

ABSTRAK

Wireless Sensor Network (WSN) memiliki peran yang cukup besar dalam beberapa bidang seperti penerapan pada area peperangan, penerapan pada rumah pintar, penerapan pada mobil pintar, penelitian tentang lingkungan serta penerapan di bidang kesehatan. Namun WSN memiliki kekurangan dimana tidak adanya sistem keamanan bawaan yang tertanam pada perangkat *sensor* yang tersebar di ruang terbuka. Selain itu *sensor node* juga memiliki keterbatasan daya dan energi, akibatnya WSN sangat rentan terhadap serangan. Salah satu serangan yang dapat mengancam keamanan WSN adalah serangan *blackhole*. Maka dari itu di perlukan sistem untuk menjaga keamanan pada WSN. Dalam penelitian ini membahas cara atau metode untuk mendeteksi dan memitigasi serangan *blackhole*, yaitu dengan menggunakan *signature based Intrusion Detection System* (IDS) dan *system shutdown* pada *sink node*. *System shutdown* yang dibangun pada penelitian ini berhasil diimplementasikan pada WSN. Ketika IDS mendeteksi adanya serangan *blackhole*, *system shutdown* dapat mengamankan data pada *sink node* dengan cara mematikan *sink node* tersebut. Maka dari itu *system shutdown* dapat digunakan sebagai alternatif serta langkah awal dalam mengamankan WSN.

kata kunci : *wireless sensor network, intrusion detection system, blackhole attack, system shutdown, signature approach.*