Abstract

Wireless Sensor Network is a wireless network that has numbers of sensors in it to analyse the condition of certain environment for example humidity, temperature and noise level but every packets that are sent is not safe due to lack of security. Security Protocol in wireless sensor network has major influence to protect the integrity, confidentiality and the capability to transmit data like an attack to the wireless network which can result the loss of capability of the sensors to be accessed by the user and the loss of the capability to transmit data about the condition of the environment and also can damage the performance in wireless network.

Protocol analysis are meant to decide which protocol that have better performance by comparing MiniSec security protocol and Sensor Network Encryption Protocol (SNEP). The simulation of the protocols used NS-3 Application and literature study for the analytical comparison of each protocols. At the end of the research, the result shows that in confidentiality, integrity and authentication point of view, MiniSec works better than SNEP due to its capability to work in flexible manner at authenticated encryption and also MiniSec has the upper hand at the energy consumption because MiniSec done its encryption and authentication in a single stage unlike SNEP for encryption and authentication are done in two separate stages.

Keywords: Wireless Sensor Network, NS-3, MiniSec, Sensor Network Encryption Protocol (SNEP).