ABSTRACT

The development of Global Navigation Satellite System (GNSS) technology has had a major impact on various sectors, such as transportation, telecommunications, and geolocation. Nevertheless, GNSS systems face a significant challenge in the form of potential GPS spoofing attacks, which can compromise the integrity of navigation data by manipulating received GPS signals. This threat can pose a high risk to applications that are highly dependent on the accuracy of location data, such as autonomous navigation systems and other critical applications. The main problem addressed in this research is how to effectively detect GPS spoofing attacks at an affordable cost for implementation on Internet of Things (IoT) based devices.

This study proposes a solution in the form of a low-cost IoT-based GPS spoofing signal detection system that integrates a u-blox NEO-6M V2 GPS module with an ESP32 microcontroller. This system acquires various GPS signal parameters, but the detection method used focuses on coordinate analysis (Latitude and Longitude). Detection is performed on the backend with a rule-based approach. The system analyzes incoming coordinate data in real-time and compares it with a valid reference point. If the deviation of the received coordinates exceeds a predetermined threshold, the system will classify it as a spoofing signal. The classification results are then displayed through a monitoring website built with Vercel.

Keywords: IoT, spoofing detection, GNSS, rule-based, thresholding, coordinate analysis.