SPECIMEN FORMAT FOR THESES OF AUGUST

Faculty	**:**	**Physical Sciences and Computational Sciences**
Department	**:**	**Computer Science**
Branch/ Area:	**:**	**Cyber Security**
Sub Subject Heading:	**:**	**VANET Security**
Candidate's Name	**:**	**Rama Mercy. S**
Candidate's Address with email	**:**	**Teaching Assistant and Research Fellow,** **Department of Computer Science** **Avinashilingam Institute for Home Science and Higher Education for Women** **Coimbatore**
Title of the thesis	**:**	
(i) In Roman Script (ii) In roman Script		**Securing the VANET through a Hybrid Approach by Mitigating DoS Attacks and its types with Self-healing and Immunization**
Nomenclature of Degree:	**:**	
Month & Year of Enrolment:	**:**	December, 2017
Month & Year of Registration:	**:**	February, 2018
Month &Year of Submission:	**:**	January, 2025
Month &Year of Award	**:**	
Name of Supervisor	**:**	Dr. G. Padmavathi
Designation of Supervisor	**:**	Professor
Centre/department/school in which research was conducted	**:**	Department of Computer Science
University's Name & Address	**:**	Avinashilingam Institute for Home Science and Higher Education for Women Coimbatore – 641043.

Abstract within 300 words:

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.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. 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. Iin phase 2, 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). The proposed research represents 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. This research provides highly relevant solutions for real-time VANET applications, effectively incorporating self-healing, immune-inspired mechanisms.

i) Major objectives :

The primary objective of this research is to secure Vehicular Ad-Hoc Networks in Intelligent Transportation System through a hybrid approach to detect and mitigate DoS attacks and types with Self-healing and Immunization.

The secondary objectives that aim to fulfill the major objective are:

i. To enhance the detection with classification of DoS attacks with improved accuracy of detection and classification, recall, precision, minimum delay.

ii. To detect, predict and isolate (Mitigate) DoS attack and types with the communication link maintained having increased accuracy of detection, recall, precision, minimum delay, improved packet delivery ratio.

iii.To enhance the security and reliability of VANET services with minimum packet loss, maximum throughput, minimum processing time and maximum packet delivery ratio.

ii) Methodology :

A three step methodology with six different contributions proposed is discussed. The framework is instantiated with the simulation of the VANET considering the datasets CIC-IDS 2018 and CIC-DDoS 2019. In the Phase 1, detection and classification of DoS attacks using Glow-worm Single Layer Feed Forward Neural Network (SLFN) is the contribution 1 proposed. Optimized selection of features and a classifier to classify as normal and DoS attacks are elaborated with its implementation process. This model was initially designed to detect and mitigate these attacks. The model is built using Glow-worm optimized technique for optimized selection of features and a classifier to classify as normal and DoS attacks. Furthermore, an enhanced model is built to deal with multiclass attacks of DoS. For such detection, at the inception, the abnormal behaviour is detected with the deviations using Response Feedback Algorithm with Micro Cluster Outlier Detection and Linear Regression (MCOD-LR) is proposed as the contribution 2. The simulation outcomes indicate that the proposed enhanced model exhibits a high degree of effectiveness in detecting anomalies or deviations in traffic flow patterns.

The malicious vehicles in the clusters are further detected based on trust based approach with the classifier as the contribution 3. In this, the Prediction of Malicious DoS Attacks using Kernel Density Estimation and Entropy-based Support Vector Machine (SVM) Classifier is detailed with its procedure. The classifier predicts the variations in the trust value and entropy for randomness deviation. Kernel Density estimation with Entropy-based Support Vector Machine classifier predicts the maliciousness of the nodes based on DoS attacks.

The mitigation process through isolation of detected malicious vehicles based on DoS attacks is proposed using contribution 4. The Pearson correlation coefficient method is used to assess the degree of similarity between the predicted and actual values of parameters for different vehicles. The diverse features and the functionalities of the vehicles are also accounted using the Bayesian aggregate model based on the trust and credibility. The self-healing capability of Artificial Immune Systems (AIS) allows them to identify and isolate malicious nodes within a network. The self-healing effect of AIS is performed by checking the similarity and credibility of the new vehicles with the predicted values. On checking, the isolation is enforced resolving the cluster quality.

Phase 2 focuses on the strengthening of the network traffic with encryption and mapping through the Triple Random Hyperbolic Encryption (TRHE) with Hex-Tuple Matched Mapping. In this contribution 5, Deep Auto Sparse Impasse NN is added to detect the twelve types of DDoS attacks. The proposed approach was evaluated by comparing its performance to that of existing methods, namely Trilateral Trust, H-IDS, Multi Filter, and SPPA.

The final Phase 3 includes the immunization of clusters and routing using the contribution 6. The security and reliability is provided by the Deep Trust Factorization Neural Network (DT-NN) based on trust scores. The Moth Flame optimization (MFO) algorithm detects the best path in the network by updating each vehicle position. Efficient routing of packets around congestion and malicious nodes is enabled by considering multiple paths simultaneously to avoid congested or unreliable links. The Cache parallelized Circulation Link routing (CCL) through time and frequency synchronization base channel hopping achieves improved throughput, reduced latency, and enhanced security.

Findings:

The proposed hybrid approach consists of three steps. The subsequent section presents a detailed performance analysis of the optimized feature selection approach, specifically the Glow Worm Swarm optimized Single Layer Feed forward Networks, implemented in phase 1. The performance analysis of the proposed techniques in phase 2 and phase 3 are continued. The overall performance of the proposed hybrid approach is evaluated using a set of relevant metrics and then compared to the performance of conventional approaches.

The performance of the proposed hybrid approach has been analyzed in terms of packet loss, throughput and detection rate. The packet loss of the proposed Self-healing AIS with Entropy-based SVM is reduced by managing the mobility nodes using Response Feedback Algorithm and stable automatic optimized cache routing by using triple random hyperbolic encryption that performs random encoding three times and maps all the same IP addresses in a symmetrically matching hex-tuple value. The higher values of 0.9499 and 0.9854 are attained by the hybrid approach.

The proposed hybrid approach significantly enhances accuracy by incorporating a novel Response Feedback Method. By effectively combining linear regression and micro-cluster outlier detection, this method enables the identification and tracking of anomalous network behavior based on temporal data, facilitating rapid attack detection and mitigation.

Furthermore, the system leverages kernel density estimation to continuously monitor crucial parameters within the RSU cluster communication, such as vehicle density, energy consumption, average delay, packet delivery ratio, and detection rate. By analyzing these parameters, the system accurately assesses the trustworthiness of each node.

To further enhance performance, the system integrates an entropy-based Support Vector Machine classifier. This classifier effectively categorizes nodes as malicious or benign with trust values, significantly improving the system's detection rate.

Finally, the introduction of a Stable Automatic Optimized Cache Routing technique significantly improves the system's precision. Notably, the proposed system demonstrates significantly lower latency compared to existing approaches. While AODV exhibits a latency of 33 seconds, the trust-based framework experiences a latency of 57 seconds, and Firecol records a latency of 90 seconds. This demonstrates a significant performance improvement in terms of latency reduction.

From the experimental results and based on the comparison made with the existing approaches, the Proposed - A Hybrid Approach for Securing the Vehicular Ad-hoc Networks by Mitigating Denial of Service Attack and types with Self-Healing and Immunization provided

a. Transactions of the packet ratio secured and increased.

b. Energy consumption reduced by isolating the malicious nodes.

c. Detection rate increased based on the trustworthiness values of the vehicle nodes.

d. Throughput considered higher reflecting the high transmission rate.

e. The delay decreasing to 0.12 seconds and packet loss for each node decreasing to 0.5 bits.

f. The system accurately detected twelve variants of DDoS attacks with 99% accuracy and exhibited a remarkably fast detection time of less than 0.1 milliseconds.

g. Accuracy, Recall and F1 Score of the proposed model in detecting DoS and DDoS attacks found higher with

i. smurf attack with 99% accuracy, 97.65% Recall and 96.3% F1 Score

ii. ping flood attack with 97.6%, 97.50%, and 96.4%

iii. NTP amplification with 97.4%, 98.6% and 96.5%

iv. SNMP reflection with 97.3%, 98.25% and 97.1%

v. SNMP with 97.35%, 98.2% and 97.2%

vi. DNS flood with 97.1%, 97.48%, and 95.1%

vii. HTTP flood with 96.4%, 97.48%, and 95.1%

viii. SYN flood with 96.4%, 98.15% and 96.1%

ix. UDP flood with 96.2%, 97.24% and 95.1%

x. LDAP with 97.5%, 97.15% and 96.85%

xi. MSSQL with 97.5%, 97.3% and 97.1%

xii. NetBIOS with 98.2%, 98.45% and 97.1%

xiii. SSDP with 98.4%, 98.15% and 97.4%

xiv.WebDDoS with 97.7%, 98.15% and 97.6%

xv. TFTP with 97.45%, 98.15% and 98.15%

The proposed hybrid approach detects the twelve variant DDoS attacks with accuracy of 99% and less detection time of 0.1ms, thereby outperforming all existing techniques.

Overall, the proposed system's performance and its potential significantly improved VANET security and reliability.

Examiners

Internal Examiner :

Dr. Digvijaysinh Mahendrasinh Rathod
Professor & Head, CoE Cyber Security,
School of Cyber Security and Digital Forensics,
National Forensic Sciences University
[An Institution of National Importance]
Ministry of Home Affairs, Government of India
Sector-9, Gandhinagar, Gujarat 382007.

External Examiner :

Dr Raja Kumar Murugesan
Associate Professor
Head of Research
School of Computer Science
Faculty of Innovation & Technology
Taylor’s University
Selangor
Malaysia