ABSTRACT

The rapid growth of internet has given birth Internet of Things (IoT). Message Queuing Telemetry Transport (MQTT) is one of the most popular protocol on IoT networks because of the constrained characteristics. MQTT uses SSL/TLS as a security standard. In 2022, there's 1 trillion devices connect to the internet. The high number of users will increase the number of cybercrimes. One of the most popular attack is Denial of Service (DoS) attacks. DoS takes on the 3rd rank which lead the biggest losses in industrial sector. However, SSL/TLS isn't an appropriate security system to deal with DoS attack.

This minor thesis uses fuzzy logic algorithm to detect DoS attack in IoT networks based on MQTT protocol. Fuzzy logic will be embedded in a network node and detect DoS based on MQTT traffics where the input variables are SUBSCRIBE and SUBACK traffics. There are five parameters to evaluate fuzzy performance, are as follows False Positive Ratio (FPR), accuracy, precision, recall, and f-score.

The simulation considered different scenarios, those are 15, 20, 25, and 30 nodes with attack interval 3, 5, 7, and 9 seconds where 20% of total nodes were simulated as malicious nodes. The best fuzzy performance obtained on 20 nodes scenarios with FPR 0,1047; accuracy 94,39%; precision 0,9062; recall 0,9915; and f-score 0,9469. Whereas the worst fuzzy performance obtained on 30 nodes scenarios with FPR 0,4048; accuracy 79,88%; precision 0,7166; recall 0,9971; and f-score 0,8339. The result based on the simulations show that the number of nodes and the traffic intensities will impact the fuzzy logic algorithm performance in which the fuzzy logic algorithm performance will decrease as the number of nodes and the traffic intensities increases.

Keywords: Fuzzy, Message Queuing Telemetry Transport (MQTT), Internet of Things (IoT), Denial of Service (DoS).