
Submission date: 28-Jul-2024 12:58AM (UTC+0800)

Submission ID: 2277289513

File name: Assigment_1_Msalelem.docx (58.89K)

Word count: 3008

Character count: 18519

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

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 29 Jun 2024

Hand-in Date: 20 July 2024

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

Name: Mahmoud Salem

Table of Content:

Number	Topic
1	literature review
2	Critical analysis
3	Conflict and connections
4	Synthesis Matrix for Literature Review
5	References

literature review:

First, For the paper "Deep network approach with stacked sparse autoencoders in the detection of DDoS attacks on SDN-based VANET."

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 Lack of real-world testing or verification of the suggested model in an existing SDN-based VANET environment.(Polat et al., 2020)

Second, for the research "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network"

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)

Third, DDoS Detection Mechanism Using a Trust-Based Evaluation System in VANET

The research proposes a trust-based framework to catch and prevent DDoS attacks in Vehicular Ad-hoc Networks (VANETs). 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)

Fourth, Improved Detection and Mitigation of DDoS Attacks in Vehicular ad hoc Network

The study paper suggests a new technique to detect and mitigate Distributed Denial of Service (DDoS) attacks in Vehicular Ad-hoc Networks (VANETs). 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.)

²³ Fifth, MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET

This Study suggests a Multilayer Distributed Self-Organizing Map (MSOM) system to protect against DDoS attacks in Vehicular Ad Hoc Networks (VANETs) employing Software-Defined Networking (SDN). 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-Mehdhar & Ruan, 2021)

Sixth, DDoS attack detection on SD-VANET using a mix of feature selection and hyperparameter tuning This work used feature selection, hyperparameter optimization, and machine learning techniques to detect DDoS attacks on SD-VANETs. 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. (Türkoglu et al., 2022)

Critical analysis:

First the Advantages, the research tackles a significant and topical matter: identifying DDoS assaults in SDN-based VANETs, an essential step in guaranteeing traffic security in intelligent transportation networks. Rather than using pre-existing generic datasets, the researchers created a unique SDN-based VANET architecture and dataset, especially for this investigation. This makes their approach to the target domain more applicable and relevant.

The suggested deep learning model outperformed conventional machine learning classifiers in identifying DDoS attacks with high accuracy (96.9%) by utilizing stacked sparse autoencoders (SSAE) and the Softmax classifier.

Second the Limitations, although the custom dataset presents a positive aspect, more information is needed regarding the data collecting process, dataset size, and feature engineering approach. More information would help evaluate the results' robustness and generalizability.

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.

Third Methodological points, 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.

In conclusion, 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.

Conflict and connections:

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.

Synthesis Matrix for Literature Review:

#	Paper Title	Year	Author	Methodology	Key findings	Limitation	Research Design
9				16			
1	Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET	2020	Polat, Huseyin Turkoglu, Muammer Polat, Onur	VANET SDN-based architecture created a sim on dataset with normal traffic and a DDoS attack. The best accuracy result of 96.9% was achieved using the SSAE + Softmax model consisting of four layers. The proposed model succeeded and outperformed other classifiers, as the primary evaluation	The SAFE and Softmax classifier has an accuracy rate of up to 96.9% in detecting DDoS attacks The model reduces the dimensions of features while maintaining classification accuracy outperforming classical methods.	Dataset size and Sample size: The exact size of the dataset is not mentioned . Challenges and limitations include the following, a single dataset, focus on DDoS attacks, and lack of a detailed research methodology.	Quantitative

				measure was classification accuracy			
2	5 A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network	2019	Gao, Ying Wu, Hongrui Song, Binjie Jin, Yaqia Luo, Xiongwen Zeng, Xing	The research used 14 public datasets: NSL-KDD and UNSW-NB15; Data preprocessing included removing duplicates, data type conversion, and normalization using MinMaxScale. The proposed system contains real-time traffic collection and detection modules, using Apache Spark and HDFS. The model used is micro-batch processing model . The classifier is Random Forest algorithm Performance as the following: for NSL-KDD: 99.95% accuracy, 0.05% FAR; for UNSW-NB15: 98.75% accuracy, 1.08% FAR.	The classifier which is Random Forest algorithm used for The turning point enhances data processing speed. The packet analyzer extracts attributes; MinMaxScale normalizes feature vectors to [0,1] range. AUC: 0.9999 on NSL-KDD, 0.9997 on UNSW-NB15.	Dataset size : The exact size of the dataset is not mentioned . Limitation in data set as the only datasets included in the study are NSL-KDD and UNSW-NB15, which might not reflect VANET traffic and DDoS attacks in the real world. The system is tested on benchmark datasets, not in real VANET environments, which may limited performance evaluation in the actual world.	Quantitative

3	DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET	2019	Poongodi, M. Hamdi, Mounir Sharma, Ashutosh Ma, Maode Singh, Pradeep Kumar	A trust-based framework has been developed to detect DDoS attacks in VANETs using trust evaluation and clustering. Mentioned Important components of trust are data factor, residual energy, trust policy, statistics on frequency values, and statistics on trust hypotheses. Work was done to create a trust assessment matrix and integrate it with clustering to enhance intrusion prevention. Algorithm DGSOT uses to determine evaluate node trustworthiness and node hierarchy. clusters for routing dominant based on Trusted nodes in hierarchical levels form. Performance metrics components are Average Latency, Packet Delivery Ratio, Detection Rate, and Energy Consumption.	A trust-based framework proposes frequency value, trust hypothesis, residual energy, trust policy, and data factor. Goals to optimize bandwidth while maintaining security evaluated using Average Latency, Packet Delivery Ratio, Detection Rate, and Energy Consumption. reduces detection costs and identifies attackers by combining trust evaluation with clustering. Lacks some quantitative outcomes on classification performance, model efficiency, feature extraction.	Potential biases in the method used to evaluate trust and a dearth of discussion around the biases of researchers or the weighting of trust factors. Limitations include indistinct VANET network scope, computational resource requirements, and dependence on simulated environments. Issues in methodology: Indefinite evaluation design No comparison to other methods	Quantitative
4	Improved Detection and Mitigation of DDoS Attack in Vehicular ad hoc Network	2018	Galgotias University, School of Computing Science and Engineering Institute of Electrical and Electronics Engineers. Uttar Pradesh Section Institute of Electrical and Electronics Engineers	The research employs simulations with no precise real-world data collection methods or dataset size The simulation applies 40 vehicular nodes and three malicious nodes: 2 bots, one attacker, and a victim node. NS-2 simulator used the following; network includes Road Side Units and communication Vehicle-to-Vehicle. How is the detection method done: through bandwidth utilization, finds an abundance of	It can be seen that the proposed method shows higher average throughput (51.98 vs 39.33) and lower routing overhead (13.48 vs 19.58). The study shows a simulation time limited to 7.5 minutes and a lower average packet loss (7.65 vs. 9.198). The method catches and separates malicious nodes by verifying bandwidth against a threshold, enhancing network performance metrics	The study employs only simulated data and environments with around 40 nodes and a single attack technique, restricting realism and generalizability. Focuses on three performance indicators (throughput, packet loss, routing overhead) and ignore statistical analysis, affecting reliability or multiple trials.	Quantitative

			control packets, and separates malevolent nodes. Performance assessed against current techniques through packet loss and network throughput. Visualization tools: X graph for simulation results and for network interpretation Network Animator (NAM)	The paper focuses on network performance and lacks more details on measurement for classification performance metrics and feature extraction.		
5	8 MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET	2021	A1- Mehdhara MRuan N The research uses a current VANET network simulation dataset; attributes on dataset cluster The precise sample size and preparation procedures are not stated. Suggests an SDN controller-integrated Multilayer Distributed Self-Organizing Map (MSOM) with two classes of clustering and classification. Model qualified and tested utilizing the NS-3 simulator with a lowest simulation time of 100 seconds. Achieves 99.67% detection accuracy; additional performance metrics are assessed, but are not covered in detail in the extract.	The MSOM method attained 99.67% accuracy in noticing DDoS attacks. Enhanced security and recovery time through better detection and mitigation when compared to regular SOMs. Illustrate the limitations of centralized SDN designs through a distributed layered approach No exact details on attribute extraction or ROC curve results are provided.	Data size are not mentioned. The study focused on DDoS attacks in VANET, without comparison with different methods or security threats Instead of testing the real world, the results were based on simulations. It may not accommodate all real-world complexities Lacks address various attack types.	Quantitative

6	10 Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection	2022	Luo, Xiongwen Polat, Hüseyin Koçak, Cemal Polat, Onur	A custom SD-VANET topology gathered data on 42 attributes, including standard and DDoS attack traffic. Selection MRMR feature decreased 42 features to the most exceptional ones for model training. The research used three classifiers: K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Decision Tree (DT). Classifiers were trained and tried on the original and MRMR-reduced datasets, and hyperparameter tweaking was done using Bayesian optimization.	21 By using MRMR feature selection and Bayesian optimization-based Decision Tree classifier, the highest accuracy of 99.35% was achieved. 24-ssed classifiers: K-Nearest Neighbors, Support Vector Machine, and Decision Tree, trained on original and reduced datasets. MRMR algorithm enhanced performance by picking the most unique features; Bayesian optimization improved accuracy. MRMR reduced the dataset size and improved accuracy. The original dataset had 42 features. The MRMR algorithm improved performance by selecting the most unique features, and Bayesian optimization enhanced accuracy.	The dataset size and samples were unspecified. In contrast to standard datasets, which are restricted to particular classifiers, the study uses a bespoke SD-VANET topology and dataset, which may introduce bias. It has limited real-world relevance due to its exclusive focus on DDoS assaults and simulated data usage; it also lacks testing on devices with limited resources.	Quantitative
---	---	------	--	---	---	--	--------------

References:

- Al-Mehdhara, 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>
- 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>

Assignment_1_Msalem.docx

ORIGINALITY REPORT

18%

SIMILARITY INDEX

14%

INTERNET SOURCES

17%

PUBLICATIONS

11%

STUDENT PAPERS

PRIMARY SOURCES

1

dr.ntu.edu.sg

Internet Source

2%

2

arxiv.org

Internet Source

1%

3

Muammer Türkoğlu, Hüseyin Polat, Cemal Koçak, Onur Polat. "Recognition of DDoS Attacks on SD-VANET Based on Combination of Hyperparameter Optimization and Feature Selection", Expert Systems with Applications, 2022

Publication

1%

4

conf.kln.ac.lk

Internet Source

1%

5

researchr.org

Internet Source

1%

6

Mohamed Ali Setitra, Mingyu Fan. "Detection of DDoS attacks in SDN-based VANET using optimized TabNet", Computer Standards & Interfaces, 2024

Publication

1%

7	link.springer.com Internet Source	1 %
8	www.hindawi.com Internet Source	1 %
9	www.semanticscholar.org Internet Source	1 %
10	avesis.gazi.edu.tr Internet Source	1 %
11	www.coursehero.com Internet Source	1 %
12	Submitted to Glasgow Caledonian University Student Paper	1 %
13	Submitted to Indian Institute of Technology- Bhubaneswar Student Paper	1 %
14	Rajendra Prasad Nayak, Srinivas Sethi, Sourav Kumar Bhoi, Kshira Sagar Sahoo et al. "TBDDoSA-MD: Trust-Based DDoS Misbehave Detection Approach in Software-defined Vehicular Network (SDVN)", Computers, Materials & Continua, 2021 Publication	1 %
15	hightechjournal.org Internet Source	<1 %

16	Huseyin Polat, Muammer Turkoglu, Onur Polat. "Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET", IET Communications, 2021 Publication	<1 %
17	Submitted to Liverpool John Moores University Student Paper	<1 %
18	Submitted to University of Hertfordshire Student Paper	<1 %
19	Submitted to University of Sunderland Student Paper	<1 %
20	docs.google.com Internet Source	<1 %
21	saucis.sakarya.edu.tr Internet Source	<1 %
22	theses.hal.science Internet Source	<1 %
23	mjee.iaumajlesi.ac.ir Internet Source	<1 %
24	pubmed.ncbi.nlm.nih.gov Internet Source	<1 %
25	Submitted to Coastal Carolina Community College Student Paper	<1 %

26

Submitted to Anna University

Student Paper

<1 %

27

M. Poongodi, S. Bose. "Stochastic model: reCAPTCHA controller based co-variance matrix analysis on frequency distribution using trust evaluation and re-eval by Aumann agreement theorem against DDoS attack in MANET", Cluster Computing, 2015

Publication

<1 %

28

assets.researchsquare.com

Internet Source

<1 %

29

ouci.dntb.gov.ua

Internet Source

<1 %

30

Ankit Kumar Jain, Hariom Shukla, Diksha Goel. "A comprehensive survey on DDoS detection, mitigation, and defense strategies in software-defined networks", Cluster Computing, 2024

Publication

<1 %

31

Goodness Oluchi Anyanwu, Cosmas Ifeanyi Nwakanma, Jae Min Lee, Dong-Seong Kim. "RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network", Ad Hoc Networks, 2022

Publication

<1 %

Ying Gao, Hongrui Wu, Binjie Song, Yaqia Jin, Xiongwen Luo, Xing Zeng. "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network", IEEE Access, 2019

Publication

<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography On