Outlook

[IAAA'2026] Review for paper #1571275638 completed

From Edas Help <help@edas.info>
Date Wed 2026-04-29 2:49 PM
To Nguyễn Duy Huy <nguyenduyhuy@humg.edu.vn>

Dear Mr. Duy-Huy Nguyen,

Thank you for completing the review of the paper #1571275638 ("An XDP/eBPF-Based Zero-Copy Processing Framework for Efficient Threat Mitigation in UAV Networks") for IAAA'2026. Below is a copy of your review.

You can modify the report by going to https://edas.info/R.php?r=14101310 up to the due date of Apr 28.

Best regards,
The conference chairs

> *** Novelty and originality: Rate the novelty and originality of the ideas or results presented in the paper.
Significant original work and novel results. (4)

> *** Technical content and scientific rigour: Rate the technical content of the paper (e.g.: completeness of the
analysis or simulation study, thoroughness of the treatise, accuracy of the models, etc.), its soundness and scientific rigour.
Solid work of notable importance. (4)

> *** Quality of presentation: Rate the paper organization, the clearness of text and figures, the completeness and accuracy of references.
Well written. (4)

> *** Relevance and timeliness: Rate the importance and timeliness of the topic addressed in the paper within its area of research.
Excellent (5)

> *** Strong aspects: Comments to the author: what are the strong aspects of the paper

- The use of Zero-Copy Processing via XDP hooks at the driver level effectively eliminates the I/O bottlenecks and context-switching overhead found in traditional libraries like libpcap.
- Maintaining CPU usage under 63% and memory consumption below 115 MB under 10GbE attack conditions is impressive and crucial for "Denial of Flight" prevention.
- By relying on L3/L4 statistical metadata instead of Layer 7 payload decryption, the framework inherently

guarantees data privacy for sensitive mission telemetry.

> *** Weak aspects: Comments to the author: what are the weak aspects of the paper?

- While the simulation uses an enterprise-grade Intel Xeon server, actual deployment on embedded UAV hardware (e.g., NVIDIA Jetson or Raspberry Pi) is mentioned as a future indication rather than presented as primary experimental data.
- The authors acknowledge that the system currently relies on a static XGBoost model, which may be vulnerable to concept drift and adversarial evasion techniques (e.g., perturbing interarrival times) as attack patterns evolve.

> *** Recommended changes: Recommended changes. Please indicate any changes that should be made to the paper if accepted.

- If possible, provide preliminary performance metrics from a common embedded platform like a Jetson Orin Nano to better validate the "UAV edge" claim.
- Include a brief discussion or a small test case on how the model performs when simple adversarial perturbations are applied to the top ANOVA features (like Flow IAT Mean).
- Briefly elaborate on how the "Asynchronous Map Update" in the control plane could facilitate continuous model retraining to handle the aforementioned concept drift.

> *** Comments to the TPC: Confidential comments to the TPC (will be not sent to Authors)

This paper presents a very strong technical solution to a real-world problem in UAV security. The results are superior to existing legacy systems (Snort/Suricata), particularly in terms of CPU stability and packet drop rates. The use of modern kernel technologies (eBPF/XDP) combined with optimized ML (XGBoost) makes this a high-impact contribution suitable for the conference.

> *** Submission Policy: Does the paper list the same author(s), title and abstract (minor wording differences in the abstract are ok) in its PDF file and EDAS registration?

The same author(s), title, and abstract are listed in the PDF file and EDAS registration.

> *** Overall Recommendation: Overall Recommendation
Accepted (1)