

# Attaque par inférence d'appartenance sur des séries temporelles agrégées en utilisant la programmation par contraintes

Antonin Voyez  
antonin.Voyez@irisa.fr  
Univ Rennes, CNRS, IRISA  
ENEDIS  
France

Tristan Allard  
tristan.allard@irisa.fr  
Univ Rennes, CNRS, IRISA  
France

Gildas Avoine  
gildas.avoine@irisa.fr  
INSA Rennes, CNRS, IRISA  
France

Elisa Fromont  
elisa.fromont@irisa.fr  
Univ Rennes, CNRS, IRISA  
France

Matthieu Simonin  
matthieu.simonin@inria.fr  
Inria, IRISA  
France

Pierre Cauchois  
pierre.cauchois@enedis.fr  
ENEDIS  
France

## ABSTRACT

L'agrégation est largement utilisée comme méthode de protection de la vie privée. Les attaques par inférence d'appartenance sur agrégat ont pour but de déterminer si une cible donnée a participé ou non au calcul de l'agrégat attaqué. Dans cet article, nous étudions la vulnérabilité de séries temporelles agrégées - où chaque point est un agrégat horodaté - face à des attaques par inférence d'appartenance. L'attaquant que nous considérons dispose de connaissances auxiliaires sur un sur-ensemble des données agrégées (e.g., issu d'une fuite de données). Nous proposons une nouvelle attaque tirant parti de ce type de connaissances auxiliaires et des multiples points formant la série temporelle agrégat. Notre attaque

est modélisée comme un problème d'optimisation linéaire en nombres entiers, permettant à l'attaquant de bénéficier de la puissance des solveurs dédiés (e.g., Gurobi). Cette attaque, testée sur des jeux de données publics, montre la vulnérabilité d'une publication de série temporelle agrégat si le nombre de séries agrégées est trop faible face au nombre de points constituant la série.

---

© 2021, Copyright is with the authors. Published in the Proceedings of the BDA 2021 Conference (October 25-28, 2021, En ligne, France). Distribution of this paper is permitted under the terms of the Creative Commons license CC-by-nc-nd 4.0.

© 2021, Droits restant aux auteurs. Publié dans les actes de la conférence BDA 2021 (25-28 octobre 2021, En ligne, France). Redistribution de cet article autorisée selon les termes de la licence Creative Commons CC-by-nc-nd 4.0.