

---

# Enhancing Network Data Into Cyber-Physical Data For Better Attack Detection Performances

Côme Frappé - - Vialatoux\*<sup>1</sup> and Pierre Parrend<sup>†1</sup>

<sup>1</sup>Laboratoire des sciences de l'ingénieur, de l'informatique et de l'imagerie – Ecole Nationale du Génie de l'Eau et de l'Environnement de Strasbourg, université de Strasbourg, Institut National des Sciences Appliquées - Strasbourg, Les Hôpitaux Universitaires de Strasbourg (HUS), Centre National de la Recherche Scientifique, Matériaux et Nanosciences Grand-Est, Réseau nanophotonique et optique – France

## Résumé

Critical systems are an essential component of today's society, ensuring needs such as water distribution or power supply. The modernization effort of these infrastructures through a general increase in connectedness allows for better efficiency, monitoring, and safety, but also comes with an increased vulnerability to cyber-attacks. Detecting such cyber-attacks as early and accurately as possible is a hard task for which machine learning (ML) algorithms show promising results, leveraging the huge amount of data that network traffic traces constitute. However, cyber-attack also have measurable impacts on physical systems, but the use of data from such systems is lacking due to a scarcity of available datasets and analysis tools. The recent release of cyber-physical datasets, which captured data from both network communication and physical systems, fills this gap, allowing a joint usage of these two data sources. This paper provides a multi-layer methodology for detection in cyber-physical systems, by combining physical and network data and evaluates its gain in detection performances on multiple ML models.

---

\*Intervenant

<sup>†</sup>Auteur correspondant: parrend@unistra.fr