ABSTRAK

Keandalan *Vehicular Ad-hoc Networks* (VANET) merupakan fondasi krusial bagi aplikasi sistem transportasi cerdas. Namun, kinerjanya secara fundamental terancam oleh keberadaan *selfish node*, yaitu *node* yang menolak untuk meneruskan paket data. Masalah ini diperparah oleh kelemahan protokol perutean konvensional yang cenderung "buta" terhadap perilaku *node*. Penelitian ini mengajukan mekanisme keamanan proaktif bernama *Fuzzy Trust Filtering*, yang dirancang untuk mengidentifikasi dan mengisolasi *selfish node* dengan mengintegrasikan kepercayaan langsung (*direct trust*) dan tidak langsung (*indirect trust*) melalui model berbasis logika *fuzzy* untuk menangani ketidakpastian. Kinerja *Fuzzy Trust Filtering* dievaluasi melalui simulasi dengan data mobilitas urban dari *Simulation of Urban Mobility* (SUMO) dan dibandingkan dengan protokol standar (*Baseline*) serta algoritma pembanding, *Filtering Algorithm of Selfish Node* (FASN), yang bekerja dengan cara menurunkan probabilitas transmisi dari *selfish node*. Metrik evaluasi mencakup *Packet Delivery Ratio* (PDR), *Average Delay*, dan *Detection Probability* (DP). Hasil eksperimen menunjukkan bahwa *Fuzzy Trust Filtering* secara konsisten mengungguli FASN dan *Baseline*, dengan PDR tertinggi dan *delay* terendah di semua skenario serangan. Dalam hal deteksi, *Fuzzy Trust Filtering* menunjukkan superioritas dengan rata-rata DP sebesar 77.78%, lebih tinggi dibandingkan FASN (64.14%), serta menghasilkan kurva *Receiver Operating Characteristic* (ROC) yang lebih efisien. Analisis internal menggunakan *Weighted Sum Model* (WSM) secara kuantitatif menunjukkan bahwa *trust threshold* optimal bersifat kontekstual: $\tau = 0.5$ unggul untuk skenario berorientasi performa, sementara $\tau = 0.9$ menjadi pilihan terbaik untuk skenario yang memprioritaskan efisiensi & keamanan. Temuan krusial ini divalidasi secara statistik melalui uji *Analysis of Variance* (ANOVA) dengan $p < 0.05$. Penelitian ini berhasil memvalidasi bahwa *Fuzzy Trust Filtering* bukan hanya solusi yang efektif dan dapat dikonfigurasi, tetapi juga menunjukkan kinerja yang lebih unggul dibandingkan dengan metode pembanding relevan dalam meningkatkan keamanan dan keandalan perutean VANET.

Kata kunci—*Vehicular Ad-hoc Network* (VANET), Manajemen Kepercayaan, *Selfish Node*, Logika *Fuzzy*, SUMO, Kinerja Jaringan

ABSTRACT

The reliability of Vehicular Ad-hoc Networks (VANETs) is a critical foundation for intelligent transportation system applications. However, their performance is fundamentally threatened by the presence of selfish nodes, i.e., nodes that refuse to forward data packets. This problem is exacerbated by the limitations of conventional routing protocols, which are often "blind" to node behavior. This study proposes a proactive security mechanism called Fuzzy Trust Filtering, designed to identify and isolate selfish nodes by integrating direct and indirect trust through a fuzzy logic model to handle uncertainty. The performance of Fuzzy Trust Filtering is evaluated using mobility data from the Simulation of Urban Mobility (SUMO) and compared against a standard baseline protocol as well as a benchmark algorithm, the Filtering Algorithm of Selfish Node (FASN), which operates by reducing the transmission probability of selfish nodes. Evaluation metrics include Packet Delivery Ratio (PDR), Average Delay, and Detection Probability (DP). Experimental results demonstrate that Fuzzy Trust Filtering consistently outperforms both FASN and the baseline, achieving the highest PDR and the lowest delay across all attack scenarios. In terms of detection, Fuzzy Trust Filtering achieves superior performance with an average DP of 77.78%, higher than FASN (64.14%), and yields a more efficient Receiver Operating Characteristic (ROC) curve. Internal analysis using the Weighted Sum Model (WSM) quantitatively shows that the optimal trust threshold is contextual: $\tau = 0.5$ is preferable for performance-oriented scenarios, while $\tau = 0.9$ is more suitable for scenarios prioritizing efficiency and security. These findings are statistically validated through an Analysis of Variance (ANOVA) test with $p < 0.05$. Overall, this study validates that Fuzzy Trust Filtering is not only an effective and configurable solution, but also achieves superior performance compared to relevant benchmark methods in enhancing the security and reliability of VANET routing.

Keywords—Vehicular Ad-hoc Network (VANET), Trust Management, Selfish Node, Fuzzy Logic, SUMO, Network Performance