Outlook

[IAAA'2026] Review for paper #1571272586 completed

From Edas Help <help@edas.info>
Date Wed 2026-04-29 2:23 PM
To Nguyễn Duy Huy <nguyenduyhuy@humg.edu.vn>

Dear Mr. Duy-Huy Nguyen,

Thank you for completing the review of the paper #1571272586 ("Obfuscation-Resilient Graph Extraction for Secure UAV Flight Controllers") for IAAA'2026. Below is a copy of your review.

You can modify the report by going to https://edas.info/R.php?r=14101279 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.
Good (4)

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

- Testing on over 10,000 samples across two architectures (ARM/MIPS) provides high confidence in the results.
- The implementation of GPS/IMU synthesis and MAVLink heartbeat simulation is a very practical and advanced approach to bypass hardware-awareness checks in modern malware.
- Achieving an average processing time of 32.4 seconds per sample makes this framework suitable for real-world industrial deployment.

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

- While the paper excels at explaining the extraction and integrity of the graphs, it does not provide an aggregate Accuracy/F1-score for a classifier (like a GNN) across the entire 10,598 sample dataset, relying instead on a case study.
- The look-ahead window size K=3 is chosen empirically. The paper would benefit from a more detailed analysis of how different values of K affect graph density and noise across different malware families.

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

- Add a table showing the performance (Accuracy, Precision, Recall) of a baseline Graph Neural Network using the extracted "Skip Edge" graphs versus standard sequential graphs.
- Provide a brief sensitivity analysis showing the impact of varying the window size on context preservation and computational overhead.
- Discuss the feasibility of deploying the "Skip Edge" logic for on-board, real-time detection rather than just offline analysis.

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

This is a high-quality, high-impact paper that bridges the gap between IoT malware analysis and UAV-specific hardware requirements. The "Safety Net" and "Skip Edge" mechanisms are robust contributions that significantly improve upon the state-of-the-art in automated dynamic analysis. The scale of the experiments is impressive for a conference submission.

> *** 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 author(s), title and abstract are the same in its PDF file and EDAS registration.

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