Campagne d'avancement de grade MCF HC

Thibault CHOLEZ

Février 2025

Note : il arrive que Galaxie désactive les liens dans les PDF. La lecture de ce dossier est plus aisée avec les liens actifs, disponible si besoin ici : http://thibault.cholez.free.fr/cv/cv-hc-cholez.pdf

Sommaire

1 Curriculum Vitae **1**

2 Activité pédagogique **3**

2.1 Résumé des services d'enseignement à TELECOM Nancy . . . 3
2.2 Modules créés . . . 3
2.3 Modules enseignés . . . 4
2.4 Innovation pédagogique . . . 4
2.5 Activités d'encadrement . . . 4
2.6 Participation aux tâches collectives . . . 5
2.7 Responsabilités pédagogiques . . . 5
2.8 Développement de plateformes technologiques . . . 6

3 Activité scientifique **7**

3.1 Thématiques de recherche . . . 7
3.2 Publications et productions scientifiques . . . 8
3.2.1 Cinq publications majeures . . . 8
3.2.2 Diffusion logicielle et jeux de données . . . 10
3.3 Encadrement doctoral et scientifique . . . 11
3.4 Diffusion et rayonnement . . . 11
3.4.1 Collaborations . . . 11
3.4.2 Invitations . . . 11
3.4.3 Réalisation de démonstrations et tutoriaux . . . 12
3.4.4 Vulgarisation scientifique . . . 12
3.4.5 Comités et jurys . . . 13
3.4.6 Activités éditoriales . . . 13
3.5 Responsabilités scientifiques . . . 14
3.5.1 Responsabilité de contrats de recherche . . . 14
3.5.2 Administration locale de la science . . . 16
3.5.3 Autres responsabilités . . . 16

A Annexes **17**

A.1 Liste des publications . . . 17
A.1.1 Revues internationales . . . 17
A.1.2 Conférences internationales sélectives . . . 17
A.1.3 Démonstrations et tutoriaux sélectionnés . . . 20
A.1.4 Conférences francophones sélectives . . . 21
A.1.5 Chapitres de livre . . . 21
A.1.6 Rapports de recherche et prépublications . . . 22
A.2 Liste complète des encadrements doctoraux et scientifiques . . . 24
A.2.1 Liste des co-encadrements de thèses . . . 24
A.2.2 Liste des encadrements de stage de Master 2 . . . 27
A.2.3 Liste des encadrements de stage de Master 1 . . . 28
A.3 Services d'enseignement à TELECOM Nancy depuis 2013 . . . 29
A.4 Résumés des différentes activités de recherche . . . 30

1 Curriculum Vitae

Docteur et Ingénieur en informatique

Sujet de recherche : Supervision, sécurité et performances des réseaux informatiques

Données administratives

État civil

Thibault CHOLEZ
Né le 15 septembre 1984
Nationalité française
Marié, 2 enfants (3 ans et 6 ans)

Emploi

Maître de Conférences (CN) à l'Université de Lorraine
Section CNU : 27 Informatique
Laboratoire : LORIA (UMR 7503 : UL, CNRS, INRIA)
Composante d'enseignement : TELECOM Nancy
NUMEN : 12S1300904FKR

Coordonnées professionnelles

LORIA / INRIA Nancy-Grand Est
615 Rue du Jardin Botanique
54600 Villers-lès-Nancy, FRANCE
Bureau B136 (03 83 59 20 53)

TELECOM Nancy
193 Avenue Paul Muller
54602 Villers-lès-Nancy, FRANCE
Bureau 2.7 (03 72 74 59 47)

Courriel : thibault.cholez@loria.fr

Site web : http://thibault.cholez.free.fr

Formation et diplômes

2011 : Diplôme de Doctorat en informatique de l'Université Henri Poincaré (Nancy1), *"Supervision des réseaux pair à pair structurés appliquée à la sécurité des contenus"*, Laboratoire LORIA (UMR 7503), Nancy, France

Composition du jury :

- Président : Claude Godart, Professeur à l'ESSTIN, Université Henri Poincaré
- Rapporteurs : Matthieu Latapy (Directeur de recherche CNRS au LIP6) et Ludovic Mé (Professeur à Supélec-Rennes)
- Examinateurs : Ernst Biersack (Professeur à EURECOM) et Guillaume Doyen (Maître de conférences à l'UTT)
- Encadrants : Isabelle Chrisment (Professeur à l'ESIAL, Université Henri Poincaré) et Olivier Festor (Directeur de recherche à l'INRIA Nancy-Grand Est)

2007 : Diplôme de Master recherche en informatique de l'Université Henri Poincaré, spécialité SDRC (Services Distribués et Réseaux de Communication), Nancy, France

- Connaissances avancées en réseaux et systèmes distribués (routage, sécurité, cohérence et réplication des données, services web, etc.)
- Projet de fin d'études : Conception de mécanismes de révocation dans les réseaux pair-à-pair

2007 : Diplôme d'Ingénieur ESIAL (devenu **TELECOM Nancy**), spécialité TRS (Télécom, Réseaux et Systèmes), Nancy, France

- École publique habilitée par la Commission des Titres d'Ingénieur et spécialisée en informatique
- Projet Industriel pour Orange Labs : Conception et implantation d'une architecture sécurisée et évolutive de honeypots distribués pour la capture de malwares

Parcours professionnel

Depuis Septembre 2013 : Maître de Conférences à l'Université de Lorraine, Nancy, France

Activités d'enseignement à TELECOM Nancy, école d'ingénieur en informatique affiliée à l'Institut Mines-Télécom et au collégium Lorraine INP.

- **Service annuel d'enseignement moyen de 303 heures**, responsable de modules de tronc commun (L3, 150 élèves) et de spécialité (M2, 30 élèves) ;
- **Responsable des formations par apprentissage** : FISA généraliste et FISEA en cybersécurité ;
- **Responsable de plate-formes technologiques** ;
- **Forte implication dans les tâches collectives** (JPO, concours Mines-TELECOM, etc.) ;
- **Membre élu du conseil de l'école**.

Plus de détails sur mes activités d'enseignement en section 2.

Activités de recherche au LORIA (Laboratoire lorrain de Recherche en Informatique et ses Applications, UMR 7503) dans l'équipe RESIST (Resilience and Elasticity for SecurIty and ScalabiliTy of dynamic networked systems).

- **44 publications internationales sélectives**, liste complète en annexe A.1 ;
- **Sept co-encadrements de thèses** (cinq soutenues et deux en cours), liste complète en annexe A.2.1 ;
- **Responsable de 7 projets de recherche collaboratifs** pour le laboratoire depuis 2013 : PEPR-NF NAI (2023-2027), PEPR-Cloud (2023-2029), ANR PRESTO(2020-2024), ANR MOSAICO (2019-2023), H2020 CONCORDIA (2018-2023), ANR DOCTOR (2015-2019), CNRS PEPS NEFAE (2016-2017), représentant 1365K€ de financements externes ;
- **PEDR** obtenue pour les périodes 2017-2021 et 2021-2025 ;
- Demi-délégation au CNRS en 2022-2023 et 2023-2024.

Plus de détails sur mes activités de recherche en section 3.

Septembre 2011 - Septembre 2013 : Chercheur Post-doctorant au centre de recherche SnT (Interdisciplinary Centre for Security, Reliability and Trust) de l'Université du Luxembourg, Ville de Luxembourg, Luxembourg.
Sujet : Supervision et sécurité des réseaux (Content-Centric Networking, IPv6) dans le cadre de l'Internet des Objets. Impliqué dans deux projets de R&D européens (BUTLER et IoT6) du FP7 ; participation aux enseignements de l'Université.

Janvier 2011 - Août 2011 : Chercheur Post-doctorant à l'UTT (Université de Technologie de Troyes), équipe ERA (Environnement de Réseaux Autonomes), Troyes, France.
Sujet : Détection des nœuds malveillants pour la sécurité des systèmes distribués. Impliqué dans le projet de recherche CNRS-GIS ACDAP2P ; participation aux enseignements de l'Université.

Octobre 2007 - Décembre 2010 : Doctorant financé par l'INRIA (Institut National de Recherche en Informatique et Automatique), équipe MADYNES (Management of Dynamic Networks and Services), LORIA, Nancy, France
Sujet : Supervision des Réseaux Pair à Pair Structurés Appliquée à la Sécurité des Contenus. Impliqué dans le projet de recherche ANR MAPE.

2 Activité pédagogique

2.1 Résumé des services d'enseignement à TELECOM Nancy

Maître de conférences depuis septembre 2013, je suis rattaché à TELECOM Nancy et participe activement aux activités pédagogiques indispensables au bon fonctionnement de cette formation d'ingénieur, dont le diplôme est habilité par la CTI. J'interviens aussi bien en formation **sous statut étudiant (FISE) qu'en apprentissage (FISA)**.

Le Tableau 1 ci-dessous présente le volume d'heures d'enseignement (en équivalent TD) dispensées à TELECOM Nancy au cours des cinq dernières années. Le détail complet de mes services d'enseignement depuis 2013 est disponible en Annexe A.3.

Il est important de souligner que la composante souffre d'un déficit structurel d'enseignants permanents, entraînant une **surcharge généralisée** des services, en raison d'une augmentation continue des effectifs liée à l'attractivité de l'école, sans compensation adéquate de la part de l'Université.

Module	Rôle	Niv.	19-20	20-21	21-22	22-23	23-24
AMIO	R [1]	M2 [2]	52H [3]	46H	42H	42H	68H
ASR	R	M1	12H	12H	12H	12H	12H
BDD	I	L3	-	-	-	-	-
CSH	R	L3	-	-	-	-	-
GDP	R	L3	12H	26H	6H	6H	6H
OCI	R	M1	26H	26H	28H	-	-
PFSI	I	L3	-	-	-	-	-
POO	I	L3	24H	-	-	-	-
RSI	R	L3	46H	78H	90H	30H	26H
TOP	R	L3	-	-	-	-	-
Encadrement [4]	-	-	128H	135H	144H	108H	140H
Service	-	-	**300H**	**323H**	**322H**	**198H** [5]	**252H** [5]

TABLE 1 – Résumé des 5 derniers services d'enseignement à TELECOM Nancy (tableau complet en Annexe A.3)

2.2 Modules créés

J'ai créé le contenu pédagogique (programme, supports de cours, TD, TP) des matières suivantes :

— **AMIO** : Applications Mobiles et Internet des Objets (programmation Android, protocoles de l'IoT (802.15.4, 6lowpan, RPL, COAP), etc.) ;

— **ASR** : Administration Réseau et Système (configuration et outils réseau sous GNU-Linux, installation et sécurisation de serveurs web, mail, DNS, SSH) ;

— **GDP** : Gestion de Projets (introduction aux systèmes de contrôle de versions avec Git et à la rédaction de documents avec LaTeX) ;

1. R : Responsable du module (CMs, TDs, TPs, examen, projet) ; I : Intervenant (TDs, TPs)
2. L3 correspond au Tronc Commun (150 élèves en CM, entre 25 et 30 en TD/TP), M1 et M2 correspondent à la Spécialité (entre 25 et 30 élèves en CM/TD/TP)
3. volume horaire en équivalent TD ; les variations de volume horaire d'une année à l'autre sont essentiellement dues au nombre de groupes pris en charge
4. détail des activités d'encadrement en section 2.5
5. années de demi-délégation au CNRS : service réduit

— **OCI** : Objets Connectés Intelligents (langage C++, multitâche coopératif, programmation de capteurs sans fil (contiki OS), etc.).

2.3 Modules enseignés

— **BDD** : Bases de données (conception, modèle entité-association, modèle relationnel, algèbre relationnel, formes normales, SQL, PL/SQL, etc.) ;

— **CSH** : Langage C (syntaxe, pointeurs, structures, gestion mémoire, makefile, gdb, valgrind, etc.) et Shell (langage bash, principales commandes et gestions des droits UNIX, expressions régulières (grep, sed), etc.) ;

— **PFSI** : Principes Fondamentaux des Systèmes Informatiques (modes d'adressages, structure d'un programme en mémoire, programmation assembleur, etc.) ;

— **POO** : Programmation Orientée Objet (langage JAVA, modélisation objet, héritage, liaison dynamique, gestion des exceptions, etc.) ;

— **RSI** : Réseaux et Services Internet (modèle OSI, architectures réseau, fonctionnement des principaux protocoles (ethernet, IP, TCP, ICMP, HTTP, DNS), contrôle de congestion TCP, programmation socket C, etc.). Responsable de ce module en tronc commun (**150 élèves**) depuis 2022 ;

— **TOP** : Techniques et Outils pour Programmer (complexité algorithmique, preuves d'algorithmes, récursivité, dérécursivation, backtracking, couverture de tests, etc.).

2.4 Innovation pédagogique

— **Exploitation du Cyber-range** : Après l'acquisition d'un Cyber-range par l'école en 2020 et une période de formation, refonte complète des travaux pratiques des modules RSI et ASR en 2021-2022 afin d'exploiter pleinement cette plateforme. Cette évolution permet à chaque élève de disposer d'une topologie réseau virtuelle persistante, dont il administre les machines virtuelles.

— **Contribution au MOOC européen "Becoming a Cybersecurity Consultant"** : Dans le cadre du projet européen H2020 CONCORDIA (2020-2022), création de contenus pédagogiques (vidéos et exercices) et animation des leçons B3 "Network Attacks" et C3 "Network Protection Methods".

— **Contribution au MOOC "Supervision de Réseaux et Services"** : Dans le cadre de l'Institut Mines-Telecom, conception des contenus de la première semaine du MOOC (2017) et animation de 2017 à 2020. Responsable de la leçon "Introduction to Network Management", couvrant les concepts clés, les aires fonctionnelles, les architectures, les stratégies de supervision, les bases de gestion des informations (MIB) et le protocole SNMP.

2.5 Activités d'encadrement

Les heures d'encadrement indiquées à la fin des Tableaux 1 et 2 correspondent aux activités suivantes :

— **Suivi académique d'apprentis ingénieurs** sur les trois années (4-5 par an) : évaluation des rapports d'activités en entreprise (1 par semestre et par apprenti) et participation aux jurys (2013-aujourd'hui) ;

— **Suivi de stages de deuxième année** (6 par an) **et de troisième année** (5 par an) : réunion de mi-stage, évaluation des rapports de stage et participation aux jurys (2013-aujourd'hui) ;

— **Encadrement de projets industriels de troisième année** (1 ou 2 par an) : réunions bi-mensuelles avec le groupe (3-4 élèves) sur un semestre, conseil méthodologique et technique, participation aux jurys (2013-2022, 2024-2025) ;

— **Encadrement de projets d'initiation à la recherche** (1 ou 2 par an) : proposition d'un sujet de recherche, initiation à la recherche, réunions bi-mensuelles avec le groupe (2-3 élèves) sur un semestre, évaluation du rapport et participation aux jurys (2013-aujourd'hui) ;

— **Responsable du projet informatique de semestre 6** en apprentissage : définition du sujet, suivi des groupes (12 binômes), organisation des soutenances (2019-2022) ;

2.6 Participation aux tâches collectives

— **Rédacteur d'exercices pour le concours Mines-Télécom** (calcul binaire, complexité algorithmique, BDD, C), épreuve d'aptitude aux sciences du numérique (2016-2018) puis épreuve d'informatique (2023) ;

— **Examinateur aux oraux du concours Mines-TELECOM** (deux à trois journées d'entretiens par an) (2015-2018, 2024) ;

— **Examinateur aux oraux de recrutement de TELECOM Nancy** (une à deux journées d'entretiens par an, suivi du jury d'admission) (2014-aujourd'hui) ;

— **Membre du conseil pédagogique de la formation par apprentissage** : réunions semestrielles avec les élèves et les industriels (2013-aujourd'hui) ;

— **Membre du jury de recrutement de la formation par apprentissage** (étude d'une dizaine de dossiers par an, suivi du jury d'admissibilité) (2013-aujourd'hui) ;

— **Animation de différents stands aux journées portes ouvertes** de TELECOM Nancy : présentation du cursus, des laboratoires partenaires (LORIA, CRAN, IECN), des plateformes technologiques (cf section 2.8) (2014-2020, 2024) ;

— Président de jury de BAC (2014, 2018) et BTS (2015).

2.7 Responsabilités pédagogiques

J'exerce ou j'ai exercé les responsabilités suivantes au sein de TELECOM Nancy :

— **Responsable des formations par apprentissage, la FISA généraliste en informatique et la FISEA en cybersécurité** (75 élèves) : Promotion de la formation dans divers salons et forums d'orientation, recrutement des apprentis sur dossier, validation des avant-projets (pré-contrat), coordination avec l'Institut des Techniques d'Ingénieur de l'Industrie de Lorraine et les entreprises partenaires, affectation des tuteurs académiques, organisation des conseils pédagogiques de semestre, suivi des élèves, évolution du programme pédagogique, remise des diplômes, etc. (2024-aujourd'hui) ;

— **Responsable des projets en entreprise de la formation par apprentissage** : communication auprès des entreprises, validation des sujets, organisation des soutenances sur site et en mode mixte, environ 100 projets par an répartis sur les 3 années (2017-aujourd'hui) ;

— **Responsable de plate-formes technologiques** (**Urbanloop**, Sensor Living Lab, Sencity) (cf section 2.8) (2015-2020) ;

— **Membre élu du conseil de l'école** : une réunion par trimestre, vote des budgets et des choix stratégiques de l'école (2019-2023) ;

— Membre du groupe de travail (4 personnes) concevant la **maquette du nouveau parcours Systèmes et Logiciels Embarqués** en partenariat avec l'ENSEM : réunions bi-mensuelles, recensement des formations similaires, étude des référentiels de compétences internationaux, recueil des besoins des entreprises, élaboration du programme, sollicitation des intervenants (2021-2023) ;

— Membre du groupe de travail (4 personnes) concevant la **nouvelle maquette pédagogique de la 2ème année** (M1) de TELECOM Nancy (2024-2025).

2.8 Développement de plateformes technologiques

Développement de plateformes d'expérimentation :

— **Plate-forme Sensor Living Lab - Internet des Objets (IoT)** : Déploiement d'un réseau de 30 capteurs TelosB au sein du bâtiment de l'école, collectant des mesures environnementales et accessibles via un web service ouvert aux étudiants. En 2018, création d'un appartement intelligent intégrant 30 capteurs et actionneurs hétérogènes pilotables par la voix, permettant d'étudier les protocoles réseau, la composition de services et les enjeux de cybersécurité.

— **Plateforme Sencity - Voitures connectées et ville intelligente** : Instrumentation d'un véhicule électrique avec divers capteurs (caméras, télédétection laser, GPS, antenne Wi-Fi, port OBD, capteurs de qualité de l'air, IMU, etc.), collectant des données en temps réel via ROS pour des expérimentations à l'échelle urbaine.

Projets d'innovation en partenariat avec des acteurs académiques et industriels :

— **Projet Urbanloop** (Lorraine INP, Région Grand Est, Métropole du Grand Nancy) : Urbanloop est un projet pionnier de mobilité urbaine porté par quatre écoles (ENSG, Mines Nancy, ENSEM et TELECOM Nancy), visant à concevoir un système de transport autonome, écologique et sans correspondance, basé sur des capsules individuelles circulant sur un réseau de boucles interconnectées. En tant que co-responsable pour TELECOM Nancy, je supervise le développement de plusieurs preuves de concept : le protocole de routage dynamique des capsules, le simulateur global du réseau, le système d'information et l'application mobile. J'ai encadré dans ce cadre 4 stages de M1, 4 projets industriels et 6 projets de recherche d'élèves ingénieurs.

— **Projet AALUM - Architectures lumineuses interactives** (En partenariat avec l'École Nationale Supérieure d'Architecture de Nancy) : Conception et développement d'une application web mobile et d'une infrastructure de commande d'éclairage LED (protocole DMX) permettant un contrôle collaboratif et en temps réel de l'illumination d'un bâtiment à des fins artistiques et participatives.

— **Plateforme Info-Autonomie - Suivi de l'autonomie des personnes handicapées** (En collaboration avec l'Office d'Hygiène Sociale et l'Institut Mines-Télécom) : Conception, développement et déploiement d'une solution IoT comprenant un réseau de capteurs sans fil et une interface graphique permettant de suivre l'évolution du niveau d'autonomie de personnes handicapées résidant dans un appartement instrumenté de l'École de la Vie Autonome (EVA).

3 Activité scientifique

3.1 Thématiques de recherche

Les évolutions récentes d'Internet, tant en termes d'usages que de technologies, ont fait émerger plusieurs tendances majeures qui posent de nouveaux défis en matière de **supervision, sécurité et performance des réseaux informatiques**. Mes travaux de recherche s'inscrivent dans cette dynamique et visent à apporter des réponses à ces enjeux à travers plusieurs axes complémentaires. Un résumé détaillé de chacune de mes activités est disponible en Annexe A.4.

Supervision des communications chiffrées

Le **chiffrement des communications** a connu une croissance spectaculaire, passant de 5% du trafic web en 2012 à plus de 80% en 2018 [6]. Ce recours massif au chiffrement rend inefficaces les techniques classiques de supervision des flux (Deep Packet Inspection), privant ainsi les opérateurs et administrateurs réseaux d'une visibilité essentielle sur le trafic.

Alors que certaines solutions contournent ce problème en déchiffrant le trafic (proxy HTTPS), au détriment de la **protection de la vie privée**, mes recherches depuis 2013 se concentrent sur des approches respectueuses de la confidentialité tout en offrant un niveau d'information suffisant pour l'analyse. Nous avons notamment démontré l'inefficacité de l'inspection du champ SNI de TLS [26] et proposé une alternative plus robuste [24]. Nous avons ensuite développé des méthodes de supervision basées sur l'**apprentissage automatique** (supervisé), exploitant les caractéristiques statistiques des flux HTTPS [25] et HTTP/2 [3, 18, 19], améliorant progressivement la fiabilité et la précision de l'identification des flux chiffrés.

Information-Centric Networking et diffusion massive de contenus

L'usage d'Internet a évolué vers une **diffusion massive de contenus multimédias** (vidéo en streaming, etc.). Toutefois, les protocoles réseaux actuels, conçus à l'origine pour des échanges client-serveur, ne sont pas optimisés pour cet usage, ce qui affecte les performances. Les Content Delivery Networks (CDN) atténuent ce problème, mais au prix d'une centralisation accrue.

Les architectures **Information-Centric Networking (ICN)**, et en particulier Named-Data Networking (NDN), proposent un changement de paradigme en adressant directement les contenus, plutôt que les machines, à l'échelle d'Internet, offrant une alternative potentielle à TCP/IP. Mes travaux explorent les **obstacles opérationnels freinant leur adoption**, en analysant **leurs performances, leur sécurité, leur interopérabilité** avec HTTP et les stratégies de déploiement progressif via la **virtualisation des fonctions réseau** (NFV).

Nous avons identifié plusieurs vulnérabilités de sécurité [22, 41, 42] et de performance [23] affectant NDN et proposé des solutions pour y remédier. Nous avons également développé un mécanisme permettant de transporter efficacement du contenu web sur NDN en bénéficiant de la mise en cache [4, 21, 43]. Enfin, nous avons introduit une architecture modulaire de routeurs NDN sous forme de micro-services [20], rendant ces derniers plus flexibles et performants.

Réduction de la latence réseau pour les applications interactives

Si les réseaux d'accès modernes (fibre, 5G) offrent désormais un débit suffisant pour l'ensemble des usages, **la latence reste un défi majeur**, notamment pour les applications nécessitant une réactivité

6. Rapport 2015-0832 de l'ARCEP : www.arcep.fr/uploads/tx_gsavis/15-0832.pdf

extrême (<10 ms) et une latence stable dans le temps.

Nous avons choisi le **Cloud Gaming (CG)** comme cas d'étude des services interactifs à faible latence. Ce service en pleine expansion, porté par des acteurs comme Google, Nvidia, Amazon, Sony et Microsoft, devrait représenter une part significative du trafic Internet à l'avenir. Mes travaux visent à concevoir des fonctions réseau **garantissant une latence faible et stable** via des traitements optimisés au niveau du réseau d'accès, exploitant des technologies comme P4, L4S et WebRTC.

Nous avons tout d'abord caractérisé le trafic de quatre plateformes commerciales dans différentes conditions réseau (simulées et réelles, notamment en 4G) afin d'**évaluer leur capacité d'adaptation** [1, 15]. Ensuite, nous avons mis au point une **méthode d'identification en temps réel du trafic CG** [13], permettant une gestion optimisée des flux et l'évitement du bufferbloat. Nous avons évalué deux mécanismes d'**isolation des flux CG dans les files d'attente réseau problématiques** (Hierarchical Token Buckets et **L4S**), démontrant leur efficacité pour préserver la qualité de service [9].

Par ailleurs, nos architectures combinent de manière originale **fonctions logicielles NFV et accélération matérielle** via P4 [10, 12] ou GPGPU [14], contribuant ainsi aux avancées dans le domaine des architectures de traitement réseau.

Supervision et sécurité des réseaux pair-à-pair (P2P) et des blockchains publiques

Mes recherches historiques portent sur la **supervision et la sécurité des réseaux pair-à-pair**, qui connaissent un regain d'intérêt avec les blockchains publiques (Bitcoin, Ethereum) et les nouveaux protocoles P2P comme IPFS.

Les blockchains sont désormais des infrastructures critiques transportant des centaines de milliards d'actifs, mais reposent sur des **réseaux P2P présentant des vulnérabilités connues**. Nos travaux visent à détecter et corriger ces faiblesses en analysant la sécurité et la résilience de ces réseaux.

Nous avons mené **des campagnes de mesure sur Bitcoin** [16, 17] et **Ethereum** [2], mettant en évidence certaines anomalies suggérant des comportements malveillants. Nous avons développé un mécanisme permettant leur **détection et révocation de manière distribuée** [2]. De plus, nous avons proposé une **méthode réduisant de 60% les besoins de stockage** d'un nœud Ethereum [11].

Ces travaux s'inscrivent dans la continuité de mes recherches sur le réseau P2P KAD, où j'avais proposé des solutions entièrement distribuées et efficaces pour détecter et **contrer les attaques Sybil** [6] et **la pollution des contenus** [33].

3.2 Publications et productions scientifiques

3.2.1 Cinq publications majeures

Je suis co-auteur de **44 publications internationales sélectives** (journaux ou conférences), dont **32 publiées entre 2013 et 2024** avec les jeunes chercheurs que j'ai encadrés. La liste complète est disponible en Annexe A.1. Ci-dessous, une sélection de cinq publications représentatives de mes principales thématiques de recherche :

1. *Efficient Identification of Cloud Gaming Traffic at the Edge*, IEEE/IFIP Network Operations and Management Symposium, 2023 [13] : Le **Cloud Gaming** (CG) pourrait bientôt représenter une part significative du trafic Internet. Cependant, ce service est **très exigeant en débit et en latence** et s'accommode mal de partager des files d'attente avec des flux régis par des algorithmes de contrôle de congestion classiques (basés sur la perte de paquets). Nous avons développé une **méthode d'identification du trafic CG en temps réel**, basée sur des arbres de décision

exploitant les **caractéristiques statistiques des flux**. Cette solution, précise et directement déployable par les opérateurs, permet d'améliorer la qualité de service des flux CG. Ce travail a été réalisé en collaboration avec **Orange**.

2. *Avoiding the 1 TB Storage Wall : Leveraging Ethereum's DHT to Reduce Peer Storage Needs*, ACM International Symposium on Blockchain and Secure Critical Infrastructure, 2023 [11] : Indépendamment des débats sur les applications des blockchains, leur architecture soulève de nombreux défis, notamment en termes de **consommation de ressources**. La transition d'Ethereum vers la preuve d'enjeu en 2022 a marqué une avancée majeure, mais le **stockage des blocs** reste un enjeu critique. Nous avons proposé une approche permettant de **réduire de 60% les besoins de stockage d'un nœud**, en **distribuant le stockage des données froides** sur la DHT tout en maintenant un niveau de fiabilité équivalent. Ce travail a nécessité une analyse approfondie du code source du client Ethereum et permettrait **d'économiser des dizaines de pétaoctets à l'échelle du réseau**.

3. *Transparent and Service-Agnostic Monitoring of Encrypted Web Traffic*, IEEE Transactions on Network and Service Management, 2019 [3] : Le **chiffrement systématique des communications** est l'un des changements majeurs de paradigme en sécurité réseau. Alors que l'analyse du trafic HTTPS était déjà un défi, l'introduction de **HTTP/2** a complexifié la tâche en **multiplexant les requêtes**, rendant l'inférence des objets échangés encore plus difficile. Nous avons conçu une **méthode d'analyse non intrusive**, fondée sur l'apprentissage supervisé des caractéristiques des paquets, permettant de détecter les actions d'un utilisateur au sein d'un flux chiffré HTTP/2. Publiée dans le **journal de référence en gestion de réseaux**, cette approche a apporté des avancées significatives en supervision du trafic chiffré étant la première à considérer HTTP/2 tout en offrant un niveau de supervision inédit.

4. *μNDN : an Orchestrated Microservice Architecture for Named Data Networking*, ACM Conference on Information-Centric Networking, 2018 [20] : L'architecture **Information-Centric Networking** (ICN) constitue une alternative à TCP/IP plus adaptée aux usages actuels d'Internet, mais son déploiement se heurte en pratique à de nombreux défis. Nous avons conçu et implanté une version avancée de Named Data Networking (NDN), reposant sur **sept micro-services orchestrés**. Cette architecture modulaire offre davantage de **flexibilité** dans le design du réseau tout en améliorant **la sécurité et les performances** via des micro-services dédiés. Ces travaux, publiés dans **la conférence de référence du domaine (ACM ICN)**, constituent une avancée significative pour l'implémentation concrète de cette technologie.

5. *Detection and mitigation of localized attacks in a widely deployed P2P network*, Springer Peer-to-Peer Networking and Applications, 2012 [6] : Cette publication représente la **contribution majeure de ma thèse**. Nous avons développé une méthode entièrement distribuée et très efficace pour détecter et contrer les **attaques Sybil** dans les réseaux P2P basés sur les **tables de hachage distribuées (DHT)**. Notre approche repose sur une **analyse locale de l'espace d'adressage combinée à des tests statistiques** et a été intégrée à des **clients P2P largement répandus**, tels que KAD et gtk-gnutella, protégeant ainsi des millions d'utilisateurs à travers le monde. Ce travail a récemment été repris par des chercheurs de Stanford à NDSS 2024 [7] et demeure une référence en matière de sécurité des réseaux P2P.

7. https://arxiv.org/pdf/2307.12212.pdf

3.2.2 Diffusion logicielle et jeux de données

Attachant une grande importance à une science ouverte et reproductible, j'ai encadré le développement de prototypes logiciels et la collecte de jeux de données afin de soutenir mes travaux de recherche. Tous sont rendus publiquement accessibles, avec des prototypes fonctionnels et des jeux de données documentés.

— Module ESCAPE pour Firefox [26] : module permettant le contournement de certaines techniques de filtrage des flux HTTPS basés sur le nom de domaine ou le champ SNI de TLS (vidéo de présentation) ;

— HTTPS Identification Framework [25] (Python) : moteur d'apprentissage automatique des caractéristiques réseau des flux de services HTTPS pour une identification sans déchiffrement ;

— HTTPS firewall (Python) : prototype de pare-feu permettant d'identifier en temps réel les services véhiculés par HTTPS ;

— Ndnperf [23] (C++) : utilitaire réseau équivalent d'iperf pour le protocole NDN ; permet d'évaluer les performances de diffusion d'un contenu de bout en bout sous différentes hypothèses ;

— HTTP/NDN gateway [4] (C++) : passerelle sous forme de proxy HTTP permettant de véhiculer de manière transparente les contenus web sur un réseau NDN tout en bénéficiant d'un cache réutilisable entre différentes sessions HTTP ;

— μNDN [20] (C++) : suite de 7 microservices et d'un orchestrateur permettant de déployer un réseau NDN virtuel et de gérer automatiquement le passage à l'échelle et la sécurité ;

— Extension du crawler Bitnodes [16] (Python) : outil permettant de découvrir tous les nœuds constituant le réseau P2P de la blockchain Bitcoin, leurs propriétés, ainsi que des scripts d'analyse.

— Crawleth [2] (Python) : outil permettant de découvrir tous les nœuds constituant le réseau P2P de la blockchain Ethereum, leurs propriétés, ainsi que des scripts d'analyse ;

— Protection d'Ethereum contre les attaques Sybils [2] (Solidity et Python) : architecture composée d'un smart-contract structurant et véhiculant l'information des menaces recensées et d'un outil de révocation exécuté par chaque pair constatant l'attaque et révoquant les liens ;

— Loader Vulkan pour applications GPGPU [14] (Rust) : bibliothèque permettant de charger et d'exécuter du code SPIR-V sur GPU compatible avec l'API Vulkan ;

— Orchestration de VNF sur GPU [14] (SPIR-V) : exemple de code assembleur faisant de la classification de flux réseau sur GPU et fichiers de configuration de Kubernetes permettant son orchestration ;

— Sonde d'analyse de trafic basse latence [15] (C++) : sonde capable d'extraire des caractéristiques statistiques de flux réseau à très haut débit (30 Gb/s) ;

— Classificateur de trafic Cloud-Gaming [15] (Python) : classificateur basé sur un arbre de décision entraîné pour reconnaître les flux applicatifs de type Cloud-gaming d'après leurs caractéristiques ;

— Plateforme expérimentale de Cloud-Gaming (C++) : plateforme permettant de maîtriser la chaîne de service de CG et notamment les aspects réseau tel que l'utilisation de nouveaux algorithmes de contrôle de congestion scalables compatibles L4S.

Jeux de données publiés :

— HTTP/2 traffic Dataset [3, 18] (611Go) : traces réseau de 2000 mots-clés recherchés sur 5 sites web majeurs (12 traces par mot-clé) et 20000 mots-clés avec 1 trace. Également, traces de 500 mots-clés pendant 4 mois et traces de 20 mots-clés recherchés sur 3096 sites web ;

— Google Images HTTPS Dataset [3] (∼200Go) : traces réseau de 10.500 mots-clés recherchés sur le service Google Images (5 traces par mot-clé) et 105.000 autres mots-clés avec 1 trace chacun ;

— Cloud-Gaming traffic Dataset [15] (17Go) : traces réseau de 4 plateformes de Cloud-Gaming (Google Stadia, Nvidia GeForce Now, Microsoft xClould, Sony Playstation Now), avec et sans perturbation du trafic ainsi que d'autres applications UDP haut débit ;

— Mesures du réseau P2P Bitcoin [16] (34Go) : ensemble des noeuds Bitcoin découverts chaque heure pendant 1 mois (période : février-mars 2019) ;

— Mesures du réseau P2P Ethereum [2] (6Go) : ensemble des noeuds Ethereum découverts chaque heure pendant 1 mois (périodes : septembre 2021 et février-mars 2022). Collecte des données en continu disponibles via une API à l'adresse suivante : http://crawleth.loria.fr:5000.

3.3 Encadrement doctoral et scientifique

— **7 co-encadrements de thèses** (5 soutenues et 2 en cours) Liste complète en Annexe A.2.1.

— **8 encadrements de stages de Master 2** (6 mois). Liste complète en Annexe A.2.2.

— **17 Encadrements de stages de Master 1** (2 à 3 mois). Liste complète en Annexe A.2.3.

Encadrement de doctorants étrangers en visite :

— stage de M. Sarmad Ullah Khan de l'Université Polytechnique de Turin (2012, 4 mois) portant sur la conception d'un schéma de gestion des clés pour l'architecture CCN [31] ;

— stage de M. Juan Caubet de l'Université Polytechnique de Catalogne (2013, 3 mois) portant sur l'amélioration d'un système de gestion des clés pour les réseaux ICN.

3.4 Diffusion et rayonnement

3.4.1 Collaborations

Collaborations internationales

— Avec **University of Oulu en Finlande** sur la conception d'une architecture ouverte permettant d'inclure des traitements sur GPU dans NFV [14] ;

— Avec **Osaka Metropolitan University au Japon**, sur l'étude de la blockchain Handshake qui propose une alternative au DNS [7].

Collaborations industrielles

— Avec **Orange** sur la gestion des réseaux ICN [4, 21, 43], puis sur l'amélioration de la prise en charge du trafic à haut-débit et basse-latence dans les réseaux [1, 9, 10, 12, 13, 15] ;

— Avec **Thales** sur la conception de méthodes de supervision du trafic chiffré respectant la vie privée [3, 18, 19].

3.4.2 Invitations

J'ai été invité à présenter mes travaux de recherche dans les colloques suivants :

— présentation sur l'état de la sécurisation des réseaux P2P contre l'attaque Sybil à la Journée commune aux GDR RSD, GPL et SI sur la sécurité des piles réseau, septembre 2024, Orléans ;

— présentation des résultats du projet ANR DOCTOR au ICN technical committee conference de l'IEICE (Institute of Electronics, Information and Communication Engineers), Mai 2022, Japon (à distance) ;
— présentation de l'architecture μNDN [20] au Journées Cloud 2018 du GdR RSD, septembre 2018, Troyes ;
— présentation de l'architecture μNDN [20] au SDN DAY 2018, novembre 2018, Paris ;
— présentation intitulée "Étude de l'impact de la publicité sur la QoS du Web" au séminaire LORIA-SHS, juin 2017, Nancy ;
— présentation à la journée Blockchain Inria des applications possibles de cette technologie à la gestion de réseaux [60], décembre 2016, Paris ;
— présentation à RESSI des limites des pare-feu dans leur traitement des flux HTTPS [61], mai 2016, Toulouse ;
— présentation aux doctorants de l'ETH Zurich des vulnérabilités et défenses possibles des réseaux P2P ouverts, avril 2014, Zurich ;
— présentation à l'école d'été RESCOM du CNRS des problématiques de gestion de réseau concernant les architectures ICN [64], mai 2013, Porquerolles ;
— autres présentations antérieures dans des colloques internationaux : [58, 59, 65–67].

Ainsi que dans le cadre d'organismes de normalisation, à l'**Internet Research Task Force (IRTF)** dans les groupes de travail ICNRG [62] et NMLRG [63].

3.4.3 Réalisation de démonstrations et tutoriaux

J'ai réalisé un tutoriel et des démonstrations dans le cadre de conférences internationales, permettant ainsi de valoriser les savoir-faire techniques acquis :

— **deux démonstrations à la conférence ACM ICN** 2016, l'une portant sur l'exploitation d'une vulnérabilité, l'autre sur une passerelle permettant d'acheminer du trafic HTTP sur ICN [42, 43] ;
— **un tutoriel d'une demi-journée à la conférence AIMS** 2012 présentant l'architecture *Content-Centric Networking* et son implantation de référence (CCNx) [44].

3.4.4 Vulgarisation scientifique

Participations récentes à des actions de CSTI (culture scientifique, technique et industrielle) à destination du grand public :

— Animation d'un webinaire "Education for Cybersecurity" à destination des lycéens Européens et de leurs enseignants (2021) ;
— Animation d'un panel "Diversity & Cybersecurity" promouvant les carrières en cybersécurité à destination du public féminin (2021) ;
— Rédaction de deux articles de blog décrivant les thématiques de recherche portées par l'Université de Lorraine dans le projet Européen CONCORDIA (article 1, article 2) (2019, 2022) ;
— Organisation d'une web-conférence pour l'IHEDN (Institut des hautes études de défense nationale) présentant les éléments de cybersécurité développés dans CONCORDIA (2021) ;
— Interview vidéo pour l'UL présentant le projet Européen CONCORDIA dans le cadre de la semaine de l'Europe (2021) ;
— Interview écrite de présentation du projet CONCORDIA dans les newsletters du LORIA et de l'Université de Lorraine (2019).

3.4.5 Comités et jurys

J'ai participé aux **comités de suivi de thèse** suivants :

— M. Thomas Bagrel pour l'école doctorale IAEM de Lorraine (encadrants : Horatiu Cirstea et Arnaud Spiwack) ;

— M. Aina Toky Rasoamanana pour l'école doctorale de l'Institut Polytechnique de Paris (encadrants : Olivier Levillain et Hervé Debar) ;

— M. Renato Juacaba Neto pour l'école doctorale de Strasbourg (encadrants : Fabrice Theoleyre et Pascal Merindol).

J'ai participé aux **jurys de thèse** suivants :

— membre du jury de Fernando Kaway CARVALHO OTA pour l'Université du Luxembourg (encadrant : Radu State) en tant que **rapporteur**, février 2023 ;

— membre du jury de Renato Juacaba Neto pour l'école doctorale de Strasbourg (encadrants : Fabrice Theoleyre et Pascal Merindol) en tant qu'**examinateur**, juillet 2022.

J'ai participé aux **comités de sélection** suivants :

— COS pour un poste de PRAG en informatique à TELECOM Nancy pour la rentrée 2025 ;

— COS pour 4 postes de CR et 4 ISFP au Centre Inria de l'Université de Lorraine pour la rentrée 2024 ;

— COS pour un poste de PRAG en mathématiques à TELECOM Nancy pour la rentrée 2024 ;

— COS pour un poste de MCF pour la rentrée 2023, profil "Programmabilité des réseaux" à l'Université Toulouse 3 Paul Sabatier ;

— COS pour un poste de MCF pour la rentrée 2021, profil "Cybersécurité" à l'Université de Lorraine ;

— COS pour un poste de MCF pour la rentrée 2020, profil "Réseaux et Sécurité" à l'Université Polytechnique Hauts-de-France.

J'ai participé au **jury de tenure track** suivant :

— membre du jury de Ihsan Ullah pour University of Balochistan (Pakistan), en tant que **rapporteur**, octobre 2022.

J'ai évalué les dossiers de bourse CIFRE suivants pour l'**ANRT** :

— 2024-0098 sur la conception d'une blockchain opérable sur des réseaux maillés opportunistes ;

— 2023-1751 sur l'analyse de données DNS pour la cybersécurité ;

— 2022-1700 sur la détection de vulnérabilités dans les blockchains publiques.

3.4.6 Activités éditoriales

Journaux : Je suis **éditeur associé** au comité éditorial du Journal of Network and Systems Management de Springer Nature (Q1 scimago) (2024-aujourd'hui).

Je suis régulièrement sollicité en tant qu'expert par les journaux suivants :

— IEEE Transactions on Network and Service Management (TNSM) ;

— Elsevier Computer Networks (COMNET).

Conférences : Je suis ou j'ai été membre du **comité technique (TPC)** des conférences suivantes :

- Network Operations and Management Symposium (NOMS 2020, 2022, 2023, 2024, 2025) ;
- IEEE International Conference on Network Softwarization, (NetSoft PhD Symposium 2023, 2024) ;
- Rencontres francophones sur la conception de protocoles, l'évaluation de performance et l'expérimentation des réseaux de communication (CoRes 2023, 2024, 2025) ;
- ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI 2024) ;
- Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2020, 2021, 2022, 2023) ;
- IEEE International Workshop on Security Testing and Monitoring (STAM 2016, 2023) (ARES conference workshop) ;
- International Workshop on High-Precision, Predictable, and Low-Latency Networking (HiPNet 2021, 2022) ;
- IEEE Conference on Blockchain and Cryptocurrency (ICBC 2019, 2020, 2021) ;
- IFIP/IEEE International Symposium on Integrated Network Management (IM 2017, 2019, 2021) ;
- IEEE International Conference on Cloud Networking (CloudNet 2019, 2020) ;
- IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2017, 2018, 2019, 2020) ;
- IEEE/IFIP International Workshop on Managing and Manged by Blockchain (Man2Block 2018, 2019) ;
- ACM Conference on Information-Centric Networking (ACM ICN 2017) ;
- IEEE International Workshop on Network Science for Communication (NetSciCom 2015, IEEE INFOCOM Workshop) ;
- International Conference on Autonomous Infrastructure, Management and Security (AIMS 2015).

J'ai été sollicité ponctuellement en tant que relecteur occasionnel pour une quinzaine d'autres journaux et conférences non listés ici par manque de place.

3.5 Responsabilités scientifiques

3.5.1 Responsabilité de contrats de recherche

Depuis 2013, j'ai **porté 7 projets collaboratifs de recherche** pour l'Université de Lorraine ou le CNRS à divers niveaux (local, national, européen). Ces projets financent principalement les doctorants j'encadre ou ai encadrés, ce qui me permet d'être autonome quant au financement de mes activités de recherche.

- **Projet PEPR-NF NAI** (Réseaux du Futur : Network Architecture & Infrastructure),
  - période : juin 2023 - décembre 2027 ;
  - partenaires : Institut Mines Telecom, CNRS, Inria, EURECOM, Toulouse INP, Centrale Supélec, CEA
  - rôle : responsable local du projet, encadrement d'un doctorant sur le contrat.
- **Projets du PEPR-Cloud TRUSTINCloudS et SPIREC** (Cybersécurité des infrastructures Cloud),

  - période : septembre 2023 - septembre 2029 ;
  - partenaires : CEA LIST, Inria, CNRS, IMT, Université Aix-Marseille
  - rôle : co-responsable local du projet (50%), co-encadrement d'un doctorant et d'un post-doctorant (à recruter) sur le contrat.
- **Projet H2020 CONCORDIA** (Cyber security cOmpeteNCe fOr Research anD InnovAtion), projet européen visant la recherche, la formation, le transfert technologique et la construction d'une communauté dans le domaine de la cyber-sécurité,
  - période : janvier 2019 - mars 2023 ;
  - partenaires : Universität der Bundeswehr München (responsable du projet : Gabrijela Dreo Rodosek) et plus de 50 partenaires européens (voir la liste complète) ;
  - rôle : responsable local du projet, responsable de livrables, encadrement d'un doctorant et d'un postdoctorant recrutés sur le contrat.
- **Projet ANR MOSAICO** (Multi-layer Orchestration for Secured and low lAtency applICatiOns - Orchestration Multi-niveaux pour des applications basse-latence et sécurisées)
  - période : décembre 2019 - décembre 2023 ;
  - partenaires : Orange Labs (responsable du projet : Bertrand Matthieu), LORIA (via CNRS), Montimage, UTT ;
  - rôle : responsable local du projet, responsable de tâches et responsable de livrables, encadrement d'un doctorant, d'un postdoctorant, et de stagiaires recrutés sur le contrat.
- **Projet ANR PRESTO** (PRocessing Encrypted Streams for Traffic Oversight - Traitement des flux chiffrés pour la gestion du trafic)
  - période : janvier 2020 - juin 2024 ;
  - partenaires : ENS Paris (responsable du projet : David Pointcheval), Orange Labs, LORIA, 6Cure ;
  - rôle : responsable local du projet, responsable de tâches et responsable de livrables, encadrement, d'un postdoctorant, et de stagiaires recrutés sur le contrat.
- **Projet ANR DOCTOR** (DeplOyment and seCurisaTion of new functiOnalities in virtualized networking enviRonnements)
  - période : décembre 2014 - décembre 2018 ;
  - partenaires : Orange Labs (responsable du projet : Bertrand Matthieu), LORIA (via CNRS), Montimage, Thales, UTT ;
  - rôle : responsable local du projet, responsable de tâches et responsable de livrables, encadrement d'un doctorant et des stagiaires recrutés sur le contrat.
- **Projet CNRS PEPS NEFAE** (NExt-generation Firewall for Analysing Encrypted traffic)
  - période : 2016-2017 ;
  - partenaires : mono-partenaire (CNRS-LORIA) ;
  - rôle : porteur et responsable du projet, encadrement de l'ingénieur recruté sur le contrat.

Projets de recherche antérieurs

— Projet ANR BottleNet (Understanding and Diagnosing End-to-end Communication Bottlenecks of the Internet), contributeur, 2015-2018 ;

— Projet Européen FP7 BUTLER (uBiquitous, secUre inTernet-of-things with Location and contExawaReness), co-responsable local, 2011-2013 ;

— Projet Européen FP7 IoT6 (Universal Integration of the Internet of Things through an IPv6-based Service Oriented Architecture enabling interoperability), contributeur, 2012-2013 ;

— Projet CNRS GIS-3SGS ACDAP2P (Grouprement d'Intérêt Scientifique pour la Surveillance, la Sûreté et la Sécurité des Grands Systèmes), **porteur**, 2010-2011 ;

— Projet ANR MAPE (Measurement and Analysis of Peer-to-peer Exchanges for pedocriminality fighting and traffic profiling), contributeur, 2007-2010.

3.5.2 Administration locale de la science

Membre du comité de pilotage et responsable de l'axe scientifique (transverse à plusieurs domaines / laboratoires) Protocols for Secure Networks and Network Monitoring du projet **I-SITE DIGITRUST** de l'Université de Lorraine (8 membres, réunions bi-mensuelles) : définition des thèmes prioritaires, définition des appels, allocation des moyens, suivi des travaux, synthèse des résultats, (2018-2022).

3.5.3 Autres responsabilités

J'exerce les responsabilités suivantes au sein de mon équipe de recherche :

— Représentant nommé de l'équipe RESIST à la Commission des Utilisateurs des Moyens Informatiques (CUMI) (2016-aujourd'hui) ;

— Responsable des achats et du matériel de l'équipe RESIST (commande, réception, installation, configuration des stations de travail, serveurs, routeurs, etc.) (2015-aujourd'hui).

A Annexes

A.1 Liste des publications

La liste complète de mes publications est accessible sur DBLP et Google Scholar. L'ensemble de mes articles est également disponible en texte intégral sur HAL.

A.1.1 Revues internationales

[1] X. Marchal, P. Graff, J. R. Ky, T. Cholez, S. Tuffin, B. Mathieu, and O. Festor, "An Analysis of Cloud Gaming Platforms Behaviour Under Synthetic Network Constraints and Real Cellular Networks Conditions," *Journal of Network and Systems Management*, vol. 31, no. 2, p. 39, Jan. 2023. [Online]. Available : https://inria.hal.science/hal-04050288

[2] J.-P. Eisenbarth, T. Cholez, and O. Perrin, "Ethereum's Peer-to-Peer Network Monitoring and Sybil Attack Prevention," *Journal of Network and Systems Management*, vol. 30, no. 4, p. 65, Jul. 2022. [Online]. Available : https://hal.inria.fr/hal-03777454

[3] P.-O. Brissaud, J. François, I. Chrisment, T. Cholez, and O. Bettan, "Transparent and Service-Agnostic Monitoring of Encrypted Web Traffic," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 842–856, Sep. 2019. [Online]. Available : https://hal.inria.fr/hal-02316644

[4] G. Doyen, T. Cholez, W. Mallouli, B. Mathieu, H.-L. Mai, X. Marchal, D. Kondo, M. Aouadj, A. Ploix, E. Montes-De-Oca, and O. Festor, "An Orchestrated NDN Virtual Infrastructure transporting Web Traffic : Design, Implementation and First Experiments with Real End-Users," *IEEE Communications Magazine*, vol. 57, no. 6, Jun. 2019. [Online]. Available : https://hal.inria.fr/hal-02353861

[5] R. Fournier, T. Cholez, M. Latapy, I. Chrisment, C. Magnien, O. Festor, and I. Daniloff, "Comparing Pedophile Activity in Different P2P Systems," *Social Sciences*, vol. 3, no. 3, pp. 314–325, Jul. 2014. [Online]. Available : https://hal.inria.fr/hal-01052773

[6] T. Cholez, I. Chrisment, O. Festor, and G. Doyen, "Detection and mitigation of localized attacks in a widely deployed P2P network," *Peer-to-Peer Networking and Applications*, vol. 6, no. 2, pp. 155–174, May 2012. [Online]. Available : https://hal.inria.fr/hal-00786438

A.1.2 Conférences internationales sélectives

[7] K. Isobe, J.-P. Eisenbarth, D. Kondo, T. Cholez, and H. Tode, "A Deeper Grasp of Handshake : A Thorough Analysis of Blockchain-based DNS Records," in *BRAINS 2024 - 6th Conference on Blockchain Research & Applications for Innovative Networks and Services*, Berlin, Germany, Oct. 2024, p. 10. [Online]. Available : https://inria.hal.science/hal-04733791

[8] T. Cholez and C.-L. Ignat, "Sybil Attack Strikes Again : Denying Content Access in IPFS with a Single Computer," in *ARES 2024 : The 19th International Conference on Availability, Reliability and Security*. Vienna, Austria : ACM, Jul. 2024, pp. 1–7. [Online]. Available : https://inria.hal.science/hal-04666290

[9] P. Graff, X. Marchal, T. Cholez, B. Mathieu, S. Tuffin, and O. Festor, "Improving Cloud Gaming traffic QoS : a comparison between class-based queuing policy and L4S," in *Network Traffic Measurement and Analysis Conference (TMA 2024)*, IFIP, Ed. Dresden, Germany : IEEE, May 2024, p. 10. [Online]. Available : https://inria.hal.science/hal-04594817

[10] B. Mathieu, O. Dugeon, J. R. Ky, P. Graff, and T. Cholez, "Segment Routing for Chaining Micro-Services at Different Programmable Network Levels," in *27th Conference on Innovation in Clouds, Internet and Networks (ICIN)*. Paris, France : IEEE, Mar. 2024, pp. 171–178. [Online]. Available : https://hal.science/hal-04544951

[11] J.-P. Eisenbarth, T. Cholez, and O. Perrin, "Avoiding the 1 TB Storage Wall : Leveraging Ethereum's DHT to Reduce Peer Storage Needs," in *The 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI 2023)*. Melbourne, Australia : ACM ASIACCS Workshop, Jul. 2023, p. 10. [Online]. Available : https://inria.hal.science/hal-04163897

[12] J. R. Ky, P. Graff, B. Mathieu, and T. Cholez, "A Hybrid P4/NFV Architecture for Cloud Gaming Traffic Detection with Unsupervised ML," in *28th IEEE Symposium on Computers and Communications (ISCC 2023)*, IEEE. Gammarth, Tunisia : IEEE, Jul. 2023, pp. 733–738. [Online]. Available : https://hal.science/hal-04130096

[13] P. Graff, X. Marchal, T. Cholez, B. Mathieu, and O. Festor, "Efficient Identification of Cloud Gaming Traffic at the Edge," in *NOMS 2023 - 36th IEEE/IFIP Network Operations and Management Symposium*, Miami, United States, May 2023, p. 10. [Online]. Available : https://inria.hal.science/hal-04056607

[14] J. Haavisto, T. Cholez, and J. Riekki, "Unleashing GPUs for Network Function Virtualization : an open architecture based on Vulkan and Kubernetes," in *35th IEEE/IFIP Network Operations and Management Symposium (NOMS 2022)*. Budapest, Hungary : IEEE, Apr. 2022, pp. 1–8. [Online]. Available : https://hal.inria.fr/hal-03793322

[15] P. Graff, X. Marchal, T. Cholez, S. Tuffin, B. Mathieu, and O. Festor, "An Analysis of Cloud Gaming Platforms Behavior under Different Network Constraints," in *3rd International Workshop on High-Precision, Predictable, and Low-Latency Networking (HiPNet 2021)*, ser. Workshops of the 17th International Conference on Network and Service Management (CNSM21), IFIP-IEEE. Izmir (Virtual), Turkey : IEEE, Oct. 2021, p. 7. [Online]. Available : https://hal.inria.fr/hal-03421031

[16] J.-P. Eisenbarth, T. Cholez, and O. Perrin, "A Comprehensive Study of the Bitcoin P2P Network," in *3rd Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS 2021)*. Paris/ Virtuel, France : IEEE, Sep. 2021, p. 8. [Online]. Available : https://hal.inria.fr/hal-03380595

[17] ——, "An open measurement dataset on the Bitcoin P2P Network," in *IM 2021 - The 17th IFIP/IEEE International Symposium on Integrated Network Management*, Bordeaux / Virtual, France, May 2021, p. 5. [Online]. Available : https://hal.inria.fr/hal-03244771

[18] P.-O. Brissaud, J. François, I. Chrisment, T. Cholez, and O. Bettan, "Encrypted HTTP/2 Traffic Monitoring : Standing the Test of Time and Space," in *WIFS2020 - IEEE International Workshop on Information Forensics and Security*, ser. IEEE International Workshop on Information Forensics and Security, New-York/Virtual, United States, Dec. 2020. [Online]. Available : https://hal.archives-ouvertes.fr/hal-03032578

[19] P.-O. Brissaud, J. Francois, I. Chrisment, T. Cholez, and O. Bettan, "Passive Monitoring of HTTPS Service Use," in *CNSM'18 - 14th International Conference on Network and Service Management*, Rome, Italy, Nov. 2018, p. 7. [Online]. Available : https://hal.inria.fr/hal-01943936

[20] X. Marchal, T. Cholez, and O. Festor, "μNDN : an Orchestrated Microservice Architecture for Named Data Networking," in *ACM-ICN'18 - 5th ACM Conference on Information-*

Centric Networking, Boston, United States, Sep. 2018, p. 12. [Online]. Available : https://hal.inria.fr/hal-01906996

[21] X. Marchal, M. El Aoun, B. Mathieu, T. Cholez, G. Doyen, W. Mallouli, and O. Festor, "Leveraging NFV for the deployment of NDN : Application to HTTP traffic transport," in *NOMS 2018 - IEEE/IFIP Network Operations and Management Symposium.* Taipei, Taiwan : IEEE, Apr. 2018, p. 5. [Online]. Available : https://hal.inria.fr/hal-01906994

[22] T. Nguyen, X. Marchal, G. Doyen, T. Cholez, and R. Cogranne, "Content Poisoning in Named Data Networking : Comprehensive Characterization of real Deployment," in *15th IFIP/IEEE International Symposium on Integrated Network Management (IM2017)*, Lisbon, Portugal, May 2017, pp. 72–80. [Online]. Available : https://hal.inria.fr/hal-01652328

[23] X. Marchal, T. Cholez, and O. Festor, "Server-side performance evaluation of NDN," in *3rd ACM Conference on Information-Centric Networking (ACM-ICN'16)*, ACM SIGCOMM. Kyoto, Japan : ACM, Sep. 2016, pp. 148 – 153. [Online]. Available : https://hal.inria.fr/hal-01386777

[24] W. M. Shbair, T. Cholez, J. François, and I. Chrisment, "Improving SNI-based HTTPS Security Monitoring," in *2nd IEEE International Workshop on Security Testing and Monitoring*, ser. Workshops of the 36th IEEE International Conference on Distributed Computing Systems (ICDCS Worshops). Nara, Japan : IEEE, Jun. 2016, p. 6. [Online]. Available : https://hal.inria.fr/hal-01349710

[25] ——, "A Multi-Level Framework to Identify HTTPS Services," in *IFIP/IEEE Network Operations and Management Symposium (NOMS 2016)*, IFIP/IEEE. Istanbul, Turkey : IEEE, Apr. 2016, pp. p240–248. [Online]. Available : https://hal.inria.fr/hal-01273160

[26] W. M. Shbair, T. Cholez, A. Goichot, and I. Chrisment, "Efficiently Bypassing SNI-based HTTPS Filtering," in *IFIP/IEEE International Symposium on Integrated Network Management (IM 2015).* Ottawa, Canada : IFIP/IEEE, May 2015, pp. 990–995. [Online]. Available : https://hal.inria.fr/hal-01202712

[27] M. Bertrand, G. Doyen, W. Mallouli, T. Silverston, O. Bettan, F.-X. Aguessy, T. Cholez, A. Lahmadi, P. Truong, and E. Montes de Oca, "Monitoring and Securing New Functions Deployed in a Virtualized Networking Environment," in *1st International Workshop on Security Testing and Monitoring*, ser. Workshops of the 10th International Conference on Availability, Reliability and Security (ARES Workshops). Toulouse, France : IEEE, Aug. 2015, pp. 741 – 748. [Online]. Available : https://hal.inria.fr/hal-01238048

[28] J. P. Timpanaro, T. Cholez, I. Chrisment, and O. Festor, "Evaluation of the Anonymous I2P Network's Design Choices Against Performance and Security," in *1st International Conference on Information Systems Security and Privacy (ICISSP 2015).* Angers, France : SciTePress, Feb. 2015, pp. 46–55. [Online]. Available : https://hal.inria.fr/hal-01238453

[29] J. François, T. Cholez, and T. Engel, "CCN Traffic Optimization for IoT," in *The 4th International Conference on Network of the Future (NoF 2013)*, IFIP/IEEE. Pohang, South Korea : IEEE, Oct. 2013. [Online]. Available : https://hal.inria.fr/hal-00922728

[30] D. Goergen, T. Cholez, J. François, and T. Engel, "A Semantic Firewall for Content-Centric Networking," in *the 13th IFIP/IEEE International Symposium on Integrated Network Management (IM 2013) : Mini-Conference*, IFIP/IEEE. Ghent, Belgium : IEEE, May 2013, pp. 478–484. [Online]. Available : https://hal.archives-ouvertes.fr/hal-00829615

[31] S. U. Khan, T. Cholez, T. Engel, and L. Lavagno, "A Key Management Scheme for Content Centric Networking," in *the 13th IFIP/IEEE International Symposium on Integrated Network*

Management (IM 2013), IFIP/IEEE. Ghent, Belgium : IEEE, May 2013, pp. 828–831. [Online]. Available : https://hal.inria.fr/hal-00922486

[32] D. Goergen, T. Cholez, J. François, and T. Engel, "Security Monitoring for Content-Centric Networking," in *5th SETOP International Workshop on Autonomous and Spontaneous Security*, vol. 7731, Workshop of the 17th European Symposium on Research in Computer Security (ESORICS Workshops). Pisa, Italy : Springer-Verlag, Sep. 2012, pp. 274–286. [Online]. Available : https://hal.inria.fr/hal-00785254

[33] G. Montassier, T. Cholez, G. Doyen, R. Khatoun, I. Chrisment, and O. Festor, "Content Pollution Quantification in Large P2P networks : a Measurement Study on KAD," in *11th IEEE International Conference on Peer-to-Peer Computing (IEEE P2P'11)*. Kyoto, Japan : IEEE Communications Society, Aug. 2011, pp. 30–33. [Online]. Available : https://hal.inria.fr/inria-00619965

[34] J. P. Timpanaro, T. Cholez, I. Chrisment, and O. Festor, "When KAD meets BitTorrent - Building a Stronger P2P Network," in *Eighth International Workshop on Hot Topics in Peer-to-Peer Systems (HotP2P 2011)*. Anchorage, ALASKA, USA : IEEE International Parallel & Distributed Processing Symposium (IPDPS Workshops), May 2011. [Online]. Available : https://hal.inria.fr/inria-00595086

[35] ——, "BitTorrent's Mainline DHT Security Assessment," in *4th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2011)*. Paris, France : IEEE, Feb. 2011, iSBN : 978-1-4244-8704-2. [Online]. Available : https://hal.inria.fr/inria-00577043

[36] T. Cholez, I. Chrisment, and O. Festor, "Monitoring and Controlling Content Access in KAD," in *IEEE International Conference on Communications (IEE ICC 2010)*. Capetown, South Africa : IEEE, May 2010. [Online]. Available : https://hal.inria.fr/inria-00490347

[37] ——, "Efficient DHT attack mitigation through peers' ID distribution," in *Seventh International Workshop on Hot Topics in Peer-to-Peer Systems (HotP2P 2010)*. Atlanta, USA : IEEE International Parallel & Distributed Processing Symposium (IPDPS Workshops), Apr. 2010. [Online]. Available : https://hal.inria.fr/inria-00490509

[38] ——, "Evaluation of Sybil Attacks Protection Schemes in KAD," in *3rd International Conference on Autonomous Infrastructure, Management and Security (AIMS 2009)*, R. Sadre and A. Pras, Eds., vol. 5637, University of Twente. Enschede, Netherlands : Springer, Jun. 2009, pp. 70–82. [Online]. Available : https://hal.inria.fr/inria-00405381

[39] ——, "A Distributed and Adaptive Revocation Mechanism for P2P networks," in *Seventh International Conference on Networking (ICN 2008)*. Cancun, Mexico : IARIA, Apr. 2008, pp. pp. 290–295. [Online]. Available : https://hal.archives-ouvertes.fr/hal-00323990

[40] F. Beck, T. Cholez, O. Festor, and I. Chrisment, "Monitoring the Neighbor Discovery Protocol," in *The Second International Workshop on IPv6 Today - Technology and Deployment (IPv6TD 2007)*, ser. Workshops of the International Multi-Conference on Computing in the Global Information Technology (ICCGI Worshops). Guadeloupe/French Caribbean, Guadeloupe : IARIA, Mar. 2007. [Online]. Available : https://hal.inria.fr/inria-00153558

A.1.3 Démonstrations et tutoriaux sélectionnés

[41] H. L. Mai, M. Aouadj, G. Doyen, D. Kondo, X. Marchal, T. Cholez, E. Montes De Oca, and W. Mallouli, "Implementation of Content Poisoning Attack Detection and Reaction in Virtualized

NDN Networks," in *ICIN 2018 - 21st Conference on Innovation in Clouds, Internet and Networks*, Paris, France, Feb. 2018, p. 3. [Online]. Available : https://hal.inria.fr/hal-01907004

[42] X. Marchal, T. Cholez, and O. Festor, "PIT matching from unregistered remote Faces : a critical NDN vulnerability," 3rd ACM Conference on Information-Centric Networking (ACM-ICN'16), ACM SIGCOMM, pp. 211 – 212, Sep. 2016, poster. [Online]. Available : https://hal.inria.fr/hal-01386809

[43] X. Marchal, M. El Aoun, B. Mathieu, W. Mallouli, T. Cholez, G. Doyen, P. Truong, A. Ploix, and E. Montes De Oca, "A virtualized and monitored NDN infrastructure featuring a NDN/HTTP gateway," 3rd ACM Conference on Information-Centric Networking (ACM-ICN'16), ACM SIGCOMM, pp. 225 – 226, Sep. 2016, poster. [Online]. Available : https://hal.inria.fr/hal-01386615

[44] T. Cholez, "Introduction to Content-Centric Networking and the CCNx framework," in *6th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2012)*, Luxembourg, Luxembourg, Jun. 2012. [Online]. Available : https://hal.inria.fr/hal-00785298

A.1.4 Conférences francophones sélectives

[45] J.-P. Eisenbarth, T. Cholez, and O. Perrin, "Valorisation de la DHT d'Ethereum pour réduire les besoins de stockage des pairs," in *CoRes 2023 - 8èmes Rencontres Francophones sur la Conception de protocoles, l'évaluation de performances et l'expérimentation de Réseaux de communication*, Cargèse (Corse), France, May 2023. [Online]. Available : https://hal.science/hal-04080219

[46] T. Cholez, C. Hénard, I. Chrisment, O. Festor, G. Doyen, and R. Khatoun, "Détection de pairs suspects dans le réseau pair à pair KAD," in *6ème Conf. sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR-SSI 2011)*. La Rochelle, France : IEEE, May 2011. [Online]. Available : https://hal.inria.fr/inria-00596677

[47] T. Cholez, I. Chrisment, and O. Festor, "Une architecture de honeypots distribués pour superviser le réseau P2P KAD," in *9e Conférence Internationale sur Les NOuvelles TEchnologies de la REpartition (NOTERE 2009)*, A. Obaïd, Ed., Montréal, Canada, Jun. 2009, pp. 76–82. [Online]. Available : https://hal.inria.fr/inria-00405771

[48] ——, "Un mécanisme de révocation distribué et adaptatif pour les réseaux pair-à-pair," in *9ème journees Doctorales en Informatique et Reseaux (JDIR 2008)*, Villeneuve d'Ascq, France, Jan. 2008, p. 87, prix du meilleur papier. [Online]. Available : https://hal.archives-ouvertes.fr/hal-00323940

A.1.5 Chapitres de livre

[49] T. Combe, W. Mallouli, T. Cholez, G. Doyen, B. Mathieu, and E. Montes De Oca, "A SDN and NFV use-case : NDN implementation and security monitoring," in *Guide to Security in SDN and NFV*, ser. Computer Communications and Networks book series (CCN). Springer, Nov. 2017. [Online]. Available : https://hal.inria.fr/hal-01652639

[50] T. Cholez, G. Doyen, I. Chrisment, O. Festor, and R. Khatoun, "Faiblesses de l'identification dans les espaces numériques ouverts de partage de contenus : le cas des réseaux pair-à-pair," in *Enseignement, préservation et diffusion des identités numériques*, ser. Traité des sciences et techniques de l'information, J.-P. Pinte, Ed. Hermès - Lavoisier, May 2014. [Online]. Available : https://hal.inria.fr/hal-01052851

[51] F. Beck, T. Cholez, O. Festor, and I. Chrisment, *Supervision IPv6 - Applications Specifiques - NDPMon*. O'Reilly, 2007, online version of a french reference book on IPv6. [Online]. Available : http://livre.g6.asso.fr/index.php/Les_applications_sp%C3%A9cifiques

A.1.6 Rapports de recherche et prépublications

[52] W. M. Shbair, T. Cholez, J. François, and I. Chrisment, "A survey of HTTPS traffic and services identification approaches," *CoRR*, vol. abs/2008.08339, 2020. [Online]. Available : https://arxiv.org/abs/2008.08339

[53] ——, "Early identification of services in HTTPS traffic," *CoRR*, vol. abs/2008.08350, 2020. [Online]. Available : https://arxiv.org/abs/2008.08350

[54] T. Cholez, G. Montassier, G. Doyen, R. Khatoun, I. Chrisment, and O. Festor, "Détection et quantification de la pollution dans le réseau P2P KAD," UTT-LORIA, Research Report, Sep. 2011. [Online]. Available : https://hal.inria.fr/hal-00644174

[55] T. Cholez, J. P. Timpanaro, G. Doyen, I. Chrisment, O. Festor, and R. Khatoun, "Vulnérabilités de la DHT de BitTorrent & Identification des comportements malveillants dans KAD," UTT-LORIA, Research Report, Aug. 2011. [Online]. Available : https://hal.inria.fr/hal-00644151

[56] T. Cholez, I. Chrisment, G. Doyen, J. Dromard, F. Olivier, and R. Khatoun, "Etat de l'art : Réseaux pair à pair, supervision, sécurité et approches collaboratives," UTT-LORIA, Research Report, Oct. 2010. [Online]. Available : https://hal.inria.fr/inria-00533385

Thèse

[57] T. Cholez, "Supervision des réseaux pair à pair structurés appliquée à la sécurité des contenus," Theses, Université Henri Poincaré - Nancy I, Jun. 2011. [Online]. Available : https://tel.archives-ouvertes.fr/tel-00608907

Affiches

[58] T. Cholez, I. Chrisment, and O. Festor, "Fighting against paedophile activities in the KAD P2P network," Advances in the Analysis of Online Paedophile Activity, Laboratoire d'Informatique de Paris 6, Jun. 2009, poster. [Online]. Available : https://hal.inria.fr/inria-00405636

[59] ——, "Un mécanisme de révocation orienté services pour les réseaux P2P," RESCOM 2008, CNRS, Jun. 2008, poster. [Online]. Available : https://hal.inria.fr/inria-00338389

Autres communications (sans actes)

[60] T. Cholez, "Blockchain et gestion de reseaux," Seminaire Blockchain Inria, Paris, France, 2016.

[61] W. M. Shbair, T. Cholez, A. Goichot, and I. Chrisment, "Efficiently Bypassing SNI-based HTTPS Filtering," Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systemes d'Information (RESSI 2016), Toulouse, France, 2016.

[62] M. Bertrand, G. Doyen, W. Mallouli, T. Silverston, O. Bettan, F.-X. Aguessy, T. Cholez, A. Lahmadi, P. Truong, and E. Montes de Oca, "Challenges and directions for the security management of ICN services," Information-Centric Networking Research Group (IRTF ICNRG), Paris, France, 2016.

[63] W. M. Shbair, T. Cholez, J. François, and I. Chrisment, "HTTPS Traffic Classification," Network Machine Learning Research Group (IRTF NMLRG), Buenos Aires, Argentina, 2016.

[64] T. Cholez, "Management of Content-Centric Networking," ResCom 2013 : Les réseaux centrés sur les contenus, Évolution ou révolution de l'Internet ?, CNRS, May 2013. [Online]. Available : https://hal.inria.fr/hal-00924363

[65] T. Cholez, I. Chrisment, and O. Festor, "Efficient DHT Attack Mitigation through Peers' ID Distribution," Grande Region Security and Reliability Day (GRSRD 2011), Trier, Germany, 2011.

[66] ——, "Exploiting KAD Vulnerabilities to Build an Efficient Honeypot Architecture," 2nd EMANICS Workshop on Peer-to-Peer Management, University College London, London, United Kingdom, 2009.

[67] ——, "A Distributed and Adaptive Revocation Mechanism for P2P Networks," 1st EMANICS Workshop on Peer-to-Peer Management, ETH Zurich, Zurich, Switzerland, 2008.

A.2 Liste complète des encadrements doctoraux et scientifiques

A.2.1 Liste des co-encadrements de thèses

1. **thèse de M. Mohammadreza Ghafari** portant sur l'amélioration de la prise en charge du réseau pour les applications à faible latence et à haut débit, codirection à 50% avec Olivier Festor
   - période : décembre 2024 - décembre 2027 ;
   - financement : projet ANR PEPR-NF (Réseaux du Futur) NAI ;
2. **thèse de M. Victor De Moura Netto** portant sur l'amélioration de la sécurité et des performances de la DHT du réseau P2P IPFS, codirection à 50% avec Claudia-Lavinia Ignat
   - période : octobre 2024 - septembre 2027 ;
   - financement : projet ANR PEPR-Cloud TRUSTINCloudS ;
3. **thèse de M. Philippe Graff** portant sur l'analyse du trafic des services de type Cloud Gaming et la conception de solutions réseau améliorant leur QoS [1, 9, 10, 12, 13, 15], codirection à 50% avec Olivier Festor :
   - période : octobre 2020 - décembre 2023 ;
   - financement : projet ANR MOSAICO et demi-bourse de la région Grand-Est ;
   - aujourd'hui chercheur postdoctorant à University of Waterloo, Canada.
4. **thèse de M. Jean-Philippe Eisenbarth** portant sur l'étude de la fiabilité des réseaux P2P soutenant les blockchains publiques [2, 11, 16, 17, 45], codirection à 50% avec Olivier Perrin :
   - période : mai 2019 - décembre 2022 ;
   - financement : projet H2020 CONCORDIA ;
   - aujourd'hui chercheur postdoctorant à l'Université du Luxembourg, laboratoire SnT.
5. **thèse de M. Pierre Olivier Brissaud** portant sur la supervision du trafic web chiffré (HTTP2) afin d'inférer les actions utilisateur. Pas de co-direction officielle mais co-encadrement à 25% avec Jérôme François, Isabelle Chrisment et Olivier Bettan. Travail très régulier avec le doctorant tout au long de la thèse comme l'attestent les publications communes [3, 18, 19].
   - période : juillet 2016 - juin 2020 ;
   - financement : CIFRE THALES ;
   - aujourd'hui analyste cybersécurité à Fenplast, Canada.
6. **thèse de M. Xavier Marchal** portant sur l'utilisation de la virtualisation de fonctions réseau (NFV) pour le déploiement de l'architecture NDN [4, 20–23, 41–43], codirection à 50% avec Olivier Festor :
   - période : décembre 2015 - juin 2019 ;
   - financement : projet ANR DOCTOR et demi-bourse de la région Lorraine ;
   - aujourd'hui chercheur postdoctorant au CNRS.
7. **thèse de M. Wazen Shbair** portant sur la supervision du trafic web chiffré (HTTPS) afin d'inférer les services communiquant [24–26, 52, 53], codirection à 50% avec Isabelle Chrisment :
   - période : décembre 2013 - mai 2017 ;
   - financement : bourse Erasmus Mundus puis projet CNRS PEPS NEFAE ;
   - aujourd'hui chercheur en Blockchain à VNX, Luxembourg.

UNIVERSITÉ DE LORRAINE IAEM	RÉCAPITULATIF D'ENCADREMENT	Date d'édition : 3 février 2025

Thibault CHOLEZ

Adresse professionnelle :	
HDR :	NON
Grade :	MCF
Fonction :	Enseignant-Chercheur
Employeur :	Université de Lorraine
Établissement de rattachement :	Université de Lorraine
École doctorale :	IAEM - INFORMATIQUE - AUTOMATIQUE - ELECTRONIQUE - ELECTROTECHNIQUE - MATHEMATIQUES
Unité de recherche :	LORIA - Laboratoire Lorrain de Recherche en Informatique et ses Applications

ENCADREMENT DE THÈSES EN COURS

Coencadrement de thèse de Monsieur DE MOURA NETTO VICTOR HENRIQUE (thèse 1A 2024)
Unité de recherche : LORIA - Laboratoire Lorrain de Recherche en Informatique et ses Applications
Sujet : Amélioration de la sécurité et de la performance de la DHT d'IPFS
Ecole doctorale : IAEM - IAEM - INFORMATIQUE - AUTOMATIQUE - ELECTRONIQUE - ELECTROTECHNIQUE - MATHEMATIQUES n°77
Etablissement : Université de Lorraine

Coencadrement de thèse de Monsieur GHAFARI MOHAMMADREZA (thèse 1A 2024)
Unité de recherche : LORIA - Laboratoire Lorrain de Recherche en Informatique et ses Applications
Sujet : Amélioration de la prise en charge réseau pour les applications à faible latence et à haut débit.
Ecole doctorale : IAEM - IAEM - INFORMATIQUE - AUTOMATIQUE - ELECTRONIQUE - ELECTROTECHNIQUE - MATHEMATIQUES n°77
Etablissement : Université de Lorraine

ENCADREMENT DE THÈSES SOUTENUES

Codirection de thèse de Monsieur GRAFF PHILIPPE (Thèse soutenue 2023 - Durée de la thèse : 38 mois) encadrement : 50%
Unité de recherche : LORIA - Laboratoire Lorrain de Recherche en Informatique et ses Applications
Sujet : Caractérisation, identification dans le réseau et optimisation du transport de trafic à faible latence - le cas du Cloud-Gaming
Ecole doctorale : IAEM - IAEM - INFORMATIQUE - AUTOMATIQUE - ELECTRONIQUE - ELECTROTECHNIQUE - MATHEMATIQUES n°77
Etablissement : Université de Lorraine

Codirection de thèse de Monsieur EISENBARTH JEAN-PHILIPPE (Thèse soutenue 2022 - Durée de la thèse : 43 mois) encadrement : 50%
Unité de recherche : LORIA - Laboratoire Lorrain de Recherche en Informatique et ses Applications
Sujet : Analyse, valorisation et protection des réseaux pair-à-pair de blockchains publiques
Ecole doctorale : IAEM - IAEM - INFORMATIQUE - AUTOMATIQUE - ELECTRONIQUE - ELECTROTECHNIQUE - MATHEMATIQUES n°77
Etablissement : Université de Lorraine

Codirection de thèse de Monsieur MARCHAL Xavier (Thèse soutenue 2019 - Durée de la thèse : 43 mois) encadrement : 50%
Unité de recherche : LORIA - Laboratoire Lorrain de Recherche en Informatique et ses Applications
Sujet : Architectures et fonctions avancées pour le déploiement progressif de réseaux orientés contenus.
Ecole doctorale : IAEM - IAEM - INFORMATIQUE - AUTOMATIQUE - ELECTRONIQUE - ELECTROTECHNIQUE - MATHEMATIQUES n°77
Etablissement : Université de Lorraine

Codirection de thèse de Monsieur SHBAIR WAZEN (Thèse soutenue 2017 - Durée de la thèse : 38 mois) encadrement : 50%
Unité de recherche : LORIA - Laboratoire Lorrain de Recherche en Informatique et ses Applications
Sujet : Identification Des Services Dans Le Trafic HTTPS
Ecole doctorale : IAEM - IAEM - INFORMATIQUE - AUTOMATIQUE - ELECTRONIQUE - ELECTROTECHNIQUE - MATHEMATIQUES n°77
Etablissement : Université de Lorraine

A.2.2 Liste des encadrements de stage de Master 2

Encadrement de 8 stages de niveau **Master 2** (6 mois) :

1. stage de M. Victor De Moura Netto (2024) portant sur la conception d'attaques Sybil actives sur IPFS ;
2. stage de Mme. Bastian (2023) portant sur l'évaluation de la vulnérabilité du réseau P2P IPFS aux attaques Sybil ;
3. stage de M. Thomas Martignon (2022) portant sur la conception d'une architecture de stockage de données optimisée pour la blockchain Ethereum tirant parti de la DHT de son réseau P2P [11] ;
4. stage de M. Juuso Haavisto (2020) portant sur l'utilisation du langage SPIR-V et de l'API Vulkan pour écrire et déployer des fonctions réseau virtuelles tirant parti de GPGPU [14] ;
5. stage de M. Xavier Marchal (2015) portant sur l'évaluation des solutions de virtualisation existantes pour le déploiement de fonctions réseau virtualisées ;
6. stage de M. Cédric Enclos (2015) portant sur l'amélioration de l'élasticité et de la robustesse d'une fonction de routage NDN virtualisée ;
7. stage de M. Guillaume Montassier (2011) portant sur la détection et l'évaluation de la pollution dans un réseau P2P [33] ;
8. stage de M. Juan-Pablo Timpanaro (2009) portant sur le passage à l'échelle d'une architecture de supervision pour les réseaux P2P.

A.2.3 Liste des encadrements de stage de Master 1

À TELECOM Nancy pour développer les plateformes technologiques (cf section 2.8) :

1. stage de M. Pierre-Antoine Grosselin (2020) portant sur l'exploitation du simulateur d'**Urbanloop** appliquée au réseau de la Métropole du Grand Nancy ;
2. stage de M. Lilian Bidet (2020) portant sur la réalisation du système d'information d'Urbanloop et de l'application Android pour les utilisateurs ;
3. stages de M. Tristan Le Godais et de M. Malo Mongard (2019) portant sur la consolidation et l'extension du simulateur du réseau de transport urbain UrbanLoop ;
4. stage de M. Syméon Carle (2018) portant sur l'intégration d'une caméra 360° et l'implantation d'algorithmes de l'état de l'art pour l'aide à la conduite ;
5. stage de M. Dylan Grill (2018) portant sur l'intégration et le pilotage de capteurs hétérogènes pour créer un appartement intelligent ;
6. stage de M. Florian Dehau (2015) portant sur la conception et réalisation de composants logiciels servant au pilotage en temps réel d'un réseau de LEDs depuis un smartphone ;
7. stage de M. Xavier Wirth (2015) portant sur l'intégration de capteurs hétérogènes sur une voiture électrique et la collecte des données ;
8. stage de M. Anthony Deroche (2014) portant sur la mise en place d'un service de géolocalisation au sein d'une plateforme d'exploitation d'un réseau de capteurs sans fil.

Au LORIA dans le cadre de mes activités de recherche :

9. stage de M. Victor de Moura Netto (2023) portant sur le contournement de filtrage réseau inspectant le champ SNI de TLS via un proxy local basé sur OpenSSL ;
10. stage de M. Ambroise Sander (2021) portant sur l'automatisation d'analyses du réseau P2P Ethereum et la détection de comportements déviants ;
11. stage de M. Gabriel Frizzo (2021) portant sur le développement de fonctions réseau en P4 pour le traitement des flux basse latence ;
12. stage de M. Paul Andrey (2016) portant sur l'étude de l'impact des logiciels antipub sur la QoS des sites web d'information en ligne ;
13. stage de M. Quentin Rouy (2016) portant sur la réalisation d'une plateforme de mesure de la QoS lors du chargement des sites web ;
14. stage de M. Nicolas Schnepf (2015) portant sur l'étude de l'impact des téléchargements en streaming sur l'infrastructure de Bittorrent ;
15. stage de M. Antoine Goichot (2014) portant sur la réalisation démonstrateur permettant de contourner des règles de filtrage appliquées au protocole HTTPS par certains pare-feu [26] ;
16. stage de M. Christopher Hénard (2010) portant sur le développement d'un outil réalisant l'exploration exhaustive des nœuds d'un réseau P2P et sur l'analyse des données collectées [46].

A.3 Services d'enseignement à TELECOM Nancy depuis 2013

Module	Rôle	Niv.	13-14	14-15	15-16	16-17	17-18	18-19	19-20	20-21	21-22	22-23	23-24
AMIO [8]	R [9]	M2 [10]	-	23H [11]	44H	44H	38H	52H	52H	46H	42H	42H	68H
ASR	R	M1	-	12H	-	12H	12H	12H	12H	12H	12H	12H	12H
BDD	I	L3	54H	30H	-	-	-	-	-	-	-	-	-
CSH	R	L3	22H	41H	43H	20H	20H	-	-	-	-	-	-
GDP	R	L3	-	-	-	14H	16H	12H	12H	26H	6H	6H	6H
OCI	R	M1	10H	32H	8H	26H	36H	26H	26H	26H	28H	-	-
PFSI	I	L3	16H	-	-	-	-	-	-	-	-	-	-
POO	I	L3	34H	27H	35H	40H	28H	28H	24H	-	-	-	-
RSI	R	L3	26H	71H	22H	46H	46H	46H	46H	78H	90H	30H	26H
TOP	R	L3	54H	44H	44H	50H	-	-	-	-	-	-	-
Encadrement [12]	-	-	42H	72H	106H	92H	145H	114H	128H	135H	144H	108H	140H
Service	-	-	**258H**	**352H**	**302H**	**344H**	**341H**	**290H**	**300H**	**323H**	**322H**	**198H** [13]	**252H** [13]

TABLE 2 – Synthèse services d'enseignement à TELECOM Nancy depuis 2013

8. voir sections 2.2 et 2.3 pour la description des modules
9. R : Responsable du module (CMs, TDs, TPs, examen, projet) ; I : Intervenant (TDs, TPs)
10. L3 correspond au Tronc Commun (150 élèves en CM, entre 25 et 30 en TD/TP), M1 et M2 correspondent à la Spécialité (entre 25 et 30 élèves en CM/TD/TP)
11. volume horaire en équivalent TD ; les variations de volume horaire d'une année à l'autre sont essentiellement dues au nombre de groupes pris en charge
12. détail des activités d'encadrement en section 2.5
13. années de demi-délégation au CNRS : service réduit

A.4 Résumés des différentes activités de recherche

Supervision du trafic web chiffré (HTTPS puis HTTP/2)

— Contexte : co-encadrement de la thèse de M. Wazen Shbair (Projet CNRS PEPS NEFAE), puis celle de M. Pierre Olivier Brissaud (CIFRE THALES), puis projet ANR PRESTO (2013-2024)

— Publications : [3, 18, 19, 24–26]

Constatant l'adoption croissante d'une technique de filtrage du trafic HTTPS basée sur l'observation du **champ SNI de TLS** dans de nombreux pare-feux, nous avons évalué sa fiabilité et démontré qu'elle **présente des failles majeures**. Deux vulnérabilités, l'une exploitant la rétrocompatibilité de TLS et l'autre s'appuyant sur les certificats partagés entre domaines, permettent de contourner facilement cette détection. Pour illustrer ces faiblesses, nous avons développé Escape, un logiciel démonstratif, et montré que **92% des sites web HTTPS** peuvent être accédés malgré cette technique de filtrage [26]. Pour remédier à ces limites, nous avons proposé une méthode de détection des tentatives de contournement reposant sur un **service DNS de confiance** [24].

Par ailleurs, les approches traditionnelles de supervision des flux chiffrés souffrent d'un compromis entre précision excessive (identification des pages web) et granularité trop large (simple distinction entre protocoles comme HTTPS ou SSH). Nous avons donc conçu une méthode innovante permettant **d'identifier les services accédés via HTTPS tout en préservant la confidentialité des utilisateurs**, car elle ne repose sur aucun déchiffrement. Notre approche s'appuie sur **l'analyse des caractéristiques du trafic et un apprentissage supervisé à plusieurs niveaux**, garantissant une identification fiable et efficace [25].

Ces travaux, issus de la thèse de M. Wazen Shbair, ont marqué une avancée significative dans l'analyse du trafic chiffré en permettant, après apprentissage, une identification en temps réel des services sur HTTPS. Cependant, l'utilisation des délais réseau comme caractéristiques rendait le modèle difficilement généralisable. La thèse de M. Pierre Olivier Brissaud a approfondi ces recherches en rendant l'approche **plus robuste, applicable à HTTP/2 et capable d'identifier les actions utilisateur au-delà des seuls services accédés.**

Dans un premier temps, nous avons conçu une méthode d'identification par **reconstruction des tailles d'objets HTTP**, permettant de générer des signatures de trafic via **l'estimation par noyau (KDE)**. Lors de l'évaluation sur plus de 10 000 mots-clés de Google Images, notre solution a atteint un taux de précision supérieur à **99% dans un scénario en monde ouvert**. Toutefois, HTTP/2, avec son multiplexage, empêche l'identification directe des tailles d'objets.

Nous avons donc sélectionné des caractéristiques adaptées au trafic chiffré sous HTTP/2 et développé un modèle basé sur l'**apprentissage supervisé par forêts d'arbres décisionnels**. Évalué sur plusieurs services (Amazon, Google, Google Images, Google Maps), il atteint un **taux de détection vraie (TPR) variant entre 61% et 98% selon le service**. Ces résultats furent publiés dans le journal de référence en gestion de trafic réseau IEEE TNSM [3].

Enfin, nous avons validé la **robustesse de notre solution** à la conférence IEEE WIFS [18], en analysant son comportement **sur une période de plusieurs mois, sur 3 096 services différents** et sous diverses configurations utilisateur.

Ces travaux constituent une **percée majeure** en proposant, pour la première fois, une **solution performante d'identification du trafic HTTP/2 sans déchiffrement**, tout en permettant d'**inférer avec précision les actions des utilisateurs sur un site web**.

Optimisation du transport du trafic basse latence

— Contexte : co-encadrement de la thèse de Philippe Graff, projet ANR MOSAICO (2019-2023)

— Publications : [1, 9, 12, 13, 15]

Les services de **Cloud Gaming (CG)** génèrent un trafic à la fois **très haut débit et faible latence**, ce qui impose des contraintes exigeantes aux réseaux et complique le maintien d'une bonne **qualité de service (QoS)** en conditions dégradées.

Dans un premier temps, nous avons cherché à **caractériser le trafic CG** ainsi que les mécanismes d'adaptation des **quatre principales plateformes** [15]. À cette fin, nous avons constitué et analysé un dataset de traces réseau issues de sessions de jeu dans différentes configurations. Afin d'évaluer leur comportement en **conditions de réseau dégradées**, nous avons appliqué plusieurs **contraintes synthétiques** telles que **la perte de paquets, la diminution de débit, l'augmentation de la latence et la variation de la gigue**. Nous avons ensuite étudié la réaction des plateformes dans un environnement **réel de réseau cellulaire**, en capturant du trafic sur le réseau 4G Orange en janvier 2022.

Nos résultats montrent que les quatre plateformes adoptent des **stratégies d'adaptation distinctes** : certaines **ne réagissent pas suffisamment**, s'exposant ainsi à des latences élevées et à des pertes de paquets, tandis que d'autres **surréagissent** en dégradant excessivement leur qualité vidéo. Ces observations soulignent la nécessité de **nouvelles solutions d'optimisation** au niveau de l'application et/ou du réseau. Ces travaux ont été publiés journal JNSM [1] (Q1).

Face aux limites des **algorithmes de contrôle de congestion (CCA)** purement end-to-end, nous avons exploré l'identification du trafic CG au sein du réseau afin de lui appliquer un traitement optimisé. Pour cela, nous avons conçu un **classificateur basé sur un arbre de décision** [13], capable de reconnaître avec une **précision de 98,5%** le trafic CG. Ce modèle s'appuie sur un **apprentissage automatique des propriétés statistiques** du trafic CG, calculées à la volée.

Afin de garantir un **traitement à haut débit (10 Gb/s et plus)**, nous avons développé notre classificateur sous forme de **fonctions réseau virtuelles (VNF)**. En partenariat avec Orange Labs, nous avons également étudié **l'accélération de certaines fonctions sur un switch matériel programmable en P4** [12], démontrant ainsi la faisabilité d'un **déploiement réaliste** chez un fournisseur d'accès. Nos captures réseau et notre code source ont été mis à disposition pour garantir la reproductibilité des résultats (cf. section 3.2.2).

Enfin, nous avons étudié l'intégration du trafic CG dans une **architecture réseau à double file d'attente** afin de :

1. **Éviter** qu'il ne traverse des **buffers surdimensionnés**, sources de latence excessive.
2. **Améliorer sa cohabitation** avec des flux utilisant des CCA basés sur la perte de paquets.

Nous avons évalué l'impact de deux disciplines de file d'attente :

— **HTB (Hierarchical Token Bucket)**

— AQM DualPI2, doté d'une file **Low Latency, Low Loss, and Scalable Throughput (L4S)**

Les plateformes de Cloud Gaming actuelles n'étant pas compatibles avec ces approches, nous avons **développé notre propre plateforme expérimentale** et intégré **SCReAM**, un CCA basé sur **la perte et le délai** pour le protocole RTP, prenant en charge la n**otification explicite de congestion (ECN)**. Nous avons ensuite évalué les performances de ces solutions face à divers flux concurrents soumis à un goulot d'étranglement.

Nos résultats, publiés à TMA [9], montrent que les **deux approches permettent de préserver parfaitement la QoS du trafic CG**, ouvrant ainsi la voie à une prise en charge du réseau plus efficace pour ces services exigeants.

Sécurisation et exploitation des réseaux P2P des blockchains

— Contexte : co-encadrement de la thèse de Jean-Philippe Eisenbarth, projet H2020 CONCORDIA (2019-2022), collaboration avec Osaka Metropolitan University (2023-2024)

— Publications : [2, 7, 11, 16, 17]

Les **blockchains** reposent sur **des réseaux P2P** indispensables à leur bon fonctionnement, assurant la **dissémination des transactions et des blocs minés** auprès des participants. Alors que **Bitcoin et Ethereum**, les deux principales blockchains publiques, capitalisent aujourd'hui des milliers de milliards de dollars et attirent chaque jour de nouveaux utilisateurs, les aspects réseau restent **peu étudiés** malgré l'existence de **nombreux problèmes pouvant affecter la fiabilité des réseaux P2P publics**.

Dans un premier temps, nous nous sommes intéressés à la **supervision des réseaux P2P des blockchains Bitcoin** [16, 17] et **Ethereum** [2]. Pour chaque réseau, nous avons développé un **crawler** capable de **découvrir l'ensemble des pairs connectés** et avons mené des campagnes de mesure sur plusieurs mois. Nous avons étudié différents critères impactant la fiabilité du réseau :

— Nombre et distribution des pairs (géographiquement et au niveau du réseau IP),

— Taux d'attrition des pairs,

— Proportion de clients présentant des vulnérabilités connues,

— Motifs journaliers de connexion,

— Capacité d'inférer la topologie du réseau.

Nos analyses montrent que **Bitcoin et Ethereum présentent globalement de bonnes propriétés de résilience** sur ces aspects.

Nous avons ensuite étudié le stockage des données de la blockchain Ethereum, en partant du constat que :

1. Son réseau P2P basé sur une **Table de Hashage Distribuée (DHT) est largement sous-exploité**, aucune donnée n'y étant réellement stockée.
2. **La croissance continue des données** de la blockchain pose un problème à terme.

Nous avons ainsi analysé le fonctionnement du principal client Ethereum (Geth) et sa méthode de synchronisation de l'état de la blockchain entre les pairs. Sur cette base, nous avons conçu **une nouvelle architecture distribuée de stockage** exploitant la DHT, tout en **restant rétrocompatible avec les clients actuels**. Cette approche permet de **réduire l'espace disque utilisé de 60%** sans compromis sur les garanties ni sur les performances d'Ethereum [11].

L'utilisation de la DHT comme solution de stockage la rend toutefois plus susceptible de subir des **attaques Sybil localisées**. Nous avons donc analysé les pairs d'Ethereum pour identifier d'éventuelles attaques et avons mis en évidence **des milliers de nœuds suspects** présentant des comportements anormaux, notamment des **concentrations de plusieurs milliers d'identifiants sous une même adresse IP** (jusqu'à 10 000/IP).

Pour contrer ces attaques, nous avons conçu et implanté une **architecture de protection distribuée** reposant sur trois éléments :

1. Un **crawler** détectant les nœuds suspects en temps réel.
2. Un **smart contract** structurant et diffusant l'information aux pairs.
3. Un mécanisme de **révocation entièrement distribué**, où chaque pair identifie localement les attaques et coupe ses connexions aux nœuds Sybil.

Nos expérimentations sur le **réseau de test Ethereum** ont démontré l'efficacité de cette approche. Ces résultats ont été publiés dans le Journal of Network and Systems Management [2].

Enfin, nous avons évalué la fiabilité de la **blockchain Handshake**, dédiée au **stockage des enregistrements DNS** [7]. Nos analyses ont mis en évidence deux faiblesses majeures :

— Une **forte exposition au squatting** de domaines,

— Une très **faible redondance des serveurs DNS faisant autorité**, menaçant la résilience du système.

Nouvelles fonctionnalités pour la virtualisation de fonctions réseau (NFV)

— Contexte : co-encadrement de la thèse de Master de Juuso Haavisto, collaboration avec University of Oulu, Finlande (2020-2022) et Orange (2022-2023)

— Publication : [10, 14]

L'exploitation du **traitement sur GPU** (GPGPU) constitue une approche prometteuse pour **accélérer les fonctions réseau à forte intensité de calcul**, notamment la classification en temps réel de trafic grâce à l'apprentissage automatique. Bien que des travaux récents aient optimisé l'usage des unités graphiques intégrées pour réduire la latence induite par l'utilisation du GPU, ces approches présentent deux limites majeures :

1. Elles génèrent souvent des **binaires spécifiques à l'architecture matérielle**, limitant leur portabilité.
2. Elles manquent de **solutions d'orchestration** pour une gestion efficace à l'échelle du réseau.

Notre objectif est de proposer une architecture GPGPU standardisée et portable, permettant la création de **fonctions réseau interopérables et orchestrables**. Pour ce faire, nous avons conçu une **solution basée sur l'API multiplateforme Vulkan**, dans laquelle nous exécutons du **code assembleur SPIR-V** [14] en tant que fonction réseau [14].

Nous avons testé notre architecture à travers un exemple de classification de trafic par forêt aléatoire et démontré qu'elle :

— **Facilite l'orchestration** des fonctions sur plusieurs nœuds via **Kubernetes**.

— **Assure une compatibilité matérielle étendue**, en permettant l'exécution d'un code SPIR-V sur divers types de GPU (cartes graphiques discrètes et intégrées, architectures x86 et ARM).

— **Offre des performances systématiquement supérieures** à une exécution sur CPU.

En complément, nous avons cherché à **étendre NFV** en combinant **des fonctions réseau virtuelles (VNF)** avec des **fonctions accélérées matériellement en P4**. Nous avons ainsi conçu une solution exploitant **le Segment Routing (SR)** pour chaîner dynamiquement des micro-services **exécutés à différents niveaux** (conteneurs logiciels et équipements P4) [10].

Le protocole SR, bien que couramment intégré aux équipements réseau, est absent des infrastructures NFV traditionnelles. Pour combler cette lacune, nous avons développé un **proxy intermédiaire entre les nœuds P4 et les VNF**, chargé de gérer les labels SR et leur association avec les fonctions réseau.

14. Standard, Portable Intermediate Representation

Sécurisation et aide au déploiement de l'architecture Named-Data Networking

— Contexte : thèse de M. Xavier Marchal, projet ANR DOCTOR (2015-2018)

— Publications : [4, 20–23, 27, 41–43]

— Les architectures réseau ICN sont prometteuses pour l'avenir d'Internet, mais leur déploiement à grande échelle rencontre des obstacles technologiques et économiques. Dans le cadre du projet ANR DOCTOR, nous avons développé une infrastructure virtualisée permettant **un déploiement progressif du protocole NDN** [27], en prenant en compte des critères essentiels de **sécurité, de performances, de gestion du réseau et d'interopérabilité** avec les protocoles actuels.

  Nous avons identifié une **vulnérabilité critique dans les spécifications** du protocole, permettant des attaques DoS efficaces [42], et proposé des corrections. Par ailleurs, en collaboration avec des chercheurs de l'UTT, nous avons caractérisé pour la première fois l'**attaque par empoisonnement de contenus** [22] selon divers scénarios de mise en œuvre. Cette étude a démontré la gravité de l'attaque et proposé une solution correctrice.

  Pour analyser les performances du protocole, nous avons conçu **Ndnperf**, un outil de mesure similaire à Iperf [23]. Nos expérimentations ont permis d'**identifier les facteurs limitant le débit** des services en temps réel (live streaming, VoIP, etc.), des résultats présentés à la conférence de référence du domaine ACM ICN.

  Nous avons conçu une **architecture à base de microservices virtualisés et orchestrés** selon le paradigme NFV (Network Function Virtualization). Cette architecture comprend **sept microservices**, chacun reprenant une fonction atomique du routeur NDN ou introduisant un nouveau service spécifique qui peuvent être chaînées pour constituer un réseau optimisé. Un orchestrateur permet une **mise à l'échelle dynamique** des composants les plus sollicités et une adaptation automatique en cas d'attaque. Cette contribution fut également publiée à ACM ICN [20].

  Nous avons conçu **deux passerelles HTTP/NDN**, assurant la conversion transparente entre les deux protocoles tout en respectant leurs spécifications. Notre solution permet de tirer parti de la **mise en cache des contenus web dans le réseau NDN** entre différents utilisateurs grâce à un hachage intelligent des en-têtes HTTP. Ces travaux ont été publiés dans le journal IEEE COMMAG [4].

  Nos contributions répondent à quatre verrous majeurs freinant l'adoption des réseaux ICN :

  1. **Interopérabilité** avec le Web et ses contenus.
  2. **Sécurité** avec des solutions contre les attaques DoS et l'empoisonnement de contenus.
  3. **Virtualisation** permettant un déploiement progressif et réduit les coûts d'investissement.
  4. **Performances** grâce à un nouvel outil de mesure et au scaling horizontal automatique.

Supervision et sécurité de l'architecture Content-Centric Networking

— Contexte : Postdoctorat (2011-2013), Centre SnT, Université du Luxembourg

— Projets EU FP7 BUTLER et IoT6, Collaboration avec l'Université Polytechnique de Turin

— Publications : [29–32]

— Comme toutes les architectures de type Information-Centric Networking, CCN soulève **de nouveaux défis en matière de gestion et de sécurité**. Pour répondre à ces enjeux, nous avons

proposé une **approche de supervision** [32], intégrant un mécanisme de détection proactive des dysfonctionnements potentiels. En parallèle, nous avons conçu un **pare-feu spécifique** permettant l'application de règles de sécurité adaptées à l'architecture CCN [30], ainsi qu'un **schéma optimisé de gestion des clés**, offrant une meilleure scalabilité et sécurité [31]. CCN doit également être en mesure d'acheminer efficacement le **trafic issu des capteurs et objets connectés** en périphérie du réseau. Pour cela, nous avons développé une amélioration architecturale [29] permettant une gestion plus efficace de ce type de trafic grâce à l'émission pro-active et optimisée de données.

Détection et quantification des attaques dans les réseaux P2P

— Contexte : Postdoctorat (2011), équipe ERA, UTT, Troyes, France

— Projet CNRS-GIS ACDAP2P

— Publications : [6, 8, 33–35]

— Afin de **détecter des nœuds malveillants** pouvant affecter la sécurité des systèmes distribués, nous avons conçu un **explorateur** permettant de découvrir l'ensemble des pairs du **réseau KAD**, ainsi qu'un algorithme capable de **quantifier les attaques Sybil** en cours sur une DHT [6].

  Nous avons également développé une **métrique innovante** basée sur l'analyse des dissimilarités entre les noms de fichiers associés à un même contenu, permettant ainsi de **détecter une nouvelle forme de pollution** particulièrement néfaste sur les réseaux P2P. Grâce à des campagnes de mesures à grande échelle, nous avons pu estimer que cette pollution affectait près de **2/3 des fichiers populaires du réseau KAD** [33].

  Par la suite, nous avons appliqué l'ensemble de ces mécanismes de sécurisation au **réseau P2P BitTorrent**, renforçant ainsi sa résilience face aux menaces similaires [34, 35].

  Plus récemment, nous nous sommes intéressés au **réseau P2P IPFS**, souvent utilisé pour stocker et distribuer les données des contrats intelligents. Nous avons mis en évidence qu'IPFS n'intègre **aucun des mécanismes de protection** contre les attaques Sybil proposés pour la DHT Kademlia. Nos expérimentations ont démontré qu'un unique ordinateur pouvait, à lui seul, **prendre le contrôle total d'un contenu partagé**, rendant le réseau particulièrement vulnérable [8].

Supervision et protection des réseaux P2P

— Contexte : Doctorat (2007-2010), équipe MADYNES, LORIA, Nancy, France

— Projet ANR MAPE, Collaboration avec le Laboratoire d'Informatique de Paris 6

— Publications : [5, 36–38]

  Les réseaux pair-à-pair constituent des infrastructures d'information majeures, rassemblant des dizaines de millions d'utilisateurs et représentant l'un des principaux usages d'Internet dans les années 2000. Cependant, ils souffrent de plusieurs **vulnérabilités affectant la sécurité des contenus stockés**.

  D'une part, l'indexation par **tables de hachage distribuées (DHT)** expose ces réseaux à des **attaques Sybil**, consistant en l'insertion massive de nœuds malveillants capables de mener diverses actions nuisibles, telles que la pollution des contenus, la suppression de données ou encore le déni de service. D'autre part, ces réseaux sont fréquemment exploités pour diffuser des contenus illégaux ou indésirables, notamment des fichiers à caractère pédopornographique ou des logiciels malveillants.

Dans nos travaux, nous avons cherché à développer et appliquer des méthodes de supervision permettant d'analyser et de contrer ces menaces, avec un focus particulier sur la détection et la prévention de la diffusion de contenus malveillants.

Dans un premier temps, nous avons analysé les mécanismes de défense contre l'attaque Sybil implantés dans KAD et montré que ceux-ci **protègent efficacement la table de routage d'un pair mais n'empêchent pas des attaques ciblées** sur la DHT [38].

Nous avons exploité cette faiblesse pour proposer une **nouvelle méthode de supervision des contenus**, capable d'observer l'ensemble des requêtes émises par un pair pour un fichier donné, afin d'identifier précisément les accès [36]. Cette approche a notamment été appliquée à la **quantification des contenus pédophiles**, permettant d'évaluer l'ampleur du problème à grande échelle [5].

Dans un second temps, nous avons travaillé à **renforcer la sécurité des données indexées dans une DHT** en concevant un algorithme de détection des attaques Sybil ciblées. Cet algorithme repose sur des **tests statistiques** analysant la distribution des identifiants des pairs situés à proximité d'un contenu donné [37].

Ces mécanismes de défense, accompagnés de contre-mesures adaptées, ont été **implémentés et évalués dans plusieurs réseaux P2P**, notamment KAD, BitTorrent et Gnutella. À ce jour, ils constituent encore la seule solution efficace et directement applicable pour contrer ces attaques.