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 Evasion Varies with the Training Seed.

Recommendation:
Accept as it is .....
Accept after minor revision.....
Accept after major revision ...✓.....
Do not accept (*Reasons below*) .....

Rating	Excel.	Good	Fair	Poor
Originality		✓		
Techn. Quality		✓		
Clarity		✓		
Significance			✓	

Reviewer's ID: JPR- **098**

Detailed Reviewer's Report

Decision: Accept after Major Revision

Major Revisions

1. **Limited Dataset Generalizability:** The experimental evaluation relies exclusively on the corrected CIC-IDS-2017 dataset. Although this dataset is widely used, it represents a limited network environment and a specific collection period. The authors should validate their findings using additional datasets, such as CIC-IDS-2018, UNSW-NB15, or other contemporary NIDS datasets, to establish whether training-seed-dependent evasion vulnerability is consistent across different network environments.

2. **Realism of the Threat Model:** The proposed attacker modifies forward traffic through padding, packet delays, and dummy packet insertion. However, the manuscript primarily evaluates the resulting changes in feature vectors rather than replaying modified packets through a real network traffic-processing pipeline. The authors should provide stronger justification that these modifications are feasible under realistic network conditions and do not unintentionally alter the intended malicious activity.

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

3. **Feature-Space Evasion Requires Further Validation:** The authors report that 22 features are recomputed using closed-form expressions, while other features are retained or approximated. This may introduce discrepancies between the modified feature vectors and the statistics that would be generated by an actual packet-level implementation. The authors should validate the modified flows using CICFlowMeter or an equivalent flow-extraction tool and report the differences.

4. **Chronological Split Strategy:** The study uses a chronological split within each attack class, assigning the oldest 70% to training, the next 15% to validation, and the latest 15% to testing. Although this helps reduce temporal leakage, it does not fully represent a realistic deployment scenario in which the detector encounters future traffic, potentially including previously unseen attack patterns. The authors should discuss this limitation and consider an additional time-based evaluation.

5. **Training-Seed Variability Needs Deeper Analysis:** The central contribution is that models trained with different random seeds exhibit substantially different evasion rates despite similar detection performance. The authors should provide a more detailed explanation of the possible causes, including weight initialization, batch ordering, dropout behavior, and differences in learned decision boundaries.

6. **Limited Number of CNN Models:** The principal CNN analysis considers nine training seeds. Although the reported variation is substantial, a larger number of independently trained models would provide stronger statistical evidence. The authors should justify the selection of nine seeds and, if feasible, extend the experiments to additional seeds to confirm the stability of the findings.

7. **Attack Budget and Query Limit Justification:** The attacker is allowed up to 1,000 queries per flow, and the experiments consider low, medium, and high modification budgets. The authors should justify these limits in terms of realistic attacker capabilities, network constraints, and computational cost. The practical implications of the query budget should also be discussed.

8. **Insufficient Evaluation of Attack Impact on Network Functionality:** The study measures evasion success primarily through benign classification.

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

However, it does not sufficiently establish whether the modified traffic preserves the original malicious functionality or whether padding, delays, and dummy packets affect the attack's effectiveness. The authors should discuss this issue and provide validation where possible.

9. **Statistical Analysis and Uncertainty Reporting:** The manuscript uses variance decomposition, bootstrap intervals, permutation tests, and Holm correction. These are useful techniques, but the statistical assumptions and interpretation of the reported detector variance share should be explained more clearly. The authors should also provide additional uncertainty measures for evasion rates and clarify the implications of the small number of attack conditions and test flows for certain attack families.

10. **Practical Deployment and Defense Implications:** The manuscript recommends evaluating multiple training runs and selecting models based on validation-set evasion performance. However, the practical cost of this approach and its effectiveness under changing attack strategies remain unclear. The authors should discuss how this model-selection procedure could be integrated into an operational NIDS and whether the selected model remains robust against adaptive attackers or changing network traffic.

Minor Revisions

1. **Abstract Presentation:** The abstract contains several important numerical findings, but the presentation is dense. The authors should improve its readability by separating the dataset and evaluation setup, principal findings, and practical contribution.

2. **Terminology Consistency:** The terms *evasion rate*, *attack success*, *false-positive rate*, *training seed*, and *attack condition* should be defined consistently and used precisely throughout the manuscript.

3. **Dataset Preprocessing Details:** The authors should provide clearer information about the corrected CIC-IDS-2017 dataset, including the exact cleaning procedures, class-label mapping, and criteria used to retain 20% of each day's flows.

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

4. **False-Positive Analysis:** The manuscript reports that traffic associated with destination port 8080 accounts for a substantial proportion of false alarms. The authors should explain this observation more clearly and discuss whether it reflects a dataset-specific artifact or a broader operational concern.

5. **Attack Family Sample Sizes:** The evaluation uses 100 test flows per family, except for Bot, which contains only 21 flows. The authors should highlight this imbalance more clearly when interpreting family-level evasion rates and correlations.

6. **Model Architecture Description:** The CNN and MLP architectures are described briefly. The authors should provide a more complete specification of their layers, activation functions, dropout settings, and other relevant training parameters to improve reproducibility.

7. **Hyperparameter Selection:** The manuscript reports the use of Adam, a learning rate of 10^-3, and a batch size of 512. The authors should clarify whether these settings were fixed in advance or selected through preliminary experimentation or validation.

8. **Figure and Table Readability:** Some figures and tables contain dense information. The authors should improve font sizes, legends, axis labels, and table alignment to make the comparisons among detectors and attack families easier to interpret.

9. **Equations and Mathematical Notation:** The mathematical expressions describing flow modification, variance decomposition, and evasion measurement should be checked for consistent notation. All variables and parameters should be clearly defined when first introduced.

10. **References and Language Editing:** The authors should carefully proofread the manuscript for grammatical consistency, technical wording, and reference formatting. The presentation of equations, section headings, abbreviations, and citations should follow the journal's prescribed style.