Implementasi Algoritma AES untuk Keamanan Akuisisi Data Estimasi Posisi pada Aplikasi *Tracking* Posisi Pasukan di Medan Perang

Nuskha Ilma Arini[1], Prima Kristalina[2], Haryadi Amran Darwito[3]
Program Studi D4 Teknik Telekomunikasi
Departemen Teknik Elektro
Politeknik Elektronika Negeri Surabaya
Kampus PENS, Jalan Raya ITS Sukolilo, Surabaya 60111
Tel: (031) 594 7280; Fax: (031) 594 6114
Email:arin.ilmaarini@gmail.com,prima@pens.ac.id, amran@pens.ac.id

Abstrak

Kemajuan teknologi komunikasi informasi, khususnya dalam bidang Jaringan Sensor Nirkabel (JSN) berkembang pesat. Lokalisasi merupakan salah satu topik terpenting dalam JSN. Kebutuhan posisi sebuah objek diperlukan untuk mengetahui posisi dari fenomena yang sedang diukur oleh sensor. Contohnya aplikasi *monitoring* dan aplikasi *tracking*. Kerahasiaan dan keamanan data juga merupakan aspek penting pada pengiriman informasi. Berbagai usaha dilakukan untuk melindungi informasi. Hal ini berlaku juga untuk data lokasi pasukan di medan perang. Sehingga diperlukan cara untuk mengamankan informasi data lokasi. Kriptografi merupakan solusi untuk masalah tersebut. Pada proyek akhir ini dibuat sebuah teknik kriptografi dengan metode AES (*Advanced Encryption Standard*) untuk menjaga kerahasiaan pada saat pengiriman data. Data yang dikirim berupa data koordinat lokasi terenkripsi yang dikirimkan melalui sebuah *node* berbasis *singlehop*. Pada penelitian ini dibuat sebuah simulasi tracking posisi pasukan di medan perang pada sisi *server* yang dilengkapi dengan metode AES, dimana data posisi yang dikirim sudah dienkripsi. Sehingga pengimplementasian metode AES hanya pada bagian dekripsinya saja.

Hasil waktu rata-rata dari pengujian algoritma AES untuk dekripsi data koordinat dengan panjang 26 karakter adalah 890052.76 μs. Sedangkan pada proses akuisisi data, setiap kelipatan jumlah baris data mengalami jumlah kenaikan waktu eksekusi sebesar 60% dari waktu awal. Error estimasi posisi rata-rata dengan menggunakan algoritma trilaterasi adalah sebesar 5,17 m.

Kata kunci: JSN, kriptografi, dekripsi, AES, lokalisasi, trilaterasi, multikanal DAS