

Detecting Jamming and Spoofing Attacks on Unmanned Aerial Vehicles with Advanced Neural Network Models

Publisher: IEEE

Cite This

♪ PDF

Veernapu Sudheer Kumar; Gajendrasinh Natvarsinh Mori; Suresh Kumar K R; P Joel Josephson; N. Kumar; R Nithya All Authors

23

Full Text Views <







Abstract

Document Sections

- I. Introduction
- II. Literature Survey
- III. Proposed System
- IV. Result and Discussion

Authors

Figures

References

Keywords

Metrics

More Like This

V. Conclusion

Abstract:

Security issues have been highlighted by the widespread deployment of UAVs in both civilian and military settings due to their susceptibility to signal jamming and spoofing. Traditional UAV autopilot systems put cybersecurity last on the list of priorities. An increasing concern in smart city security systems is the vulnerability of UAVs to GPS spoofing and jamming, which can lead to signal loss, hacking, or hijacking. Because of these problems, this study suggests using the Attn-BiLSTM model for preventative and attack detection purposes. Normalisation of z-scores is the first step in preprocessing. Attribute selection using chi-square and correlation analyses. Using a CNN to extract spatial-temporal information and a BiLSTM to process them are necessary for UAV signal integrity prediction. Important aspects for the safety of UAV communications are brought to light by the attention mechanism's expansion. The proposed method achieves a prediction accuracy of 99.18%, which is higher than four leading deep learning models, according to the experimental results. By protecting UAVs against jamming and spoofing assaults, this study improves their operational security and reliability in dangerous areas, demonstrating the significance of AI in UAV cybersecurity.

Published in: 2025 Global Conference in Emerging Technology (GINOTECH)

Date of Conference: 09-11 May 2025 **DOI:** 10.1109/GINOTECH63460.2025.11076803

Date Added to IEEE Xplore: 17 July 2025 Publisher: IEEE

▼ ISBN Information: Conference Location: PUNE, India

CD:979-8-3315-0771-8 DVD ISBN:979-8-3315-0772-5 USB ISBN:979-8-3315-0774-9

Electronic ISBN:979-8-3315-0775-6

Print on Demand(PoD) ISBN:979-8-3315-0776-3

Sign in to Continue Reading

Authors

Veernapu Sudheer Kumar



Department of Mechanical Engineering, Siddhartha Academy of Higher Education, Deemed to be University, Vijayawada, India

Gajendrasinh Natvarsinh Mori

Department of MCA, The Mandvi Education Society Institute of Computer Studies, Surat, Gujarat, India

Suresh Kumar K R

Department of Information Science and Engineering, M S Ramaiah Institute of Technology, Bangalore, India

P Joel Josephson

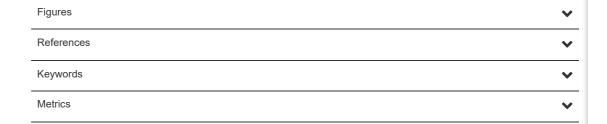
Department of ECE, Malla Reddy Engineering College, Secunderabad, Telangana, India

N. Kumar

Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamil Nadu, India

R Nithya

School of Computing Science, KPR College of Arts, Science and Research, Coimbatore, Tamilnadu, India



Back to Results



IEEE Personal Account

CHANGE USERNAME/PASSWORD **Purchase Details**

PAYMENT OPTIONS

VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES

PROFESSION AND EDUCATION

TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333

WORLDWIDE: +1 732

981 0060

CONTACT & SUPPORT

Follow



About IEEE Xplore | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting 🔀 | Sitemap | IEEE Privacy Policy

A public charity, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2025 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.