

ABSTRAK

Keamanan merupakan perhatian utama dalam *Mobile Wireless Sensor Network* (MWSN) dan sangat sulit untuk menerapkan sistem keamanan tersebut. Banyak tantangan terjadi karena sensor membatasi jumlah kekuatan pemrosesan, penyimpanan, node yang bersifat mobile, *bandwidth* dan energi. Tantangan-tantangan ini harus diatasi karena disebabkan oleh pentingnya keamanan dalam *mobile sensor node* dan domainnya yang menangani informasi yang sensitif. Penelitian ini akan membahas tentang keamanan autentikasi dan performansi MWSN.

Pada penelitian ini, akan diterapkan penggabungan metode algoritma *Elliptic Curve Cryptography* (ECC) dan fungsi *HASH SHA-256* yang akan memungkinkan autentikasi mudah dan cepat antara node sensor yang bergerak serta mengamankan komunikasi didalam jaringan dari serangan-serangan yang mungkin terjadi tentunya dengan konsumsi energi yang rendah.

Setelah dilakukan pengujian antara MWSN tanpa menggunakan dan dengan menggunakan penggabungan metode, hasil penerapan penggabungan metode ECC dan SHA-256 mengalami peningkatan kualitas dan diperoleh rata-rata QoS dengan parameter *delay* sebesar 1310,28 ms, *packet loss* sebesar 92,14%, *throughput* sebesar 0.0192 Mbit/s dan konsumsi total energi sebesar 16.0125200175166 J. Dari hasil tersebut, penggabungan metode algoritma dan SHA-256 dapat meningkatkan kualitas QoS dan dapat diterapkan pada MWSN.

Kata Kunci: *Mobile Wireless Sensor Network, Elliptic Curve Cryptography, SHA-256, keamanan, autentikasi*