isentia

5G: Innovation, disruption and opportunity ahead

isentia.com

curiosity innovation

In a 5G business environment, security is necessary for the continuity of a business.

We know in earlier mobile generations, there was continuity of (perceived) security and privacy, however the security mechanisms to combat the 5G network may be different therefore jeopardising the trust placed with the 5G network. As a result, it is thought, the same security features used in legacy systems would be insufficient as 5G brings new requirements and challenges with privacy leakage being one of them.

In this report, we delve into the evolution of the mobile network, the factors driving the move to 5G, understand the benefits of its deployment as well as its challenges, including the concerns around security threats and a global leading tech giant, being at the forefront of an alleged security breach.

Evolution of the mobile network

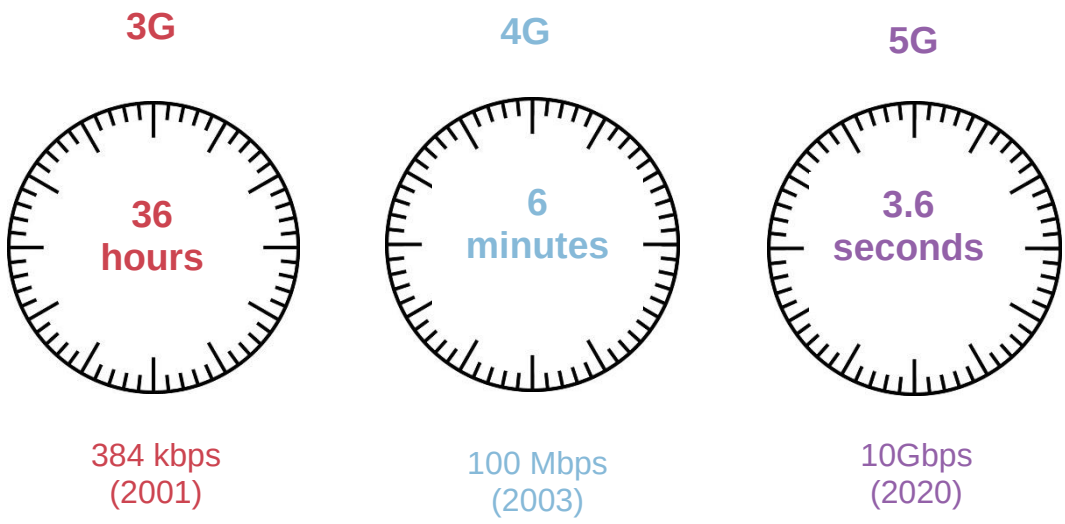
The telecommunications industry is a rapidly changing arena and is a key enabler for productivity and efficiency. 5G is the next innovation of the mobile network evolution and is set to transform the way we experience technology.

Here we look at the progression and advancements of each network generation:

- 1G brought voice to a mobile platform
- 2G introduced text
- 3G delivered higher speeds and enabled music and video streaming
- 4G or Long-Term Evolution (LTE) brought up to 10-times higher speeds than 3G
- 5G developments in mobile computing with faster download speeds, low latency, the ability to enable self-driving car, advancements in A.I, remote healthcare and more.

The below depicts the advancements of each mobile network generation, with an astounding difference in download speed for a two-hour movie from 3G to 5G.

The comparison of download time between generations



What's driving the push to 5G?

A 5G connected world is just over the horizon and will greatly impact and revolutionise the Internet of Things (IoT). In its simplest form, the Internet of Things is the concept of connecting any device to the Internet or to each other via the internet. These could include mobile phones, computers, tablets, headphones, washing machines, cars, refrigerators or just about any appliance you can think of. The Internet of Things is the connected network of these devices and can be between people, people and things or things and things.

By continuing to develop the IoT, it will enable 5G to unlock the full potential of leading trends in technology and deliver an innovative combination of speed, energy efficiency and responsiveness – which will then have a flow on effect to the IoT and will impact the following stakeholders:

- **For the innovator**, 5G will improve the capability and reliability of current products as well as invent new services and provide greater accessibility. It will provide global connectivity in the most remote and challenging areas of the world, whether it's on land, air or at sea.
- **For the manufacturer**, 5G will streamline operations and provide better efficiencies in factories and warehouses.
- **For the consumer**, having the 5G network in place will allow IoT to become more accessible and provide limitless connectivity.[1]

Benefits of 5G and IoT[2]

5G is set to deliver a more IoT friendly ecosystem, with vast improvements over the current capabilities of the 4G network, these include:

- 100x faster transmission speeds - strengthening network performance.
- Lower latency – improving device connections, application delivery and responsiveness. Latency refers to the end-to-end travel time it takes for data or commands to travel across the network.
- 1,000x greater data capacity – providing improved support to simultaneous device connections.
- Better user experience through enabled value-added services.[2]

1 https://www.iselect.com.au/internet/5g-australia/5g-internet-of-things/
2 https://blog.radware.com/security/2018/08/mobile-network-attacks/

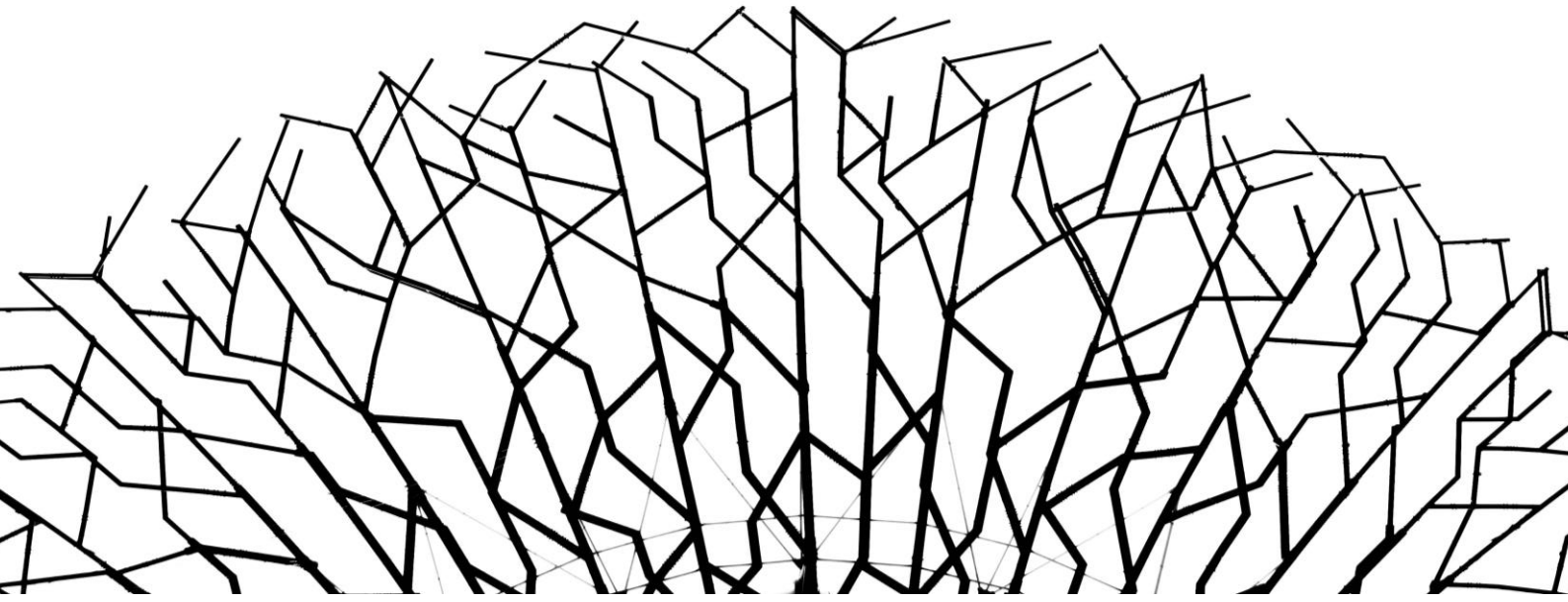
5G will mark a key step forward to progressing society and will impact and benefit many industries with its low latency and high data transfer speeds.

Healthcare will be greatly impacted, including faster transfer of large patient files and improved assistance with remote surgery in terms of patient monitoring via IoT devices. With such low latency, world class healthcare services like remotely performed surgeries will become a possibility. Although these are great operational benefits in healthcare, they also increase the risk of security breaches, medical identity theft and invasion of health privacy. This is where data management is crucial and strong security is required more than ever.

Self-driving cars will become a more widely used product. Sensors on these intelligent cars will generate a large amount of data, including measuring weather conditions, traffic conditions, obstacles and GPS locations and will also be heavily reliant on real time transmission of data to provide an optimum service.

Smart cities will be enabled as a result of smart initiatives from water and waste management, traffic monitoring and enhanced healthcare technology. 5G will enable the ability to facilitate the large amounts of data required, it will also enable the integration of various intelligence systems that will continuously be communicating with each other – providing a truly connected city.

Retail will be positively impacted as customer engagement and experiences can be simplified through mobile devices. New and innovative ways of customer engagement incorporating Augmented Reality and Virtual Reality will not only become more popular but become the norm. 5G will enable retailers to drive omnichannel retail practices more effectively and enhance the customer experience.



New capabilities. New Security Concerns

One of the defining features of 5G networks is that it relies heavily on network virtualisation giving operators the ability to serve up custom network slices - providing specific customers, verticals, applications etc., a simulation of a telecommunications network.

With new “things” (or devices) being deployed everywhere, they are disrupting the attack surface. Gartner forecasts there will be 20.8 billion connected things by 2020 and on average, there will be seven IoT devices per person come 2025.[3] The IoT is creating a great digital future where interactions between things we wear, touch or utilise become integrated into the digital ecosystem. However, as IoT grows, security risks grow with it and its implementation means all connectivity and services need to move to the cloud, resulting in a haven for attacker to target IoT. This is due to:

- Embedded devices are easily exploitable (especially if using default credentials)
- Always on devices are available 24/7, 365 days per year
- IoT devices are rarely monitored and poorly maintained, making it easy for hackers to shut down or overrun a large number of devices

Can mobile service providers create a secure environment that protects customers’ data and devices?

The 5G network supports a large number of connected devices and enables a huge increase of bandwidth over wireless broadband communication or Long Term Evolution (LTE). While concerns have been raised with the security of the 5G network, in more recent months, a leading global provider of information and communications technology (ICT) infrastructure has been at the forefront of various allegations including espionage, intellectual property theft and security vulnerabilities in its software which has resulted in the billion-dollar company being banned from usage in the several countries including access to Android giant’s Play Store – resulting in a decline in smartphone shipments and significantly reduced forecast revenue.

3 https://www.gartner.com/smarterwithgartner/the-internet-of-things-is-shifting-hackers-targets/

So, who holds the solution?

With security and cyber-attacks being the main concerns and many fingers being pointed, who holds the solution to this problem? Below we outline some key stakeholders who will be at the forefront:

Device manufacturers – IoT device manufacturers are focused on delivering solutions customers want at the lowest possible costs whilst also achieving the highest possible margins. If extra security features are added it simply increases development time and cost and therefore there is little regulatory control.

Enterprises – implementing endpoint protection security solutions and enforce a strict list of devices to be used within the business could assist with security issues.

Service providers – While they don't own the emerging 5G issues, it is ultimately up to the operators to deal with and mitigate attack traffic.

Are there associated health risks?

As the 5G network is unlike current and previous spectrum used, small cell towers need to be erected to redirect the 5G millimeter waves as they do not pass through solid objects very well and are very susceptible to interference. Due to these cell towers, some concerns have been raised around the radiation waves these towers emit and if there is any correlation between the technology and the health of people – this is still yet to be proven.

The alleged risks of having these towers throughout cities and neighbourhoods are as follows:

- Increased cancer risk
- Cellular stress
- Increase in harmful free radicals
- Genetic damage
- Neurological disorders
- Negative impact to the well-being of humans
- Negative impact on reproductive systems

However, there is currently insufficient data for a meaningful health risk assessment between the 5G network and associated infrastructure.

The future of 5G security

Currently there are four elements of 5G security required in order to build digital trust and to allow flexibility within the network, these include:

- **Network availability** - devices must be protected on the inbound points of the network
- **Network adaptability** – the network needs to meet the increasingly sophisticated techniques of cyber-attackers and therefore response time needs to be swift
- **IoT device protection** – good and bad Bot traffic must be examined in real time to create a secure IoT ecosystem
- **Cloudification of mobile access and core networks**
    - Devices need to be virtual and cloud-based
    - Security protections must adapt to the new 5G infrastructure

In response to the security concerns, companies such as Nokia have since opened a 'Threat Intelligence Lab' - a new security testing and verification lab that delves into ways of mitigating security threats. They have also launched a program to address 5G WAN security needs as well as creating an end-to-end security solution for cloud services. With all these tactics in place, they hope to address the issue of managing the increased amount of bandwidth available and the increased attack surface across IoT, 5G and devices.

As communication technology grows and progresses towards the future, the need for enhanced and secure communication and infrastructure needs to grow with it. Although a lot of research and efforts are being done to standardise and create a secure framework for 5G, there are still grey areas within the 5G technology however its architecture and security is of paramount importance.

For more information, please contact

Australia 1300 136 806
nbt@isentia.com
isentia.com