Projet 5A EIS Innovation

2016-2017

Liste de sujets

Contenu

(A) Système de communication MISO pour drone aquatique

Encadrants : Pierre Lemaître-Auger, Darine Kaddour, **Yoann Hervagault**, doctorant LCIS et ingénieur à la société CT2MC

Contact : pierre.lemaitre-auger@lcis.grenoble-inp.fr, Darine.Kaddour@esisar.grenoble-inp.fr

Mots clés : Antenne, radiofréquence, système de communication, diversité temporelle, drone, MIMO, MISO, SIMO, diversity combining, chanel state information.

Thématiques scientifiques : Systèmes radiofréquences ; antennes ; systèmes numériques

Contexte du projet

Le développement de drones aquatiques est un sujet de développement actuel et porteur pour les industriels. Ainsi, on peut imaginer disposer de drones pour du sauvetage en mer, ou pour accomplir des tâches précises de prélèvement, de cartographie ou autre dans des endroits dangereux ou difficilement accessibles par bateau. Les retombées économiques seront importantes pour les sociétés impliquées dans un tel marché.

D'un point de vue technique, la communication avec un drone aquatique est un défi intéressant à relever. En effet, la présence de l'eau modifie de manière très importante le diagramme de rayonnement d'une antenne, tout comme les éléments métalliques présents sur le drone. Pour pallier à ces problèmes, une thèse industrielle est en cours au laboratoire LCIS en collaboration avec la société CT2MC.

C'est dans ce cadre que se situe ce projet. La portée de communication entre un drone et la berge est un paramètre clé. La stratégie développée durant la thèse est d'utiliser 2 antennes sur le bateau. Le sujet du stage portera sur le système de communication qui doit optimiser l'utilisation de ces deux antennes afin de maximiser la portée de communication.

Description du projet et travail attendu

Il faudra implémenter sur une carte électronique le protocole de communication envisagé. Ce protocole consiste à n'utiliser que l'antenne qui reçoit le plus d'énergie. Il faut donc tester en permanence les antennes et pouvoir reconfigurer le réseau en fonction du résultat obtenu. On nomme ce genre de technique MISO (Multiple Input, Single Output).

Dans un deuxième temps, il faudra réaliser un démonstrateur avec deux antennes fournies, une paroi métallique entre les deux et un système simple de pivotement pour simuler le changement d'orientation du drone. Selon l'avancement du projet, un test en situation réelle sur un lac pourra être réalisé.

(B) Régulation d'une maquette de canal d'irrigation par réseau de capteurs/actionneurs sans fil

Encadrants : André LAGREZE , Laurent LEFEVRE, Youness LAMI

Contact : andre.lagreze@lcis.grenoble-inp.fr

Mots clés : interface RF de commande et de supervision, protocole LoRa, asservissement moteur brushless, programmation microcontrôleur ARM.

Compétences : informatique embarquée, programmation Matlab, réseaux sans fil

Sujet : Le laboratoire LCIS possède une maquette de canal d'irrigation (appelé micro canal) permettant la validation de modèles de régulation de systèmes d'irrigation. Cette maquette comprend 3 vannes permettant de commander le débit d'entrée et de sortie des 2 biefs composant le microcanal (sans compter le bief amont et le bief aval). Chaque vanne est constituée de deux capteurs ultrasons mesurant la hauteur d'eau en amont et en aval de la vanne et d'un moteur brushless pilotant une porte coulissante ouvrant plus ou moins le passage à l'eau. Les vannes existantes sont vieillissantes et demandent à être remplacées. Un projet d'étudiants de l'année précédente a déjà bien dégrossi ce travail de remplacement et d'amélioration des vannes existantes et le projet de cette année consistera à finaliser le travail de l'année précédente et à le compléter par une partie régulation. Ce projet, qui sollicitera les connaissances des étudiants à la fois dans le domaine de l'automatique, de l'informatique embarquée, et de celui des transmissions RF et des réseaux associés, consistera donc à :

- prendre en main et améliorer la plate-forme existante (programmation en langage C sur microcontrôleur ARM, amélioration de la communication sans fil).
- prendre en main un nouveau moteur Crouzet incluant un asservissement de position et le paramétrer.
- déployer le réseau sans fil de capteurs/actionneurs.
- mettre en place une interface de contrôle/commande en Matlab en utilisant XPC Target et implanter une loi de commande simple.
- caractériser temporellement le système.

(C) Open Platform For Secure Processor Architecture Evaluation

Info: david.hely@lcis.grenoble-inp.fr

Keywords: Embedded System Programming, Processor Architecture, FPGA, VHDL, C, Security

Systems-on-chip (SoCs) are found in daily computing electronics including smartphones, industrial and automotive control devices, and embedded systems. The growing use of SoCs make them vulnerable to runtime software attacks such as memory hijacking, memory extraction, code injection, and code reuse.

In **memory hijacking**, malicious software uses the shared system bus or network-on-chip to write to a restricted memory segment to modify SoC configurations and execution settings. In memory extraction, malicious software reads from a restricted memory segment to leak critical data such as cryptographic keys or boot firmware. In **code injection**, an attacker leverages vulnerability such as stack-based or heap-based buffer overflow to control the return address in the stack or a function pointer in the heap. The attacker then writes arbitrary (malicious) code in the stack or heap and points the stack return address or the heap function pointer to the malicious code. In **code reuse**, the attacker also leverages a vulnerability to control the return address. The attacker uses code pieces (gadgets) already loaded in memory (i.e. shared library or the original software) and jumps from one gadget to another by updating the return address. The sequence of gadgets form the arbitrary code.

We enhance the SoC with a Memory Access Monitoring Module, to detect hijacking and extraction attacks and a Control Flow Monitoring Module for each processor core to detect code injection and code reuse attacks. A Security Kernel Process dynamically configures the added components and disables the malicious software upon attack detection.

An FPGA based Platform has been designed in order to evaluate new countermeasures against such software attacks. The objectives of this project are the following:

- Platform enhancement:
  - Addition of existing hardware countermeasures within the processor
  - Programming Flow enhancement for an user friendly use
- Demonstration Development
  - Integration of Security Benchmarks
  - Evaluation of Security Benchmarks
- New Secure Solution and Attacks Developments:
  - Proposition of new hardware countermeasures
  - Development of new software Attacks to enhance the security benchmarks

The Project will be performed in collaboration with New York University and the Institute of Technology Blanchardson (Ireland)

(D) Testing and implementation on a laboratory helicopter system

Ionela Prodan, ionela.prodan@lcis.grenoble-inp.fr,

Laurent Lefèvre, Laurent.lefevre@lcis.grenoble-inp.fr

Required scientific fields : Modeling and identification, Control Theory, Electronics, Informatics

Context: The project will focus on modeling and closed-loop control of a laboratory helicopter using conventional control methods. The system consists of a body, carrying two propellers driven by DC motors, and a massive support. The body has two degrees of freedom. Both body position angles (elevation and azimuth) are influenced by rotation of propellers. Center of gravity is changed by moving small weight along the main horizontal axis of helicopter by a servomotor. The mathematical model of the helicopter system is a typical MIMO 2 × 2 system with significant cross-couplings. The electromechanical system can be linearized to a linear sixth-order model when operating near the steady state.
A multifunctional card MF624 is used as interface module between PC based controller and helicopter system. It is designed for data acquisition and transmission. The card can be optimized for use with MATLAB/Simulink Real Time Toolbox. It also provides implementation of the control algorithms from the PC to the helicopter system. The user communicates with the system via Real Time Toolbox interface, all input/output signals are dimensionless and scaled into the MU (Machine Unit). The MATLAB/Simulink xPC Target Toolbox can be used to perform the experiments in real time applications.

An extensive range of experiments can be carried out with this apparatus. An example of experimental workflow is provided in the following: direct derivation of a general mathematical model using Lagrange equations, linearization and simpli- fication; on-line identification of linear model parameters; system decoupling techniques, diagonalization of system transfer matrix and state space methods; the PC based controllers of the elevation and azimuth angle can be designed in MATLAB/Simulink.

At the start of their project activities the students have to: (1) familiarize with existing nonlinear Helicopter dynamics, (2) provide trajectory generation mechanisms and optimization-based control strategies; (3) apply them in simulations over SISO/MIMO systems (nonlinear and linear systems).

At the end of the project the students are expected to: (1) be proficient with the Matlab/ Simulink environment and various toolboxes (Yalmip, MPT, Cplex for Matlab toolboxes); (2) have tested the theoretical notions over experimental platforms provided by LCIS laboratory and to have obtained results validating them.

References

[Ref. 1] R.W. Beard, T.W. McLain (2012) : Small unmanned aircraft: Theory and practice. Princeton University Press.

[Ref. 2] Y. Zhai, M. Nounou, H. Nounou, and Y. Al-Hamidi (2011): Model predictive control of a 3-dof helicopter system using successive linearization. International Journal of Engineering, Science and Tech- nology, vol.2(10).

(E) Développement d'une application Web d'identification RF issue d'un lecteur chipless UWB

Encadrants : S. Chollet, N. Barbot, E. Perret
Contact : stephanie.chollet@lcis.grenoble-inp.fr

La technologie RFID chipless est une solution d'avenir permettant d'identifier un objet par ondes radio fréquences. Ce système se compose d'un tag sans puce (placé sur l'objet à identifier) ainsi que d'un lecteur permettant d'interroger et de récupérer l'identifiant du tag totalement passif.

Dans le cas de la technologie RFID sans puce (chipless), le lecteur reprend les fonctionnalités d'un radar UWB à savoir l'émission d'un pulse très court et l'échantillonnage du signal rétrodiffusé par le tag. Le LCIS a développé sa propre solution chipless, à savoir un lecteur dédié ainsi que des tags réalisés par impression jet d'encre conductrice. Une démonstration de cette toute nouvelle technologie à mi-chemin entre le code à barres et la RFID avec puce a été faite dernièrement lors du salon international *la Drupa* à Düsseldorf. La vidéo consultable à l'adresse suivante https://tresor.it/s#Ma3mYvlgvs7tfNxMfmRcrg permet de voir les possibilités de lecture offertes par cette technologie.

Aujourd'hui la récupération des données d'identification RF est faite avec l'outil Matlab. Cet outil permet de s'interfacer avec le lecteur ainsi que de traiter et d'afficher les résultats localement. L'objectif du projet est de développer une application répartie qui permette de consulter ces mêmes résultats via une interface Web et de garder un historique des valeurs d'identification lues. L'interface Web doit être responsive ; c'est-à-dire s'adapter aux écrans des smartphones, tablettes et PC. En parallèle, il est demandé de modifier l'algorithme de traitement Matlab pour augmenter la performance ainsi que de déterminer d'autres informations comme la distance ou encore l'orientation du tag.

A terme, la fonction d'identification et de récupération des informations venant des capteurs devra se rapprocher des solutions de mesures autoalimentées, comme le WISP, mais ici uniquement à partir d'un objet totalement passif que l'on déplacerait dans la zone de lecture du radar. De plus, l'interface Web devra se mettre à jour dynamiquement en fonction des mesures faites avec la technologie des WebSockets.

Mots-clés : UWB, RFID Chipless, Capteurs, Matlab, Java EE, Red Hat WildFly, HTML5/CSS3, Bootstrap, WebSocket.
Compétences : Programmation Java et Matlab, Applications/Programmation réparties, Antennes, Electromagnétisme.

Vidéo du WISP contrôlant par sa position, son orientation :
https://youtu.be/SKQ3wkAqA_8
Informations sur les WISP :
http://sensor.cs.washington.edu/WISP.html

(F) Réalisation d'une communication haut débit par rétro-modulation

Encadrants : Nicolas Barbot, Laurent Guilloton, Etienne Perret

Contact : nicolas.barbot@lcis.grenoble-inp.fr

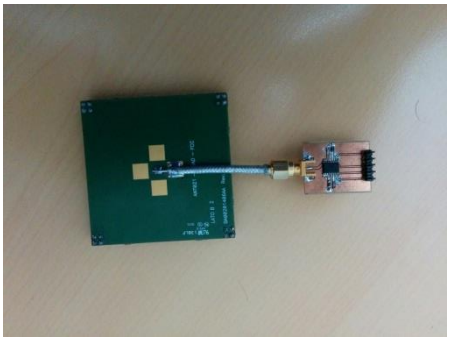
La technologie RFID utilise le principe de rétro-modulation pour moduler l'énergie envoyée par le lecteur. Il est ainsi possible de transmettre une information du tag vers le lecteur sans ajouter de module d'émission et sans consommation d'énergie supplémentaire.

L'objectif de ce projet est de mettre en place une liaison haut débit 4-QAM en utilisant le principe de rétro-modulation (le tag reste semi-passif).

L'architecture de la liaison repose sur un émetteur/récepteur de signaux vectoriels, le VST 4546R de National Instruments (pour le coté lecteur) et le switch ADG904 de Analog Devices (pour le coté tag). Le VST 4546R permet d'émettre et de recevoir un signal arbitraire dans la bande 70MHz-6GHz et de largeur de bande de 100MHz. Les traitements peuvent être effectués sur un FPGA présent dans le VST. Le switch ADG904 est un switch 4 états permettant générer la modulation 4-QAM. Cette modulation permet d'augmenter l'efficacité spectrale de la transmission (la RFID classique utilise une modulation 2 états).

Les opérations à réaliser pour mener à bien ce projet sont, pour le coté lecteur, le développement d'un programme en LabVIEW pour générer la porteuse, et d'extraire les caractéristiques du signal rétro-modulé (diagramme IQ). Pour le tag, un premier prototype est déjà disponible, il devra être piloté par un micro-contrôleur (ou un FPGA).

VST



Tag

La description détaillée du système peut être obtenue à l'adresse :
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.700.8007&rep=rep1&type=pdf

Mots-clés : Rétro-modulation, Démodulation IQ, LabVIEW, C.

(G) Création de comportements collectifs dans le contexte des systèmes cyber-physiques

Encadrants : Clément Raïevsky, André Lagrèze, Jean-Paul Jamont

Contact : clement.raievsky@lcis.grenoble-inp.fr

Mots clés : Systèmes multi-agents ; Robotique collective ; Systèmes cyber-physiques.

Contexte

Dans le cadre de la plateforme Easynov, l'équipe MACSY-COSY du laboratoire LCIS a pour objectif de mettre en œuvre un démonstrateur permettant de mettre en application ses activités de recherche. L'outil MASH (MultiAgent Software/Hardware tool) développé au sein du laboratoire est un outil qui permet l'exécution et la simulation de systèmes distribués mixtes logiciels/matériels. Ces systèmes sont par exemple des réseaux de capteurs, des applications de robotique collective, etc. Des robots EPuck, TurtleBot et GoPiGo (et les cartes Raspberry Pi associées) sont disponibles sur la plateforme.

Objectifs

L'objectif de ce projet est de mettre en place des applications permettant de démontrer les capacités d'un groupe de robots dans des tâches collectives (maintien en formation, jeu proies-prédateurs, exploration d'environnement, manufacturing control, réseaux VANET, etc.). Les membres de ces groupes pourront être à la fois des robots physiques et simulés, interagissants via le simulateur inclus dans MASH. Ce sujet est donc à la frontière de l'Intelligence Artificielle Collective (les systèmes multiagents), des systèmes embarqués et des systèmes cyber-physiques.

(H) Conception et implémentation d'un système de géolocalisation UWB robuste pour des systèmes cyber-physiques

Encadrants : N. Fourty, V. Beroulle

Contact : nicolas.fourty@lcis.grenoble-inp.fr, vincent.beroulle@lcis.grenoble-inp.fr

Mots-clés : UWB, géolocalisation, système embarqué, objet connecté, Sécurité et sûreté.
Compétences : Programmation embarquée, Communication sans fils, sécurité et sûreté

Ce travail vise la géolocalisation de robots mobiles. A l'heure actuelle, la géolocalisation en extérieur est très répandue et de plus en plus précise. L'enjeu de ces prochaines décennies est l'élaboration d'un système de géolocalisation en intérieur de très bonne précision et de faible consommation.

L'objectif premier de ce projet est de pouvoir localiser et tracer des robots mobiles en finalisation un prototype utilisant une technologie sans fil de type UWB. Toutefois la technologie UWB utilisée comme toutes les technologies sans fil est particulièrement vulnérable aux perturbations ou aux attaques de personnes malveillantes. Le second objectif est de rendre robuste la solution proposée vis à vis de ces perturbations ou attaques.

Dans le prototype existant, la localisation des robots est réalisée par un algorithme de positionnement. Le système est constitué de robots mobiles, d'ancres fixes et d'un PC central. Chaque robot mobile communique avec les ancres fixes. Les ancres envoient les messages reçus au PC central. Les distances entre les robots et les ancres sont alors déterminées par le PC en calculant les temps de vol des messages. Les ancres sont constituées d'un module Raspberry PI et d'un module de communication UWB. Le module RPI gère alors la communication UWB et la communication vers le PC central. Les tags sont les parties mobiles implantées sur les robots. Elles seront interfacées aux ancres via les ondes radios UWB (module UWB). Le rôle du tag est de : (1) recevoir les données provenant des ancres et de les transmettre aux robots, (2) recevoir les données des robots et les transmettre aux ancres. Le PC central a un rôle de supervision. Il permet : (1) d'afficher la position en coordonnée (X,Y) des robots à l'écran, (2) d'émettre et recevoir des données vers les robots, (3) de sauvegarder les informations dans une base de données.

La technique de géolocalisation sans fil utilisée doit prendre en compte des contraintes de sûreté et de sécurité; c'est-à-dire assurer l'intégrité des données transmisses et permettre la géolocalisation des robots même en présence de perturbations. La solution proposée doit être faible coût et faible énergie.

Le travail consistera tout d'abord à finaliser le prototype de géolocalisation et notamment le séquencement des commandes de localisation. La seconde étape consistera à étudier sa vulnérabilité vis-à-vis à de perturbations (désynchronisations, attaques de type dénis de service reposant sur le brouillage du signal et/ou l'utilisation de faux signaux). Finalement des contremesures (redondance ancre/tag, code correcteur d'erreur, authentification des signaux, facteur d'étalement) permettant de détecter ces attaques et/ou de rendre robuste le système à ces attaques devront être développées et validées sur l'environnement de test. Le coût énergétique de ces contremesures devra également être quantifié afin de pouvoir évaluer leur impact sur l'autonomie du système.

(I) Développement et attaques de brique d'authentification pour l'IoT

Encadrants : Rahma BEN FRAJ, Vincent BEROULLE

Contact : benfrajrahma@gmail.com, vincent.beroulle@lcis.grenoble-inp.fr

Mots clés : RFID, VHDL, FPGA, attaque SCA, attaque EMA, attaque DPA, protocoles d'authentification, protocole d'authentification Gossamer

Contexte : D'ici 2020, il y aura plus de 50 milliards d'objets connectés sur terre. L'interconnexion de ces objets connectés avec le web crée l'internet des objets : nous sommes alors à l'aube de ce que certains qualifient de "4ème révolution industrielle". Dans ce contexte, le développement des moyens de transmission sans fils dont la technologie RFID UHF est devenu un élément décisif. En effet, la technologie RFID UHF fait partie des objets indoor, qui constituent la majorité des objets connectés. Elle permet d'écrire et de lire des informations sur des étiquettes électroniques à très faible coût. Un système RFID se compose de puces électroniques (équipées d'une antenne), de lecteurs et d'un middleware. En RFID UHF, la portée des tags RFID de quelques mètres et les débits de communication importants rajoutent une dimension supplémentaire au problème de sécurité. En effet, à cause des ondes radios, les données dans un tag peuvent être piratées et lues à une certaine distance. Aucun contact visuel direct n'est nécessaire, pas plus qu'une intervention active de la personne concernée. Cela signifie que le traitement des données peut avoir lieu sans que la personne concernée ne le sache. Ainsi, la technologie RFID est accusée de porter atteinte à la vie privée des personnes et à la confidentialité des données personnelles. Authentifier fortement les objets est devenu donc un besoin crucial. Pour cela, nous avons choisi le protocole d'authentification ultraléger 'Gossamer' car il est le plus efficace et le plus sécurisé dans la famille des protocoles ultralégers et on propose dans ce travail de l'implémenter et de valider sa sécurité.

Objectifs :

- Le premier point consiste à développer et valider le protocole d'authentification Gossamer en VHDL et à l'implémenter sur FPGA.

- Le deuxième point se focalisera sur le développement d'un modèle d'attaque par canaux cachés contre Gosssamer.

- Enfin, il sera nécessaire de procéder à l'évaluation de contremesures contre ces attaques (développement d'une architecture robuste vis à vis des attaques identifiées).

Compétences demandées : Conception d'architecture matérielle numérique, mise en place des attaques sur circuits intégrés, vérification prototypage.

(J) Analyse de vulnérabilité du crypto système léger PRESENT contre les attaques par canaux cachés

Encadrants : NAIJA Yassine, BEROULLE Vincent

Contact : yassine.naija@gmail.com, vincent.beroulle@lcis.grenoble-inp.fr

Les crypto systèmes légers sont de plus en plus utilisés dans les applications RFID (contrôle d'accès, billetteries, etc). Ils peuvent être une solution économique pour sécuriser les composants RFID. PRESENT est l'un des crypto systèmes légers utilisé dans les architectures des tags RFID.

Objectifs du projet :

Les objectifs de ce projet sont d'étudier les fuites d'information en cas d'attaque SCA (attaques par canaux cachés) et de développer des contremesures matérielles pour lutter contre ces attaques sur PRESENT. Deux types d'attaques seront étudiées : DPA (attaque par analyse de la puissance consommée) et EMA (attaque par analyse du rayonnement électromagnétique).

Les attaques en faute sur PRESENT pourront également être étudiées afin de proposer une implémentation robuste vis à vis de ces attaques.

Mots clés : RFID, PRESENT, Attaques par canaux cachés, DPA, EMA, contremesures matérielles, attaques en faute.

Travail demandé :

- Etude bibliographique sur les attaques par canaux cachés (DPA et EMA) et leurs contremesures, et sur le fonctionnement du crypto système PRESENT
- Implémentation de PRESENT avec les contremesures puis vérification de l'efficacité de ces contremesures.
- Optionnel : Etude des attaques en faute sur PRESENT et proposition d'une implémentation robuste vis à vis de ces attaques.

Matériels utilisés :

Logiciel ISE (Xilinx), Plateforme FPGA (SAKURA-G), Oscilloscope 4GHz (640Zi), sonde électromagnétique RF-U5-2 (en cas d'attaque EMA), Banc 2D.

Moyens et réalisations existants :

Implémentation de PRESENT sur FPGA et une première attaque EMA ont été développées.

Compétences : Conception d'architectures sécuriées en VHDL, Traitement du signal (Matlab), Cryptoanalyse.

(K) Traceur GPS LORA

Contact : david.hely@lcis.grenoble-inp.fr

Mots clés : STM32, GPS, réseau LORA, internet des objets

Compétences : programmation embarquée, systèmes de communication, mise en place de serveur

L'objectif du projet est de réaliser un démonstrateur de traceur GPS échangeant sur le réseau LORA. Ce démonstrateur consistera à renvoyer sur un serveur les coordonnées GPS du module (STM32 + GPS) via le réseau LoRa. Il faudra définir et implémenter une gestion dynamique du système afin d'optimiser la consommation du traceur tout en gardant une précisions de localisation suffisante. Par exemple, on pourra modifier les modes Low Power du module depuis le serveur pour augmenter ou diminuer la fréquence d'envoie des coordonnées et ainsi économiser la consommation du module qui sera être autonome.

Ce projet nécessitera la mise en place d'un serveur LORA et le développement du système embarqué constituant le traceur.

Ce projet se fera dans le cadre d'une collaboration avec STMicroelectronics.

(L) Mise en œuvre de la plate-forme AWS Iot

Encadrant : Oum-El-Kheir Aktouf

Contact : Oum-El-Kheir.Aktouf@grenoble-inp.fr

Mots-clés : cloud, capteurs, AWS

Contexte : cloud, AWS, capteurs, données, mesures de performances

Les plates-formes de Cloud sont de plus en plus présentes dans divers domaines d'applications. Leur utilisation est notamment adaptée à la gestion de gros volumes de données, comme celles issues de plusieurs capteurs géographiquement répartis et plus généralement de diverses applications de type IoT (« Internet of Things », ou Internet des objets connectés). On parle alors souvent de « sensor cloud ».

Amazon est une entreprise pionnière dans le domaine du cloud, aussi sa plate-forme phare AWS intègre des fonctionnalités permettant la communication avec les objets connectés, en particulier (cf documentation Amazon) :

- Communication sécurisée bidirectionnelle entre les objets connectés et la plate-forme AWS,
- Collecte des données à partir de plusieurs équipements répartis et analyse de ces données,
- Fourniture aux utilisateurs des fonctionnalités leur permettant de contrôler les équipements distants au moyen de leurs téléphones portables et tablettes,
- etc.

L'objectif de ce projet est de mettre en œuvre cette plate-forme, appelée AWS-IoT, et de développer un démonstrateur illustrant son utilisation avec un ensemble de capteurs (cours de 4A). Si le temps le permet, des mesures de performances pourront être effectuées, notamment sur les aspects communication avec les capteurs.

(M) Data interpretation of a Crazyflie quadcopter platform

Thinh Nguyen – D222, ngoc-thinh.nguyen@lcis.grenoble-inp.fr **Ionela Prodan** – D223, ionela.prodan@lcis.grenoble-inp.fr

Project topic

The platform is composed from an aerial unit (the Crazyflie) and a host which sends/receives data through a dedicated USB radio dongle (the Crazyradio). The host platform can be either a Linux or Windows PC or an embedded system like Raspberry Pi or smartpone (in which case the communication is done via Bluetooth LE protocol). The Crazyflie receives references from the ground and follows them in low-lovel control loops which are implemented on the embedded CPU installed on it. These references can be provided either manually (via joystick controllers) or as the result of computations on the host platform.

The project will be focused on the following issues (any other ideas and innovative directions are strongly encouraged):

- First of all, it is important to understand the platform and its capabilities (Crazyflie http://www. bitcraze.se/crazyflie/). Other components can be added during the project execution (e.g., cam- eras for position recognition and the like).
- Receive, filter and plot the angles (all the data, in general) received from the Crazyflie on real time with Matlab and compare the results with the built-in interface.
- Apply suitable PI, PID and also optimization-based control techniques for efficiently acomplish some specific tasks like, trajectory tracking, path following, area coverage, formation control and the like.
- Provide Matlab/Simulink and/or C/C++ simulations.
- Experimental results on the actual UAV system should be a priority.

Prerequisites

At the start of this project the student has to be:

familiar with Matlab programming environment, knowledge of C, C++ and/or Python (for inter- facing with Quadcopter);familiar with system modeling and control theory;

knowledge of micro-controller implementations and low-level programming;

strongly motivated and with initiative spirit.

References

[Ref. 1] R.W. Beard, T.W. McLain (2012) : Small unmanned aircraft: Theory and practice. Princeton University Press.

[Ref. 2] M. Burger, K.Y. Pettersen (2010) : Smooth transitions between trajectory tracking and path fol- lowing for single vehicles and formations. Estimation and Control of Networked Systems, pp. 115–120.

[Ref. 3] I. Prodan, S. Olaru, F.A.C.C. Fontes, S.-I. Niculescu (2013): A predictive control-based algorithm for path following for autonomous aerial vehicles. The IEEE Multi-Conference on Systems and Control, pp. 1042–1047.