1. Petra DOSTALOVA[1], 2. Martin HROMADA[1]

Tomas Bata University in Zlin, Czech Republic (1)
ORCID:1. 0000-0001-5706-218X, 2. 0000-0003-0347-7528

doi:10.15199/48.2023.08.14

Use of 5G networks in security technologies

Abstract. *Telephone devices and telecommunication networks have always helped to overcome communication difficulties. Their rapid development is related to the overall digitization of the world. The article dealt with the use of 5G networks in essential sectors of human activities. Although increased risks accompany every step forward, 5G networks and their possible successors will make workouts more efficient in the industry, transport and logistics, healthcare, and personal safety. This publication aims to present the most critical sectors and the use of 5G networks in them.*

Streszczenie. *Urządzenia telefoniczne i sieci telekomunikacyjne zawsze pomagały przezwyciężać trudności komunikacyjne. Ich szybki rozwój związany jest z postępującą cyfryzacją świata. Artykuł dotyczył wykorzystania sieci 5G w istotnych sektorach działalności człowieka. Chociaż każdemu krokowi naprzód towarzyszy zwiększone ryzyko, sieci 5G i ich potencjalni następcy sprawią, że treningi będą bardziej efektywne w przemyśle, transporcie i logistyce, opiece zdrowotnej i bezpieczeństwie osobistym. Niniejsza publikacja ma na celu przedstawienie najbardziej krytycznych sektorów i wykorzystania w nich sieci 5G. (**Wykorzystanie sieci 5G w technologiach bezpieczeństwa**)*

Keywords: 5G, networks, security, technologies, phone
Słowa kluczowe: 5G, sieci, bezpieczeństwo, technologie, telefon

Introduction

Our phones have gone through a lot of development, not only in aesthetics, or in terms of performance in their cameras, processors, or batteries. The way we communicate with our smartphone, which gives meaning to everything else, is the one that has achieved something unthinkable in a few years, when there was talk of 1G or the first generation of telecommunications networks at the end of the 70s. We now have 5G mobile phones in our hands and there is even talk of its development.

Our mobile phones have gone from being used only and exclusively for calling to becoming a complete multimedia center in which constant connectivity is essential for the vast majority. Even if there are generations that only know 4G or 5G, the truth is that there is a history behind the whole evolution, and we have not always had the same means or the current concept of using a mobile phone.

5G aims to become a reliable and trusted innovation platform for businesses and organizations to build and deliver new value-added services, but it is also seen as an enabler to digitize and modernize critical national infrastructures such as energy, transportation, etc. setting the bar for 5G systems, which provides greater availability and better guarantees of secure communication services.

Network development

The 5G mobile network builds on the previous standards of wireless networks (1G, 2G, 3G and 4G), improves their shortcomings, increases capacity and speeds up. At the end of this decade, 5G should be followed by an even more perfect 6G. [1]

1G: transfer speeds from 1 to 2.4 Kbps. It was only possible to make phone calls using this network. [2]

2G: transmission speeds from 14 to 64 kb/s. Thanks to this network it was possible to make phone calls and send SMS messages. [2]

3G transmission speed of 384 Kbps at 2M. Using this network, we were able to make phone calls, send SMS messages and light Internet functions. [2]

4G: transmission speeds from 100 Mbps to 1 Gbps. This network offers more options. Thanks to it, you can make phone calls, send SMS messages, internet, videos and photos. [2]

5G: transfer rates from 1 to 10 Gb/s. This network offers high-speed Internet, photo-video (HD quality, 3D), broadband connection. Higher battery capacity. [2]

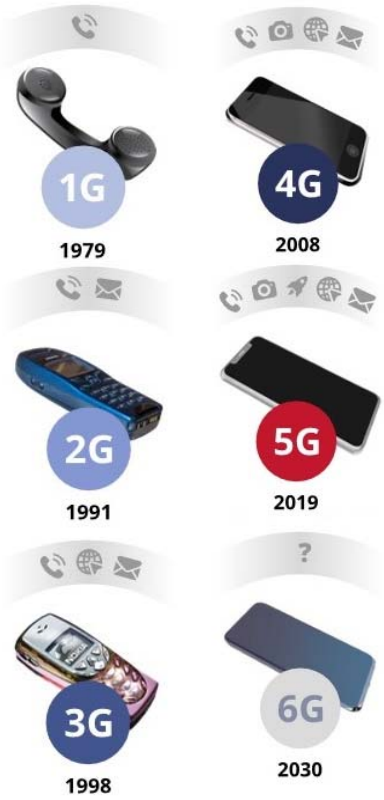

Fig. 1 – Network development [1]

5G networks

Constant exposure to electromagnetic radiation – from television and radio signals, and from a range of technologies, including mobile phones, from natural sources – sunlight.

5G uses higher frequency waves than previous mobile networks, this allows more devices to access the Internet at the same time and at higher speeds. [3]

As these waves travel shorter distances through urban spaces, 5G networks require more transmitters than previous technologies, which are located closer to ground level.

The radio wave band – used for mobile phone networks – is non-ionizing, meaning it lacks enough energy to break DNA and damage cells.

5G meets the growing demands of industries in particular for a fast, reliable and high-capacity network that would be able to connect everyone and everything (appliances, homes, industrial buildings, cars and public transport).

]

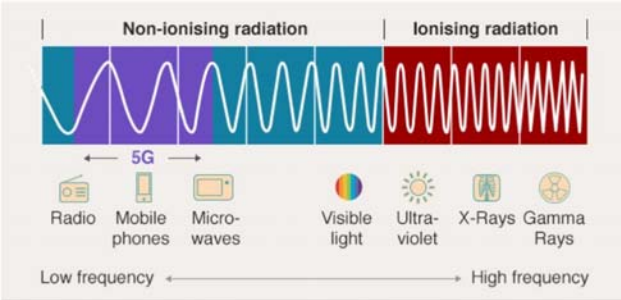

Fig. 2 – Radio wave band [1

The expansion includes new relationships in the form of digitized and automated business processes of enterprises, management, and operation of machinery of industrial enterprises. In addition, new ways of accessing the mobile network will enable mutual cyber and physical interconnection between telecommunication networks and smart connectivity of other infrastructure providers (cities, energy, public services, transport, etc.). Examples of 5G applications for enhanced mobile broadband, fixed wireless access and mobile IoT (Figure 3) embody new types of data transmitted over mobile networks. [4]

Fig. 3 – 5G use cases [4]

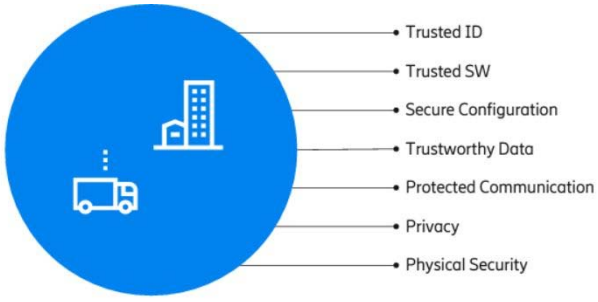

Fig. 4 – IoT device security aspects [4]

For applications that rely on 5G machine-critical communications, they will benefit from an ultra-reliable, low-latency connection where data volumes can be high and business-critical. In this case, the communicating endpoints are intelligent machines, vehicles and robots with or without human intervention, i.e. autonomous. Industries and services expected to benefit from this connectivity are healthcare, manufacturing, transportation and consumer goods. IoT is a phenomenon that has already emerged and can be exploited by 4G as well as other non-3GPP access technologies, machine-like communication cases in 5G networks will empower IoT with network capabilities such as ultra-low latency that have not been available before.

5G network – application in industry

Artificial intelligence and IoT technologies are increasing work efficiency in may processing companies. The main potential besides the possibility of implementing new types of sensors and intelligent devices for data collection and subsequent analysis is augmented reality. [5]

Using 5G technology, the American operator also performs predictive analysis to dermine the viability of individual components, quality control through robotic visual recognition or continuous monitoring of the performance od engineering equipment.

Europe also has 5G projects - HUAWEI DISTRIBUTION CENTER near Budapest.

Difficult logistics can be handled by automatically controlled handling technology in combination with augmented reality, or automated 5G solutions controlled by artificial intelligence. [5]

The benefit of the 5G network in industry: [2]

- the efficiency of the entire distribution center increased,
- private 5G network helped to better secure data,
- it also helped to increase work safety, especially in the case of handling.

5G network – application in healthcare

Using this network, monitoring of sleep, physical activity, and the amount of oxygen in the body is more effective than any better smart watch. The speed of 5G and the reliability of the connection will allow the development of devices that we will be able to implant directly into the body instead of being worn externally.

With the help of 5G technology, the condition of the patient's organs can be streamed live with microscopic cameras, enabling remote diagnosis and more complex operations. Example: stroke patients, for whom repeated hospital visits are a burden, but remote monitoring runs into the limits of 4G technology.

Smart ambulances - thanks to a stable connection, they enable the crew to communicate with the hospital staff, but also with experts on the other side of the country if necessary. Monitoring in 4K HD quality (a resolution that is 4x higher than Full HD, has a much sharper image) allows important information about the patient to be shared in real time, as well as video material, thanks to which doctors do not lose even a minute when taking over the patient.

Digitization thus helps not only efficient information processing, but also significantly contributes to the timely treatment of the patient.

5G network – application in transport and logistics

The automotive industry is going through a rapid transformation, and in the face of the climate crisis, it faces increasing demands for sustainability. Connected, autonomous, shared and electric mobility is offered as a solution, to which modern technologies will lead us.

In the future, smart vehicles are expected to integrate almost all advanced next-generation technologies, including, for example, AR or VR applications, voice and image recognition, computing devices, sensors, computing platforms, and HD maps.

The implementation of innovative technologies in transport is expected to go hand in hand with the development of smart cities. Smart traffic lights, an intelligent parking system and easy travel in the metropolis may not be far away with the arrival of 5G.

5G network – in security technologies

5G networks – creation of conditions for the deployment and development of applications to support the performance of PPDR activities.

The possibility of providing detailed information to PPDR units intervening in the field, e.g.:

- identification and registration of persons,
- visual information from the site of intervention before arrival,
- advanced navigation,
- use of biometric elements during control.

Transmission of detailed information from the site of intervention to remote control components, e.g.:

- real time video transmission.

These capabilities are key in increasing the efficiency and safety of the performance of PPDR activities.

Transition to procedures that are more based on the exchange of situational information before, during, or after the intervention, as well as during the routine daily activities of the relevant components. It is mainly about the quick availability of accurate information without distortion (videos and photos), which is created by the exchange of information through voice communication.

These new possibilities bring more effective decision-making, faster mobilization of relevant PPDR components and units in sufficient quantity, and more effective linking of operational control across individual PPDR components. The result is timely and more efficient performance of PPDR activities.

New applications that will increase the safety and efficiency of PPDR activities and will monitor the vital functions of members of PPDR units in real time will be especially important for PPDR units intervening in dangerous and unknown terrain during ground operations (e.g. fire rescue units).

Biomedical telemetry includes, for example:

- monitoring,
- recording,
- measurement of basic physiological functions,
- as well as other quantities such as air quality in the environment, including the presence of toxic gases
- ambient temperature.

Intervening PPDR units forward this information to operational control at the site of the intervention and eventually to remote workplaces. The use of this application is subject to additional investments, e.g. in equipment.

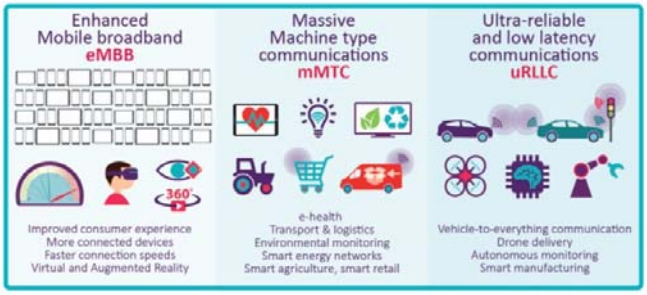

Fig. 5 – Examples of specific applications in the scope of the three mentioned areas of use of 5G mobile systems. [5]

Biomedical telemetry can also be used in the future for remote medical assistance and for specific applications such as person identification:

- facial recognition
- fingerprints,
- irises,
- eye corneas,
- dentition, body proportions and movement pattern.

These applications can be used within a specific activity (i.e. during an intervention) or permanently (i.e. during long-term surveillance using camera systems).

5G networks – risks

Potential attackers: external actors of cyber threats (states, hackers, cybercrime groups) and suppliers with malicious intentions (hardware, software suppliers or service operators. this division is not strict, and the mentioned groups of attackers can be linked. A state actor can, for example, abuse his influence on the supplier and penetrate the network through him.

The risk is also represented by so-called insiders - individuals working in the supply chain with their own agenda, which may be in the interest of personal, economic or external actors.

From the point of view of risks based on the CIA triad, the security of data sent via 5G networks can be evaluated as follows:

Confidentiality: ensuring unauthorized access to foreign actors - represents a problematic aspect of electronic communications networks. The risk of attacks by external actors is low, but there is a very significant risk from some suppliers, or their close ties to state actors with potentially problematic interests going against the country.

Integrity: Data integrity (that is, the certainty that the data has not been altered by a foreign actor) is the least threatened in electronic communications networks, provided that end-to-end encryption is used.

Vulnerability: there is a significant risk and vulnerability of the entire network due to incorrect SW development, intentional programming of SW with unsolicited specific functionality for monitoring, collecting and sending information through hidden interfaces using backdoors. they may also discover other security weaknesses, especially in connection with the transition to software and virtualization through software-defined technologies (Software Definition Network - SDN) together with the virtualization of network functions (Network Functions Virtualization - NFV).

Availability: is the primary vulnerability of electronic networks. communication. While decentralization increases the network's resilience against external threats, the enhanced role of the supplier in 5G networks increases vulnerability on their part. In any attempt to disrupt data availability, suppliers have a significant advantage in the form of direct control over the network or the possibility of controlling some of its elements through a backdoor, etc. If an operator, vendor, or outside attacker disables key parts of the network, important data transmitted over the network will almost certainly become unavailable.

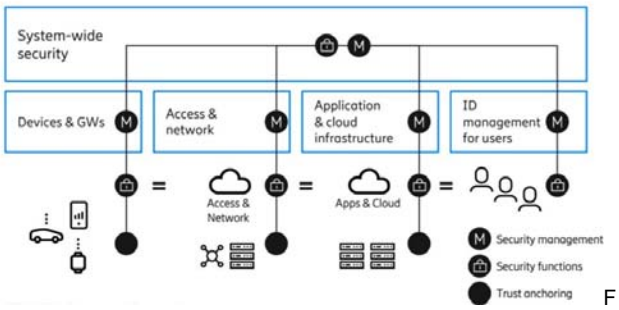

Fig. 6 – System-wide security [4]

The 3GPP standardization section focused on security mechanisms in scope for 3GPP, which are functional elements and interfaces. Additional security

considerations related to 5G system deployment scenarios are covered in this section, including: [4]
• System-wide security (horizontal security)
• Network level
• Slicing
• Application-level security
• Confidentiality and integrity protection
• Interconnection (SBA).
Deployment of 5G functional elements (vertical security)
• NFVi (virtualized or cloud native)
• Device-based features
• Distributed clouds and edge computing.

Social behavior and business services are evolving, increasing the expectation that mobile networks will provide reliable and secure communications.

Horizontal security (Figure 6) is achieved by combining and coordinating a large number of security controls across different domains in telecommunications networks, including radio access (e.g. radio units, baseband units, antennas), transport networks (e.g. IP/MPLS routers, controller SDN), packet core (e.g. MME, S-GW, PGW, HSS), network support services (e.g. DNS, DHCP), cloud infrastructure and various management systems (e.g. network management, customer experience management, security management). Security in all these domains must be coordinated to ensure the targeted availability of services and confidentiality and integrity of data sent, stored and processed within the 5G system. Horizontal security will also protect the privacy of 5G users by ensuring that data sent through the system is always protected by confidentiality and integrity. The previous section described the controls available in 3GPP nodes, but now we will explore the controls and design aspects in the transport and cloud domains of the 5G system. [4]

Mobile network information assets

Core network functions and management systems are critical assets of a mobile network. Affecting the core network or management systems can compromise the confidentiality, availability, and integrity of all mobile network services. The radio access network is also a sensitive asset because it processes user data and may be in critical locations. As edge computing is deployed, some core network functions are expected to be deployed closer to access points, making access critical as well. [4]

Data is one of the most important assets in mobile networks, subscriber data is the most critical in this category. Subscriber data includes communication data (voice, text and data sessions) as well as subscriber-related information such as identity, location, subscription profile and connection metadata (eg call data records or signaling traces). To protect subscriber privacy, this data must be protected during storage and transmission. Public networks carry encryption at the layer and monitor router and firewall configuration changes. Data availability must be ensured by implementing and practicing data backup procedures. In addition to subscriber data, information assets related to network management are required for the proper operation of a mobile network. Management data includes infrastructure and service configuration data, network configuration data, security-related data, monitoring data such as performance metrics, logs, and traces. [4]

Understanding which data is critical, where it is located, and how it can be accessed is a prerequisite for data protection. All data that is considered critical must be protected throughout its lifecycle, including secure deletion. To ensure permanent protection, it is necessary to enforce the safe handling of encryption keys and the use of encryption algorithms and protocols of appropriate strength. For long-term data retention requirements, it may be necessary to re-enforce protection with stronger cryptography.

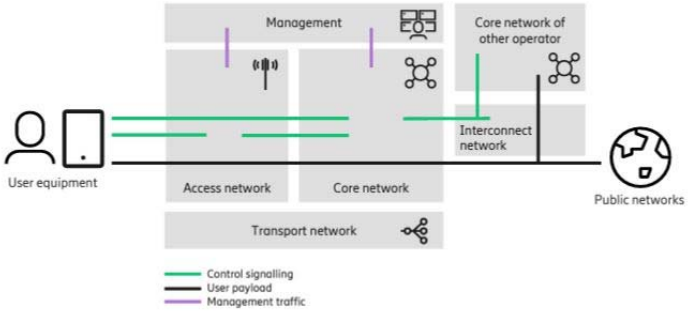

Fig. 7 – The telecommunication network – logical elements and logical planes [4]

Ericsson´s 5G product security

SRM divides security and privacy controls into four key areas: 1 Functionality, 2 Assurance, 3 Compliance and Documentation, 4 Deployment and Operations. We apply controls in these four areas continuously through well-defined activities across our product value stream, from our suppliers to our customers.

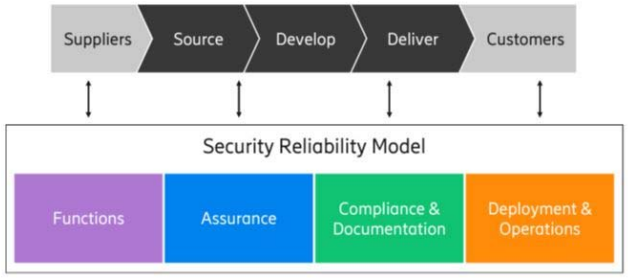

Fig. 8 – Ericsson Security Reliability Model [4]

The Security Reliability Model (SRM) enables a risk-based, controlled approach to security and privacy implementation where requirements are tailored to the target environment and requirements. This approach helps us meet the expectations of stakeholders and meet the rapid development of technology and constant changes in legislation around the world.

SRM defines Ericsson's approach to achieving our security and privacy goals by design. Its purpose is to:
• set product security and privacy ambition levels for our products and solutions [4]
• specify a control framework that will enable Ericsson to meet the ambition levels
• outline how this control framework covers the product value stream from component acquisition during development activities to after deployment and operation in customer networks
• demonstrate how we achieve compliance with applicable laws and regulations.

SRM Area 1: The SRM function mandates that each product organization analyse, decide, and document applicability and compliance with our General Product Requirements (GPR) for security and privacy. To help them in this work, it also defines a set of general security and privacy features for Ericsson products. Risk assessment and privacy impact assessment processes are used to identify and prioritize appropriate security and privacy features from the GPR suite.

SRM Area 2: Assurance refers to the activities performed to ensure the security of the product as it runs in

the target environment. They include risk assessment, privacy impact assessment, secure coding, vulnerability analysis and hardening. SRM specifies the appropriate verification activities for each category at each stage of the product value stream: source, development, and delivery. Depending on the characteristics of the product, the appropriate level of assurance activities is set for each category - basic, advanced, or customized.

SRM Area 3: Compliance and Documentation the Compliance and Documentation area covers all information that demonstrates the security and privacy status of product release and customer documentation. It also defines valid certificates and declarations of conformity for external stakeholders and provides the necessary guidance maintain security and privacy in customer environments. Customer Product Information, security test reports and security standard conformance all play a key role in this area.

SRM area 4: Deployment and operations The Deployment and operations area groups together the operational aspects of product security that arise in the product value flow, including security in system integration, guidance that operators require to operate their network in a secure way and customer support to resolve any incidents that arise.

Acknowledgments

This study was prepared with the help of funds provided by Tomas Bata University in Zlín - Faculty of Applied Informatics within the project IGA/FAI/2023/003.

Authors:

1 Ing. Petra Dostálová, Tomas Baťa University in Zlín, Faculty of applied informatics. Nad Stráněmi 4511, 760 05 Zlín, Czech Republic, E-mail: pdostalova@utb.cz

2 doc. Ing. Martin Hromada, Ph.D., Tomas Baťa University in Zlín, Faculty of applied informatics. Nad Stráněmi 4511, 76005 Zlín, Czech Republic. E-mail: hromada@utb.cz

REFERENCES

1 Implementace a rozvoj 5g sítí v České republice, [online]. [cit. 2022-11-12]. Avaible from: https://www.tacr.cz/wp-content/uploads/documents/2022/04/26/1650968198_Implementace%20a%20rozvoj%20s%C3%ADt%C3%AD%205G%20v%20%C4%8CR.pdf

2 Mobile data consumption continues to grow – a majority of operators now rewarded with ARPU, [online]. [cit. 2022-11-20]. Avaible from: https://tefficient.com/wp-content/uploads/2019/09/tefficient-industry-analysis-3-2019-mobile-data-usage-andrevenue-1H-2019-per-operator-5-Sep.pdf

3 Czech Republic in the Digital Economy and Society Index, [online]. [cit. 2022-08-3]. Avaible form:https://digital-strategy.ec.europa.eu/en/policies/desi-czech-republic

4 Conceptualizing security in mobile communication networks – how does 5G fit in, [online]. [cit. 2022-12-12]. Avaible from: https://www.ericsson.com/en/security/a-guide-to-5g-network-security

5 5G aliance. Vstříc rychlé budoucnosti [online]. 2020 [cit. 2022-12-14]. Dostupné z: https://www.5galiance.cz/