ABSTRACT

Wireless Sensor Network (WSN) has a significant role in areas such as deployment in warfare areas, smart home deployment, smart car deployment, environmental research and healthcare applications. However, WSN has a deficiency in the absence of an innate security system that is embedded in a sensor device that is spread out in open space. In addition node sensors also have limited power and energy, consequently WSN is very vulnerable to attack. One of the attacks that could threaten the security of the WSN is the blackhole attack. Therefore in need of a system to maintain security on WSN. In this study discuss ways or methods to detect and mitigate blackhole attacks, namely by using the signature based Intrusion Detection System (IDS) and system shutdown on sink nodes. The system shutdown built in this research was successfully implemented on WSN. When IDS detects a blackhole attack, system shutdown can secure data on the sink node by shutting down the node's sink. Therefore the system shutdown can be used as an alternative as well as the initial step in securing WSN.

keywords: wireless sensor network, intrusion detection system, blackhole attack, system shutdown, signature approach.