ABSTRACT

Wireless Sensor Network (WSN) is a technology that is being warmly used both for research and to help human activities. System security is one of the important things that must be considered both in wireless network and wireline network. Wireless sensor networks are expanding which are vulnerable and therefore require an effective security mechanism. Wireless sensor networks have several constraints such as limited memory, energy and computational capabilities that create constraints when coupled with security at sensor nodes.

To solve the above problem, this final project will implement and analyze security system in wireless sensor network refers to ZigBee standard. ZigBee schemes can be synchronized with new protocols targeted at low rates, small power devices, and sensor nodes. ZigBee requires cryptography that is expected to save power, computing power, and storage resources. To that end, the chosen security system is using AES128 encryption algorithm (Advanced Encryption Standard) which is implemented directly on ZigBee.

In this final project successfully apply AES128 decryption and encryption algorithm on wireless sensor network. The test used is a passive attack that can only see and capture the package only. In a security performance analysis, the confidentiality parameter is not fulfilled if it does not use security. Integrity parameters are fulfilled using or without using security. The largest throughput value is 1122 bytes / s at a distance of 21 meters. And the last delay at a distance of 49.5 meters with a value of 4.1483 s.

Keyword : WSN, ZigBee, AES128