PHÁT HIỆN GIẢ MẠO TÍN HIỆU GPS TRONG PHƯƠNG TIỆN TỰ HÀNH SỬ DỤNG MÔ HÌNH HỌC MÁY BÁN GIÁM SÁT CNN

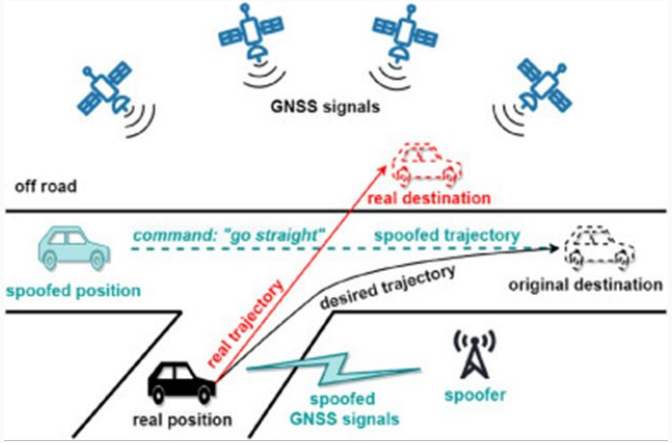
Ngô Thái Hưng - 230202006

Tóm tắt

- Lớp: CS2205.MAR2024
- Link Github: https://github.com/ESTA-2509/CS2205.DeCuong.FinalReport.git
- Link YouTube video: https://youtu.be/IoTLNu0f9K8
- Ảnh + Họ và Tên: Ngô Thái Hưng
- Tổng số slides không vượt quá 10

Giới thiệu

- Sự phụ thuộc vào GPS khiến các phương tiện tự hành (AVs) dễ bị tấn công giả mạo GPS (GPS spoofing), dẫn đến hậu quả nghiêm trọng như mất kiểm soát hoặc tai nạn. Do đó, phát hiện và ngăn chặn các cuộc tấn công này là rất cần thiết.



Hình 1. Cuộc tấn công giả mạo GPS nhằm vào xe tự hành[4]

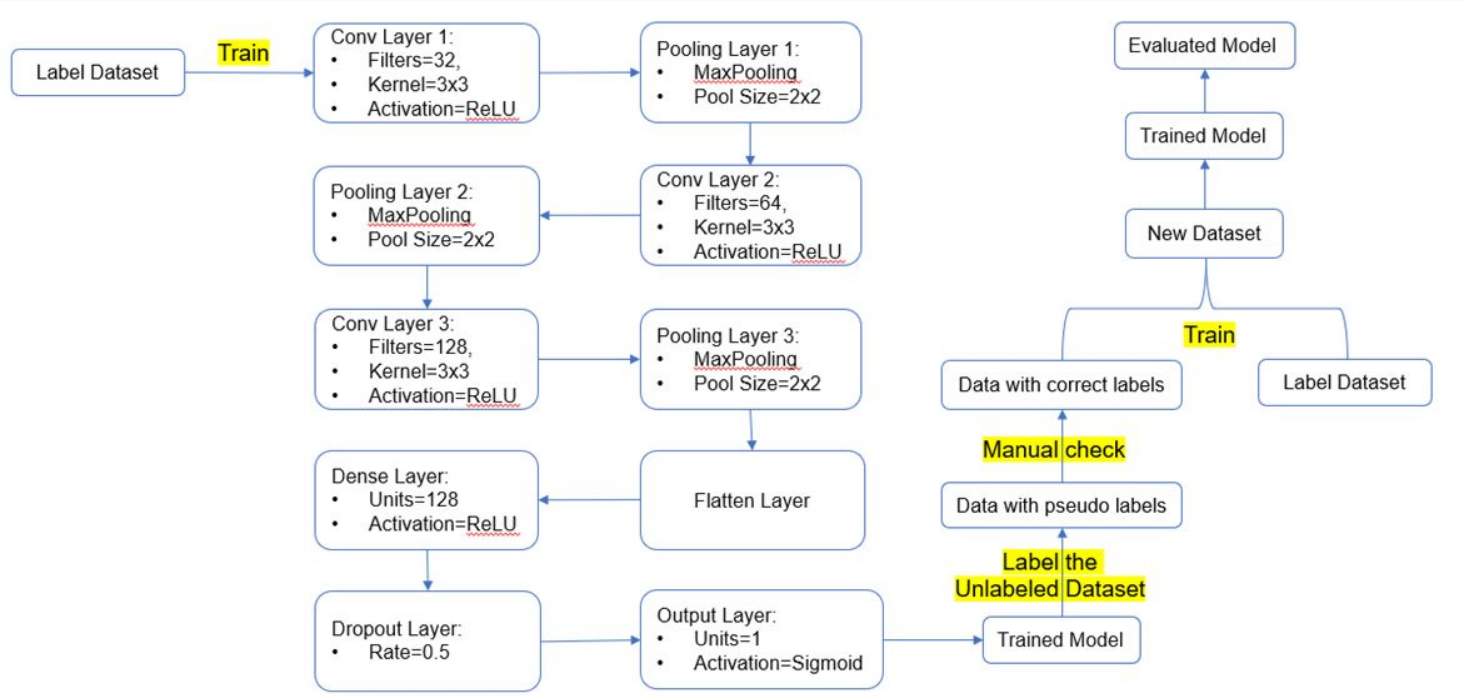
Mục tiêu

- Xây dựng model phát hiện tín hiệu giả mạo GPS: Phát triển và đánh giá một hệ thống có khả năng phát hiện và xác định các tín hiệu GPS bị giả mạo sử dụng bộ dataset có gán nhãn, phân phối cân bằng “A DATASET for GPS Spoofing Detection on Autonomous Vehicles [1]” để huấn luyện.
- Nâng cao khả năng tổng quát của mô hình thông qua việc sử dụng dữ liệu mô phỏng không nhãn, giúp mô hình học hỏi tốt hơn và tăng khả năng thích ứng với các tình huống mới.
- Kiểm thử và áp dụng hệ thống trong môi trường thực tế: Thực hiện các thử nghiệm và đánh giá hiệu suất của hệ thống trong các tình huống và môi trường thực tế khác nhau, đảm bảo hệ thống có thể hoạt động ổn định và hiệu quả trên các phương tiện tự hành.

Nội dung và Phương pháp

- Phát triển mô hình học máy CNN hiệu quả cho việc phát hiện giả mạo tín hiệu GPS trong phương tiện tự hành sử dụng dữ liệu tín hiệu GPS có nhãn từ A DATASET for GPS Spoofing Detection on Autonomous Vehicles [1].
- Theo dõi và điều chỉnh các tham số huấn luyện để tối ưu hóa hiệu suất mô hình.
- Nâng cao khả năng tổng quát của mô hình thông qua việc sử dụng dữ liệu mô phỏng không nhãn sử dụng các công cụ mô phỏng như CARLA để tạo ra dữ liệu tín hiệu GPS.
- Thiết kế kịch bản thử nghiệm và tối ưu hóa mô hình.

Nội dung và Phương pháp



Hình 2. Mô hình hệ thống máy học CNN bán giám sát đề xuất

Kết quả dự kiến

- Mô hình học máy bán giám sát CNN có khả năng phân biệt chính xác giữa tín hiệu GPS thực và giả mạo với độ chính xác cao, độ nhạy cao và độ đặc hiệu cao.
- Hệ thống có khả năng thu thập, xử lý và phân loại tín hiệu GPS theo thời gian thực và có thể được tích hợp dễ dàng vào các hệ thống lái tự động hiện có.
- Phát triển các thuật toán học máy bán giám sát mới hiệu quả hơn cho các bài toán phân loại khác.

Tài liệu tham khảo

[1] S. B. H. E. A. a. N. K. Ghilas Aissou, "A DATASET for GPS Spoofing Detection on Autonomous Vehicles," 19 11 2022. [Online]. Available: http://ieee-dataport.org/documents/dataset-gps-spoofing-detection-autonomous-vehicles.

[2] S. B. H. E. A. a. N. K. Ghilas Aissou, "A DATASET for GPS Spoofing Detection on Autonomous Vehicles," 19 11 2022. [Online]. Available: http://ieee-dataport.org/documents/dataset-gps-spoofing-detection-autonomous-vehicles.

[3] X. Sun, F. R. Yu, P. Zhang, "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)," IEEE Transactions on Intelligent Transportation Systems, vol. 23, 2022.

[4] S. V. T. S. P. Vipin Kumar Kukkala, Roadmap for Cybersecurity in Autonomous Vehicles, 2022.

[5] H. W. C. X. Peng Jiang, "DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network," Digital Communications and Networks, 2021.

[6] P. S. Pranav Singh Chib, "Recent Advancements in End-to-End Autonomous Driving using Deep Learning: A Survey," IEEE Transactions on Intelligent Vehicles, vol. 9, no. 1, pp. 103 - 118, January 2024.

[7] C. Guo, H. Yang, D. Huang, J. Zhang, N. Dong, J. Xu and J. Zhu, "Review Sharing via Deep Semi-Supervised Code Clone Detection," IEEE Access, 2020.