ABSTRACT

The development of mobile communication technology has reached a transformative stage with the coming of the concept of the sixth generation of telecommunications (6G) system aimed at meeting the needs of future connectivity that is fast, reliable, and secure. This thesis conducts a study and development of intelligent 6G communication systems with a focus on: (i) unknown optimal machine learning for channel estimation architecture that is simple yet accurate, (ii) unknown 6G path loss exponent, and (iii) unknown working principle of E91 and BB84 and unknown keys generated against practical parameters such as eavesdropping and channel errors. 6G systems are expected to deliver higher reliability, capacity, and security than previous generations, especially in the face of complex signal propagation challenges.

To overcome these problems, this thesis proposes three main solutions, namely: (i) application of machine learning for adaptive channel estimation, (ii) measurement of path loss to obtain 6G path loss exponent, and (iii) application of E91-based quantum key distribution (QKD) protocol to ensure the security of future quantum communication. The machine learning methods evaluated to estimate the channel are long short-term memory (LSTM) and fully connected deep neural network (FDNN). Path loss measurements are performed with 50-500 m distance variations in increments of 50 at frequencies of 4.4-4.8 GHz, meanwhile, we simulate the E91 protocol in real-world scenarios involving eavesdropping and errors on the quantum channel.

The results show that the LSTM model with one hidden layer and 16 neurons is able to produce channel estimation with the performance of bit error rate (BER) and frame error rate (FER) equivalent to that of perfect channel estimation. *Path loss exponent* 6G yields (i) n values of 2.48 for the line of sight (LOS) scenario and 2. 69 for the non-line of sight (NLOS) scenario at 4.4 GHz, (ii) n values of 2.45 (LOS) and 2.62 (NLOS) at 4.5 GHz, (iii) at 4.6 GHz n values of 2.51 (LOS) and 2.61 (NLOS), (iv) n values of 2.54 (LOS) and 2.59 (NLOS) at Frequency 4.7 GHz, and (v) n values of 2.55 (LOS) and 2.66 (NLOS) for Frequency 4.8 GHz using the *curve fitting* method from field measurements. Furthermore, the E91 protocol generates fewer keys than BB84, but offers higher security thanks to the utilisation of the Clauser-Horne-Shimony-Holz (CHSH) inequality without requiring any additional verification process. In addition, eavesdropping or channel errors may result in a

reduced number of keys being generated during the key production process.

Keywords: 6G, channel estimation, path loss exponent, quantum cryptography