Count-min-sketch collaboratifs pour la construction de systèmes distribués résilients aux attaques byzantines

1 Contexte

Le peer sampling est une abstraction de première classe permettant la construction de systèmes distribués à grande échelle. Elle est notamment utilisée pour la gestion des réseaux overlays [Vv13, JMB09] et pour la diffusion d'informations [MSF+13, EGH+03]. En général, les noeuds possèdent une connaissance partielle (également appelée leur *vue*) de la composition globale et dynamique du système. L'objectif du service de peer sampling est de construire et de rafraîchir continuellement cette vue locale afin qu'elle corresponde autant que possible à un échantillon uniforme des noeuds constituant le système. La mise en œuvre du service de peer sampling est généralement basée sur des protocoles de gossip qui implémentent des échanges d'informations périodiques entre pairs. Une pléthore de protocoles ont été publiés et étudiés [VGVS05, JVG+07, ABS13] adressant des problématiques de pannes de noeuds, de churns, de performance, d'ergodicité, et de propriétés structurelles souhaitables telles qu'un in-degree équilibré, un faible diamètre, et la capacité de retirer rapidement les nœuds en panne de la vue des nœuds actifs.

La résilience des protocoles de peer sampling aux fautes byzantines (i.e., aux noeuds malveillants) est cruciale pour la sécurité des applications qui en dépendent. En effet, les nœuds malveillants qui réussissent à être sur-représentés dans les vues des nœuds honnêtes peuvent prendre le contrôle des protocoles de couches supérieures. Par exemple, il a été découvert que le protocole d'échantillonnage par les pairs de Bitcoin était exposé aux attaques éclipse [HKZG15], ouvrant la porte à de multiples types d'attaques telles que le selfish mining ou la double-dépense au niveau du consensus. Dans l'état de l'art des protocoles d'échantillonnage par les pairs résistants aux attaques byzantines [BGK+09, ABS13], les vues des nœuds honnêtes peuvent rapidement être empoisonnées par des identifiants byzantins lorsque la proportion de nœuds malveillants dans le système augmente. Avec BRAHMS [BGK+09], le protocole le plus résistant aux attaques byzantines, les vues des nœuds honnêtes peuvent contenir jusqu'à 81% d'identifiants byzantins lorsque seulement 18% des nœuds du système sont malveillants.

2 Objectif

L'objectif de ce stage est de proposer des solutions permettant d'améliorer la résilience des protocoles de peer sampling face aux attaques byzantines. Pour cela, nous nous proposons de construire à partir des récents travaux RAPTEE [PBB+22] qui se basent sur l'existence, dans le système, de quelques noeuds de confiance qui (1) peuvent se reconnaitre entre eux et (2) ne dévieront jamais du protocole de peer sampling. Dans ces travaux, les noeuds de confiance ralentissent la dissémination des identifiants transmis par les noeuds qui ne sont pas de confiance alors qu'ils font en sorte d'accélérer celle des identifiants transmis par les autres noeuds de confiance.

Afin d'améliorer ces travaux, nous souhaitons explorer la piste qui consiste à utiliser les count-min-sktech, une structure de données probabiliste permettant à un noeud d'estimer la fréquence d'apparition d'un élément dans un flux de données. L'idée consiste à permettre aux noeuds de limiter la probabilité d'ajouter ou de conserver dans leur vue des identifiants sur-représentés. Une première approche [ABS13] a déjà partiellement exploré cette piste en considérant que chaque noeud honnête puisse localement utiliser une telle structure.

Nous souhaitons combiner cette dernière approche avec l'approche de RAPTEE afin de permettre aux noeuds de confiance de collaborer via leurs count-min-sketch pour dépolluer la connaissance partielle qu'ils ont de la composition du système. Ainsi ces noeuds pourraient agir en tant que source d'information la moins biaisée possible pour le noeuds honnêtes.

Environnement et contacts

Profil recherché : Étudiant(e) en M2 université/ 3ième année d'école d'ingénieur motivé(e) par les aspects recherche et développement avec de bonnes connaissances et compétences en programmation dans au moins un langage.

Candidatures : Veuillez joindre un CV et une courte motivation à votre candidature.

Contacts :

- Joachim Bruneau-Queyreix: joachim.bruneau-queyreix@u-bordeaux.fr
- Yérom-David Bromberg: david.bromberg@irisa.fr
- François Taiani francois.taiani@irisa.fr
- Laurent Réveillère: laurent.reveillere@u-bordeaux.fr

References

[ABS13] Emmanuelle Anceaume, Yann Busnel, and Bruno Sericola. Uniform node sampling service robust against collusions of malicious nodes. In *43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, DSN. IEEE, 2013.

[BGK+09] Edward Bortnikov, Maxim Gurevich, Idit Keidar, Gabriel Kliot, and Alexander Shraer. Brahms: Byzantine resilient random membership sampling. *Computer Networks*, 53(13):2340–2359, 2009.

[EGH+03] P Th Eugster, Rachid Guerraoui, Sidath B Handurukande, Petr Kouznetsov, and A-M Kermarrec. Lightweight probabilistic broadcast. *ACM Transactions on Computer Systems (TOCS)*, 21(4):341–374, 2003.

[HKZG15] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In *24th USENIX Security Symposium*, pages 129–144, 2015.

[JMB09] Márk Jelasity, Alberto Montresor, and Ozalp Babaoglu. T-man: Gossip-based fast overlay topology construction. *Computer networks*, 53(13):2321–2339, 2009.

[JVG+07] Márk Jelasity, Spyros Voulgaris, Rachid Guerraoui, Anne-Marie Kermarrec, and Maarten van Steen. Gossip-based peer sampling. *ACM Trans. Comput. Syst.*, 25(3):8–es, August 2007.

[MSF+13] Miguel Matos, Valerio Schiavoni, Pascal Felber, Rui Oliveira, and Etienne Riviere. Lightweight, efficient, robust epidemic dissemination. *Journal of Parallel and Distributed Computing*, 73(7):987–999, 2013.

[PBB+22] Matthieu Pigaglio, Joachim Bruneau-Queyreix, David Bromberg, Davide Frey, Etienne Rivière, and Laurent Réveillère. RAPTEE: Leveraging trusted execution environments for Byzantine-tolerant peer sampling services, March 2022.

[VGVS05] Spyros Voulgaris, Daniela Gavidia, and Maarten Van Steen. Cyclon: Inexpensive membership management for unstructured p2p overlays. *Journal of Network and systems Management*, 13(2):197–217, 2005.

[Vv13] Spyros Voulgaris and Maarten van Steen. VICINITY: A Pinch of Randomness Brings out the Structure. In *Middleware 2013*, pages 21–40, Berlin, Heidelberg, 2013. Springer.