Received 10-09-22; Accepted 25-09-22; Published 30-09-22

The Emergence of Heterogeneous Networks

Gautam Srivastava SRIVASTAVAG@BrandonU.CA
Computer Science, Brandon University,
Canada.

Corresponding Author: Gautam Srivastava

1. INTRODUCTION

Fifth generation (5G) communication provides high-speed data transfer and low latency, serving the better for multiple heterogeneous applications over previous technologies. This has led to the development of heterogeneous networks (HetNets) by integrating diverse information and communication technologies (ICTs) into a single view to provide better quality of service (QoS) for different classes of users [1]. HetNets are poised to see more widespread acceptance of a means of communication favored in 5G and beyond as we look to 6G as well. The fundamental components of a 5G HetNet scenario include the user equipment (UE) and enhanced node B (eNB). The communications between the UEs is facilitated using eNBs that act as a gateway for inward and outward data exchange. User equipment is classified under pico or macro cells in a HetNet whereas the integration of 5G supports distributed communication modes through device-to-device (D2D) features. Along with the support of eNBs, interference cancellation, carrier aggregation, massive multi-input multi-output, and coordinated transmissions are facilitated in this network to meet the QoS requirements of different applications and users [2, 3]. The interoperable nature of the heterogeneous platform provides pervasive and anonymous access to resources and UE communications. In such a pervasive access scenario, security becomes a prime concern due to the interruptions in D2D communications [4]. Unauthorized devices or adversaries focus on the exchanged data to inject malicious or falsified content, changing its freshness and reliability. Therefore, authentication-centric solutions are designed for data security along with integrity checks to ensure transmitted data is delivered at the receiver end [5]. Globally, the data security and privacy of the Internet of Things (IoT) has been a concern to all users. As more and more individuals see themselves conducting their day-to-day livelihood on mobile devices, they also see themselves sharing personal information over open channels. Robust data authentication and efficient key management are assimilated in the heterogeneous communication platform for leveraging the security level of data exchange to preserve user data security and privacy. Key management and hash-based authentication methods are designed with less complexity to reduce the computational and communication-based overheads, along with lower latency to support the design goal of 5G environments. Therefore, the adaptiveness of the authentication method is required to be two-fold, namely user-centric and application-centric, as guided by the service and security provider. We have seen many different areas fuse to offer strong authentication methods in 5G. These tend to include Artificial Intelligence, Machine Learning, Deep Learning, and more recently, blockchain technology [6]. Artificial intelligence techniques tend to

Citation: Gautam Srivastava The Emergence of Heterogeneous Networks. Advances in Artificial Intelligence and Machine Learning. 2022;2(3):31.

focus on the examination of network data to be able to identify packets as normal or potentially malicious. Machine Learning and Deep Learning techniques also aim to achieve the same thing, although using different methodologies. Blockchain technology, on the other hand, can assist in both the realms of data/user authentication and data/user integrity. By using the blockchain to store and share authentication information, we will see more efficiency in our ability to control which devices have access to data and networks and for how long. Research in this area will continue to flourish, and readers are encouraged to explore open problems in this domain.

References

[1] Lee CN, Lin JH, Wu CF, Lee MF, Yeh FM. A Dynamic CRE and ABS Scheme for Enhancing Network Capacity in LTE-Advanced Heterogeneous Networks. Wireless Networks. 2019;25:3307-3322.

[2] Hu W, Li J, Cheng J, Guo H, Xie H. Security Monitoring of Heterogeneous Networks for Big Data Based on Distributed Association Algorithm. Computer Communications. 2020;152:206-214.

[3] Arfaoui G, Bisson P, Blom R, Borgaonkar R, Englund H, et al. A Security Architecture for 5G Networks. IEEE Access. 2018;6:22466-22479.

[4] Braeken A, Liyanage M, Kumar P, Murphy J. Novel 5G Authentication Protocol to Improve the Resistance Against Active Attacks and Malicious Serving Networks. IEEE Access. 2019;7:64040-64052.

[5] Guan J, Wei Z, You I. GRBC -Based Network Security Functions Placement Scheme in SDS for 5G Security. Journal of Network and Computer Applications. 2018;114:48-56.

[6] Srivastava G, Parizi RM, Dehghantanha A. The Future of Blockchain Technology in Healthcare Internet of Things Security. Part of the Advances in Information Security book series. 2020;79:161-184.