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 vulnérabilé 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 linéraire 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.