A Survey: Beyond 5G Toward 6G—Network Security Issues, Thrust Areas and Challenges

K. S. Lavanya and B. Nagajayanthi

Abstract Fifth generation (5G) network is being rapidly deployed in real time. The exploratory research mind drives toward 6G networks. For further investigation and research toward 6G technologies, foundational research is carried out in a 6G network security, and privacy is presented as a survey in this paper. The survey begins with the key areas to be considered beyond 5G network toward 6G network such as intelligent radio, distributed artificial intelligence, real-time intelligent edge and 3D intercom. The survey also states the key issues of 5G network such as data security and authentication along with the countermeasures to overcome these issues in 6G network. Finally, the survey concludes with a new design idea based on the deep learning method (CNN-LSTM) for implementation in a 6G network for authentication by detecting the attack in network traffic.

Keywords 6G · Network security · Artificial intelligence · Deep learning

1 Introduction

Even though 5G network is not deployed fully, certain inherent limitations tend to move research focus toward 6G network. Researchers worldwide have started working on 6G communication and its network security challenging facts. There is no solid differentiation with respect to standards or specifications between 5 and 6G networks. Research focus has evolved from 5 to 6G to improvise the network and spectrum as depicted in Fig. 1 and also due to the features enlisted in Table 2. 6G network is expected to be faster than 5G Network.

K. S. Lavanya
Vellore Institute of Technology, Chennai, India
e-mail: lavanya.ks2020@vitstudent.ac.in

B. Nagajayanthi (✉)
Associate Professor, Vellore Institute of Technology, Chennai, India
e-mail: nagajayanthi.b@vit.ac.in

A. Sivasubramanian et al. (eds.), *Futuristic Communication and Network Technologies*,
Lecture Notes in Electrical Engineering 792,
https://doi.org/10.1007/978-981-16-4625-6_87

The 6G network is expected to work with higher artificial intelligence (AI) technology. It should be "6G-AI-empowered." The 5G networks also use AI technology, but here, the future limitations show that 6G network should use AI tools in deep integration manner. Over the years, security and privacy of communication networks become the important factor. Beyond 5G, the network security and privacy concern with four major components stated (Fig. 2) as intelligent radio subsided with distributed AI and real-time intelligent edge.

These three areas are interconnected as AI exists with intersection factor and 3D intercoms. These are the areas of focus for AI-empowered 6G researchers. The main security issues here in 6G network are related to data transmission, encryption, access control and authentication. However, the issues are somehow particularly sensitive in some nature of communication. The communication intended in 6G are visible light communication (VLC), molecular communication, block chain technology-based communication and quantum communication.

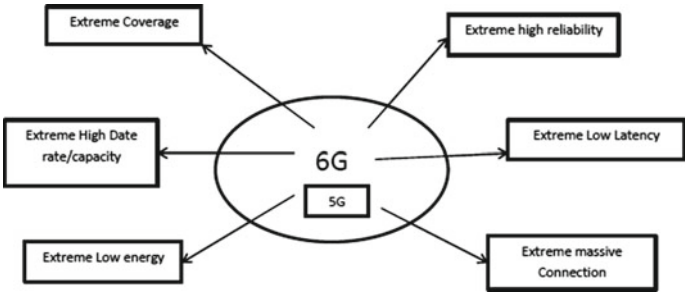

Fig. 1 Beyond 5G toward 6G

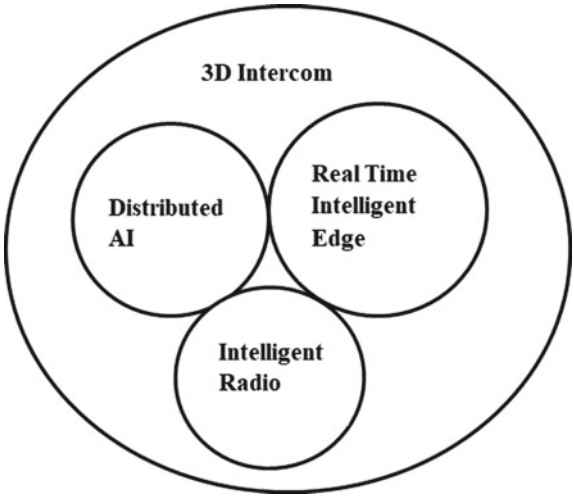

Fig. 2 Key areas of 6G network

VLC along with real-time intelligent edge is weak against malicious behavioral attacks. Molecular communication has issues toward authentication and encryption while it processes under THz technology. Both quantum and block chain technology face the issue due to malicious attack.

2 6G Network: Key Areas and Security Issues

The 5G coverage is deployed only at ground level since it has risk factors to be dealt with for work in space and undersea communication at 3D intercom levels. Four thrust areas in 6G networks with added network security are highlighted as follows:

2.1 Distributed Artificial Intelligent Edge

Fifth generation is deployed in Internet of Things (IoT), whereas 6G is deployable in Internet of Everything (IoE). 6G network could take intelligent decision at a different level (i.e., decentralized system). To have the decentralized system, the dataset is trained unevenly over edge devices, with the edge devices capable of accessing and controlling the data part. Data is computed and stored independently by reducing the dimension. It also cleans and makes abstract out of the data [1]. Here, the shared data is processed as the training set irrespective of the state of personal information. Using this process, security and privacy of the network are enhanced. Machine learning plays a vital role to solve data integrity issues. Block chain methods can solve issues raised in distributed edge technology due to authentication.

2.2 Intelligent Radio

Over the years in network generation, the transceiver and device algorithm are designed together. In recent research and for 6G networks, the possible ways are measured to separate the transceiver algorithm from hardware by making the development in antenna and circuit boards. Intelligence-based radio can operate as a framework in a unified manner where the algorithm gets configured dynamically, and from the hardware, information is updated automatically.

Huang et al. [2] noted that the design of operating system and interfacing layer is based on the information available from the hardware, and also with AI, the transceiver algorithm gets configured. They also researched that design constraints should make the frequency band to adhere to hardware as well as to the environment. AI-enabled spectrum sharing is deployed. Further, Jiang et al. [3] stated that data security issues arise from signal jamming and wideband interference.

2.3 3D Intercom

Sixth generation networks need to improve certain factors relating to optimization capabilities, planning and analyzing of the network from previous network generation. Apparently, beyond 5G, 6G networks should support 3D space communication; i.e., it should be able to conform to both undersea communication and satellite communication. The 3D intercom could serve a service-based communication in such aspects.

The main question of 3D intercom is whether the 6G network would be able to operate in undersea is a controversial fact because of its complex nature. Grimmett [4] discussed the security issues involved in the transmission process in undersea communication network. From this, it can be inferred that undersea communication network will be the primary aspect of 6G network.

2.4 Real Time-based Intelligent Edge

The 5G networks still face the issue in the implementation of unmanned aerial vehicle (UAV) network because of its lack in controlling the network due to its high latency. UAV needs low latency and real-time intelligence where the current technologies are limited to this [5]. The 6G network should be able to handle these functions to support all power services interactively. The key areas concerning 6G network technologies are shown (see Table 1) and the key comparison between 5G and 6G is shown (see Table 2).

Table 1 Key areas in relation with 6G

Key areas	6G relation	Features
Distributed artificial intelligence	Capable of decision-making	Intelligent decision-making
Intelligent radio	Communication responsibility	Self-adaptive nature
3D intercom	Responsible for coverage	3D coverage
Real-time intelligent edge level heading	Capacity control	Real time response

Table 2 Fifth generation versus sixth generation

Key areas	5G	6G
Performance	Speed: 0.1 Gbps 1 ms—low latency 2D positioning Improved performance	Speed: 1–10 Gbps 0.1 ms—very low latency 3D positioning Guaranteed performance
Spectrum	Approx. 100 GHz Use in unlicensed spectrum High bands: limited no of national Licenses	Up to 10 THz Open in shared spectrum bands High bands: large no of local licenses
Network	Massive machine type communication Area traffic: 10Mbps/s/m^2	Machine support: broadband Area traffic: 1 Gbps/s/m^2
Network characteristics	Cloudization Softwarization Virtualization Slicing	Intelligentization Cloudization Softwarization Virtualization Slicing
Other aspects	Limited AI	Massive AI

3 Network Security: New Paradigm Shift

3.1 Security Issues

The 6G core key is to achieve customized secure services in human-centric mobile communication. The potential privacy and security issues faced in 5G networks are due to the following aspects mentioned below. The countermeasures for the issues in 5G and the reasons for the evolution from 5 to 6G are also highlighted below.

AI: Security Issue: Though it is always stated that 6G is AI-empowered, AI also raises the security issue like malicious utilization of AI technology. To train the AI model, the service provider collects user information (sensitive information) such as location, trajectory and identity of the user [6]. There is a high probability of the data getting leaked during transmission of data and during processing of data. The AI model could be attacked via white-box attacks though the attacker does not have any data about the architecture and parameter of the AI model. This approach could be made by checking the input and output. For dynamic protection of AI, a model needs to be framed**.**

IoT Network: Security Issue: For IoT deployment, an efficient authentication mechanism is required. Key management and resources for computing require encryption and decryption. IoT device security is limited by constrained storage

space and battery energy [7]. Therefore, to overcome these limitations, a lightweight security algorithm is designed to support low power IoT devices with energy efficiency.

UAV Networks: Security Issue: Like terrestrial-based station, UAV could not support complex nature of cryptographic algorithm due to power and weight requirements. As a result, UAV is prone to network security vulnerabilities. To overcome this, mechanisms are required to counteract the internal attack.

3.2 Security Issue: Possible Countermeasures

To overcome the above stated issues, advancement in security and privacy technologies need to be framed.

Method based on Physical Layer: This method provides defense layer besides the upper cryptographic layer in 6G network. It also provided secure transmission in wireless signals. The combination of secret key and authentication key of the physical layer can give secure protection with a lightweight algorithm for the air interface. Most robust and efficient physical layer security (PLS) technology should be framed to satisfy throughput, latency and overhead requirements [8]. PLS provides lightweight mechanism to provoke against the security threat. Also, to achieve intelligence-based network security, distributed PHY protocol could be designed.

Method based on Traditional Cryptography with lightweight algorithm: In network security and data privacy, traditional encryption, authentication, authorization, signature and privacy are still a safeguarding procedure. Anonymous and group-based authentication gives lightweight and flexible solutions for development and research direction in cryptographic-based security and privacy. This method could be incorporated into both IoT network and UAV network security issue. Both the networks have the need to work under lightweight mechanism to overcome threat issue. This lightweight cryptography method or protocol under elliptic curve cryptographic (ECC) method provides reliable data security and authentication.

Method based on Quantum Technique: More lightweight and higher processing capability with absolute randomness is obtained by quantum-based method (quantum communication and quantum computing) when compared with the binary-based technique. The pre- and post-quantum cryptography is a stronger solution for data security, and privacy in quantum key distribution (QKD) gives unconditional guarantee of a secure key. By the above-stated process, the key gets generated in a manner irrespective of certainty and productivity of quantum state. The key is implemented randomly [2]. The evolution of 5G toward 6G is more of an AI network where multiple data are to be processed, so QKD will play the major role for high secured key generation to provoke against AI network issue. This method could be designed with continuous variable-quantum key distribution (CV-QKD) for both heterodyne and homodyne detections.

Method based on Block Chain: Block chain-based methods are decentralized methods. By this, it has the anti-corruption ability (stronger) and recovering ability which tend to have a stronger factor for authentication. This block chain-based algorithm could be designed for strong authentication and secured data sharing, whereas this method would be a wall to the authentication process in AI Network and IoT network. This block chain-based method could be implemented with the interplanetary file system (IPFS) for high data privacy and authentication.

Method based on Artificial Intelligence: The 6G network has the highest peak rate where it promotes the integration of AI in 6G network security mainly for anomalies detection and authentication. This AI-based method is used especially in machine learning-based auto-coder work for the detection of traffic date abnormality [9]. ML-based physical layer authentication is a much needed technique to achieve robust and reliable authentication. As we move forward, in intelligence-based automation, ML algorithm will provide security against abnormal attack in AI network. Convolutional neural network with long short-term memory (CNN–LSTM) technique can be used for abnormality detection in AI network platform since it gives instant prediction factor with known results of the previous state.

4 New Research Design for Security Issue

Beyond 5G toward 6G network, many researches have been deployed in various aspects. As mentioned above, 6G is AI driven where the main part deals with security and privacy. Deep learning technique helps to build a better networking platform prone to security attacks [10, 11].

4.1 Deep Learning-based Design

When the future networks get attacked, the certain factor is to find the attack with its category and information. By combining convolutional neural network with long short-term memory (CNN-LSTM), the spatial and temporal characteristics of the network are known in order to know the abnormality in network traffic. The design can be framed with three parts. The flow model of CNN-LSTM model is stated in Fig. 3 where network traffic states the temporal data.

1. Spatial feature of CNN can be implemented to process the network traffic data (to form spatial classification network model).
2. CNN-processed transmission vectors are nest processed in training set. Using LSTM, time characteristics are learned to form model which works for recognition.
3. By combining spatial and temporal model, the network traffic classification model is designed, and it acts as a prone to the network attacks.

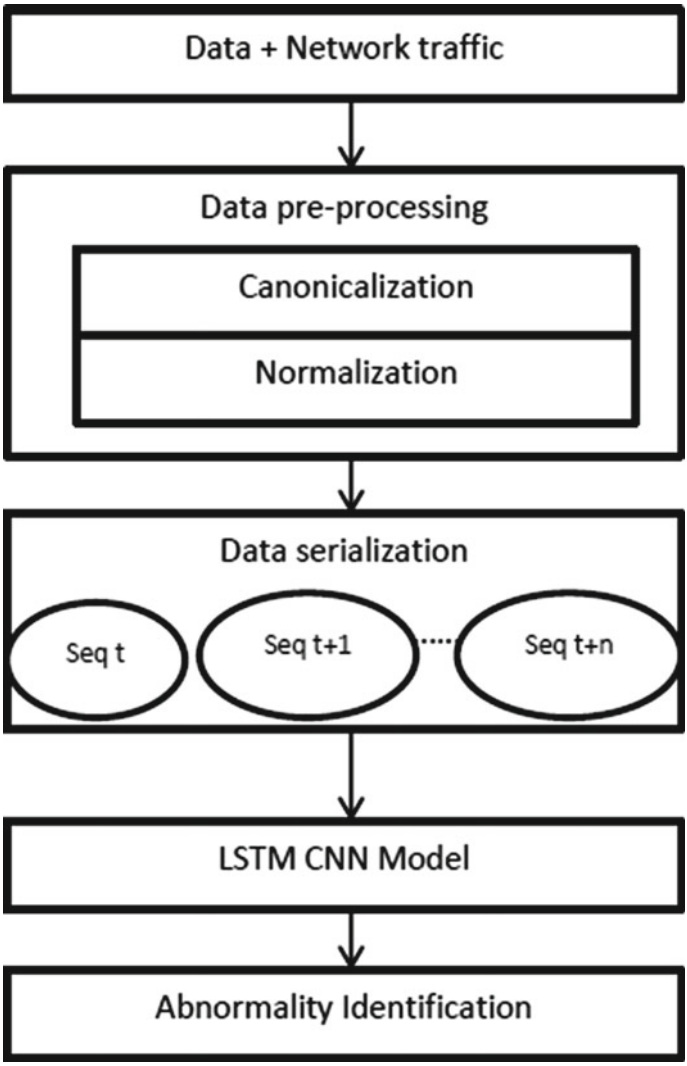

Fig. 3 CNN-LSTM model for abnormality detection (authentication)

5 Conclusion

The 6G network is the new agenda for many researchers. From the survey, it is inferred that 6G network gives high-level service compared to the previous generations. In this survey, analysis of 6G is based on security and privacy perspectives. The new research idea is stated under deep learning for implementation. The survey provides an insight into the technologies relating to 6G network.

References

1. McMahan HB, Moore E, Ramage D, Hampson S, et al (2017) Communication-efficient learning of deep networks from decentralized data. In: Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), JMLR: W&CP, Vol 54
2. Huang W, Stokes JW (2016) MtNet: a multi-task neural network for dynamic malware classification", Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, Berlin, Germany, pp 399–418
3. Jiang C, Zhang H, Ren Y, Han Z, Chen K-C, Hanzo L (2016) Machine learning paradigms for next-generation wireless networks. IEEE Wireless Communications 24(2):98–105
4. Grimmett DJ (2007) Message routing criteria for undersea acoustic communication networks. in: OCEANS, IEEE, Europe, pp 1–6
5. Katz M, Pirinen P, Posti H (2019) Towards 6G: Getting ready for the next decade. In: 16th International Symposium on Wireless Communication Systems (ISWCS), pp 714–718, IEEE
6. Buczak AL, Guven E (2016) A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials 18(2):1153–1176
7. Zhang Y H, Deng R, Bertino E, et al (2020) Robust and universal seamless handover authentication in 5G HetNets. In: IEEE Trans Dependable Secure Computer
8. Liang YC, Larsson EG, Niyato D, et al (2020) 6G mobile networks: Emerging technologies and applications
9. Sharafaldin I, Lashkari AH, Ghorbani AA (2018) Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), Madeira, Portugal
10. Rawat DB, Reddy SR (2017) Software defined networking architecture, security and energy efficiency: a survey. IEEE Communications Surveys & Tutorials 19(1):325–346
11. Ren J, Hussain A, Zhao H et al (2020) Advances in brain inspired cognitive systems. In: International Conference on Brain Inspired Cognitive Systems, Vol. 11691 of Lecture Notes in Computer Science, Springer, Berlin, Germany