

Candidature au recrutement sur l'emploi de Professeur des Universités n°4225

Université Polytechnique Hauts-de-France (UPHF)

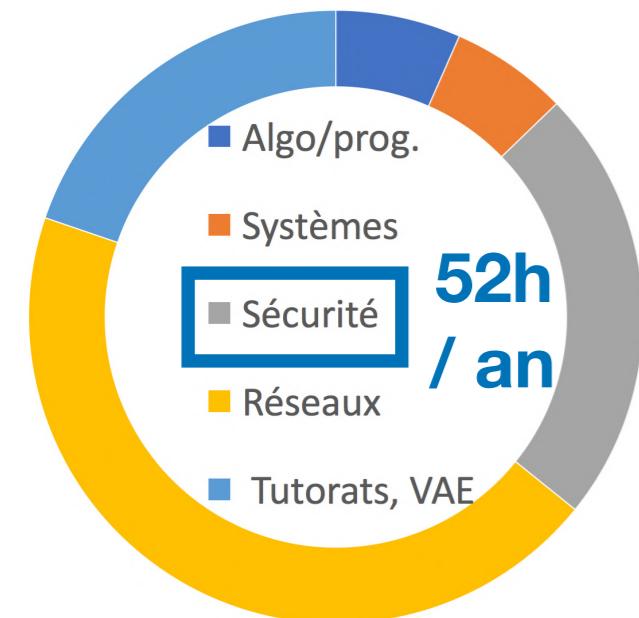
Antoine GALLAIS, qualifié aux fonctions de Professeur des Universités, CNU 27 (n°18127184517)

Présentation en ligne : <http://antoine-gallais.github.io/2019-pu-uphf-audition-gallais.pdf>

Coordonnées :	Web	http://antoine-gallais.github.io
	Mails	gallais@unistra.fr / antoine.gallais@inria.fr

Enseignant-chercheur

Resp. pédag. 11 UE
(CM, TD, TP)



~265h/an
(eq. TD, 2009-17)

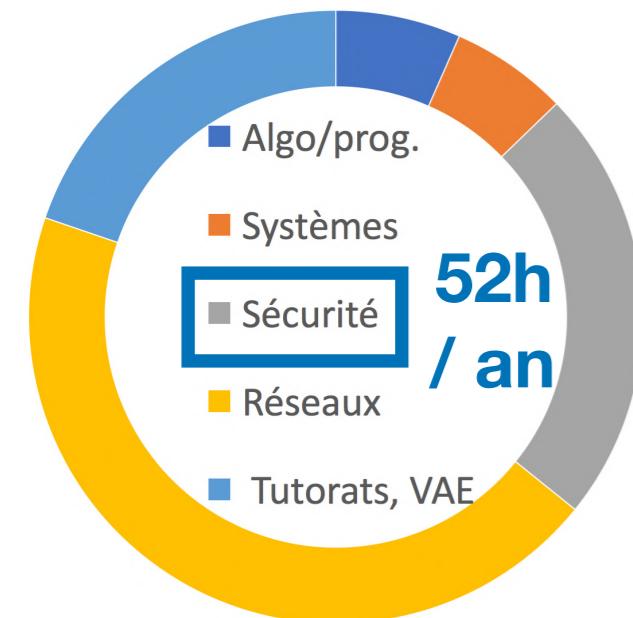
- Formation initiale (classique et alternance)
- Enseignements à distance (EAD, ~100h)
- Validation des acquis de l'expérience (LP et M)

- Concepts de base (**CIA**) et aspects juridiques (**CNIL**)
- Cryptographie** (sym., asym., signatures)
- Certificats, PGP, X.509, **TLS**
- Attaques/protections (virus, vers, DoS, DDoS)
- Sécurité de l'Internet (**DNS, BGP**)
- IPsec**, Radius, Kerberos, EAP, VPN, IDS, AAA
- Sécurité des **systèmes embarqués** (e.g., RFID)
- Outils (e.g., **openssl**, iptables, **openvpn**, snort, **nmap**, nessus)

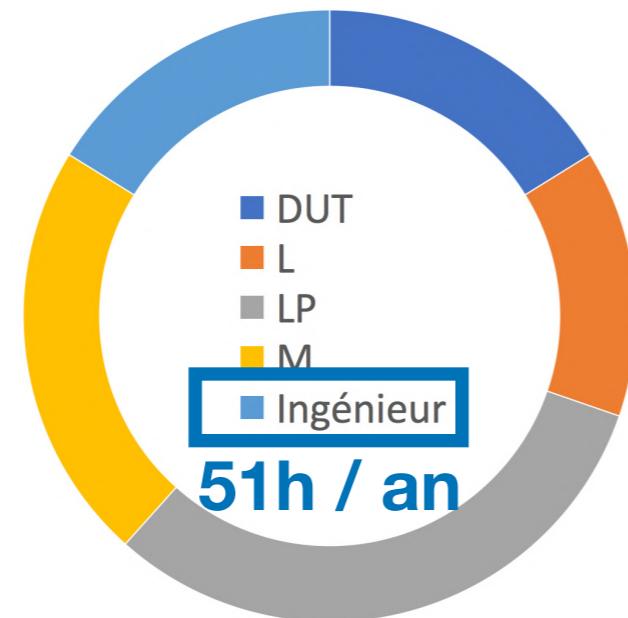


Enseignant-chercheur

**Resp. pédag. 11 UE
(CM, TD, TP)**



**~265h/an
(eq. TD, 2009-17)**



- Formation initiale (classique et alternance)
- Enseignements à distance (EAD, ~100h)
- Validation des acquis de l'expérience (LP et M)

- Telecom Physique Strasbourg
- ESIROI (Réunion)
- ENSIIE (mutualisations Master info.)



**Resp. pédag.
2 filières**

7 campagnes d'évaluation et d'accréditation

**Master informatique, 2^{ème} année,
spécialité Réseaux Informatiques
et Systèmes Embarqués
(RISE)**

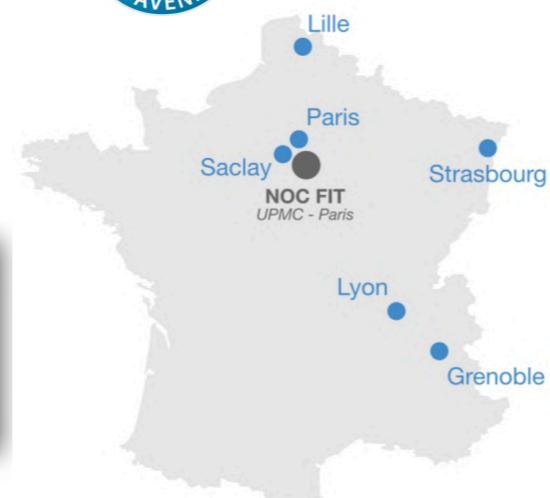
**Licence
Professionnelle SIL,
spécialité
"Administration de
Réseaux et Services"**

"administration et
sécurité des
systèmes et des
réseaux"

Enseignant-chercheur



Résidence séniors,
Brumath, Alsace



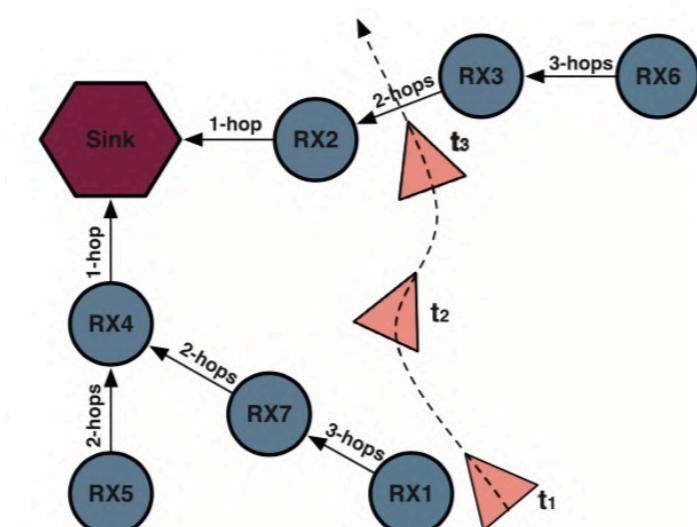
2008 Efficacité énergétique ? Acheminement des données ?

2016

Contrôle d'accès au medium
Routage

→ Disponibilité/sécurité
→ Mobilité intelligente

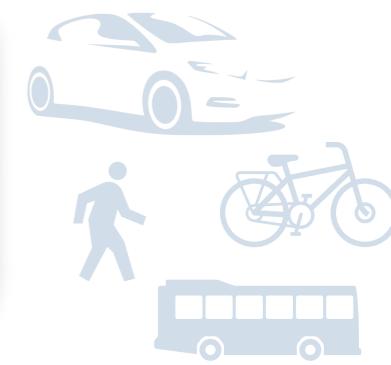
Auto-configuration/adaptation



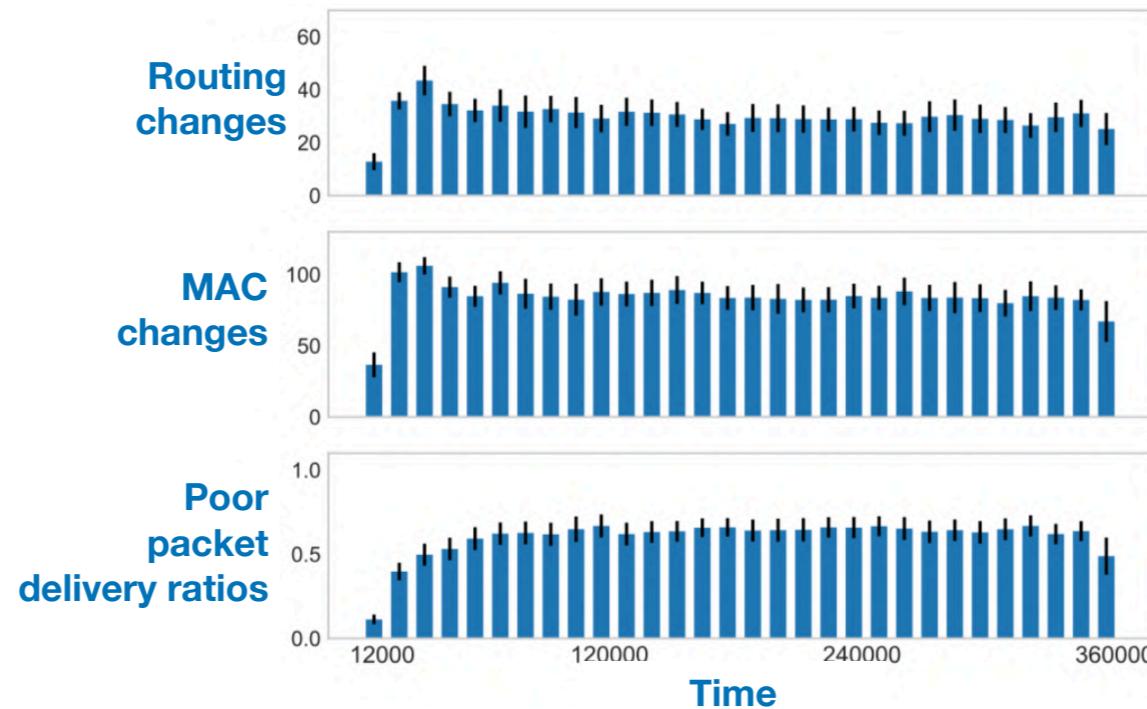
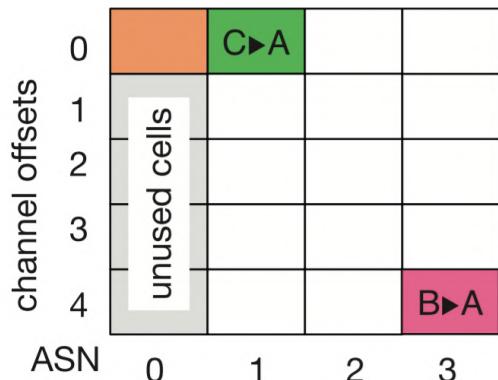
**46 co-auteurs
60 publications**

- 14 revues inter.
 - 7 à **FI>2.5**
 - 2 à **FI>9** depuis 2016
- 29 conf. inter.
 - **2 best paper**
 - **2 A et 1 B** depuis 2018
- 3 démos (conf. inter.)
- 10 conf. nat.
- 4 ouvrages collectifs

2016-* : disponibilité/sécurité et mobilité intelligente



- Garanties avec réseaux  (IPv6+IEEE 802.15.4-2015 TSCH)



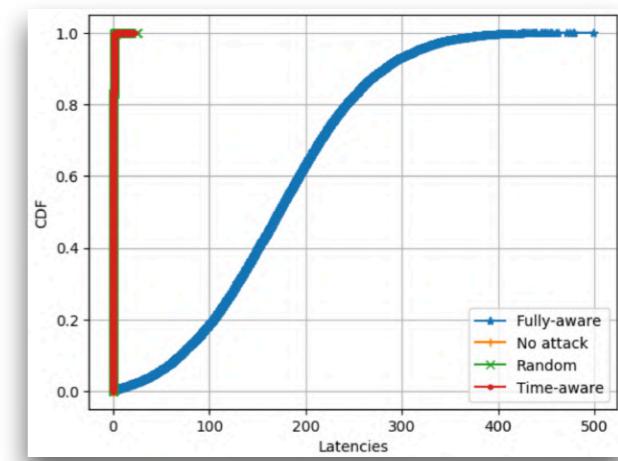
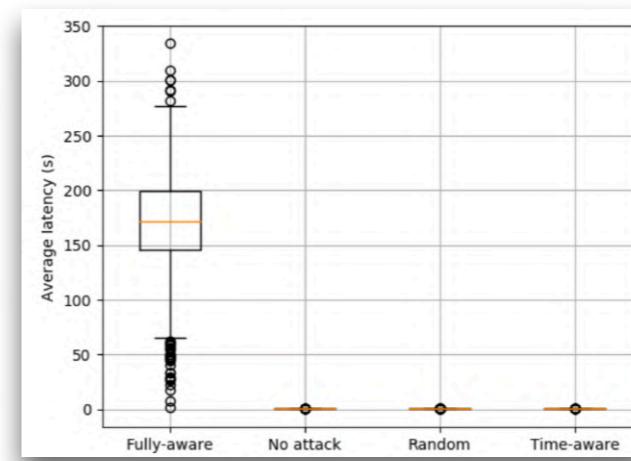
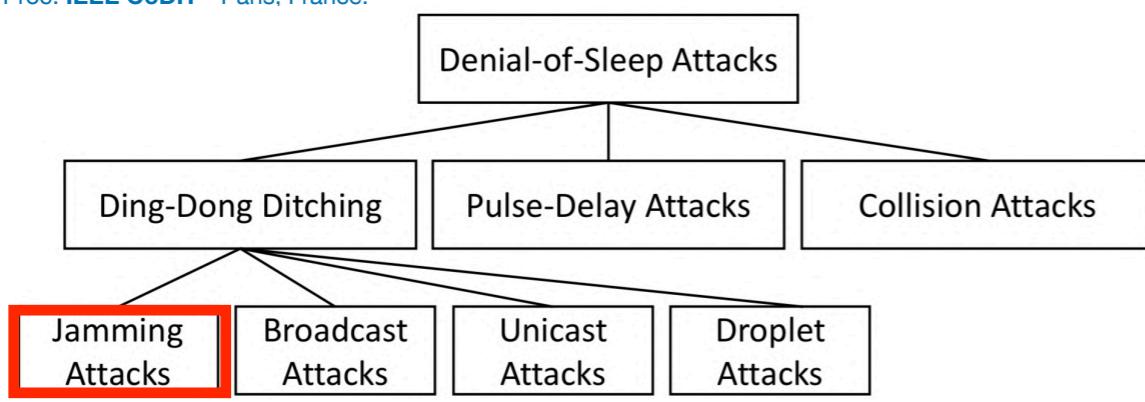
R. Teles Hermeto, A. Gallais and F. Theoleyre, *Impact of the Initial Preferred Parent Choice in Wireless Industrial Low-Power Networks*, In IEEE COMSOC MMTC Communications - Frontiers. pp. 43-46, Vol.12, No.6. 2017

R. Teles Hermeto, A. Gallais, K. Van Laerhoven and F. Theoleyre, *Passive Link Quality Estimation for Accurate and Stable Parent Selection in Dense 6TiSCH Networks*, in Proc. ACM EWSN - Madrid, Spain

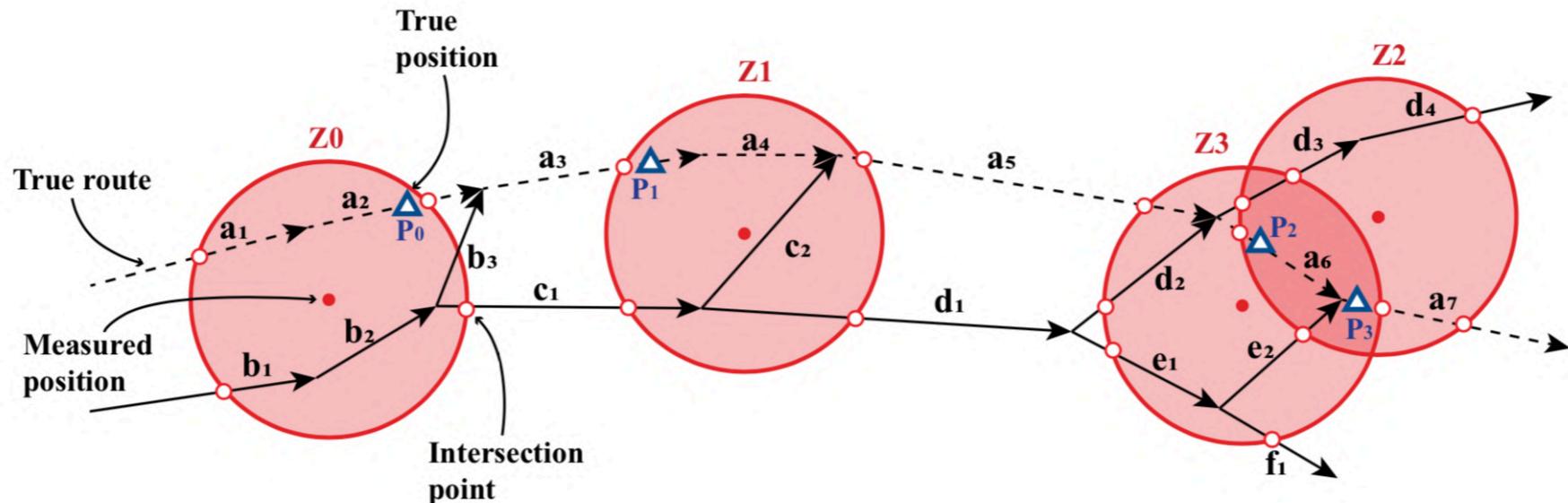
R. Teles Hermeto, A. Gallais and F. Theoleyre, *On the (over-)Reactions and the Stability of a 6TiSCH Network in an Indoor Environment*, in Proc. ACM MSWiM - Montreal, Canada. 2018

- Déni de sommeil et 6tisch

2019 A. Gallais, T.-H. Hedli, V. Loscri and N. Mitton, *Denial-of-Sleep Attacks against IoT Networks*, in Proc. IEEE CoDIT - Paris, France.

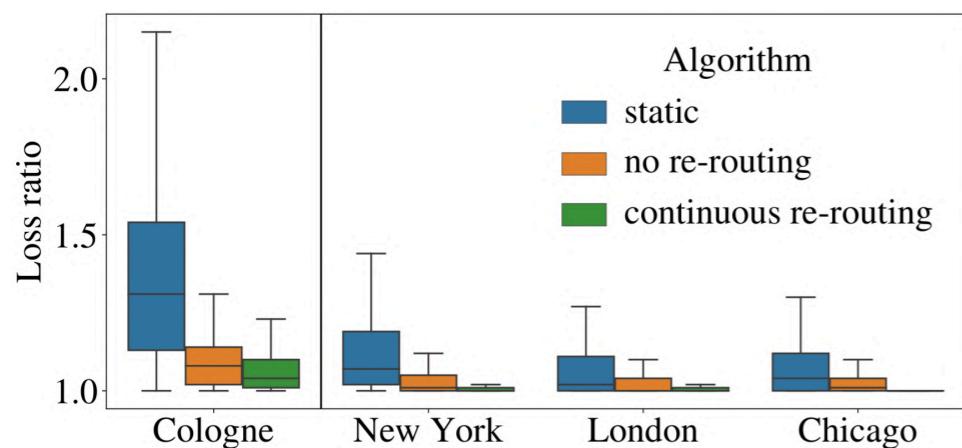


2016-* : disponibilité/sécurité et mobilité intelligente



2018 M. A. Falek, C. Pelsser, A. Gallais, S. Julien and F. Théoleyre, *Unambiguous, Real-Time and Accurate Map Matching for Multiple Sensing Sources*, in Proc. IEEE WiMob - Limassol, Cyprus.

- Objectif : planification d'itinéraires multi-modaux et personnalisés



2019 M. A. Falek, C. Pelsser, A. Gallais, S. Julien and F. Théoleyre, *De l'(in)utilité du temps-réel pour le calcul d'itinéraire dans les réseaux routiers*, in Proc. AlgoTel.

- Utilisation des données historiques ou temps-réel
 - Quand et où les utiliser ? Equilibrage de charge ?



Transition vers l'UPHF

* Rapport annuel Cour des comptes - février 2019, Tome I - Les observations, Chapitre IV « Les territoires »

- **Défis***

- Paysage académique en pleine évolution (Univ. Lille, UPHF, INSA)
- UPHF = Université « périphérique » / « de proximité »
 - ➡ Doit affirmer son identité pour se démarquer
 - ➡ Mobilité, cybersécurité, ingénierie

- **Enseignement**

- Reconfiguration de l'offre de formation et des composantes
 - Projet d'enseignement et d'animation dans l'axe cybersécurité

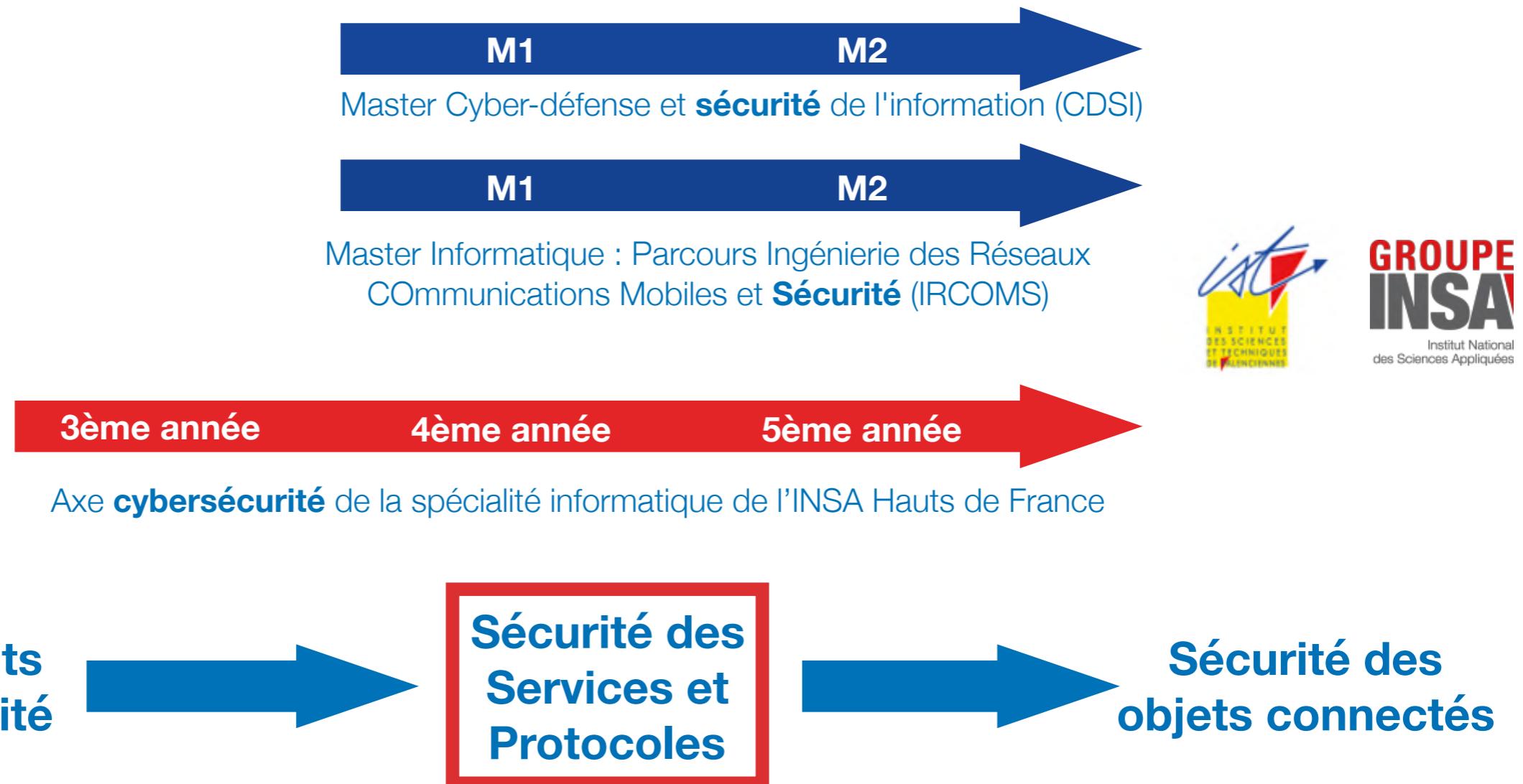


- **Recherche**

- LAMIH : Identité reconnue sur Transport/Sécurité, Mobilité/Handicap
 - Interactions avec les 2 thèmes du département informatique
 - Optimisation et Mobilité (OptiMOB)
 - Interaction et Agents (InterA)



Projet d'enseignement



Sécurité des Services et Protocoles

(10h CM / 10h TD / 9h TP, 3 ECTS)

Pré-requis

Utiliser un environnement **Unix**

Exposer les principaux **protocoles réseau** (IP, TCP, DNS, etc.)

Exploiter les bibliothèques existantes afin de **chiffrer/déchiffrer** un texte

Demander, générer, signer des **certificats électroniques**

Compétences visées

Mettre en place un **pare-feu**

Mettre en œuvre des protocoles garantissant l'authentification, l'autorisation, et la traçabilité (**AAA**)

Mettre en œuvre un **réseau privé virtuel** et un système de **détection d'intrusion**

Réaliser l'**audit de sécurité** d'une infrastructure système et réseau

Sécurité des Services et Protocoles

(10h CM / 10h TD / 9h TP, 3 ECTS)

Intro. (1h)

★ *lightning talks* (e.g., « *R. Morris* », « *R. Lychev* »)

★ (D)DoS (1,5h)

Cache poisoning (2h)

★ BGP / RPKI

BGP/politiques

★ Pare-feu

Eval./corr. (1h)

iptables

★ AAA

Kerberos

★ VPN et IDS

OpenVPN

Placement de solutions

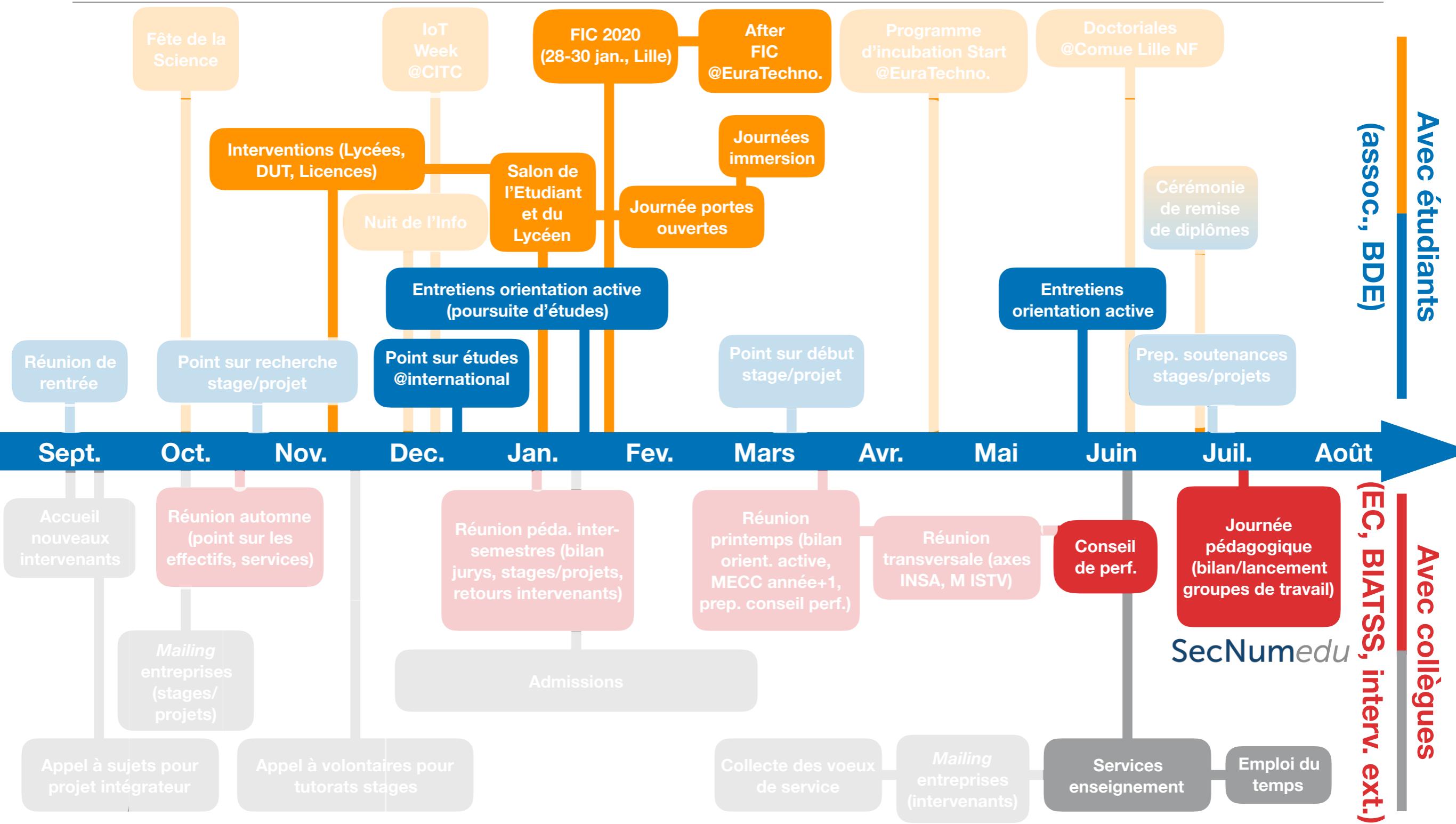
Eval./corr. (1h)

Snort et nessus (3h)

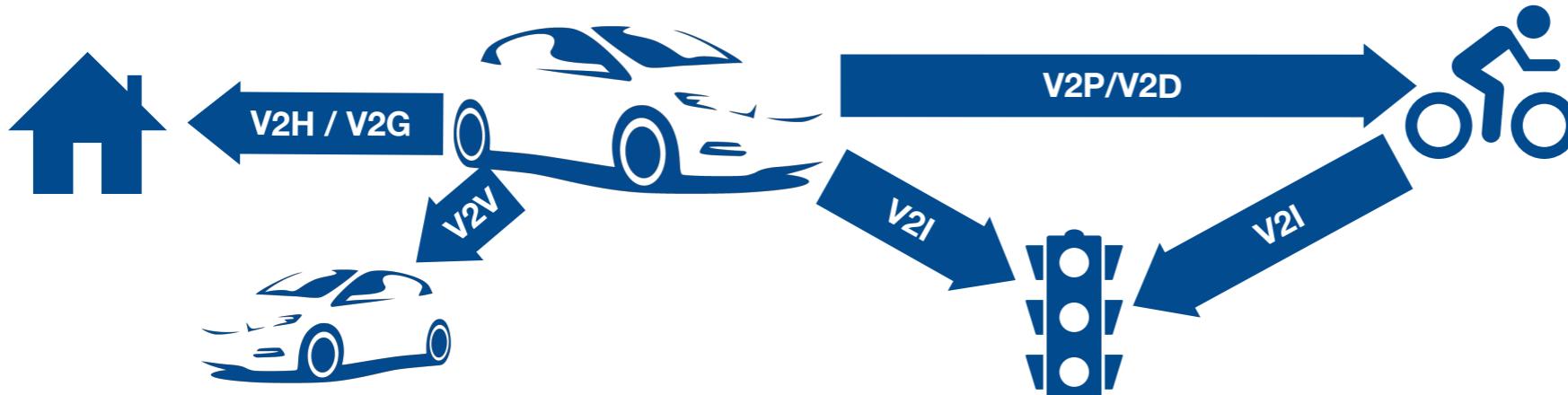
★ Audit de sécurité

nmap

Animation de l'axe cybersécurité @INSA



Mobilité intelligente et cybersécurité



- **Inciter à la multi/inter-modalité ?**

ELSAT 2020 **SmartMOB** (Services mobiles incitatifs à l'inter-modalité, **S. Lecomte**) et **OLOGMAESTRO** (Optim. des Opérations en Logistique et en Maintenance des Syst. de Transport, **D. Duvivier et R. Ben Atitallah**)

- Fournir des certitudes (e.g., parking, premier/dernier kilomètre)

M. Mladenovic, T. Delot, G. Laporte, and C. Wilbaut, *The parking allocation problem for connected vehicles*, Journal of Heuristics, Jan 2018.

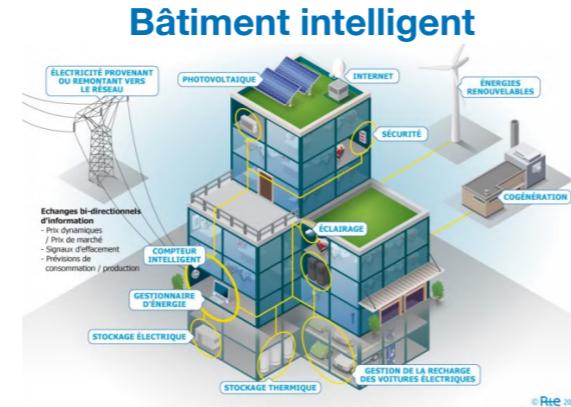
ELSAT 2020 **TASTE** (Ecomobilité à la demande intelligente et fiable, **R. Ben Atitallah**)

- **Etudier les communications V2X (e.g., IEEE 802.11p)**

B. Fall, S. Niar, A. Sassi, and A. Rivenq, *Adaptation of LTE-Downlink Physical Layer to V2X and T2X communications*, International Journal of Engineering and Innovative Technology (IJEIT), vol. 4, no. 10, pp. 182–192, 2015.

F. Salem, Y. Elhillali, and S. Niar, *Efficient modelling of IEEE 802.11p MAC output process for V2X interworking enhancement*, IET Networks, 2018.

Mobilité intelligente et cybersécurité



Aide à la conduite,
véhicule autonome

Alarmes incendie,
assistance à distance

Maintenance prédictive,
sécurité des personnes

Alimentation
domicile/véhicule

- Applications critiques reposant sur les objets connectés

- Détection d'attaques
- Résilience (i.e., disponibilité des réseaux et des données)
- Sécurité des communications et protection de la vie privée



Détection d'attaques ? Résilience ?

- Détection d'attaques de brouillage

- Conditions normales d'opération ?

- e.g., signatures des attaques sur les porteuses

ELSAT 2020 SECOURT (Cyber-SECurité dans les systèmes COmmUnicants pour les Transports, **S. Niar et A. Rivenq**)

. Sadoudi, U. Biaou, M. Bocquet, E. Moulin, **A. Rivenq**, and J. Assaad, *Experimental characterisation of IEEE 802.15.4 channel running at 2.4 GHz inside buildings*, in IEEE International Workshop on Measurements Networking (M N), Oct 2015, pp. 1–6.

- Apprentissage ?

→ Réseaux de neurones artificiels utilisés dans ENOrMOUS

I. Chaib Draa, **S. Niar, E. Grislin-Le Strugeon**, M. Biglari-Abhari, and J. Tayeb, *ENOrMOUS: ENergy Optimization for MOBILE plateform using User needS*, Sep. 2018, working paper or preprint.

- Résilience face au déni de sommeil

- Maintenir l'accès aux données ?

→ IA pour redondance des données

- Riposter ?

- SMA pour décisions collectives

→ Isolations des attaquants (e.g., MAC, routage)

F. Chakchouk, **J. Vion, S. Piechowiak, R. Mandiau**, M. Soui, and K. Ghedira, *Replication in Fault-Tolerant Distributed CSP*, in Advances in Artificial Intelligence: From Theory to Practice, 2017, pp. 136–140.

Sécurité des communications ? Protection de la vie privée ?



- Ext-store (Cisco, Fondation Unistra), avec IIJ (R. Bush)

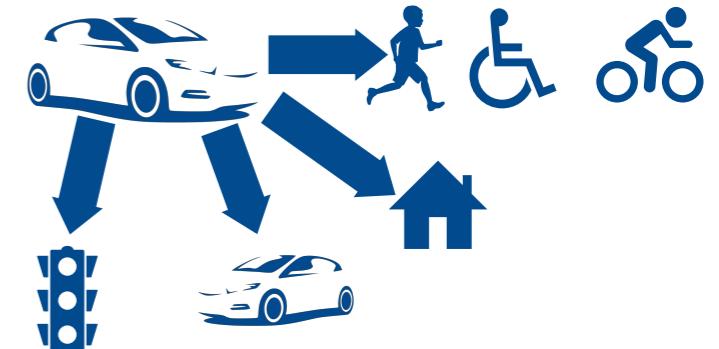


L. Miller (Projet Cisco, 2018-*)

- Authentification et Autorisation dans les systèmes de stockage en Cloud

→ Sécurité des services mobiles avec Edge/Cloud

ELSAT 2020 SmartMOB (Services mobiles incitatifs à l'inter-modalité)
ingénierie logicielle (M. Martinez)
réseaux et sécurité (D. Gantsou)
services mobiles (M. Desertot, S. Lecomte)



- Nano-NET (ANR JCJC), avec P. Mérindol, F. Theoleyre et C. Pelsser



- Nano-systèmes autonomes pour la protection de la vie privée dans l'IoT

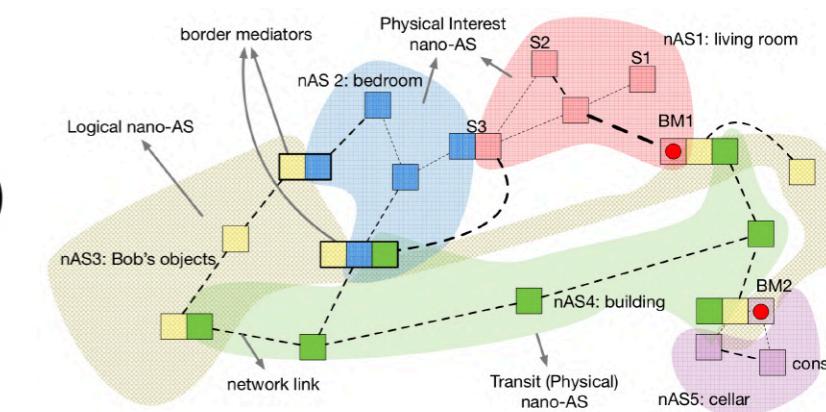
R. Juacaba Neto (ANR JCJC, 2019-*)

$$I = (\text{Node}, \text{Edges}, \text{Data streams}, \text{Exports})$$

$$ds = (\text{Producer}, \text{Name}, \text{Transformation})$$

→ Politiques de Sécurité pour communications V2X

→ Blockchain pour vérification des politiques ?



Collaborations extérieures

• Collaborations académiques existantes au LAMIH



Prof. Gilles Grimaud



IFSTTAR
DR Marion Berbineau



UNIVERSITÉ D'ARTOIS
Prof. Hamid Allaoui



Lab. Inter. Ass. (LIA-ROI-TML)



Prof. Soumaya Cherkaoui
(Univ. Sherbrooke)
Prof. Abdelhakim S. Hafid
(Univ. Montréal)



• Collaborations académiques envisagées



Prof. T. Noel
Prof. C. Pelsser



DR Nathalie Mitton
Dr. Valeria Loscri
& Dr. Diego
Cattaruzza

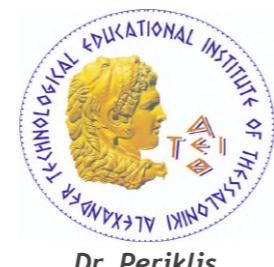


Université de Mons
Dr. Bruno Quoitin



UNIVERSITEIT
STELLENBOSCH
UNIVERSITY

Pr. Riaan Wolhuter



Dr. Periklis
Chatzimisios



Prof. Bjorn De Sutter
University of
Kent
Prof. Shujun Li



Prof. Bart Preneel
KU LEUVEN



Prof. Ramin Sadre

• Collaborations industrielles



Things next



Conclusion

- **Enseignement**
 - Compétences et expérience (cybersécurité et animation pédagogique)
- **Recherche**
 - Continuité de l'évolution entamée depuis 2016 (sécurité et mobilité)

→Cohérence entre activités d'EC et convictions/valeurs personnelles

- Mobilité intelligente et cybersécurité
- Humain au cœur des stratégies INSA et LAMIH

Candidature au recrutement sur l'emploi de Professeur des Universités n°4225

Université Polytechnique Hauts-de-France (UPHF)

Antoine GALLAIS, qualifié aux fonctions de Professeur des Universités, CNU 27 (n°18127184517)

Enseignement @Unistra (2009-17)	Responsabilités	~265h /an ~350h Ingénieur, ~450h Master, ~1400h Licence (FI, Altern., EAD, VAE) <i>Systèmes et réseaux (113,5h/an), sécurité des systèmes et des réseaux (52h/an)</i> 2 filières (M2, LP), 11 UE (CM, TD, TP) <i>7 campagnes d'évaluation/habilitation/accréditation</i>
Recherche @ICube (2008-*)	60 publications 46 étudiants 17 projets	14 revues inter., 29 conf. internationales <i>MAC, routage, éval. perf., tolérance aux pannes, sécurité</i> 7 doctorants dont 4 en cours <i>Planification d'itinéraire et mobilité intelligente</i> <i>Nano-systèmes autonomes pour la protection de la vie privée dans l'IoT</i> <i>Authentification et Autorisation pour stockage en Cloud</i> 5 internationaux, 5 nationaux, 7 locaux <i>en cours : 1 ANR JCJC, 2 collab. indus. (T&S, Cisco)</i>

Fondements de la sécurité

(10h CM / 10h TD / 9h TP, 3 ECTS)

Prérequis

Manipuler **arithmétique modulaire** (congruence, exponentiation modulaire)

Exposer les principaux **protocoles réseau** (IP, TCP, DNS, etc.)

Utiliser un environnement **Unix**

Utiliser un langage de **script** (Shell, Python)

Compétences

Expliquer les différences fondamentales entre cryptographie **symétrique** et **asymétrique**

Évaluer la robustesse d'un mécanisme de chiffrement donné face à une **attaque de force brute**

Déterminer quel type de **cryptanalyse** adopter pour un mécanisme de chiffrement donné

Demander, générer, signer des **certificats électroniques**

Fondements de la sécurité

(10h CM / 10h TD / 9h TP, 3 ECTS)

Introduction (1,5h)

Chiffrement sym.

openssl chiffr. sym. (2h)

Cryptanalyse

Cryptanalyse (sym., 2h)

Feistel, DES, AES

Chiffrement asym.

Eval./corr. (1h)

openssl chiffr. asym.

RSA

RSA (théorie et pratique)

Factorisation RSA, MitM

Sign. et certificats

Eval./corr. (1h)

GPG

PKI + SSL/TLS

openssl certif. X.509 (3h)

Fondements de la sécurité

(10h CM / 10h TD / 9h TP, 3 ECTS)

Introduction (1,5h)

Chiffrement sym.

Cryptanalyse

Chiffrement asym.

RSA

Sign. et certificats

PKI + SSL/TLS

Diffie-Hellman (Merkle)

The new technique makes use of the apparent difficulty of computing logarithms over a finite field $GF(q)$ with a prime number q of elements. Let

$$Y = \alpha^X \pmod{q}, \quad \text{for } 1 \leq X \leq q-1, \quad (4)$$

where α is a fixed primitive element of $GF(q)$, then X is referred to as the logarithm of Y to the base α , mod q :

$$X = \log_{\alpha} Y \pmod{q}, \quad \text{for } 1 \leq Y \leq q-1. \quad (5)$$

Calculation of X from Y is easy, taking at most $2 \times \log_2 q$ multiplications [6, pp. 398-422]. For example, for $X = 18$,

$$Y = \alpha^{18} = (((\alpha^2)^2)^2) \times \alpha^2. \quad (6)$$

Computing X from Y , however, is difficult and, for certain values of q , requires on the order of q operations. An algorithm [7, pp. 9, 57]

http://ciscac.fsi.stanford.edu/people/whitfield_difflie



RSA : fondements mathématiques

Factorization of a 768-bit RSA modulus

version 1.4, February 18, 2010

Thorsten Kleinjung¹, Kazumaro Aoki², Jens Franke³, Arjen K. Lenstra⁴, Emmanuel Thomé⁴, Joppe W. Bos⁴, Pierrick Gaudry⁴, Alexander Kruppa⁴, Peter L. Montgomery^{5,6}, Dag Arne Osvik¹, Herman te Riele⁶, Andrey Timofeev⁶, and Paul Zimmermann⁴

¹ EPFL IC LACAL, Station 14, CH-1015 Lausanne, Switzerland
² NTT, 3-2-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan
³ University of Bonn, Department of Mathematics, Beringstraße 1, D-53115 Bonn, Germany
⁴ INRIA CNRS LORIA, Équipe CARAMEL - bâtiment A, 615 rue du jardin botanique, F-54602 Villers-lès-Nancy Cedex, France
⁵ Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA
⁶ CWI, P.O. Box 94079, 1090 GR Amsterdam, The Netherlands

<https://eprint.iacr.org/2010/006.pdf>

2 ans et demi de calculs (équivalent de 1700 cœurs, soit 425 PC quadri-cœurs pendant 1 an)

Cluster	number of nodes	CPU type	clock speed (GHz)	cores per node	GB RAM per node	interconnect	nodes per job	cores per job	seconds per iteration	stage 1	stage 3	communication
Lausanne	56	2xAMD 2427	2.2	12	16	ib20g	12	144	4.3-4.5	4.8	40%	
Tokyo	110	2xPentium 4	3.0	2	5	eth1g	110	220	5.8 ¹ , 6.4	7.8	33% ¹ , 44%	
Grenoble	34	2xXeon E5420	2.5	8	8	ib20g	24	144	3.7	n/a	30%	
Lille	46	2xXeon E5440	2.8	8	8	mx10g	36	144	3.1	3.3	31%	
							32	256	3.8	n/a	38%	
							24	144	4.4	n/a	33%	
Nancy	92	2xXeon L5420	2.5	8	16	ib20g	64	256	2.2	2.4	41%	
							36	144	3.0	3.2	31%	
							24	144	3.5	4.2	30%	
							18	144	n/a	5.0	31%	
							16	64	n/a	6.5	19%	
Orsay	120	2xAMD 250	2.4	2	2	mx10g	98	196	2.8	3.9	32%	
Rennes	96	2xXeon 5148	2.3	4	4	mx10g	64	256	2.5	2.7	37%	
							49	196	2.9	3.5	33%	
Rennes	64	2xXeon L5420	2.5	8	32	eth1g	49	196	6.2	n/a	67%	
							24	144	8.4	n/a	67%	
							18	144	10.0	n/a	68%	
							8	64	n/a	18.0	56%	

Table 2: Data and first and third stage block Wiedemann timings for all clusters used. "n/a" means that the job configuration was not used.
[: figure per iteration per sequence when two sequences are processed in parallel, in which case a part of the communication time is hidden in the local computation time (the communication number above the rmp communication percentage) for all other figures but the last one in the table.]

A. Gallais

Sécurité des Systèmes et des Réseaux

Fondements de la sécurité

(10h CM / 10h TD / 9h TP, 3 ECTS)

Introduction (1,5h)

Chiffrement sym.

openssl chiffr. sym. (2h)

Cryptanalyse

Cryptanalyse (sym., 2h)

Feistel, DES, AES

Chiffrement asym.

Eval./corr. (1h)

openssl chiffr. asym.

RSA

RSA (théorie et pratique)

Factorisation RSA, MitM

Sign. et certificats

Eval./corr. (1h)

GPG

PKI + SSL/TLS

openssl certif. X.509 (3h)

Fondements de la sécurité

(10h CM / 10h TD / 9h TP, 3 ECTS)

Introduction (1,5h)

Chiffrement sym.

openssl chiffr. sym. (2h)

Cryptanalyse

Cryptanalyse (sym., 2h)

Feistel, DES, AES

La suite gpg vous permet de générer vos clefs PGP, avec lesquelles vous pouvez chiffrer et signer des documents. Vous pouvez également diffuser vos clefs à l'aide de serveurs de clefs et ainsi accéder facilement à celles des autres. Vous pourrez en profiter pour signer les clefs de personnes de confiance.

Actuellement, la clef 135C7E3E est disponible sur keys.gnupg.net.

Voyez comment signer cette clef et ensuite initier votre toile de confiance.

La clef 135C7E3E a été utilisée pour signer des documents, dont (je crois, à vous de vérifier) :

- <https://clarinet.u-strasbg.fr/~gallais/uploads/Teaching/test.txt.asc>
- <https://clarinet.u-strasbg.fr/~gallais/uploads/Teaching/test2.txt.asc>

Chiffrement asym.

Eval./corr. (1h)

RSA

RSA (théorie e

Vous pourrez alors lister et vérifier les signatures pour une clef donnée. Il vous arrivera également de devoir supprimer de votre trousseau une ou plusieurs clefs publiques , voire de révoquer des signatures que vous aurez apposées sur les clefs d'autres personnes .

L'objectif du TP est de visualiser la toile de confiance établie au sein de la promotion¹.

Pour finir, si vous souhaitez organiser une *key signing party* :

http://cryptnet.net/fdp/crypto/keysigning_party/en/keysigning_party.html

Factorisation RSA, MitM

Sign. et certificats

Eval./corr. (1h)

PGP

PKI + SSL/TLS

openssl certif. X.509 (3h)

Exemple : Sécurité des systèmes et des réseaux (M1 info.)

- 20h CM, 17h TP

Cours (A. GALLAIS et C. ZORN)

Partie A. GALLAIS

- Introduction
- Chiffrement
- Certificats
- SSL/TLS
- Logiciels malveillants
- Attaques réseau
- Pare-feux, IDS, AAA, VPN
- Authentification CAS

En complément de la partie Kerberos du cours.

Partie C. ZORN

- Support
- Droit

<https://moodle3.unistra.fr/course/view.php?id=2163>

Exercices



Cahier d'exercices



Cas pratique "Données personnelles"

Utilisez ces documents pour répondre à votre amie avocate dans un dossier où elle doit conseiller la société Top Medoc.

En particulier, travaillez à qualifier toutes les données utilisées par cette société : à caractère personnel ou non.

Evaluations



Interrogation écrite (correction)



TP noté



Fichiers relatifs au TP noté



DS 2016/17



Eléments de correction DS 2016/17

TP (A. GALLAIS et S. SCHMITT)

- TP 1 : mots de passe
 - Archive des fichiers nécessaires au TP 1
 - Les mêmes mots de passe que dans crackme.txt mais avec des hashes LM
 - Correction TP 1 - John the Ripper (2015/16)
 - Correction TP 1 - John the Ripper (2016/17)
- TP 2 : chiffrement symétrique
 - Archive des fichiers nécessaires au TP 2
 - Correction TP 2 - Chiffrement symétrique (2015/16)
 - Correction TP 2 - Chiffrement symétrique (2016/17)
- TP 3 : chiffrement asymétrique
 - Archive des fichiers nécessaires au TP 3
 - Correction TP 3 - Chiffrement asymétrique (2015/16)
 - Correction TP 3 - Chiffrement asymétrique (2016/17)
- TP 4 : certificats x509
 - Archive des fichiers nécessaires au TP 4
 - TP 4 : éléments de correction
 - Correction TP 4 - Certificats x509
- TP 5 : GPG
 - Correction TP 5 - GPG
- TP 6 : iptables statique
 - Correction TP 6 - iptables
 - Matrice de Flux Réseau
 - Matrice de Flux Réseau
- TP 7 : audit de sécurité
 - Correction TP 7 - Audit sécurité
- Contrôle TP 2016/17
 - Fichiers exercice 1
 - Fichiers exercice 2
 - Fichiers exercice 3
 - Dépôt de vos réponses au TP noté
 - [NE PAS AFFICHER] Eléments de correction du CTP