Intelligent Mobile Device Lab @KSU

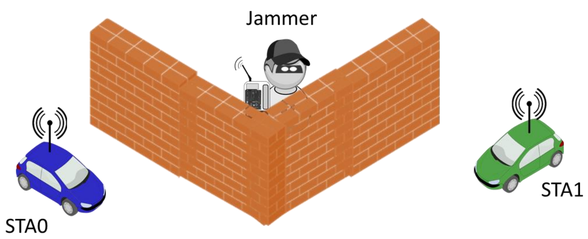
Detecting Primitive Jamming Attacks using Machine Learning in Vehicle-to-Everything Networks

Dr. Billy Kihei, Hakeem Wilson, and Muhamed Fall
Research Mentor: Dr. Billy Kihei

Department of Electrical and Computer Engineering
KENNESAW STATE UNIVERSITY

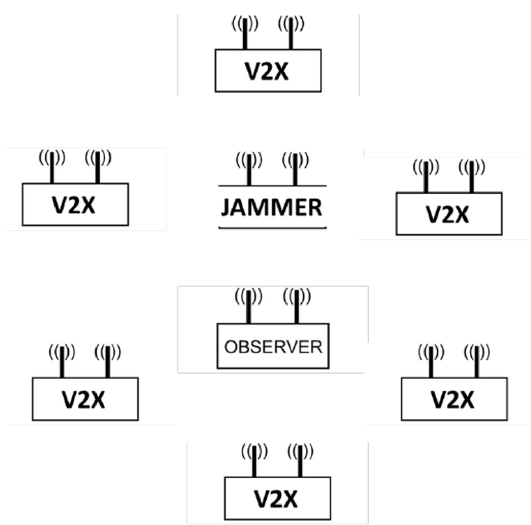
Problem

Vehicle-to-Everything (V2X) communications can enable safer roads, however, V2X is susceptible to jamming attacks.

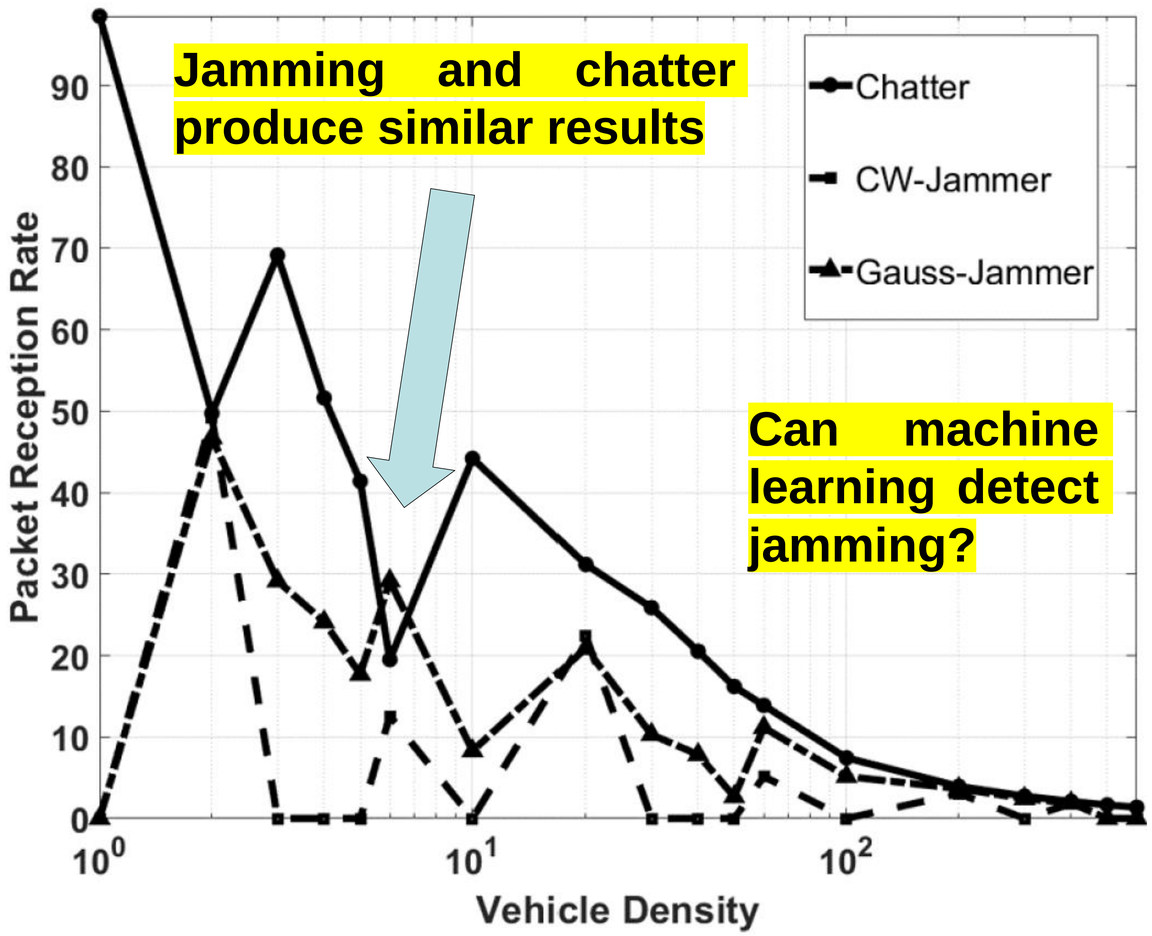


Solution

Use signal processing and machine learning (ML) to detect and classify the type of jamming.



Methodology



Jamming can appear in two forms: **Continuous Wave (CW) Jammer** and **Gaussian Noise Jammer**.

Jamming can **mimic** normal radio chatter.

A machine learning algorithm was trained to detect jamming.

Results

Accuracy: 99.84%

Classify between:

Chatter
CW-Jammer
Gauss-Jammer
Noise

ML Model:
k-Nearest Neighbors (kNN)

Key ML features:

Time series
Fast Fourier Transform
Cepstral coefficients

Implications

Light-weight ML model can **accurately** and **reliably** detect jamming in V2X.

Save lives by detecting jamming.

Improve user trust in V2X technology.

Submitted to IEEE SPAWC 2020