ABSTRACT

LoRa is a wireless communication system that has the advantage of being able to reach long distances and saving power. In its implementation, LoRa has drawbacks in the form of being vulnerable to eavesdropping or disguising signals and data packets so that they can be stolen by irresponsible parties. This final project aims to demonstrate this vulnerability by carrying out a MITM Attack (Man In The Middle Attack) using tests in the form of reverse engineering (decoding, encoding, sniffing, and parsing) with temperature and humidity indicators using GNU Radio. The validity test method used is reverse engineering with transmitter and receiver devices, and will display data in the form of temperature, humidity, delay time, and frequency. This system will be able to perfect LoRa so that it is not vulnerable to eavesdropping.

Keywords: LoRa, *Reverse Engineering*, GNU Radio