Ontological Representation of CVNs for Anomaly Detection Purposes

Quentin Ricard
qricard@laas.fr

September 26, 2019
Problem Statement

Continental’s E-Horizon

- New communication channel between vehicles and the rest of the world

Hence new attack vectors

- Jeep Cherokee, 2015, (Charlie Miller and Chris Valasek)
- Nissan Leaf, 2016, (Troy Hunt)
- Volkswagen/Audi, 2018, (Daan Keuper and Thijs Alkemade)
Towards Anomaly Detection

Idea

- Apply existing algorithms to cellular vehicular networks:
  - Adapt to cellular networks behaviour;
  - Adapt to connected vehicles communications;

- Represent anomalies w.r.t the context of the communication.
Ontological representation of the traffic
The Ontology

Traffic representation

- Multiple Scales
- Formal representation of key features:
  - Sequences of packet class
  - Sequences of Frame attributes and Flow properties
    ($\approx 70$ Features)
## Detection process

### Multiple algorithms (Grocery List)

- Hierarchical Temporal Memory (HTM) ?
- DBSCAN
- One-Class SVM
- Perhaps Markov models ... 

### Comparative Study : WE NEED YOU

- With the Ontology using other algorithms ?
- Without the Ontology using same algorithms ?
- How about feature selection, should we use the same ?
But Quentin, what are your anomalies ???

State of the Art! (and what our intern was able to do during the summer)

- Data exfiltration via DNS-tunelling
  - That might’ve been a bad idea
- SCAN ALL THE THINGZ
  - Xmas for now, `todo`: moooore scanz
- Telemetry anomalies
  - i.e. We stop the flow for a while
- Malware contamination

(todo… somebody stop time pls)
Conclusion

**This is going to work eventually**

- Vehicular communication representation
- Feature creation on multiple scales
- Anomaly representation (more on this later)

**Anomaly generation**

- Still lacks realism in my opinion
- Easy enough to set up new ones though
Thanks !