Titre : Detection d'attaques dans les réseaux à très faible latence

Financement : PEPR Cybersécurité (projet SUperviz)

Durée : 24 mois

Contexte : On assiste actuellement une évolution conséquente des bouquets de services à venir à l'échelle de l'Internet (Internet immersif et haptique, par exemple) et par voie de conséquences du trafic réseau sous-jacent, en termes de latence, gigue et régulation de débit. Par ailleurs, l'évolution des piles protocolaires, par exemple avec QUIC, place des fonctions de transport (contrôle de congestion par exemple) dans le user-space, permettant de facilement exploiter ces fonctionnalités à des fins détournées (par exemple *bandwidth starvation*). Dans ce contexte, il apparaît de nouveaux phénomènes que les sondes de supervision classiques qui traitent les flux à échelle gros grain ne voient pas. C'est par exemple le cas des micro-bursts qui peuvent être destructeurs pour les files d'attente des routeurs à très faible latence en induisant temporairement des facteurs conséquents d'augmentation de la latence, qui sont invisibles à l'échelle macroscopique mais néfastes pour les services qui sont censés consommer ces paquets en un temps minimal.

Objectif : Cette proposition de postdoc, faisant suite à une thèse en cours qui développe ce sujet[1],[2] vise à proposer de nouveaux outils de détection fins, de nouvelles métriques caractérisant au mieux les anomalies intentionnelles visant la faible latence et des algorithmes de traitement qui permettent de réagir avec un temps de réaction compatible avec ces contraintes de trafic très fortes.

Approche envisagée : L'approche suivie dans ce postdoc sera avant tout expérimentale. On utilisera la plateforme réseau hébergée à Nancy au sein de l'équipe RESIST pour mettre en œuvre un testbed hébergeant (1) des routeurs L4S qui permettent de router du trafic sous des conditions de très faible latence, et (2) des entités terminales qui permettront d'injecter du trafic émulé/réel ou reproduire des traces de trafic réel soumis à une latence prescrite. On utilisera des implémentations open-source (par ex. pico-quic) comme injecteurs de charge pour reproduire différents modèles d'attaque (unresponsive ECN, micro-bursts, etc.). Les solutions de détection et remédiation seront évaluées par leur capacité à identifier le trafic nocif pour la très faible latence, leur impact sur la performance du routage et leur capacité à permettre au réseau de maintenir une latence prescrite une fois une attaque détectée.

Resultats attendus : Il est attendu de ce travail la conception et la mise en œuvre de solutions de détection d'attaques portant sur la très faible latence réseau ainsi que la contre-mesure associée. On envisage à ce stade des solutions de réseaux programmables (P4) ou de micro-services pour assurer ces fonctions de détection et régulation de trafic.

[1] Letourneau, M., N'Djore, K. B., Doyen, G., Mathieu, B., Cogranne, R., & Nguyen, H. N. (2021, October). Assessing the Threats Targeting Low Latency Traffic: the Case of L4S. In 2021 17th International Conference on Network and Service Management (CNSM) (pp. 544-550). IEEE.

[2] M. Letourneau, G. Doyen, R. Cogranne, B. Mathieu: A Comprehensive Characterization of Threats Targeting Low-Latency Services: The Case of L4S. Journal of. Network andd System Management 31(1): 19 (2023)