ABSTRACT

The Bluetooth Special Interest Group (SIG) has developed Bluetooth Low Energy (BLE), which is one of the classic Bluetooth protocols with the main feature of low power consumption. However, BLE is still vulnerable in terms of security. Therefore, this final project makes a *Signature-Based* Intrusion Detection Sistem (IDS) which has the ability to analyze sistem behavior based on the rules that have been made. The advantage of using a *Signature-Based* IDS is that there are no errors in detecting known attacks

This final project uses BLE with mesh network and DHT11 sensor as the network to be tested. In BLE Mesh itself uses the library from Espressif to support mesh networks. The DHT11 sensor is used as a form of implementation of the Wireless Body Area Network (WBAN). The topology that has been built will be monitored by the watchdog *node*. Watchdog is a *Signature-Based* IDS *node* with the purpose of unifying and analyzing network traffic. The Watchdog *node* uses a Raspberry Pi 3B+ that has the IDS and Wireshark applications installed. Every packet caught by watchdog will be recorded using Wireshark. Then the IDS App will analyze the traffic and provide alerts.

The results show that the IDS is able to read Wireshark logs in the form of capturing BLE Network traffic and can identify the state of BLE Network traffic. Indication of traffic state with “Unknown” packets and “Delta Time” in 0µs. IDS finds normal traffic if does not detect “Unknown” packets and “Delta Time” in 0µs, while IDS detects interference if it detects “Unknown” packets and no “Delta Time” in 0µs. Then the IDS detects the network is under attack if it detects “Unknown” packets and “Delta Time” in 0µs. In addition, IDS can provide information in the form of the number of packets and packet capture time and the number of packets indicating an attack. This study also calculates the quality of the BLE network and the results show that the BLE network has an average jitter value of 2µs and an average delay of 3.7ms. Based on the TIPHON standard, it means that the BLE network formed is of very good quality.

Keywords: *Bluetooth Low Energy, Mesh Network, Signature-Based IDS, Watchdog*