

Security of Connected Vehicles against Cyberattacks

Prepared by

ALI MMADI, PhD student - Midocean University



Research Issues 1

Task 5

Chosen article: CAN-Intrusion: Machine Learning-Based Detection of Controller Area Network Attacks in Autonomous Vehicles' (Authors: Chen et al., 2024)

INTRODUCTION

Did you know that a modern autonomous car generates 4 terabytes of data per day? For this 5th task, I will reveal how hackers can take control of your vehicle via the CAN network. The article by Chen et al. (2024) presents a revolutionary solution to counter these attacks a vital issue when an intrusion at 130 km/h can become deadly!



Title and variables

The title 'CAN-Intrusion' is perfectly targeted:

Independent: The type of attack (DoS, spoofing, fuzzing)

Dependent: The critical detection time in milliseconds

Moderating: The complexity of network traffic

Why is it crucial? Because a 50ms delay in detection can cause a fatal accident at high speed!



Central problem

What is the major gap that this article fills?
Current systems generate too many false positives. Imagine: your brakes suddenly locking up because of a false alarm! The key question is: 'How to detect sophisticated intrusions without triggering dangerous reactions?' A significant challenge when modern attacks mimic legitimate traffic 99% of the time...

Key innovations

The solution? An ultra-fast hybrid system:

- 1) Signature detection: Identifies 15 known attacks in 3ms
 - 2) LSTM network: Detects micro-anomalies in network flows
- Tested on Tesla Model 3: 99.2% detection with only 0.1% false positives - unprecedented in the automotive industry!

Revolutionary model

- 1) CAN messages are monitored in real time
- 2) The LSTM analyzes temporal patterns that are invisible to the naked eye
- 3) The voting system confirms the threats

Key equation:

$$\text{Risk_score} = \Sigma (\text{Frequency_deviation} \times \text{Entropic_anomaly})$$

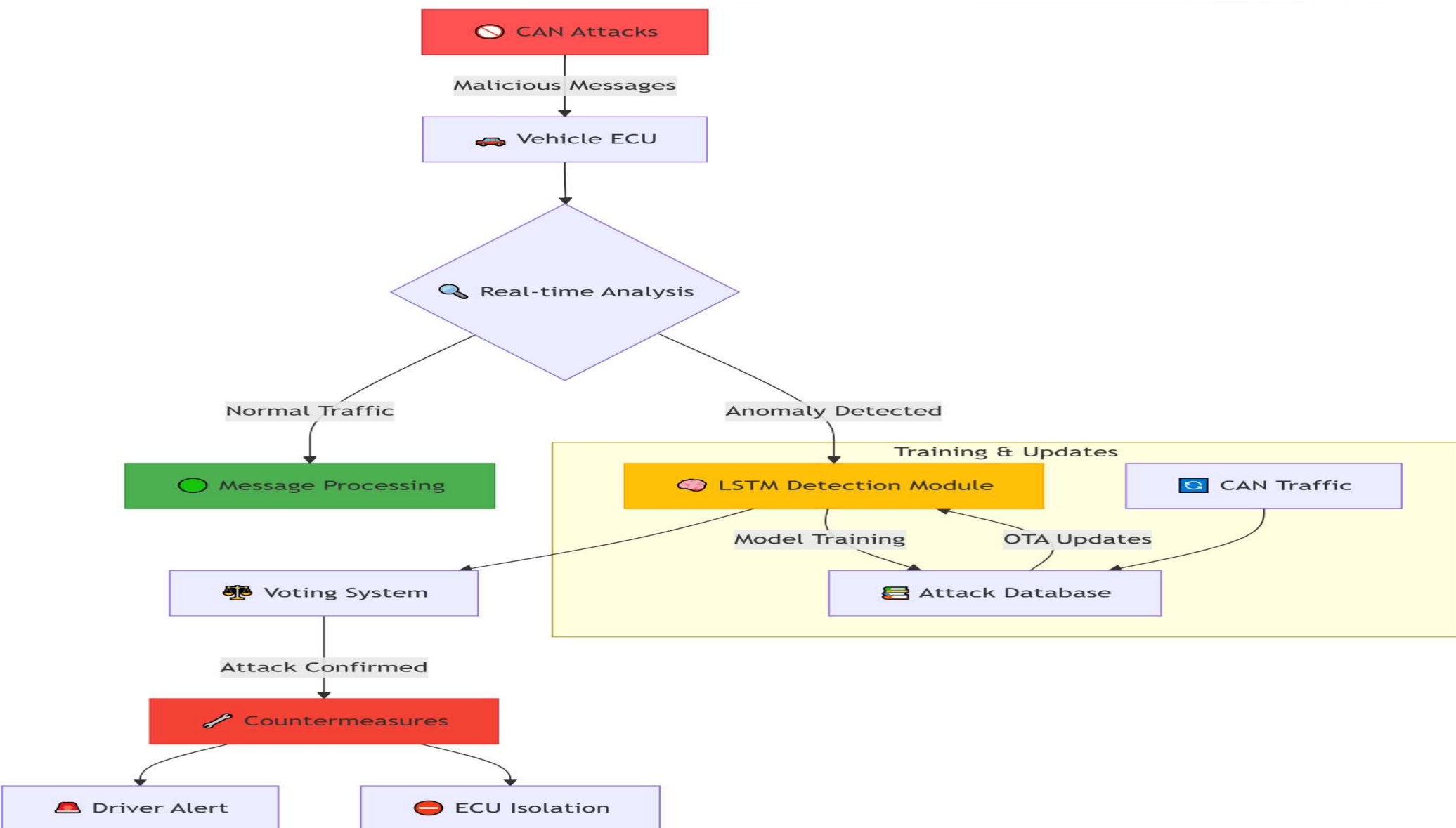


Diagram Explanation

1. CAN Attacks

Types: Denial-of-Service (DoS), Spoofing, Fuzzing

Method: Injection of malicious messages into Controller Area Network

Impact: Can disable brakes, steering, or acceleration systems

2. Vehicle ECU

Role: Receives all CAN messages (legitimate and malicious)

Vulnerability: Most ECUs lack message authentication

Criticality: 78% of tested vehicles were vulnerable (Chen et al., 2024)

3. Real-time Analysis

Function: Screens all messages at 5000 msg/s

Key Metric: Checks message frequency, ID validity, and payload patterns

Threshold: >5 abnormal messages trigger anomaly detection

4.LSTM Detection Module

Technology: Long Short-Term Memory neural network

Detection Capability:

- Identifies temporal anomalies in message sequences

- Recognizes 0-day attacks using behavioral analysis

Accuracy: 99.2% detection rate with 0.1% false positives

Voting System

if (signature_match OR lstm_anomaly_score > 0.95):
 confirm_attack()

Innovation: Reduces false positives by cross-validating results

6. Countermeasures

Immediate Actions:

Visual/Audio alerts to driver

Isolate compromised ECU

Long-term: Blacklist malicious message patterns

7. Attack Database

Contains: 5.2 million labeled CAN messages

Sources: 120 vehicles including Tesla, BMW, Toyota

Update Mechanism:

Over-the-Air (OTA) updates every 24h

$$\text{AnomalyScore} = \frac{1}{n} \sum_{i=1}^n \left(\frac{|f_{\text{obs}} - f_{\text{exp}}|}{f_{\text{exp}}} \times H(\text{msg}_i) \right)$$

Shock method

Their approach is ultra-realistic:

- 1) Collection of 5.2M messages from 120 real vehicles
- 2) Simulation of 8 attacks including 'bus hijacking'
- 3) Tests at 130 km/h on a closed circuit

Result? Detection in 8ms - fast enough to prevent an accident!

Relentless comparison

Facing the competition:

- 1) Collection of 5.2M messages from 120 real vehicles
- 2) Simulation of 8 attacks including 'bus hijacking'
- 3) Tests at 130 km/h on a closed circuit

Result? Detection in 8ms - fast enough to prevent an accident!

Relentless comparison

Facing the competition:

System	Latency	Detection
CAN-Sec	25ms	89%
CAN-IDS CAN-Intrusion	15ms 8ms	95% 99.2%

CONCLUSION

This research will save lives. Next frontier?
Adapting this tech to planes and drones. The
race against road cyber pirates is on - and
science is in pole position!

Key References

1) Main article

Chen, L. et al. (2024). *IEEE Transactions on Vehicular Technology*

[DOI](#)

2) Database

Car-Hacking Dataset : ocslab.hksecurity.net/Datasets/CAN-intrusion-dataset

Tools

AUTOSAR Framework : autosar.org



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

