Abstrak

LoRa atau *Long Range* dengan teknologi LoRaWAN adalah contoh baru dari kelas jaringan dan sedang digunakan dalam skala besar di beberapa negara. Kekurangan dari jaringan LoRaWAN yaitu tidak adanya proses enkripsi pada *payload data*. Saat proses pengiriman pesan sedang berjalan antar perangkat, *sniffing process* dapat mengetahui semua pesan yang dikirim maupun yang diterima oleh perangkat, sehingga besar kemungkinan dapat terjadi serangan dari proses *sniffing* tersebut yang menyebabkan tidak adanya privasi dalam *payload data*. Penelitian ini menggunakan metode *digital signature* untuk mengamankan pesan yang dikirimkan oleh perangkat jaringan LoRaWAN menggunakan algoritma *Advanced Encryption Standard* (AES) pada proses enkripsi dan dekripsi pesan, serta menggunakan algoritma Ed25519 pada proses *signature*, penelitian ini juga menganalisis *overhead* dari penerapan metode *digital signature*. Tujuan penerapan *digital signature* dalam sistem ini adalah untuk memverifikasi bahwa *payload data* yang dikirim adalah asli dan tidak berubah selama proses transmisi, serta menjamin kerahasiaan pada *payload data*. Penambahan mekanisme keamanan pada jaringan LoRaWAN seperti proses enkripsi, dekripsi dan hasil verifikasi telah menghasilkan *overhead* pada beberapa aspek. Setelah dilakukan analisis, terdapat peningkatan ukuran untuk beberapa aspek saat diterapkannya metode *digital signature*.

Kata kunci: LoRaWAN, sniffing, digital signature, AES, overhead.