ABSTRAK

Wireless sensor network (WSN) merupakan sebuah jaringan nirkabel yang terdiri dari sejumlah *sensor node* berukuran kecil untuk memantau kondisi lingkungan tertentu. Setiap *sensor node* akan saling berkomunikasi dan mengirimkan informasi ke *base station*. Seperti halnya *router*, *sensor node* pada WSN juga memiliki kemampuan *routing*. Protokol *routing* pada WSN salah satunya dalah AODV yang memiliki karakteristik mencari jalur *routing* ketika adanya permintaan dari *souce node* untuk mengirim pesan ke *destination node*. Dikarenakan *sensor node* yang dipasang di lingkungan dapat diakses secara fisik maka meningkatkan potensi terjadinya serangan. Serangan *wormhole* merupakan jenis serangan di mana penyerang memindahkan jalur *routing* pada WSN ke terowongan yang dibuat diantara *source* dan *destination node*. Serangan *wormhole* dapat menjadi pemicu timbulnya serangan lain pada WSN. Berdasarkan kondisi yang rentan terhadap adanya serangan, maka dibutuhkan adanya mitigasi serangan pada *wireless sensor network* menggunakan protokol *routing* AODV dengan sistem *shutdown*. Hal ini bertujuan untuk mematikan *sensor node* yang telah mengalami modifikasi dari penyerang sebelum informasi tersebut diproses oleh sistem dan dikirim ke *user*. Dari hasil pengujian yang dilakukan diketahui bahwa pada penerapan sistem *shutdown* terjadi efisiensi energi yang dikonsumsi dengan tidak adanya penurunan dalam performansi jaringan. Sehingga sistem *shutdown* dapat menjadi salah satu solusi efektif dalam memitigasi serangan *wormhole*.

Kata Kunci : *Wireless sensor network*, serangan *wormhole*, AODV, sistem *shutdown*.