CYBER-PHYSICAL MACHINE LEARNING ARCHITECTURE FOR DETECTING CYBERATTACKS IN UAV INTRUSION DETECTION SYSTEMS

FAMU-FSU College of Engineering
CPML
FSU | FLORIDA STATE UNIVERSITY

Bianca Avlonitis, Salma Aboelmagd, and Dr. Abdulrahman Takiddin

FSU UNDERGRADUATE RESEARCH OPPORTUNITY PROGRAM
CENTER FOR UNDERGRADUATE RESEARCH & ACADEMIC ENGAGEMENT

Introduction

Unmanned Aerial Vehicles (UAVs), also known as drones, are being explored in the following areas:

- Package/Cargo Delivery [1]
- Soil Monitoring, and Crop Watering [2]

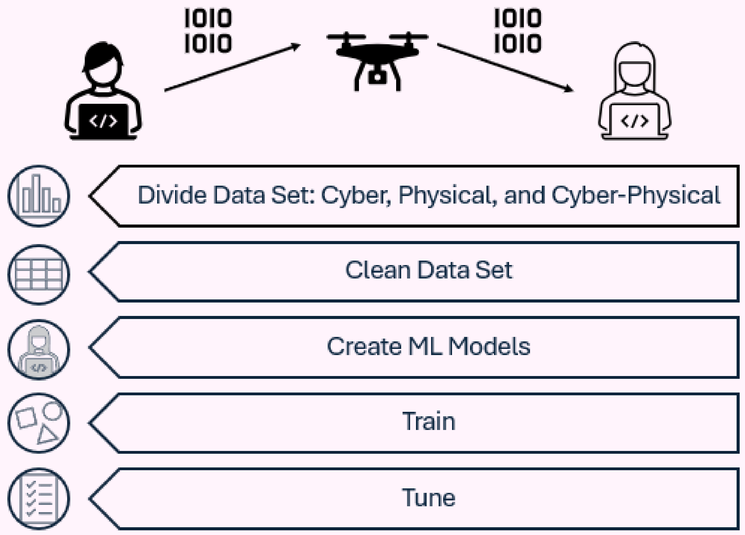
Before adopting these UAV applications, it is essential to assess associated risk factors [3], including cyberattacks [4].

- Denial-of-service: Flood a system with requests until it slows down or crashes.
- Replay: Old data is sent as new data.
- Evil Twin: Establishing a fraudulent access point capable of collecting sensitive information from connected devices.
- False Data Injection (FDI): Skewed data is injected into the system to confuse.

Objective

- Current research examines the cyber effects of cyberattacks on UAVs, but overlooks the physical effects.
- To bridge the cyber-physical gap in research, the cyber-physical effects of cyberattacks on the UAV Intrusion Detection System (IDS) will be considered.
- **Will ML models yield the highest F1 scores on cyber, physical, or cyber–physical data from a UAV IDS? What models will perform best in terms of accuracy, precision, and F1 scores?**
- ML models are expected to perform best with the cyber-physical dataset.
- Recurrent and Convolutional Neural Networks are expected to yield the highest overall scores.

Methodology



Results

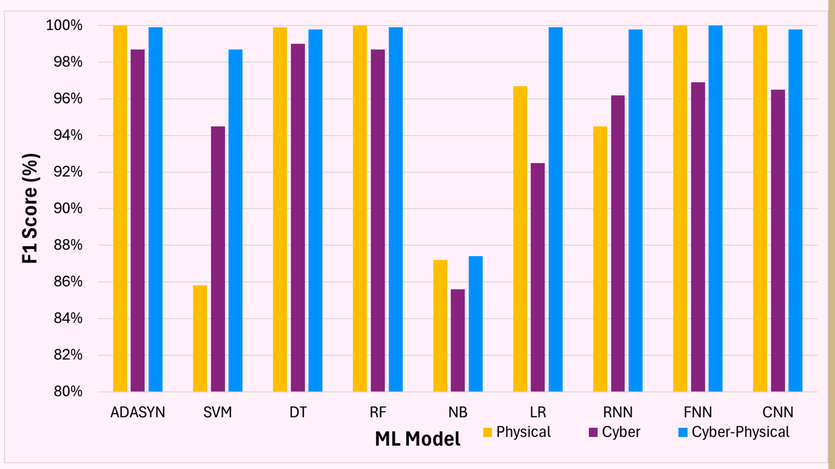


Figure 1: F1 Score (%) Comparison Based on ML Model for Physical, Cyber, and Cyber-Physical Datasets

Results Continued

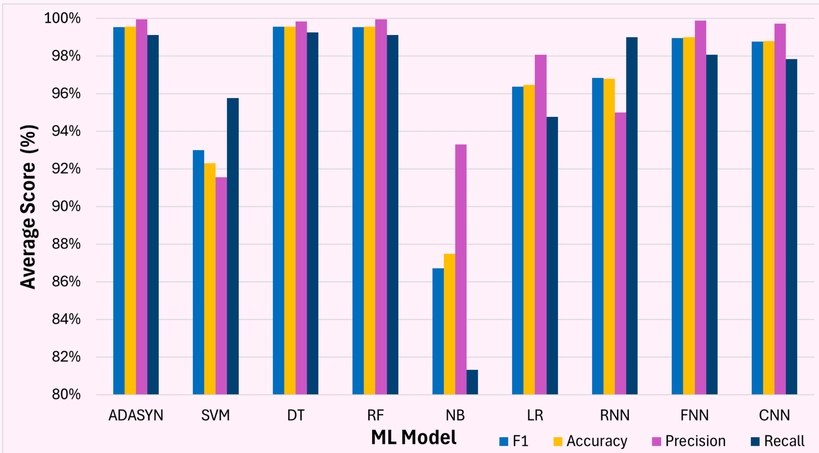


Figure 2: Average Score (%) Among all Datasets Compared to ML models for F1, accuracy, precision, and recall

Discussion & Conclusion

- ML models train best on cyber-physical data.
- RNN and Decision Tree models yield the highest overall scores (accuracy, precision, recall, and F1)
- UAV IDS should consider implementing RNN, DT, and RF architectures.
- This provides insight into how UAV systems can uphold higher cybersecurity standards.
- Moving forward, it is essential to test more cyberattacks, such as GPS jamming or SQL injections.

References

Please scan the following QR code.

Acknowledgements

I would like to thank the Undergraduate Research Opportunity Program for this wonderful opportunity to explore academic research. Additionally, I would like to thank Dr. Takiddin and Salma Aboelmagd for their support and guidance throughout the process.