# CONTENTS


| Chapter No. | Title | | Page No. |
|---|---|---|---|
| | **ABSTRACT** | | |
| 1 | **INTRODUCTION** | | 1 |
| | 1.1 | Intelligent Transportation System and Vehicular Ad-Hoc Networks | 1 |
| | 1.2 | Security in VANET | 4 |
| | 1.3 | Security Challenges in VANET | 5 |
| | 1.4 | Attacks in VANET | 8 |
| | 1.5 | Classification of Attacks and Security Requirements | 8 |
| | 1.6 | Classification of Attacks on Layers | 9 |
| | 1.7 | Statistical Survey on DDoS Attacks in VANET | 13 |
| | 1.8 | DoS and DDoS attacks in VANET | 14 |
| | | 1.8.1 DoS attacks | 14 |
| | | 1.8.2 DDoS attacks | 15 |
| | 1.9 | Defense Landscape for VANETs | 17 |
| | | 1.9.1 Cryptography-based Solutions | 17 |
| | | 1.9.2 Encryption and Decryption Techniques | 18 |
| | | 1.9.3 Intrusion Detection System based Solutions | 19 |
| | | 1.9.4 Swarm intelligence-based techniques | 19 |
| | | 1.9.5 Artificial Intelligence-based Techniques | 20 |
| | | 1.9.6 Artificial Immune System | 20 |
| | 1.10 | Limitations of Existing Defense Landscape for VANET | 23 |
| | 1.11 | Motivation and Justification | 25 |
| | 1.12 | Problem Statement | 26 |
| | 1.13 | Research Questions | 26 |
| | 1.14 | Objective of the Thesis | 26 |

| Chapter No. | Title | | Page No. |
|---|---|---|---|
| | 1.15 | Significant Contributions of the Thesis | 27 |
| | 1.16 | Organization of the Thesis | 30 |
| | 1.17 | Conclusion | 32 |
| | 1.18 | Chapter Summary | 32 |
| **2** | **REVIEW OF LITERATURE** | | 34 |
| | 2.1 | Introduction | 34 |
| | 2.2 | Manifestation of DoS Attacks in VANETs | 34 |
| | 2.3 | Review on VANET Performance and Security Attacks | 36 |
| | 2.4 | Review on Security Solutions handling DoS attacks and its types in VANET | 44 |
| | | 2.4.1 Review on Cryptography-based Techniques in VANET | 44 |
| | | 2.4.2 Review on ML-based IDS in VANET | 54 |
| | | 2.4.3 Review on AIS in Securing VANETs | 61 |
| | 2.5 | Conclusion | 65 |
| | 2.6 | Chapter Summary | 66 |
| 3 | **PROPOSED METHODOLOGY** | | 67 |
| | 3.1 | Introduction | 67 |
| | 3.2 | Phases in the Proposed Methodology | 69 |
| | 3.3 | Phase 1: Enhanced Feature Selection and Mitigation | 76 |
| | | 3.3.1 Introduction | 78 |
| | | 3.3.2 Contribution 1: Optimized Feature Selection for Malicious Nodes Detection and Classification of DoS Attacks using Glow-worm (GLW) Single Layer Feed Forward Neural Network (SLFN) | 79 |
| | | 3.3.2.1 (a) Glow-worm Attraction Factor Update Stage | 82 |
| | | 3.3.2.2 (b) Glow-worm Movement Stage | 83 |

| Chapter No. | Title | | Page No. |
|---|---|---|---|
| 3 | | 3.3.2.3 (c) Glowworm Neighborhood Stage | 85 |
| | | 3.3.2.4 (d) Single Layer Feed Forward Network (SLFN) Classifier | 87 |
| | | 3.3.3 Contribution 1 Merits | 91 |
| | | 3.3.4 Contribution 1 Limitations | 91 |
| | | 3.3.5 Contribution 2: Abnormal Behaviour Detection using Response Feedback Algorithm with Micro Cluster Outlier Detection Algorithm using Linear Regression (MCOD-LR) | 91 |
| | | 3.3.6 Contribution 3: Novel Adaptive Nodal Detection Algorithm for the Prediction of Malicious DoS Attacks using Kernel Density Estimation and Entropy-based Support Vector Machine (SVM) Classifier | 97 |
| | | 3.3.6.1 Introduction | 97 |
| | | 3.3.6.2 Kernel Density Estimation with Entropy based SVM | 97 |
| | | 3.3.7 Contribution 4: Isolation using Reliance Node Estimation Approach using Pearson correlation coefficient and Bayesian aggregate model with Self-healing effect of Artificial Immune System (AIS) | 103 |
| | | 3.3.7.1 Introduction | 103 |
| | | 3.3.7.2 Pearson correlation coefficient Method | 103 |
| | | 3.3.7.3 Bayesian Aggregate Model with the Self-healing Effect | 106 |
| | | 3.3.8 Phase 1 MeritsP | 109 |

| Chapter No. | Title | | Page No. |
|---|---|---|---|
| | | 3.3.9 Phase 1 Limitations | 109 |
| | | 3.3.10 Phase 1 Summary | 109 |
| | 3.4 | Phase 2: Strengthening the Access Control and Mapping | 110 |
| | | 3.4.1 Introduction | 110 |
| | | 3.4.2 Contribution 5: Strengthening the Access Control and Detecting DDoS Attacks using Triple Random Hyperbolic Encryption (TRHE) with Hex-Tuple Matched Mapping | 112 |
| | | 3.4.3 Deep Auto Spare Impasse NN | 115 |
| | | 3.4.4 Phase 2 Merits | 118 |
| | | 3.4.5 Phase 2 Limitations | 118 |
| | | 3.4.6 Phase 2 Summary | 118 |
| | 3.5 | Phase 3: Immunization of Clusters and Routing | 119 |
| | | 3.5.1 Introduction | 119 |
| | | 3.5.2 Contribution 6: Deep Trust Factorization Neural Network with Trust Score | 120 |
| | | 3.5.3 Moth Flame Optimization with Cache Parallelized Circulation Link Routing | 122 |
| | | 3.5.4 Phase 3 Summary | 127 |
| | 3.6 | Chapter Summary | 127 |
| 4 | **RESULTS and DISCUSSIONS** | | 129 |
| | 4.1 | Experimental Setup and Results | 129 |
| | | 4.1.1 Dataset and Simulation | 130 |
| | 4.2 | Evaluation Metrics | 137 |
| | 4.3 | Performance analysis | 141 |
| | | 4.3.1 Phase 1: Enhanced Feature Selection and Mitigation | 143 |

| Chapter No. | Title | | Page No. |
|---|---|---|---|
| | | 4.3.2 Phase 2: Strengthening the Access Control and Mapping and Phase 3 – Immunization of Clusters and Routing Contributions 5 and 6 | 158 |
| | 4.4 | Performance Comparison of the Proposed Hybrid Approach | 162 |
| | 4.5 | Chapter Summary | 166 |
| 5 | | **CONCLUSION** | 167 |
| | | **FUTURE SCOPE** | 170 |
| · | | **BIBILIOGRAPHY** | 171 |
| | | **PUBLICATIONS** | |
| | | **PLAGIARISM REPORT** | |