

ABSTRAK

Wireless Sensor Network merupakan seperangkat alat yang digunakan untuk mengambil data dari lingkungan sekitar dengan cara *sensing*, lalu mengubahnya menjadi data digital untuk kemudian diteruskan ke *base station* melalui komunikasi nirkabel dan diproses. Dalam komunikasi nirkabel terdapat tujuh hal yang menjadi *security requirement*, antara lain *message confidentiality*, *message integrity*, *message authentication*, *freshness*, *availability*, *self-organization*, dan *secure localization*. Dalam penelitian ini akan dilakukan pengujian untuk membandingkan dua jenis protokol keamanan (*security protocol*), yaitu TinySec dan SPINS. Aspek yang menjadi tolak ukur performansi keduanya adalah autentikasi, *size overhead*, dan *energy & power consumption*. Masing-masing aspek tersebut memiliki *output packet capture* yang menunjukkan adanya paket yang diterima / di-drop, berupa jumlah byte yang ditambahkan pada *message*, dan tabel penggunaan energi dan daya beserta persentase *energy overhead*. Simulasi pengujian akan dilakukan pada *software* NS3 dengan memberikan penyerangan jenis *Packet Injection* kepada kedua protokol dengan tiga skenario berbeda. Hasil pengujian menunjukkan TinySec dan SPINS sama baiknya pada aspek *size overhead* dan autentikasi dengan hasil 11 byte overhead dan 100% kesuksesan autentikasi. Namun pada aspek *energy & power consumption* TinySec lebih unggul daripada SPINS dengan *energy overhead* masing-masing 2,8321% dan 8,0413%.

Kata Kunci : *Security Protocol, Wireless Sensor Network, TinySec, SPINS*