ABSTRAK

Jaringan sensor dalam *Internet of Things (IoT)* sangat penting untuk Sistem Fisik-Siber, yang mengintegrasikan dunia fisik dan digital. Sinkronisasi waktu yang efektif sangat penting untuk mengelola jaringan ini, termasuk dalam proses seperti keamanan, lokalisasi, perutean, dan pelacakan. Tanpa sinkronisasi yang tepat, korelasi file log antar perangkat menjadi sulit, yang dapat menyebabkan konflik dan hilangnya layanan. Memastikan sinkronisasi waktu yang aman sangat penting, dengan menggunakan algoritma dan protokol yang kuat. Sinkronisasi waktu menyelaraskan waktu jam lokal di seluruh node, melawan drift jam perangkat keras. Algoritma konsensus terdistribusi telah menunjukkan ketahanan terhadap ancaman seperti serangan *Denial of Service* (DoS) dan manipulasi data, tetapi kinerjanya sangat dipengaruhi oleh perubahan topologi jaringan, menjadikan serangan topologi sebagai fokus penelitian yang signifikan. Ketahanan sinkronisasi waktu berbasis konsensus bergantung pada topologi jaringan, yang direpresentasikan oleh matriks kedekatan dan nilai eigen graf Laplacian, yang menunjukkan kekuatan konektivitas. Penetapan Bobot Tetap (FWA), Penetapan Bobot Terpusat (CWA), dan Penetapan Bobot Bergerak (MWA) adalah algoritma penetapan bobot konsensus yang digunakan dalam sinkronisasi WSN, masing-masing beradaptasi secara berbeda terhadap kondisi jaringan. Namun, metode ini sering mengabaikan dampak perubahan topologi selama serangan. Penelitian ini mengusulkan metode penetapan bobot sinkronisasi konsensus berbasis graf menggunakan nilai eigen Laplacian untuk menguji ketahanan terhadap serangan topologi, dengan fokus pada kecepatan konvergensi dan akurasi sinkronisasi. Temuan menunjukkan bahwa menggabungkan gain Laplacian meningkatkan toleransi kesalahan, mengurangi iterasi konvergensi sekitar 40,42%, dan meningkatkan akurasi jaringan sekitar 9,34%. Hal ini menunjukkan peran penting metode konsensus berbasis Laplacian dalam menjaga kecepatan konvergensi jaringan dan akurasi jaringan di bawah perubahan topologi, merekomendasikan penerapannya untuk meningkatkan ketahanan WSN terhadap serangan.

Kata kunci: Keamanan *IoT*, Sinkronisasi Waktu, Serangan *Clock,* MWA, Laplacian