# Offre de Thèse:
# Études et Performances de Contre-Mesures de Cybersécurité pour des Réseaux et Plates-Formes IoT

**Laboratoire** : Institut d'Électronique det de Télécommunication de Rennes (IETR), UMR CNRS 6164
`https://www.ietr.fr/?lang=fr`
**Mots-clefs** : Cybersécurité, architecture logicielle/matérielle, IoT, réseaux de capteurs

## Contexte

Les objets connectés (Internet of Things, IoT) permettent d'envisager de nouveaux services dans de nombreux domaines : transport intelligent, ville intelligente, santé & bien-être, agriculture, etc. La sécurité et la confidentialité des données transitant via les futurs réseaux de systèmes IoT sont devenues une nécessité afin de convaincre les acteurs du marché et l'utilisateur final. D'ailleurs, il est fort probable que la sécurité d'un produit sera dans l'avenir un élément permettant de faire la différence dans un marché concurrentiel. Tous les domaines d'application sont concernés : maison intelligente (Ambient Assisting Living), industrie 4.0, santé & bien-être, agriculture, etc. Un système utilisant des objets connectés met en oeuvre de nombreux protocoles. La sécurité est quelque chose qui doit se faire de bout en bout et donc se penser à tous les niveaux du modèle OSI. C'est pourquoi, les questions de sécurité et de confidentialité des données transmisses doivent aussi s'imaginer dès la conception au niveau des couches PHY/MAC. Enfin, l'essort de la radio logicielle et de plateforme à bas coût offre au cybercriminel un accès beaucoup plus aisé aux couches basses des réseaux de communication [1] ce qui risque d'accroître les menances sur un système d'information.

## Problématique

La sécurité dans les systèmes d'information a et fait l'objet de travaux depuis de nombreuses années. Les réseaux IoT font progressivement leur arrivée et eux aussi sont sujets à des attaques. Nous pouvons relever des attaques sur la couche PHY du type écoute et brouillage. La couche MAC fait elle aussi l'objet de menace comme par exemple l'attaque Ghost dans les réseaux Zigbee (IEEE 802.15.4) [2] qui agit pour réduire la durée de vie sur batterie d'un noeud réseau. Les problèmatiques générales pour un réseau IoT vont être :

— l'authenticité des données
— la confidentialité des données
— l'intégrité des données
— la disponibilité du réseau

L'intégration de mécanismes de défense à un problème de sécurité dans le cadre d'un réseau d'objets connectés se trouve être un challenge. Les contraintes sont fortes dans le domaine de l'embarqué : complexité, efficacité énergétique des noeuds mais aussi scalabilité. Dans ce contexte, la question de l'implémentation, de l'utilisation et de la faisabilité d'un mécanisme de contre-mesure à une attaque se pose.

Les récentes réflexions autour de nouveaux réseaux de capteurs/actionneurs dits cognitifs permettent d'envisager une meilleure utilisation du spectre et par la même de réduire les interférences. Néanmoins, l'accès dynamique au spectre introduit de nouveaux problèmes en terme de sécurité comme des attaques du type "Primary User Emulation Attack" (PUEA). Le challenge pour ce type de réseau est particulier car il est dynamique par nature. Il convient donc d'étudier les problèmes et de proposer des solutions de sécurité pour ces futurs réseaux. Par ailleurs, les noeuds de ces réseaux sont contraints en terme de ressources matérielles, logicielles, et réseau.

Pour résumer, les verroux scientifiques sont :

1. Réseaux cognitifs et les ménaces de sécurité associées
2. Connaissance et évaluation du coût d'utilisation de contre-mesures à une attaques sur un noeud cyber-physique en terme de ressources et contraintes : mémoire, batterie, ressources de calcul.

## Objectifs

Le premier objectif sera d'analyser les faiblesses en terme de sécurité des futurs réseaux IoT en étudiant les attaques recensées dans la littérature. Les attaques relatives à la couche PHY et la couche MAC seront étudiées. Cette première étude se focalisera aussi bien sur les attaques passives et actives. Un regard spécifique sera porté sur les réseaux contraints de capteurs et actionneurs dits cognitifs. Cette première phase permettra de définir le scénario d'étude et influencera le développement de l'environement de test final. Le domaine d'application des réseaux du type LR-WPAN (IEEE 802.15.4, etc.) sera un référentiel pour le futur cas d'étude.

Dans un second temps, un travail sur des propositions et évaluations correspondantes spécifiques aux couches PHY/MAC sera fait. Elles se porteront sur la détection (Intelligent Spectrum Sensing) et les contre-mesures que le réseau peut mettre en place pour s'adapter à une menace active : attaque DoS, Primary Users Emulation, etc. Le caractère adaptatif d'un réseau cognitif est un risque en terme de sécurité mais aussi une piste intéressante en terme d'adaptation à un environnent menacé.

Au sein de l'équipe SYSCOM de l'IETR, un hyperviseur léger (KER-ONE) [3] dédié à des systèmes sur puce (System On Chip, SOC) ayant une partie reconfigurable a été développé. Cela apporte de la flexibilité et de l'adaptabilité pour de futurs noeuds de communication. Cette solution technique sera utilisée afin de mettre en oeuvre les solutions proposées dans ce travail de thèse.

Enfin, l'adéquation entre les propositions algorithmiques et le matériel est un point important du travail dont l'étude précédente donnera des indications de faisabilité. L'évaluation des performances se fera en fonction des contraintes de compléxité et d'energie des dispositifs cyber-physique ciblés. Les travaux seront valorisés par le développement d'un démonstrateur afin de permettre d'évaluer les solutions dans un environnement réel. Outre l'aspect démonstration, cela permettra de créer une plate-forme de cybersecurité pour des tests dans le domaine des réseaux IoT.

Les contributions attendues sont les suivantes :

1. Propositions de solutions algorithmiques et méthodologiques visant à aider la communauté sur les aspects sécurité des couches PHY/MAC dans le cadre de réseaux de capteurs/actionneurs. Le cas spécifique des réseaux dits cognitifs sera abordé.
2. Etude de l'impact de l'implémentation des contre-mesures à une attaque sur un réseau contraint en terme de complexité, énergie, scalabilité des systèmes embarqués. L'adéquation algorithmique architecture est un angle d'étude afin de démontrer la faisabilité des solutions proposés.
3. Mise en oeuvre des mécanismes proposés et valorisation avec un démonstrateur matériel basé sur les travaux de l'équipe SYSCOM (hyperviseur KER-ONE).

## Références

[1] C. Kasmi, A. Ebalard et P-M. Ricorder. "De la radio matérielle à la radio logicielle : impact sur l'étude de la sécurité des réseaux sans fil".

[2] Devu Manikantan Shila, Xianghui Cao, Yu Cheng, Senior Member, Zequ Yang, Yang Zhou, and Jiming Chen. "Ghost-in-the-Wireless : Energy Depletion Attack on ZigBee", CoRR, volume abs/1410.1613, 2014.

[3] Tian Xia. "Étude des techniques de virtualisation pour des systèmes temps-réel et reconfigurables dynamiquement", Thèse, 2016.

## Profil et compétences

— Diplôme d'ingénieur ou Master 2
— Compétences : Réseau (niveau 1,2 et 3), Informatique (Logicielle & Matérielle). Des notions de communications numériques ainsi que des connaissances en cybersécurité seront un plus.

## Informations

— Laboratoire d'acceuil : IETR (`https://www.ietr.fr/?lang=fr`)
— Equipe de recherche : SYSCOM
— Lieu : IETR/INSA
— Date début : Octobre 2017 (durée 3 ans)
— Financement : Contrat Doctoral Ordinaire (`http://matisse.ueb.eu/fr/financements/`)

## Candidature

Courriel avec :
— Lettre de motivation et CV complet (projets étudiants, ...)
— Bulletin de notes des deux dernières années

Date limite : 1 Juin 2017

## Contacts

Nouvel Fabienne
✉ fabienne.nouvel@insa-rennes.fr
☎ 02.23.23.84.47
Fonction Enseignant / Chercheur
Département Signal & Communications (SC)
Équipe SYSCOM (SYStems COMmunication)
Bât. 6
Institut National des Sciences Appliquées de Rennes
20, Avenue des Buttes de Coësmes - CS 70839
35708 RENNES Cedex 7
FRANCE

Tanguy Philippe
✉ philippe.tanguy@insa-rennes.fr
☎ 02.23.23.82.68
Fonction Enseignant / Chercheur (Contractuel)
Département Signal & Communications (SC)
Équipe SYSCOM (SYStems COMmunication)
Bât. 6
Institut National des Sciences Appliquées de Rennes
20, Avenue des Buttes de Coësmes - CS 70839
35708 RENNES Cedex 7
FRANCE

# PhD Offer:
# Studies and Performances of Counter-measures in Cybersecurity for IoT Networks and Platforms

**Laboratory**: Institut d'Électronique det de Télécommunication de Rennes (IETR), UMR CNRS 6164
`https://www.ietr.fr/?lang=fr`
**Keywords**: Cybersercurity, architecture software/hardware, IoT, sensor networks

## Context

Nowadays with the Internet of things paradigm (IoT) new services emerge in many area such as: intelligent transport, smart cities, health & well-being, agriculture, etc. Security and privacy of the data transfered in those networks is a key objective for the next generation of networks in order to convince end users and operators in the market. Moreover, the security of a product will be probably a key factor to make the difference in a high concurential market. Every domain is concerned: smart home (Ambient Assisting Living), digital industry 4.0, health & well-being, agriculture, etc. Many protocols are used in the system with IoT object from small devices to high level services. The security needs to be thought at each level of the OSI model. That is why, the PHY and MAC layers are also concerned by security issues. Indeed, software defined radio (SDR) and low-cost SDR platforms make easier the access to the PHY/MAC layers of sensors/actuators networks by cybercriminal [1].

## Problem overview

The security of information system is studied since a long time. The IoT paradigm is recent but he is also subject to attacks. Indeed attacks dedicated to the PHY layer such as eavesdropping and jamming have been studied in the litterature. The MAC layer is also threatened like for example the Ghost attack on Zigbee networks (IEEE 802.15.4) [2] with the objective to reduce the battery level of a node. The issues of an IoT networks are:

— Data authenticity
— Data confidenciality
— Data integrity
— Network availability

The Counter measures to attacks is something challenging to implement in resource constrained IoT devices and networks. We will study the faisability of counter measures implementation in this context.

Recently, cognitive radio networks have been studied. The basic idea is to have a better utilization of the spectrum and reduce interferences. It is a paradigm shift compare to usual sensor networks. Nevertheless, a dynamic access to the spectrum introduce new problems from the security point of view as shown by the "Primary User Emulation Attack" (PUEA). In this context, it is interesting to study issues and propose solutions of security for these futur networks.

To resume the main scientific questions are:

1. Cognitive networks and related security threats
2. Evaluate the cost of counter measures implementation on cyber-physical nodes in terms of memory, batterie, etc.

## Objectives

The first objective will be to analyze the weakness of IoT networks. This first study will target passive and active attacks. A specific attention will be done on cognitive networks. This first step will allow to define a scenario for the next step and the testbed. The Sub-GHz communications and networks such as LR-WPAN (IEEE 802.15.4, etc.) will be a good starting point.

In a second step, a study around intelligent spectrum sensing algorithms to detect attacks should be done. Then we will see how to propose counter measures strategies to reduce or avoid attacks such as DoS, Primary Users Emulation, etc.

In the SYSCOM research team of the IETR laboratory, a lightweight hypervisor (KER-ONE) has been developed [3] dedicated to System On Chip (SOC) with a reconfigurable hardware (ARM-FPGA). It allows flexibility and adaptability for maybe the next generation of IoT nodes. This solution will be exploited in this PhD work.

Finally, the adequation between algorithms and hardware will be studied. The performance evaluations will be done in function of the complexity and energy consumption of the cyber-physical nodes targeted. All this work will be enhanced with the development of a demonstrator in order to evaluate our solutions in a real environment. Besides the demonstration aspect it will allow to make a cybersecurity platform to make test in the domain of IoT networks.

At the end, the attended contributions should be the following:

1. Algorithms and methodologies related to cybersecurity counter measures in the context of IoT networks and their PHY/MAC layers. The specific case of the cognitive networks will be take into account.
2. Study of the impact of counter measuers implementation in the context of embedded IoT nodes. The software/hardware adequation will be study in order to show the faisability of the proposed solutions.
3. Implementation of proposed mechanisms on the testbed which will be based on the research work of the SYSCOM team (hypervisor KER-ONE).

## References

[1] C. Kasmi, A. Ebalard et P-M. Ricorder. “De la radio matérielle à la radio logicielle: impact sur l’étude de la sécurité des réseaux sans fil”.

[2] Devu Manikantan Shila, Xianghui Cao, Yu Cheng, Senior Member, Zequ Yang, Yang Zhou, and Jiming Chen. “Ghost-in-the-Wireless: Energy Depletion Attack on ZigBee”, CoRR, volume abs/1410.1613, 2014.

[3] Tian Xia. “Étude des techniques de virtualisation pour des systèmes temps-réel et reconfigurables dynamiquement”, Thèse, 2016.

## Profil et compétences

— Master degree or equivalent.
— Key skills: Networks (level 1,2 et 3), Computer science (low level software & hardware). A knowledge of digital communications and cybersecurity will be appreciate.

## Informations

— Laboratory: IETR (`https://www.ietr.fr/?lang=fr`)
— Research team: SYSCOM
— Location: IETR/INSA
— Starting date: October 2017 (3 years)
— Contract: Contrat Doctoral Ordinaire (`http://matisse.ueb.eu/fr/financements/`)

## Candidature

Email with:
— Cover letter and full CV (student projects, ...)
— Complete academic records (MSc)

Deadline: 1st June 2017

# Contacts

Nouvel Fabienne
✉ fabienne.nouvel@insa-rennes.fr
☎ 02.23.23.84.47
Enseignant / Chercheur
Département Signal & Communications (SC)
Équipe SYSCOM (SYStems COMmunication)
Bât. 6
Institut National des Sciences Appliquées de Rennes
20, Avenue des Buttes de Coësmes - CS 70839
35708 RENNES Cedex 7
FRANCE

Tanguy Philippe
✉ philippe.tanguy@insa-rennes.fr
☎ 02.23.23.82.68
Fonction Enseignant / Chercheur (Contractuel)
Département Signal & Communications (SC)
Équipe SYSCOM (SYStems COMmunication)
Bât. 6
Institut National des Sciences Appliquées de Rennes
20, Avenue des Buttes de Coësmes - CS 70839
35708 RENNES Cedex 7
FRANCE