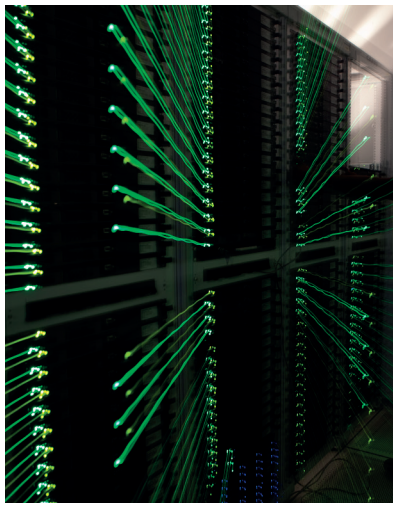
PORTFOLIO

DEPARTMENT 3

Networks, Systems and Services

mecsyco



Loria cnrs Inria UNIVERSITÉ DE LORRAINE

En partenariat avec : CentraleSupélec

Portfolio Département 3 : Réseaux, Systèmes et Services

Nous présentons dans ce portfolio les 7 éléments suivants.

D3-1 :
Rapport Bilan HCERES 2016-2020, synthèse du département et rapports des équipes

L'Université de Lorraine a demandé aux laboratoires de rédiger pour juin 2021 les bilans des laboratoires en vue de l'évaluation HCERES 2016-**2020**, ceci sans attendre les recommandations de l'HCERES. Nous avons donc rédigé un rapport complet (en anglais), structuré sur la base des anciennes évaluations de l'HCERES. Ce rapport contient une première partie qui présente une vision générale du département et de ses réalisations, suivi d'un rapport détaillé pour chacune des équipes au sein du département. Nous avons naturellement réutilisé pour le DAE (bilan 2016-**2021**) une partie substantielle de la première partie, ce qui explique la présence de parties en anglais et en français dans le DAE. Nous présentons ce rapport bilan 2016-2020 dans le document D3-1.

Nous présentons par la suite les six autres éléments (3 publications et 3 logiciels) du portfolio.

D3-2 :
Pierre-Olivier Brissaud, Jérôme François, Isabelle Chrisment, Thibault Cholez, Olivier Bettan, "Transparent and service-agnostic monitoring of encrypted web traffic", *IEEE Transactions on Network and Service Management*, 16 (3), pp 842-856, 2019. (SJR Q1)

Cet article est représentatif de nos travaux autour de la classification de trafic web chiffré.
La porte d'entrée sur Internet pour le grand public se fait le plus souvent via l'usage d'un navigateur. Ainsi, la protection des données échangées entre un serveur et un navigateur web est devenue une priorité et a conduit à la généralisation du protocole HTTPS pour garantir la sécurité de ces échanges. Cependant, la généralisation du chiffrement rend les tâches de supervision plus complexes car les outils disponibles pour du trafic en clair ne sont plus adéquats. Deux besoins antagonistes sont en effet apparus. D'un côté, il est important de respecter la vie privée des utilisateurs en assurant la confidentialité de leurs communications. D'un autre côté, les actions de détection et de surveillance face à des comportements illicites ou malveillants doivent pouvoir, pour des raisons d'ordre légal, être opérées malgré la présence du chiffrement.
Plus spécifiquement, nous avons considéré le protocole HTTP/2 récemment déployé après adoption comme standard en 2015 [1]. Nous avons défini une solution de supervision du trafic chiffré HTTP/2 qui soit à la fois passive, transparente (pas de configuration sur les terminaux utilisateurs) et respectueuse de la vie privée. En effet, notre solution n'a pas vocation à identifier le comportement complet de chaque utilisateur. Le but est de lever des alertes ou de bloquer le trafic d'un utilisateur qui ne serait pas conforme à des règles préétablies, dans le cadre d'un réseau d'entreprise par exemple. De ce fait, notre méthode permet de détecter ce type de comportement en définissant des règles a priori. A partir de ces règles, nous collectons automatiquement des données via un crawler, modélisons le trafic associé avec un nombre restreint d'attributs liés aux en-têtes TLS et apprenons alors automatiquement un modèle de classification.
Après avoir défini une approche similaire sur HTTP/1.1 [2], nous sommes, à notre connaissance, les premiers à avoir proposé et validé dans cet article une méthode permettant de déduire les actions utilisateurs sur HTTP/2 (requêtes dans un service web). Nous avons également vérifié

l'applicabilité de notre technique sur plus de 3000 services web tout en évaluant le cycle de reconstruction des signatures au cours du temps [3].

Références :

[1] R. Peon and M. Thomson, "Hypertext transfer protocol version 2 (http/2)," RFC 7540, 2015.
[2] P.-O. Brissaud, J. François, I. Chrisment, T. Cholez, and O. Bettan, "Passive monitoring of https service use," in 14th International Conference on Network and Service Management (CNSM). IEEE, 2018.
[3] P.-O. Brissaud, J. François, I. Chrisment, T. Cholez, and O. Bettan, "En- crypted http/2 traffic monitoring: Standing the test of time and space," in IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2020.

D3-3 :

Claudia-Lavinia Ignat, Quang-Vinh Dang, and Valerie L. Shalin. 2019, "The Influence of Trust Score on Cooperative Behavior", *ACM Trans. Internet Technol.* 19, 4, Article 46 (November 2019), 22 pages. (SJR Q1)

The work was done in collaboration with the Department of Psychology of Wright State University and combines game theory (trust game) with experimental design with users. The findings show that the presence of partner trust score benefits cooperative behavior and that the trust score has a similar effect relative to identity. Therefore, trust scores may complement current systems that employ identifiers to identify users. While it is possible for participants to change their ID in online systems, they cannot change the trust level other participants assigned to them. If a trust score is available, participants do not need to remember individuals by name, nor do they need to assess previous experience with imprecise mental calculations. Instead, they can make decisions based on their partner's current trust score. Our proposed solution for computing partner trust scores scales well with the number of partners. We made the dataset from the organized experiment publicly available at https://github.com/coast-team/trust_influence_analysis. The collected datasets are currently used by several research groups working on trust between humans and robots such as the group at University of Oxford and on meta-analysis about learning in repeated trust games such as the group at Berlin School of Mind and Brain, at Humboldt Universität zu Berlin.

D3-4 :

Meihui Gao, Bernardetta Addis, Mathieu Bouet, Stefano Secci, "Optimal Orchestration of Virtual Network Functions", *Computer Networks*, Elsevier, 2018, 142, pp.108-127. (CORE rang A)

In the last years, we have been focusing on the Network Function Virtualization (NFV) paradigm. VNFs are executed on commodity servers (or clouds) located in nodes distributed across the network. Demands must be routed in the network, and pass by the nodes where the requested VNFs are installed. The resulting optimization problem is the combination of a facility location problem (to decide where to install VNFs) and a routing problem (to route all the demands in such a way that they pass by all the requested VNFs). Even taken separately, these problems are NP-hard when resources have limited capacity.

In our work, extending our previous work (see [C1]), we introduced a Mixed Integer Linear Programming formulation to represent a general version of the problem, the so-called "VNF Placement and Routing" (VNF-PR) optimization problem. We introduced important constraints from the application point of view: compression/decompression of demand flows, maximal demand latency (introduced by links and VNFs), etc. To reduce the computational time needed for solving the problem, we designed a metaheuristic. We integrated a dichotomic search and a sequential resolution of different models, starting from a simplified version of the model to the

complete one. The proposed model and solution algorithm allowed us to perform a detailed analysis of the impact of network topology, allocation strategies, and latency profiles.
It is worth noticing that before our seminal work (C1) and its extension, the VNF chaining was considered a network embedding problem. Even if this kind of approach is correct for some cases, it has two main drawbacks. First, in the VNF chaining problem, the embedded graphs are linear. Thus, all the complexity proofs obtained using the network embedding model are wrong. Only using the idea of combining facility location and routing, correct results can be derived (see, for example, J1). Second, but no less important, some features cannot be introduced using the network embedding paradigm, such as the compression/decompression of flows along the virtual path or the absence of loops in the routing. Therefore, our modeling perspective allowed the optimization community to work on new formulations, solution algorithms, and extensions for the VNF placement and routing problem.

References:
[C1] B. Addis, D. Belabed, M Bouet, and S. Secci. Virtual network functions placement and routing optimization. In Proc. of IEEE CLOUDNET 2015, 2015.
[J1] B. Addis, M. Gao, and G. Carello. On the complexity of a virtual network function placement and routing problem. Electronic Notes in Discrete Mathematics, 69:197–204, 2018.

D3-5 :
Logiciel SCUBA https://scuba.gitlabpages.inria.fr/docs/ (+ création en cours de CybAI : https://www.loria.fr/fr/la-startup-cybai-presente-scuba/)

SCUBA est une suite logicielle développée au cours d'une Action de Dévelopement Technologique et d'un projet soutenu par l'AID (Agence de l'Innovation Défense). Il s'agit d'une suite d'outils permettant de prédire des potentielles attaques, en générant automatiquement des chaînes de vulnérabilités associées aux systèmes informatiques. La construction de ces chaînes se fait par l'intermédiaire de techniques de l'intelligence artificielle. Nous sommes ainsi capables de prévenir ces attaques en découvrant les possibles chemins multi-sauts qu'un attaquant peut utiliser. A la différence des solutions classiques n'évaluant la sécurité d'un équipement que de manière isolée, nous prenons ici l'ensemble de son contexte (son intégration dans un système) pour affiner notre prévision du risque.
Ces travaux font l'objet d'un brevet en cours de validation. La technologie développée a reçu un accueil très favorable de la part des industriels dans le domaine de la cyber sécurité. Cette technologie sera transférée vers une startup en cours de création impliquant les membres de RESIST A. Lahmadi, J. François et F. Beck en plus de deux autres personnes extérieures au laboratoire. (https://www.youtube.com/watch?v=tzmFGtgkJj8)

D3-6 :
Logiciel MUTE: a real-time collaborative peer-to-peer editor (https://github.com/coast-team/mute)

Existing collaborative systems generally rely on a service provider that stores and has control over user data which is a threat for privacy. MUTE is an online real-time collaborative editor that overcomes this limitation by using a peer-to-peer architecture relying on WebRTC. Several users may edit in real-time a shared document and their modifications are immediately sent to the other users without transiting through a central server. Our editor offers support for working offline while still being able to reconnect at a later time, which gives it a unique feature. Data synchronization is achieved by using the CRDT algorithm called LogootSplit developed by

Coast team. In MUTE data communication is end-to-end encrypted. LogootSplit algorithm resolves locally the conflicts and there is no need to decrypt data during data transmission as it is the case for centralized architectures where servers require un-encrypted data in order to perform merging.
MUTE has been transferred in the context of OpenPaaS-NG project (https://ng.open-paas.org/).

D3-7 :
Logiciel MECSYCO (http://www.mecsyco.com/)

La modélisation et simulation numérique est une étape maintenant incontournable dans une démarche de conception et de dimensionnement de très nombreux systèmes.
Dans beaucoup de domaines (et notamment dans les systèmes cyber physiques), modéliser un système fait intervenir plusieurs domaines (par exemple pour les smart-grids les domaines électrique, thermique, et de télécommunication) qui chacun utilise ses propres logiciels et formalismes.
Cela correspond à une problématique de **multi-modélisation et de co-simulation** : utiliser plusieurs modèles pour représenter un système cible et le simuler à partir de différents logiciels. Le verrou central est alors d'intégrer rigoureusement l'hétérogénéité des composants qu'elle soit au niveau des logiciels ou des formalismes.
MECSYCO (*Multi-agent Environment for Complex System CO-simulation*) est un intergiciel de co-simulation qui propose une approche rigoureuse d'intégration en s'appuyant sur une stratégie de wrapping DEVS (Discrete EVent system Specification). Cette approche est compatible avec la réutilisation de simulateurs existants et bénéficie des avantages de DEVS : intégration rigoureuse de formalismes hétérogènes, simulateurs abstraits, fermeture par couplage, … De plus elle fournit une vision homogène de composants hétérogènes [1].
Mecsyco est distibué sur www.mecsyco.com. Il utilise un algorithme de co-simulation entièrement décentralisé permettant des exécutions hybrides (Java/C++, Windows/linux/MacOs).
Il intègre différents simulateurs (dont la norme FMI) et propose des outils de visualisation, d'analyse et de reporting. De plus il fournit un environnement de développement intégré (au-dessus d'Eclipse, cf. Fig. 1) avec des langages dédiés pour définir modèles, multi-modèles et simulations.
Il est utilisé dans le domaine de l'énergie, notamment pour la simulation de smart-grids et micro-grids ; pour l'enseignement. Enfin il est aussi utilisé en dehors du LORIA dans le cadre de travaux universitaires (cf. [2,3,4,5]), dans le cadre d'un projet avec EDF R&D, par la société ANSYS, …

Références :
[1] Benjamin Camus, Thomas Paris, Julien Vaubourg, Yannick Presse, Christine Bourjot, Laurent Ciarletta, Vincent Chevrier, "Co-simulation of cyber-physical systems using a DEVS wrapping strategy in the MECSYCO middleware", SIMULATION, SAGE Publications, 2018, 94 (12), pp.1099-1127.
[2] Mirko D'Angelo, Annalisa Napolitano, and Mauro Caporuscio. "CyPhEF: a model-driven engineering framework for self-adaptive cyber-physical systems". In: Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings. 2018, pp. 101–104,
[3] Jalal Possik, Aicha Amrani, and Grégory Zacharewicz. "Development of a co-simulation system as a decision-aid in Lean tools implementation". In: 2018 Summer Simulation Multi-Conference. Society for Modeling and Simulation International (SCS). 2018.
[4] Benjamin Camus, Fanny Dufossé, and Anne-Cécile Orgerie. "A stochastic approach for optimizing green energy consumption in distributed clouds". In: SMARTGREENS 2017 - International Conference on Smart Cities and Green ICT Systems. Porto, Portugal, April 2017.
[5] Danial Jafarigiv, Keyhan Sheshyekani, Houshang Karimi, Jean Mahseredjian, "A Scalable FMI-Compatible Cosimulation Platform for Synchrophasor Network Studies". IEEE Transactions on industrial informatics, pp270-279, vol. 17, no. 1, january 2021.

```
multimodel autonomousHouse
submodels

    //Source
    name Source path "Library/Multimodel/WindTurbineSystem.xml"
    // name Source path "Library/Multimodel/Module_PV.xml"

    // EMS
    name EMS path "Library/Basic/EnergyManagementSystem.xml"

    // load
    // name Load path "Library/Multimodel/House.xml"
    name Load path "Library/Basic/autonomousHouse.xml"

    name Storage path "Library/Basic/Storage.xml"

interface
        /**
         * for details about the parameters: see the m2xml files of the models
         */

internal couplings
    //  {EMS."Charge_power_out" -> Load."Charge_power_in"}
        {Load."Charge_power_need" -> EMS."Charge_power" }
        {Source."Source_power" -> EMS."Source_power"}
        {EMS."Stock_power_out" -> Storage."Power"}
        {Storage."CapacityBus" -> EMS."Stock_power"}
information
    keywords
        "Modularity" "Autonomous House"
    description
        "The goal of this simulation is to be used with the switching models launcher"

simulator
    simulation variables
        stopTime:86400. refers to (Source:"stopTime") (EMS:"stopTime")(Load:"stopTime")(Storage:"stopTime")

        timeStep:120.  refers to (Source:"timeStep")  (EMS:"timeStep")(Load:"timeStep")(Storage:"timeStep")

```

Fig. 1 : Un exemple de définition de co-simulation avec le DSL.