ABSTRACT

Vehicular Ad Hoc Networks (VANETs), crucial for Intelligent Transportation Systems (ITS), face significant security threats, especially Denial of Service (DoS) and Distributed DoS (DDoS) attacks. These attacks disrupt communication, leading to packet loss, increased latency, and reduced reliability. While existing solutions like trust-based models, cryptographic techniques, and machine learning approaches exist, they often fall short in detection accuracy, energy efficiency, adaptability to mobile environments, and managing system overhead.

This research, titled "Securing VANETs through a Hybrid Approach: Mitigating Denial of Service (DoS) Attacks and its types with Self-healing and Immunization," proposes a three-phase methodology to enhance the security of VANETs. It leverages a hybrid approach having six key contributions with the major objective to secure VANETs—a key part of Intelligent Transportation Systems—from DoS attacks by detecting and preventing these attacks including self-healing and immunization features. The scope of the research tends to focus on DoS attacks and its types with multi-layered defense incorporating security and robustness.

In Phase 1, the objective is to detect and isolate vehicles under malicious DoS attacks with optimized feature selection using GLW-SLFN (Glow-worm Single Layer Feed Forward Neural Network). MCOD-LR (Micro Cluster Outlier Detection and Linear Regression) is applied to detect malicious behavior for multi-class DoS attacks. Furthermore, Kernel Density Estimation and Entropy-based SVM (Support Vector Machine), incorporating trust factors, are leveraged to detect, predict, and classify DoS attacks. A Bayesian aggregate model, in conjunction with Self-healing AIS (Artificial Immune Systems), ensures the continuous monitoring, detection, and isolation of these attacks.

The changing topology in VANET remains a challenge in securing VANET operations. This challenge is addressed in phase 2, as the traffic signals are encrypted using Triple Random Hyperbolic Encryption (TRHE) integrated with Hex-Tuple Matched Mapping, which classifies twelve types of DoS attacks. The classification relies on mapping reports and a Deep Trust Factorization Neural Network (DT - NN).

Furthermore, to achieve stable data transmission and routing even with dynamic network topology, phase 3 is proposed to immunize the behavior of its clusters by the Deep Trust Factorization Neural Network (which provided trust scores), the Moth Flame Optimization (MFO) Algorithm, and Cache Parallelized Circulation Link Routing (CCL). The system achieved stable data transmission and routing, even with dynamic network topology, due to the immunized behavior of its clusters. The Moth Flame Optimization (MFO) algorithm optimizes the Packet Delivery Rate (PDR) essential for ensuring data is delivered efficiently. This system efficiently creates stable clusters and identifies reliable relay nodes within a VANET. This feature enables the isolation of malicious nodes, directly leading to a significant increase in the Packet Delivery Rate (PDR).

The performance of Phase 1 demonstrated significant improvements: a 37% increased detection rate over AODV, 32% over Trust-based methods, and 20% over Firecol. The approach also reduced energy consumption by 38% compared to AODV, Trust-based, and Firecol. Furthermore, it achieved a 25% lower latency, markedly outperforming AODV (95%), Firecol (58%), and the Trust-Based Framework (27%).

Building on this, Phases 2 and 3 collectively enhanced overall performance, resulting in a minimized packet loss of 0.5 bits for 200 nodes, a maximized attack detection accuracy of 97%, and a Packet Delivery Ratio (PDR) of 98%. These figures represent a substantial improvement over existing techniques: Trilateral Trust (42% accuracy, 60% PDR), Host-based Intrusion Detection System (H-IDS) (60% accuracy, 70% PDR), Multi-filter (80% accuracy and PDR), and Stream Position Performance Analysis (SPPA) (90% accuracy and PDR).

This approach demonstrates remarkable scalability and adaptability, particularly in challenging environments with high node mobility and dense vehicular traffic. The methods ensure resilient network operations in intelligent transportation systems, delivering reduced energy usage, lower communication delays, and high detection accuracy for secure, reliable, and scalable communication. This research provides highly relevant solutions for real-time VANET applications, effectively incorporating self-healing, immune-inspired mechanisms.