CONASENSE 2022 SYMPOSIUM

Cybersecurity in the era of Next Generation wireless networks

Prof.dr Milica Pejanović-Djurišić

Faculty of Electrical Engineering, University of Montenegro

To meet the demands of wireless mobile networks of the year 2030 and beyond, a paradigm shift towards Next Generation (Next G) wireless networks (beyond 5G, 6G, and beyond), which will offer support for a rich variety of devices, as well as several types of integrated network and communication technologies, is necessary.

While ongoing discussions and research are yet to give directions about the true nature of 2030 wireless networks, it is realistic to expect further data rates increase, reduced latency, larger coverage (land, sea, space), softwarization, virtualization, network computing.

In such circumstances it will be possible to adjust service levels to the needs of particular end users in different vertical industry segments (smart cities, smart agriculture, telemedicine, virtual reality, autonomous vehicles, smart homes, automated industrial processes, etc.) with the application of new innovative business models. However, moving towards hyper-connected society would not be efficient unless conditions are created for providing and supporting services in a safe and controlled manner.

Thus, in addition to requiring an end-to-end integration of communication, control, computing, localization and sensing functionalities, new intelligent services will need trustworthy networks to ensure security and overcome privacy and integrity threats in an integrated way.

With the plethora of devices and technologies supported with the Next G wireless heterogenous networks, creating the trustworthy wireless networks becomes a significant challenge which cuts across multiple domains and disciplines (technology, regulations, economy, politics, ethics) in addressing fundamental issues: trust, security, privacy. At the same time, balancing performance expectations and security needs will become more complex as threats become more sophisticated.

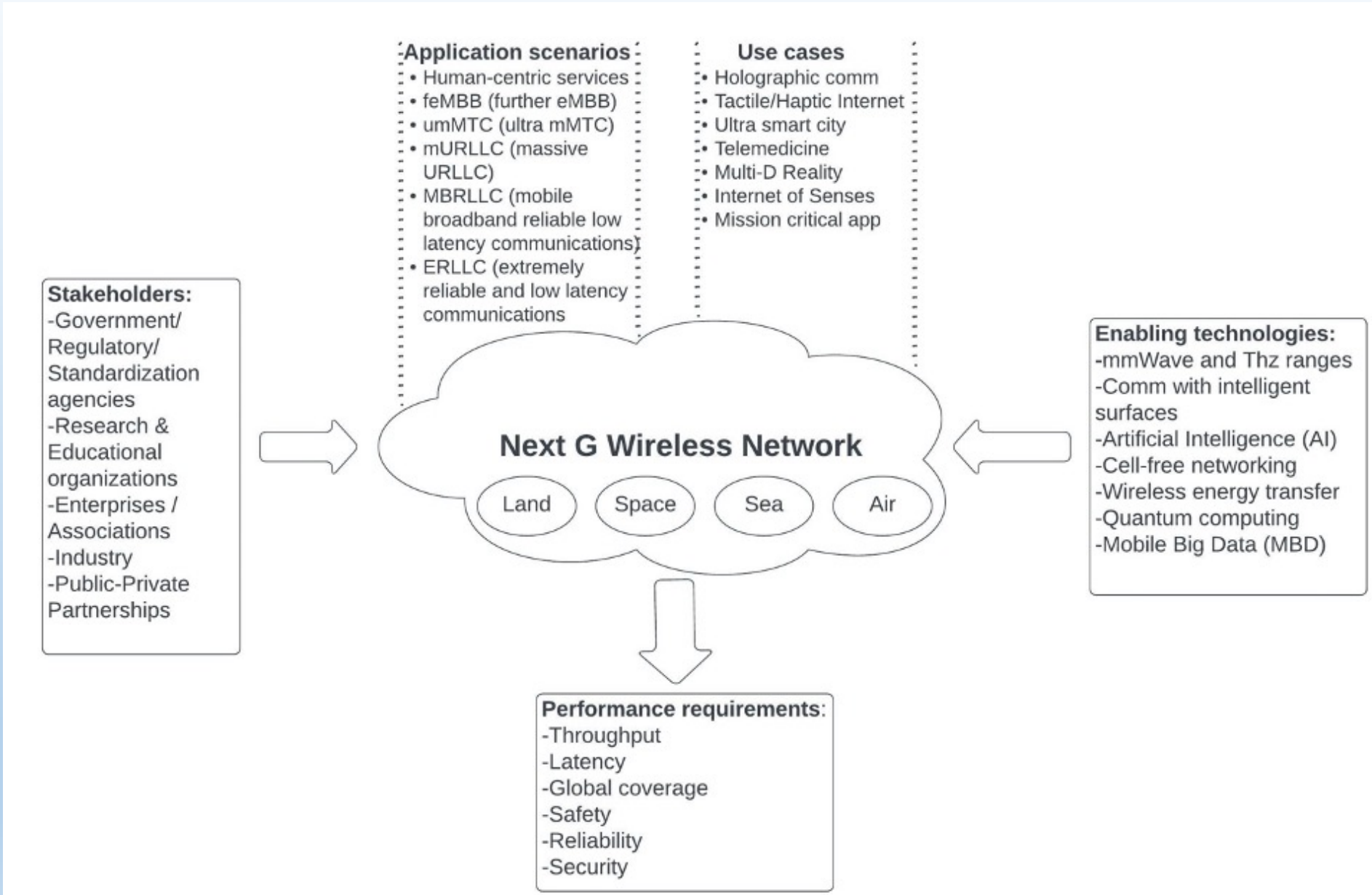
Next G Wireless Network Ecosystem

In order to respond to requirements of the future wireless near-instant and limitless connectivity , Next G wireless networks have to be enhanced and extended in a number of dimensions when compared with the current networks.

A set of new and disruptive use cases characterizing Next G wireless environment will emerge, such as: Tactile/Haptic Internet, Holographic verticals, Industrial Internet of Things, Internet of bio-nano things… At this point it is realistic to assume that these developments will be met in stages: beyond 5G evolution, disruptive 6G step, beyond 6G …. and that the drivers of such a process will be a combination of already exploited trends in wireless networks and emerging trends related with new categories of wireless devices (including human-embodied implants), smart surfaces, artificial intelligence (AI), computing and sensing.

To enable envisaged applications, and those still not envisioned, and to guarantee required performance, foundations of Next G wireless networks will be laid on a broad range of promising and integrated technology solutions, such as:

- Frequencies in mmWave and THz ranges, with further shrinking of the cell size and their densification.
- Communication with large intelligent surfaces, as a leap from traditional MIMO, being critical for holographic based applications.
- Artificial Intelligence (AI), together with Machine Learning (ML), in the context of “AI everywhere” with the emphasis on the network edge, to provide distributed autonomy.
- Global integration of terrestrial, air and space communications, enabled through efficient dynamic collaboration for data transmission, processing and sensing.
- Cell-free networking, enabling mobile devices to connect seamlessly without depending on a type of access point.
- Wireless energy transfer, and harvesting, essential for realizing energy autonomous networks and to reduce costs.
- Quantum computing, which can be instrumental in long-distance networking and enhancing security.
- Mobile big data (MBD), combining mobile computing and big data.


Application scenarios
• Human-centric services
• feMBB (further eMBB)
• umMTC (ultra mMTC)
• mURLLC (massive URLLC)
• MBRLLC (mobile broadband reliable low latency communications)
• ERLLC (extremely reliable and low latency communications
Use cases
• Holographic comm
• Tactile/Haptic Internet
• Ultra smart city
• Telemedicine
• Multi-D Reality
• Internet of Senses
• Mission critical app
Stakeholders:
-Government/ Regulatory/ Standardization agencies
-Research & Educational organizations
-Enterprises / Associations
-Industry
-Public-Private Partnerships
Next G Wireless Network
Land
Space
Sea
Air
Enabling technologies:
-mmWave and Thz ranges
-Comm with intelligent surfaces
-Artificial Intelligence (AI)
-Cell-free networking
-Wireless energy transfer
-Quantum computing
-Mobile Big Data (MBD)
Performance requirements:
-Throughput
-Latency
-Global coverage
-Safety
-Reliability
-Security

Security challenges in the Next G Wireless network ecosystem

Taking into account the envisaged nature of Next G wireless networks, potential security and privacy issues can be related with both physical and network layer:

- Physical layer- With a huge number of connected devices and an extremely frequent data exchanges, it becomes easier to corrupt data, not only during the transmission phase, but also while processing and storing. New intelligent solutions, including mmWave and THz frequencies, channel codes and reflective surfaces, will improve the security at the physical layer, but still corruptive activities and malicious attacks will not be completely eliminated. Also, when it comes to Internet of senses and molecular communications new concerns related with communications and authentication processes will appear.
- Network layer - It is already well known that SDN (Software Defined Network) and NFV (Network Functions Virtualization), have issues linked with reliability and security. Moving the intelligence from the central cloud to edge nodes, will be adding to that, with vulnerabilities related to all forms of computing. While introduction of blockchain will improve security, it is still not clear how to tackle the issue of latency.

In such circumstances, with the high performance requirements of the Next G wireless networks applications and use-cases, it can be envisaged that a trade-off with demands for better security will be of a significant importance.

Therefore, the strong end-to-end network security should be an option for both physical layer and network layer in order to properly address reliability and trustworthiness of the whole ecosystem.

From the research perspective, when dealing with cybersecurity in Next G wireless networks the required performance should be taken into account together with security and privacy potential of implemented novel technology solutions. Thus, the physical layer security could be increased using advantages of disruptive technologies, like: THz, massive MIMO, channel coding, AI, Quantum computing and blockchain. At the network layer, softwarization and virtualization could be advanced enabling flexibility and programmability of security integrated with networks and applications. In doing so, comprehensive approach for the whole ecosystem is necessary to integrate security in order to deliver “security as a service”.

To have the benefits of such an approach, wider and efficient cooperation at the global level is necessary, especially when it comes to capacity building and enhancing the trust.

Cybersecurity initiatives and their future

The UN General Assembly established two processes to discuss the issue of security in the use of ICTs, an Open-ended Working Group and a Group of Governmental Experts (GGE). The work of the Groups of Governmental Experts has focused on the following topics:

- Existing and emerging threats
- How international law applies in the use of ICTs
- Norms, rules and principles of responsible behavior of States
- Confidence-building measures
- Capacity building.

Through resolution 73/27, the General Assembly established an Open-Ended Working Group (OEWG), in which all UN Member States were invited to participate, ensuring the possibility of holding intersessional consultative meetings with industry, non-governmental organizations and academia.

UN – Cybersecurity initiatives

1. Group of Governmental Experts have focused on the following topics:

- Existing and emerging threats
- How international law applies in the use of ICTs
- Norms, rules and principles of responsible behavior of States
- Confidence-building measures
- Capacity building

2. Through resolution 73/27, the General Assembly established an **Open-Ended Working Group (OEWG)**, in which all UN Member States were invited to participate. The Group convened for the first time in 2019 and report back to the General Assembly in 2020. It concluded its work with the Final Report in March 2021.

The OEWG process provided the possibility of holding intersessional consultative meetings with industry, non-governmental organizations and academia.

ITU Cyber for Good aims to bridge the cybercapacity gap between and within countries, through the promotion of inclusion of women and youth, and the development of cybersecurity capacity in LDCs and developing countries.

Cyber for Good seeks to improve capacity and tackle the Cybercapacity Gap, through:

Low barriers to entry and exit for beneficiaries

Giving opportunities for beneficiaries to test and try new ideas and tools, without being locked into a system

Network effects

Promoting services and tools that can have multiplicative effects, where one positive change can lead to another

Customized plans for high impact

Informed by best practices and experiences of beneficiaries to help others

Empowering beneficiaries

Beneficiaries are in the driving seat, able to choose options that best fit their needs

Current areas addressed by Cyber for Good include:

Services
Connecting LDCs to services

Women in Cybersecurity
Enabling new leadership

Youth in Cyber
Developing the next generation

Therefore, for embracing fully innovative opportunities new models of cooperation between stakeholders of the ecosystem should take into account:

- A myriad of threat actors, many stakeholders (civilian authorities, military, industry, civil society organisations, individuals etc.), the rapid technological change that expands the cyberattack surface (increasing vulnerabilities).
- Burden sharing in emerging multi polar world of old and new adversaries.
- A cybersecurity gap as adversarial cyberattacks are continuously outrunning defender security improvements in technology, processes and education.

In order to be effective, a framework of such partnerships has to be structured around the shared vision of future networks and development of innovations through fully coordinated cooperation. In addition to agile methods, such framework should have a clear structure of roles, artifacts and the integrated roadmap for reaching the required level of technology solutions, while minimizing cyber risk. Adopting this kind of approach to cooperation among diverse partners is the key for effective governance and development in virtual and digital domains which are *per se* technologically extremely demanding.

In order to be effective in such endeavor, a **ROADMAP** for considering important issues should be established, with the following type of steps:

- Creating a whole government approach and fostering meaningful inclusion of stakeholders in order to promote common understandings, existing and potential cybersecurity threats and possible cooperative measures to prevent and counter such threats.
- Leveraging the convening power and function of GGE and OEWG to share best practices with regard to critical infrastructure protection, at the bilateral, regional, and global levels.
- Identifying already existing channels of communications (rather than inventing new ones) to share information on existing and potential threats in real-time.
- Facilitating the implementation of the agreed normative framework while building on existing efforts, avoiding duplication, and fostering complementarity.
- Enabling a meaningful discussion on how international law applies to cyberspace, driving greater transparency and understanding.
- Engaging with regional organizations to learn from their experiences with regard to confidence-building measures in order to avoid the duplication of efforts and focus on implementation of already successful confidence building measures.

Applying the suggested roadmap a regular, transparent, institutional dialogue would be established among all relevant stakeholders of the Next G wireless network ecosystem, ensuring timely advancements on:

- promotion of norms and best practices;
- application of international law to cyberspace;
- expansion of cybersecurity capacity building and
- advancement of multistakeholder inclusion.

In that manner, identifying threats and possible mitigation actions, together with fostering prevention, a foundation for building a cyber-resilient hyperconnected intelligent environment would be created.

Conasense

Thank you!

Q & A