Designing Security for the Sixth Generation: About Necessity, Concepts and Opportunities

Christoph Lipps[1], Annika Tjabben[1], Matthias Rüb[1], Jan Herbst[1], Rekha Reddy[1], Sogo Pierre Sanon[1],Yorman Munoz[1] and Hans Dieter Schotten[1,2]

[1]Intelligent Networks Research Group, German Research Center for Artificial Intelligence, Kaiserslautern, Germany

[2]Institute for Wireless Communication and Navigation, RPTU Kaiserslautern-Landau, Kaiserslautern, Germany

Christoph.Lipps@dfki.de
Annika.Tjabben@dfki.de
Matthias.Rueb@dfki.de
Jan.Herbst@dfki.de
Sogo_Pierre.Sanon@dfki.de
Rekha.Reddy@dfki.de
Yorman.Munoz@dfki.de
Hans_Dieter.Schotten@dfki.de

Abstract: Intelligent, comprehensive and, above all, secure wireless interconnection is the driving force behind technological progress. To ensure this, the development towards Sixth Generation (6G) Wireless Systems has been launched and is scheduled to be operational by 2030. This data technology of the future turns 6G into the infrastructure of a new generation of mobile, intelligent, and context-sensitive services, available everywhere and featuring high trustworthiness and performance, relying on both, network-side and off-network context sources. In addition, the networks themselves ought to become intelligent and thus more efficient and resource-saving, which requires a high degree of automated utilization of Artificial Intelligence (AI). Building upon the principles of information and communication theory for both the physical (bit)-transmission layer (PHY) and media access, new communication concepts for 6G will be developed providing the foundations for research into new single and multi-user operation, access and core networks.

The flip side of this coin of opportunities: Sophisticated technology inevitably leads to additional security vulnerabilities, open access systems and Open-Radio Access Network (O-RAN) approaches imply new attack vectors. The holistic interconnection of everything renders it ever more attractive to attackers to harm systems, and create damage. Furthermore, enhanced computational power along with quantum computers make conventional systems more vulnerable than ever, and the value of the transmitted data increases tremendously: It is not only machine and sensor data, but also very personal and healthcare data transmitted with 6G.

Therefore, the aim is to build a resilient and secure 6G system capable of recognizing attacks and uncertainties, flexibly absorbing them, recovering in a timely and sustainable manner, and compensating for impaired functionality through transformation. This holistic resilience-by-design approach is based, among other things, on technology such as Quantum Key Distribution (QKD) and Post Quantum-Crypto to achieve end-to-end security, Reconfigurable Intelligent Surfaces (RISs) to rely, control and manipulate the wireless transmission channel, Wireless Optical Communication (WOC), Physical Layer Security (PhySec), but also Body Area Networks (BANs), the integration of the human body relying on biometrics and the Tactile Internet (TI). These concepts will be discussed and shed light on in the scope of this work.

Keywords: Physical Layer Security; Physically Unclonable Functions; Human-PUFs; Channel-PUFs; (Cyber)Security; Sixth Generation; Body Area Networks (BANs);

1. The Next Generation Mobile Network: The Sixth Generation

The level of interconnection is continuing apace: While wired connectivity has been the standard in many areas, ranging from private applications to complex industrial networks, just a few years ago, a trend towards wireless connectivity is rapidly developing. Above all, the advantages of scalability (no need for cumbersome new cables as components are added), flexibility (no restriction on location), and cost efficiency (connectors and cables are expensive) speed up the process even more. And even if there is already a broad portfolio of technologies and standards, like Long Range Wide Area Networks (LoRaWAN), ZigBee, Industrial Radio and IEEE 802.11ax Wireless LAN -with the push to the 6GHz frequency range-, each associated with different advantages and disadvantages, (cellular) mobile radio is shifting into the scientific spotlight: Although the Fifth Generation (5G) Wireless System is currently in the global roll-out phase there are strong arguments for already considering its successor. The International Telecommunication Union (ITU), for instance, estimated that the total number of Mobile Broadband (MBB) subscribers worldwide will reach 17.01 billion by 2023 and Machine-to-Machine (M2M)

terminals will cross the 100 billion threshold within this time frame (International Telecommunication Union, 2015). Alongside the mere number of devices, the requirements for the technology are rising as well: disruptive innovations such as Holographic-Type Communications (HTC), Augmented- and Virtual Reality (AR/VR) towards an (industrial) metaverse, (Medical) Digital Twins ((M)DTs), Tactile Internet (TI) and a ubiquitously global connectivity are (over)demanding the existing infrastructure. Nevertheless, there is currently no single technology which can meet the whole range of requirements. Instead, contrary to this, and among other things, this is the key aspect during the development of 6G. Different technologies are considered as "6G enabling technologies": heterogeneous Radio Access Technology (RAT) and Open – Radio Access Networks (O-RANs) should provide flexibility, virtualization and intelligence while defining disaggregation and openness; the available and feasible spectrum will include mmWave and (sub)Terahertz (THz) ranges, including the spectrum of visible light as well as the dynamic management of the spectrum; Wireless Optical Communication (WOC) and Visible Light Communication (VLC) shall enable applications such as "data kiosks" and indoor communication unaffected by Radio Frequency (RF) interference; Reconfigurable Intelligent Surfaces (RISs), Intelligent Reflecting Surfaces (IRSs) and meta materials in general, shall be capable of controlling the wireless channel and its properties and of steering and relaying electromagnetic waves in the sense of sustainability and GreenICT as passive but controllable elements; Joint Communication And Sensing (JCAS) will enable a symbiosis between mobile communication and mobile sensing, allowing robots and Extended Reality (XR) applications to scan and perceive their environment (in indoor and outdoor environments); methods of Artificial Intelligence (AI) will have a huge impact, not simply because a core concept will be distributed computing, processing, and putting AI in the edge, but also because AI will be integrated into the air interfaces and applied as the basis for signal detection, synchronisation, channel estimation, equalisation, as well as modulation and coding. And all of these technological enablers, whose interconnections are highlighted in **Figure 1**, will have a direct impact on the security of the systems, the selection of appropriate security applications and the implementation of security measures.

The overall necessity for secure applications, as well as a general perspective, is described in Section 2. Based on this, the enabling technologies mentioned are specified in more detail in Section 3. These are evaluated, discussed and set in relationship to each other in Section 4, afterwards, Section 5 concludes the work and gives an outlook.

Figure 1: 6G as an enabler for the interconnection of the future of everyday life. In addition to increased availability, one of the design goals is to integrate "intelligence" into the edge and to incorporate the methods of artificial intelligence more effectively. This is achieved through a set of enabling technologies, including Wireless Optical Communication, Reconfigurable Intelligent Surfaces, Ultra-Massive MIMO and the usage of higher frequency ranges compared to the past.

2. Security of the Sixth Generation: A General Perspective

The demand for security and reliability is certainly as old as humanity itself: Potential threats emanating from strangers require detection and appropriate assessment; Trust has to be established, maintained and extended over time; Access and disclosure of information to untrustworthy persons shall be restricted. This is nothing particularly new, however, with increasing globalisation, the interconnection of everything with each other and the possibility of remote access from anywhere, the need for technological is increasing further. In addition, the development of the Sixth Generation Wireless Systems is oriented towards the infrastructure: the focus should be on people, and services and "intelligence" should be decentralized and brought to the edge and to the applications. This is accompanied by a particular need for security and privacy, especially if sensitive and personal information is transferred.

Already during the development of the previous version, the Fifth Generation (5G) mobile radio, self-optimisation, self-healing and self-configuration of the network had been one of the design criteria. This aspect is taken into account and extended towards a resilient infrastructure, which is covering the holistic cyber-resilience lifecycle including the detection of anomalies and threats, appropriate deception technology -to mislead, distract and gather (attack) information from the attacker-, but also mitigation and defensive applications as well as active encryption and recovery methods.

In addition, methods of Artificial Intelligence will be integrated into all parts of the processing stack. As AI is another enabling technology, and of pervasive and of pivotal relevance, trusted AI (Cohen, et al., 2019), trustworthy AI (Kaur, et al., 2022) and Machine Learning (ML) (Porambage, et al., 2021) addressing the privacy and security of the systems (Ma, et al., 2022), will be a crucial issue, also in terms of the acceptance of a wide range of people in the use of 6G and AI in general. The decentralisation of resources and the associated approach of integrating intelligence into the edge is achieved by methods of federated learning, secured, for instance, by Fully Homomorphic Encryption (FHE) (Sanon, et al., 2023).

Based on Industrial Internet of Things (IIoT) approaches to achieve integrity and authenticity of the entities involved (Lipps, et al., 2019), Trusted Execution Environment (TEE), Trusted Platform Modules (TPMs), Physically Unclonable Functions (PUFs) and flexible trust anchors (Ziegler, et al., 2021) will be taken into account to harden the multi-stakeholder environments against the multitude of potential attacker scenarios and -vectors.

Besides the general concepts, there are a number of key enabling technologies which in turn can have an individual impact on the security of the system.

3. Enabling the Sixth Generation: Technologies and their Security Implications

Starting in 2020, the development of Sixth Generation mobile communications is currently gaining momentum in Europe (Jiang, et al., 2021). Thereby, a decisive design feature is the integration and diversification of different technological approaches, so-called key enabling technologies: Due to the variety of requirements placed on the future infrastructure, there is no one-size-fits-all solution, but rather a conglomerate of these technologies deliberately intended to operate together and interact with each other.

3.1 (Sub) Terahertz Communication

One aspect of the 6G discussion is the use of higher frequency ranges in the Terahertz spectrum from 95 GHz up to 10 THz (Singh & Sicker, 2020), for which there are a number of relevant reasons to take a closer look: For numerous use cases such as Wireless Sensor Networks & Wireless Body Area Networks (BANs), (Unmanned) Aerial Vehicles ((U)Avs), Intelligent Transport Systems (ITS), Holographic-Type Communications (HTC) and application in the medical sector, this frequency range is considered particularly advantageous (Lipps, et al., 2021). One reason therefore is the reduced interference with the common spectrum which would unload the data traffic of these frequencies (Singh & Sicker, 2020). Furthermore, due to the huge potentially applicable frequency band, it is considered as an enabler for Ultra-high throughput applications. Applications like Tactile Internet, Extremely Dense Networks (EDN)s & Internet of Things (IoT) will benefit therefrom.

However, the shift to higher frequencies is also of relevance particularly in terms of security: Vulnerabilities of commonly used spectrum related to Fake Base Station-, Man-in-the Middle (MitM)-, and Denial of Service (DoS) attacks, as well as user impersonation and eavesdropping could be remedied significantly. A lower coverage and lower penetration power renders the system inherently more secure, as, for instance, Non-Line-of-Sight (N-LoS) attacks can be blocked and mitigated by performing enhanced beamforming and smart shielding. The higher

energy radiation -in comparison to the common spectrum-, has a lower penetration depth into different materials which leads to fast absorption in N-LoS situations. Besides, systems working in the scope of anti-jamming could be enhanced: Due to the large frequency range of the THz-Spectrum, the approach of Frequency Hopping (FH) for anti-jamming could be extended. The aspect of enhanced beamforming adds an extra level of security against jammers; attackers would have to perfectly align to the signal which is a almost impossible task, due to the complex technology needed to achieve this in an undetected manner (Singh & Sicker, 2020).

3.2 Reconfigurable Intelligent Surfaces

Reconfigurable Intelligent Surfaces are another emerging topic in the context of the new generation wireless communications. Building up of several, commonly passive, antennas elements these “man-made surfaces” (Pan, et al., 2021) are capable of manipulating the reflecting characteristics of electromagnetic waves. To achieve this, such surfaces consist of a multitude of sub-wavelength wide elements each of which independently controllable and adjustable. Specific modification of the characteristic enables an impinging wave signal to be reflected in the desired direction.

These attributed features of being able to manipulate a channel have a direct influence on security, therefore *Lipps et al.* (2022) specified conceivable scenarios in which RIS can be used to increase this security: i) RIS-enabled beamforming and -splitting, which can mitigate the risk of eavesdropping through the possibility of steered communication towards legitimate users. Besides, tighter beams up to pencil-sharp beamforming can chance the overall properties of a radio link from a broadcast medium to a targeted communication. ii) RIS-based Anti-jamming, whereby the mentioned broadcast characteristic renders the system in general vulnerable to conscious and unconscious interferences, and RISs can help by destructive and constructive superimposition of signals, as well as by phase-shifting the reflected signals; iii) RIS-manipulated channel-profiles, which are the basis for Physical Layer Security (PhySec) Secret Key Generation (SKG) and whose key derivation can be enhanced by additionally introduced entropy, thereby increasing security; iv) RIS-individual fingerprints, where, based on the principle of Physically Unclonable Functions (PUFs). It can be assumed that each RIS exhibits a hardware-based individual fingerprint and thus characteristic properties which can be measured and included as a security feature, and v) RIS-supported additional context information, which, similar to unintentional fingerprinting, can also be actively and consciously used as an additional context.

Besides, the combination of RISs with other technologies such as VLC is a conceivable approach to enable the combined potential of both. *Rüb et al*. (2022) are discussing some of the benefits regarding the use of laser-based VLC with RIS and are describing approaches towards the security of a VLC system.

3.3 Wireless Optical Communications

With increasing interconnectivity there is a rising number of devices communicating with each other. As the available Radio Frequencies spectrum is limited, this will cause major challenges in the future. Besides the shift of higher THz frequency ranges, the consideration of Optical Wireless Communication is discussed.

This form of communication uses the broad unregulated optical spectrum, which is sub-divided into Infrared, Visible Light and Ultraviolet, each giving rise to different implementations for high-speed wireless communication. Furthermore, for OWC, in contrast to RF, the interference problem does not arise. Current research on OWC focuses on establishing a connection with a sufficiently high data rate (an overview of recently achieved data rates is given in (Elgala, et al., 2011)) while at the same time ensuring the security of the transmission.

At first glance OWC seems to provide a higher level of security due to the transmission being limited by walls and obstacles. Yet the low cost and limited computing power of many devices renders them unsuitable for standard cryptographic approaches (Anon., 2019). Since OWC differs fundamentally from other wireless networks different approaches need to be followed to ensure secure transmission. One method tries to adapt different modulation schemes to bring a positive benefit to the security of the system. Recently *Panayirci et al.* (2020) apply the Spatial modulation technique, which reduces inter-channel interference, together with a novel spatial constellation design technique aimed at enhancing the physical layer security. Furthermore, it turns out that OWC is vulnerable to integrity attacks. *Soderi and De Nicola* (2021) show that the Watermark Blind Physical Layer Security (WBPLSec) algorithm, a combination of watermarking and jamming, can be used to ensure secure communication against these attacks. These recent approaches are promising, but they only consider single security aspects. To find a general solution for the security of OWC further research is required.

3.4 Localisation & Sensing

Robots and (U)AVs are just one aspect of future technologies expected to be a part of our everyday life. As by now autonomous driving vehicles can already be seen on the streets. Mobile working robots and vehicles should record their 3D surrounding, which mostly is done using radar, camera, or spectroscopy systems. To meet the demand for accuracy in sensing and supported data rates of up to 100 Gb/s the idea is to combine both, communication and sensing together into a joint system and frequency spectrum (Fettweis et. al., 2021). The mobile spectrum itself will barely support needed data rates with the common frequency spectrum, on the other hand, mobile resources for broadband communication are only rarely needed at the same time for mobile sensing. JCA&S is the integration of both, communication and localization sensor technology in one common system. *Fang et al.* (2022) pointed out, that regarding security there is a conflict of interest between those topics as the sensing part needs to interact strongly with the environment which increases the risk of eavesdropping on the communication. Additionally, they highlight the risk of sensing targets being malicious, as in contrast to communication they are not checked for legitimacy.

Another issue is the information leakage that could occur between the two activities. *Günlü et al.* (2022) investigate several modelling approaches for the complex interplay of sensing performance and secrecy performance which are both evaluated based on the signal strength at the sensed target, which could be malicious. In general, a convincing security solution to address the above-mentioned issues requires more future investigations.

3.5 Link Integrity Monitoring and Anomaly Detection

Integrity monitoring comprises the regular review of available information regarding correctness and origin. This is an important concept in a variety of applications, like position parameters of vehicles in the scope of self-driving cars and sensor data in IoT networks, for example, in agriculture scenarios. Link integrity monitoring of wireless communication refers to the question if an established link is originated by a legitimate source or a malicious third party. For upcoming wireless networks, it is necessary to evaluate, if it could be possible to transfer existing concepts of integrity monitoring with methods of AI onto the specific use-case of link integrity monitoring in wireless networks.

Furthermore, integrity monitoring is closely related to anomaly detection, as non-legitimate sources will stand out for example in their high-level parameters (data rate, time of connection, reception angle) or the content of information. With the dynamic adaption of attackers and the expected high density of IoT devices, state-of-the-art solutions for Intrusion Detection Systems (IDS) are no longer sufficient (Oleiwi, et al., 2022). Recent works have applied new combinations of different AI approaches including data preparation and feature extraction with classic machine learning algorithms (Mittal, et al., 2021) and the final step of intrusion detection with deep learning (Gupta, et al., 2022). Especially promising is the combination of several models in an ensemble learning approach to detect anomalies (Jaw & Wang, 2021). *Oleiwi et al.* (2022) proposed in 2022 an approach for intrusion detection with two modified classic algorithms: random forest and support vector machine, achieving an accuracy above 99 %.

Recent approaches especially focus on energy efficiency, as multiple AI algorithms for intrusion detection – especially deep learning techniques– require a high computing power. Especially for dynamic systems which require retraining of existing artificial neural networks could be very energy consuming. In summary, integrity monitoring and anomaly detection in upcoming wireless networks will most likely consist of ensemble models of multiple machine learning approaches. One major concern will be to make the utilized algorithms energy efficient to positively impact the trade-off between cost and security.

3.6 Security in the Post-Quantum era

Post-Quantum Cryptography (PQC) constructs and studies cryptosystems that are secure against both quantum and classical computers. Existing public-key cryptosystems are based on the difficulty of factoring and the difficulty of calculating elliptic curve discrete logarithms, but then, *Shor (1994)* developed a quantum algorithm which can effectively solve those problems. Hence, proving that quantum computers would eventually be able to break current security systems in a relatively short amount of time.

In recent years, many systems conjectured to resist quantum attacks have been proposed for the replacement of current public-key protocols. This prompted the National Institute of Standards and Technology (NIST) to start a standardization process (Chen, et al., 2016), to produce strong quantum cryptographic standards which are

expected to appear in 2024. NIST is well known for standardizing cryptographic algorithms. For instance, the symmetric-key algorithm Advanced Encryption Standard (AES), which is widely used nowadays, was established by NIST in 2001 after a process like the PQC Standardization (Nechvatal, et al., 2001). The PQC algorithms established by NIST are expected to be adopted in most use cases around the world.

At the time of writing, NIST has already completed three rounds in the selection process and has already selected four algorithms to be standardized, one public-key encryption algorithm and three digital signature algorithms. There are four additional algorithms, all for public-key encryption, that will go through the fourth round and any of them can be standardized. More details on the algorithms can be found in (Alagic, et al., 2022).

As wireless communication becomes increasingly important and use cases getting diverse more than ever, the security aspect becomes crucial. PQC needs to be considered in future generations and incorporated in their architectures. In addition, further investigations regarding the most suitable algorithm for wireless communication among those that will be standardized need to be conducted.

4. Discussion and Evaluation of 6G-enabling Technologies

The development of the Sixth Generation Wireless Systems will not rely on a specific technology, but rather on different aspects, each associated with individual strengths and weaknesses. Yet, as already indicated, they cover a wide range of topics, from Reconfigurable Intelligent Surfaces to Wireless Optical Communication to Post-Quantum Security. To still provide a statement about the suitability and usability of the applications in possible uses-cases, several Key Performance Indicators (KPIs) are to be defined, on the basis of which an evaluation can be carried out. However, these KPIs only represent a high-level overview and have to be fine-tuned to be finer-grained and more specific in further work:

- **Detection**: This refers to an assessment of the extent to which the technology can contribute to the detection of attackers and intruders.
- **Prevention**: The ability to stop intruders from stealing or altering information of the legitimate communication link.
- **Cost**: Total cost of a system including the initial setup/purchase and continuous cost like energy consumption.
- **Applicability**: For a widespread application, it is necessary that the system does not affect the performance and functionality of the communication link.
- **Usability:** Describes how practicable a technology is (especially in daily use).
- **State of development:** This KPI evaluates the subjective state of research regarding the topic. Especially many open challenges will result in a low evaluation.

4.1 (Sub)THz communication

The usage of higher frequency ranges offers advantages, especially with regard to the possible data rate and the applicability in combination with localisation, but also entails disadvantages such as higher susceptibility to interference. Nevertheless, it remains a broadcast system rendering it difficult to detect attackers and intruders. However, tighter beams allow for narrower band communication and can make eavesdropping more difficult. Another limiting factor can be the communication itself: The usage of higher frequencies is associated with high path losses and low coverage in the range of only a few meters. Thereby, this limits the accessibility, does not allow long-range communication and indicates at least the need for expensive communication hardware. In addition, various materials and molecules have their absorption resonance in the range of this frequency space, leading to high spreading losses. Even for short communication distances between the THz links sensitive user information are needed and must be shared across the wireless system, for instance, user´s localization, device orientation, mobile patterns, and surrounding environments up to blockages because of LOS requirements.

(Singh & Sicker, 2020) therefore talked about the “Gap of THz” communication and the lack of efficient and cheap THz signal generators as well as receivers. They propose to use existing and developed technologies in the field of imaging/ spectroscopy, which are having increased knowledge, hardware, and detectors related to THz.

4.2 Reconfigurable Intelligent Surfaces

RISs are a frequently discussed and active field of research. Even though the idea is not completely new, the approach provides advantages, especially when used as a passive element and in terms of sustainability and

GreenICT. These increase the flexibility of the communication system and allow the radio channel to be tailored to the current conditions and needs. However, if the RIS implementations are used in combination with higher frequencies (THz) range, they are offering “raw-power” in terms of transmission rate, but are very inflexible due to the limited transmission range due to high absorption not only by air but also by (moving) obstacles like persons or vehicles. In addition, it is not yet clear how large functional RIS will really be in the end. Their acquisition and construction - especially using PIN diodes - is still very expensive and there are few to no commercial manufacturers on the market. What remains to be observed is the effect once the corresponding meta-materials are available and can be used accordingly.

4.3 Wireless Optical Communication

The approach of using (visible) light for communication is also not entirely new; this technology has been proven and is effective, especially in fibre-optic and photonic systems. Using wireless technology - which is likewise just electromagnetic waves - poses challenges, however, as systems are interfered with by natural light, sunlight and lamps, for example. On the other hand, the systems are not affected by RF signals, which makes a combination with them attractive. For security applications: visible light is already blocked by simple walls, in contrast to RF signals, which complicates eavesdropping and at the same time increases the probability of detecting an attacker. Moreover, the technology and the use of for instance lasers are well researched and open source systems already exist for the utilization and simple implementation.

4.4 Localisation & Sensing

Joint Communication and Sensing offers promising possibilities, particularly in combination with high frequencies in the THz range and the associated accuracy in the sub-centimetre range, although the above-mentioned effects and disadvantages of THz must be taken into account. In combination with the possibility of tight beams and beam-steering, JCAS offers the opportunity of targeted communication and thereby minimizing jamming, spoofing and eavesdropping, as the directions of the attackers can be localized and avoided. In addition, it is a technology that requires either no or very few additional hardware, but rather is to be integrated into existing communication systems, making it a by-product. This reduces costs, which in turn makes it more attractive for industrial applications.

4.5 Link Integrity Monitoring and Anomaly Detection

Monitoring and verifying the integrity of network nodes in operation is an essential component of network security and cyber resilience. By monitoring anomalies, suspicious events in networks are detected and appropriate countermeasures such as re-routing, shifting of resources or shutdown are made possible. By integrating methods of artificial intelligence, which only require appropriate computing power, these systems can be operated at rather low costs, but provide important and essential information about the status of a network. With appropriate configuration, many of these systems are quite applicable, but can be strongly enhanced with appropriate expert knowledge.

Table 1: Key performance indicators for the enabling Technologies discussed, related to security applications. (The evaluation of the different approaches is indicated as positively (+) / average (o) / below average (-). If current research is not feasible yet to give a convincing indication, the topic is marked as under investigation (UI).

	(sub)THz communication	RIS	WOC	Localization & Sensing	Link Integrity Monitoring & Anomaly Detection	Post-Quantum Security
Detection	o	+	+	+	+	o
Prevention	+	+	o	-	+	+
Cost	o	UI	+	+	+	-
Applicability	+	+	+	+	+	+
Usability	+	o	+	+	+	o
State of Develop-ment	+	-	+	UI	o	-

4.6 Post-Quantum Security

Developments in quantum communications are a sword of Damocles hanging over the current security landscape. Experts often postulate that breakthroughs in quantum technology will have a massive impact on existing cryptographic methods, as they can be broken in a fraction of the time it used to take. However, these developments i) are currently not available and ii) there are also ambitions for quantum security applications such as quantum tokens. Nevertheless, it is certainly sensible to rely on quantum safe solutions such as Physical Layer Security (at least as complement/extension and additional factor), as these are not based on computational complexity but rather on inherent secrets and characteristics.

5. Conclusion and Future Work

The work discusses the ideas and directions emerging in the current development of the Sixth Generation Wireless Systems, being worked on in different research directions. Thereby, starting from expectations of applications such as Holographic-Type Communication, Tactile Internet, Augmented-/Virtual- and Extended Reality, (Medical) Digital Twins and the (industrial) metaverse in general, technologies have been identified in order to satisfy them. Because these applications not only transfer much more business-sensitive information, but also personal data and data requiring special protection. The security requirements are perhaps higher than ever before. For this purpose, the 6G-enabling technologies were not just described in this work, but their influence and impact on security and security applications have been discussed as well.

All of the technologies discussed have a direct impact on security, but are at different stages of development. Reconfigurable Intelligent Surfaces, for instance, are a frequently discussed topic within the research community (even if the idea is not that new) and a lot of time and resources are being invested right now. Although these are rather expensive to produce (particularly the PIN diodes), and it is currently assumed that larger surfaces will be required (in the direction of the walls of the houses), which remains open for discussion. However, since a lot of research is being done in this field right now, it is worthwhile to focus on security requirements as well and to consider these fundamental aspects. Generally speaking, this is the major advantage of the current stage of development: 6G is still in the development phase, with the first steps toward standardization not being taken before roughly 2025. Right now, fundamental aspects such as Security-as-a-Service, Security-by-Design and the trend towards Post-Quantum Security can be taken into consideration within the development. It is essential to raise awareness and to already create broad acceptance, not only among the scientific community, but also among future applicants, not only for technology 6G, but also and above all for the methods of Artificial Intelligence. After all, this is where a significant amount of work will be required and where is potential for further research: trusted AI and trustworthy AI.

Acknowledgment

This work has been supported by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 16KIS1283 AI-NET PROTECT). The authors alone are responsible for the content of the paper.

References

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D. and Liu, Y.-K., "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process", *Information Technology Laboratory, Computer Security Resource Center,* National Institute of Standards and Technology, Gaithersburg, MD, USA, 2022.

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D., "Report on Post-Quantum Cryptography", *Computer Security Division, Applied and Computational Mathematics Devision, Information Technoloy Laboratory,* National Institute of Standards and Technology, Gaithersburg, MD, USA, 2016.

Chorti, A., Barreto, A.N., Köpsell, S., Zoli, M., Chafli, M., Sehier, P., Fettweis, G. and Poor H.V., "Context-Aware Security for 6G Wireless: The Role of Physical Layer Security", *IEEE Communications Standards Magazine,* vol. 6, no. 1, pp. 102--108, DOI: 10/1109/MCOMSTD.0001.2000082, 2022.

Cohen, R., Schaekermann, M., Liu, A. and Cormier, M., "Trusted AI and the Contribution of Trusted Modelling in Multiagent Systems", *Proceedings of the 18th International Conference on Autonomous Agents MultiAgent Systems,* pp. 1644--1648, DOI:1.5555/3306127.3331890, 2019.

Elgala, H., Mesleh, R. and Haas H., "Indoor Optical Wireless Communication: Potential and State-of-the-Art", *IEEE Communications Magazine*, vol. 49, no. 9, pp:56--62, DOI:10.1109/MCOM.2011.6011734, 22011.

Fang, X., Feng, W., Chen, Y., Ge, N. and Zhang, Y., "Joint Communication and Sensing: Models and Potentials of Using MIMO", *ArXiV - Electrical Engineering and Systems Science - Signal Processing*, arXiv:2205.09409, 2022.

Günlü, O., Bloch, M., Schaefer, R.F. and Yener, A., "Secure Joint Communication and Sensing", *IEEE International Symposium on Information Theory (ISIT)*, Espoo, Finland, DOI: 10.1109/ISIT50566.2022.9834748, 2022.

Gupta, N., Jindal, V. and Bedi, P., "CSE-IDS: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network.based intrusion detection systems", *Computer & Security*, vol. 112, DOI: 10.1016/j.cose.2021.102499, 2022.

IEEE Standard for local and Metropolitan Area Networks -- Part 15.7: Short-Range Wireless Optical Communication Using Visible Light, IEEE Std 802.15.7-2011, DOI:10.1109/IEEESTD.2011.6016195

International Telecommunication Union, "IMT Traffic estimated for the years 2020 to 2030", M Series Mobile, radiodetermination, amateur and related satelliteservices Report ITU-R M.2370-0.

Jaw., E. and Wang, X., "Deature Selection and Ensemble-Based Intrusion Detection System: An Efficient and Comprehensive Approach", *symmetry,* vol. 13, no. 10, DOI:10.3390*sym13101764, 2021.

Jiang, W., Han, B., Habibi, M.A. and Schotten, H.D., "The Road Towards 6G: A Comprehensive Survey", *IEEE Open Journal of the Communications Society*, vol. 2, pp. 334--366, DOI:10.1109/OJCOMS.2021.3057679, 2021.

Kaur, D., Uslu, S., Rittichier, K.J. and Durresi, A., "Trustworthy Artificial Intelligence: A Review", *ACM Computing Surveys,* vol. 55, no. 39, pp. 1--38, DOI: 10.1145/3491209, 2022.

Lipps, C., Baradie, S., Noushinfar, M., Herbst, J., Weinand, A. and Schotten, H.D., "Towards the Sixth Generation (6G) Wireless Systems: Thoughts on Physical Layer Security", *Mobile Communication - Technologies and Applications; 25th ITG-Symposium*, Osnabrück, Germany, 2021.

Lipps, C., Duque Anton, S. and Schotten, H.D., "Enabling Trust in IIoT: A PhySec Based Approach", *International Conference on Cyber Warfare and Security*, Stellenosch, South Africa, 2019.

Lipps, C., Herbst, J., Reddy, R., Franke, L., Becker, S., Rahm, M. and Schotten, H.D., "Reconfigurable Intelligent Surfaces: A Physical Layer Security Perspective", *4th International Conference on Data Intelligence and Security (ICDIS)*, Shenzhen, China, DOI: 10.1109/ICDIS55630.2022.00034, 2022.

Lipps, C., Weinand, A., Krummacker, D., Fischer, C. and Schotten, H.D., "Proof of Concept for IoT Device Authentication Based on SRAM PUFs Using ATMEGA 2560-MCU", *1st International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, USA, DOI: 10.1109/ICDIS.2018.0001, 2018.

Ma, C., Li, J., Wei, K., Liu, B., Ding, M., Yuan, L., Han, Z. and Poor, V., "Trusted AI in Multi-Agent Systems: An Overview of Privacy and Security for Distributed Learning", *Computer Science - Distributed, Parallel, and Cluster Computing*, arXiv:2202.09027, 2022.

Mittal, M., de Prado, R.P., Kawai, Y., Nakajima, S. and Munoz-Exposito, J.E., "Machine Learning Techniques for Energy Efficient and Anomaly Detection in Hybrid Wireless ensor Networks", *energies*, DOI: 10.3390/en14113125, 2021.

Nechvatal, J.R., Barker, E.B., Bassham, L.E., Burr, W.E., Dworkin, M.J., Foti, J. and Roback, R., "Report on the Development of the Advanced Encryption Standard (AES)", *Journal of Research (NIST JRES),* National Institute of Standards and Technology, Gaithersburg, MD, USA, 2001.

Oleiwi, H., Mhawi, D.N. and Al-Raweshidy, H., "MLTs-ADCNs: Machine Learning Techniques for Anomaly Detection in Communication Networks", *IEEE Access*, vol. 10, pp. 91006--91017, DOI: 10.1109/ACCESS.2022.3201869, 2022.

Panayirci, E., Yesilkaya, A., Cogalan, T., Poor, H.V. and Haas, H., "Physical-Layer Security With Optical Generalized Space Shift Keying", *IEEE Transactions on Communications,* vol. 68, no. 5, pp. 3042--3056, DOI: 10.1109/TCOMM.2020.2969867, 2020.

Pan, C., Ren, H., Wang, K., Kolb, J.F., Elkashlan, M., Chen, M., Di Renzo, M., Hao, Y., Wang, J., Swindlehurst, A.L., Yoi, X., and Hanzo, L., "Reconfigurable Intelligent Surfaces for 6G Systems: Principles, Applications, and Research Directions", *IEEE Communications Magazine*, vol. 59, no. 6, DOI: 10.1109/MCOM.001.2001076, 2021.

Porambage, P., Gür, G..m Osorio, D.P.M, Livanage, M. and Yilanttila, M., "6G Security Challenges and Potential Solutions", *Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit),* Porto, Portugal, DOI: 10.1109/EuCNC76GSummit51104.2021.9482609, 2021

Rüb, M., Tjabben, A., Munoz, Y., Grüber, J., Ahr, P., Herbst, J. and Lipps, C., "A Symbiotic 6G Enabler: Combining Laser based Visible Light Communication with Reconfigurable Intelligent Surfaces", *Workshop on Next Generation Networks and Applications (NGNA),* Kaiserslautern, Germany, DOI: 10.13140/RG.2.2.24818.38084, 2022.

Sanon, S. P., Reddy, R., Lipps, C. and Schotten, H.D., "Secure Federated Learning: An Evaluation of Homomorphic Encrypted Network Traffic Prediction", *IEEE Consumer Communications & Networking Conference*, Las Vegas, USA, 2023.

Shor, P.W., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, DOI: 10.1109/SFCS.1994.365700, 1994.

Zeng, S., Zhang, H., Di, B., Han, Z. and Song, L., "Reconfigurable Intelligent Surfaces /RIS) Assisted Wireless Coverage Extension: RIS Orientation and Location Optimization", *IEEE Communication Letters*, vol. 25, no., 1, pp. 269--273, DOI:10.1109/LCOMM.2020.3025345, 2021.

Singh, R. and Sicker, D., "THz Communications - a Boon and/or Bane for Security, Privacy, and National Security", *TPRC48: The 48th Research Conference on Communication, Information and INternet Policy,* 2020.

Soderi, S., and De Nicola, R., "6G Networks Physical Layer Security Using RGB Visible Light Communications", *IEEE Access*, vol. 10, pp. 5482--5496, DOI: 10.1109/ACCESS.2021.3139456, 2021.

Ziegler, V., Schneider, P., Viswanathan, H., Montag, M., Kanugovi, S. and Rezaki, A., "Security and Trust in the 6G Era", *IEEE Access*, vol. 9, pp.142314--142327, DOI: 10.1109/ACCESS.2021.3120143, 2021.