ABSTRACT

Wireless Sensor Network is a set of devices used to retrieve data from the external environment by sensing, then convert them into a set of digital data and then forwarded to the base station through wireless communication to be processed. In wireless communication there are 7 security requirements, including message confidentiality, message integrity, message authentication, freshness, availability, self-organization, and secure localization. This study will compare 2 WSN security protocols: TinySec and SPINS. The testing parameters will be authentication, size overhead, and energy *& power* consumption. The outputs of each parameters will be: packet captures that show the valid or invalid packets, number of additional bytes in the message, and energy and power consumption tables and percentage of energy overhead. This testing simulation will be conducted on a network simulator application called NS3 with Packet Injection attack in 3 scenarios. The test results showed that TinySec and SPINS just as well on aspects of size overhead and authentication with the results 11 bytes size overhead and 100% success rate on authentication. But on the aspect of energy and power consumption TinySec superior spins with energy overhead 2.8321% for TinySec and 8.0413% for SPINS.

Keywords: Security Protocol, Wireless Sensor Network, TinySec, SPINS