ABSTRACT

Wireless Sensor Network (WSN) is a wireless networking technology that consists of a large number of low-cost, low-power, and multifunctional node sensors. Sensor nodes on WSN also have routing capabilities such as routers. One of the routing protocols on WSN is Ad hoc On-Demand Distance Vector (AODV). AODV performs a routing path search when a request from a source node is sent to the destination node. Because the node sensors installed in the environment are physically accessible, the potential for attack will increase. The sinkhole attack is one of the threats to WSN. A sinkhole attack is a type of attack on a network layer where a compromised node sends false routing information to its neighbor to pull network traffic to itself. To reduce the impact caused by the sinkhole attack, it is necessary to do a mitigation attack on WSN using AODV routing protocol with shutdown system. It aims to turn off packet delivery between the source node, sinkhole node and destination node directly before the packet is processed by the system. From the results of network perfomance testing can be seen that sinkhole attacks reduce network performance in the packet delivery ratio and throughput while the end to end delay increased, with a decrease in packet delivery ratio of 99.8%, decreased throughput 99,8 kbps, then delay increased of 3200 ms. While the value of energy consumption in system shutdown stable. With the system shutdown, sinkhole attacks can be mitigated and not reduce and disrupt network performance on WSN.

Keywords: Wireless sensor network, mitigation, sinkhole attack, AODV, system shutdown.