7th Workshop on Advanced Analytics and Learning on Temporal Data
AALTD@ECML

19 – 23 September 2022

RESIST: Robust Transformer for Unsupervised Time Series Anomaly Detection

Authors

Naji NAJARI[1,2], Samuel BERLEMONT[1], Grégoire LEFEBVRE[1]
Stefan DUFFNER[2,3], Christophe GARCIA[2,3]

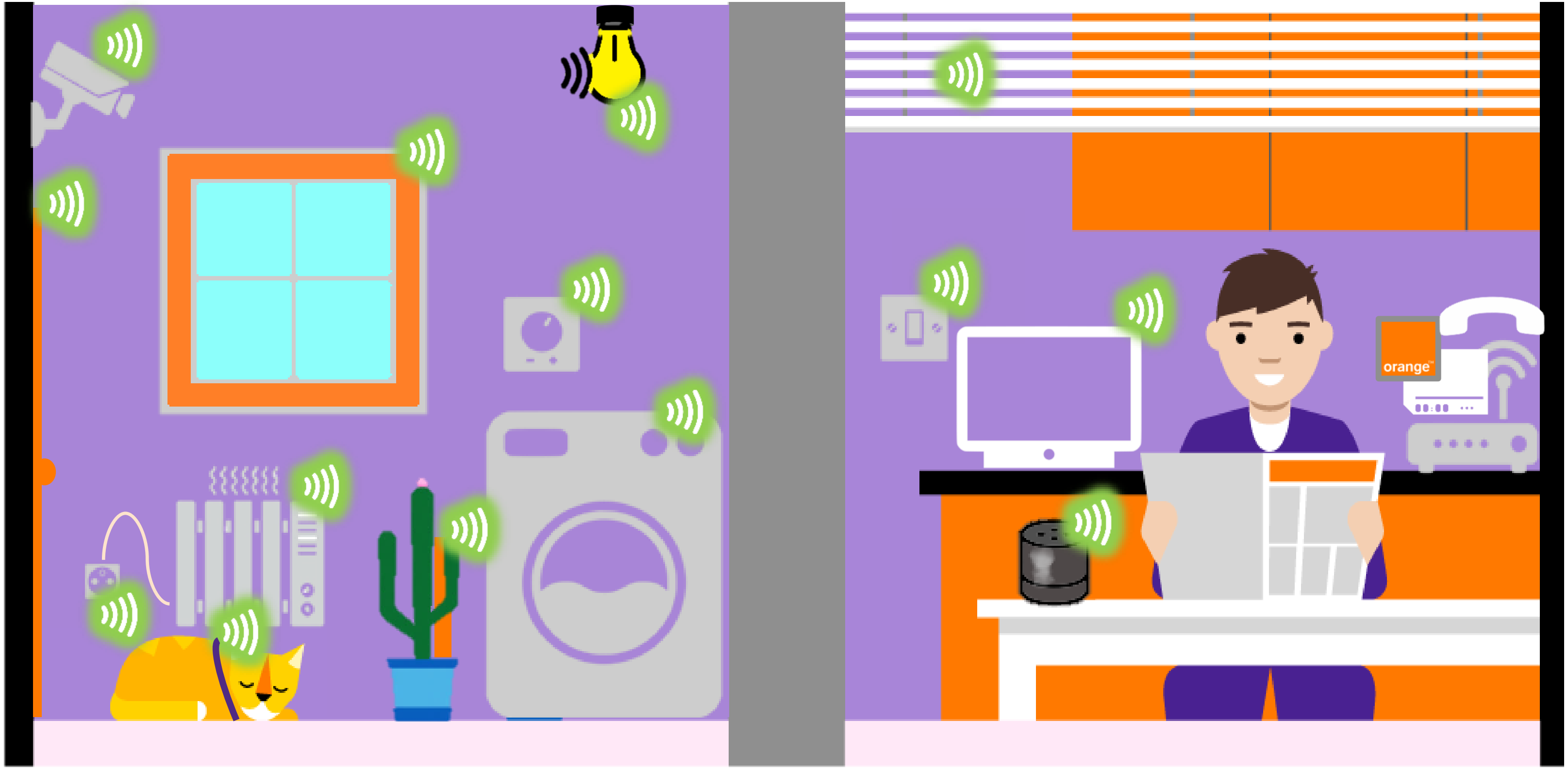
orange 1

LIRIS 2

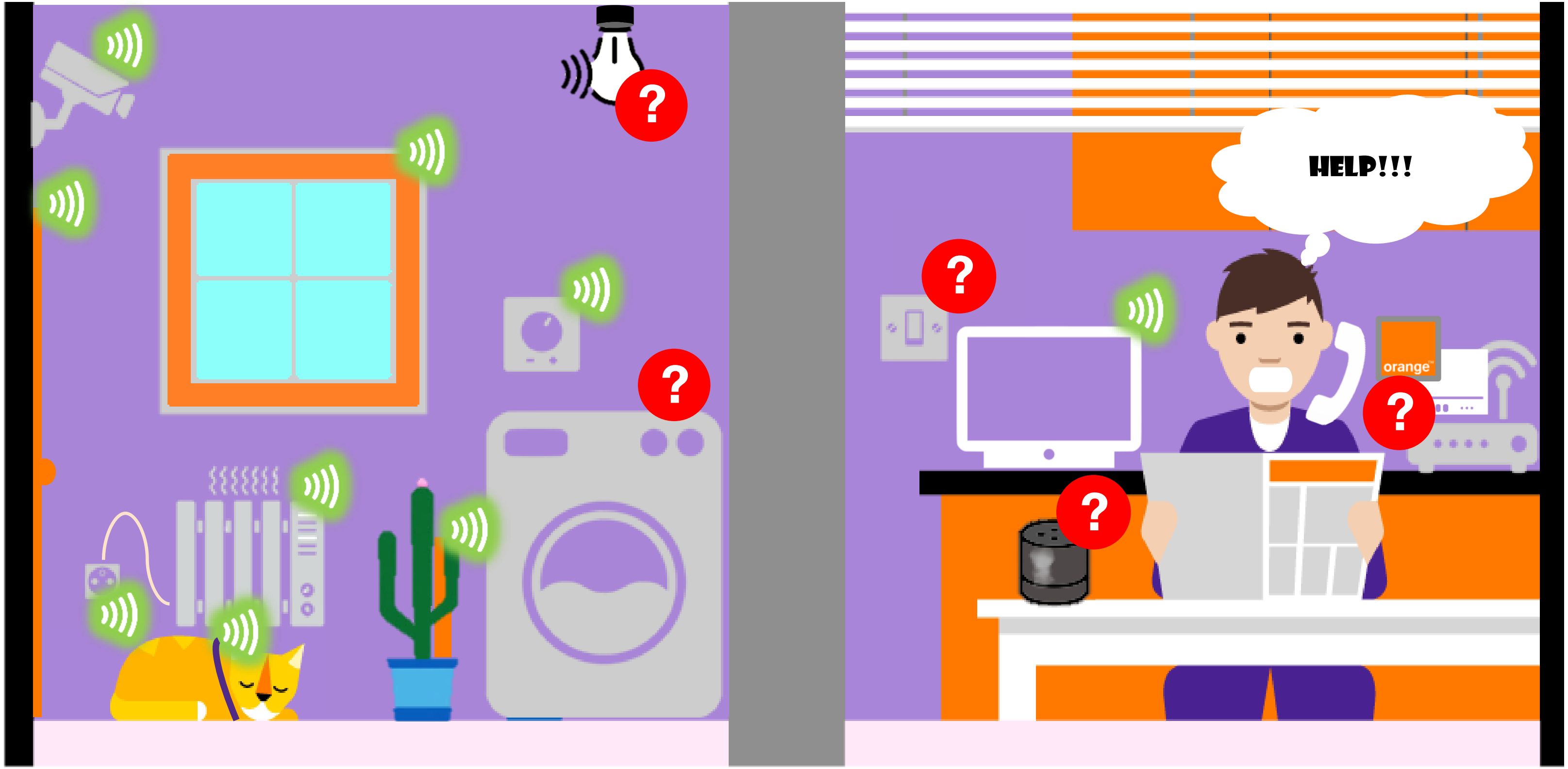
INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON 3

1. Context

Smart Home Device Management



1. Context
Smart Home Device Management



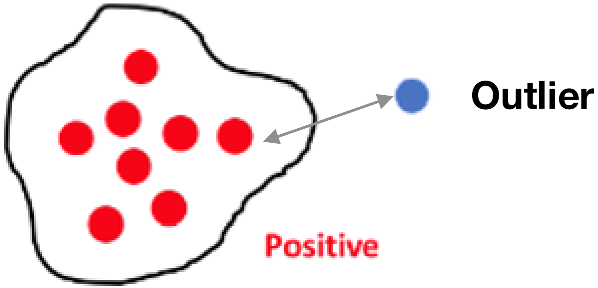
2. Related Work
Time Series Anomaly Detection

Definition:

– Anomalies are patterns in data that do not conform to a well-defined notion of normal behavior [1]

Classical anomaly detectors [2]**: 2 steps**

1. Models the normal expected network behavior
2. Anomalies are deviations of the current behavior from the previously built model



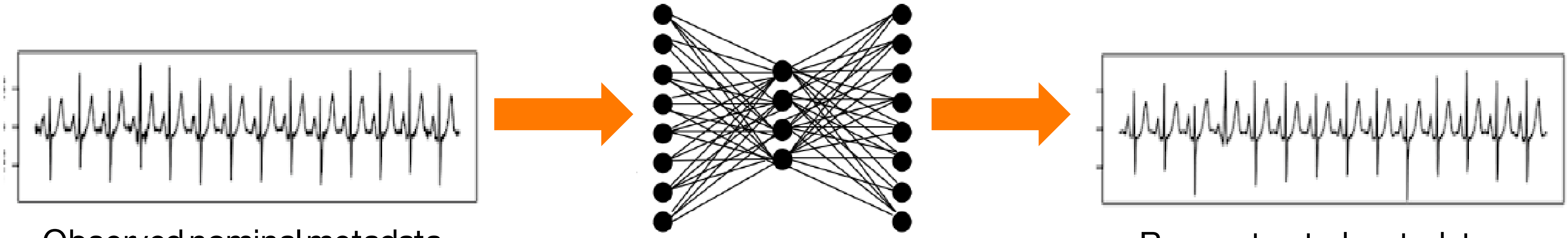
[1] Chandola, V., Banerjee, A. & Kumar, V., Anomaly Detection: A Survey. ACM Computing Surveys, 2009.

[2] Bulusu, Saikiran, Bhavya Kailkhura, Bo Li, Pramod K. Varshney and Dawn Xiaodong Song. "Anomalous Example Detection in Deep Learning: A Survey." IEEE Access, 2020.

2. Related Work

Reconstruction-based anomaly detection:

– Training : train a *sequence-to-sequence AE* model to reconstruct normal data



Observed nominal metadata

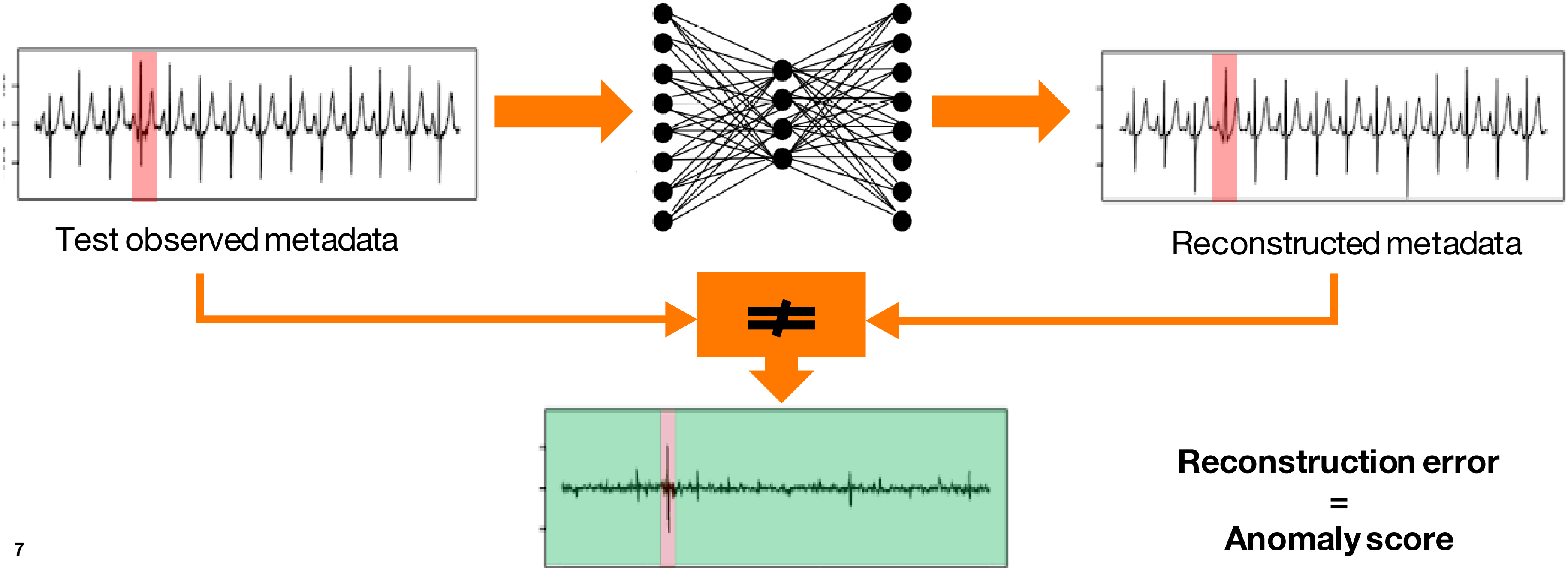
Reconstructed metadata

Objective : minimize the reconstruction error

2. Related Work

Reconstruction-based anomaly detection:

– Training : train a *sequence-to-sequence AE* model to reconstruct normal data
– Testing: detect any large deviation



2. Related Work

Literature Review:

- LSTM-based autoencoder [1]
- LSTM-based variational autoencoder [2]
- RNNs and Normalizing Flows [3]
- Transfomers [4,5,6]

[1] Zhang, Ang, Xiaoyong Zhao and Lei Wang. "CNN and LSTM based Encoder-Decoder for Anomaly Detection in Multivariate Time Series." IEEE 5th Information Technology Networking Electronic and Automation Control Conference (ITNEC), 2021.

[2] PARK, Daehyung, HOSHI, Yuuna, et KEMP, Charles C. A multimodal anomaly detector for robot-assisted feeding using an lstm-based variational autoencoder. IEEE Robotics and Automation Letters, 2018

[3] Su, Ya, et al. "Robust anomaly detection for multivariate time series through stochastic recurrent neural network." Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining. 2019.

[4] Tuli, Shreshth, Giuliano Casale, and Nicholas R. Jennings. "TranAD: Deep transformer networks for anomaly detection in multivariate time series data." 2022.

[5] Xu, Jiehui, et al. "Anomaly transformer: Time series anomaly detection with association discrepancy." 2021.

[6] Wang, Xixuan, et al. "Variational transformer-based anomaly detection approach for multivariate time series." Measurement, 2022.

2. Related Work

Limitations of existing approaches

- RNN-based sequence-to-sequence models:
  - Recurrence: difficult to parallelize training: slow training
  - Short-term memory: bias toward the last part of the sequence

→ **Transformers**

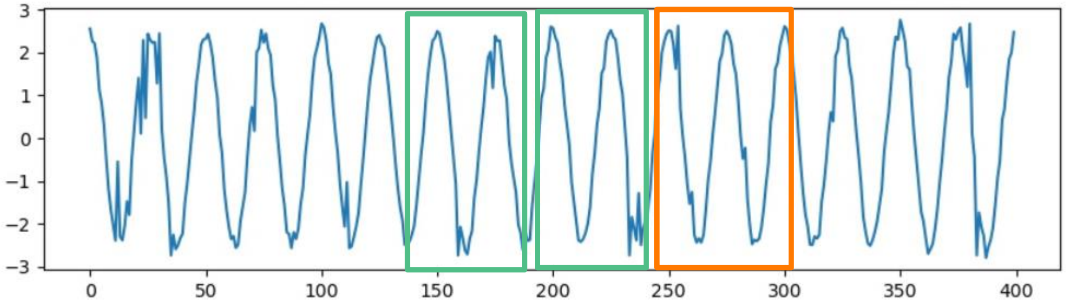
- Anomaly-free training data:
  - Sensitivity to data contamination with anomalies.

→ **Robust loss function and Siamese architecture**

3. Proposed Approach

Problem statement:

– Robust unsupervised time series anomaly detection



Intuition:

– Anomalies are rare by definition : significantly less frequent than the norm.

→ **Rejection criterion:**

  – Split the time series with a non-overlapping sliding window
  – The data point has been observed in the adjacent windows ?

3. Proposed Approach
Siamese-based Architecture

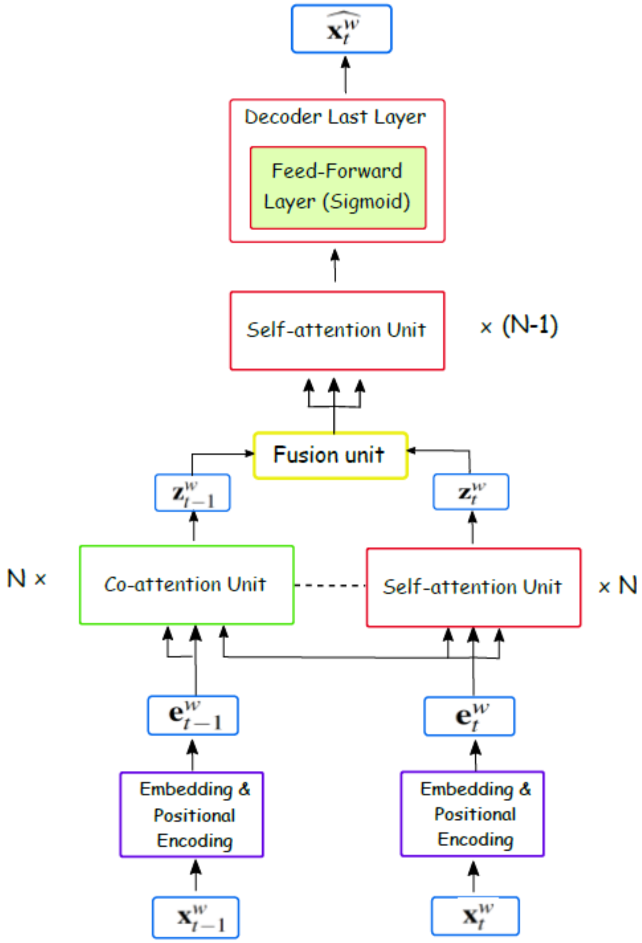


Fig. 1. RESIST architecture.

3. Proposed Approach
Siamese-based Architecture

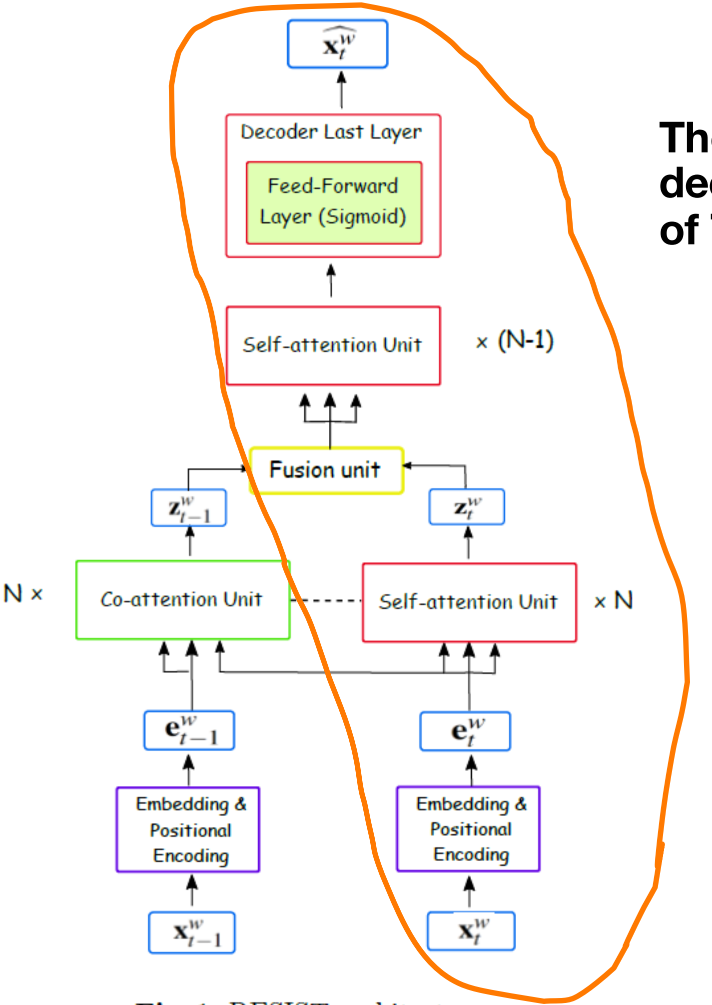


Fig. 1. RESIST architecture.

The classical encoder-decoder architecture of Transformers

3. Proposed Approach
Siamese-based Architecture

Siamese encoder

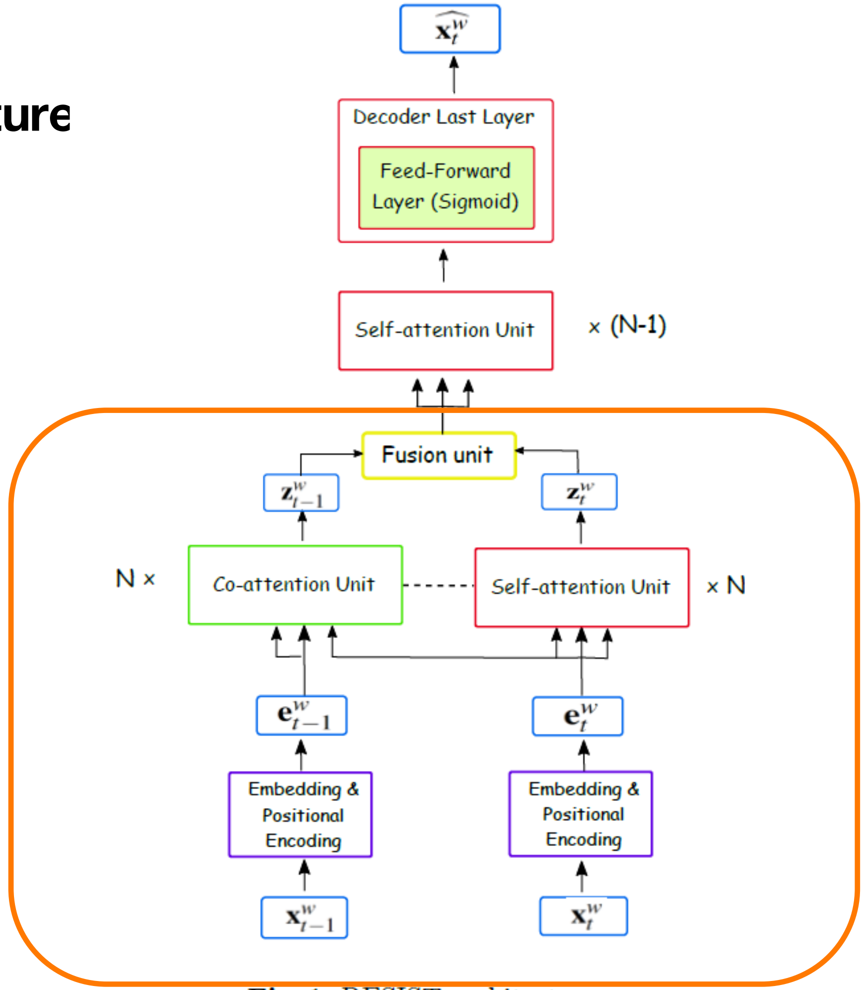


Fig. 1. RESIST architecture.

3. Proposed Approach
Siamese-based Architecture

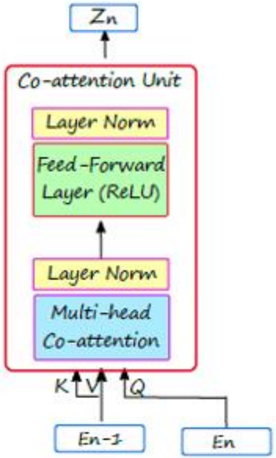
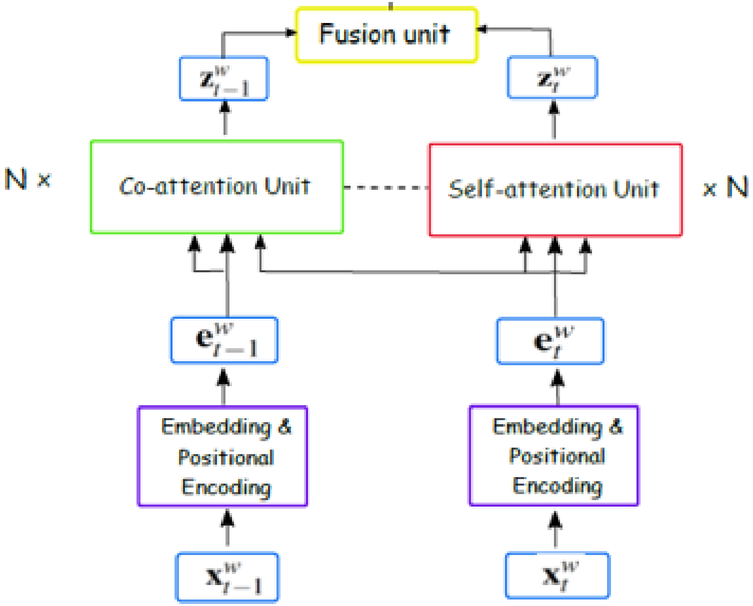


Fig. 3. Co-attention unit



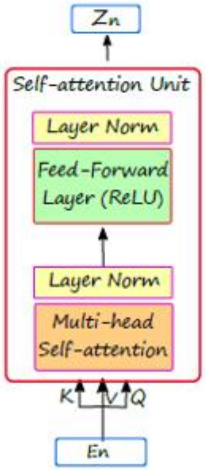


Fig. 2. Self-attention unit

3. Proposed Approach
Siamese-based Architecture

Multiple possible configurations :

- 2 configurations or N = 2 :

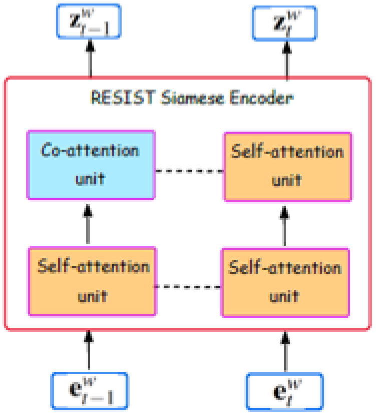


Fig. 6. RESIST-SC

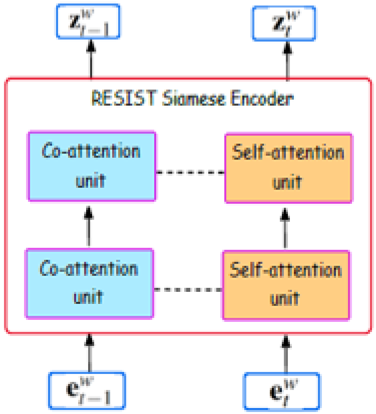
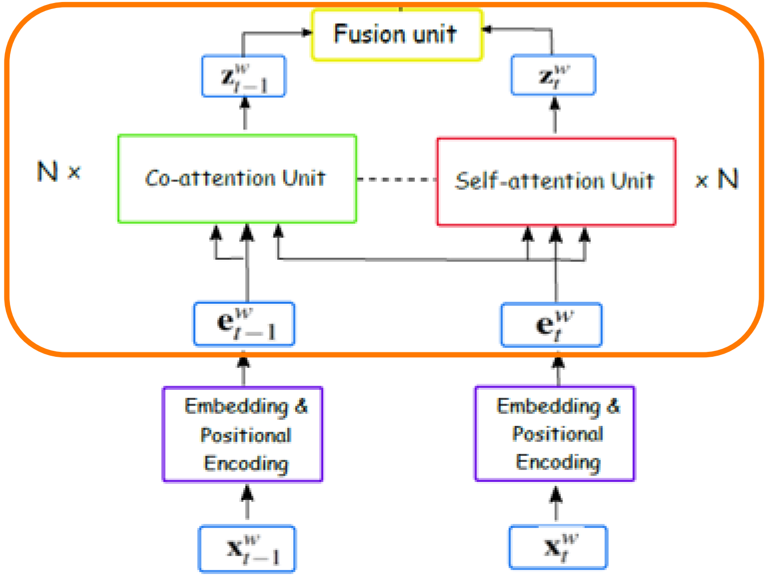


Fig. 7. RESIST-CC



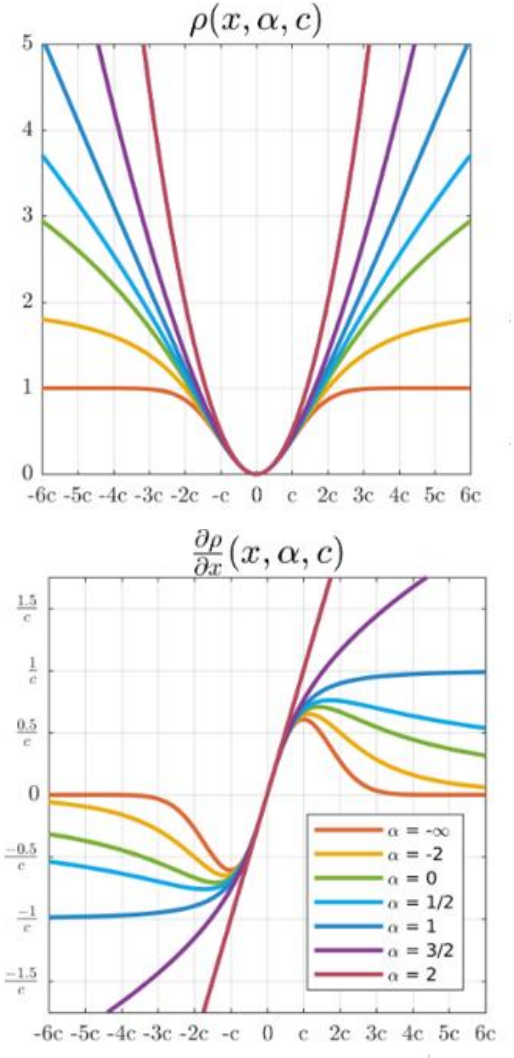
3. Proposed Approach
Robust loss function

- Mean Squared Error (MSE) is sensitive to outliers
  → Robust loss function

- Parametric function that generalizes literature robust functions [1]

$$\rho(x,\alpha,c)=\begin{cases}\frac{1}{2}(\frac{x}{c})^2 & if\ \alpha=2\\ \log(\frac{1}{2}(\frac{x}{c})^2+1) & if\ \alpha=0\\ 1-\exp(-\frac{1}{2}(\frac{x}{c})^2) & if\ \alpha=-\infty\\ \frac{|\alpha-2|}{\alpha}((\frac{(\frac{x}{c})^2}{|\alpha-2|}+1)^{\frac{\alpha}{2}}-1) & otherwise\end{cases}$$

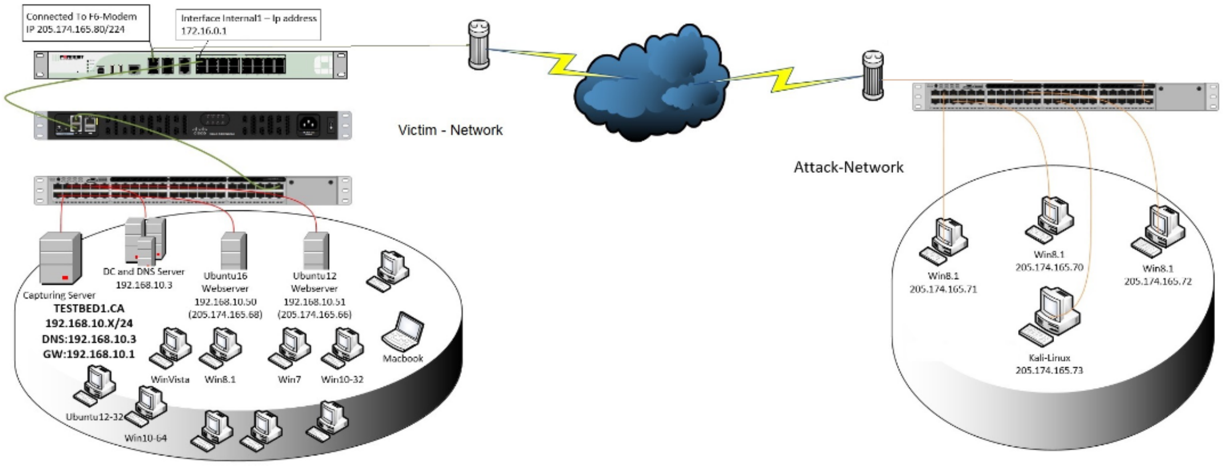
- α: robustness parameter
  - L2 loss ($\alpha = 2$)
  - Charbonnier loss ($\alpha = 1$)
  - Cauchy loss ($\alpha = 0$)
  - Geman-McClure loss ($\alpha = -2$)
  - Welsch loss ($\alpha = -\infty$).



Experimental Results

CICIDS2017 dataset description:

- a public dataset developed by the Canadian Institute of Cybersecurity (CIC) for IDS evaluation.
- ~3 million labeled network flows collected over 5 days, in 2017
- Contextual and collective anomalies: DDoS, web attacks, port scans, heartbleed



[1] Gilberto Fernandes, Joel J. Rodrigues, Luiz Fernando Carvalho, Jalal F. Al-Muhtadi, and Mario Lemes Proença. A comprehensive survey on network anomaly detection. Telecommunications Systems, 2019.

Experimental Results

Comparison with SOTA methods

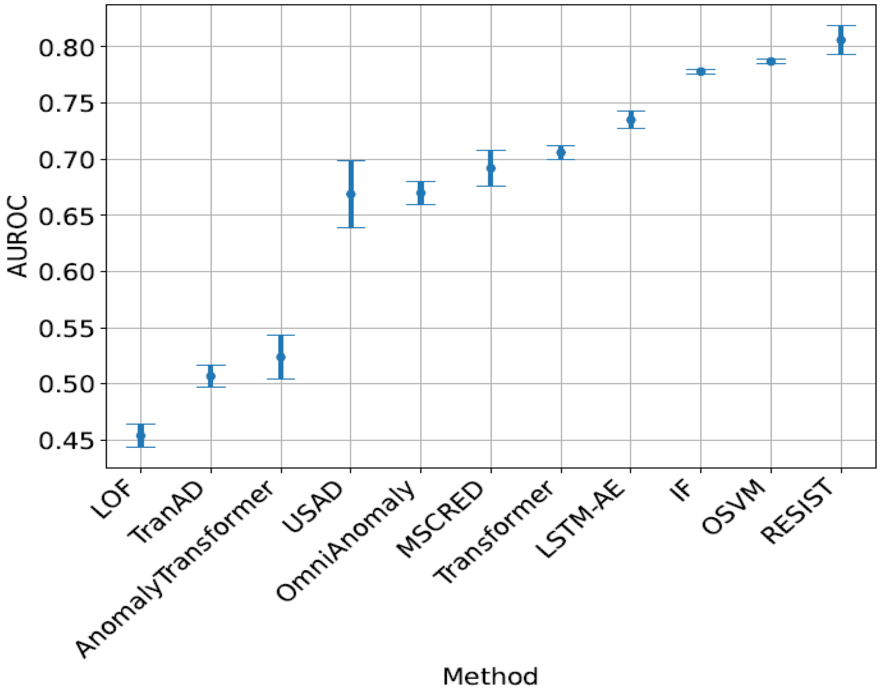


Fig. 10. Comparison between RESIST and the baselines on CICIDS17 dataset.

Experimental Results

Ablation study

Configurations

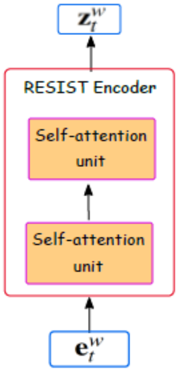


Fig. 5. RESIST-SS

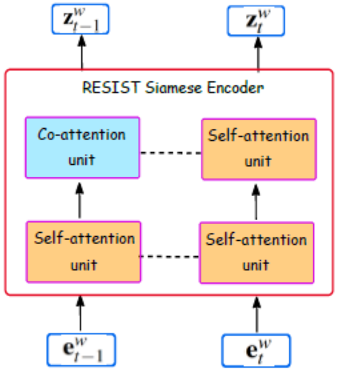


Fig. 6. RESIST-SC

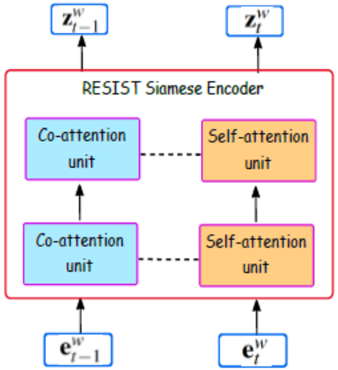


Fig. 7. RESIST-CC

Results

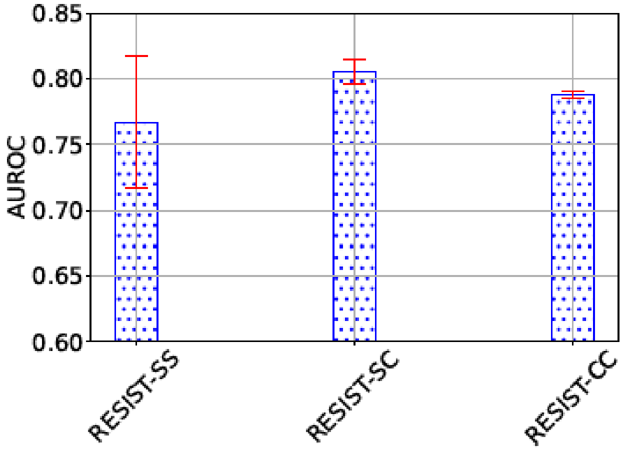


Fig. 8. Comparison between RESIST three variants: RESIST-SS, RESIST-SC, and RESIST-CC, on the CICIDS17.

4. Conclusions And Perspectives

Conclusions:

- RESIST, a Robust Transformer for Unsupervised Time Series Anomaly Detection
  - Siamese architecture: detect infrequent observations, i.e., contaminants
  - Robust training: robust loss function (Geman-McClure Loss)

Limitations and Perspectives:

- Limitation: RESIST is sensitive to the selection of one hyperparameter: the scale parameter of the robust loss
- Perspective: replace the robust training function with an explicit rejection strategy based on the analysis of the reconstruction error distribution (cf. [1,2])

[1] Najari, N., Berlemont, S., Lefebvre, G., Duffner, S., & Garcia, C. RADON: Robust Autoencoder for Unsupervised Anomaly Detection. In 14th International Conference on Security of Information and Networks (SIN) IEEE, 2021.

[2] Najari, N., Berlemont, S., Lefebvre, G., Duffner, S., & Garcia, C. Robust Variational Autoencoders and Normalizing Flows for Unsupervised Network Anomaly Detection. In International Conference on Advanced Information Networking and Application, Springer, 2022.

Thank you

Naji NAJARI naji.najari@orange.com
Samuel BERLEMONT samuel.berlemont@orange.com
Grégoire LEFEBVRE gregoire.lefebvre@orange.com
Stefan DUFFNER stefan.duffner@liris.cnrs.fr
Christophe GARCIA christophe.garcia@liris.cnrs.fr

orange™

LIRIS

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

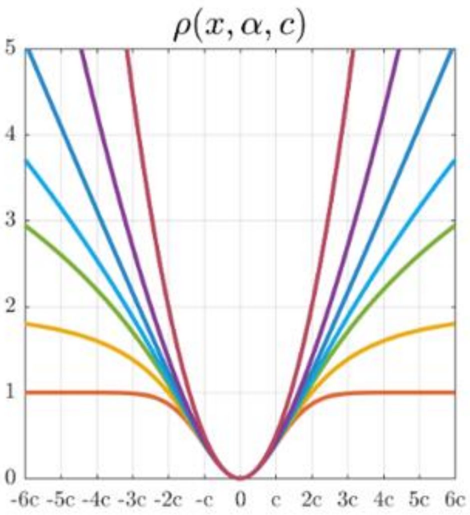
TABLE I: Extracted flow features using NFStream. See [35] for detailed feature descriptions.

Features			Abbreviations
src_port	src2dst_stdev_piat_ms	src2dst_duration_ms	src : source (e.g., src_port means the source port of the packet)
dst_port	src2dst_max_piat_ms	src2dst_packets	dst : destination
protocol	dst2src_min_piat_ms	src2dst_bytes	src2dst : traffic from source to destination
ip_version	dst2src_mean_piat_ms	bidirectional_min_piat_ms	piat : packet inter arrival time.
dst2src_stdev_piat_ms	dst2src_max_piat_ms	bidirectional_mean_piat_ms	stdev : standard deviation
bidirectional_duration_ms	bidirectional_syn_packets	bidirectional_stdev_piat_ms	ps : packet size
src2dst_mean_piat_ms	bidirectional_max_piat_ms	bidirectional_packets	
bidirectional_cwr_packets	bidirectional_bytes	bidirectional_ece_packets	
bidirectional_urg_packets	bidirectional_ack_packets	src2dst_syn_packets	
bidirectional_psh_packets	bidirectional_rst_packets	bidirectional_fin_packets	
dst2src_mean_ps	dst2src_stdev_ps	dst2src_max_ps	
src2dst_cwr_packets	dst2src_duration_ms	src2dst_ece_packets	
bidirectional_max_ps	src2dst_min_ps	src2dst_mean_ps	
dst2src_cwr_packets	dst2src_ece_packets	dst2src_urg_packets	
dst2src_syn_packets	src2dst_max_ps	dst2src_ack_packets	
dst2src_min_ps	dst2src_psh_packets	src2dst_stdev_ps	
dst2src_rst_packets	dst2src_fin_packets	src2dst_min_piat_ms	
dst2src_packets	src2dst_urg_packets	dst2src_bytes	
src2dst_ack_packets	bidirectional_min_ps	src2dst_psh_packets	
bidirectional_mean_ps	src2dst_rst_packets	bidirectional_stdev_ps	
src2dst_fin_packets			

Experimental Results

Ablation study : H1

Configurations



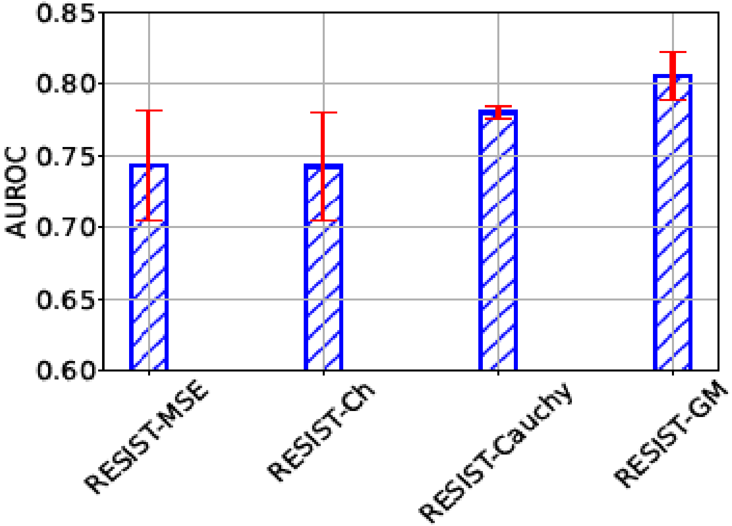


Fig. 9. Experimental results for RESIST trained with different loss functions, on the CICIDS17 dataset.