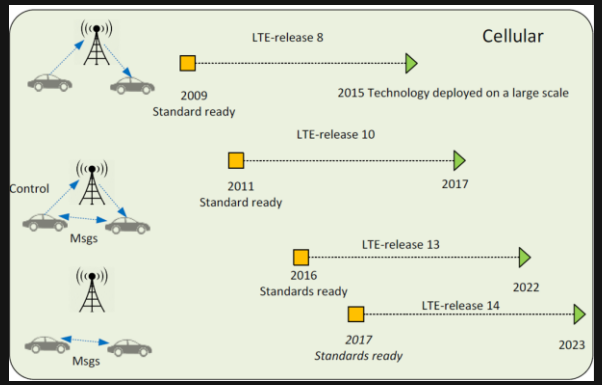
Misbehaviour Detection of 5G Connected Vehicles Using Deep Learning

By: Aidan Lochbihler, Adam ALi Husseinat, Josimar Kouam

SYSC 5804
March 31st , 2023

CAVs, VANETS & V2X

- Connected Autonomous vehicles, Vehicular Ad Hoc Networks, and Vehicle to everything
- Dedicated short range communication for vehicle to vehicle
- 5G Network for vehicle to Base Station
- For communication vehicles broadcast Basic Safety Message (BSMs)



Introduction

- Cooperative Intelligent Transport Systems (C-ITS) is an ongoing technology that will change our driving experience in the near future, vehicles and Road–Side Unit (RSU) cooperate by broadcasting V2X messages over the vehicular network. Safety applications use these data to detect and avoid dangerous situations on time.
- MisBehavior Detection (MBD) in Cooperative Intelligent Transport Systems (C-ITS) is an active research topic which consists of monitoring data semantics of the exchanged Vehicle-to-X communication (V2X) messages to detect and identify potential misbehaving entities.
- The detection process consists of performing plausibility and consistency checks on the Received V2X messages. If an anomaly is detected, the entity may report it by sending a Misbehavior Report (MBR) to the Misbehavior Authority (MA). TheMA will then investigate the event and decide to revoke the sender or not [1].

Abbreviations

- BSM: Basic Safety Message
- C-ITS: Cooperative Intelligent Transport Systems
- DDOS: Distributed Denial of Service attack
- VeReMi: Dataset
- SMOTE: Synthetic Minority Oversampling TEchnique
- DSRC: Dedicated Short-Range Communications
- OBU: ON-Board Unit

Importance of BSM

Sub group	Element
Header	MsgCount
	TemporaryID
	DSecond
PositionLocal3D	Latitude
	Longitude
	Elevation
	PositionalAccuracy
Motion	TransmissionAndSpeed
	Heading
	SteeringWheelAngle
	AccelerationSet4Way
Control	BrakeSystemStatus
VehicleBasic	VehicleSize

Importance of BSM

Type	Description	Size (byte)
DSRCmsgID	Data elements used in each message to define the Message type	1
MsgCount	It can check the flow of consecutive messages having the same DSRCmsgID received from the same message sender.	1
TemporaryID	Represents a 4-byte temporary device identifier. When used in a mobile OBU device, this value is periodically changed to ensure anonymity.	4
Dsecond	Represents two bytes of time information.	2
Latitude	Represents the geographic latitude of an object.	4
Longitude	Represents the geographic longitude of an object.	4
Elevation	Represents an altitude measured by the WGS84 coordinate system.	2
PositionAccuracy	Various quality parameters used to model the positioning accuracy for each given axis.	4
TransmissionAndSpeed	Represents the speed of the vehicle.	2
Heading	The current direction value is expressed in units of 0.0125 degrees.	2
SteeringWheelAngle	Represents the current steering angle of the steering wheel.	1
AccelerationSet4Way	It consists of three orthogonal directions of acceleration and yaw rate.	7
BrakeSystemStatus	Represents a data element that records various control states related to braking of the vehicle.	2
VehicleSize	Represents the length and width of the vehicle.	3

How Attackers can Exploit BSMs

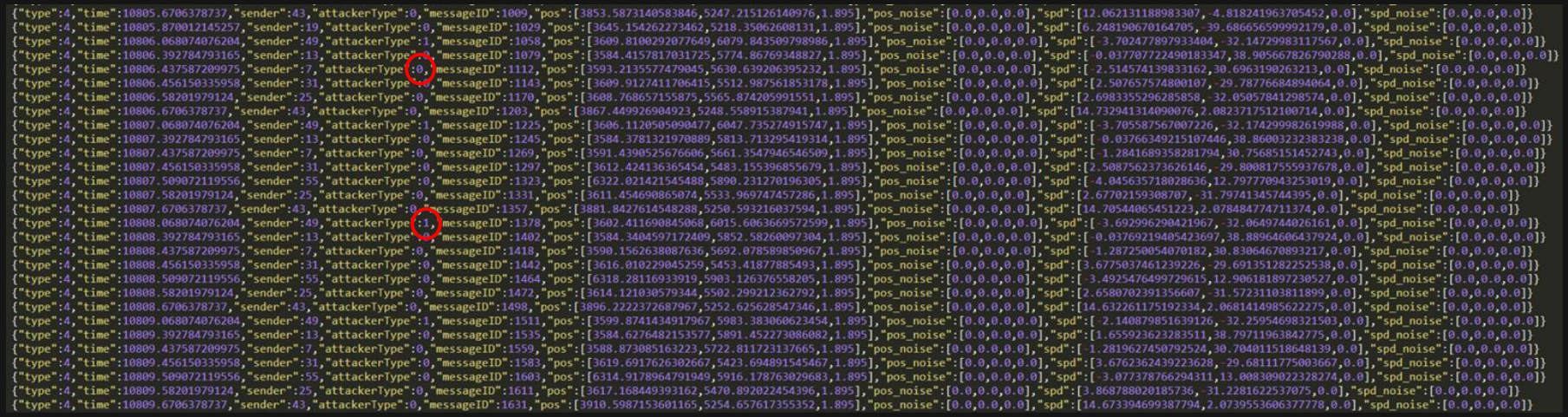
Can exploit systems by either:

1. Overloading the BSM network (Like a DDOS attack)
    a. Can be solved with conventional solutions (I.e. messaging thresholds, message identifiers)

1. Mimicking a real vehicle and sending ghost vehicle positions and speed
    a. Much more difficult to fix with conventional methods (Which we will aim to solve)

Methods: The Dataset

- Vehicular Reference Misbehavior (VeReMi) dataset, a simulated simplified dataset for the evaluation of misbehavior detection mechanisms for VANETs using BSMs
- Includes malicious messages intended to trigger incorrect application behavior, which is what misbehavior detection mechanisms aim to prevent



{"type":4,"time":10805.6706378737,"sender":43,"attackerType":0,"messageID":1009,"pos":[3853.5873140583846,5247.215126140976,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[12.062131188983307,-4.818241963705452,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10805.870012145257,"sender":19,"attackerType":0,"messageID":1029,"pos":[3645.154262273462,5218.35062608131,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[6.248190670164705,-39.686656599992179,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10806.068074076204,"sender":49,"attackerType":1,"messageID":1058,"pos":[3609.8100292077649,6079.843509798986,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-3.702477897933404,-32.14729983117567,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10806.392784793165,"sender":13,"attackerType":0,"messageID":1079,"pos":[3584.4157817031725,5774.86769348827,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-0.037707722490183347,38.905667826790288,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10806.437587209975,"sender":7,"attackerType":0,"messageID":1112,"pos":[3593.2135577479045,5630.639206395232,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-2.514574139833162,30.696319026321 3,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10806.456150335958,"sender":31,"attackerType":0,"messageID":1143,"pos":[3609.9127411706415,5512.987561853178,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[2.507657574800107,-29.78776684894064,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10806.58201979124,"sender":25,"attackerType":0,"messageID":1170,"pos":[3608.768657155875,5565.874205991551,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[2.6983355296285858,-32.05057841298574,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10806.6706378737,"sender":43,"attackerType":0,"messageID":1203,"pos":[3867.449926904923,5248.558915387941,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[14.732941314090076,2.0823171512100714,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10807.068074076204,"sender":49,"attackerType":1,"messageID":1225,"pos":[3606.1120505090477,6047.735274915747,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-3.7055875670072 26,-32.174299982619988,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10807.392784793165,"sender":13,"attackerType":0,"messageID":1245,"pos":[3584.3781321970889,5813.713295419314,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-0.03766349215107446,38.86003232383238,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10807.437587209975,"sender":7,"attackerType":0,"messageID":1269,"pos":[3591.4390525676606,5661.3547946546509,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-1.2841689358281794,30.756851514527 43,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10807.456150335958,"sender":31,"attackerType":0,"messageID":1297,"pos":[3612.424136365454,5483.155396855679,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[2.5087562373626146,-29.800817555937678,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10807.509072119556,"sender":55,"attackerType":0,"messageID":1323,"pos":[6322.021421545488,5890.231270196305,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-4.045635718028636,12.797770943253019,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10807.58201979124,"sender":25,"attackerType":0,"messageID":1331,"pos":[3611.454690865074,5533.969747457286,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[2.6770215930870 7,-31.797413457443395,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10807.6706378737,"sender":43,"attackerType":0,"messageID":1357,"pos":[3881.8427614548288,5250.593216037594,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[14.70544065451223,2.078484774711374,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10808.068074076204,"sender":49,"attackerType":1,"messageID":1378,"pos":[3602.411690845068,6015.6063669572599,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-3.6929969204219 67,-32.0649744026161,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10808.392784793165,"sender":13,"attackerType":0,"messageID":1402,"pos":[3584.3404597172409,5852.58260097304,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-0.03769219405423697,38.88964606437924,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10808.437587209975,"sender":7,"attackerType":0,"messageID":1418,"pos":[3590.1562638087636,5692.078589850967,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-1.2872500540701 82,-30.830646708932 17,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10808.456150335958,"sender":31,"attackerType":0,"messageID":1442,"pos":[3616.010229045259,5453.41877885493,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[3.6775037461239226,-29.691351282252538,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10808.509072119556,"sender":55,"attackerType":0,"messageID":1464,"pos":[6318.28116933919,5903.126376558205,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-3.4925476499729615,12.906181897230527,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10808.58201979124,"sender":25,"attackerType":0,"messageID":1472,"pos":[3614.121030579344,5502.299212362792,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[2.6580702391356607,-31.572311038118 99,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10808.6706378737,"sender":43,"attackerType":0,"messageID":1498,"pos":[3896.2222372687967,5252.625628547346,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[14.632261175192334,2.068141498562227 5,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10809.068074076204,"sender":49,"attackerType":1,"messageID":1511,"pos":[3599.8741434917967,5983.383060623454,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-2.140879851639126,32.25954698321503,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10809.392784793165,"sender":13,"attackerType":0,"messageID":1535,"pos":[3584.6276482153577,5891.452273086082,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[1.655923623283511,38.797119638427775,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10809.437587209975,"sender":7,"attackerType":0,"messageID":1559,"pos":[3588.873085163223,5722.811723137665,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-1.2819627450792524,30.704011518648139,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10809.456150335958,"sender":31,"attackerType":0,"messageID":1583,"pos":[3619.6917626302667,5423.694891545467,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[3.6762362439223628,-29.681117750036 67,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10809.509072119556,"sender":55,"attackerType":0,"messageID":1603,"pos":[6314.9178964791949,5916.178763029683,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[-3.077378766294311,13.008309022328274,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10809.58201979124,"sender":25,"attackerType":0,"messageID":1611,"pos":[3617.168449393162,5470.892022454396,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[3.868788020185736,-31.228162537507 5,0.0],"spd_noise":[0.0,0.0,0.0]}
{"type":4,"time":10809.6706378737,"sender":43,"attackerType":0,"messageID":1631,"pos":[3910.5987153601165,5254.657617355352,1.895],"pos_noise":[0.0,0.0,0.0],"spd":[14.673394699387794,2.073955360637778 8,0.0],"spd_noise":[0.0,0.0,0.0]}

Time snippet of VeReMi Dataset

Methods: The Dataset


```
{"type":4,"time":10800.392784793165,"sender":13,"attackerType":0,"messageID":38,
"pos":[3597.1520859538707,5542.199221013564,1.895],"pos_noise":[0.0,0.0,0.0],
"spd":[-3.178365760312756,38.7989694164331,0.0],"spd_noise":[0.0,0.0,0.0]}
```


Single BSM

Method: BSM Densities

In all cases vehicles are sending BSMs at ~10Hz. Percent of cars that are attackers remains similar

Low Density:

- 35-39 vehicles

Medium Density:

- 97-108 vehicles

High Density:

- 491-519 vehicles

Method: Machine Learning and Deep Learning

Speed vs Accuracy:

- In most deep learning problems high classification accuracy is all that matters
- But in this case speed can be equally as important (Inference time & number of BSMs needed*)

Speed:

- XGBoost, Neural Network

Accuracy:

- LSTM, Transformer

Method: Organizing the Data

Inter-Threat Detection: Analyzing the BSM messages of a car within itself
*(Promising for high density scenarios)

Intra-Threat Detection: Analyzing a BSM message from a car within the context of many BSM messages before it from all cars
*(Can detect threats faster)

Method: 2 Model Approach

Model 1:

Sequence to Sequence LSTM:

- Learns what the normal behaviour of a Real vehicle
- Given 10 BSMs predicts the next one in the sequence

Model 2:

- 16 Feature Binary Classification (Non-Attacking, 0, or Attacking, 1, Vehicle)
- Model takes 5-100 sets of:
    - Current vehicle position & speed, predicted vehicle position & speed (@ that time point), position and speed of 2 closest vehicles (Totals 16 features)

5G Vision

As in PMI (Precoding Matrix Information) of CSI (Channel-State-Information) message in 5G eMBB network, BSM provide information about the vehicular position that system use to control and coordinate the other vehicles and overall traffic safety.

An attacker may manipulate this information and cause a traffic congestion or blocking, more dangerous, false BSM information may lead to a sudden actions from other vehicles as a response for these false information and lead to serious dangers like sudden breaking or speeding behaviour while a vehicle is in front and close in reality so an accident happened.

5G Network Security Potential Solutions

1 - BSM contents Verification using gNB.
2 - BSM contents Verification using other Vehicles.
3 - BSM contents Verification using RSUs.
4 - BSM contents Verification optional fields in the BSM.
5 - Other 5G features and aspects.

All above are a prospective solutions to achieve an accurate and effective MDS using AI.

References

[1] Kamel, Joseph & Ansari, Mohammad & Petit, Jonathan & Kaiser, Arnaud & Ben Jemaa, Ines & Urien, Pascal. (2020). Simulation Framework for Misbehavior Detection in Vehicular Networks. IEEE Transactions on Vehicular Technology. PP. 10.1109/TVT.2020.2984878.

[2] Kim, Jae-Wan & Jeon, Dong-Keun. (2018). A Cooperative Communication Protocol for QoS Provisioning in IEEE 802.11p/Wave Vehicular Networks. Sensors. 18. 3622. 10.3390/s18113622.