Next Generation Computing Applications, Mauritius, 24-26 October 2024

A review of PFCP cyber attacks in 5G standalone for robotic telesurgery service

Makondo, Ntshuxeko; Baloyi, Errol; Kobo, Hlabishi I; Mathonsi, TE

Abstract

The emergence of fifth-generation technology (5G) has revolutionised telecommunication networks, offering enhanced mobile broadband, ultra-reliable (eMBB), ultra-lowlatency communications (uRLLC), and massive machine-type communication (mMTC) service classes. This breakthrough has garnered significant attention and investment worldwide, driving innovation and growth in the digital era. However, the adoption of cloud-based 5G core (5GC) networks, while offering scalability and deployment flexibility, has posed challenges to meeting stringent latency requirements, particularly for uRLLC services specifically for robotic telesurgery. To address this problem, mobile network operators (MNOs) have turned to edge computing (EC), using the control and user plane separation (CUPS) architecture introduced in the thirdgeneration partnership project (3GPP) release 14 specification. This architecture enables the deployment of the user plane function (UPF) closer to users, reducing latency, and improving quality of service (QoS). However, the deployment of the UPF as a standalone node on the edge of the network exposes the packet forwarding control protocol (PFCP) to cybersecurity attacks, which pose risks to telesurgery services and could even lead to loss of life. In the existing literature, only a few techniques focus on minimising these attacks when the UPF is deployed on the edge of the network far from the 5GC. Therefore, this paper reviews PFCP attacks and explores machine learning (ML) techniques to mitigate these security threats. This paper further provides recommendations and future research directions for mitigating these attacks.