ABSTRACT

The use of drones has grown rapidly over the years, both in the military and in the civilian field. Drones not only have positive impacts, but it also has negative impacts because many civilians use drones to carry out arbitrary actions that violate the law, this has created new security risks. Drones / *Unmanned Aerial Vehicles* (UAV) that are used by civilians are civilian *Global Positioning System* (GPS) signals that are unencrypted, unauthorized, and very easy to predict and duplicate. The GPS on the drone has a role as a satellite navigation system that is used to show the position where the UAV is flying. Therefore, if the civil signal is faked, the position of the civilian UAV can be manipulated and the movement from the civilian UAV to the target point will not be achieved.

In this final project, a low-cost fake GPS research will be carried out using HackRF One based a *Software Defined Radio* (SDR). This fake GPS will take advantage of civilian GPS signals to be duplicated. The spoofer will broadcast a fake GPS signal at a higher power level than the original satellite signal on the drone causing the real signal to be lost under a stronger spoofer signal. This research is about the transceiver of the antenna. The results of this project, this fake GPS will broadcast a fake GPS signal with a power level much higher than the original satellite signal on the drone which causes the original signal to be lost under a stronger signal spoofer.

From the results of research and analysis, the GPS receiver can receive fake GPS signals with a maximum distance of 40m. Differences in measurement distance and room conditions greatly affect the accuracy of the false GPS signal received. The farther the measurement distance, the smaller the power received, and the difference in distance between the coordinates read by the GPS receiver and the actual GPS coordinates will be further away. Research conducted indoors also showed better results with a reception reaching -52.48 dBm and a distance difference of 31.43m at a measurement distance of 10m compared to the results of research conducted in the open field. Test results and calculations show this system is feasible to use to overcome the use of unauthorized drones.

Keywords: Fake GPS; *Software Defined Radio*; HackRF One