



Projet ANR: MOSAICO
Multi-layer Orchestration for Secured and low lAtency appllCatiOns
Projet No.: ANR-19-CE25-0012

Compte-Rendu Meeting #11
15-16/06/2022
Orange - Lannion

Participants:

- Orange : Bertrand Mathieu, Joël Ky, Stéphane Tuffin, Olivier Dugeon, Laure Ki
- ICD-UTT : Guillaume Doyen, Marius Letourneau, Hichem Magnouche
- Montimage : Edgardo Montes De Oca, Huu Nghia Nguyen
- CNRS-Loria : Thibault Cholez, Philippe Graff, Xavier Marchal

L'agenda proposé est validé.

Administratif/Dissémination :

- Site Web

L'UTT doit mettre à jour le site Web pour y ajouter les derniers comptes-rendus de réunion, les derniers papiers acceptés et les informations vers les jeux de données open data.

- Réunions

La prochaine réunion plénière en physique aura lieu à Nancy, sous organisation Loria, début octobre. Il reste à finaliser la date en fonction de la réponse de Guillaume, attendue pour fin juin.

PA Guillaume : Remplir dès que possible.

PA Thibault : Réserver la salle et préparer l'organisation de cette réunion.

La réunion plénière suivante aura lieu en décembre à Paris Chatillon, dans les locaux d'Orange, mais sous hébergement Montimage.

PA Bertrand : Proposer un Doodle pour valider les dates et réserver une salle.

PA Edgardo : Préparer l'organisation de cette réunion et voir avec Eures pour les pause-café, tickets repas, etc.



La prochaine visio-conférence de suivi de projet prévue le lundi 27 juin est annulée et celle du 11 juillet est décalée au vendredi 08 juillet. Les 2 réunions suivantes (25 juillet et 8 août) sont annulées pour congés.

- Dissémination

Le papier JNSM cloud gaming et le papier JNSM L4S Secu ont été soumis le 31 mai au journal JNSM special Issue « Special Issue on High-Precision, Predictable and Low-Latency Networking ». La notification devrait être rendue dans les 2 mois.

Le papier sur la détection de trafic cloud gaming va être soumis à CNSM. Il a été décidé pour ce papier de se focaliser sur la détection de trafic cloud gaming en VNF uniquement, avec les micro-services de capture, report, classifier, aggregator. La partie détection en P4, bien plus complexe qu'initialement prévue, pourra faire l'objet d'un papier ultérieurement. Une dernière relecture a été faite par Thibault.

PA Philippe: Soumettre le papier sur le site EDAS le 17 juin.

Stéphane va reprendre le papier à soumettre à IEEE Comm Mag. L'objectif est de le finaliser et soumettre avant les vacances. C'est un papier de positionnement, pas trop technique.

PA Stéphane : Finir la réécriture du papier.

PA Tous : Relire, corriger, adapter, etc.

Suite à l'acceptation de son papier NetSoft, Hichem envisage de soumettre un papier journal (par ex TNSM en appel libre) avec son modèle amélioré/adapté et en faisant plus de tests, etc. L'objectif est de soumettre mi-juillet.

Il est envisagé de soumettre un papier Montimage/Orange/UTT sur L4S/P4/INT au Workshop HiPNet'22. La deadline est le 22 juillet.

Huu-Nghia doit initier ce papier. Une réunion doit être mise en place rapidement pour discuter de cette activité et organiser le papier.

PA Bertrand : Organiser une réunion.

PA Huu-Nghia : Réfléchir à la structure du papier et aux contributions possibles.

En fonction des avancements de l'étude de Joël, il est prévu de soumettre un papier à HiPNet'22 sur la détection d'anomalie dans le trafic cloud gaming.

PA Joël : Avancer sur les jeux de données, les solutions ML et l'évaluation des modèles.

PA Bertrand : Voir pour organisation du papier ensuite.

Les traces de tests cloud gaming, ainsi que les traces capturées (txops) sur le réseau Orange 4G sont mises en Open Data sur le serveur du Loria : <https://cloud-gaming-traces.lhs.loria.fr/index.html>

Joël a contacté le MIT pour proposer en Open Data sur le github de Mahimahi les traces capturées (txops) sur le réseau Orange 4G. Un « pull request » a été fait, nous sommes en attente de la décision d'intégration ou pas. Si positif, cela serait un bon résultat de dissémination d'Open Data, résultats du projet, à l'extérieur.



Tous les thésards du projet (Hichem, Joël, Marius, Philipe) ont réussi leur passage de CSI (ou CIS). Félicitations à eux.

Edgardo annonce vouloir déposer un projet sur la sécurité à l'appel Horizon Europe pour novembre. Guillaume est intéressé pour en savoir plus sur cet appel et le projet. Stéphane aussi, par pour l'équipe Orange impliquée dans MOSAICO mais une autre.
PA Edgardo : Envoyer un mail sur cet appel.

Bilan des derniers tests et 1ères réflexions sur la solution de détection : Marius

Marius a présenté les derniers résultats de ces tests.

Parmi les représentations, il y a une décomposition en PCA assez claire et orthogonale, démontrant bien le fonctionnement de L4S. Dans ses résultats, la comparaison d'un cas normal et d'un cas « malveillant » (ECN unresponsive, micro-burst, burst regulier) est assez nette et différente. Par exemple, les PCA sont différentes : constitués par des métriques différentes ou avec des poids différents, des angles de rotation suivant le cas, etc.). Il y a un peu moins d'impacts avec le cas burst régulier.

Dans ses travaux, Marius détecte l'évènement (quand cela arrive), mais ne le voit pas en état stationnaire (s'il commence l'analyse quand déjà dans cet état).

Il est vu que la détection de flux peut être fait en asynchrone (donc peut-être moins de contraintes).

Pour la suite, il faudra décider d'un premier cas (quelle attaque d'abord) pour valider, avant de passer à un suivant.

PA Marius : Choisir le cas prioritaire et partir sur la détection du trafic malveillant.

Faisabilité d'implémenter la détection sécurité avec la sonde MMT : Huu-Nghia

Huu-Nghia rappelle l'architecture de la solution de détection sécurité avec MMT.

Les règles de sécurité peuvent être chargés dynamiquement.

Nous voyons que nous pouvons faire le traitement off line, en appelant par exemple des méthodes Python, etc.

Montimage prend le lead sur la partie testbed pour L4S/P4/INT/sécu et va refaire un testbed local pour pouvoir reproduire les tests de Marius et y intégrer MMT, L4S, P4 et INT.

Il faut aussi voir ensemble les métriques dont on a besoin (toutes les métriques utiles à Marius ne sont pas prises en compte dans la librairie INT de base de P4, comme par ex les marquages ECN ou step-marks, etc.) et voir comment on les remonte (soit en mode in-band et avec une sonde MMT dans le réseau, soit en out-of-band, vers un collecteur). La 2^{ème} option semble privilégiée car cela permet au collecteur de pouvoir gérer plusieurs nœuds P4/L4S.

Il faudra aussi réfléchir aux scénarios de test pour la détection et sécurité.

PA Bertrand : Organiser une audio-conf avec Montimage/UTT/Orange pour discuter de tout cela et permettre la mise en place du testbed chez Montimage.



Evolution de la solution d'orchestration et derniers résultats : Hichem

Suite aux échanges lors des précédentes réunions et à son CSI, Hichem a abandonné le parallélisme externe dans son modèle, car c'est trop complexe à faire, pour notamment reconstruire les paquets ensuite.

Hichem a fait évoluer son modèle avec 2 types de SFC (LL et BE) et en ajoutant un poids de SFC LL et SFC BE pour favoriser le placement des SFC LL. Après différents tests, il obtient à chaque fois un résultat équivalent quel que soient les poids. Cela s'explique car les contraintes BE (80ms) sont très larges, donc toujours respectées. Il ne sert donc à rien de complexifier le modèle avec des poids.

Durant les échanges, nous nous sommes posé la question de la borne pour les SFC BE. Ne faudrait-il pas plutôt définir une borne minimum (par ex SFC BE toujours > à 80ms), plutôt que maximum (< 80ms) comme fait dans les tests d'Hichem. Eventuellement, même tester avec aucune contrainte pour les SFC BE.

PA Hichem : Voir si possible de modifier le modèle ainsi, faire les tests et comparer les résultats pour voir si cela donne quelque chose de différent.

Dans ces tests, Hichem configure des SFC de taille non connue (aléatoire dans le modèle), donc des SFC LL peuvent être très longues et des BE moins. Cela serait intéressant de faire des tests avec des SFC de taille identique pour voir si résultat différent.

PA Hichem : Faire les tests et comparer les résultats.

On se pose aussi la question de savoir s'il ne serait pas judicieux de placer d'abord les SFC LL puis les SFC BE, avec un modèle en 2 étapes (voir si cela revient à faire 2 modèles et lancer 2 fois ?). Ensuite, il faudra comparer avec le modèle initial pour évaluer si plus de SFC LL sont déployées ou pas.

PA Hichem : Faire cette évolution et les tests et comparer les résultats.

Bilan des derniers tests avec Mahimahi : Xavier

Xavier rappelle les contraintes de tests fixes et les résultats et comportements des PFs.

Ensuite, il présente les résultats en situation réseaux cellulaires avec les tests mahimahi et les réactions des PFs suivant les différentes traces txops.

Un objectif de l'étude est d'analyser les stabilités des PFs.

Parmi les tests à venir possible, il serait intéressant de voir si ce serait meilleur avec L4S et un algo de contrôle congestion, mais ce n'est pas certain, car CG joue sur le codec vidéo pour l'adaptation, qui est moins réactif que le protocole de transport comme TCP.

Mais avant, il serait aussi intéressant de tester les flux CG en passant via des AQMs pour voir si les PFs s'adaptent et comment et si c'est mieux. Pour ces tests, il est convenu de faire une réunion Loria-Oranger.

PA Bertrand : Organiser une réunion Loria-Orange sur les tests CG avec AQMs.

Nous avons rediscuté de la possibilité de trouver un radar global qui regroupe toutes les analyses/conclusions sur un schéma unique. Ce ne paraît pas simple, mais ce serait très bien. Le Loria n'a pas trouvé, Orange va essayer.

PA Stéphane/Bertrand : Voir si possible de définir un tel radar.



Enfin, il a été discuté de la possibilité de présenter ces résultats à un congrès/forum CG avec des acteurs industriels. A voir si on trouve une cible intéressante.

PA Loria/Orange : Voir si congrès/forum intéressant pour présenter ces résultats.

Méthodes IA pour détecter le trafic CG et 1ères réflexions sur méthode de configuration : Philippe

Philippe rappelle le testbed mis en place, les configs de tests, les features extraits et les modèles de classifieur.

Un papier (« Assessing the Privacy Benefits of Domain Name Encryption ») a montré que les adresses IP des services ne changent pas si souvent et cela pourrait être un indicateur important. Peut-être pas pour l'apprentissage du modèle, mais peut-être en 2^{ème} phase pour confirmer la classification.

PA Philippe/Thibault : Lire le papier et voir si possible d'intégrer cela à la fin de l'analyse.

Actuellement, il y a une erreur dans le modèle, puisqu'il détecte le trafic iperf3 comme du CG. Il faudrait enrichir le jeu de données Non-CG pour avoir plus de services.

Orange va voir s'il peut entraîner/tester le modèle avec un jeu de données Otarie pour enrichir les services non-CG.

PA Bertrand : Organiser une réunion Loria-Orange sur les tests CG avec trafic réseau réel.

Actuellement, le modèle détecte les PFs apprises mais pas les autres ou difficilement, ce qui fait que le modèle n'est pas trop généralisable. Il faudrait voir comment pouvoir généraliser : autre modèle ? Autre solution IA ?

Enfin, Philippe présente son implémentation du modèle en P4: comment cela est fait mais aussi les limitations dues à P4. Le code revient à faire des conditions (Decision Tree) et actions pour décision trafic CG ou pas en fonction des valeurs conditions.

Il n'est pas possible de faire 2 lookups dans la même table, donc Philippe a fait 2 tables identiques pour up et down.

Le Loria et Orange vont continuer sur cette implémentation P4 (linux puis surtout hardware) et on pourra ensuite penser à rédiger un papier de retour d'expérience.

PA Laure : Continuer à essayer de porter ce code P4 Linux sur le Tofino.

Equipement programmable P4 matériel : Laure

Laure présente les différences entre le modèle v1model (switch Linux) et le modèle tna (modèle adapté au switch hardware Tofino).

Laure présente aussi les caractéristiques du switch hardware EdgeCore avec le chipset Tofino, et notamment les capacités physiques matériels : 2 pipes de 16 Gbit/s chacun, 12 MAUs par pipe, 16 tables par MAU, etc.

Elle décrit ensuite les limitations du switch hardware et les recommandations de programmation.

Enfin, Laure montre comment écrire le code P4, le compiler et le déployer sur le chipset. Actuellement, le déploiement n'est pas dynamique et nécessite un arrêt/redémarrage du composant.



Suite à discussion, il est vu qu'il serait intéressant de mesurer le temps d'indisponibilité du switch pendant le téléchargement/mise à jour du code P4 dans le chipset.

PA Laure : Mesurer ce temps quand elle pourra le faire.

Parmi les échanges, on a vu les limitations de P4, mais serait-ce bloquant pour l'évolution/déploiement de P4 ? Il serait bien de connaître le panorama du monde autour P4 : industriels, fabricant switch, chipset. Etc. Olivier va regarder.

PA Olivier : Faire un petit document sur l'écosystème P4 et les éventuelles roadmaps.

Diagnostic de dégradation de la qualité CG : Joël

L'objectif de ces travaux est d'essayer de détecter les dégradations de qualité de sessions cloud gaming (en détectant une anomalie) et éventuellement identifier la cause.

Pour cela, Joël a fait un testbed et pour ses tests, collecte des métriques WebRTC (en parallèle, il enregistre les traces wireshark).

Joël a ensuite fait une analyse de ces valeurs, en fonction des fichiers mahimahi joués, en traçant des courbes mais même si des tendances ressortent, il est difficile d'en tirer des généralités. Il a donc réfléchi à l'utilisation de CPA, de matrices de corrélation ou d'arbre de décision pour aider. Plus tard, des modèles IA plus évolués (isolation forest, réseaux GAN, auto-encodeurs, etc.) pourraient être utilisés.

Suite à discussion, il est proposé de voir s'il serait possible d'accéder aux infos de GeForceNow natives, qui pourraient compléter les données collectées.

Pour le changement de résolution vs débit, il faudra essayer de voir si Joël peut trouver l'information relative au quantification factor.

PA Joël : Voir s'il peut trouver ces infos pour enrichir son jeu de données.

Sur les courbes, on peut voir un léger décalage entre les freeze et le RTT. Est-ce dû à l'affichage (plot des données) ou à un horodatage des données pas cohérente. IL faut vérifier.

PA Joël : Vérifier horodatage des traces.

Concernant la matrice de corrélation, il ne faut pas s'arrêter à une seule matrice. Il faut faire plusieurs matrices, par ex en situation normale et en situation freeze et ainsi observer d'éventuelles différences qui pourraient permettre de détecter une anomalie. De même, on peut imaginer faire une matrice de corrélation sur fenêtre glissante et voir l'évolution des valeurs. Par ex, on pense qu'il pourrait y avoir une corrélation gigue vs débit qui évolue en fct normal et anormal.

PA Joël : Faire toutes ces matrices de corrélation et analyser.

Il faudra aussi voir s'il n'y a pas de problème avec des valeurs catégorielles (0,1 : freeze ou résolution) vis-à-vis des autres.

Il y a actuellement une inefficience du modèle car le jeu de données normal n'est pas bon vs le jeu de tests. Il faut voir pour faire un jeu de données vraiment normal pour pouvoir comparer avec les situations anormales. On peut extraire des parties dans les fichiers, ou peut-être simplement jouer (en capturant les données) et voir humainement si anormal ou pas et noter le moment.

PA Joël : Voir pour obtenir un jeu de données normal.



Joël a fait une ACP pour réduire le nombre d'échantillon, il faudrait aussi faire une ACP qui réduit les dimensions. Cela apporterait peut-être d'autres infos. Et avec ces nouvelles métriques ACP réduites et éventuellement les nouvelles données, on pourrait peut-être identifier des anomalies, en observant une rotation des axes ou des valeurs différentes sur les axes, etc.

PA Joël : Faire une ACP pour réduction des features.

Parmi les approches discutées, nous avons aussi mentionné la solution avec un apprentissage supervisé en prenant la valeur client QoE pour labelliser les données et en utilisant les valeurs réseau pour apprendre. Cela pourrait peut-être permettre de faire ce diagnostic uniquement avec les données réseau.

Livrable D1.2

Le livrable D1.2 « Final description of micro-services and preliminary architecture » est dû pour fin juin 2022. Il y aura du contenu, peut-être plus ou moins détaillé suivant les sections, mais il y aura ensuite le livrable D2.1 pour les implémentations et évaluations des micro-services. Nous décidons que dans le D1.2, nous rédigerons principalement la description des micro-services (détecteur de trafic CG Python et P4, détecteur sécurité, INT P4, P4 L4S, Anomalie CG, etc.) en #1,5 page. Cette section de base pourra être complétée avec des analyses ou mesures mettant en évidence certains problèmes, limitations, qui conduiront à la réalisation des micro-services (par ex tests de Xavier ou Marius, etc.).

PA Tous : Insérer dans le D1.2 le contenu de chaque micro-services dont le partenaire est responsable.

Concernant la partie orchestration de MOSAICO, il est convenu que nous n'orchestrerons pas dynamiquement les modules P4 (déployés plutôt de manière figée, avec un redémarrage nécessaire du switch et avec des fréquences de mises-à-jour très rares) mais que nous orchestrerons les composants applicatifs VNF, comme les modules de détection sécurité et détection CG (ex : détection CG avec plusieurs modules).

Il y a eu une discussion sur la solution d'orchestration. Nous décidons de ne pas prendre ONAP, envisagé au lancement du projet, car cette solution est trop complexe, lourde à mettre en œuvre et pas totalement adapté à nos besoins. Deux solutions ont été abordées : EMOC (Edge Multi-Cluster Orchestrator), un orchestrateur pour les clusters Kubernetes (Linux Fondation) ou MANO (Open Source NFV Management and Orchestration), un orchestrateur défini à l'ETSI, et déjà connu de Montimage.

PA Montimage : Etudier les 2 solutions et sélectionner la plus adaptée et pertinente.

Dans le projet, nous ne retenons pas le use-case de station désagrégée (RU, DU, CU) pour notre implémentation et testbed, mais cela pourrait servir de cas d'usage à Hichem pour valider son modèle.

Enfin, nous avons fait une session sur les testbeds.

Pour l'instant, nous ne pouvons pas converger sur la réalisation d'un testbed unique intégrant tous les modules étudiés dans le projet, car les solutions P4/L4S/INT utilisées par exemple avec le module de sécurité L4S, n'est pas utilisable avec les activités cloud gaming. Cela pourrait éventuellement être fait quand Xavier aura finalisé notre



propre plateforme de CG, en ayant intégré L4S à RTP et en pouvant piloter codec pour CG. Pour s'aider, Xavier peut regarder Scream et le White paper d'Ericsson (Enabling time-critical applications over 5G with rate adaptation).

Pour l'instant, nous décidons donc de faire 2 testbeds : 1 testbed basé sur L4S avec des flux à générer et intégrant des nœuds P4/L4S/INT et utilisé avec le module de détection L4S Secu ; 1 autre testbed pour le CG avec plateformes CG, détecteur de trafic CG et détecteur d'anomalie CG. Il est prévu de faire ce testbed avec des accès 4G/5G, avec OAI, les serveurs CG à distance et avec plusieurs clients mobiles (faire bouger client UE) et des flux concurrents pour avoir conditions radio qui évoluent. Montimage va héberger les 2 testbeds.

PA Montimage : Mettre en place ces 2 testbeds physiques.

PA Tous : Fournir tous les codes des modules et docs/infos nécessaires à Montimage.

Photos souvenirs de cette réunion plénière à Lannion

