ISSN(O): 2320-5407 | ISSN(P): 3107-4928

ISSN NO. 2320-5407

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

Manuscript No.: IJAR-59747

Title: Vulnerability of Deep Network Intrusion Detectors to EvasionVaries with the Training Seed

Recommendation:

Accept as it is .....

Accept after minor revision.....

Accept after major revision .....yes.....

Do not accept (*Reasons below*) .....

Rating	Excel.	Good	Fair	Poor
Originality			y	
Techn. Quality			Y	
Clarity			Y	
Significance			Y	

Reviewer's ID: JPR-Dr.Shaweta sachdeva

Detailed Reviewer's Report

1. The authors should clearly emphasize the novelty and significant contributions of the proposed research compared with existing studies on adversarial evasion and deep learning-based intrusion detection systems.
2. The experimental evaluation is limited to the corrected CIC-IDS-2017 dataset. The authors should consider validating the findings using additional benchmark datasets to establish the generalizability of the results.
3. The manuscript demonstrates considerable variation in adversarial vulnerability across different training seeds. The authors should provide a deeper theoretical explanation of why models with similar detection performance exhibit significantly different evasion rates.
4. The proposed adversarial attack operates primarily through feature-space modifications. The authors should further investigate whether these modifications can be realistically implemented in actual network traffic environments.
5. The authors should justify the selection of nine CNN models and 33 MLP models and explain whether the chosen number of training seeds is sufficient for reliable statistical conclusions.
6. The chronological splitting strategy is an important aspect of the study. However, the authors should further discuss its limitations and evaluate how the results might change under a strictly time-based deployment scenario.
7. The manuscript reports a significant increase in false-positive rates under chronological evaluation. The authors should provide additional analysis of the factors contributing to this increase and discuss possible mitigation strategies.
8. The proposed adaptive attack methodology should be compared more comprehensively with existing adversarial attack techniques to demonstrate its effectiveness and computational efficiency.
9. The authors should provide a detailed justification for selecting the low, medium, and high attack-budget configurations. The practical implications of these constraints should also be discussed.
10. The results indicate that conventional detection metrics are insufficient to predict adversarial vulnerability. The authors should further explain how the proposed validation-based vulnerability assessment can be integrated into practical model selection and deployment procedures.

ISSN(O): 2320-5407 | ISSN(P): 3107-4928
International Journal of Advanced Research
Publisher's Name: Jana Publication and Research LLP
www.journalijar.com

REVIEWER'S REPORT

11. The study should include additional experiments involving different deep learning architectures to determine whether the observed training-seed sensitivity extends beyond CNN and MLP models.
12. The authors should elaborate on the computational overhead associated with adversarial robustness evaluation, particularly when a large number of models and attack conditions are considered.
13. The statistical analysis is comprehensive; however, the authors should provide clearer interpretations of the variance decomposition, confidence intervals, and significance testing results for readers.
14. The figures and tables should be improved in terms of readability, labeling, and formatting. Some graphical representations contain densely presented information that may be difficult to interpret.
15. The discussion section should be strengthened by presenting practical recommendations for improving the robustness and reliability of deep learning-based intrusion detection systems.
16. The authors should expand the limitations and future work discussion to include real-world network traffic validation, concept drift, and the effectiveness of defensive mechanisms against adaptive adversarial attacks.
17. The manuscript should be carefully proofread to correct minor grammatical errors, inconsistent spacing, mathematical notation, and formatting issues.
18. The conclusion should more explicitly summarize the principal research contributions, practical implications, and potential directions for future investigation.

Overall Comments to the Authors

The manuscript presents a relevant and technically interesting investigation into the influence of training randomness on adversarial vulnerability in deep learning-based network intrusion detection systems. The experimental analysis and statistical evaluation are valuable aspects of the study. Nevertheless, further clarification of the methodological choices, validation across additional datasets, stronger justification of the attack constraints, and improved discussion of practical applicability would enhance the manuscript's scientific quality. The authors are encouraged to address these concerns before publication.

Recommendation: Revision Required.