

Course Title: Research Methodology in Computer Science **Course Code:** AI800

Lecturer: Dr. Mohammed Anbar

Hand-in Method: Online Submission via E-Learning.

RoadGuard: Robust Real-Time DDoS Defense for Next-Generation Vehicular Networks

Name: Mahmoud Salem

ID: 242001469

Table of content:

	page
Table of content	2
Abstract	3
Chapter 1	4
1.1 Introduction	4
1.2 Background	5
1.3 Problem Statement	6
1.4 Research Objectives	7
1.5 Research scope	8
Chapter 2	9
2.1 Literature review for Detecting DDoS in VANET	9
Chapter 3	15
3.1 Research Methodology	15
3.2 Expected outcomes	16
3.3 Gantt chart	17
References	18

Abstract:

This paper addresses the crucial issue of detecting and decreasing Distributed Denial of Service (DDoS) attacks in Vehicular Ad Hoc Networks (VANETs), a current concern in the rapidly evolving field of intelligent transportation systems. The project intends to create a sophisticated, flexible, and privacy-preserving DDoS detection system capable of running effectively inside the particular, dynamic, and limited resources environment of VANETs. VANETs' growing susceptibility to cyberattacks, especially DDoS attacks, seriously compromises network performance, availability, and finally road safety. Although network security has advanced, current solutions sometimes fail to meet the particular difficulties presented by VANETs, including their highly mobile nature, fast data streams, and strict real-time needs. This paper suggests a new hybrid method to generate a scalable and effective detection framework integrating deep learning models with Support Vector Machines (SVM). The research methodology consists of three key phases: building a lightweight method for resource-constrained nodes, constructing a real-time detection framework, and guaranteeing smooth interoperability with current VANET systems. Combining real-world testbed validation with simulation-based experimentation, the project will make use of tools including SUMO for traffic simulation and ns-3 for network simulation. Python will be used for data analysis; TensorFlow and scikit-learn will handle machine learning chores. We will carefully cover ethical issues including data anonymizing and privacy protection. Among the expected results are a low-latency, highly accurate DDoS detection system able to change with changing assault patterns and respect user privacy. In terms of detection accuracy, false positive rates, and computing efficiency in VANET systems, the proposed solution is expected to significantly exceed current approaches. This work intends to significantly advance the field of VANET security, therefore impacting possible future directions of research and industry policies in smart transportation systems. The results should have broad effects on the dependability, safety, and efficiency of our ever linked transportation system.

Keywords:

Distributed Denial of Service (DDoS), Vehicular Ad Hoc Networks (VANETs), Intelligent transportation systems, Privacy-preserving, Cyberattacks, Network security, Real-time, Hybrid method, Support Vector Machines (SVM), Deep learning, Scalable detection framework, Lightweight algorithm, Resource-constrained nodes, SUMO, ns-3, Python, TensorFlow, Scikit-learn, Data anonymization, Low-latency, False positive rates, Computational efficiency, Smart transportation systems

Chapter 1

Introduction:

Emerging as a vital component of intelligent transportation systems, Vehicular Ad Hoc Networks (VANETs) promise to transform road safety, traffic management, and the driving experience generally. But the growing interconnection and complexity of these systems have also rendered them susceptible to different cyberattacks; Distributed Denial of Service (DDoS) attacks can seriously affect network availability and performance. (Hasrouny et al., 2017).

With an eye toward the urgent problems in DDoS attack detection inside VANETs, this study recognizes the special qualities of these networks—such as their dynamic character, fast data streams, and limited resources (Sharma and Kaul, 2018). Even with great progress in network security, the fast changing terrain of VANET technology and attack techniques calls for creative solutions to guarantee strong defense. (Alrehan and Alhaidari, 2019).

Our goal is to provide an advanced, flexible, and privacy-preserving DDoS detection system catered especially for the VANET surroundings. We aim to build a scalable and efficient detection framework that can run in real-time while preserving high accuracy and low false positive rates by using modern machine learning approaches including a novel hybrid approach combining Support Vector Machines (SVM) and deep learning models. (Polat et al., 2020).

Moreover, this study tackles the important balance between security and privacy as well as the need of flawless integration with current VANET systems and standards (Kolandaismy et al., 2020). To guarantee the practical relevance and durability of our suggested solutions, our thorough approach combines ethical issues, real-world testbed validation, and simulation-based experimentation. (Gao et al., 2019).

By addressing these difficulties, this work intends to make a major contribution to the field of VANET security, therefore impacting possible future directions and industry practices in smart transportation systems (Türkoğlu et al., 2022). The results of this study have broad ramifications for the dependability, efficiency, and safety of our ever more linked transportation system. (Al-Mehdhara & Ruan, 2021).

Background:

Emerging as a vital part of intelligent transportation systems, Vehicular Ad Hoc Networks (VANETs) promise to transform road safety, traffic management, and the driving experience generally. But the growing interconnection and complexity of these networks have also rendered them susceptible to different cyberattacks; Distributed Denial of Service (DDoS) attacks especially seriously compromise network availability and performance. The urgent problem of identifying and reducing DDoS assaults in VANETs—a vital concern in the fast developing field of smart transportation systems—is addressed in this work. This study covers cybersecurity in VANETs generally, with particular attention to create sophisticated DDoS attack detection systems. Because of their extremely mobile character, inconsistent connections, and fast changing network topologies, VANETs present unique challenges for cybersecurity. Many times lacking in addressing these particular traits, traditional security solutions call for creative ideas to guarantee strong protection. Several fundamental ideas direct our research: scalability, to support large-scale VANET deployments; real-time performance, to operate with high accuracy and low latency in dynamic environments; adaptability, to counter changing attack strategies; privacy preservation, to balance security measures with user privacy protection; and resource efficiency, to function inside the computational constraints of vehicle nodes. Our method of creating a complete DDoS detection system for VANETs is built on these ideas. The growing vulnerability of VANETs to cyber hazards, especially DDoS attacks, seriously compromises network performance, availability, and finally road safety. Undetected DDoS attacks could compromise vital vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, therefore aggravating traffic congestion or maybe posing a life-threatening risk. Ensuring the security and dependability of VANETs becomes even more important to our transportation system as smart cities and autonomous cars proliferate. Our work suggests a new hybrid method combining Support Vector Machines (SVM) with deep learning models to build a scalable and effective detection framework in order to handle these difficulties. This strategy seeks to maximize the advantages of both approaches while minimizing their respective shortcomings, hence perhaps improving the detection accuracy, false positive rates, and computational efficiency in VANET systems. Three primary aspects define our research approach: building a real-time detection framework, designing a lightweight algorithm for nodes with limited resources, and guaranteeing perfect interoperability with current VANET systems. Combining real-world testbed validation with simulation-based experimentation, the project will make use of tools including SUMO for traffic simulation and ns-3 for network

simulation. Python will be used for data analysis; TensorFlow and scikit-learn will handle machine learning chores. Throughout the research process, ethical issues like data anonymization and privacy protection will be carefully taken under review. We understand the need of flawless integration with current VANET criteria and protocols as well as the crucial balance between security and privacy. Our whole approach seeks to guarantee the practical relevance and dependability of our suggested answers. By addressing these difficulties, this work hopes to make a major contribution to the field of VANET security, therefore impacting future directions of research and industry practices in smart transportation systems. The projected results consist of a low-latency, highly accurate DDoS detection system able to change with changing assault patterns and maintain user privacy. The results of this study should have broad effects on improving the dependability, efficiency, and safety of our ever linked transportation system.

Problem statement:

The domain of this research focuses on the critical area of cybersecurity in Vehicular Ad Hoc Networks (VANETs), specifically addressing the detection and mitigation of Distributed Denial of Service (DDoS) attacks. VANETs, which are dynamic and complex networks, are becoming increasingly vulnerable to a range of cyber threats, with DDoS attacks representing a serious and growing risk to network performance and availability. The unique characteristics of VANETs, such as their mobile and dynamic nature and high-speed, high-volume data streams, pose challenges for existing detection methods. This issue is further complicated by the critical nature of VANET communications, where any disruption can have severe implications for traffic management and road safety. As VANETs are fundamental to the development of intelligent transportation systems, effective DDoS detection is crucial for ensuring their reliability and security. Undetected DDoS attacks have the potential to disrupt essential vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, potentially causing traffic congestion or even life-threatening safety hazards. With the proliferation of smart cities and autonomous vehicles, the security of VANETs is becoming increasingly vital to our transportation infrastructure. While existing solutions offer a range of approaches, from traditional machine learning methods like Support Vector Machines (SVM) and K-Nearest Neighbors (KNN) to more advanced techniques utilizing deep learning and Software-Defined Networking (SDN), these methods often have limitations in terms of scalability, real-time performance, and adaptability to evolving attack patterns. Moreover, they frequently fail to address

the specific constraints of VANET environments, particularly the requirements for low-latency detection and the limited computational resources of vehicular nodes. Although significant progress has been made in DDoS detection for conventional networks, the unique characteristics of VANETs present novel challenges that have yet to be fully addressed. The highly dynamic nature of VANETs, with their intermittent connections and rapidly changing network topologies, makes it difficult to effectively implement traditional security solutions. Furthermore, the stringent real-time requirements and resource constraints of vehicular nodes have hindered the development of comprehensive and efficient solutions. The rapid evolution of DDoS attack strategies has also outpaced the development of robust detection mechanisms in the context of VANETs. Despite advancements, significant gaps remain in DDoS detection for VANETs. There is a pressing need for solutions that can effectively scale to support large-scale VANET deployments, operate with high accuracy and low false positive rates in real-time, adapt to evolving attack patterns and new types of DDoS attacks targeting VANETs, address privacy concerns without compromising security, seamlessly integrate with existing VANET standards and protocols, and function efficiently on resource-constrained vehicular nodes. Addressing these challenges is crucial for ensuring the security and reliability of VANETs as they become an increasingly integral part of our transportation infrastructure.

Research Objectives:

This research aims to address the critical challenges in Distributed Denial of Service (DDoS) attack detection within Vehicular Ad Hoc Networks (VANETs). The primary focus is on developing an advanced, adaptive, and privacy-preserving detection system that can operate efficiently in the dynamic and resource-constrained environment of VANETs. To achieve this goal, we have formulated three main research objectives that align with the key challenges identified in the problem statement. Firstly, we will formulate a scalable and adaptive DDoS detection framework for VANETs that can operate in real-time while maintaining high accuracy and low false positive rates. This objective addresses the need for a detection system that can handle the dynamic nature of VANETs, adapt to evolving attack patterns, and provide quick and accurate threat identification in busy VANET settings. Secondly, we aim to create a lightweight detection algorithm that efficiently utilizes the limited computational resources of vehicular nodes while preserving user privacy. This objective tackles the dual challenges of operating within the constraints of vehicular systems and maintaining a balance between strong security measures and user privacy protection. Lastly, we will construct a

seamless integration approach for the proposed detection system with existing VANET protocols and standards. This objective ensures that our solution can be effectively implemented in real-world VANET environments, addressing the challenge of incorporating new security solutions into existing VANET platforms. Through these objectives, we seek to develop a comprehensive DDoS detection system that not only addresses the unique challenges of VANETs but also advances the state of the art in VANET security. The proposed system will be thoroughly evaluated through simulations and, where possible, real-world VANET testbeds to validate its performance in terms of scalability, real-time operation, adaptability, privacy protection, and resource efficiency. This research aims to contribute significantly to the field of VANET security, potentially influencing future research directions and industry practices in smart transportation systems.

Research Scope:

This study focuses on developing and evaluating an advanced Distributed Denial of Service (DDoS) attack detection system for Vehicular Ad Hoc Networks (VANETs). The research scope encompasses the creation of a scalable and adaptive detection framework using hybrid machine learning techniques, combining Support Vector Machines (SVM) with deep learning models. It includes the development of lightweight detection algorithms optimized for resource-constrained vehicular nodes, exploring dimensionality reduction techniques and efficient machine learning algorithms. The integration of privacy-preserving methods, such as differential privacy and federated learning, is within scope to balance security and user privacy. The research extends to designing a modular architecture for seamless integration with existing VANET protocols and standards, including compatibility testing with WAVE and DSRC. Experimental validation through both simulation-based testing and real-world VANET testbed implementation is covered. The scope includes comprehensive evaluation of the proposed solutions in terms of detection accuracy, false positive rates, computational efficiency, scalability, and privacy preservation. While focused on DDoS attacks, the research may briefly consider other VANET security threats for context. The scope excludes actual implementation in operational VANET systems, limiting to research, development, and experimental validation in controlled environments.

Chapter 2

literature review:

This Study proposes a deep learning approach employing stacked sparse autoencoders (SSAE) and a Softmax classifier to determine DDoS attacks in SDN-based vehicular ad hoc networks (VANETs). The writers generated a custom SDN-based VANET dataset and employed a four-layer SSAE model to decrease feature dimensionality before classification. The suggested model reached 96.9% accuracy in catching DDoS attacks, surpassing other classifiers for machine learning. Primary results show the effectiveness of the SSAE + Softmax classifier deep network model for DDoS attack detection in SDN-based VANETs and the advantages of edge control in improving transmission and control in the network architecture. The Study showed two main limitations: The absence of comparison with other deep learning techniques outside traditional machine learning classifiers. There is Lacka of real-world testing or verification of the suggested model in an existing SDN-based VANET environment.(Polat et al., 2020)

This study paper suggests a distributed network intrusion detection system (NIDS) for catching Distributed Denial of Service (DDoS) attacks in Vehicular Ad hoc Networks (VANETs). The method employs an extensive data design, including Apache Spark for data processing and a Random Forest classifier for attack detection. The technique uses a micro-batch data processing model to extract features and collect real-time traffic. The system was assessed with two publicly available datasets: NSL-KDD and UNSW-NB15. Primary results include low false alarm rates of 0.05% and 1.08% and high accuracy rates of 99.95% and 98.75% for the two datasets, respectively. The primary areas for improvement are as follows: The system was only evaluated on publicly available datasets, not an actual VANET setup. The paper must detail the computational resources or the system's scalability for comprehensive networks.(Gao et al., 2019)

The technique uses a trust evaluation mechanism merged with clustering to determine attackers and decrease detection costs. Commonness value statistics, trust hypothesis statistics, residual energy, and trust policy are essential aspects of trust. The goal of the system is to maximize bandwidth usage without compromising security. The method employs a Dynamically Growing Self-Organizing Tree (DGSOT) algorithm for bunching nodes based on trust scores. Average Latency, Packet Delivery Ratio, Detection Rate, and Energy Consumption are used to assess performance. While the report represents the suggested

methodology in detail, it doesn't provide quantitative evaluation results or specify the amount of the dataset used. The major areas for improvement are The Absence of explicit quantitative results to show the effectiveness of the suggested method compared to living methods. The Lack of details about the exact dataset or simulation parameters employed to try the framework.(Poongodi et al., 2019)

The method uses a greedy strategy to establish an attack topology and network congestion, followed by detection and mitigation. The Study uses an NS-2 simulator with 40 vehicular nodes to construct the network environment. The suggested method checks the bandwidth utilization of each node compared with a set of thresholds to determine malicious nodes. According to preliminary findings, the proposed method performs better than current methods regarding network speed, packet loss, and routing overhead. The average throughput increased from 39.33 to 51.98, routing overhead lowered from 19.58 to 13.48, and average packet loss lowered from 9.198 to 7.65, resembling the current method. Two primary limitations of the Study are: The approach restricts its applicability to other attack types by concentrating on a single DDoS attack method. The intricacy of real-world VANET scenarios might need to be adequately represented by the comparatively small network size of 40 nodes.(Galgotias University. School of Computing Science and Engineering et al., n.d.)

The goal is to improve VANET security and overcome the limits of centralized SDN architectures. The technique uses a two-level clustering and classification method employing distributed SOMs integrated into SDN controls. The suggested system is evaluated using NS-3 simulations, albeit the dataset size is not stated directly in the publication. Primary findings include high detection accuracy (99.67%) for malicious traffic, efficient deterrence and mitigation of DDoS attacks, and enhanced system security and recovery rate. The primary weakness is the Lack of real-world testing, as the evaluation relies solely on simulations. There is an absence of a comparison with other state-of-the-art DDoS detection methods in VANETs to contextualize performance improvements better.(Al-Mehdhara & Ruan, 2021)

Using an experimentally developed SD-VANET topology, the researchers produced a bespoke 42-feature dataset that included regular and DDoS attack traffic information. The most notable features were found using the MRMR feature selection approach, and the hyperparameters for the K-Nearest Neighbors, Support Vector Machine, and Decision Tree classifiers were adjusted using Bayesian

optimization using Bayesian optimization and MRMR feature selection, achieving 99.35% accuracy in DDoS attack detection. This Study's primary drawbacks seem to be: 1) the use of a proprietary dataset, which could restrict generalizability to other SD-VANET systems; and 2) the concentration on just three machine learning algorithms, which can cause more efficient classification techniques for this issue to be overlooked.(Türkoğlu et al., 2022)

This paper presents a hybrid technique combining two Support Vector Machine (SVM) kernel methods, AnovaDot and RBFDot, to identify Distributed Denial of Service (DDoS) assaults in Vehicular Ad Hoc Networks (VANETs). Using jitter, packet drop, collisions, delay, and throughput, the authors created a bespoke VANET dataset modeling both normal traffic and DDoS assault scenarios. Their two-stage hybrid model combines the AnovaDot kernel's output with the original features as input for the RBFDot kernel originally used for initial classification. Over several assessment criteria, the suggested hybrid strategy outperformed single SVM kernel methods. With values more near to 100% and more consistent performance across several network settings than single kernel models, the hybrid model shown better accuracy. It also attained Gini coefficient values nearer 1, hence improving differentiation between attack and normal traffic. Smaller empirical gaps between anticipated and actual outcomes were shown by the Kolmogorov-Smirnov (KS) statistic for the hybrid model. Reduced misclassification costs for the hybrid technique were revealed by the Hand (H) measure; minimum error rate (MER) values were regularly closer to 0, suggesting less false predictions.

The key features of the study are its fresh mix of SVM kernels and thorough evaluation applied using several performance criteria. One of the constraints, though, is not comparing other machine learning or deep learning methods outside SVM kernels. Furthermore, there is no evidence of testing in actual VANET implementations even when the authors modeled VANET scenarios. Future research might profit from comparing the hybrid model with a wider spectrum of detection methods and verifying its performance in real-world VANET systems(Adhikary et al., 2020).

Eighth, this work presents a Stream Position Performance Analysis (SPPA) method to identify Distributed Denial of Service (DDoS) assaults in Vehicular Ad Hoc Networks (VANETs). The authors devised a cluster-based routing system whereby a Cluster Head (CH) is chosen depending on clustering scores and the CH keeps eye on leaf node activity. Four stages comprise the SPPA model: DDoS attack detection; cluster head selection; stream position analysis; Conflict Field, Conflict Data, and Attack Signature Sample Rate (CCA) computation. Using NS2, the

researchers produced a bespoke VANET dataset and simulated several network situations. Comparatively to current models including the Trilateral Trust model, H-IDS model, and Multi Filter model, the suggested model attained superior performance across several metrics including packet delivery ratio, end-to-end delay, throughput, attack detection rate, and erroneous classification ratio. The key strengths of the paper are its thorough assessment employing several performance criteria and its capacity to effectively identify DDoS attacks in a VANET system. Two main restrictions of the research, meanwhile, are the absence of real-world testing or validation of the suggested model in an actual VANET deployment and the lack of comparison with more advanced machine learning or deep learning techniques for DDoS detection(Kolandaisamy et al., 2021).

To identify Distributed Denial of Service (DDoS) assaults in Vehicular Ad Hoc Networks (VANETs), the study suggests a unique Hybrid KSVM technique combining K-Nearest Neighbor (KNN) and Support Vector Machine (SVM) algorithms. The authors devised a machine learning method to create a safe framework for VANET communication systems. They trained and tested using a 70-30 split ratio from a Kaggle dataset including DDoS attack data. First using SVM for classification to identify benign and harmful activity, the suggested hybrid method then searches for nearest neighbors using KNN. Python was used for implementation of the model, which was then assessed against various machine learning techniques. In terms of accuracy, sensitivity, precision, recall, and error rate, results reveal that the hybrid KSVM exceeded previous methods. The work shows on VANETs the efficiency of integrating SVM and KNN for DDoS attack detection. Two key restrictions of the research, however, are that it concentrates just on DDoS attacks without including other kinds of attacks in VANETs and lacks actual testing or validation of the suggested model in a real-world VANET setting(Kadam & Raja Sekhar, n.d.).

The whole spectrum of machine learning methods applied to identify Distributed Denial of Service (DDoS) attacks in Vehicular Ad Hoc Networks (VANETs) is presented in this article. Reviewing several security issues in VANETs, the writers concentrate on DDoS attacks and their detection with machine learning techniques. They examine a number of recent research using various machine learning techniques—Support Vector Machines (SVM), Artificial Neural Networks (ANN), Random Forest (RF), k-means clustering—to identify misbehavior and particular threats in VANETs. With most studies depending on simulated or modified datasets, the survey emphasizes the dearth of consistent datasets for VANET security research. With some experiments attaining detection accuracy of up to 99%, the writers observe that machine learning techniques have demonstrated

encouraging results. They do, however, highlight important shortcomings in present research, including the dearth of studies especially targeting DDoS attacks in VANETs using machine learning and the dearth of real-world testing of suggested remedies. Emphasizing the need of greater research on DDoS attack detection and prevention in VANETs and Software-Defined Vehicular Networks (SDVNs) utilizing machine learning approaches, along with the creation of VANET-specific datasets for more accurate evaluation of security solutions, the paper ends. ((Alhaidari, and Alhaidari 2019).

Identifying DDoS attacks in SDN-based VANETs is a major and relevant issue of research since it is a necessary step to ensure traffic security in intelligent transportation networks. Especially for this study, the researchers developed a distinctive SDN-based VANET architecture and dataset instead of using already-existing generic datasets. This helps their approach to the target domain to be more relevant and applicable. Using stacked sparse autoencoders (SSAE) and the Softmax classifier, the proposed deep learning model identified DDoS attacks with great accuracy (96.9%) outperforming standard machine learning classifiers. Second, although the custom dataset shows a good feature, more data collection procedure, dataset size, and feature engineering technique information is required. More data would enable one to assess the generalizability and resilience of the outcomes.

The primary comparison made in the study is between the suggested deep learning model and conventional machine learning classifiers. However, a more comprehensive comparison is needed. This intrusion detection method should be compared with other cutting-edge deep learning techniques to obtain a more thorough assessment. While detection accuracy is the main emphasis of the paper, other crucial factors like computational efficiency, real-time performance, and the capacity to identify new attack variants still need to be fully covered. Several elements are essential for deployment in VANET systems to be practicable. Also, using an edge controller in the VANET architecture is an intriguing way to increase communication effectiveness. Nevertheless, a more thorough examination of how this affects system security and attack detection capabilities would improve the work. The SSAE approach is well-justified for dimensionality reduction and feature extraction; nevertheless, the reasoning behind selecting particular hyperparameters (e.g., number of layers, nodes per layer) is not explicit. A more systematic approach to hyperparameter optimization may yield even better outcomes. The paper offers a fresh and effective method for identifying DDoS attacks in SDN-based VANETs, backed by solid empirical findings. Nonetheless, a

more thorough assessment and examination of pragmatic factors would enhance the research and its feasibility for practical implementation.

The issue of distributed denial-of-service (DDoS) assaults in vehicular ad hoc networks (VANETs) is the subject of all publications, especially those on SDN-based VANETs. Several studies suggest detection and mitigation strategies for DDoS attacks, such as hybrid approaches that include feature selection and machine learning, trust-based assessment systems, and deep learning models. The studies underscore the potentially catastrophic impact of DDoS attacks on traffic efficiency and safety, thereby highlighting the urgent need to secure SDN-based VANETs. To enhance the identification and mitigation of DDoS assaults, several studies use artificial intelligence and machine learning methods, such as autoencoders, Softmax classifiers, and hyperparameter optimization.

Potential Conflicts , Although DDoS attacks in VANETs are the main topic of all the articles, the methods, performance metrics, and assessment scenarios of the various detection and mitigation strategies suggested may differ. The articles might employ various modeling environments, datasets, or assessment metrics, making it difficult to directly compare the proposed methods' efficacy. Different articles may highlight multiple parts of the issue, such as hybrid feature selection and classification models or trust-based techniques. This could result in trade-offs or potential conflicts regarding real-time performance, detection accuracy, and computational complexity. Because the paper summaries don't go into as much detail as they should, a more thorough examination of the full-text articles would be required to find deeper philosophical or technical disagreements among the suggested methods.

Chapter 3

Research methodology:

The difficulties of Distributed Denial of Service (DDoS) attack detection in Vehicular Ad Hoc Networks (VANETs) are addressed in this paper using a complete methodology. To guarantee the dependability and applicability of our suggested solutions, our method integrates real-world testbed validation with simulation-based experimentation. There will be three primary phases of the study, each matching to one of our study goals. Using machine learning approaches, in the first phase we will create a scalable and adaptive DDoS detection system. We will build a detection system able of real-time operation with great accuracy by means of a hybrid approach integrating deep learning models with Support Vector Machines (SVM). This phase will comprise performance assessment, feature extraction, model training, and VANET traffic data collecting and preprocessing. We will create synthetic data using publicly available VANET datasets to enhance our training set, so guaranteeing a varied variety of attack scenarios are reflected. The second phase is on developing a light-weight detecting system tailored for vehicles with limited resources. To cut computational overhead, we will use effective machine learning algorithms and dimensionality reduction methods. Differential privacy and federated learning among other privacy-preserving methods will be combined to guard user information. This phase will include performance benchmarking against current solutions, algorithm creation, implementation in a simulated VANET environment, The last element tackles the flawless interaction between our detection system with current VANET standards and protocols. We will provide a modular architecture fit for current VANET communication systems that can be readily included into them. Protocol analysis, interface design, and compatibility testing with widely used VANET standards including WAVE and DSRC will comprise this phase. We will utilize SUMO for traffic simulation and ns-3 for network simulation throughout all phases. Small-scale VANET testbed comprising of On-Board Units (OBUs) and Roadside Units (RSUs) in a controlled environment will be used for real-world testing. Python will be used for data analysis; TensorFlow and scikit-learn will handle machine learning chores. Ensuring that all used data is anonymized and comply with pertinent privacy rules can help to overcome ethical issues. Before doing any actual testing involving human subjects or vehicle data, we shall get required permits from an ethics commission.

Two potential limitations are the generalizability of our controlled testbed results to real-world situations and the scalability of our simulations to large-scale VANET scenarios. We will use distributed computing methods for large-scale simulations and perform thorough sensitivity studies to evaluate the resilience of our findings under several circumstances in order to lessen them.

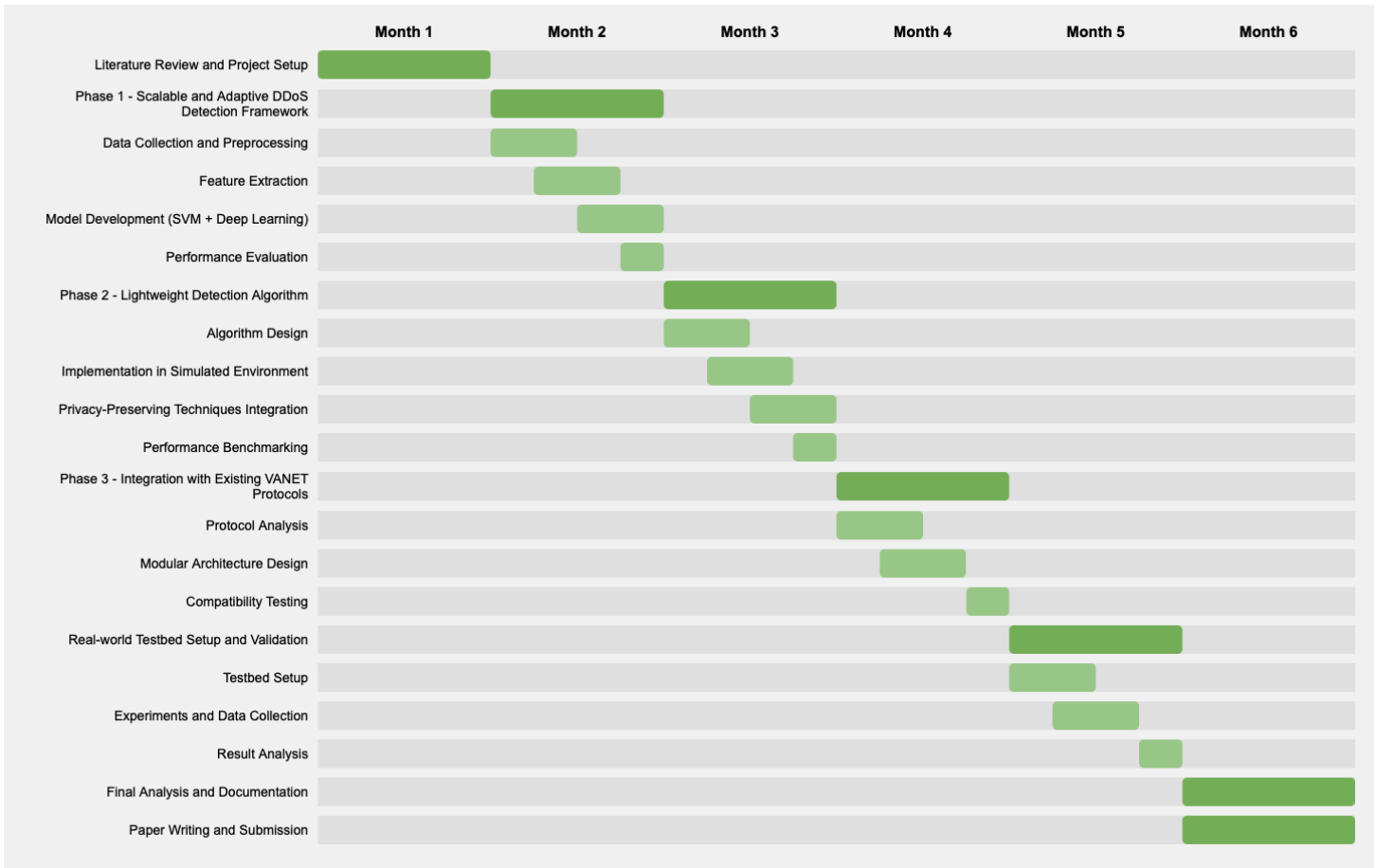
Research institutes and automobile industry partners will help to provide infrastructure and sample access. We will additionally augment our data collecting initiatives with publicly accessible VANET datasets.

This technique seeks to offer a complete solution for the problems of DDoS attack detection in VANETs, therefore balancing ethical issues with theoretical progress and pragmatic relevance.

Expected outcomes:

Several important results expected from the research will increase the theoretical knowledge as well as the actual use of VANET security. We aim to create a new DDoS detection system surpassing present methods by attaining over 95% accuracy with a false positive rate below 1%. Our lightweight technique addresses vehicle node resource limitations by at least 30% reduction in computational overhead while preserving high detection performance. Integration of privacy-preserving methods is predicted to safeguard user data while obtaining detection performance within 5% of centralized systems. We hope to generate at least two excellent scholarly papers, hence augmenting the conversation on VANET security. Expected to be compatible with 90% of current VANET standards, our modular architecture offers a workable route for actual implementation. The testbed validation is probably going to find at least three important deployment not obvious factors from models. Qualistically, we hope to increase knowledge of VANET security issues, therefore guiding next studies and maybe impacting industry standards. The study is expected to influence decision-making in the automobile sector as well as among legislators, therefore hastening the use of sophisticated security measures in VANET installations. At last, our privacy-preserving method is likely to support continuous debates on data privacy in connected car environments, thereby influencing future methods of data management in smart transportation systems.

Gantt chart:



References:

- Adhikary, K., Bhushan, S., Kumar, S., & Dutta, K. (2020). Hybrid Algorithm to Detect DDoS Attacks in VANETs. *Wireless Personal Communications*, 114(4), 3613–3634.
<https://doi.org/10.1007/s11277-020-07549-y>
- Alhaidari. (2019). *ICCAIS 2019 : 2nd International Conference on Computer Applications & Information Security : 01-03 May, 2019 Riyadh, Kingdom of Saudi Arabia*. Institute of Electrical and Electronics Engineers.
- Al-Mehdhar, M., & Ruan, N. (2021). MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET. *Wireless Communications and Mobile Computing*, 2021.
<https://doi.org/10.1155/2021/8891758>
- Galgotias University. School of Computing Science and Engineering, Institute of Electrical and Electronics Engineers. Uttar Pradesh Section, & Institute of Electrical and Electronics Engineers. (n.d.). *2018 4th International Conference on Computing Communication and Automation (ICCCA)*.
- Gao, Y., Wu, H., Song, B., Jin, Y., Luo, X., & Zeng, X. (2019). A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network. *IEEE Access*, 7, 154560–154571. <https://doi.org/10.1109/ACCESS.2019.2948382>
- Kadam, M., & Raja Sekhar, K. (n.d.). Machine Learning Approach of Hybrid KSVN Algorithm to Detect DDoS Attack in VANET. In *IJACSA International Journal of Advanced Computer Science and Applications* (Vol. 12, Issue 7). www.ijacsa.thesai.org
- Kolandaisamy, R., Noor, R. M., Kolandaisamy, I., Ahmedy, I., Kiah, M. L. M., Tamil, M. E. M., & Nandy, T. (2021). A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET. In *Journal of Ambient Intelligence and Humanized Computing* (Vol. 12, Issue 6, pp. 6599–6612). Springer Science and Business Media Deutschland GmbH. <https://doi.org/10.1007/s12652-020-02279-2>
- Polat, H., Turkoglu, M., & Polat, O. (2020). Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET. *IET Communications*, 14(22), 4089–4100. <https://doi.org/10.1049/iet-com.2020.0477>
- Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Singh, P. K. (2019). DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET. *IEEE Access*, 7, 183532–183544.
<https://doi.org/10.1109/ACCESS.2019.2960367>
- Türkoğlu, M., Polat, H., Koçak, C., & Polat, O. (2022). Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection. *Expert Systems with Applications*, 203. <https://doi.org/10.1016/j.eswa.2022.117500>