Real-Time Modeling for Intrusion Detection in Automotive Controller Area Network

Habeeb Olufowobi Gedare Bloom Clinton Young Joseph Zambreno

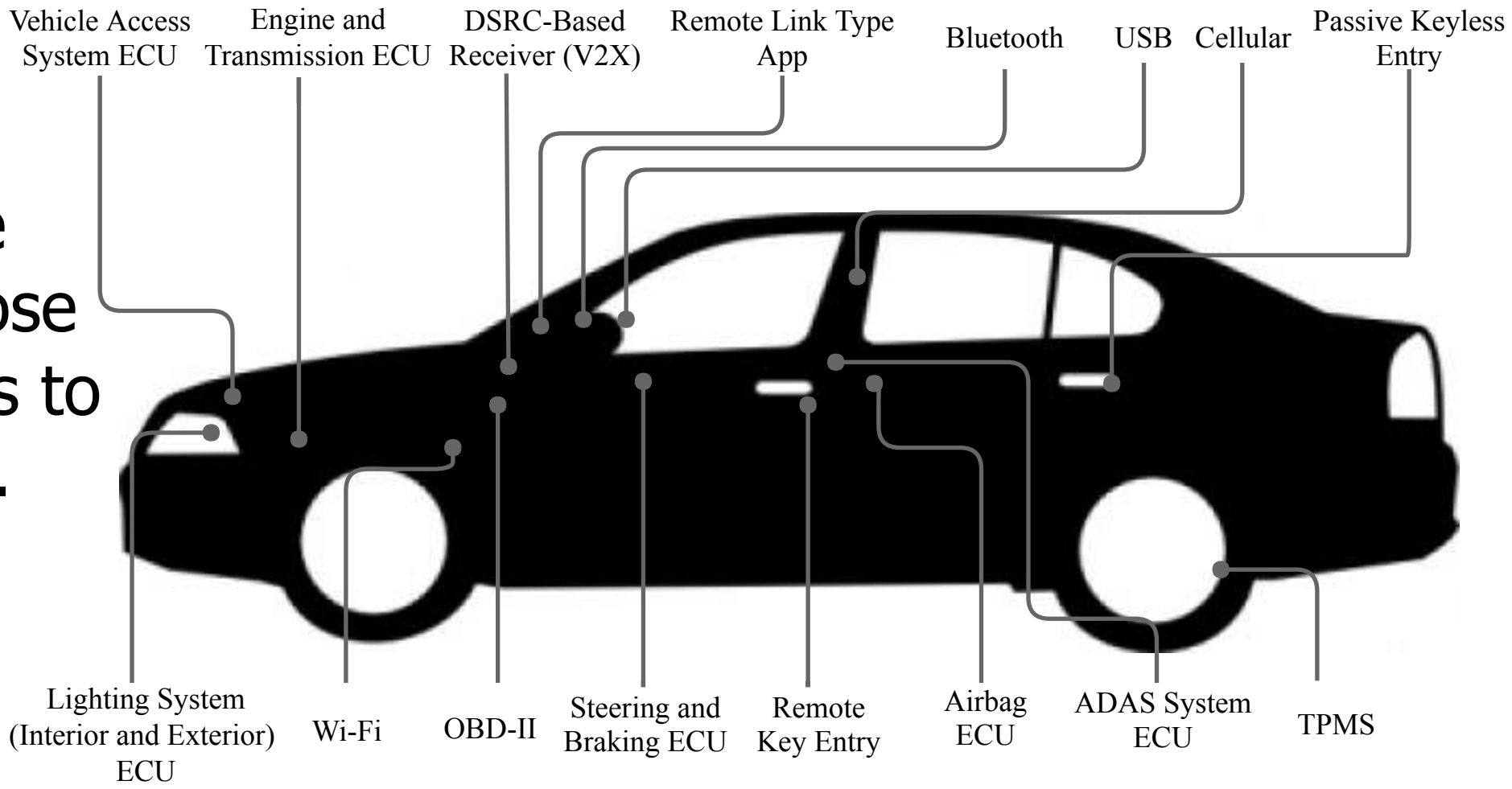
Howard University Iowa State University

RTSS 2018, Nashville, TN

Motivation

Interconnection of the automotive in-vehicle network with the outside world poses a significant security risk.

Modern vehicle interfaces expose driving systems to **cyberattacks**.



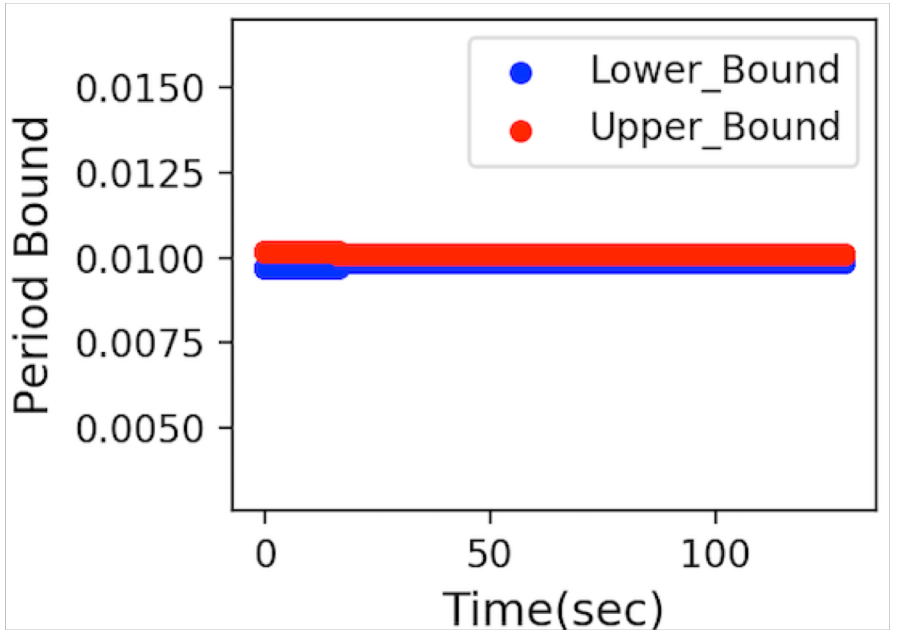
Approach

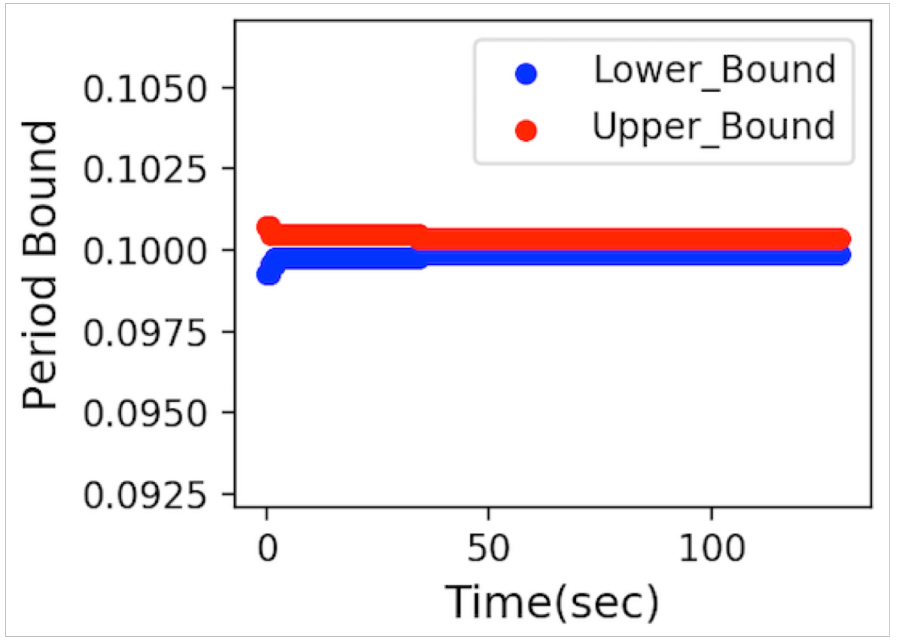
Timing Model Reconstruction

We observe CAN messages and infer real-time model parameters (periods) iteratively.

Specification-based IDS

We use inferred periods with response time analysis as a specification of the normal behavior to detect injected messages.





Preliminary Results

Cars	TN	FP	FN	TP	Precision	Recall
X	485467	624	620	6331	0.91	0.91
	323666	276	152	1672	0.86	0.92
	241056	101	95	2446	0.96	0.96
	246650	91	308	1379	0.94	0.82
	239047	60	208	2424	0.98	0.92
Y	345451	330	130	1019	0.76	0.89
	327310	294	122	2433	0.89	0.95
	381383	524	230	1933	0.79	0.89
	337086	489	1	1293	0.73	0.99

Conclusion and Future Work

- We propose a specification-based intrusion detection system for automotive in-vehicle networks.
  - Uses response time analysis of CAN as the specification
  - Estimates message periods online in a black-box approach
- We have evaluated our approach experimentally on datasets generated from the CAN busses of two different cars.
- We are improving our algorithms and real-time model to reduce false positives and accommodate aperiodic messages.