ABSTRAK

Menjamin keamanan dan privasi merupakan salah satu prioritas tertinggi dalam WSN karena data yang dikumpulkan oleh sensor node tidak jarang merupakan data yang bersifat rahasia. Terdapat sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas mencurigakan dalam sebuah sistem atau jaringan berbasis nirkabel, yaitu *Wireless Intrusion Detection System* (WIDS). Namun, dari sekian banyak teknik pendekatan untuk WIDS belum ada yang dapat sepenuhnya terhindar dari kesalahan berupa *false negative* maupun *false positive*.

Mekanisme cara kerja teknik pertahanan jaring laba – laba akan diterapkan pada alur kerja WIDS yang dibangun dengan tujuan mengurangi adanya *false negative*. Penerapannya dalam sistem nyata adalah memberikan *delay* untuk setiap paket yang masuk. Metode pengujian yang dilakukan berupa pengujian deteksi serangan dan perhitungan *false negative*. Pengujian deteksi serangan dilakukan dengan memberikan serangan *inside attack* berupa serangan *access point spoofing* dan serangan *de-authentication flood*. Hasil dari pengujian deteksi serangan menunjukkan bahwa WIDS mampu mendeteksi adanya serangan *inside attack*. Sementara perhitungan *false negative* mendapatkan hasil bahwa seiring ditambahkannya waktu *delay*, presentase *false negative* yang didapatkan mengalami penurunan namun kemudian dapat naik kembali. Pemberian waktu *delay* paling ideal kurang lebih 500 ms dengan tingkat presentase *false negative* berkurang hingga 66.37%.

Kata kunci : *false negative, Wireless Intrusion Detection System* (WIDS), sistem keamanan, teknik pertahanan jaring laba-laba, *Wireless Sensor Network* (WSN).