A design science approach to fingerprinting and signal localization on the Internet of Medical Things based on RFML

Our study delves into securing communication and data protection on the Internet of Medical Things (IoMT), an interconnected system linking medical devices and systems to the Internet. The primary obstacle in IoMT security is keeping malicious actors from infiltrating the network. To address this, we utilized the attack detection approach, a cutting-edge approach that detects unauthorized transmitters in the wireless signal network. Our testing found that the framework boasted a 96% accuracy rate in detecting these transmitters. This research shows promise in the signal security of IoMT, which is crucial for safeguarding the privacy and well-being of patients who rely on these medical devices long-term.

Abstract

The area of research related to securing communication and data protection on the Internet of Medical Things (IoMT) spectrum is growing rapidly. However, preventing malicious actors from compromising spectrum network security is a critical challenge in IoMT spectrum security. To overcome this challenge, reliable radio frequency fingerprinting and radio localization techniques are necessary. In this study, we implemented the IoMT spectrum security framework, the DSRM-based attack detection model (DAD), to predict rogue transmitter accuracy and localization. The hybrid approach uses RF fingerprinting techniques that rely on IQ balance datasets derived from Hack-RF device datasets and RSSI simulation using a Java-based test bed. The study utilized Deep Convolutional Neural Networks (CNN) to develop predictive models for detecting rogue transmitters. The model was trained and achieved 96% accuracy. Received Signal Strength Indicator (RSSI) localization simulation experiments were conducted on a Java test bed to locate rogue transmitter nodes. The framework was implemented using the Design Science Research Methodology (DSRM). Further extension of this research and commercialization will benefit the security and healthcare aspects of IoMT.