Detection of In-Vehicle Network Cyber Attacks Using Packet Timing Anomalies

Andrew Tomlinson, Jeremy Bryans, Siraj Ahmed Shaikh, Harsha Kumara Kalutarage

Systems Security Group, Institute for Future Transport and Cities, Coventry University, Coventry, CV1 5FB, UK.

Centre for Secure Information Technologies (CSIT), Queen’s University, Belfast, BT9 5BN, UK.

Objectives

- Determine and evaluate suitable unsupervised CAN attack detection methods based on packet timing anomalies.
- Test using data representative of likely CAN cyber-attacks.

Background – Why this research matters.

- Increasing use of vehicle computer code and electronic control units.
- Increasing vehicle connectivity and autonomy.
- Automotive Industry concerns.
- Publicised vehicle attacks.
- Emergence of hackers.

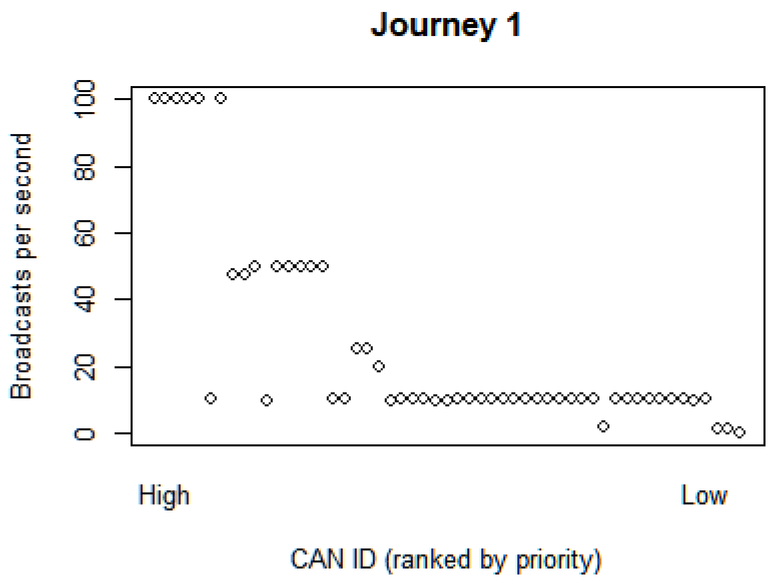
Controller Area Network (CAN) Cyber-Threat

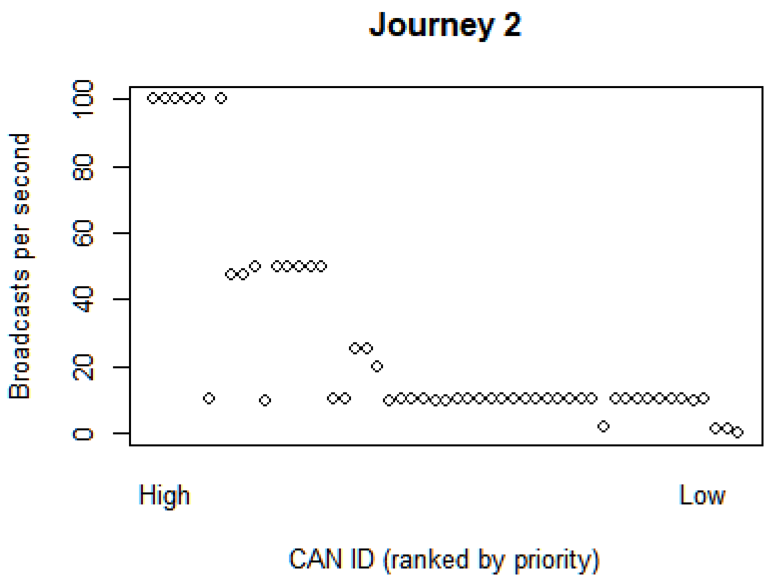
- Cars - interconnected computer networks.
- CAN - safety critical electronic control units (ECUs).
- Lacks security features.
- Cyber attacks controlling braking, speed and steering, warning lights, battery drain...
- Cyber attacks alter packet timings and/or packet data contents.

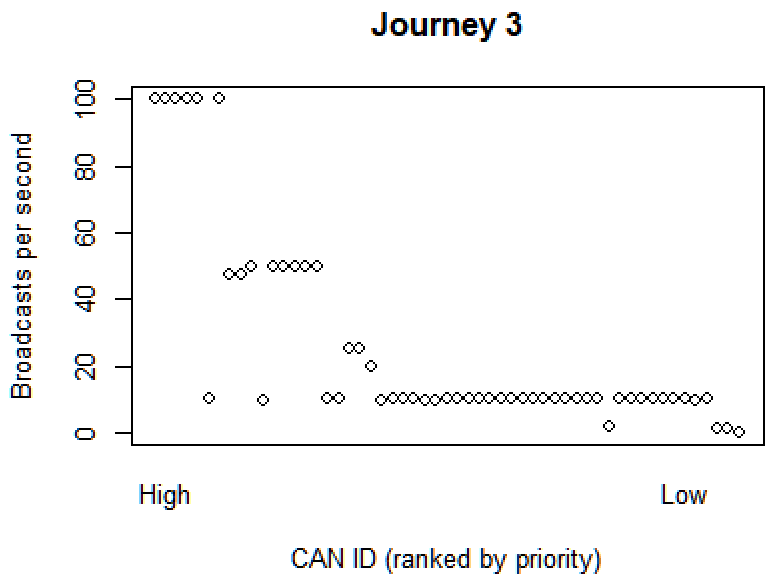
CAN Packet Traffic

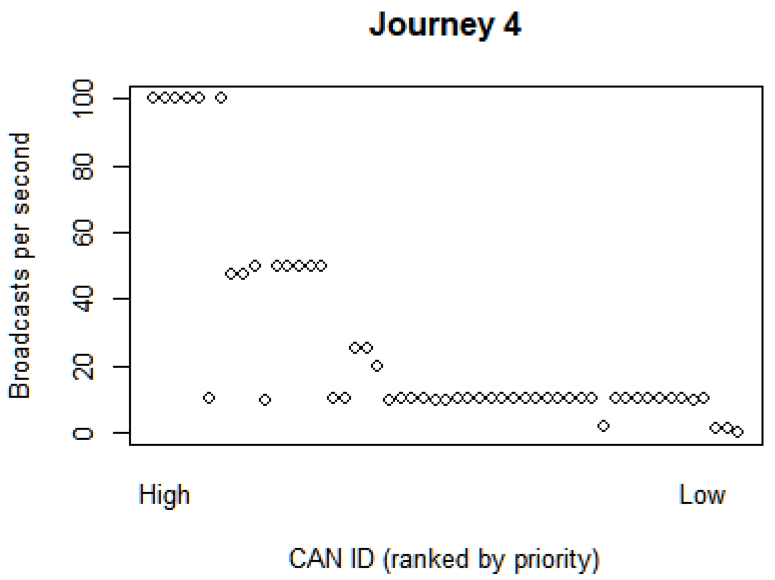
- CAN ID -> broadcast priority.
- CAN packets with matching IDs (hence broadcast by the same ECU) are broadcast at fairly consistent rates.
- CAN broadcast-rates and data definitions are proprietary and secret. This suggests unsupervised detection.

CAN Packet Broadcast Rates


Journey 1


Journey 2


Journey 3


Journey 4

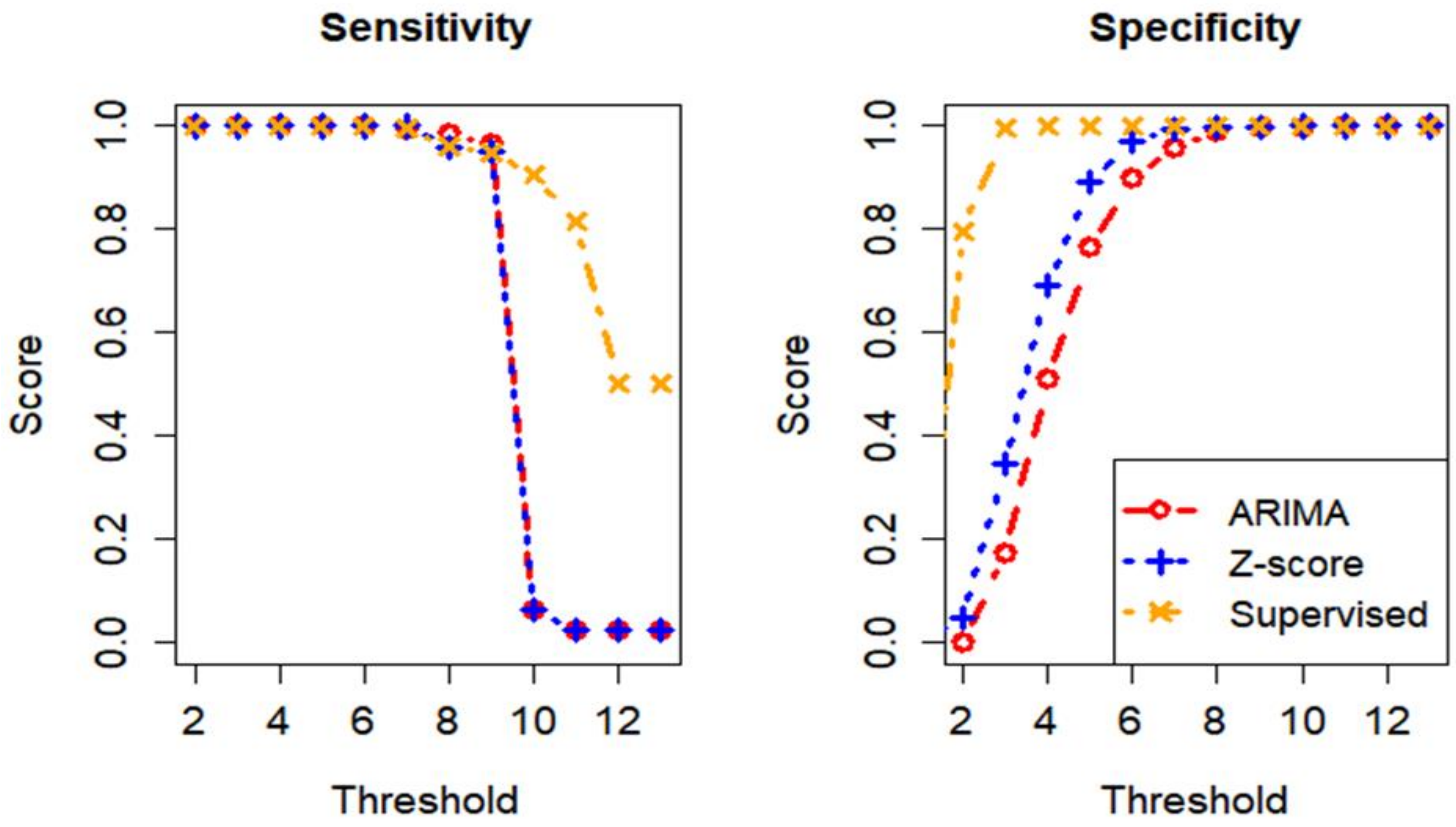
Attack Simulation

- CAN logs from a popular car.
- Attacks simulated at random locations in a CAN log by altering the data to mimic documented attack effects:
  - Injected packets.
  - Dropped packets.

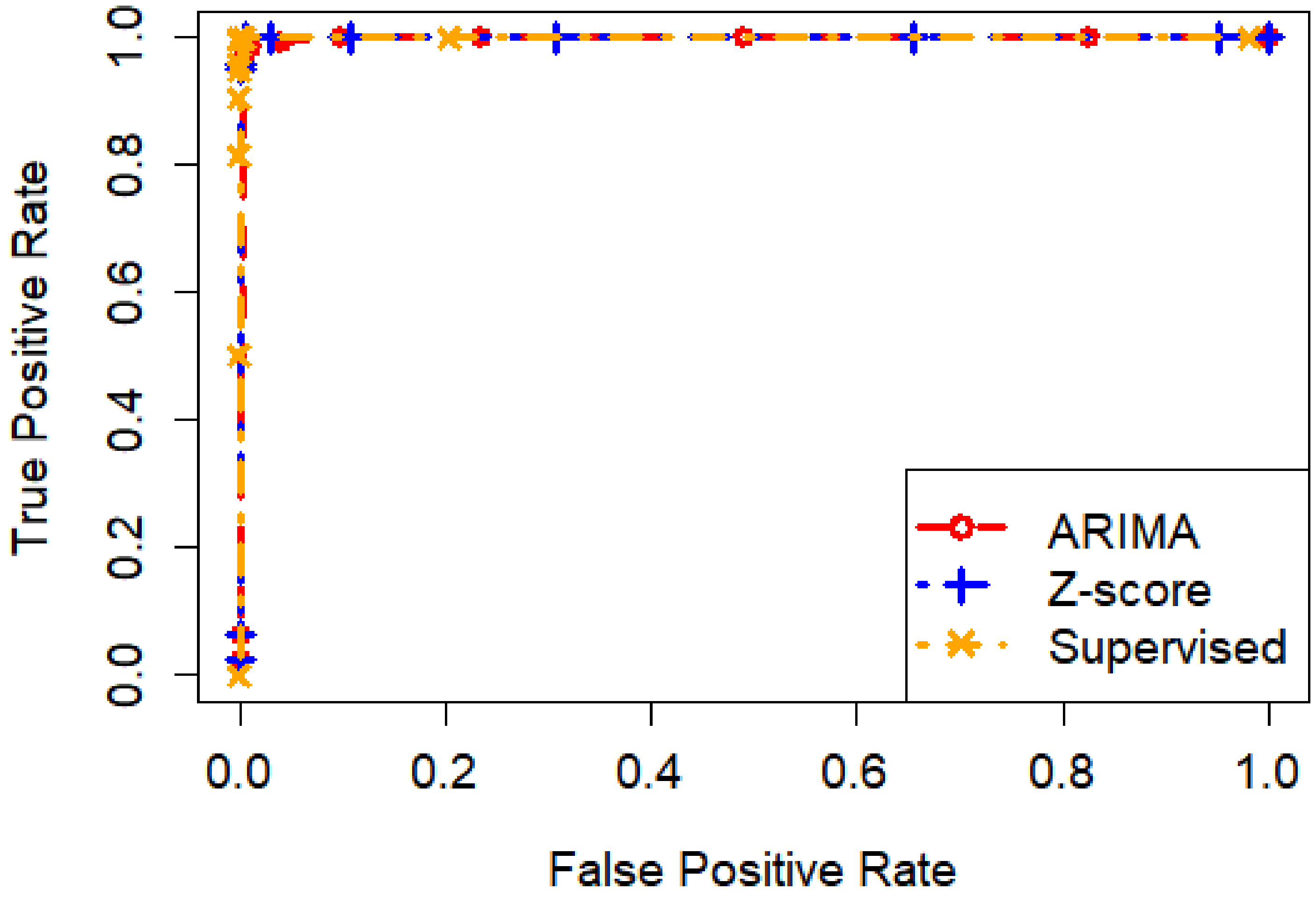
Method Testing

- CAN test logs were processed in 1 second windows.
- Broadcast-interval means, grouped by packet ID.
- Three comparison methods were tested:
    - **ARIMA** (autoregressive integrated moving average) model of the window used for Mean Squared Error based broadcast-interval anomaly detection.
    - **Z-score** for each broadcast interval compared with window mean.
    - **Supervised** comparison of broadcast interval with window mean (<> 0.003 second variation).

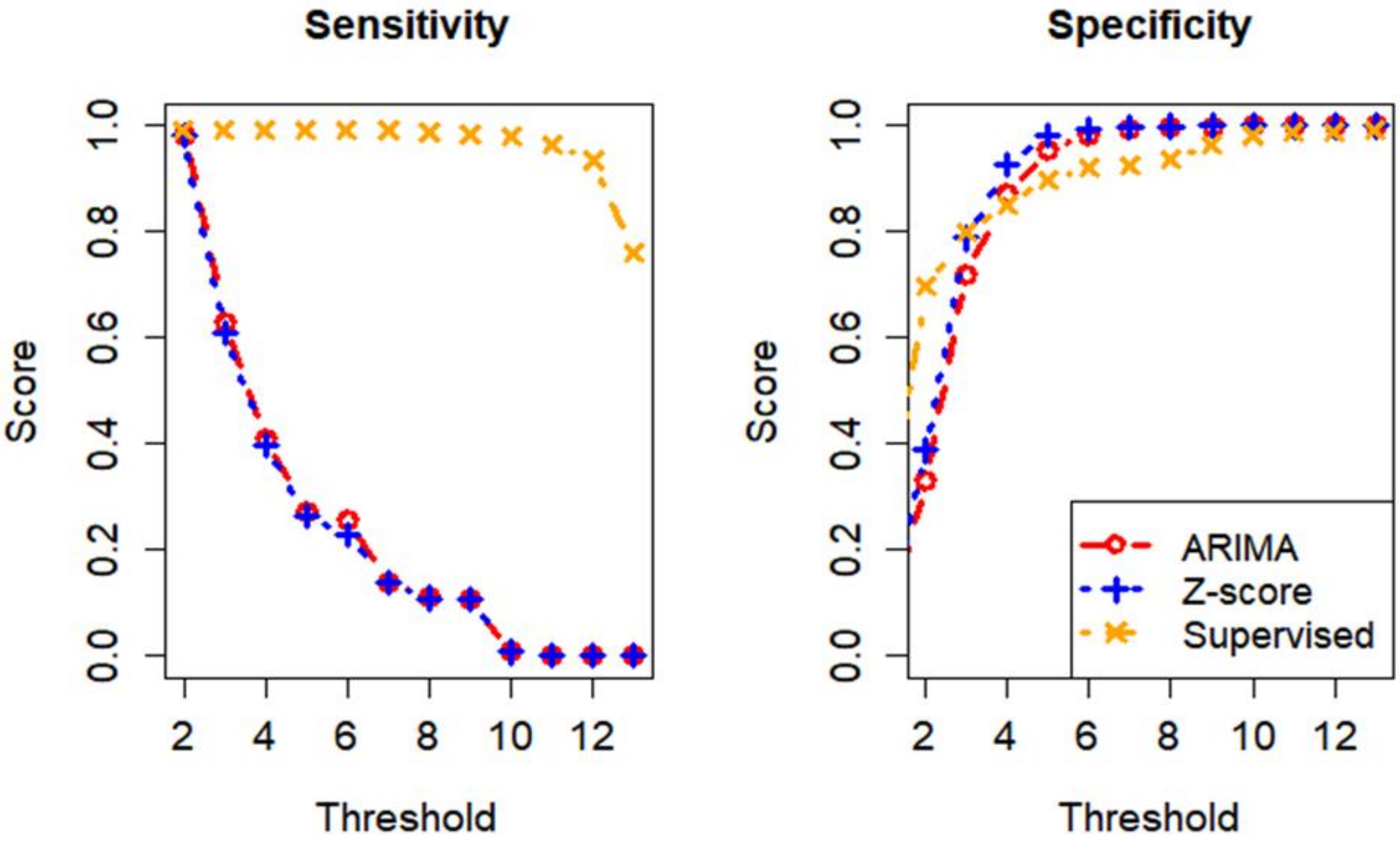
Combined injection and dropped packet results for 5 highest priority packet IDs at various thresholds.



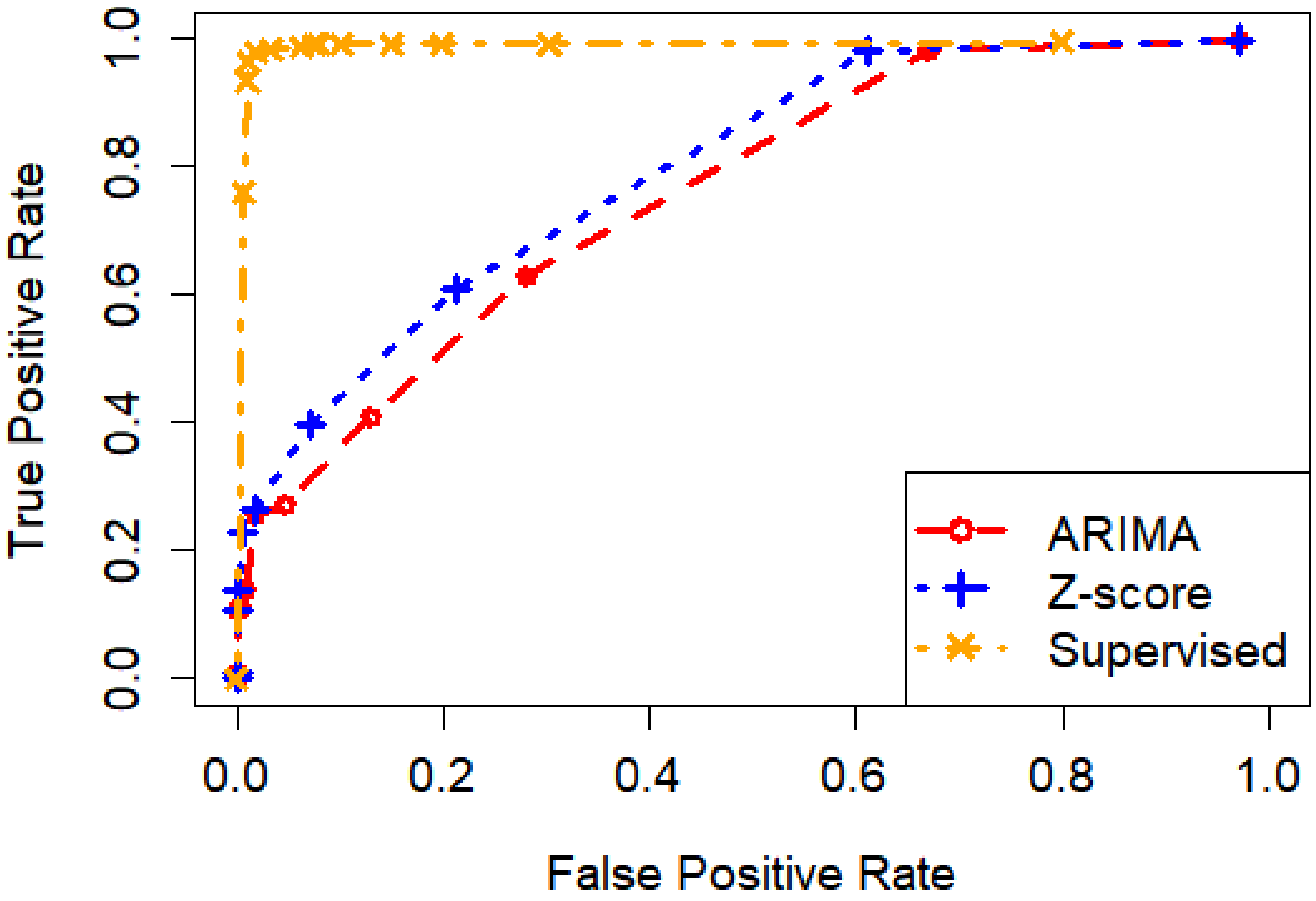
Combined injection and dropped packet ROC for 5 highest priority packet IDs at various thresholds.



Combined injection and dropped packet results for all packet IDs at various thresholds.



Combined injection and dropped packet ROC for all packet IDs at various thresholds.



Implications

- With high priority packets, unsupervised ARIMA and Z-score detection was nearly as good as a specifically calculated threshold.
- ARIMA and Z-Score require no pre-calculated threshold.
- Potential, with refinement, in car IDS.

Future Work

- Wider range of vehicles and journey types.
- Detailed analysis of attack types.
- Payload anomaly detection.
- Simulation methods.