ÉLÉMENT DE PORTFOLIO 02

Distinction

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : Prix de recherche d'étudiants de l'équipe Phare

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

Durant la période 2017-2022, les thésards de l'équipe Phare ont eu d'excellentes contributions scientifiques. Nous présentons dans cet élément deux prix de recherche obtenus par nos étudiants.

3 PRÉSENTATION DE CET ÉLÉMENT

3.1 Accessit du prix de thèse du GDR Réseaux et Systèmes Distribués 2021

La thèse de doctorat de Agathe Blaise, intitulée "Nouveaux algorithmes de détection d'anomalies et de classification pour les réseaux IP et mobile" [1], a été soutenue en décembre 2020.

Ces dernières années ont été marquées par une nette augmentation de la fréquence et de la diversité des attaques réseau, qui apparaissent toujours plus sophistiquées et conçues pour être indétectables. En parallèle, l'essor des techniques statistiques et d'apprentissage machine ont permis un développement rapide de techniques innovantes visant à détecter de telles attaques. Cette thèse propose de nouveaux algorithmes de détection d'anomalies et de classification appliqués aux réseaux IP et mobiles.

Dans la première contribution, nous proposons une solution Split-and-Merge qui détecte des botnets (réseau d'ordinateurs infectés qui servent à lancer des attaques) se propageant lentement sur Internet en exploitant des vulnérabilités émergentes. Cette méthode analyse l'évolution à long-terme de l'usage des ports applicatifs. Nous obtenons une très grande précision de détection et très peu de faux positifs grâce aux contre-validations dans divers sous-réseaux. Notre technique de détection est aussi très légère et serait idéale pour être implémenté au niveau d'un switch dans un contexte de réseaux programmables.

La deuxième contribution aborde la détection d'hôtes infectés par un botnet, cette fois en utilisant des techniques de classification au niveau de l'hôte, dans une solution nommée BotFingerPrinting. Les approches récentes de l'état de l'art tendent à délaisser les approches classiques par flux induisant une complexité algorithmique très importante. Notre technique vise à rendre compte des relations entre les hôtes, tout en simplifiant ces graphes de communication pour éviter d'éventuels problèmes de scalabilité. Grâce à une approche supervisée, nous apprenons les signatures des hôtes bénins et des hôtes infectés pour ensuite les classifier dans un jeu de test. Nous démontrons par le jeu de données CTU-13 que notre approche est considérablement plus légère que les approches de l'état de l'art et également plus efficace, avec une précision de détection très importante.

La troisième contribution propose l'algorithme nommé "Anomaly SpatioTEmporal Convex Hull detection" (ASTECH) qui permet la détection d'anomalies brutes dans les séries temporelles des réseaux mobiles, les regroupe en enveloppes convexes spatio-temporelles, et finalement induit plusieurs classes d'événements. Nous avons appliqué notre système de détection sur des données réelles provenant de l'opérateur Orange et montré l'existence de cinq grandes catégories d'événements : les événements nationaux, les évènements locaux, les mises à jour et les pannes applicatives, les jours fériés et les pannes d'un opérateur cloud ou réseau. Nous étudions précisément la nature des applications mobiles impactées pour chaque catégorie d'événements ainsi que l'évolution spatio-temporelle de ces jeux d'applications mobiles pour un même événement.

3.2 Deuxième prix de Student Research Competition à la conférence ACM SIGCOMM 2021

La démonstration "Blockgraph proof-of-concept" [2], présentée par David Cordova, a obtenu le deuxième prix de recherche étudiant (Student Research Competition) à la conférence ACM SIGCOMM 2021, une des conférences

les plus sélectives dans notre domaine. Une vidéo associée à cette publication est disponible (`https://youtu.be/dC37jCzj0tI`).

La technologie Blockchain permet de maintenir un registre des informations d'une manière distribuée tout en garantissant la sécurité des données. Pour bénéficier d'une telle technologie, il est nécessaire de disposer d'une connectivité fiable. Les réseaux maillés ad-hoc mobiles rendent l'utilisation de blockchain difficile car la mobilité des nœuds crée des instabilités dans la topologie du réseau, résultant ainsi des partitions (splits) et des fusions (merges) qui peuvent être intentionnelles ou non. Cela pose un problème pour une blockchain traditionnelle car un split du réseau cause une bifurcation (fork) de la blockchain, ce qui entraîne des chaînes concurrentes et un risque sur la cohérence des données. Ce problème est souvent résolu en choisissant la chaîne la plus longue et ignorant les autres. Or, les chaînes concurrentes créées par l'effet de la mobilité et des partitions du réseau doivent être considérées comme des chaînes légitimes portant des informations relatives à une partition de réseau donnée. Il est donc important d'inclure ces chaînes dans le registre distribué.

Pour faire face aux problèmes de split et merge dans les réseaux maillés adhoc mobiles, nous proposons le Blockgraph, une structure de données de type blockchain capable de gérer les partitions de réseau. Le Blockgraph prend la forme d'un graphe orienté acyclique qui est créé en fonction de la mobilité des nœuds et qui hérite de toutes les propriétés de sécurité de la blockchain. Le Blockgraph utilise une architecture modulaire qui sépare le consensus, la gestion de mobilité et la gestion du registre distribué. Chaque module de notre architecture est conçu pour fonctionner dans un contexte de mobilité. Nous avons également conçu le Consensus-for-Mesh (C4M), un algorithme de consensus tolérant aux partitions réseaux inspiré de RAFT. La gestion de mobilité est basée sur l'exploitation des tables de routage d'Optimized Link State Routing Protocol (OLSR) pour déterminer les changements qui ont lieu dans la topologie du réseau.

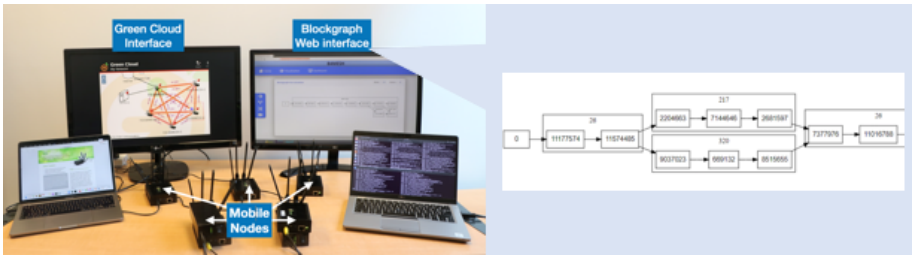

FIGURE 1 – Blockgraph

Pour évaluer notre concept de Blockgraph, nous avons commencé par implémenter notre architecture dans le simulateur réseau NS-3 pour réaliser une première étude des performances du système. Puis nous avons implémenté le Blockgraph dans de vrais routeurs maillés comme une preuve de concept. Notre banc d'essai est composé de cinq routeurs maillés à faible consommation déployés au laboratoire LIP6. Tous les routeurs exécutent le système Blockgraph. La démonstration consiste à créer une partition réseau en éloignant deux routeurs maillés des trois autres jusqu'à ce que le réseau soit partitionné en deux clusters. Nous laissons les clusters se séparer suffisamment longtemps pour qu'ils puissent générer de nouveaux blocs. Lorsque les clusters sont réunis à nouveau, notre système a pu fusionner les deux chaînes en une seule structure de données formant ainsi le Blockgraph.

4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Agathe Blaise. *Novel anomaly detection and classification algorithms for IP and mobile networks*. PhD thesis, 2020. Thèse de doctorat dirigée par Secci, Stefano Informatique Sorbonne université 2020.

[2] David Cordova Morales, Pedro Velloso, Alexandre Guerre, Thi-Mai-Trang Nguyen, Guy Pujolle, Khaldoun Alagha, and Guillaume Dua. Blockgraph proof-of-concept. In *Proceedings of the SIGCOMM '21 Poster and Demo Sessions*, SIGCOMM '21, page 82–84, New York, NY, USA, 2021. Association for Computing Machinery.