Journal of Information Technology and Software Engineering

OPEN ACCESS Freely available online

Short Communication

Significance of 6G Wireless Infrastructure and its Applications

Oliva Chirstopher*

Department of Digital Technology, Raytheon Technologies, Waltham, Massachusetts, USA

ABSTRACT

Due to the implementation of 5G technology, academics and industry began to investigate 6th generation wireless network technologies (6G). Around the year 2030, 6G is projected to be operational. By allowing hyper-connectivity between people and things, it will provide a profound experience for everyone. Furthermore, it is planned to expand mobile communication capabilities in areas where previous generations were unable to do so. Sixth-generation networks are expected to be built using a variety of technologies.

Keywords: 6G wireless networks; Visible light communication; Artificial Intelligence

ABOUT TE STUDY

Post-quantum encryption, Artificial Intelligence (AI), Machine Learning (ML), improved edge computing, molecular communication, THz, Visible Light Communication (VLC), and Distributed Ledger (DL) technologies such as blockchain are among the next and existing technologies. From the perspective of security and privacy, these advances need a reconsideration of previous security measures. The increased critical needs future networks will necessitate unique authentication, encryption, access control, communication, and activity detection.

To assure trustworthiness and privacy, new security measures are also required. This article delves into the important concerns and challenges that 6G networks incur in terms of security, privacy, and trust. Furthermore, the typical technologies as well as the security problems associated with each technology are explained. This article discusses the 6G security architecture and how it differs from the 5G security architecture. The security risks and challenges of the 6G physical layer are also discussed.

6G networks can still benefit from 5G technologies like Multi-access Edge Computing (MEC), SDN, NFV, and network slicing. As a result, the security issues that come with them will continue. Vulnerabilities in the SDN controller, interfaces, and SDN application platforms, for example, are among the most serious security problems associated with SDN. Attacks against virtual machines, hypervisors, and Virtual Network Function (VNF) administrators are among the security challenges connected with NFV. Finally, MEC is subject to physical threats, denial-of-service attacks, and the massively spread nature of 6G systems. Network slicing attacks that use 6G network slices might result in data theft and DoS attacks. The ability of the 6G network to achieve high dynamicity and full network automation is shown through attacks on network automation technology. According to 6G, the Internet of Everything will become a reality, involving billions of complicated connected devices [1,2].

Because 6G devices, such as in-body sensors, will be smaller than prior devices, the device's primary security based on SIM cards will be inadequate for IoE deployment. In such a large network, the needed distribution and management duties are inefficient. Because IoT devices with limited resources are unable to provide advanced encryption, they are a popular target for cybercriminals. These inconspicuous gadgets might be hacked and utilised to carry out attacks. Furthermore, the data acquired by intermediate IoE to facilitate 6G apps raises issues about privacy. Data privacy is threatened when system is hacked from IoE devices with limited resources. Local 5G network deployments frequently target vertical industries including industry, healthcare, and education. 6G explores the concept a level further by enabling even smaller networks with longer battery life, such as in-body networks, drone swarms, and environmental sensor networks. These networks connect with wide-area networks in a self-contained manner.

Despite local 5G networks, numerous industry enablers support 6G with variable levels of embedded security. A 6G network with inadequate security provides an opportunity for attackers to launch assaults. With high-density deployment, 6G cells will decrease from small to microscopic. The 6G deployment

Correspondence to: Oliva Chirstopher, Department of Digital Technology, Raytheon Technologies, Waltham, Massachusetts, USA, E-mail: chirstopheroliva23@yahoo.com

Received: 18-Mar-2022, Manuscript No. JITSE-22-17017; **Editor assigned:** 21-Mar-2022, Pre QC No. JITSE-22-17017 (PQ); **Reviewed:** 04-Apr-2022, QC No. JITSE-22-17017; **Revised:** 12-Apr-2022, Manuscript No. JITSE-22-17017 (R); **Published:** 20-Apr-2022, DOI: 10.35248/2165-7866.22.S6.002.

Citation: Chirstopher O (2022) Significance of 6G Wireless Infrastructure and its Applications. J Inform Tech Softw Eng. S6:002.

standard will be Device-to-Device (D2D) communications and mesh networks with multi-connectivity. Malicious devices have a good opportunity of assaulting a dispersed network with more vulnerable devices linked *via* the mesh, hence increasing the hazard surface. The wide area network is incapable of providing security for the massive number of devices included inside each sub-network [3,4].

CONCLUSION

In 6G, it would be preferred to have a hierarchical security mechanism that distinguishes communication security at the sub-network level from sub-network to comprehensive area network security. Convergence of the RAN and core functions synchronizes top layer RAN services with distributed core functions like User Plane Micro Services (UPMS) and Control Plane Micro Services (CPMS). Attackers might go after UPMS and CPMS, affecting a large number of radio devices that are served by micro services. Zero-touch networking and Service Management (ZSM) architecture are used in 6G networks to provide for faster services, lower operational costs, and less human error. In closed-loop systems, complete automation paired with self-learning allows to evolve. Due to important automation needs with limited human involvement, data privacy protection in zero-touch networks is difficult.

REFERENCES

1. Khan R, Kumar P, Jayakody D, Liyanage M. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Commun Surv Tutor. 2020;22:196-248.
2. Yazar A, Dogan-Tusha S, Arslan H. 6G vision: An ultra-flexible perspective. ITU J Future Evol Technol. 2020;1:121-140.
3. Alwis C, Kalla A, Pham QV, Kumar P, Dev K, Hwang WJ. Liyanage M. Survey on 6G frontiers: Trends, applications, requirements, technologies and future research. IEEE Open J Commun Soc. 2021;2:836-886.
4. Ray P, Kumar N, Guizani M. A vision on 6G-enabled NIB: Requirements, technologies, deployments, and prospects. IEEE Wirel Commun. 2021;28:120-127.