ACICE
ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON
THE CYBER DOMAIN

Issue 12/23 (December)

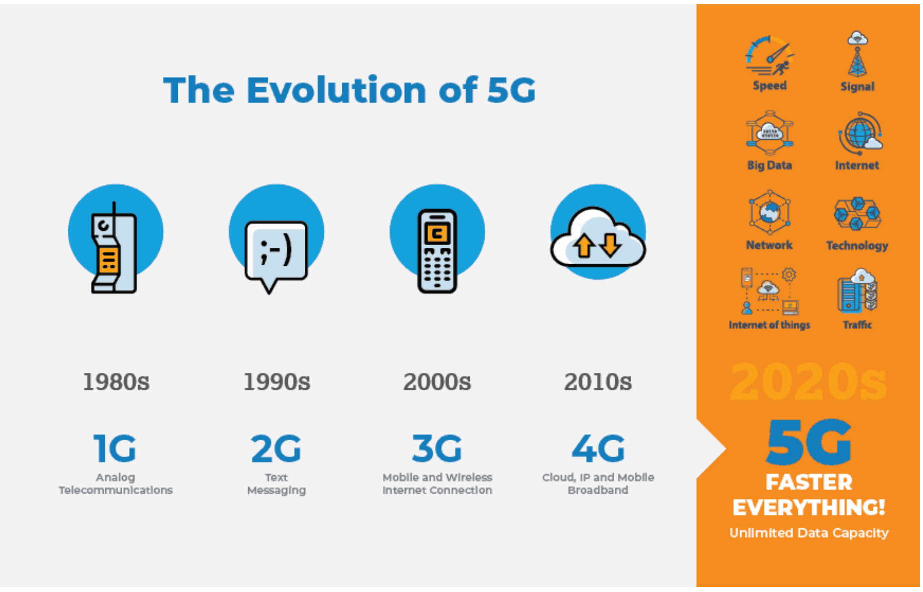
Understanding 5G – Benefits, Risks, and Implications on Cybersecurity for Cellular Networks

OVERVIEW

1. 5G, the fifth-generation technology standard for cellular networks, has gained significant attention for its potential to completely transform telecommunications networks by providing a plethora of benefits that bring faster speeds and increased capabilities to support connectivity for applications like smart cities, autonomous vehicles and telemedicine. These network improvements will revolutionise how people live, work and play all over the world.

WHAT IS 5G?

2. Roughly every 10 years, the next generation of mobile communications networks is released, bringing faster speeds and increased capabilities to users. 5G represents the latest transformation of telecommunications networks with higher data transfer rates, and lower latency to handle a significantly higher number of connected devices simultaneously over the same network.



The evolution of 5G. Source: (Earthlink, 2022).

KEY BENEFITS OF 5G

Faster Speeds

3. The 5G networks are expected to go at speeds of 1 gigabit per second (Gbps) and up to 10 Gbps. This represents a 100 times increase compared to 4G networks. As an illustration, this means that a 3-gigabyte movie would only take 35 seconds to download on 5G networks, as compared to 40 minutes on 4G networks.

Lower Latency

4. Latency measures how long a signal takes to go from its source to its receiver, and then back again. The low latency made possible by 5G networks is faster than human visual processing, making it possible to control devices remotely in near-real time. Applications that provide near-real time sharing of information has benefitted a range of industries, such as transport, healthcare, and manufacturing. In self-driving/autonomous vehicles, it prevents delays in transmissions of signals from traffic lights and other road users, potentially making the difference between a safe ride or a serious accident. In healthcare, it ensures near-immediate detection, analysis and response by emergency responders, enabling quicker medical interventions. In logistics and manufacturing, it supports the predictive analytics necessary for real-time supply chain optimisation, thus lowering costs and fulfilment times.

Enhanced Network Capacity

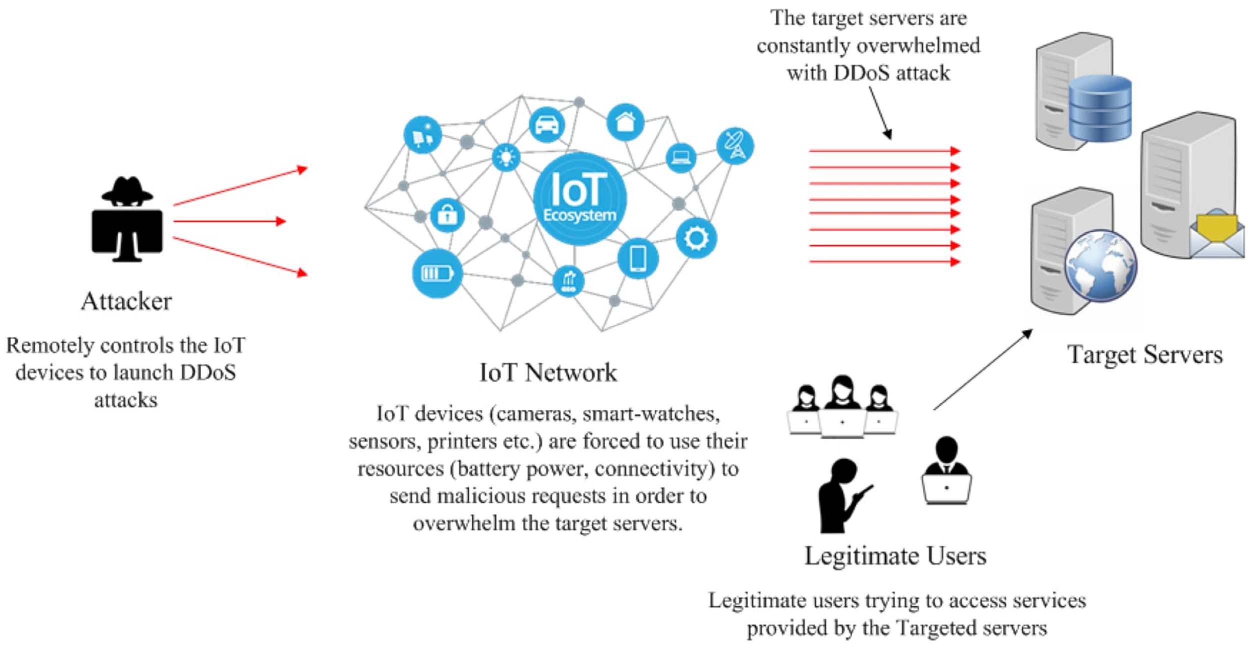
5. 5G networks will deliver up to 1,000 times more capacity than 4G networks. This creates space for development in Internet of Things (IoT). For instance, millions of devices can now be seamlessly connected to the same network in the same area, which allows new applications and communications in cities, factories, farms, schools, and homes to flourish.

RISKS ASSOCIATED WITH 5G

Proliferation of DDoS Attacks

6. A Denial of Service (DoS) attack aims to disrupt or block access to a specific resource, like a website, by overwhelming it with too much data. This can prevent legitimate users from accessing the resource. DoS attacks can be intensified when many infected computers (bots) are used to flood the target with data all at once; this is known as a Distributed Denial of Service (DDoS) attack. With the increased speed and capacity of 5G networks, it is easier for malicious actors to amplify the scale and impact of DDoS attacks. For example, attackers may leverage the proliferation of 5G-connected devices to escalate DDoS attacks to involve millions of sources – rendering existing means of protecting against DDoS attacks useless.

7. As conventional DDoS prevention methods are primarily centred on obstructing the origins of DDoS traffic, keeping 5G networks safe from DDoS attacks will require not just a proactive approach, but also a different one. DDoS attacks need to be mitigated at the network edge, with threats detected and mitigated as close to the access layer as possible. Instead of only protecting and monitoring important clients, all traffic and connected devices should be monitored and protected. This would require proactive steps to be taken, with comprehensive security measures installed to filter out DDoS attacks.


The target servers are constantly overwhelmed with DDoS attack
IoT Ecosystem
Attacker
Remotely controls the IoT devices to launch DDoS attacks
IoT Network
IoT devices (cameras, smart-watches, sensors, printers etc.) are forced to use their resources (battery power, connectivity) to send malicious requests in order to overwhelm the target servers.
Target Servers
Legitimate Users
Legitimate users trying to access services provided by the Targeted servers

A DDoS attack scenario in IoT networks. Source: (MDPI, 2022).

Decentralised Security

8. In the past, networks had fewer hardware traffic points of contact allowing for easier implementation of cybersecurity measures and practices. However, modern 5G networks are decentralised – this means that an expansion of digital routers and software-based systems is required to cover the entire network. This increase in hardware and software significantly elevates the difficulty of enforcing cybersecurity measures.

9. Given the increased difficulty in identifying cyber intrusions, fortifying cyber systems is critical. Organisations should place emphasis on software protection and updates as part of their cybersecurity measures. Micro-segmentation to create smaller, isolated network segments within networks can limit lateral movement and reduce the attack surface to ensure that the impact of a breach remains localised. This approach of validating every interaction and communication within the network, mitigates the risk of unauthorised access or malicious activities. Collectively, these measures can enhance the organisation’s cybersecurity posture.

PREPARING FOR 5G

Implementing a ‘Zero-Trust Architecture’ Security Approach

10. To better protect themselves from the extant cybersecurity risks associated with 5G, organisations may consider implementing a ‘zero-trust architecture’ (ZTA) security approach throughout their systems. ZTA treats network elements at all levels as potential threats, with all requests inspected, all users and devices authenticated, and all permissions assessed before granting access. Moreover, as the security policy in ZTA is adaptive, the list of trusted devices and user access privileges are continually reassessed as the security context changes.

11. The protection required to support ZTA may take the form of additional authentication mechanisms (e.g., multi-factor authentication), automated intelligent traffic monitoring, and/or logging and filtering mechanisms installed throughout the system. The widespread installation of such preventative measures reduces the risk of a data breach, provides granular access control over cloud environments, and mitigates the impact and severity of successful attacks.

Top-Down Emphasis on Cybersecurity

12. While the financial outlay needed to install these preventative cybersecurity measures may be substantial, organisations should view it as an investment that sets the foundations necessary to accrue the benefits of 5G. Sufficient top-down emphasis must be provided to implement the necessary security measures at all levels, to ensure that cyber-attacks do not result in negative financial, operational, or reputational costs to one’s organisation.

CONCLUSION

13. While 5G offers numerous advantages, its transition is not without risks. A comprehensive understanding of these challenges, along with a well-structured plan and 5G expertise, is crucial for organisations to ensure a smooth and secure migration into the 5G ecosystem.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

REFERENCES

News Articles

1. What is 5G? - Earthlink
[Link: https://www.earthlink.net/blog/what-is-5g-mobile/]

2. Benefits of 5G Technology: 5g Features and Advantages - Intel
[Link: https://www.intel.com/content/www/us/en/wireless-network/5g-benefits-features.html]

3. How 5G Technology Affects Cybersecurity: Looking to the Future - Upguard
[Link: https://www.upguard.com/blog/how-5g-technology-affects-cybersecurity]

4. Dynamic Reconfiguration in 5G Mobile Networks to Proactively Detect and Mitigate Botnets - University of West Scotland
[Link: https://core.ac.uk/reader/227578010]

5. Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things - MDPI
[Link: https://www.mdpi.com/1424-8220/22/3/1094]

6. Why 5G requires new approaches to cybersecurity - Brookings
[Link: https://www.brookings.edu/articles/why-5g-requires-new-approaches-to-cybersecurity/]

7. What is a Zero Trust Architecture? – Palo Alto Networks
[Link: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture]