CHAPTER 5

CONCLUSION

The research work entitled “Securing the VANET through the hybrid approach by Mitigating DoS attacks and types with Self-Healing and Immunization” is a three-phase methodology in enhancing the security of VANET. This hybrid approach successfully fulfilled the major objective of securing VANETs by mitigating DoS attacks and their variants, while also addressing several inherent challenges in VANET environments.

Enhanced Feature Selection and Mitigation as phase 1 utilized MCOD-LR, Entropy-based SVM, and the self-healing capabilities of AIS**,** achieving a 97% DoS attack detection rate, notably surpassing AODV (60%), trust-based frameworks (65%), and Firecol (77%) by identifying optimized feature sets.

In Phase 2, strengthening the access control and mapping integrated Triple Random Hyperbolic Encryption and Deep Auto Sparse Impasse Neural Networks (NN). This integration significantly enhanced attack detection capabilities, preventing data breaches and unauthorized access, even as vehicle nodes increased.

Finally, Phase 3 integrated MFO and immunized cluster-based routing with trust-aware mechanisms, efficiently creating stable clusters and identifying reliable relay nodes to isolate malicious activity, thereby significantly increasing the Packet Delivery Rate (PDR). Overall, the proposed framework maintained a 98% PDR, 99% attack detection accuracy, and a rapid 0.1 ms detection time, enabling adaptive routing, malicious node isolation, and synchronization-based channel hopping to manage dynamic vehicular traffic, outperforming existing methods like Trilateral Trust, H-IDS, Multi-filter, and SPPA (Poongodi et al., 2019).

This framework significantly enhances VANET security, leading to more robust, energy-efficient, and scalable Intelligent Transportation System (ITS) infrastructures. It's particularly valuable for real-time VANET deployments because it lowers communication latency, reduces energy consumption, and increases attack detection accuracy, maintaining strong performance in dense, mobile networks. The framework's

superior Packet Delivery Ratio (PDR) and reduced latency demonstrate its effectiveness in busy urban and high-mobility traffic environments.

The review of current methods, in chapter 2, for mitigating DoS attacks in VANETs—including trust-based frameworks, cryptographic schemes, and machine learning-based intrusion detection—revealed persistent challenges. These issues primarily revolve around adaptability, energy consumption, detection granularity, and scalability. The proposed methodology systematically addresses the shortcomings of existing solutions, as discussed below:

Improved Detection Accuracy: Unlike traditional ML-based IDS models (e.g., Firecol, AODV), often producing high false positives lacks adaptability, the proposed framework leverages MCOD-LR, Entropy-based SVM, and the self-healing effect of AIS significantly improved detection accuracy while simultaneously lowering latency and energy consumption, surpassing the performance of AODV and other trust-centric solutions.

Efficient and Secure Encryption: The computational inefficiencies of existing cryptographic methods (e.g., ASCII-ECC, ECC-GA-PASR) are overcome with TRHE model featuring Hex-Tuple Matched Mapping. This provides secure, lightweight encryption of traffic with minimal delay, guaranteeing confidentiality and authenticity even in highly mobile environments.

Precise Attack Classification: Older models (e.g., SVAP, host-based IDS) struggled to classify various attack types. This research framework uses a DTFNN with semantic trust mapping for the precise classification of distinct DoS attack variants.

Stable and Reliable Routing: To combat routing instability and malicious interference in VANETs, MFO with trust scores and cache-parallel circulation link routing dynamically creates stable clusters and identifies trustworthy relay nodes. This resulted in higher Packet Delivery Ratios (PDR) and more effective in isolation of malicious activity than methods like KSVM or fuzzy ensemble models.

Enhanced Scalability and Resilience: The hybrid approach in this research work tackles the inherent challenges of scalability, redundancy, and training complexity found in methods such as H-IDS, Trilateral Trust, and SPPA. Immunization-based resilience, preemptive threat isolation, and semantic-based relay selection are the key to significantly reducing packet loss and enabling real-time adaptation in challenging dense, high-mobility VANETs.

The contributions incorporated in this research demonstrates superior performance across key metrics, including detection accuracy, resource efficiency, robustness against various attacks, and adaptability to highly mobile vehicular networks.

The research framework, despite its significant advancements, faces a few limitations. The narrow focus of immunization strategy with MFO mainly optimizes PDR and cluster stability limiting its adaptability in highly dynamic VANET environments where a simultaneous balance of multiple objectives, such as latency, energy efficiency, and scalability, is crucial. Furthermore, while the framework effectively counters DoS and DDoS attacks, it doesn't address other emerging threats like insider threats or privacy breaches. Finally, the system's effectiveness under extreme network conditions or very high node mobility requires further empirical validation to confirm its robustness.