ABSTRACT

The Wireless Sensor Network (WSN) consists of various devices with limited resources and is capable of detecting and tracking a certain space to gather data and transmit it to the root node by utilizing a routing protocol. To acquire and transfer data, these budget-friendly wireless devices are often deployed in a hostile, empty, and wide-open area, rendering them especially vulnerable to attack. Routing protocol for low power and lossy networks (RPL)-based low power and lossy networks (LLNs) largely determine the lifetime and quality of the network and the devices itself.

This research attempts to examine the RPL and exploring various types of cyberattacks against RPL, including Hello Flood, Version Number Modification Attack, and Blackhole. Based on this premise, the ultimate objective of this study is to implement these attacks against RPL and to holistically simulate them using the Cooja Simulator. Eventually, as data was collected through a simulation, the data was therefore processed and analyzed using relevant parameters such as Network's Lifetime, Packet Delivery Ratio, End-to-End Delay, and Routing Overhead.

The performance test results obtained for a normal WSN with RPL are E2E Delay around 150-300 ms, PDR = 100%, Routing Overhead = 60%, and an Estimated Network's Lifetime around 1.5 years. The following are the impact of each attack scenario caused. First, Network's Lifetime reduced by 20 times (Hello Flood Attack), and 4 times (VNM Attack). For PDR, there is a decrease of 20% (Hello Flood Attack), 70% decrease (VNM Attack), and 60% decrease (Blackhole). E2E Delay increased by 15 times (Hello Flood Attack), and 10 times (VNM Attack). Lastly, Routing Overhead had an increase of 30% (Hello Flood Attack), and 35% (VNM Attack).

Keywords: Wireless Sensor Network (WSN), Routing protocol for low power and lossy networks (RPL), Cooja Simulator.