Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions

ABSTRACT

Challenges faced in network security have significantly steered the deployment timeline of Fifth Generation (5G) communication at a global level; therefore, research in Sixth Generation (6G) security analysis is profoundly necessitated. The prerogative of this paper is to present a survey on the emerging 6G cellular communication paradigm to highlight symmetry with legacy security concepts along with asymmetric innovative aspects such Artificial Intelligence (AI), Quantum Computing, Federated Learning, etc. We present a taxonomy of the threat model in 6G communication in five security legacy concepts, including Confidentiality, Integrity, Availability, Authentication and Access control (CIA3). We also suggest categorization of threat-countering techniques specific to 6G communication into three types: cryptographic methods, entity attributes and Intrusion Detection System (IDS). Thus, with this premise, we distributed the authentication techniques in eight types, including handover authentication, mutual authentication, physical layer authentication, deniable authentication, token-based authentication, certificate-based authentication, key agreement-based authentication and multi-factor authentication. We specifically suggested a series of future research directions at the conclusive edge of this survey