Review Scientific Paper/pregled naučni rad UDC/UDK: 004.738.5.056
Paper Accepted/Rad prihvaćen: 15. 1. 2021. 621.39:004.8
doi: 10.5937/SJEM2101001H

Kvantna bezbednost i 6G kritična infrastruktura

Miloslav Hoschek[1]

[1]e-Silk Road, NGO, mhoschek@yahoo.com

Apstrakt: Sredinom 2030-ih na polju odbrane i komunikacija nacionalne bezbednosti kvantni računari i 6G veštačka inteligencija će imati prevalst. 6G komunikacija je prihvaćena u različitim mobilnim poređenjima podataka koja se prenose spektralnim tehnologijama. Ljudsko telo postaje deo mrežne arhitekture 6G. Skup mrežnih čvorova ili nosivih uređaja, ugrađeni senzori ili nanodi prikupljaju poverljive informacije koje se razmenjuju u više svrha, kao što su zdravlje, statistika i bezbednost. Važan deo nove paradigme 6G biće inteligentne reflektujuće površine, kvantna teleportacija, kvantno šifrovane poruke, 6G holografija, distribuirana knjiga, 6G bezbednosne pretnje. 6G bežični standardi omogućiće brzu Internet komunikaciju u vremenskom pojasu u realnom vremenu sa podacima od 1TB u sekundi. Mreže radio frekvencija, THZ komunikacije, molekularne komunikacije i kvantne komunikacije dramatično će poboljšati brzine prenosa podataka.

Ključne reči: 6G kvantna bezbednost, kvantna metrologija, kvantna teleportacija, 6G šifrovane poruke, 6G holografija, ljudske veze 6G ere, 6G bezbednosne pretnje, 6G harmonija,

Quantum Security and 6G Critical Infrastructure

Abstract: In the mid 2030-s in the field of defense and national security communications the quantum computers and 6G artificial intelligence will have domination. 6G communication is accepted in a variety of mobile data comparts transmitted through spectral technologies. The human body becomes a part of the 6G network architecture. A set of network nodes or wearable devices, embedded sensors or nanodes collect confidential information that is exchanged for multiple purposes, such as health, statistics, and safety. An important part of the 6G new paradigm will be intelligent reflective surfaces, quantum teleportation, quantum encrypted messaging, 6G holography, distributed ledger, 6G layer security threats. The 6G wireless standards will allow real-time time zone high-speed internet communication with 1TB data per second. The radio frequency networks, THZ communications, molecular communications, and quantum communications will dramatically improve data rates.

Key words: 6G quantum security, quantum metrology, quantum teleportation, 6G encrypted messaging, 6G holography, human-bonds 6G era, 6G security threats, 6G harmony,

1. Introduction

A single quantum computer is more powerful than all supercomputers in today's world. In theory, if quantum computing is fully mastered, it will be very dangerous to the state critical infrastructure, due to the very difficult nature of protecting networks, databases or artificial intelligence. Armed conflicts can be fought on a larger scale than ever before and faster than humans can understand the threat to national security. It is now the subject of ongoing debate in the world of standards such as immutability, privacy protection, transparency, verifiability, anonymity, and the functionality of quantum technologies. The cyber attacks on existing artificial intelligence systems; the implementation of artificial intelligence in conventional military wars is a greater overall threat to national security.
Cyber attacks against individuals, businesses and governments for destruction in such a way that puts a great strain on artificial intelligence databases. The pace of operation and engineering challenges of quantum mechanics and the rapid development of quantum computers double the number of qubits on quantum computer processor chips every six months.

2. Review

6G warranty for hyper-connected world

6G is considered to be a complete connecting fabric, the nodes of which range from satellites to the interior of the human body. This ultra-dense network of heterogeneous nodes often provides tons of highly confidential information.The 6G will have a password to enter the connection of the world. These combinations of billion devices and nodes on the land, in the marine, and space providing a high bandwidth, high density and cloud intelligent security functions (Ylianttila et al., 2020). 6G containers are grouped into pods, each pod consists of multiple containers on a single quantum machine.The 6G traffic gateway (Boixo et al., 2014) and container technology meet the needs of security functions with ultra fast restart, with enhanced utilization, and storage.

The performance constraints of common internet of things - IoT devices, the offload of computing, storage, and network features to other nodes will increase and eventually become a common place feature of 6G. A reliable and low latency throughput is estimated, it is natural that a variety of 6G calculations will be both off-load from the terminal to the IoT network and off-load from the network to the network. Specific terminals or data centers of customer facilities in factories, smart cities, and smart hospitals.

Quantum Computing Security

A cyber attack on a top secret database or on a power grid database can result serious infrastructure damage and massive human casualties (Kline and Salvo, 2019). A large-scale cyber attack can cause more damage than the use of hard-force by conventional methods of weaponry. Code-breaking and public-key encryption vulnerabilities make users more susceptible to cyberterrorism threats. Cybersecurity could be a threat to quantum computing (Table 1). A vulnerable cyberattack that does not send a message to the optical particles of the network using quantum.

Table 1. Quantum Security in 6G Architecture

Quantum Security in 6G Architecture
Wide-area trust management across multiple trust domains
Privacy trust systems protection
AI anonymization
High network scalability and different forms of active malicious attacks
Artificial intelligence dynamically adjust physical layer security algorithms
Access security (inbound, outbound gateway endpoint security
Cloud security edge cloud central cloud
Automation vision based on full visibility
Leverage AI to provide complete end-to-end real-time protection
Challenging characterized by high network scalability

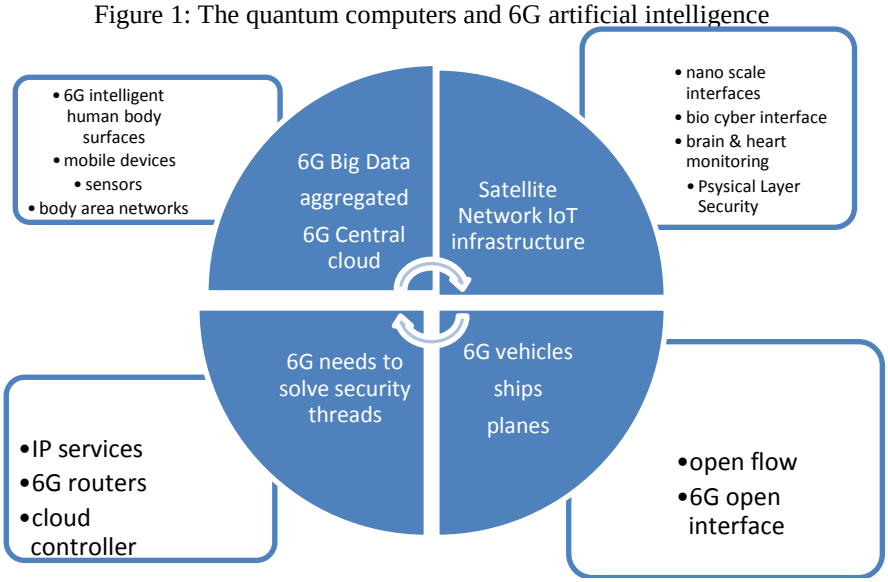
(Source: author)

The implications of artificial intelligence and quantum computing are enormous. The enormous capabilities and vulnerabilities of intelligence in these two fields over cyber warfare can be exploited as a big advantage among new battlegrounds in cyberspace. The purpose of the efficient feedback control is to adapt the idle time to a given value for learning the change of the traffic dynamics by the constitutive intelligence. The capabilities of these threads, whether passive or active, help to identify and protect the artificial intelligence against cybersecurity attacks. The importance of this process is the ability to effectively manage multiple current threads while simultaneously performing high-traffic tasks such as data transfer.

6G artificial intelligence

Quantum computers exist in multiple "states" at once, exploiting the unique qualities of subatomic particles rather than manipulating bits. Quantum computers can manipulate these particles to perform many calculations at the same time, which speeds up solving complex problems such as cracking encryption. More companies are using machine learning and other tools to build algorithmic trading systems that learn from data without resorting to rule-based systems (Merat and Almuhtadi, 2015).

Figure 1: The quantum computers and 6G artificial intelligence



(Source: author)

The evolution of artificial intelligence and quantum computing in modern warfare will also have an impact on security (Allen and Chan, 2018). The digital artificial intelligence must resist the future attacks to secure cyberspace. The artificial intelligence can harm as a weapon. However, the current encryption measures will be outdated. With the adoption of data scientists, advances in cloud computing, and access to an open-source framework for the artificial intelligence (Figure 1) quantum computing machine learning model, big banks are already developing self-learning algorithms.

Traditional algorithms are created by programmers and quant strategists, but these algorithms, based on if/then rules, use machine learning to learn the best trading patterns and pass them on to machines to automatically update the algorithms without human intervention. Instead of using mathematical complexity to encrypt messages, it relies on certain rules of quantum physics. With quantum information, you can't copy it or cut it in half, and you can't even see it without changing it. This allows for much more secure encryption than it is today.

6G quantum internet

Quantum internet will demonstrate the integration of the first of both sub-systems, pushing the frontier of technologies for both end nodes such as trapped ion qubit, diamond NV qubit, neutral atomic quantum bit and quantum rare earth-based memory repeaters, atomic gas. This makes the leap from a simple point-to-point connection to the first multi-node network. The major possible features for memory-based quantum repeaters.

Performance constraints of common IoT devices, increased offloading of computing, storage, and network features to other nodes, will eventually result in a common place feature of reliable and low latency 6G. This ultra-dense network of heterogeneous nodes often provides very sensitive information. It is natural that the various 6G calculation will be both loaded from the terminal to the IoT network. 6G is considered to be a complete connecting the nodes from satellites (Björnson, 2019) to the human body or to the smart customer facility as hospital, factory or smart city.

The 6G potential technologies

Cyberattacks on a top secret databases and power grid databases can cause serious damage to infrastructure and to massive human casualties. The main cause of cyber attacks can be traced back to software that guarantees system errors, rather than other causes such as hardware intelligence. This type of failure can result in problems such as firewalls or security programs, which can lead to repeated task management errors and incorrect threads in the soft process (Gyongyosi and Imre, 2019). A new

6G cyber security technologies (Table 2) will make users more susceptible to quantum computing cyber threats against code-breaking vulnerability and public key encryption.

Table 2. The 6G potential technologies

The 6G potential technologies
New meta data commands
The cross layer design breaks the end to end principle
High precission synchronisation
Multiplex advanced network functions
Multipath transmission
New network protocol architecture
New internet architecture
Cannot guarrantee future application delivery contrains such as deterministic throughput, metric or security details or ultra low latency
Distributed artificial inteligence
Communication catching control
Local patterns sent to central cloud
Obtaining global model
New classification ITU International Telecommunication Union
The evolution of connectivity ultra-high speed, large capacity, and low latency
Development of new frequency bands including terahertz frequency
Providing ultra-low energy and ultra-low cost communications
6G devices-connectivity

(Source: author)

The impact of artificial intelligence and quantum computing of cyber warfare can be exploited as a major advantage among new battlefields in cyberspace. The large-scale cyberattacks can cause more damage than the use of hard force by conventional weapon methods. The purpose of efficient feedback control is to adapt the idle time to a given value to learn changes in traffic dynamics by cognitive intelligence (Latva-aho and Leppänen, 2019). High-traffic tasks data transfer protection can effectively manage multiple threads. The firewall is excluded because of either passive or active attacks that can be initiated within the security. The functionality of these threads helps simultaneously to identify and protect artificial intelligence from cyber security attacks perimeter.

Quantum teleportation

The easiest way to understand the concept of the quantum Internet is through the concept of quantum teleportation. The possibility of a space-based quantum internet where satellites continuously broadcast entangled photons down to the Earth's surface. In quantum teleportation, two people who want to communicate share a pair of intertwined quantum particles.

Through a series of operations, the transmitting side can transmit any quantum information to the receiving side. It can't do faster than the speed of light, but it's a common misconception. The central research question is how best to distribute these intertwined pairs to people distributed around the world.

Hand in hand with hardware development, quantum internet industry partners have verified elementary safe quantum cloud computing platform verified by a large-scale simulation of the pan-european quantum Internet (EU, 2015). The design of the blueprint architecture is providing fast and reactive control when used in the real world.

Quantum encrypted messages

A space-based quantum internet is a new type of computer based on quantum physics could break modern cryptography (Bernstein and Lange, 2017). In quantum encrypted messages, the shared key is discarded and everyone is alerted about the compromised an ultra-secure communication network. The current artificial intelligence systems are starting to see data breaches from unknown sources because of insecure centralized servers that hold valuable information. An artificial intelligence will be used not only to implement complex problem solving and reasoning skills like humans, but also weapon systems that can have fully autonomous capabilities. If this growth pattern continues, qubit processors will be able to decipher the one of the most widely cryptographic system, the Rivest–Shamir–Adleman tool.

The singularity of a quantum superposition, where the quantum properties of an object occupy multiple states at once, and these quantum states are shared among multiple objects. The future 6G internet are based on these quantum principles. The quantum internet of the future, quantum internet, platforms, quantum ecosystems (Durak et al., 2019), computers and networks, sensors will utilize qubits of quantum information that can take an infinite number of values.

According to the forecast by the International Telecommunication Union (ITU), global mobile data traffic will reach 5 zetabytes by 2030. In 2018, Finland announced the 6G flagship program, the British and German governments invested in 6G potential technologies such as quantum technology, and the United States began research (National Quantum Computing Centre, 2019) on Terahertz-based 6G mobile networks. Autonomous driving will operate the global mobile data traffic and intelligent connection network in next decade.

Three-dimensional 6G environment

An analytical framework designed for two-dimensional wireless communication, derived from probability geometry and graph theory readjusted into a three dimensional environment used in 6G network devices in different applications and 6G communication (Table 3).

Table 3. 6G HARMONY

6G HARMONY
Distributed trust
Cyber Psychical Security
Terraherz Technologies
4D imaging and image projection
Automatic Orchestrated Transceiveres
Haptic Remote Telepresence
Full Spectrum fotonic Processing
Proactive Decissions Making
Non Device Centric Communication
Consent and Privacy Preserving
Support for Ambient Novel Sharing
Small Data AI
Distributed Learning
Informations offering
Data Sharing

(Source: author)

Considering to achieve network optimization of the three dimensional equipment it leads to the realization of advanced beamforming 6G architecture. Some of these notable technologies have been already incorporated these three dimensional schemes are satellites, unmanned aircraft or underwater communications.

Holographic 6G communication

The holographic communication allows transmitting virtual vision of people, events using real sight haptic touch techniques. The environment of holographic technology may implement to the abolition of the open system interconnection network model and the adoption of the inter-layer communication

system design. Such research has led to the creation of a hybrid communication technology that extracts various physical quantities and distributes them to the desired receiver via a safe 6G quantum internet channel.

Holograms are three dimensional technologies that manipulate the rays emitted from an object and capture the resulting interference patterns using a recording device. In fact, just sending a three dimensional image without stereo sound is not enough to depict the face-to-face presence characteristics. In the 6G era (Saad et al., 2019) reconfigution is utilized on the development three dimensional configuration platform used for multiple physical presence. The holographic data and images require consuming reliable 6G network links.

The following aspects of holographic communication are related to the human-bonds 6G era. Focused on a human-corporate 6G bond technology communication using an access to a physical features share and express physical phenomena. As a result, such new techniques facilitate the diagnosis of diseases, the detection of emotions, the collection of biological features and remote interaction with the human body. The design of communication systems that mimic human senses requires interdisciplinary research cooperation.

6G Distributed ledger

Blockchain can provide authentication and access control through optimization of privacy storage data sharing mechanism, ensure integrity, traceability monitoring of characteristic data such as keys in distributed computing architecture, and provide classic encryption.

A distributed system has been developed by the open internet, where the participants are freely separated and become a part of a distributed system. This leaves the trust issues in the end of the system to verify the trust of a service or participant. The traditional solutions are based on the third parties that certify and validate the accuracy of the service.

In many cases, parties cannot agree to a single 3rd trusted party. In practice many 3rd parties are used in parallel to weaken the overall security. Currently, the distributed ledger is a consensus with many alternative mechanisms that can support on trust between all parties. In the distributed ledger is ideal when deterministic facts are immutable.

A 6G distributed ledger will automatically trigger the trust network function based on the evaluated relationship. These autonomous ledger trusts will be able to generate smart contracts. The 6G ledger trust can utilize for different parties long-term operation improvement to facilitate a quality or reliability. A 6G distributed ledger will apply a definitive data into a dynamic trust relationships handled for the definitive responses.

6G Psysical Security Thread

The physical layer security technology is located between the body sensor or hub node. Security algorithm 6G high network scalability, heterogeneous devices in various forms of malicious attacks. Unconfirmed data sets can identify individuals as thresholds and determine whether they are as clear as they are today. This is a major unanswered issue for many digital technologies in different sectors, such as smart healthcare, industrial automation. Furthermore, the theoretical method for developing the maximum achievable secret capacity and secret rate of the physical layer security algorithm is very different from the approach adopted in the conventional system.

The intelligent reflecting surface consists of an array of units that can be used to change the phase, amplitude, or frequency of the incident signal. Typically, the intelligent reflecting surface signals are sent to different antennas. The intelligent reflect surface send a beamformed signals of legitimate users. Attackers inject eavesdropping directly by exploiting the internal lines of malicious software and configuration parameters.

Passive attacks such as eavesdropping on authentication keys, user-specific keys, and short-term session keys can also be easier because they are in vulnerable locations. The algorithm must have high power efficiency and the ability to operate in multi-user scenarios. In particular, the artificial fill signal generation characteristics of these modulation techniques are the most important advantages in

providing physical layer security technology (Panayirci et. al., 2020) as compared to conventional approaches.

6G security protocol

When it comes to data confidentiality and integrity, state-of-the-art encryption itself is considered difficult, but the design of traditional authentication and key distribution in the future is questionable. These many proposals have survived decades of attacks, which are believed to be safe even in classical and quantum settings. Replacing modern asymmetric cryptography with post-quantum secure schemes will cost both the communication and operational efficiency of the network.

The 6G security protocol to provide keyless generates secure communication channels through maximization of secret rate, distributed and coordinated in the network. The 6G symmetric encryption of physical layer security technology can also utilize the unique features of wireless channels to co-generate encrypted communication scenarios. The 6G physical layer security technology based key generation solution is fully distributed and does not rely on fixed parameters designed by a particular entity, but rather on radio channels. To meet the expected performance and functionality of the 6G architecture, research is needed to identify the correct application of post-quantum secure cryptography.

3. Conclusion

Quantum communication using the principles of quantum mechanics will ensure the global security architecture. The quantum computing security paradigm brings a new strategy to client data scenarios of 6G connectivity, privacy laws and data sharing and preventing agreements. The 6G security network environment, combined with the trend of artificial intelligence will take the new constraints of the network dynamic topology and algorithms network security.

The behavior of 6G intelligent physical layer will be dynamically activated. This approach allows communication in terms of low energy consumption and long battery life, complete customization and distributed artificial intelligence structure. Quantum key distribution channels can share keys without the possibility of stealing data.

The future intelligent 6G wireless privacy protection applications will use the different privacy data before privacy sending to the artificially designed final output. The local or national authorities responsible for security will not be able to court with 6G sensors and haptic internet data. An artificial intelligence supported on the quantum computing has a t impact on harmful cyber attacks warfare and will significantly increase the number of threats. The 6G communication security strategy can lead to the definition of new technologies (Arafa et. al., 2019) such as network node computing and energy resources, mobility, network node density, frequency spectrum utilization. Understanding quantum computing artificial intelligence has essential parts like technological advances of artificial intelligence.

References

1. Allen, G., Chan, T. (2018). Artificial intelligence and National Security. Retrieved June 28 2020 from https://thebulletin.org/2018/02/artificial-intelligence-and-national-security/
2. Arafa, A., Panayirci, E., Poor, H. V. (2019) Relay-Aided Secure Broadcasting for Visible Light Communications, *IEEE Trans. Commun*, 67, no. 6, pp. 4227-4239, Feb. 2019.
3. Bernstein, D., Lange. T. (2017). Post-quantum cryptography. *Nature*, 549(7671):188-194, 9 2017.
4. Björnson, E., Sanguinetti, L., Wymeersch, H., Hoydis, J., Marzetta, T. L. (2029) Massive MIMO is a reality—What is next?: Five promising research directions for antenna arrays. *Digital Signal Processing*, vol. 94, pp. 3–20, 2019.
5. Boixo, S., Rønnow T. F., Isakov S., Wang Z., Wecker D., Lidar D., Martinis J. M., Troyer, M. (2014). Evidence for quantum annealing with more than one hundred qubits, *Nature Physics*, volume 10, pages 218–224(2014).
6. EU. (2015). EU Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic

communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union OJ L 310, 26.11.2015, p. 1–18. Retreived from http://data.europa.eu/eli/reg/2015/2120/oj

7. Kline, K., Salvo, M. (2019). Artificial Intelligence and Quantum Computing are Evolving Cyber Gyongyosi, L., Imre, S. (2019). A survey on quantum computing technology. *Computer Science Review*, 31:51-71, 2019.
8. Latva-aho, M., Leppänen, K. (eds.) (2019). Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence, 6G Flagship, University of Oulu, Finland, September 2019.
9. Merat, S., Almuhtadi, W. (2015). Cyber-Awareness Improvement Using Artificial Intelligence Techniques. *International Journal on Smart Sensing and Intelligent Systems*, 8(1), 620-636. doi:10.21307/ijssis-2017-775
10. Panayirci, E., Yesilkaya, A., Cogalan, T., Haas, H., Poor, V. (2020). Physical-Layer Security with Generalized Space Shift Keying", Early Accesses *IEEE Trans. Commun*, pp. 1-1, DOI: 10.1109/TCOMM.2020.2969867, Jan 2020.
11. Qanta magazine. (2019). Google and IBM Clash over Milestone Quantum Computing Experiment The Quanta Newsletter National Quantum Computing Centre. Retreived from https://www.quantamagazine.org/google-and-ibm-clash-over-quantum-supremacy-claim-20191023/
12. Kadir, D., Jam, N., Dindar, C. (2019). Object tracking and identification by quantum radar, Proc. SPIE 11167, *Quantum Technologies and Quantum Information Science V*, 111670N. https://doi.org/10.1117/12.2550479
13. Saad, W., Bennis, M., Chen, M. (2019). A vision of 6g wireless systems: Applications, trends, technologies, and open research problems", IEEE network, 2019.
14. Warfare, Cyber Intelligence Initiatives Retreived from https://www.iwp.edu/cyber-intelligence-initiative/2019/03/27/how-artificial-intelligence-and-quantum-computing-are-evolving-cyber-warfare/ on March 27, 2019.
15. Yilantila (Ed.), et al. (2020). 6g White Paper: Research Challenges for Trust, Security and Privacy, Retreived Apr. 7th 2020 from https://arxiv.org/ftp/arxiv/papers/2004/2004.11665.pdf