# 6G Wireless Communications: Security Technologies and Research Challenges

Huangqing Chen*
Communication NCO Academy
Army Engineering University of PLA
Chongqing, China
* Corresponding author: chenhuangq@163.com

Ke Tu
Communication NCO Academy
Army Engineering University of PLA
Chongqing, China

Jian Li
Communication NCO Academy
Army Engineering University of PLA
Chongqing, China

Shuang Tang
Communication NCO Academy
Army Engineering University of PLA
Chongqing, China

Tingquan Li
Communication NCO Academy
Army Engineering University of PLA
Chongqing, China

Zemin Qing
Southwest Institute of electronic and telecommunication technology
Chengdu, China

***Abstract*—By analyzing the expectations and requirements of the intelligent information society in 2030, it becomes clear that what technologies would be demanded in 6G wireless network, especially for security. As promising security technologies, Artificial Intelligence, Quantum Computing and Communications, and Blockchain are deliberately provided and discussed, and these technologies certainly have the ability to enhance the security for 6G. In addition, two research challenges are presented, and the problems and corresponding research directions of them are provided.**

***Keywords-6G; wireless network; security techenology; inelltgence; challege***

## I. INTRODUCTION

In recent years, researchers and engineers of mobile wireless communication have been committed to improving the quality of user experience, from 4G to 5G and to 6G in future. Tab. 1 shows the characteristics of human-oriented 4G, IoE-oriented 5G, and everything-oriented 6G[1]. Besides data rate and latency, there are evident differences between 6G and 5G in performance. To meet the requirements and expectations of the intelligent information society in 2030, the researches on 6G wireless network have already been put on the agenda, such as the project "Broadband Communications and New Networks" for 2030 and beyond in China.

From the perspective of the space coverage of communication network, 5G is still a divergent coverage centred on the base station. As a result, there will be communication blind districts in the desert, unmanned area, ocean and other areas not covered by the base station. It is estimated that more than 80% of the land area and more than 95% of the ocean area will still have no mobile communication signals in 5G era. In addition, 5G communication objects are concentrated in a limited space within 10km above the ground, which can not realize the communication vision of "space-air-ground-underwater" seamless coverage. With the expectations of greater connection density, greater transmission bandwidth, lower end-to-end delay, higher reliability and certainty, and more intelligent network characteristics, 6G wireless network with seamless coverage is essential to integrated applications in future. Because of the complexity of the network, 6G will face serious safety challenges. Artificial Intelligence (AI), Quantum Computing and Communications, and Blockchain will be powerful tools for network security.

TABLE I. THE NETWORK CHARACTERISTICS OF 4G,5G,AND 6G[1]

(FeMBB: further-enhance mobile broadband; ERLLC: extremely reliable and low-latency communications; umMTC: ultra-massive machine-type communications; LDHMC: long-distance and high-mobility communications; LDPC: low-density parity check codes; NOMA: nonorthogonal multiple access; SDN: software-defined networking; NFV: network function virtualization. )

| Characteristic | 4G | 5G | 6G |
|---|---|---|---|
| Usage Scenarios | MBB | eMBB, URLLC, mMTC | FeMBB, ERLLC, umMTC, LDHMC, ELPC |
| Peak Data Rate | 100MB/s | 20GB/s | ≥1TB/s |
| Experienced Data Rate | 10MB/s | 0.1GB/s | 1GB/s |
| Spectrum Efficiency | 1* | 3* that of 4G | 5-10* that of 5G |
| Network Energy Efficiency | 1* | 10-100* that of 4G | 10-100* that of 5G |
| Area Traffic Capacity | 0.1MB/s/$m^2$ | 10MB/s/$m^2$ | 1GB/s/$m^2$ |
| Connectivity Density | $10^5$ Devices/$km^2$ | $10^6$ Devices/$km^2$ | $10^7$ Devices/$km^2$ |
| Latency | 10ms | 1ms | 10-100 μ s |
| Mobility | 350km/h | 500km/s | ≥1000km/s |

978-1-7281-8832-4/20/$31.00 ©2020 IEEE
DOI 10.1109/ICUEMS50872.2020.00130

| | | | |
|---|---|---|---|
| Technologies | • OFDM<br>• MIMO<br>• Turbo Code<br>• Carrier Aggregation<br>• Hetnet<br>• ICIC<br>• D2D Communications<br>• Unlicensed Spectrum | • mm-wave Communications<br>• Massive MIMO<br>• LDPC and Polar Codes<br>• Flexible Frame Structure<br>• Ultradense Networks<br>• NOMA<br>• Cloud/Fog/Edge Computing<br>• SDN/NFV/Network Slicing | • THz Communications<br>• SM-MIMO<br>• LIS and HBF<br>• OAM Multiplexing<br>• Laser and VLC<br>• Blockchain<br>• Quantum Computing and Communications<br>• AI |

## II. SECURITY TECHNOLOGY AND APPLICATIONS

There are many promising technologies which are able to increase system capacity for 6G. Among these technologies, the ones that can be used to ensure network security are AI technologies, Quantum Computing and Communications, and Blockchain technologies.

### *A. Artificial Intelligence*

As 6G is developed for the intelligent information society in 2030, Intelligence is the key characteristic of 6G autonomous wireless network, and AI technologies will be applied in almost all aspects of 6G. Actually, AI will effectively realize seamless connection between devices of space-air-ground-underwater network through learning and big data training of multi-dimensional data such as network data, service data and user data. Furthermore, AI can sense network status in real time, optimize network and improve the quality of user experience.

In terms of network security, AI technologies can realize self-organization of knowledge, especially for pattern recognition learning and classifier construction in firewall and intrusion detection. For example, in Distributed Denial of Service (DDoS) attack, AI algorithm can be used to learn intrusion recognition rules[2]. Network Behaviour Analytics(NBA) with AI have the ability to detect network attack, abnormal behaviour and advanced threat through big data analysis technology with user digital trace[3]. In addition, Network Security Situation Awareness could lift the ability of Information extraction, information preprocessing, information fusion, situation awareness and situation fusion with AI technologies[4].

### *B. Quantum Computing and Communications*

With the development and integration of information theory and quantum theory, quantum technologies have advanced rapidly in the past two decades, and have gradually entered the practical stage. Based on the quantum no-cloning theorem and uncertainty principle, quantum communications can achieve absolute security in theory, as eavesdroppers secretly launch interception or copy actions or measurements, the eavesdropping behaviours can be easily detected due to quantum state disturbance. Quantum communications mainly involves quantum cryptography communication, quantum teleportation, quantum dense coding, and so on.

The superposition and entanglement principle of quantum mechanical states makes the state of quantum information units be in more possibilities, which leads to quantum computing with much greater potential in capacity and efficiency compared with classical computing[5]. Therefore, using unitary transformations in form of qubits, quantum computing can dramatically accelerate big data analysis and deep learning, which would not only promote the capacity of network security but generate more powerful and efficient AI algorithm for 6G.

### *C. Blockchain*

Blockchain is a shared distributed database essentially, in which the data or record blocks stored. With the characteristics of “unforgeability”, “whole process trace”, “traceability”, “openness and transparency”, and “collective maintenance”, blockchain technologies have constructed a solid “trust” foundation and created a reliable “cooperation” mechanism. In other words, blockchain is a new integrated application mode of distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm and other computer technologies. The abundant application scenarios of blockchain are basically based on the fact that blockchain can solve the problem of information asymmetry and achieve cooperative trust and concerted action among multiple subjects

In the application scenarios of blockchain, blockchain-based spectrum sharing is an available technology for 6G to provide secure, intelligent, low-cost and highly efficient decentralized spectrum sharing[6]. Besides, blockchain can be used to build security systems such as identity authentication system to enhance the safety of 6G wireless network.

## III. RESEARCH CHALLENGES

### *A. Integrated Security Architecture of Space-air-ground-underwater Network*

There remains a view that 6G wireless network is an effective integration of 5G network, satellite communication network and deep-sea-ocean network, and the global seamless coverage would be achieved in 6G. The space-air-ground-underwater network in 6G would optimize the links of underwater (offshore, subsea and island communication equipments), ground (cellular mobile network and other networks), air (all kinds of aircrafts), and space (all kinds of satellites and spacecrafts), for satisfying the requirements of 6G such as seamless coverage and ubiquitous connectivity, as shown in Fig.1.

The space-air-ground-underwater network is an integrated, heterogeneous, efficient and intelligent network, and the heterogeneity characteristic brings a lot of complexity to the network, especially in consideration of security. It is necessary to consider the functions and features of different types of networks, and design the network security architecture from an overall perspective. To realize the service security and data security, the integrated security architecture is always constructed on proper security technologies and management mechanisms to ensure safe communication in the global seamless network.

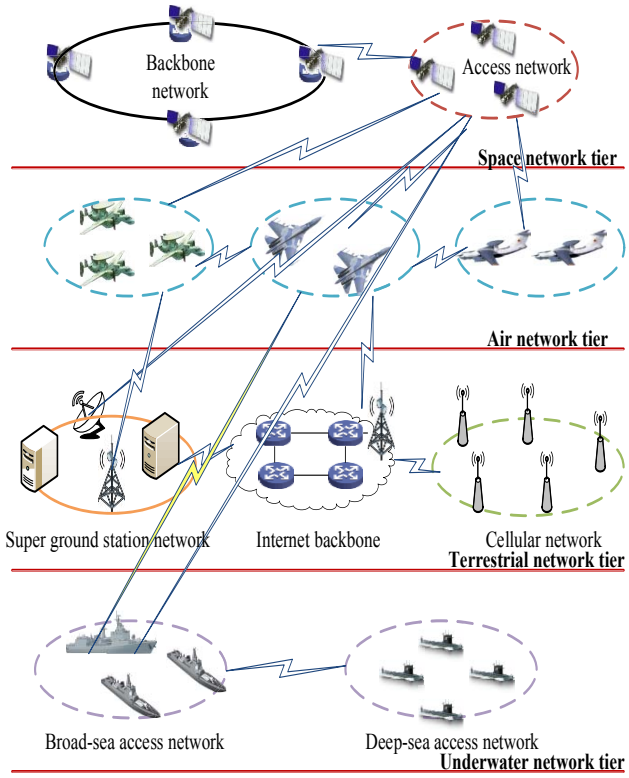


Figure 1. The architecture of space-air-ground-underwater network

### B. Blockchain-based Identity Authorization System

Among the technologies used in blockchain, consensus algorithm is the core one. The consensus algorithm is designed to solve the problem that how to make all nodes of the whole network reach an agreement and make the final result credible without a trusted third party. The common consensus algorithms include Proof of Work(PoW)[7], Proof of Stack(PoS)[8] , Delegated Proof of Stack(DPoS), Distributed Consensus(DC), and so on. The comparison of these algorithms is displayed in Tab.2.

TABLE II. THE COMPARISON OF CONSENSUS ALGORITHMS

| Characteristics | PoW | PoS | DPos | DC |
|---|---|---|---|---|
| Mechanism | Find specific hash value of nonce, difficult to compute and easy to verify | Determine the difficulty of mining according to the existing assets and time of personal ownership | Delegates elected, accounting in turns | Classic distributed consensus technologies |
| Efficiency | Low | Medium | High | High |
| Recording | All | All | Delegates | Leader |
| Advantage | Decentralization, free access of nodes | Reduce consensus time to some extent | Effectively record | Realize consensus in seconds |
| Weakness | Waste of computing capacity | The Matthew effect | Prone to branching | Low degree of decentralization |

According to different participants, blockchain can be divided into Public Blockchain, Consortium Blockchain and Private Blockchain. Various kinds of blockchains can form a network, in which the chains are interconnected and intercommunicated, and the interchains are naturally generated. Different consensus algorithms have distinct characteristics, which one is the most appropriate depends on the application scenario and requirements. As identity authentication is a complex and important problem in heterogeneous network, how to use appropriate type of blockchain with proper consensus algorithms to realize identity authentication in 6G wireless network is a challenging issue.

## IV. CONCLUSION

Based on the analysis and discussions presented above, the conclusions are obtained as below:

- The advantages of 6G compared with 4G and 5g are described, especially in the key performance indicators and technologies. And it is evident that 6G wireless network would provide more broad coverage and much better quality of user experience.
- The security technologies including AI, quantum technologies and blockchain can be used for 6G to ensure network security, therefore, the functions and application methods of these technologies have been discussed.
- The research challenges including integrated security architecture of space-air-ground-underwater network and blockchain-based identity authorization system are briefly analyzed, and the problems and research directions of the two topics are provided.

## ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (No. 61631013).

## REFERENCES

[1] Z. Zhang *et al*., "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," in *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 28-41, Sept. 2019.

[2] A. Mitrokotsa, N. Komninos and C. Douligeris, "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET," *IEEE International Conference on Pervasive Services*, Istanbul, 2007, pp. 118-127.

[3] M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 303-336, First Quarter 2014.

[4] Hu Dongxing,et al. Information Network Security Situation Aware Technology Based on Artificial Intelligence[J]. Journal of Information Communication, 2012 (6):80-81.

[5] P. Botsinis et al., "Quantum search algorithms for wireless communications,"*IEEE Commun. Surveys Tut.*, vol. 21, no. 2, pp. 1209–1242, 2019. doi: 10.1109/COMST.2018.2882385.

[6] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 32–39, Mar. 2018. doi: 10.1109/MVT.2017.2740458.

[7] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao and M. A. Imran, "Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment," in *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5791-5802, June 2019.

[8] G. Drakopoulos, E. Kafeza and H. Al Katheeri, "Proof Systems In Blockchains: A Survey," *2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, Piraeus, Greece, 2019, pp. 1-6