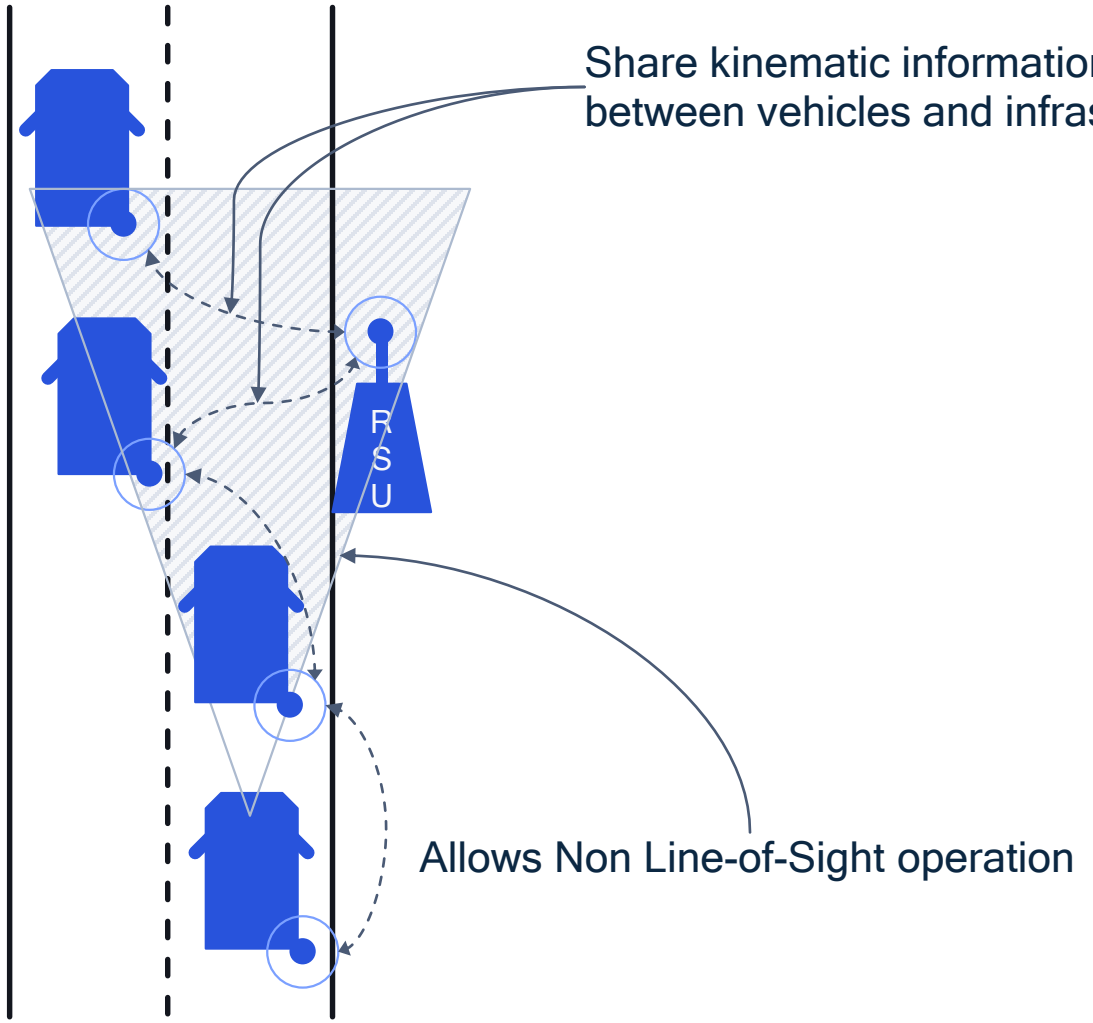
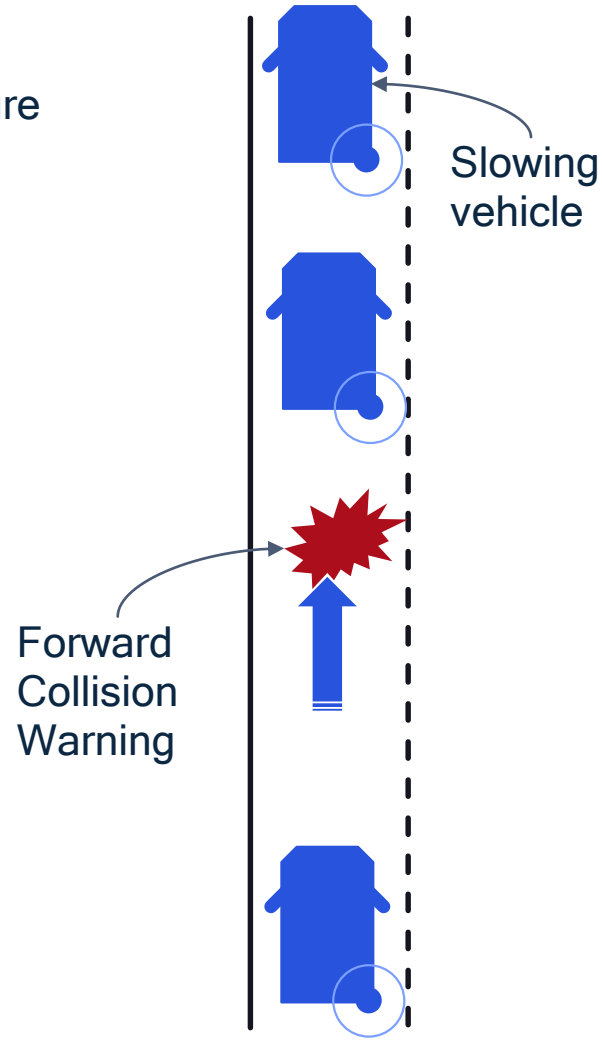
VASP: V2X Application Spoofing Platform

Mohammad Raashid Ansari, Jonathan Petit, Jean-Philippe Monteuuis, Cong Chen
Qualcomm Technologies, Inc.

ransari@qti.qualcomm.com

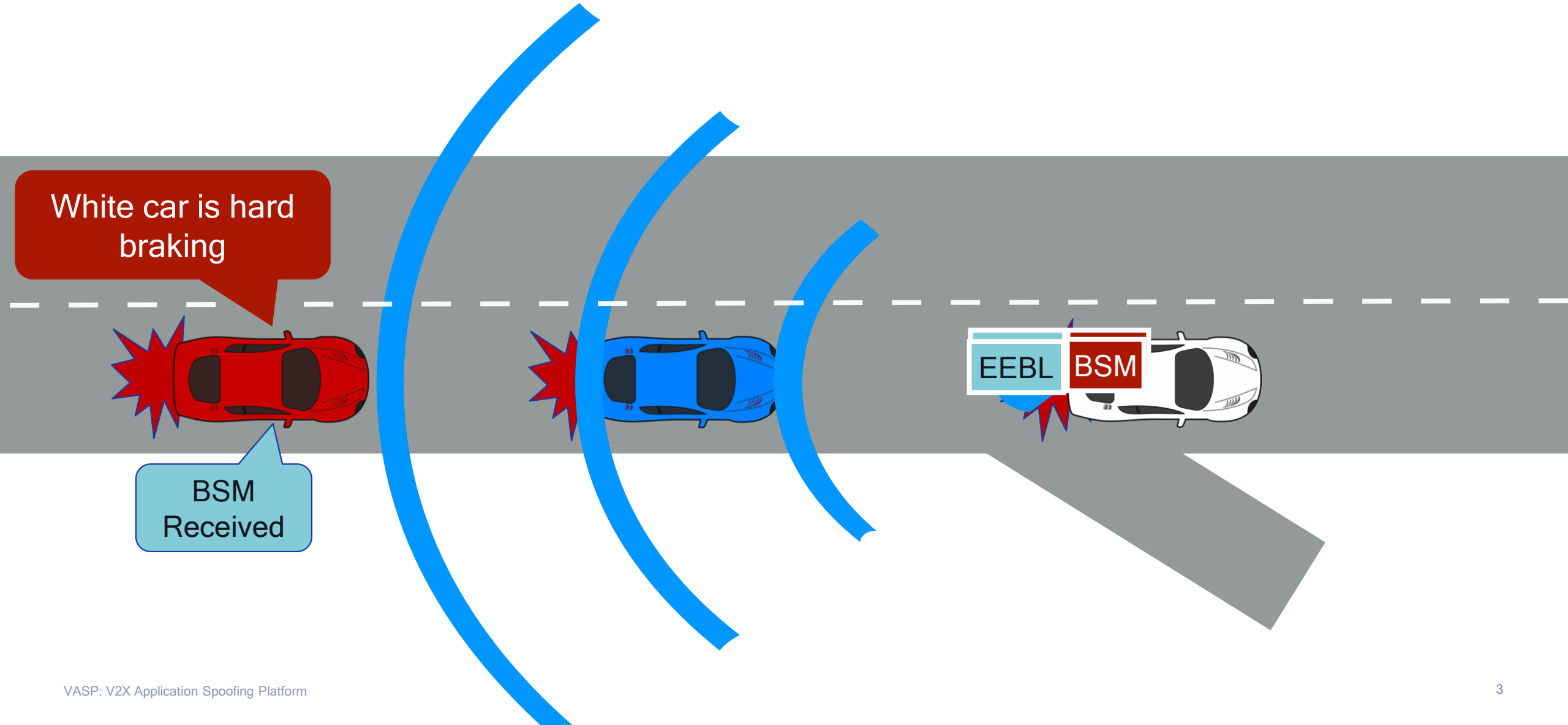
Vehicle to Everything (V2X) Communication



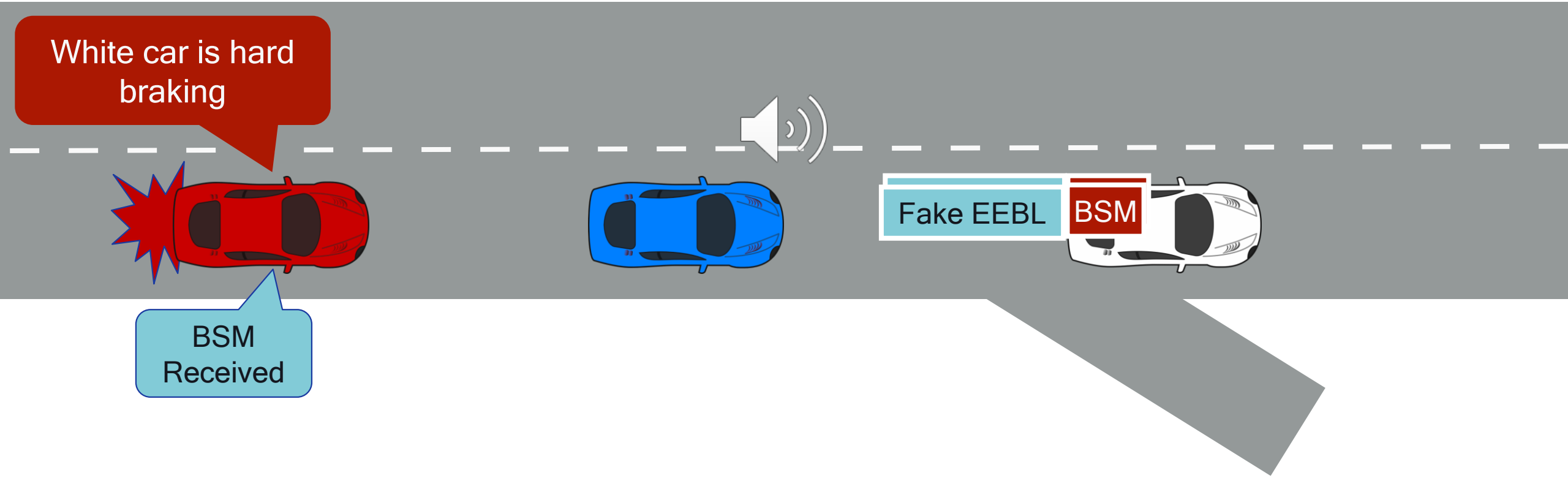


Potential to
save lives

Example (Emergency Electronic Brake Light)



Example (Fake EEBL)



V2X Security

- Data integrity and security is important for proper functioning of the whole V2X system
- Malicious insider actor could perform carefully crafted attacks to cause reactions from vehicles that may be harmful for traffic flow
- To ensure data quality, and hence proper action, V2X data must be authenticated and correct.

- Misbehavior Detection Systems (MDS) help ensuring correctness of data
- Tools to test MDS
  - VeReMi (2018, extension in 2020)
  - F2MD (2020)
  - VASP ← this paper

Prior Work

VeReMi – Vehicular Reference Misbehavior (VeReMi) dataset

- Dataset for the evaluation of misbehavior detection mechanisms for VANETs
- Only 5 attacks implemented, all position based
- No directly usable source code for writing new attacks and generating data from them
- Data from single road network – LuST scenario
- No V2X data consuming applications to test upon

F2MD – Framework for Misbehavior Detection

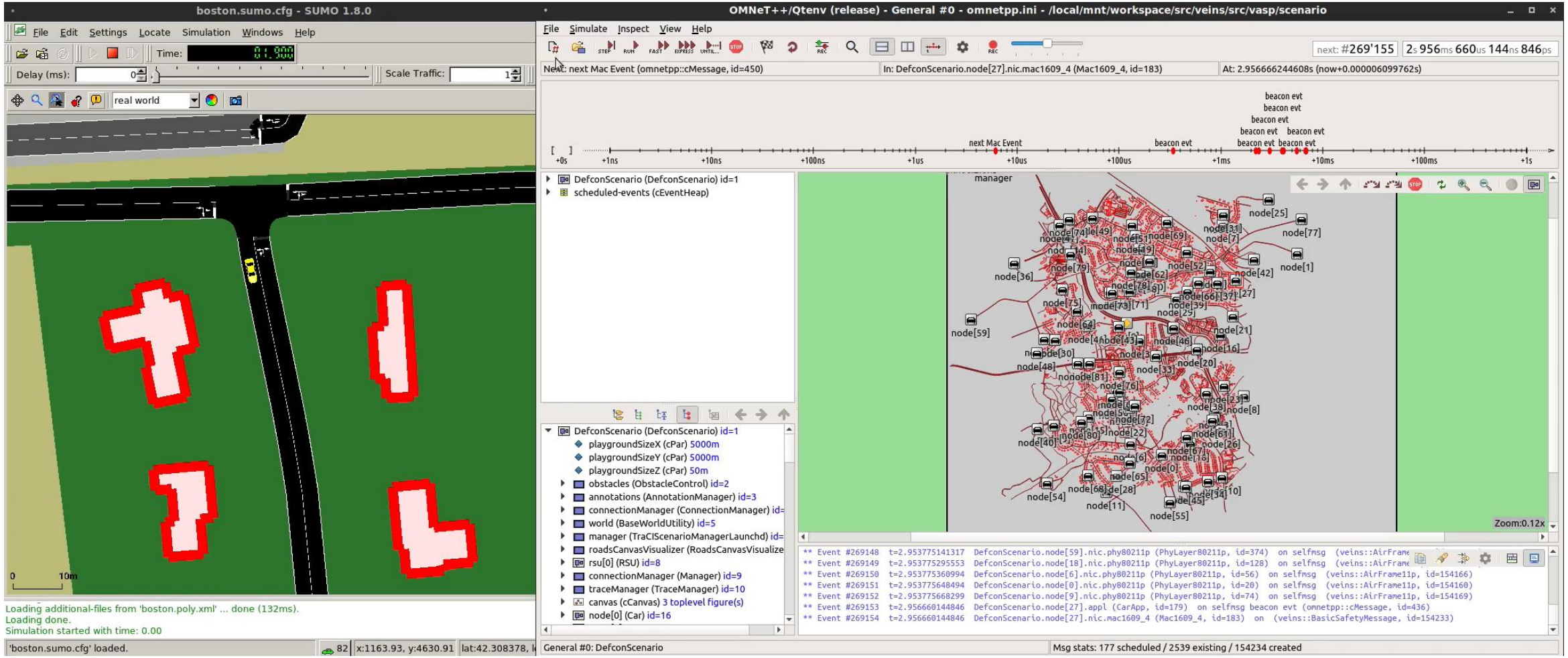
- Contains 20 attacks and 16 detectors
- Difficult to install and get started
- Cumbersome to implement new attacks – steep learning curve
- No V2X data consuming applications to test upon
- Little to no documentation

VASP: V2X Application Spoofing Platform

- Open-Source @ https://github.com/quic/vasp
- Integrates modularly to the VEINS simulator (instructions in the repo)
- 68 attacks covering more fields of a BSM that can be attacked
- Well-documented if you want to add new attacks
- Easy to add new road networks and simulate

		VeReMi	F2MD	VASP
# of attack		5	20	68
Attack Strategy	Persistent	x	x	x
	Sporadic	-	-	x
Attacked BSM Fields	Position	x	x	x
	Speed	-	x	x
	Heading	-	-	x
	Size	-	-	x
Attacks on V2X applications	EEBL	-	-	x
	IMA	-	-	x

VASP: V2X Application Spoofing Platform



System Model

All vehicles transmit Basic Safety Messages (BSM) with location and kinematic information

Vehicles have BSM consuming applications such as EEBL, IMA

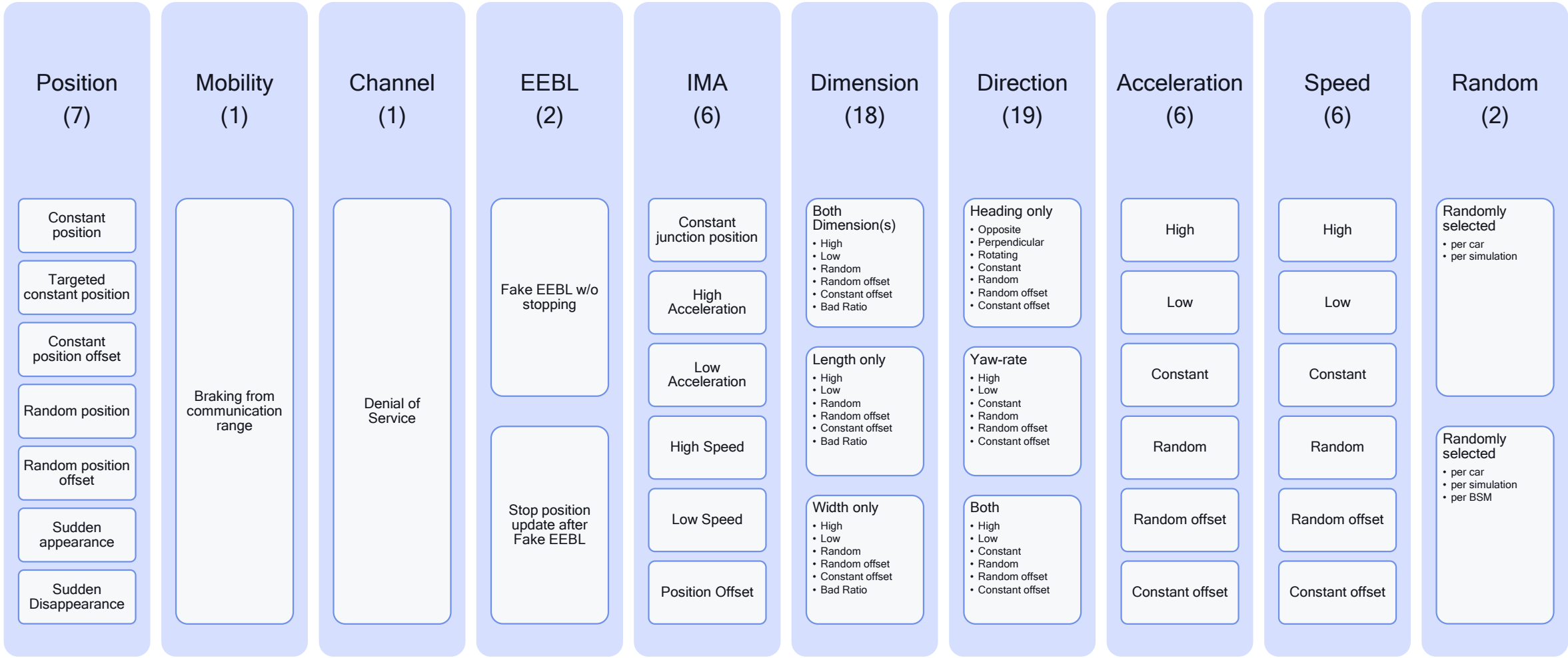
Applications implemented based on SAE J2945/1 spec

Attacker Model

Internal attacker that has all credentials to actively participate in V2X communication, rationally launch targeted and local attacks

BSM Attacks (68)

Attacker can lie about its own kinematic state or create ghost vehicle(s)



Attack Policies

When to attack

Persistent

- Every message is an attack message

Sporadic

- Attack messages are transmitted using a probability distribution to make attacks seem random and stealthy

F2MD and VeReMi only have Persistent attackers

Threat analysis

- We assessed risk of the attacks based on the following table:

Criteria	High	Medium	Low
Reproducibility	The attack is easily reproducible	The attack is reproducible with some limitations	The attack is hard to reproduce due to its complexity or operational cost.
Impact	The attack infects the system and can lead to catastrophic damage (e.g., an accident)	The attack infects the system and can lead to moderate damage (e.g., traffic jam)	The attack has no impacts on the system but can inflict minor harm
Stealthiness	Unknown attack occurs in certain applications	The attack needs several misbehavior detectors, message types, or data sources to be detected	Broadcasted information readily explain the misbehavior

Detector Evaluation

Good Result

Bad Result

- $c(p,r,f1) = \begin{cases} Low, & 0.0 \leq p,r,f1 < 0.6 \\ Medium, & 0.6 \leq p,r,f1 < 0.8 \\ High, & 0.8 \leq p,r,f1 < 1.0 \end{cases}$
  - c = Performance Level
  - p = Precision
  - r = Recall
  - $f1$ = F1-score
- F2MD and VeReMi do not cover majority of attacks on other fields than position and speed since they do not have high quality detectors for those fields
- Using VASP we designed detectors to protect these fields and shift the coverage towards a little high-quality detectors

		F2MD			VeReMi			VASP		
	∑	Low	Med	High	Low	Med	High	Low	Med	High
Constant	16	6.25%	0.00%	18.75%	6.25%	0.00%	6.25%	62.50%	0.00%	37.50%
Random	18	0.00%	5.56%	11.11%	0.00%	5.56%	5.56%	33.33%	22.22%	44.44%
High	7	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.00%	0.00%	100.00%
Low	7	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	57.14%	0.00%	42.86%
Position	7	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	28.57%	0.00%	71.43%
Speed	6	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	66.67%	16.67%	16.67%
Acceleration	6	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	33.33%	33.33%	33.33%
Heading (H)	7	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	85.71%	0.00%	14.29%
Yaw Rate (YR)	6	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	50.00%	0.00%	50.00%
H-YR	6	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	66.67%	0.00%	33.33%
Dimension	18	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	16.67%	0.00%	83.33%
Bad Ratio	3	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.00%	0.00%	100.00%
EEBL	2	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.00%	50.00%	50.00%
IMA	6	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	16.67%	0.00%	83.33%
Mobility	1	100.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	100.00%	0.00%
Channel	6	16.67%	0.00%	83.33%	100.00%	0.00%	0.00%	0.00%	0.00%	16.67%
Random Select	2	0.00%	0.00%	50.00%	100.00%	0.00%	0.00%	50.00%	0.00%	50.00%
∑(Overall)	68	82.35%	1.47%	16.18%	95.59%	1.47%	2.94%	36.76%	8.82%	54.41%

Conclusion

- Significantly increased attack set, covering all BSM fields and targeted V2X application attacks.
- Attacks against position, speed, acceleration are the riskiest as these 3 fields are used in V2X applications and for misbehavior detection as primary values.
- Acceleration is the root value used to estimate next position and speed →this needs to be correct every time.
- Attacks can be combined or sequenced to generate further disruption
  - High speed + large dimensions (simulating a high speed truck) would have more effect on path planning of other vehicles than a high speed + small dimensions (simulating a high speed small car)
- VASP improves upon prior (VEINS) simulation plugins by enabling further the research community to perform offensive tests against V2X applications.

Let’s Collaborate

- https://github.com/quic/vasp
- Contribute implementation of V2X applications
- Contribute V2X attacks (BSM/CAM, CPS, MSCS)
- Contribute detectors

Thank you

Qualcomm

Follow us on:

For more information, visit us at:

qualcomm.com & qualcomm.com/blog