LOCoCAT: Low-Overhead Classification of CAN Bus Attack Types

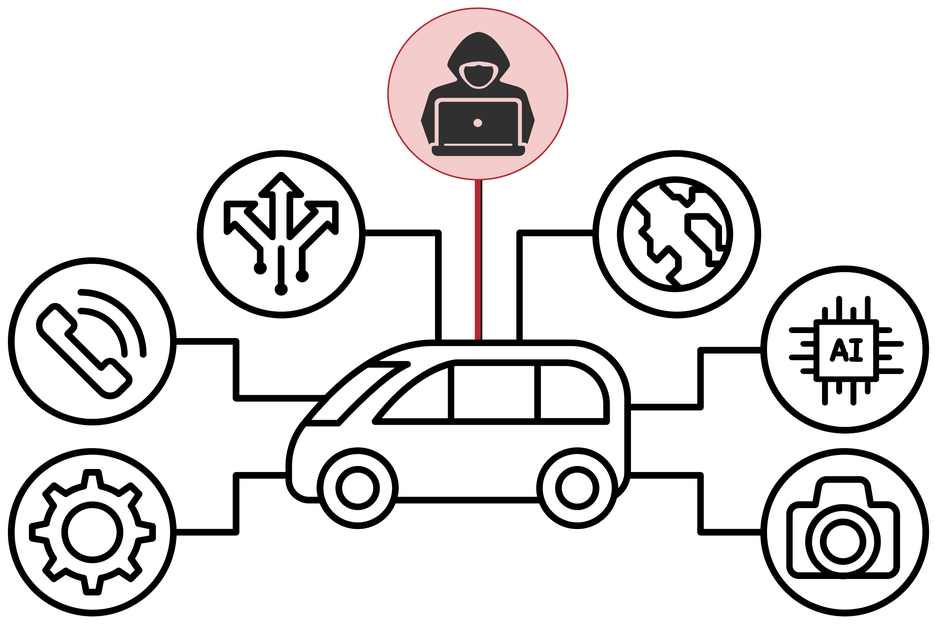
Caio Batista de Melo (cbatista@uci.edu) and Nikil Dutt (dutt@ics.uci.edu)
University of California, Irvine

1) CAN Bus Attacks

- Modern cars can have 70+ ECUs [1]

- The standard to connect ECUs is the CAN Bus, which is vulnerable to intruders/attacks

- Most work in the literature has focused on only detecting CAN Bus attacks, disregarding types



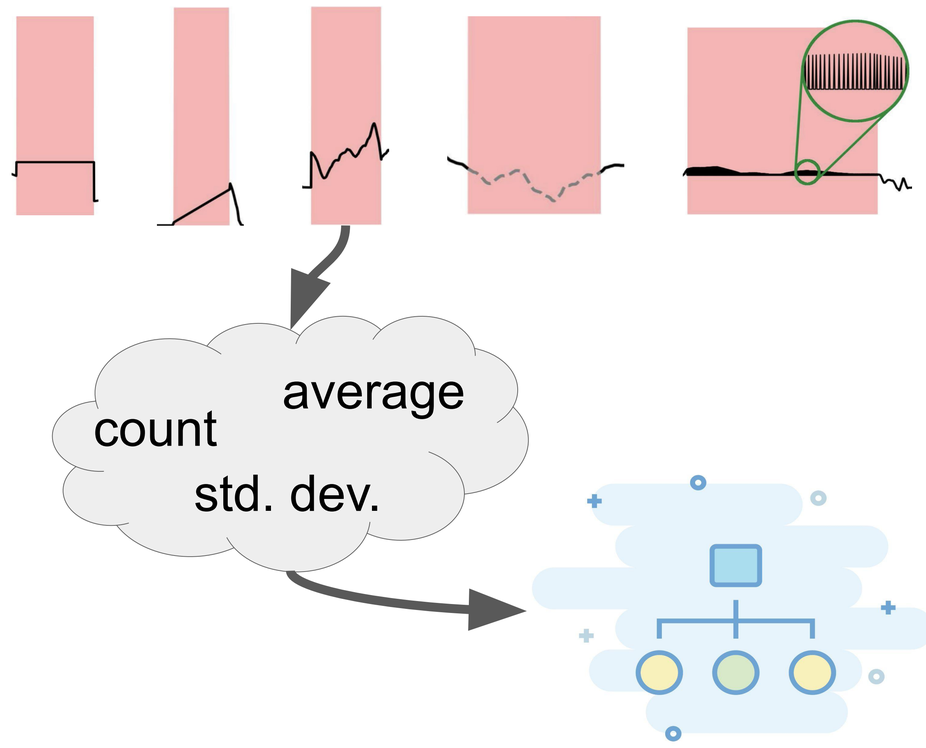
- The few works that distinguish between attack types [2, 3] do not consider the overhead added by their approaches

2) LOCoCAT

- Group messages from an attack into blocks

- Extract features from each block

- Use lightweight models to classify featureset



3) Experimental Results

Model	Car-Hacking	Survival	SynCAN	Latency	Size
LSTM [2]	100%	99.26%	41.04%	35.21 ms	4 MB
MLP3 [3]	98.75%	100%	44.03%	5.07 ms	45.3 KB
LOCoCAT	**99.16%**	**100%**	**77.98%**	**5.30 ms**	**4.0 KB**

Acknowledgements: This work was partially supported by the following NSF grants: IPF grant CCF-1704859, and SARE EAGER grant ECCS-2028782.

1: Hegde et al., *"An Insight into the Hardware and Software Complexity of ECUs in Vehicles"*, ACITY 2011
2: Hossain et al., "LSTM-Based Intrusion Detection System for In-Vehicle Can Bus Communications", IEEE Access 2020
3: Amato et al., "Can-bus attack detection with deep learning", IEEE Transactions on Intelligent Transportation Systems 2021