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

Compte-Rendu Meeting #14
29/03/2023
UTT/IMT- Rennes

Participants :

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

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, ajouter le livrable D234 et pour chaque livrable, inclure les PDF.

- Réunions

La prochaine réunion plénière en physique aura lieu à Lannion les 6 et 7 juillet, sous organisation Orange.
PA Bertrand : Réserver une salle et préparer l'organisation.

Ensuite, il est prévu une dernière réunion de fin de projet fin novembre, à Nancy ou à Paris, encore à décider.
Une journée en visio-conférence sera organisée fin septembre (et peut-être fin octobre si nécessaire) pour finaliser les dernières contributions, résultats, livrables.

Les visio-conférences de suivi de projet prévue les lundi 11 avril et 8 mai sont annulées (jours fériés).

- Dissémination

Hichem va soumettre sa révision révisée du papier TNSM début avril. Il a fait évoluer le papier sur impact de la mutualisation/parallélisation avec plusieurs cas, a refait quelques tests pour prendre en compte les reviews.

Joël va soumettre sa révision révisée du papier TNSM pour mi avril. Il a fait des tests complémentaires de ses 8 modèles sur PSN et XC (en plus de STD dans la version initiale) et évaluer avec l'approche PA%K comme suggéré par un reviewer. Il doit aussi mieux expliquer l'objectif du papier et l'explication des seuils et métriques pour la dégradation de QoE. Il faudrait s'inspirer des autres papiers de recherche pour appuyer la démarche d'évaluer les modèles à partir d'un ground truth. Et il faut bien circonstancier le papier en précisant les conclusions pour ce cas d'usage. Joël doit aussi faire la réponse aux reviewers.

Le papier IEEE Network sur l'analyse du trafic Airlink pour la VR/Metavers est reviewé en révision majeure. Thibault a demandé le délai pour faire la révision, mais pas de réponse. Thibault va reprendre Xavier en CDD et il pourra travailler dessus.
Il faut faire une réunion Orange/Loria la semaine prochaine pour voir comment adresser les commentaires et choisir des directions.
PA Thibault : Organiser cette réunion.

Orange et le Loria finalisent un papier pour soumettre à ISCC sur la détection de CG en micro-services multi-niveaux avec un module P4 pour l'extraction des features et un modèle ML non supervisé. Le papier est quasiment finalisé.
PA Joel : Soumettre le papier.

Nous n'avons toujours pas de nouvelles du MIT, suite à la proposition de donner en Open Data les traces Mahimahi capturées (txops) sur le réseau Orange 4G.
Il est décidé d'essayer de mettre plus en avant ce jeu de tests et le lien de téléchargement, par exemple en soumettant un papier pour les présenter et les caractériser. Ce peut être un Short Paper dans une très bonne conf measurement comme IMC/TMA avec track dataset ou une autre conf data à cibler. Il est aussi possible de déposer sur IEEE DataPort.
Il est aussi envisagé de refaire des traces plus récentes pour avoir un dataset 5G.

Xavier devant être réembauché au Loria, nous verrons avec lui pour les scripts pour faire des stats des traces.
PA Joël/Bertrand/Stéphane : Réfléchir à ce point.

Il faut que chaque partenaire vérifie que les papiers publiés dans le cadre du projet MOSAICO soient bien sur HAL.
PA Tous : Vérifier dépôt dans HAL.

Le stagiaire Orange (Nazim) qui va travailler sur P4/NFV/SR pour le chainage de micro-services multi-technos a commencé le 20 mars.

Livrable D2.1 :

Dans ce livrable, nous décrivons et présentons les évaluations des micro-services testés de manière unitaire.
Cela inclut les papiers NOMS (CG detector et INT P4 L4S), TNSM (Analyses solution ML détection anomalies CG) et JNSM (Enrichissement impact attaques sécurité), qui sont déjà insérés. Il faut maintenant les adapter pour faire un livrable cohérent (par ex adapter l'introduction, related work, etc.).

Il est aussi décidé d'y inclure l'évaluation de la détection de sécurité L4S sur le testbed Montimage (Marius, Huu-Nghia, Joël) et la détection de CG en micro-services multi-niveaux (P4 et NFV) avec un modèle ML non supervisé (Orange/Loria). Les travaux CG/P4/NFV seront bientôt insérés. Il restera ensuite les tests L4S de sécurité.

L'objectif est de finaliser le livrable D2.1 pour fin avril.
PA Bertrand : Insérer le contenu CG/P4/NFV.
PA Marius : Insérer le contenu Sécu L4S.

Point sur solution orchestration : Hichem

Hichem rappelle sa solution de méthode exacte, efficace mais très longue : 2-3h pour une instance de petite taille.
Il présente ensuite les derniers résultats de son heuristique, modèle approchée vs la méthode exacte, mais bien plus rapide.
Hichem a fait évoluer son heuristique plusieurs fois.
Il a une approche en 2 étapes : calcul plus court chemin puis placement/chainage.
Il a fait un algo de prétraitement pour l'heuristique, identique à celui de méthode exacte, avec le calcul des x plus courts chemins et essaie de déployer sur 1, si NOK, essaie le 2ème etc.

Mais il y a le double de SFC qui ne respecte pas la latence vs la méthode exacte. Il a ensuite modifié l'heuristique pour faire l'étude du parallélisme durant le déploiement et non après.
Comme l'heuristique traite les SFC les unes après les autres (et non toutes ensemble comme la méthode exacte), l'ordre des traitements des SFC a une importance. Il a donc défini un processus adaptatif pour déterminer l'ordre de traitements des SFC en donnant un score de priorité en fonction de la possibilité de déployer en respectant la latence ou pas.
Cette 2ème version de l'heuristique est meilleure que la 1ère, mais plus longue, mais quand même bien moins longue que la solution CPLEX exacte.
Enfin, dans une 3ème version, il fait le déploiement des micro-services en parallèle (et non plus en séquentiel) : le 1er micro-service de la 1ère SFC, puis le 1er de la 2ème SFC, etc. puis le 2ème micro-service du 1er SFC, puis le 2ème du 2ème SFC, etc.
L'ordre de traitement dépend du nombre de micro-services et de la latence globale.
L'heuristique 3 est moins bonne que CPLEX, mais les SFC qui ne respectent pas la latence dépassent de très peu (1ms), alors qu'avec CPLEX, 1 seule dépasse mais de beaucoup, et certaines respectent la latence de beaucoup.
La continuité des travaux est de faire une meta-heuristique à partir de la V3 et la 1ère approche serait de limiter les SFC qui respectent de beaucoup la latence et améliorer celles qui dépassent de peu.

Hichem va mettre le code de l'heuristique V3 sur le github et voir avec Huu-Nghia pour un transfert de connaissances. Huu-Nghia pourra ensuite intégrer à l'orchestrateur pour faire le démonstrateur.
PA Hichem/Huu-Nghia : Voir pour transfert de compétences/code.

Intégration et tests sécurité L4S dans Testbed : Huu-Nghia/Marius

Huu-Nghia a intégré dans MMT le calcul du RTT sur QUIC avec le spin bit.
Il y a une limitation avec le spin bit, tous les paquets transmis durant 1 RTT ont la même valeur de RTT. Cela pourrait être gênant pour les attaques micro-burst (mais on n'est pas parti pour ce cas d'usage) mais c'est moins gênant pour les attaques ECN (on a pour objectifs de voir l'impact sur les autres flux quand il y a une attaque ECN). De plus, cette solution fonctionne moins bien avec les paquets non ordonnés, mais on n'en a pas sur le testbed car les clients et serveurs sont connectés directement au switch. Il faudrait toutefois présenter cette limitation et voir comment et quand cela pourrait se produire dans la vraie vie.

Huu-Nghia a fait des tests pour valider son implémentation du Spin bit dans MMT, mais il a eu un souci de code avec les valeurs de priority et de clone INT. Il a contourné cela en configurant différemment.

Huu-Nghia a fait des tests avec un flux LL picoquic, pour valider le code, pour calibrer le testbed et vérifier que les données récoltées soient exploitables par le modèle ML. Les premiers tests réalisés montrent des données mesurées qui ne semblent pas bonnes, et peut-être très certainement dues à l'utilisation des VMs. Huu-Nghia va voir pour utiliser 3 PCs différents et installer le P4L/L4S/INT sur 1 PC, utiliser les 2 autres pour les clients et les serveurs en utilisant des namespaces pour isoler les @ réseaux plutôt que des VMS (et tous les impacts que cela engendre) et refaire les tests de base pour la calibration.
PA Huu-Nghia : Revoir le testbed et tester.
PA Bertrand : Envoyer à Huu-Nghia ses scripts de configuration de namespace et interfaces virtuelles.

Huu-Nghia doit ensuite faire les tests de la campagne de Marius.
Marius a prévu une batterie de tests en faisant varier 3 paramètres (débit routeur, type de flux, durée) et mesure 13 métriques.
Les tests de QoS mono-flux servent à valider que ce qu'on obtient correspond à ce qu'on attendait. Les tests mutli-flux sont à faire avec 1 ou x serveurs et x clients : faire des tests avec x=5 et éventuellement x=10 si OK avec 5.
L'objectif de cette campagne de tests est de reproduire les tests JNSM, faire varier le niveau de discrétion de l'attaque ECN et évaluer la performance d'un algo de ML type USAD ou DAGMM pour détecter les attaques.
PA Marius : Finaliser la campagne de tests.

Le code picoquic est prêt, Marius va adapter les scripts JNSM et ensuite dès que le testbed Montimage sera OK, Huu-Nghia pourra lancer les tests.
PA Huu-Nghia & Marius : Faire les tests.
PA Joël : Passer les données dans son modèle ML.

Ils ont prévu de faire des tests avec un débit à capacité fixe, mais il serait intéressant de voir si cela fonctionne avec des réseaux à capacité variable et dans ce cas, est-ce que les modèles /features permettront de détecter les attaques ou pas.

Présentation de la PF CG Maison avec Scream : Philippe

Philippe présente la PF CG Maison, avec serveur, client et proxy Scream.
Une remote_session par client se fait avec 2 flux : 1 RTP Audio et 1 RTP video.
Pour la commande du jeu, la PF utiliser un virtual keyboard, virtual mouse.
La gestion de la PF se fait avec TCP (protocole SDP).
Cote client, il y a 2 sockets réseaux pour les 2 connexions (commandes et pour décrire la session en SDP) et 4 ports UDP en écoute pour les flux RTP et RTCP pour l'audio et la vidéo (ports définir dans le SDP).

Scream a été ajouté dans la PF. Scream se base sur la perte et le délai et fixe le bitrate vidéo en fonction des paquets en file d'attente, des pertes et du bit ECN.
L'intégration de Scream est utilisée seulement pour la vidéo, pas l'audio.
La PF a des infos qui sont récupérées par RTCP et fournies au codec vidéo lui permettant, si besoin, de s'adapter.
Philippe a fait des tests avec des conditions réseaux perturbées synthétiques : latence, gigue, bandwidth, comme pour le papier HiPNet.
Dans un 2eme temps, il envisage des tests avec Mahimahi et éventuellement plus tard avec L4S.
Les tests de la PF CG réalisés sans Scream avec mahimahi (trace B d'Orange) montrent que la PF ne fonctionne pas bien (qualité vidéo pas bonne). Il y a quelques pics de latence, mais pas de perte.
Pour les tests de la PF CG réalisés avec l'ajout du CCA Scream, le proxy semble avoir un bug encore en ce moment, il y a un problème côté client (image noire). Le Loria doit regarder cela.
PA Philippe/Xavier : Debugger et faire les tests.

Le Loria doit voir avec Montimage si c'est possible intégrer le noeud L4S/Mahimahi dans leur testbed pour tester la PF CG Maison avec Scream.

Détection CG en micro-services multi-niveaux (P4/NFV) : Bertrand
Bertrand présente l'architecture et les résultats de tests de la solution de détection de trafic CG à 2 niveaux (P4 et NFV) avec une solution de ML non supervisé (USAD), à comparer avec la solution toute logicielle avec un Decision Tree (papier NOMS).
La solution DT fonctionne très bien pour ce qu'elle a appris (CG ou applications non CG) mais moins bien pour les contenus non vus de PFs apprises et pas bien pour les PFs non vues. La solution non supervisée USAD n'apprend à détecter que le trafic CG (pas le non CG). Elle fonctionne très bien pour détecter le CG (appris ou non vus) et classifie aussi très bien le NonCG (même si un peu moins bien que le DT avec les applis apprises). Nous retenons donc le modèle USAD qui est performant et rapide.
Bertrand présente ensuite l'implémentation en P4 sur un switch hardware à base de Tofino du module d'extraction des features nécessaires au modèle ML et notamment les diverses limitations ou contraintes (nombre d'actions possibles limitées, nombre d'actions sur les registres limitées, nombre de fonctions maths possibles limitées, taille des digest message limitée et actions possibles uniquement sur réception de paquet pour notre cas car actions sur timer limitées). Malgré ses limitations, une implémentation P4 efficace a pu être réalisée, mais en modifiant le modèle USAD, en supprimant les features de variance qui sont impossibles à calculer tel quels avec P4. Il est discuté d'essayer d'utiliser l'algorithme de Welford pour un calcul approximé de la variance dans P4.
PA Bertrand : Voir si possible d'implémenter cet algo.

Bertrand a intégré la notion de rapports vides pour être plus représentatif des comportements des applications. Sans cette connaissance, le modèle USAD pouvait assimiler du trafic NonCG à du CG. Avec les rapports vides, il classifie très bien.
Actuellement, c'est le contrôleur qui tourne sur le switch qui émet les rapports vides, mais il est proposé de générer les rapports vides dans le NFV compute node, plutôt que dans le contrôleur pour éviter un décalage temporel de l'envoi de ces rapports vides.
PA Bertrand : Voir si possible et les impacts.

Enfin, une option discutée est d'étudier la possibilité d'émettre les rapports directement depuis le module P4 vers le NFV compute node, en utilisant INT. Cela permettrait de rejoindre une autre activité du projet et montrer une intégration encore plus forte et cohérente.
PA Bertrand : Etudier vette possibilité et voir avec Huu-Nghia si possibe d'intégrer ensuite au testbed.

Analyse des opportunités de transmission des stations de base et premières réflexions pour AQM cellulaire : Stéphane

Stéphane présente le contexte de l'étude en rappelant les besoins/objectifs/principes des AQM, en relation avec les bottlenecks.
Les AQM sont surtout conçus et utilisés actuellement pour les débits à capacité fixe. L'intérêt des AQM est un peu remis en cause de nos jours, car les nouveaux CCA ont trouvé une solution alternative avec leur propre mécanisme, puisque les AQM ne sont pas déployés dans les équipements réseaux actuels (livebox, Stations de base, etc.). Cependant, ils pourraient l'être.
Stéphane explique les causes de variation de capacité réseaux : CQI pour 1 terminal, charge de la cellule, carrier agreggation en recevant data sur plusieurs bandes de fréquence, MIMO quand on utilise plusieurs antennes ; etc.
Mais il y a actuellement peu de papiers sur les AQM pour réseaux à capacité variable (Stéphane les présente rapidement) et donc un besoin de travailler sur ce point.

Stéphane a adapté un code du papier LowerBound pour voir les lower de Bound de latency sur les traces Mahimahi Orange que nous avons capturées et calculé le temps de délai dans la file d'attente pour voir l'évolution. Il présente les courbes de 99 percentiles de délai en fonction de la taille du RTT sur les 6 traces mahimahi et les simulations montrent qu'en cas idéal, sans prévision, les résultats sont quand même corrects (sauf trace sur Highway).

Ce n'est que le début, il faut prolonger l'étude pour mieux évaluer cela, peut-être implémenter un comportement de CCA représentatif, voir les résultats avec de la prédiction, etc.

Il est discuté de la possibilité de soumettre un papier outil pour faire la communication (et peut-être l'usage plus large) de cet outil (quand il sera plus avancé) et sur le modèle de calcul de délai minimum (lower bound) pour réseaux cellulaires.

Discussion sur le testbed

Nous commençons à avoir différents modules qui pourront être intégrés dans le testbed mis en place par Montimage. Il faudra voir si nous pourrons au final avoir un démonstrateur unique qui les intègre tous (mais pas évident car beaucoup de contributions) ou plusieurs démonstrateurs sur le testbed.
Une possibilité est d'intégrer les composants de détection de CG (P4 et NFV) et de sécurité L4S. Il faut raffiner le scénario mais quelque chose peut se faire.
Il faudrait aussi implémenter l'algorithme d'orchestration d'Hichem (par Montimage) et le déployer sur le testbed. Comme nous n'aurons que peu de services et micro-services, on peut imaginer faire des tests avec des "faux" micro-services qui génèrent simplement du trafic. Montimage utilise et connait bien OpenMano. On décide donc de partir sur cette techno pour l'orchestrateur.
Il est convenu de faire une réunion spécifique dans les prochains jours et que Huu-Nghia prépare des slides du démonstrateur intégré et on en discute lors de la réunion.
PA Huu-Nghia : Faire les slides.
PA Edgardo : Organiser la réunion testbed.

Stéphane suggère la possibilité de proposer le démonstrateur MOSAICO au salon de la recherche Orange qui aura lieu en novembre/décembre (dates encore à définir). C'est une option intéressante et elle sera discuté lors de la réunion spécifique testbed. Pour l'instant, seul un titre et un court descriptif suffit.