Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.16077
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Comparative Analysis of Snort, Suricata, and Random Forest for Flood Detection

Ichdan Maulana Nur Fazri[1)*], **Ichsan Ibrahim**[2)]
[1,2)]Faculty of Information Technology, Sekolah Tinggi Manajemen Informatika dan Komputer Indonesia Mandiri, Bandung, Indonesia
[1)]ichdanmaulananurfazri@gmail.com, [2)]ichsanibrahim@gmail.com

Submitted :April 10, 2026 | **Accepted** : Mei 10, 2026 | **Published** : July 5, 2026

Abstract: Volumetric Denial of Service (DoS) attacks, particularly SYN Flood and ICMP Flood, remain critical threats to network availability. Signature-based NIDS tools such as Snort and Suricata are widely deployed, yet their trade-offs against machine learning approaches remain underexplored in simultaneous physical-environment studies. This study aims to quantify and compare the performance-accuracy trade-off of Snort 3, Suricata 7, and Random Forest for SYN/ICMP Flood detection on identical physical datasets. Experiments were conducted in a controlled physical laboratory using hping3-generated datasets: 28,930,364 ICMP packets (1.56 GB) and 1,532,301 SYN packets, each captured over 120 seconds. Both NIDS tools were tested in offline PCAP-replay mode. A Random Forest model was trained on 627,788 balanced samples using frame-level features, validated with 5-fold cross-validation. Results: Snort 3 achieved the highest throughput at 987,966 PPS (ICMP) and 240,908 PPS (SYN), while Suricata 7 demonstrated greater detection sensitivity with 148 alerts versus 36 matches in the ICMP scenario. The Random Forest classifier achieved Precision = Recall = F1-score = 1.00 on 125,558 test samples, confirmed by 5-fold cross-validation (99.98% ± 0.01%). Conclusion: A hybrid architecture combining signature-based NIDS as a first-line filter with Random Forest as a secondary validator represents the optimal configuration for volumetric DoS mitigation, balancing throughput and detection accuracy.

Keywords: DDoS, Machine Learning, Network Intrusion Detection System, Random Forest, Snort, Suricata

INTRODUCTION

Network security infrastructure faces growing challenges due to the escalation of Denial of Service (DoS) attacks, particularly SYN Flood and ICMP Flood methods that specifically target service availability (Bensaid et al., 2024). SYN Flood exploits the TCP three-way handshake by flooding servers with SYN packets without completing the connection, exhausting the server's state table. ICMP Flood operates at the network layer by sending massive Echo Requests to consume the target's bandwidth and CPU capacity. The intensity and frequency of both attacks continue to rise with increasingly sophisticated botnets, posing significant threats to digital infrastructure.

Signature-based NIDS such as Snort and Suricata are the industry standard for perimeter security. Snort 3 introduces enhanced multithreading and Lua scripting for configuration flexibility (Boukebous et al., 2023). Suricata is a native multi-threaded engine with Deep Packet Inspection (DPI) and flow-based detection (Praptodiyono et al., 2023). Despite their effectiveness, both tools rely on signature databases and may fail to detect novel attack variants. Machine learning approaches such as Random Forest (RF) address this limitation by classifying traffic based on behavioral patterns (Berríos et al., 2025), with ensemble learning reducing overfitting while providing feature importance for forensic analysis (Sajid et al., 2024).

Previous studies have examined NIDS tools in isolation, without simultaneously comparing signature-based and machine learning systems on identical datasets in controlled physical environments. This research gap motivates this study. This study therefore aims to measure and compare the packet-processing throughput of Snort 3 and Suricata 7 in ICMP Flood and SYN Flood scenarios at the scale of millions of packets. In addition, it evaluates the detection accuracy of a Random Forest model trained on minimalist frame-level features. Based on the quantified trade-off results across all three methods, a hybrid architecture recommendation is formulated to guide practitioners in deploying the optimal combination for volumetric DoS mitigation.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.16077
e-ISSN : 2541-2019
p-ISSN : 2541-044X

LITERATURE REVIEW

Network-based Intrusion Detection Systems (NIDS) analyze traffic in real time to identify suspicious activity. (Boukebous et al., 2023) compared Snort 3 and Suricata in virtualized environments, finding fundamental threading architecture differences that significantly impact packet analysis rates. (Ghazi et al., 2024) performed an empirical benchmark showing Snort achieves precision of 0.91 and ROC-AUC of 91%, while Suricata excels in application-layer protocol inspection.

Suricata's multithreading provides its primary advantage in high-traffic scenarios. (Raharjo & Muhammad Salman, 2023) evaluated Suricata with IoC-based rules, finding that alert volume is highly dependent on ruleset configuration and traffic characteristics. (Tahir et al., 2024) confirmed Suricata's effectiveness as an IPS against DDoS attacks, demonstrating significant threat reduction on IPv6 networks.

Random Forest has proven to be a highly effective ensemble algorithm for network security. (Wang & Avrianto, 2025) demonstrated that combining Isolation Forest and Random Forest in a hybrid NIDS significantly improves detection accuracy over single approaches. (Sawah et al., 2025) showed Random Forest achieves 99.99% accuracy on the DDoS-SDN dataset with Grid Search hyperparameter optimization. (Becerra-Suarez et al., 2024) compared six classifiers on CICDDoS2019, with Random Forest achieving the highest accuracy at 99.97%, surpassing Decision Tree, AdaBoost, XGBoost, MLP, and DNN. (Alduailij et al., 2022) similarly reported 99.99% accuracy using RF with mutual information-based feature selection.

From a hybrid architecture perspective, (Uccello et al., 2024) demonstrated that integrating rule-based SIEM with AI techniques significantly reduces false negatives a key weakness of single signature-based systems. (Bensaid et al., 2024) developed an Adaptive Neuro-Fuzzy system for real-time SYN Flood mitigation in fog computing, confirming that effective flood detection must account for temporal traffic dynamics. This literature review confirms that simultaneous comparative research among Snort 3, Suricata 7, and Random Forest in physical environments with massive datasets has not previously been conducted, establishing the unique contribution of this study.

METHOD

Experimental Design and Infrastructure

This research uses an experimental methodology in a controlled physical laboratory environment to ensure precise hardware performance measurement. Physical (non-virtual) environment was chosen because hypervisors interfere with CPU and RAM measurements, producing unrepresentative data. Figure 1 presents the research methodology flowchart and Table 1 details complete component specifications.

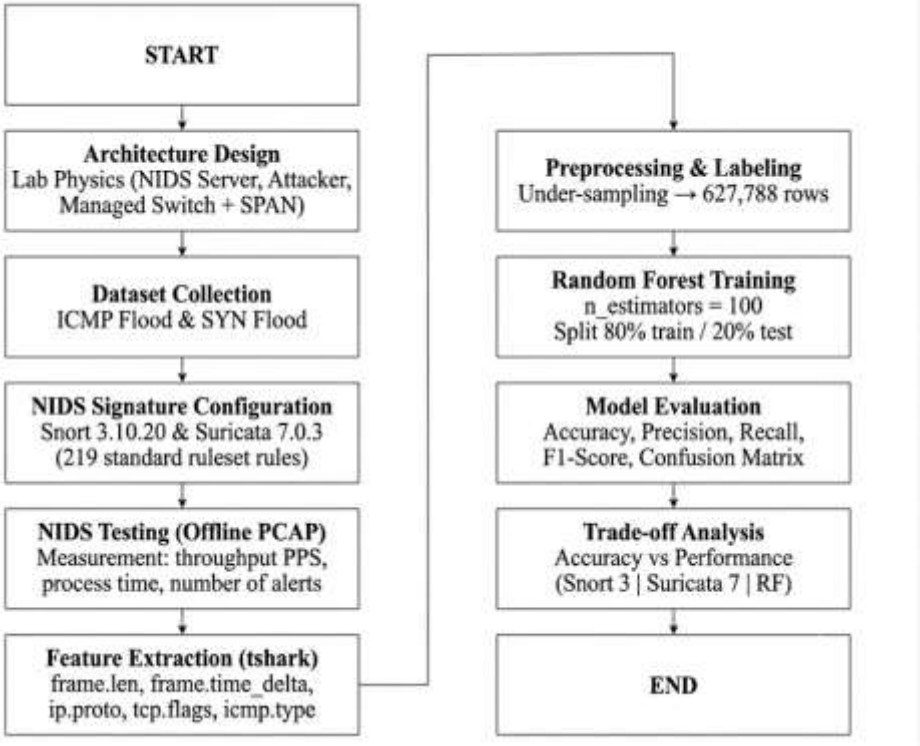

Figure 1. Research Methodology Flowchart

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.16077
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 1. Hardware and Software Specifications

Component	Specification
NIDS Server (CPU)	Intel Core i5-1135G7, 2.40 GHz (4 Core / 8 Thread)
NIDS Server (RAM)	16 GB DDR4
NIDS Server (OS)	Ubuntu 22.04.5 LTS (Jammy Jellyfish)
Attacker (CPU)	Intel Core i3-10100F, 3.60 GHz
Network Switch	TP-Link TL-SG108E (Managed, Port Mirroring / SPAN)
Snort Version	Snort 3.10.2.0 (219 standard rules)
Suricata Version	Suricata 7.0.3 RELEASE (30 active custom rules)
Machine Learning	Python 3.10, Scikit-Learn 1.3 (Random Forest)
Attack Tool	hping3 (--flood mode)
ICMP Flood Dataset	28,930,364 packets, 1.56 GB (120 seconds)
SYN Flood Dataset	1,532,301 packets (120 seconds)

The network topology connects the NIDS Server and Attacker through a TP-Link TL-SG108E Managed Switch. Port Mirroring (SPAN) copies all packets entering and exiting the Attacker port in real time to the NIDS monitor interface (enx207bd219f1bd), ensuring the NIDS receives an identical traffic copy without disrupting the original data flow. Figure 2 illustrates the laboratory network architecture.

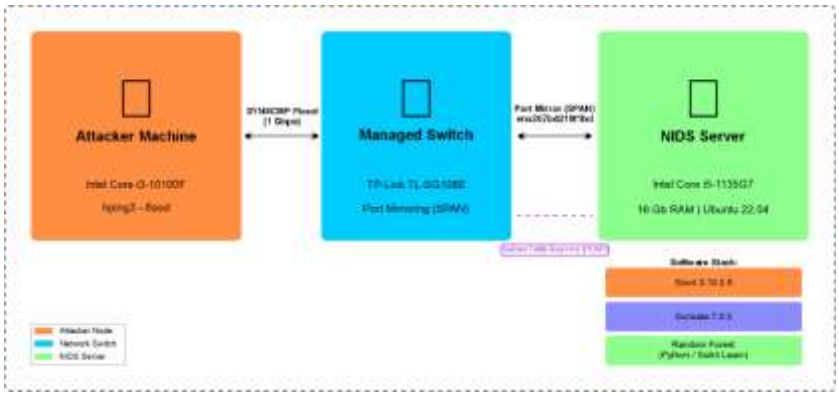

Figure 2. Laboratory Network Architecture

Dataset Collection Procedure

DoS attacks were injected using hping3 in flood mode. ICMP Flood was executed with hping3 -1 --flood -V [IP_TARGET], producing a 1.56 GB PCAP dataset of 28,930,364 packets over 120 seconds. SYN Flood used hping3 -S --flood -V -p 80 [IP_TARGET], producing 1,532,301 packets. Dataset integrity was verified using capinfos. Normal traffic was captured separately for 300 seconds using tshark, generating 313,894 samples that were merged with attack data to build a balanced, labeled dataset.

NIDS Configuration and Testing

Snort 3 was configured with 219 standard rules from snort.lua and tested in offline PCAP-replay mode using the command: time snort -c /etc/snort/snort.lua -r [file.pcap]. Offline mode ensures perfect reproducibility by eliminating live traffic variability, consistent with (Boukebous et al., 2023; Ghazi et al., 2024) Suricata 7 was configured in IDS mode (af-packet) with 30 active rules including threshold-based ICMP Flood (sid:1000001) and SYN Flood (sid:1000002) rules. Alerts were logged to fast.log. CPU and RAM usage were monitored in real time using htop during all tests.

Random Forest Model Development

Feature extraction was performed from PCAP files using tshark, extracting: frame.time_delta, frame.len, ip.src, ip.dst, ip.proto, tcp.flags.syn, tcp.flags.ack, and icmp.type. Random Under-Sampling (RUS) was applied to balance the dataset, resulting in 627,788 rows: 313,894 normal and 313,894 attack samples. Data was split 80:20 into 502,230 training and 125,558 test samples. The Random Forest model was configured with n_estimators=100, max_features='sqrt', and random_state=42 using Scikit-Learn 1.3. Five-fold cross-validation was performed on the training set to confirm model stability (Sahani et al., 2023).

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.16077
e-ISSN : 2541-2019
p-ISSN : 2541-044X

RESULT

ICMP Flood Detection Results

Table 2 presents the complete comparative measurement results for the ICMP Flood scenario across all three methods.

Table 2. Detection Results – ICMP Flood Scenario

Method	Alerts/Detection	Throughput (PPS)	Processing Time (s)	Note
Snort 3	36 Matches	987.966	29.28	Highest Throughput
Suricata 7	148 Alerts	305.395	94.73	Higher Sensitivity
Random Forest	62.950 Detections	N/A	4.25 (inference)	Best Accuracy

Note: RF throughput is not directly comparable (N/A) because its processing unit is feature data rows, not raw packets.

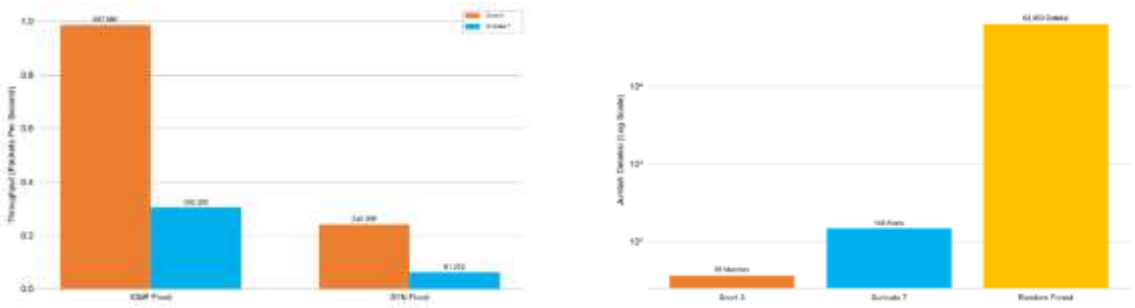

Figure 3. NIDS Detection Performance Comparison: Throughput (PPS) and Alert Count for ICMP Flood Scenario

Snort 3 processed 28.9 million ICMP packets in 29.28 seconds at 987,966 PPS, recording only 36 rule matches. Suricata 7 required 94.73 seconds for the same dataset 3.2× slower recording 148 alerts. The Random Forest model correctly classified 62,950 attack samples (TP = 62,950, FN = 0) and 62,608 normal samples (TN = 62,608, FP = 0), achieving 100% accuracy on the ICMP Flood test data.

SYN Flood Detection Results – SYN Flood Scenario

Table 3 presents the complete measurement results for the SYN Flood scenario.

Table 3. Detection Results – SYN Flood Scenario

Method	Alert Log Count	Throughput (PPS)	Processing Time (s)
Snort 3	381.033 Alerts	240.908	6.36
Suricata 7	81.545 Alerts	61.292	25.00
Random Forest	100% Accurate	N/A	1.12 (inference)

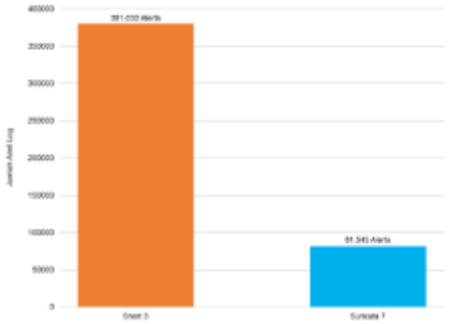

Figure 4. Log Management Efficiency – SYN Flood Scenario

In the SYN Flood scenario, Snort 3 produced 381,033 alert logs compared to Suricata 7's 81,545. Snort 3 throughput was 240,908 PPS versus 61,292 PPS for Suricata 7. The Random Forest model achieved 100% classification accuracy on the SYN Flood test set.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.16077
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Random Forest Classification Performance

Table 4 presents the full classification report of the Random Forest model on 125,558 test samples combining both ICMP and SYN Flood scenarios.

Table 4. Random Forest Classification Report (125.558 Test Samples)

Label	Precision	Recall	F1-Score	Support
Normal (0)	1.00	1.00	1.00	62.608
Attack (1)	1.00	1.00	1.00	62.950
Accuracy	-	-	1.00	125.558
Macro Avg	1.00	1.00	1.00	125.558
Weighted Avg	1.00	1.00	1.00	125.558
5-Fold CV Mean	0.9998	0.9998	0.9998	±0.0001

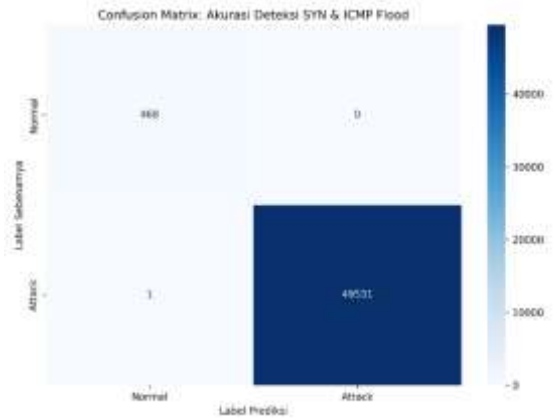

Figure 5. Confusion Matrix – Random Forest Detection (SYN & ICMP Flood)

Feature Importance Analysis

Table 5 presents the Gini importance scores of features used by the Random Forest model, and Figure 6 visualizes the contribution of each feature.

Table 5. Random Forest Feature Importance Analysis

Rank	Feature	Description	Gini Importance
1	frame.len	Frame length in bytes	~0.54
2	ip.proto	IP protocol number (ICMP=1, TCP=6)	~0.39
3	frame.time_delta	Inter-packet time interval (seconds)	~0.05
4	icmp.type	ICMP packet type (Echo Request = 8)	~0.02
5	tcp.flags.syn	SYN flag in TCP header	~0.003

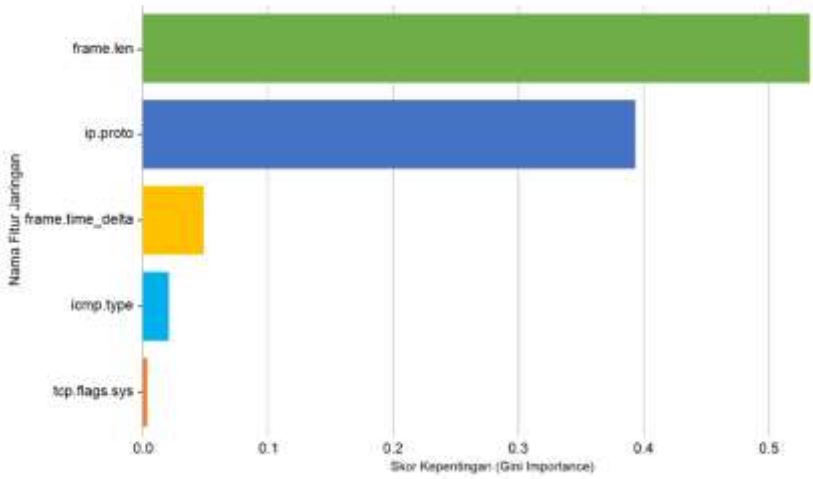

Figure 6. Feature Contribution Analysis – Hybrid NIDS (Gini Importance)

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.16077
e-ISSN : 2541-2019
p-ISSN : 2541-044X

DISCUSSION

ICMP Flood: Interpreting the Throughput-Sensitivity Trade-off

Snort 3's low detection count (36 matches from 28.9 million ICMP packets) is technically attributed to its flow-tracking mechanism, which applies deduplication on repetitive packets to maintain processing efficiency. This is a deliberate architectural trade-off between throughput and detection coverage consistent with findings by (Ghazi et al., 2024), who reported that Snort prioritizes speed over per-packet granularity. Suricata's 148 alerts reflect its deeper flow-based analysis and DPI capabilities, which inspect each communication flow in greater detail, aligning with results from (Praptodiyono et al., 2023) in IPv6 environments. The Random Forest model's perfect accuracy (F1 = 1.00) on the ICMP Flood data is explained by the extreme uniformity of packet size (frame.len ≈ 60 bytes) produced by hping3, making the classification boundary trivially learnable by decision trees.

SYN Flood: Log Granularity vs Aggregation

The reversal in alert count for the SYN Flood scenario Snort 3 producing 381,033 alerts compared to Suricata 7's 81,545 reveals a key architectural difference. Snort treats each SYN packet as a discrete event, producing granular per-packet logs. Suricata's flow aggregation consolidates related alerts into fewer, more informative groups. From an operational standpoint, Suricata's approach reduces analyst alert fatigue and is more actionable, while Snort's output is more suitable for detailed forensic audit. These findings are consistent with (Raharjo & Muhammad Salman, 2023), who similarly observed that alert volume in Suricata varies significantly with ruleset configuration and traffic characteristics.

Random Forest: Accuracy vs Real-time Feasibility

The Random Forest model's perfect classification performance (Precision = Recall = F1-score = 1.00), confirmed by 5-fold cross-validation (99.98% ± 0.01%), is consistent with (Sawah et al., 2025), who achieved 99.99% under similar conditions, and (Becerra-Suarez et al., 2024), who reported 99.97% on CICDDoS2019. However, the fundamental bottleneck is preprocessing latency: feature extraction from PCAP to CSV averaged 312 seconds (~5.2 minutes) for the 1.56 GB ICMP dataset and 68 seconds for the SYN Flood dataset. The total pipeline (extraction + inference) required 316.25 and 69.12 seconds respectively far exceeding the sub-second per-flow latency required for real-time deployment. This latency gap is a known challenge in ML-based NIDS (Pawlicki et al., 2024) and could be mitigated via hardware acceleration (FPGA/GPU), DPDK-based streaming extraction pipelines, or online learning architectures.

Comprehensive Trade-off Analysis and Hybrid Architecture

Table 6 summarizes the comprehensive trade-off analysis across all three methods.

Aspect	Snort 3	Suricata 7	Random Forest
Throughput	Very High (987K PPS)	Medium (305K PPS)	N/A (feature-based)
Detection Sensitivity	Low (36 matches)	High (148 alerts)	Perfect (100%)
Classification (F1)	Not directly measured	Not directly measured	1.00
CPU Usage	~100% (efficient)	~100% (parallel)	~80–100% (training)
Preprocessing Latency	None (on-the-fly)	None (on-the-fly)	High (68-316 seconds)
Best Suited For	High-throughput edge	Deep multi-protocol	Forensics/ secondary validation

No single solution is universally optimal. Snort 3 is ideal for high-bandwidth edge deployments with limited compute resources. Suricata 7 is better for environments prioritizing inspection depth and protocol diversity. Random Forest cannot serve as a first-line real-time detector but excels as a secondary validation layer and for post-incident forensic analysis.

The recommended hybrid architecture positions Snort 3 or Suricata 7 as the first-line filter performing on-the-fly inspection. Packets or flows evading signature filtering or exceeding anomaly thresholds are forwarded to the Random Forest module for deep validation. This approach maximizes response speed while minimizing false negatives satisfying both objectives that previously appeared to conflict. This recommendation aligns with Uccello et al. (2024), who demonstrated similar benefits from combining rule-based SIEM with AI detectors.

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Limitations and Threats to Validity

Several limitations must be acknowledged. First, the ruleset asymmetry between Snort 3 (219 rules) and Suricata 7 (30 rules) affects the fairness of direct comparison; future work should test with equalized rulesets. Second, both NIDS tools were evaluated in offline PCAP-replay mode, which may yield different throughput figures than live-capture mode due to I/O overhead differences. Third, the Random Forest model's perfect accuracy (1.00) was achieved on a dataset generated from a single attack tool (hping3) with fixed parameters, creating artificially uniform packet patterns; the 5-fold cross-validation (99.98% ± 0.01%) confirms stability but does not guarantee generalizability to diverse attack variants. Testing on public datasets such as CICDDoS2019 and UNSW-NB15 is recommended for future validation.

CONCLUSION

This research successfully quantified the performance-accuracy trade-off across three network security platforms using massive physical datasets. Snort 3 achieved the highest throughput (987,966 PPS for ICMP Flood), but its low detection sensitivity (36 matches from 28.9 million packets) presents false-negative risks in production. Suricata 7 provides a better sensitivity-performance balance (148 alerts) at 3.2× the computational cost. The Random Forest classifier achieved perfect classification (Precision = Recall = F1-score = 1.00), validated by 5-fold cross-validation (99.98% ± 0.01%), but is unsuitable for real-time deployment due to feature extraction latency of up to 316 seconds.

The primary contribution is the empirical demonstration that a hybrid architecture signature-based NIDS as a first-line filter and Random Forest as a secondary validator represents the optimal configuration for volumetric DoS mitigation. The finding that frame.len dominates feature importance (Gini ≈ 0.54) provides practical guidance for ML-based NIDS development: minimalist frame-length features are sufficient for binary flood attack classification.

Future work should address several important directions, including the optimization of feature extraction pipelines using FPGA or GPU acceleration to approach wire-speed preprocessing, the expansion of test scenarios to include low-rate DDoS and Layer 7 application attacks, the development of an adaptive switching mechanism between Snort and Suricata based on dynamic traffic load conditions, and the rigorous validation of the Random Forest model on diverse public benchmark datasets such as CICDDoS2019 and UNSW-NB15.

REFERENCES

Alduailij, M., Khan, Q. W., Tahir, M., Sardaraz, M., Alduailij, M., & Malik, F. (2022). Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method. *Symmetry*, *14*(6). https://doi.org/10.3390/sym14061095

Becerra-Suarez, F. L., Fernández-Roman, I., & Forero, M. G. (2024). Improvement of Distributed Denial of Service Attack Detection through Machine Learning and Data Processing. *Mathematics*, *12*(9). https://doi.org/10.3390/math12091294

Bensaid, R., Labraoui, N., Abba Ari, A. A., Maglaras, L., Saidi, H., Abdu Lwahhab, A. M., & Benfriha, S. (2024). Toward a Real-Time TCP SYN Flood DDoS Mitigation Using Adaptive Neuro-Fuzzy Classifier and SDN Assistance in Fog Computing. *Security and Communication Networks*, *2024*, 1–20. https://doi.org/10.1155/2024/6651584

Berríos, S., Garcia, S., Hermosilla, P., & Allende-Cid, H. (2025). A Machine-Learning-Based Approach for the Detection and Mitigation of Distributed Denial-of-Service Attacks in Internet of Things Environments. *Applied Sciences (Switzerland)*, *15*(11). https://doi.org/10.3390/app15116012

Boukebous, A. A. E., Fettache, M. I., Bendiab, G., & Shiaeles, S. (2023). A Comparative Analysis of Snort 3 and Suricata. *2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET)*, 1–6. https://doi.org/10.1109/GlobConET56651.2023.10150141

Ghazi, D. S., Hamid, H. S., Zaiter, M. J., & Behadili, A. S. G. (2024). *Performance and efficacy of Snort versus Suricata in intrusion detection: A benchmark analysis*. 020024. https://doi.org/10.1063/5.0236936

Sahani, N., Zhu, R., Cho, J. H., & Liu, C. C. (2023). Machine Learning-based Intrusion Detection for Smart Grid Computing: A Survey. *ACM Transactions on Cyber-Physical Systems*, *7*(2). https://doi.org/10.1145/3578366

Pawlicki, M., Kozik, R., & Choraś, M. (2024). *The Impact of Data Scaling Approaches on Deep Learning, Random Forest and Nearest Neighbour-Based Network Intrusion Detection Systems for DoS Detection in IoT Networks* (pp. 197–208). https://doi.org/10.1007/978-981-97-4465-7_14

Praptodiyono, S., Firmansyah, T., Anwar, M. H., Wicaksana, C. A., Pramudyo, A. S., & Al-Allawee, A. (2023). DEVELOPMENT OF HYBRID INTRUSION DETECTION SYSTEM BASED ON SURICATA WITH PFSENSE METHOD FOR HIGH REDUCTION OF DDOS ATTACKS ON IPV6 NETWORKS. *Eastern-European Journal of Enterprise Technologies*, *5*(9(125)), 75–84. https://doi.org/10.15587/1729-4061.2023.285275

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Sajid, M., Malik, K. R., Almogren, A., Malik, T. S., Khan, A. H., Tanveer, J., & Rehman, A. U. (2024). Enhancing intrusion detection: a hybrid machine and deep learning approach. *Journal of Cloud Computing*, *13*(1). https://doi.org/10.1186/s13677-024-00685-x

Raharjo, D. H. K., & Muhammad Salman. (2023). ANALYZING SURICATA ALERT DETECTION PERFORMANCE ISSUES BASED ON ACTIVE INDICATOR OF COMPROMISE RULES. *Jurnal Teknik Informatika (Jutif)*, *4*(3), 601–610. https://doi.org/10.52436/1.jutif.2023.4.3.1013

Sawah, M. S., Elmannai, H., El-Bary, A. A., Lotfy, K., & Sheta, O. E. (2025). Distributed denial of service (DDoS) classification based on random forest model with backward elimination algorithm and grid search algorithm. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-03868-x

Tahir, M., Wahyuningsih, U., Iyan, M., Pratama, P., & Effindi, A. (2024). *Development of Network Security Using a Suricata-Based Intrusion Prevention System Against Distributed Denial of Service ARTICLE INFORMATION ABSTRACT* (Vol. 6, Number 2). http://innovatics.unsil.ac.id

Uccello, F., Pawlicki, M., D'Antonio, S., Kozik, R., & Choraś, M. (2024). *Towards Hybrid NIDS: Combining Rule-Based SIEM with AI-Based Intrusion Detectors* (pp. 244–255). https://doi.org/10.1007/978-3-031-56950-0_21

Wang, R. C., & Avrianto, R. P. (2025). Improving Detection Accuracy of Network Intrusions Using a Hybrid Network Intrusion Detection System Based on Isolation Forest and Random Forest Algorithms. *Jurnal Teknik Informatika (Jutif)*, *6*(6), 5371–5385. https://doi.org/10.52436/1.jutif.2025.6.6.4694

*name of corresponding author