Meet-up 2019 | Doctorants & Industrie

Machine learning for intrusion detection in autonomous transportation systems

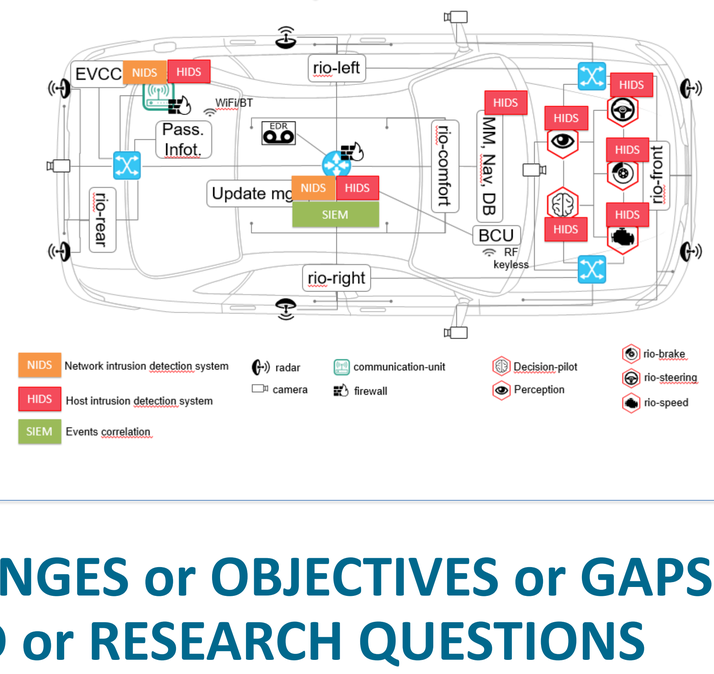
Elies GHERBI [1, 2]

Blaise Hanczar[1], Jean-christophe Janodet[1], Witold Klaudel [3]

[1]IBIS, UEVE; [2]IRT SystemX; [3]Renault

1. CONTEXT

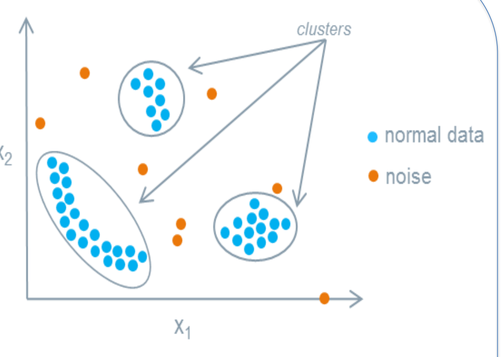
Intrusion detection systems & Autonomous transportation



2. CHALLENGES or OBJECTIVES or GAPS or NEED or RESEARCH QUESTIONS

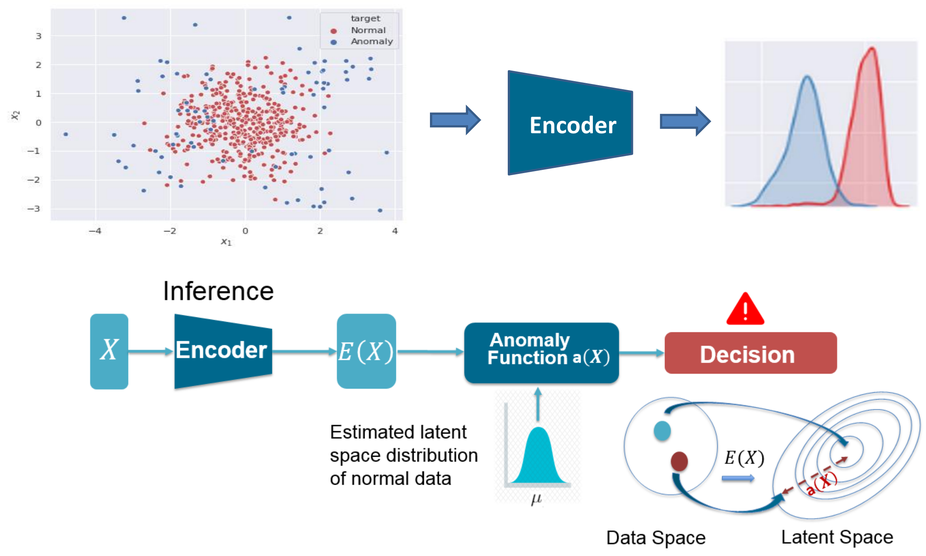
Anomaly detection:

- Multiple normal behavior modelization
- A distributed IDS
- Real-time detection
- Low ressource consumption



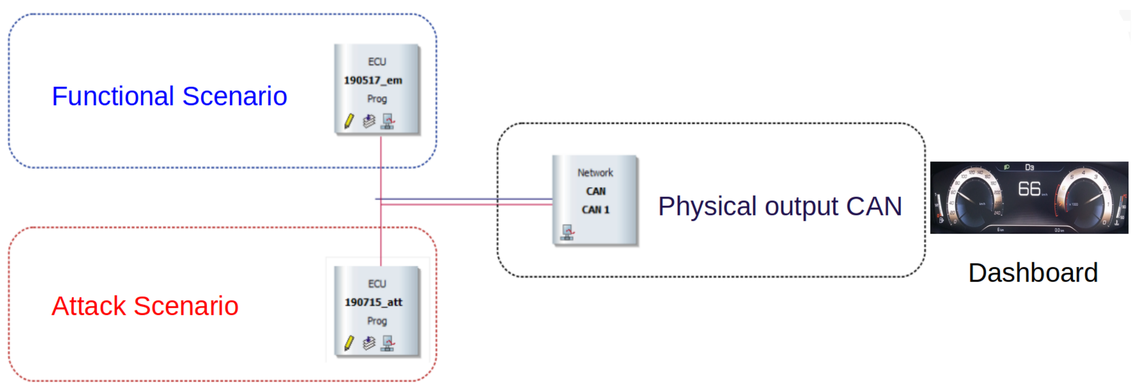
3. CONTRIBUTION or PROPOSITION or RESEARCH METHOD

An Encoding Adversarial network for anomaly detection



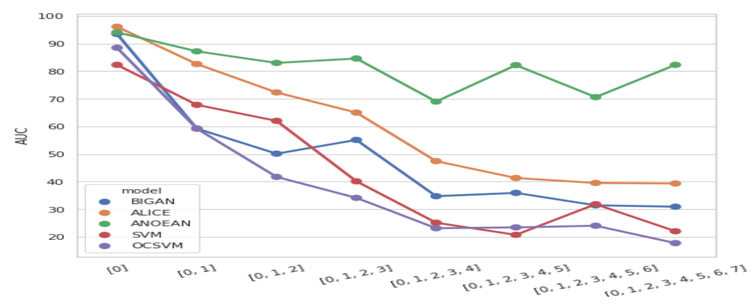
4. CASE STUDY or APPLICATION (or EXPECTED)

CAN bus Anomaly detection



5. RESULTS or EXPECTED RESULTS

Image Dataset (Mnist)



Network Dataset (KDD)

AUC	F1	ROC	accuracy	Model
79.6	80.5	82.3	81.9	AnoGAN
93.8	87.1	95.4	97.3	EGBAD
93.7	88.1	95.7	97.0	ALAD
94.1	89.3	97.0	97.2	OCSVM
98.0	95.0	99.1	98.0	**AnoEAN**
97.3	93.3	98.9	97.2	SVM

Table 1: NSL-KDD

AUC	F1	ROC	accuracy	Model
72.9	73.4	79.3	77.1	AnoGAN
95.4	96.6	98.4	98.6	EGBAD
89.1	93.9	97.9	97.6	ALAD
73.8	87.0	88.3	88.1	OCSVM
97.5	96.3	99.1	98.5	**AnoEAN**
97.2	**98.7**	98.7	99.1	SVM

Table 2: KDD99

6. FUTURE WORK

- Adapt our method to the case where no anomalies are available in the training set.
- Apply Time series approaches to learn the normal behavior of car embedded UCUs (CAN-bus).
- Multi-view learning model on different sub-systems.

REFERENCES

- E.Gherbi, B.Hanczar, J-C .anodet, W.Claudel. An Encoding Adversarial Network for anomaly detection. ACML(2019).
- E.Gherbi, B.Hanczar, J-C .anodet, W.Claudel. An EncodingConstruction d'espace latent pour la detection d'anoamly (Cap 2019)

ED STIC
UEVE
Antoine Durand: antoine.durand@irt-systemx.fr