Abstract

In the Wireless Sensor Network (WSN), security of data delivery is paramount, see the data obtained and sent by WSN is important. Many many threats that can attack WSN in collecting data, such as data theft, conversion of data without permission and much more [18]. So had to do a treatment against such attacks so that the main purpose of the WSN systems are met. Much can be done to against attacks aimed into WSN, one of which introduced a system of WSN security protocols, one of which Minisec. Minisec WSN is a security protocol that implement security systems work two layers, namely authentication and encryption.

Minisec are in the process of securing skipjack Encryption systems are still considered unsafe, view of skipjack that is quite old (Skipjack out in 1998) and the number of Keys used in the process. Viewed from the need to amend it so that shortage of it can be tackled. Advanced Encryption Standard (AES), is a system that can replace Encryption Encryption skipjack. AES encryption which is fairly strong and able to overcome the shortage of Encryption skipjack. But AES Encryption is pretty heavy, deep computing requires a great source. So it is necessary to test to be able to see the side effects in terms of improving energy efficiency in terms of security.

In this final project was tested and compared by looking at two aspects, namely security and energy efficiency. In terms of security, the development of the test bruteforce attack and avalanche effect and in terms of energy efficiency seen changes in energy use before and after applying the AES Encryption.

The conclusion of these tests, AES encryption process can replace diprotokol Minisec security. By comparison testing in terms of safety and energy efficiency, it was found that by using AES increased security level and in terms of energy use rose 10.35%

Keywords: Encryption, Cooja, Contiki, AES, Skipjack, WSN.