asrc=EM_NLN_101615023&utm_medium=EM&utm_source=NLN&utm_campaign=20181009_City%20buses%20use%20Cloudian%20object%20storage.

[27]. Social Internet of Things. Social Internet of Things. Social Internet of Things. [Online] http://www.social-iot.org/.