ABSTRACT

Wireless Sensor Network (WSN) is a technology using wireless networking that consist of several embedded platform sensor nodes integrated to each other. In the implementation, the sensor nodes are placed in the areas that can be accessed real-time. So that attack may occur directly. WSN attack on network layer is to steal packages or to modify some routing information that can disturb routing lines. Based on WSN vulnerable condition, it needs mitigation attacks on WSN by system shutdown. This is to shutdown communication directly before the information is processed in the system. The research tested the energy consumption and network performance with AODV routing protocol given sybil attack and shutdown system using NS-2.35 software. Network performance measured was the amount of packet delivery ratio, through put, end to end delay. Besides that, energy consumption was also measured. The results showed on that the sybil attack decrease the wireless performance on packet delivery ratio and throughput while wireless performance on delay increase, decrease on Packet Delivery Ratio by 0,26%, decrease on throughput by 0,26 kbps, and increase on delay by 3000 ms. The result showed on scenario of attack occurrence without implementing shutdown system using AODV protocol with node of 100. Energy consumption rate is lower than attack occurrence and nonoccurrence. Because, the energy consumed comes only from the node in the best routing line at discover route. Sybil attacks can be tackle by shutdown system, but the implementation does not decrease on disturb the WSN performance.

Keywords : Wireless sensor network, sybil attack, AODV, shutdown system.