Compas'2025 : Parallélisme/ Architecture/ Système
Centre Inria de l'université de Bordeaux - Bordeaux - France, 24-27 juin 2025

AUPE : Protocole collaboratif d'échantillonnage de pairs tolérant aux fautes byzantines

Augusta Mukam, Joachim Bruneau-Queyreix, Laurent Réveillère.

Université de Bordeaux,
Laboratoire LABRI - 351, cours de la Libération
F-33405 Talence cedex - France
Augusta.mukam@u-bordeaux.fr, joachim.bruneau-queyreix@u-bordeaux.fr,
laurent.reveillere@u-bordeaux.fr

Résumé
L'échantillonnage de pairs constitue une primitive fondamentale dans les systèmes distribués, permettant le partage d'informations à grande échelle, notamment dans les blockchains. Son objectif est de maintenir et de mettre à jour dynamiquement une vue locale et partielle de l'ensemble des membres du système. Cependant, ces protocoles sont vulnérables aux attaques de la part d'adversaires cherchant à perturber le fonctionnement des protocoles de plus haut niveau de la blockchain. En particulier, un adversaire contrôlant un ensemble de nœuds byzantins peut manipuler la perception des nœuds honnêtes en augmentant la représentation des nœuds malveillants dans leur vue locale.
Bien que les protocoles d'échantillonnage de pairs tolérants aux fautes byzantines présent dans la littérature atténuent en partie ce biais, leur efficacité diminue significativement à mesure que la proportion de nœuds malveillants dans le système augmente. Cet article introduit AUPE, le premier protocole collaboratif d'échantillonnage de pairs tolérant aux fautes byzantines. AUPE exploite la présence de nœuds de confiance, tels que des dispositifs compatibles avec Intel SGX, afin de suivre de manière collaborative la propagation des identifiants au sein du système et de réajuster localement la représentation des nœuds byzantins.
Des simulations menées sur un réseau de 10 000 nœuds montrent qu'AUPE surpasse les solutions de l'état de l'art, atteignant une résilience quasi parfaite même face à un adversaire contrôlant jusqu'à 26% des nœuds. En intégrant seulement 10% de nœuds de confiance, AUPE améliore la tolérance du protocole BRAHMS de 60%, tout en réduisant considérablement l'impact des attaques adversariales, y compris lorsque l'adversaire possède jusqu'à 40% des nœuds.

Mots-clés : Blockchain, Tolérance aux byzantines, Gossig, Peer sampling, Noeud de confiance.
