STELLANTIS

TELECOM Paris

INSTITUT POLYTECHNIQUE DE PARIS

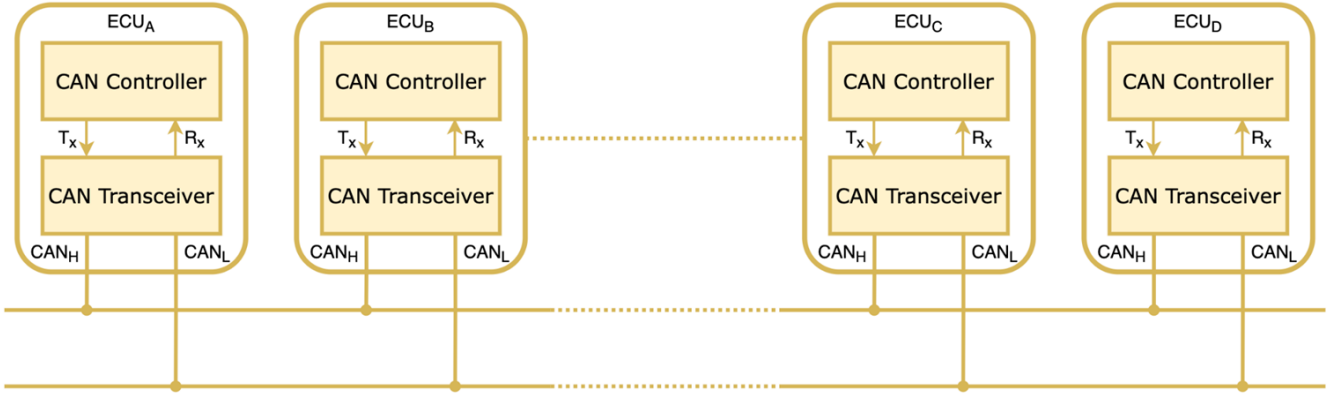
AMICA: Attention-based Multi-Identifier model for asynchronous intrusion detection on Controller Area networks

Natasha Alkhatib*, Lina Achaji*, Maria Mushtaq, Hadi Ghauch, and Jean-Luc Danger

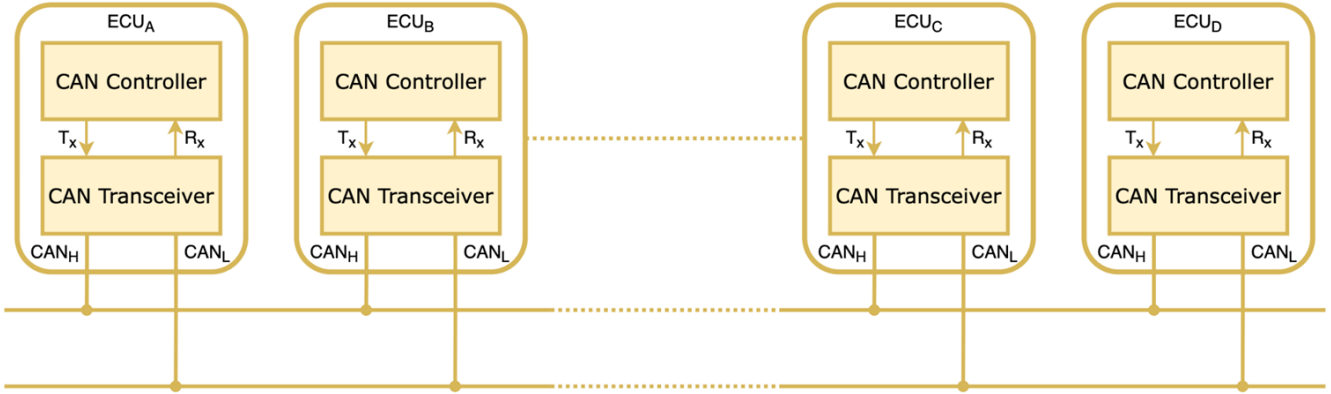
Outline

1. Problematic
2. AI-based Solution
3. Anomaly Score and Results

Problematic



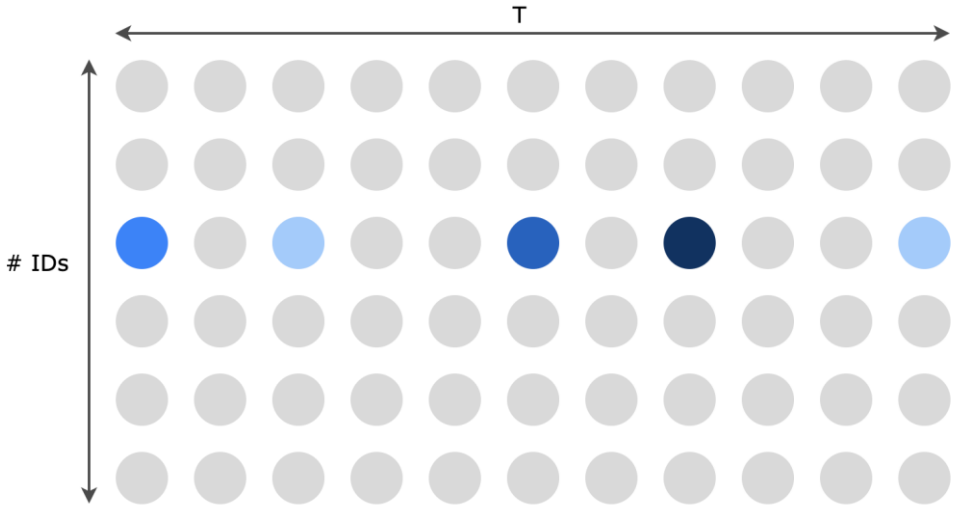
Problematic



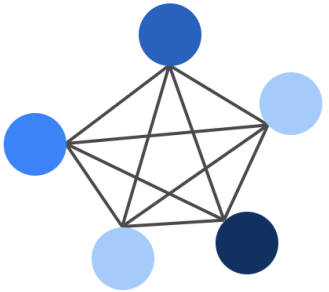
Time	ID	Signals of A				Signals of B			Signals of C			Signals of D
1.04	B	-	-	-	-	54.1	0	7.4	-	-	-	-
3.10	D	-	-	-	-	-	-	-	-	-	-	31.7
4.97	A	12	44.1	38.2	0	-	-	-	-	-	-	-
7.01	C	-	-	-	-	-	-	-	17.9	7	2	-
8.99	B	-	-	-	-	55.2	1	7.1	-	-	-	-
9.75	A	13	44.2	39.7	0	-	-	-	-	-	-	-

Schematic representation of CAN bus data payload

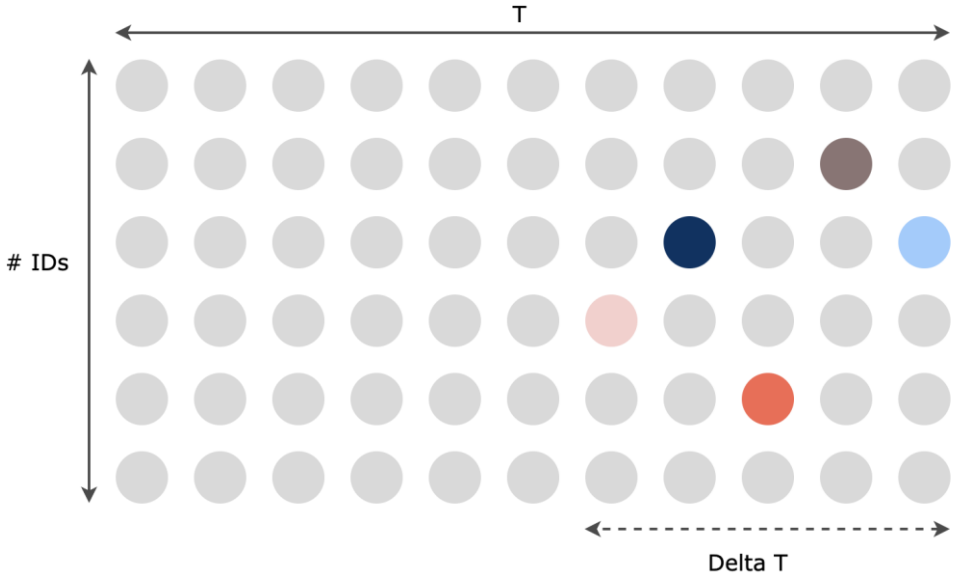
Problematic



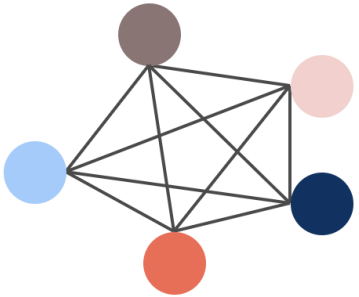
Time Dimension



Problematic

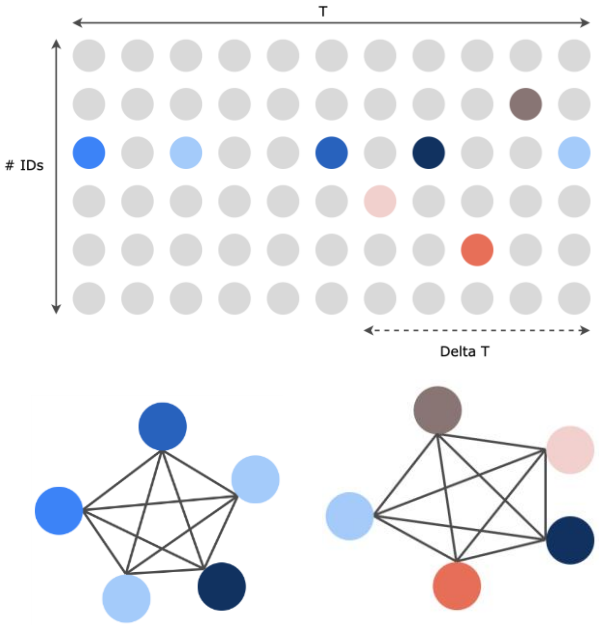


Interaction Dimension



AI based solution

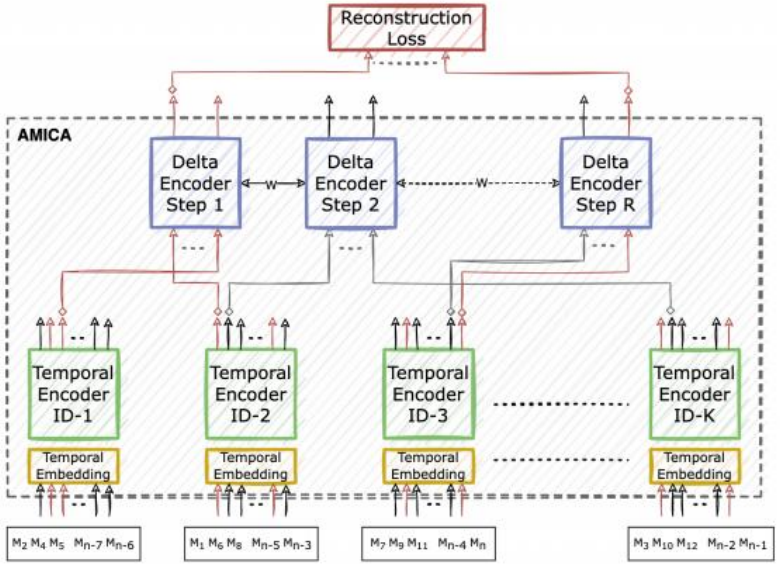
Asynchronous CAN Data



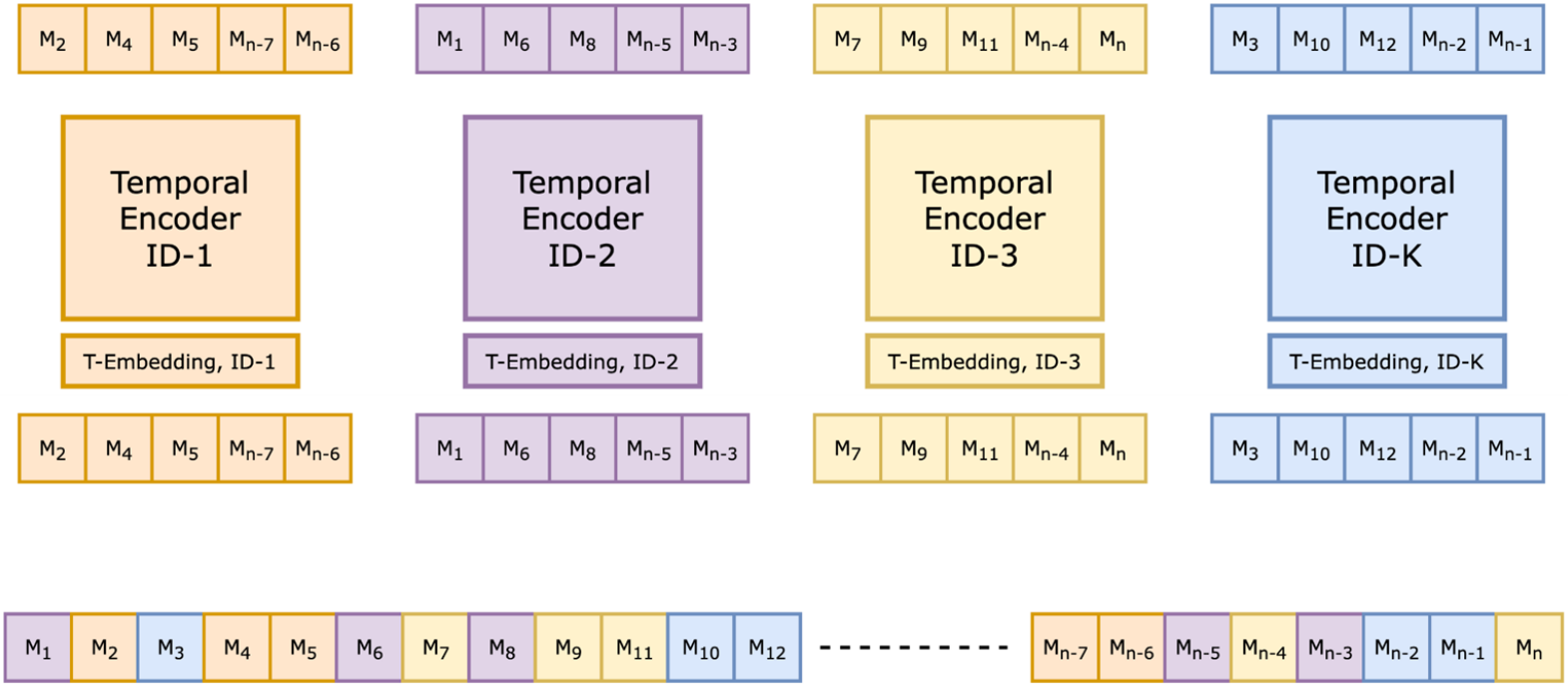
Temporal Dimension

Interaction Dimension

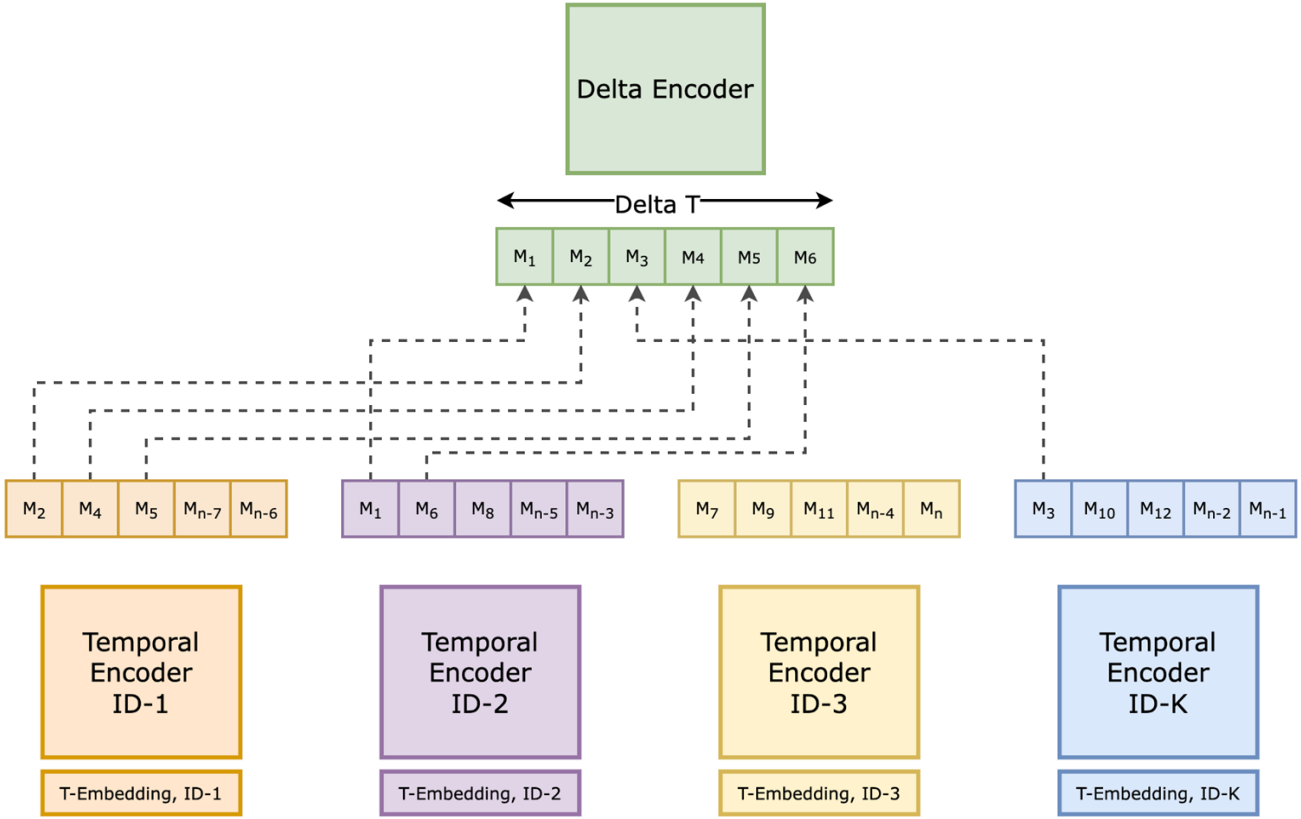
Proposed Model: AMICA



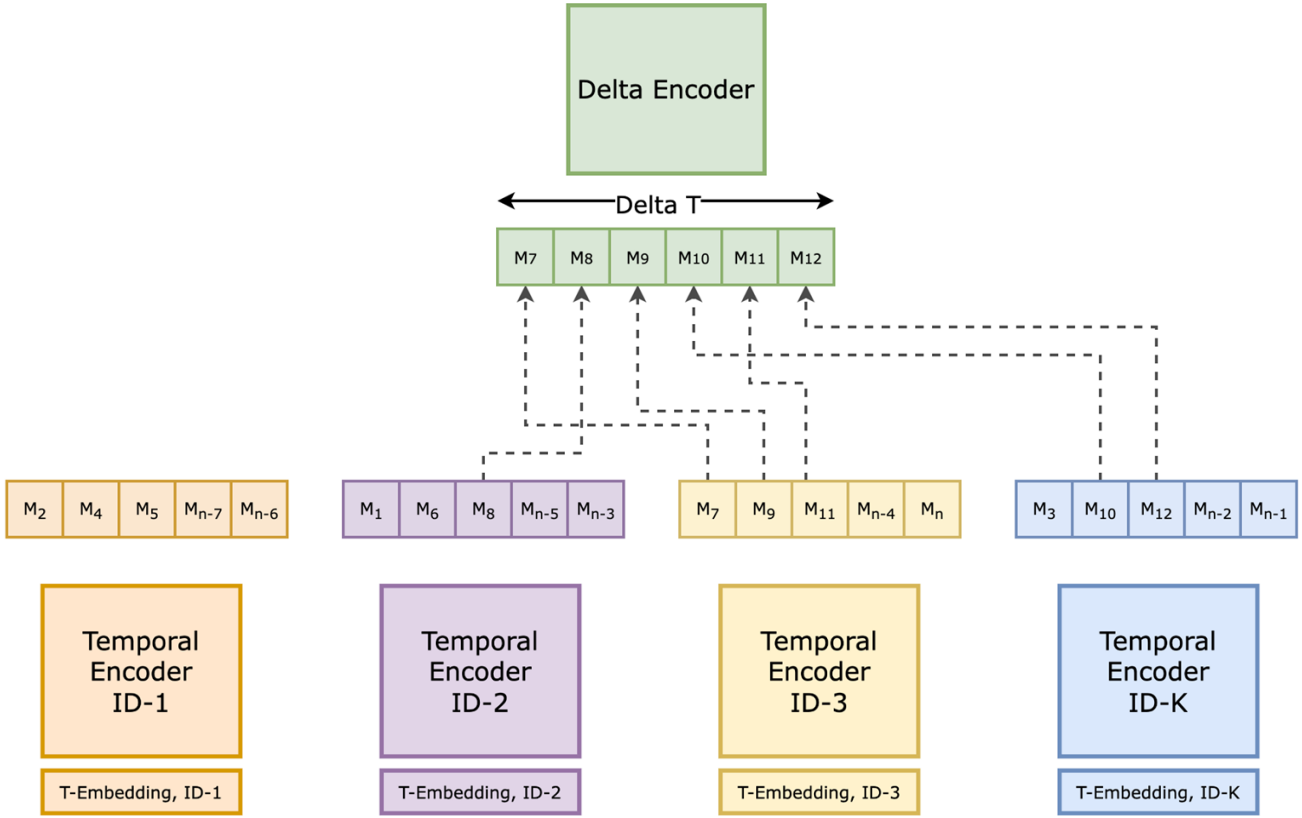
Temporal Encoding



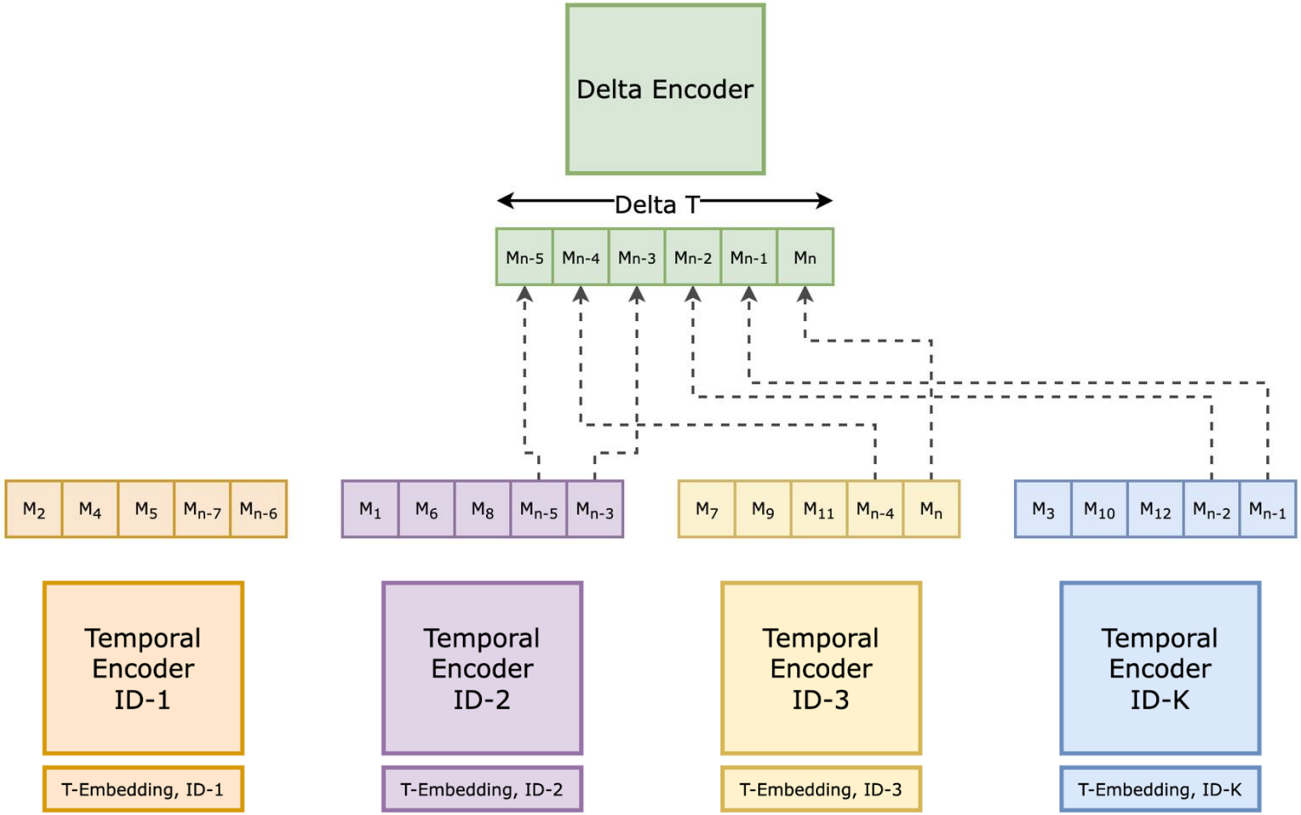
Delta Encoding



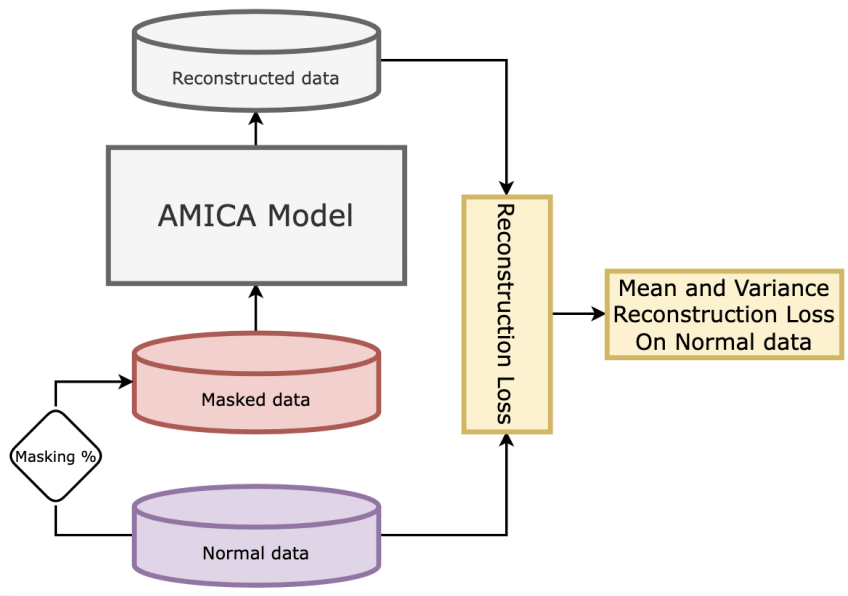
Delta Encoding



Delta Encoding

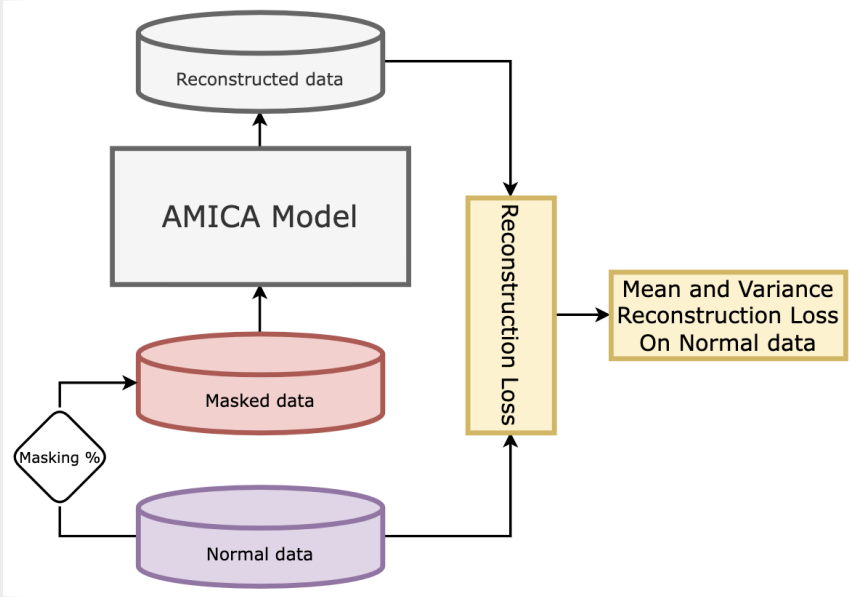


Training workflow

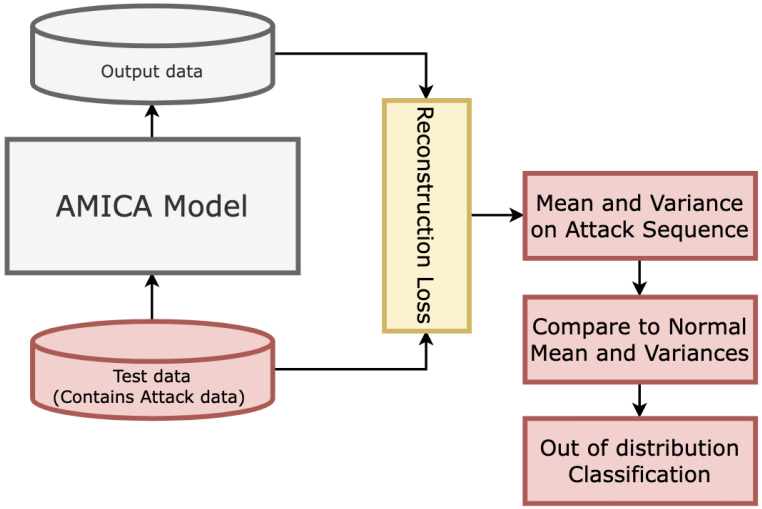


Training workflow

Training and Testing workflow



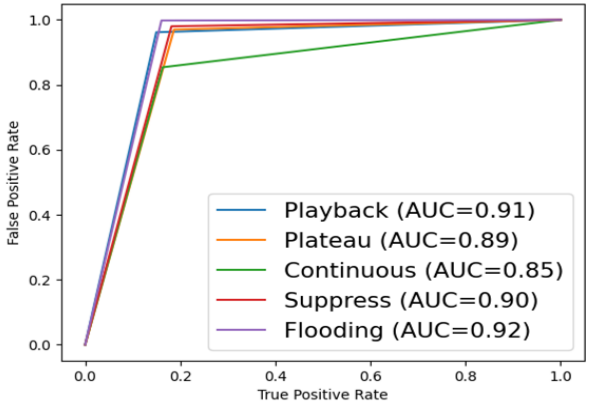
Training workflow

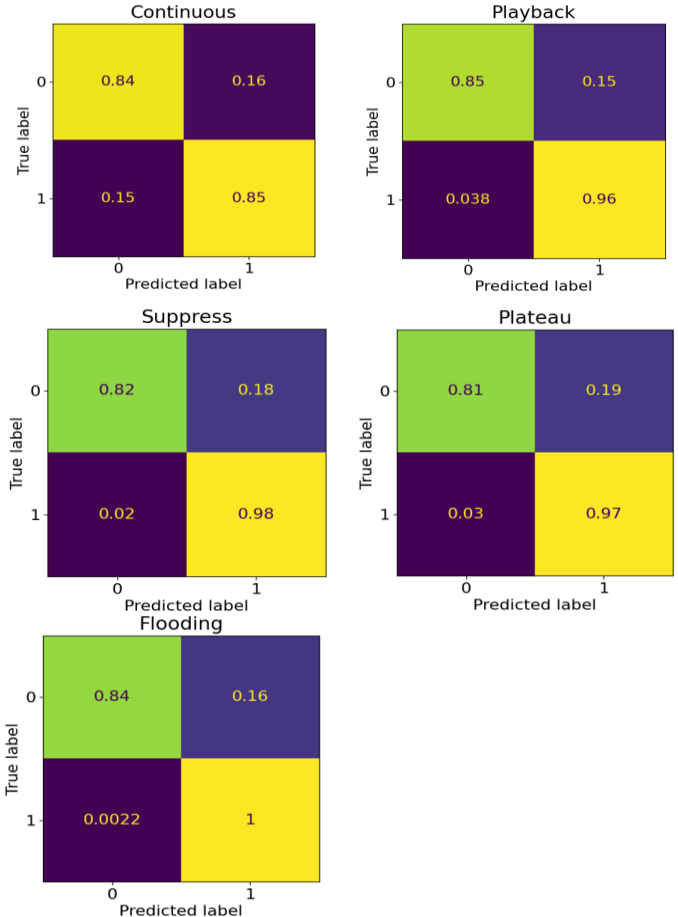


Testing workflow

AMICA Results on SynCAN Dataset

Attack	Recall	Precision	F1-score	FPR
Plateau	78.65	97.73	87.16	1.4
Continuous	57.96	98.43	72.96	0.5
Playback	64.50	97.79	77.73	0.7
Suppress	86.43	98.91	92.25	0.7
Flooding	99.56	99.34	99.45	0.7





Conclusion & Future work

- AMICA, a novel deep learning based multi-agent system for detecting intrusions on CAN bus.
- Detection of ***different and sophisticated intrusions*** in long CAN message sequences by :
  - Modeling contextual information between CAN signals
  - Devising suitable training process
- **Future research:**
  - Anomaly threshold for each signal separately
  - Ablation study on the model architecture with exhaustive hyperparameter tuning
  - Comparison with state-of-the-art models (ex: CANET, etc.)

Thank you