Contribution à l'amélioration de la qualité de service et de la sécurité pour les communications de données en environnement réseau contraint

Nicolas Larrieu

Habilitation à diriger les recherches

Contribution à l'amélioration de la qualité de service et de la sécurité pour les communications de données en environnement réseau contraint

Nicolas LARRIEU

Enseignant- Chercheur

Ecole Nationale de l'Aviation Civile (ENAC)

Laboratoire ENAC/TELECOM
Groupe de recherche **ResCo** (Réseaux de Communication)

Département Science et Ingénierie de la Navigation Aérienne (SINA)
Subdivision Systèmes, Architectures et Réseaux (SAR)

Ecole doctorale EDSYS

Université Paul Sabatier

RESUME

Titre du manuscrit d'HDR : contribution à l'amélioration de la qualité de service (QdS) et de la sécurité pour les communications de données en environnement réseau contraint

Mot clés du travail de recherche : amélioration de la QdS, gestion de la sécurité, lien entre QdS et sécurité, réseaux contraints, communication de données

Ce manuscrit présente les travaux que j'ai mené depuis 2002 sur les thématiques d'amélioration de la Qualité de Service (QdS) et de la sécurité des réseaux dans les environnements réseaux dits contraints. Ces travaux ont été menés successivement au travers de différentes structures. Dans un premier temps, j'ai été doctorant puis ATER au LAAS-CNRS et à l'INSA de Toulouse. J'ai eu l'opportunité d'avoir une expérience de post doctorant à l'étranger pendant cette période au sein du KAIST en Corée du Sud. En 2006, j'ai été recruté par l'ENAC et son laboratoire TELECOM pour exercer les fonctions d'enseignant chercheur. Le fil directeur de ma contribution pour ce mémoire d'habilitation à diriger les recherches est centré sur la notion d'environnement réseau contraint. Un environnement réseau contraint dispose par définition d'un niveau limité de ressources (de calcul, réseau ou énergétique) pour rendre un service à ses usagers. Dans ce manuscrit nous nous intéresserons en particulier à l'optimisation de l'utilisation des ressources réseaux : pour cela, les paramètres de QdS tels que la "capacité" ou encore le "délai d'acheminement" des liens réseaux considérés seront déterminant pour l'optimisation de l'utilisation des ressources réseaux. Néanmoins, il est important de noter que nous ne considérons pas spécifiquement la problématique de l'optimisation de la gestion de l'énergie dans cet environnement. Le contexte d'application des réseaux contraints est très vaste. Ainsi, nous nous intéresserons au travers de ce manuscrit aux réseaux mobiles qui peuvent intégrer une ou plusieurs liaisons sans fil (satellite, Wifi, Wimax) qui, par construction, offrent un niveau de service plus faible qu'un réseau classique filaire lorsqu'on considère les paramètres traditionnels d'estimation de la QdS : débit, délai ou encore taux de perte. Nous verrons en particulier comment différentes solutions novatrices ont été proposées par l'intermédiaire des travaux que nous avons menés afin de pouvoir optimiser l'utilisation des ressources réseaux dans ce contexte et élever le niveau de robustesse offert par ce dernier.

TABLES DES MATIERES

TABLE DES ILLUSTRATIONS

LISTE DES TABLEAUX

INTRODUCTION

Ce mémoire d'habilitation à diriger les recherches (HDR) présente les travaux que j'ai menés depuis 2002 sur les thématiques d'amélioration de la Qualité de Service (QdS) et de la sécurité des réseaux dans les environnements réseaux dits contraints.

Ces travaux ont été menés successivement au travers de différentes structures. Dans un premier temps, j'ai été doctorant puis ATER au LAAS-CNRS et à l'INSA de Toulouse. J'ai eu l'opportunité d'avoir une expérience de post doctorant à l'étranger pendant cette période au sein du KAIST en Corée du Sud. En 2006, j'ai été recruté par l'ENAC et son laboratoire TELECOM pour exercer les fonctions d'enseignant chercheur.

Un environnement **réseau contraint** dispose par définition d'un niveau limité de ressources (de calcul, réseau ou énergétique) pour rendre un service à ses usagers. Dans ce manuscrit nous nous intéresserons en particulier à l'optimisation de l'utilisation des ressources réseaux : pour cela, les paramètres de QdS tels que la "capacité" ou encore le "délai d'acheminement" des liens réseaux considérés seront déterminant pour l'optimisation de l'utilisation des ressources réseaux. Néanmoins, il est important de noter que nous ne considérons pas spécifiquement la problématique de l'optimisation de la gestion de l'énergie dans cet environnement. Un grand nombre de réseaux rentrent dans le cadre des réseaux dits contraints. Nous nous intéresserons au travers de ce manuscrit aux réseaux mobiles qui peuvent intégrer une ou plusieurs liaisons sans fil (satellite, Wifi, Wimax) qui, par construction, offrent un niveau de service plus faible qu'un réseau classique filaire lorsqu'on considère les paramètres traditionnels d'estimation de la QdS : débit, délai ou encore taux de perte.

Dans un premier chapitre, je présenterai mon parcours académique au travers d'un curriculum vitae détaillé. Ensuite, je m'attacherai au cours d'un deuxième chapitre à synthétiser les contributions en matière de recherche que j'ai pu mener dans le domaine des réseaux de communication de données contraints. J'aborderai également les partenariats que j'ai pu établir ainsi que les différents encadrements que j'ai réalisés dans ce cadre. Le troisième chapitre présentera les activités administratives et collectives que j'ai menées en tant qu'enseignant-chercheur depuis 2002 dans mes différents établissements d'appartenance. Enfin, le quatrième chapitre résumera les différentes activités d'enseignement que j'ai dispensées en parallèle de mes activités de recherche au sein de l'INSA de Toulouse et de l'ENAC. L'ensemble des publications que j'ai rédigées dans le cadre de ces activités de recherche est listé dans le chapitre 6 présent à la fin de ce manuscrit.

CHAPITRE 1- CURRICULUM VITAE DETAILLE

ENSEIGNANT-CHERCHEUR DANS LE DOMAINE DES RESEAUX DE COMMUNICATION

Date et lieu de naissance : 21 avril 1979 à Auch (France)
Nationalité: Française
Situation familiale : Pacsé

Adresse personnelle :
4 rue Georges BRASSENS
31320 CASTANET TOLOSAN
Mob : (+33) 628 070 519
Email : nicolas.larrieu@enac.fr
Web : www.nicolas-larrieu.com

SITUATION ACTUELLE

- **Qualifié** pour les **sections 27 et 61** du CNU depuis **février 2006**, qualification renouvelée en **février 2010** puis **février 2014** (dossier en cours d'étude) pour ces deux sections.

- **Enseignant-chercheur** dans le **domaine des réseaux de communication** à l'**Ecole Nationale de l'Aviation Civile (ENAC - Toulouse),** département **Science et Ingénierie de la Navigation Aérienne** (SINA).

- **Activités de recherche** réalisées dans le cadre **du laboratoire TELECOM et le groupe de recherche Réseaux de Communication** (ResCo) au sein de l'ENAC.

ACTIVITES ET RESPONSABILITES A L'ENAC DEPUIS 2006

Activités de recherche :

- **Co-directeur de thèse** de Slim Ben Mahmoud (octobre 2008-février 2012) et dans ce cadre **contribution au projet FAST** (24 mois à partir de janvier 2009 – label Aerospace Valley) pour les activités réseaux et sécurité.

- **Responsable** de la **collaboration Thalès/Enac** pour le projet « **MILSAVION** » sous couvert de la convention cadre THAVENAC : cette collaboration a permis notamment de financer les travaux d'Antoine VARET pour la thèse qui a été soutenue au sein du laboratoire TELECOM le 1er octobre 2013 ;
  - Dans ce contexte j'ai été **responsable de l'encadrement de la thèse d'Antoine VARET** pour la période septembre 2010 – septembre 2013 dont l'objectif était la conception, la mise en œuvre et la validation d'un routeur embarqué de nouvelle génération pour les communications aéronautiques.

- **Co-encadrement de thèse d'Ouns Bouachir** depuis septembre 2011 pour les activités de définition d'une architecture de communication pour les réseaux ad hoc : thèse financée dans le cadre du projet européen D3COS.

- **Directeur de thèse de Jean Aimé Maxa** dans le cadre d'une bourse de thèse CIFRE avec l'entreprise DELAIR TECH (dérogation d'encadrement accordée par

l'Université de Toulouse) pour les activités de définition d'une architecture de communication sécurisée pour les réseaux de drones. Ce travail a débuté le 1er novembre 2013.

- **Encadrement de stage niveau M2R :** 4 étudiants (INSA Toulouse, UPS Toulouse, Université Paris Descartes et ENSEEIHT).

- **Encadrement de stage niveau ingénieur :** 2 étudiants (INSA Toulouse et ENAC Toulouse).

- **Responsable** pour le laboratoire TELECOM des **activités de recherche** en réseaux menées en partenariat avec la DSNA-DTI pour le projet européen **SESAR** ;
  - Dans ce contexte je suis **responsable de l'activité de recherche « security »** qui se concrétise au travers des **Work Packages (WPs) SESAR 15.2.4 et 15.2.7 ;**
  - Ce partenariat me permet de **coordonner le postdoc** de Slim Ben Mahmoud qui a débuté en mars 2012 et a été renouvelé en septembre 2013 pour une nouvelle période de 24 **mois au sein du WP 15.2.4 SESAR**.

- **Relecteur pour les revues suivantes** : IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Parallel and Distributed Systems, Compuper Communications Journal, Elsevier Ad Hoc Networks Journal, Techniques et Sciences Informatiques.

- **Relecteur pour les conférences suivantes** : Workshop on Protocols for Fast Long-Distance Networks, Workshop on Quality of Future Internet Services, Workshop on Multimedia Interactive Protocols and Systems, International Conference on Internet & Information Technology in Modern Organizations.

Activités d'enseignement :

- **Environ 200 h d'enseignement par an** entre septembre 2006 et juin 2013, à l'ENAC **en cycle ingénieur** (1ère et 3ème année ingénieur IENAC, 2ème et 3ème année ingénieur IESSA), **master spécialisés** (master « Cooperative Avionics » et « Air Traffic Management ») et **formations continues** pour le personnel de l'aviation civile (ingénieur IESSA en poste dans la DGAC).

Responsabilités collectives :

- **Co-organisateur du workshop WAS'COM 2014** : IEEE Workshop on Adaptive Techniques for Communication Networks.

- **Membre du groupe de travail EUROCAE WG 82** : « new air-ground datalink technologies ».

- **Enseignant référent (définition, mise en place et développement)** des activités d'enseignement dans le domaine de la **« sécurité des réseaux »** pour l'ENAC (cursus ingénieur IENAC et IESSA).

- **Responsable** des **stages de formation continue** (gestionnaire de ressources pédagogiques) NARCI, SECRE et SECRE++.

- **Représentant suppléant au Conseil des Etudes** de l'ENAC depuis 2010.

DIPLOMES ET QUALIFICATIONS

- *Février 2014 :* **renouvellement de la qualification** (dossier de qualification en cours d'étude par les rapporteurs des différentes CNU) **aux fonctions de Maître de Conférences** pour les *sections CNU 27 et 61***.**

- *Février 2010 :* **renouvellement de la qualification aux fonctions de Maître de Conférences** pour les *sections CNU 27 et 61***.**

- *Février 2006 :* **qualifié aux fonctions de Maître de Conférences** pour les *sections CNU 27 et 61***.**

- *Juillet 2005 :* diplômé de l'**INSA** de Toulouse avec un **doctorat en Informatique**, spécialité **Réseaux et Télécommunications** - *Mention « très honorable ».*

  - **Titre : « Contrôle de congestion et gestion du trafic à partir de mesures pour l'optimisation de la QdS dans l'Internet »**
  - **Etablissement ayant délivré le diplôme :**
    - INSA de Toulouse
    - Ecole Doctorale Informatique et Télécommunications
    - Spécialité : Réseaux Informatiques
  - **Laboratoire où a été préparée la thèse :** LAAS-CNRS (Laboratoire d'Analyse et d'Architecture des Systèmes – Centre National pour la Recherche Scientifique)
  - **Mention :** très honorable
  - **Directeur de Thèse :** OWEZARSKI Philippe – Chargé de Recherche CNRS au LAAS (titulaire d'une dérogation de l'INSA permettant l'encadrement à 100 % d'un doctorant)
  - **JURY**

    - *Président :* FESTOR Olivier - Directeur de Recherche INRIA au LORIA *(Section 27 CNU)*

    - *Rapporteurs :* FDIDA Serge - Professeur à l'université Paris 6 *(Section 27 CNU)*
      LEDUC Guy - Professeur à l'université de Liège (Belgique)

    - *Examinateurs :* CHASSOT Christophe – Professeur à l'INSA de Toulouse *(Section 61 CNU)*
      GUILLEMIN Fabrice - Ingénieur R&D à France Télécom Lannion
      OWEZARSKI Philippe – Chargé de Recherche CNRS au LAAS-CNRS (*Section 7 CNRS)*

- *Septembre 2002 :* diplômé de l'**INP** (Institut National Polytechnique) de Toulouse avec un **D.E.A.** spécialité **Réseaux et Télécommunications** – *Mention TB*.
  - *Responsable du mémoire :* Philippe OWEZARSKI.
  - *Sujet du mémoire :* « Métrologie des réseaux IP : modélisation de la qualité de service, caractérisation et analyse ».

- *Juin 2002 :* diplômé de l'**INSA** de Toulouse avec un **diplôme d'ingénieur**, département **Génie Electrique et Informatique,** orientation **Génie Industriel et Informatique**, spécialité **Réseaux et Télécommunications** – *Major de promotion*.
  - *Responsable du stage d'ingénieur :* Philippe OWEZARSKI.
  - *Sujet du stage d'ingénieur :* « Métrologie des réseaux IP : développement de nouveaux outils pour caractériser, analyser et rejouer le trafic réseau ».

- *Septembre 1999 – Juin 2002 :* **cycle ingénieur** à l'**INSA** de Toulouse, département **Génie Electrique et Informatique,** orientation **Génie Industriel et Informatique**, spécialité **Réseaux et Télécommunications**.

- *Septembre 1997 – Juin 1999 :* **DEUG MIAS** (Mathématiques et Informatique Appliquées aux Sciences) à l'**Université Paul Sabatier de Toulouse III**.

- *Juin 1997 :* **Baccalauréat S** option mathématique obtenu au lycée Bossuet à Condom (Gers) – *Mention AB.*

FONCTIONS ASSUREES

- *Depuis Septembre 2006 :* **enseignant-chercheur[1] en réseaux informatiques** à **l'ENAC** de Toulouse, **département SINA** ; activités de recherche réalisées dans le cadre du **groupe de recherche ResCo du laboratoire TELECOM** au sein de l'ENAC.

- *Mars 2006 – Août 2006 :* **ATER** à l'**INSA** (Institut National des Sciences Appliquées) de Toulouse dans le département « **Génie Electrique et Informatique** », poste d'ATER complet avec une charge de 128 H eq. TD sur les 6 mois de contrat.

- *Septembre 2005 – Février 2006 :* **séjour post-doctoral** au **KAIST** (Corée) dans le « Department of **Electronical Engineering Computer Science**, Division of **Computer Science** », équipe du **Professeur Sue B. MOON**.

- *Octobre 2002 - Août 2005 :*
  - **Doctorant** au **L.A.A.S.** (Laboratoire d'Analyse et d'Architecture des Systèmes) - **C.N.R.S.** (Centre National pour la Recherche Scientifique) dans le groupe de recherche « Outils et Logiciels pour la Communication ».
  - **Moniteur** à **l'INSA de Toulouse** dans le département « Génie Electrique et Informatique », charge d'enseignement de 192 H eq. TD délivrée sur les 3 ans de monitorat.

- *Mars 2002 – Septembre 2002 :* **stagiaire** de **DEA** au **LAAS-CNRS** dans le groupe OLC sur le sujet : « Métrologie des réseaux Internet : modélisation de la qualité de service, caractérisation et analyse ».

- *Juin 2001 – Août 2001 :* **stagiaire ingénieur (4ème année INSA)** au **LAAS-CNRS** dans le groupe OLC ; travail de recherche et réalisation logicielle sur le sujet : « Supervision active non intrusive dans le réseau Internet pour l'ingénierie coopérative ».

[1] Contrat à durée indéterminé (selon le statut du décret de la fonction publique n°84-16) pour le ministère des transports

CHAPITRE 2- ACTIVITE EN MATIERE DE RECHERCHE

1- INTRODUCTION

Dans ce manuscrit nous allons nous intéresser aux mécanismes permettant d'améliorer le niveau de QdS (Qualité de Service) mais aussi de sécurité qui permettent de rendre plus performantes les communications de données échangées en environnement réseau contraint. Dans un premier temps, il est donc nécessaire de définir le concept de réseau contraint.

1.1- CONCEPT DE RESEAU DE COMMUNICATION CONTRAINT

Comme nous l'avons résumé dans l'introduction de ce manuscrit, un environnement **réseau contraint** dispose par définition d'un niveau limité de ressources (de calcul, réseau ou énergétique) pour rendre un service à ses usagers. Dans ce manuscrit nous nous intéresserons en particulier à l'optimisation de l'utilisation des ressources réseaux : pour cela, les paramètres de QdS tels que la "capacité" ou encore le "délai d'acheminement" des liens réseaux considérés seront déterminant pour l'optimisation de l'utilisation des ressources réseaux. Néanmoins, il est important de noter que nous ne considérons pas spécifiquement la problématique de l'optimisation de la gestion de l'énergie dans cet environnement. D'autre part, un grand nombre de réseaux rentre dans le cadre des réseaux dits contraints. Nous nous intéresserons au travers de ce manuscrit aux réseaux mobiles qui peuvent intégrer une ou plusieurs liaisons sans fil (satellite, Wifi, Wimax) qui, par construction, offrent un niveau de service plus faible qu'un réseau classique filaire lorsqu'on considère les paramètres traditionnels d'estimation de la QdS : débit, délai ou encore taux de perte.

Nous nous sommes intéressés à différents types de réseaux sans fil possédant les caractéristiques des réseaux contraints ; il s'agit des réseaux aéronautiques et des réseaux de flottes de drones. Dans la section qui suit, nous résumons les enjeux actuels en matière de recherche de ces environnements pour l'optimisation de la QdS et la gestion de la sécurité de leurs communications.

1.2- CONTEXTE D'AMELIORATION DES COMMUNICATIONS DE DONNEES EN ENVIRONNEMENT CONTRAINT

1.2.1- Le contexte aéronautique

- **Mutualisation d'un lien unique de communication**

Un des besoins de l'aéronautique concerne le multiplexage des flux sol-bord : actuellement, les réseaux avioniques sont fermés et ne communiquent pas entre eux. Les moyens de communication sol/bord sont dupliqués pour chaque domaine réseau s'étendant de l'avion au sol, garantissant ainsi la disponibilité du lien et dédiant toute la capacité au domaine utilisant le lien. Cela entraîne une augmentation du nombre de liens et d'équipements (et donc des coûts associés). La Figure 1 récapitule les différents types et moyens de communication qui leur sont généralement associés.

Une solution consiste à mutualiser la liaison sol/bord, quand les moyens techniques et la capacité du lien le permettent. La liaison transporte alors simultanément plusieurs flux issus de domaines différents. On parle alors de multiplexage des flux de données sur un lien. Le multiplexage est assuré par le routeur lorsque les données provenant d'interfaces réseaux différentes sont envoyées vers l'équipement de télécommunication embarqué, via une même interface réseau du routeur. Le démultiplexage, opération inverse du multiplexage, est alors effectué par un ou plusieurs routeurs au sol.

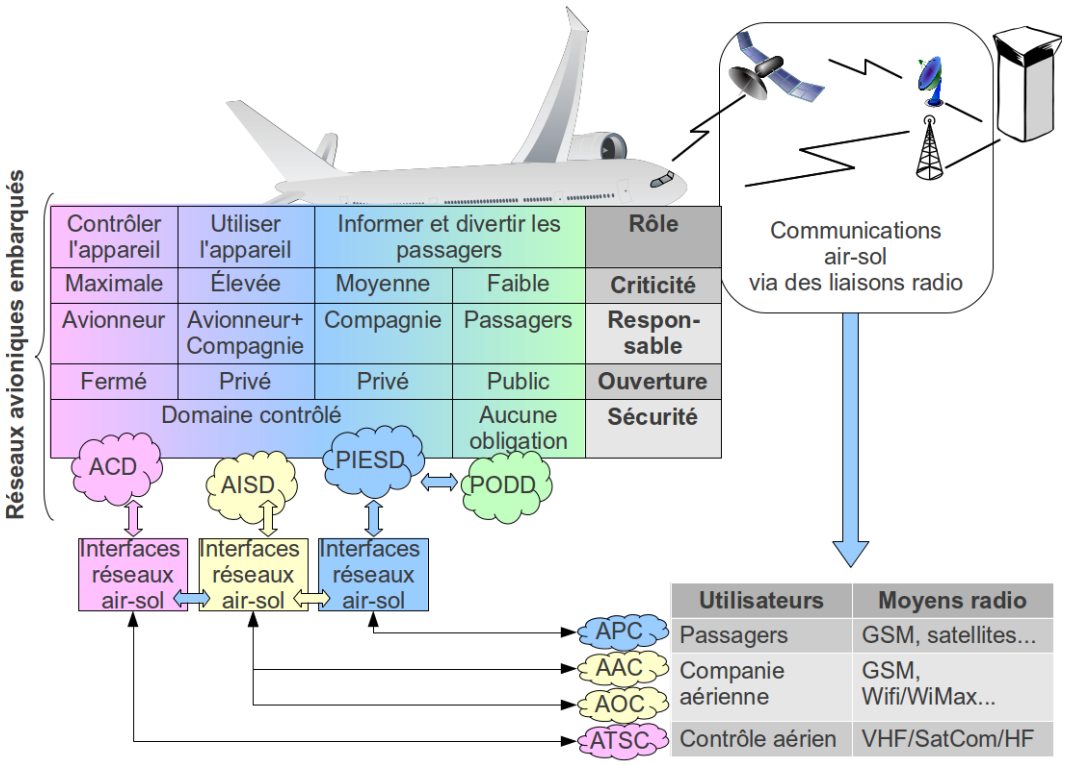


Figure 1 : réseaux avioniques et aéronautiques

La Figure 2 présente un exemple d'utilisation de la mutualisation air-sol. Un routeur embarqué est connecté physiquement à trois réseaux avioniques, il dispose d'un lien unique avec le sol pour acheminer les données des trois réseaux. Au sol, un premier routeur sépare les données non critiques des passagers et assure la connectivité avec un Fournisseur de services d'Accès à l'Internet (FAI). Les flux avioniques dédiés à l'exploitation commerciale de l'appareil sont transmis à un second routeur au sol qui démultiplexe les flux et les routes vers les équipements adéquats de la compagnie aérienne exploitant l'avion. L'ARINC 811 *(ARINC811, 2005)* et son complément l'ARINC 821 *(ARINC821, 2008)* qui approfondit les problématiques de sécurité préconisent l'exploitation de tunnels pour transporter les données en maintenant la ségrégation, comme présenté Figure 2. Ces tunnels doivent être sécurisés en raison de la sensibilité potentielle des informations transportées : données commerciales, personnelles...

- **Traitement conjoint des approches « security » et « safety »**

Le développement des systèmes embarqués à bord des aéronefs est fortement contraint, que ce soit en terme de sûreté de fonctionnement qu'en terme de sécurité. En aéronautique, on parle de « safety » pour la sécurité ou encore la sûreté de fonctionnement des systèmes aéronautiques, c'est-à-dire les propriétés intrinsèques des systèmes leur permettant de « résister » aux dysfonctionnements. Le terme « security » désigne la sûreté des systèmes aéronautiques, c'est-à-dire les protections contre les menaces volontaires (attaques de pirates...). Nous emploierons par suite les termes techniques anglais « safety »

et « security » afin de ne pas les confondre avec les définitions françaises de sécurité et de sûreté.

Le domaine avionique est depuis toujours fortement contraint en terme de « safety ». Un dysfonctionnement général de l'appareil peut en effet conduire à sa destruction partielle ou totale, des vies humaines sont alors menacées. Différents standards aéronautiques spécifient les contraintes de « safety » devant être respectées afin que l'appareil soit autorisé à voler. Les logiciels avioniques embarqués critiques, tels que les pilotes automatiques par exemple, sont ainsi soumis au standard RTCA[2] DO-178B *(DO-178B, 1992)*.

[2] RTCA : Radio Technical Commission for Aeronautics

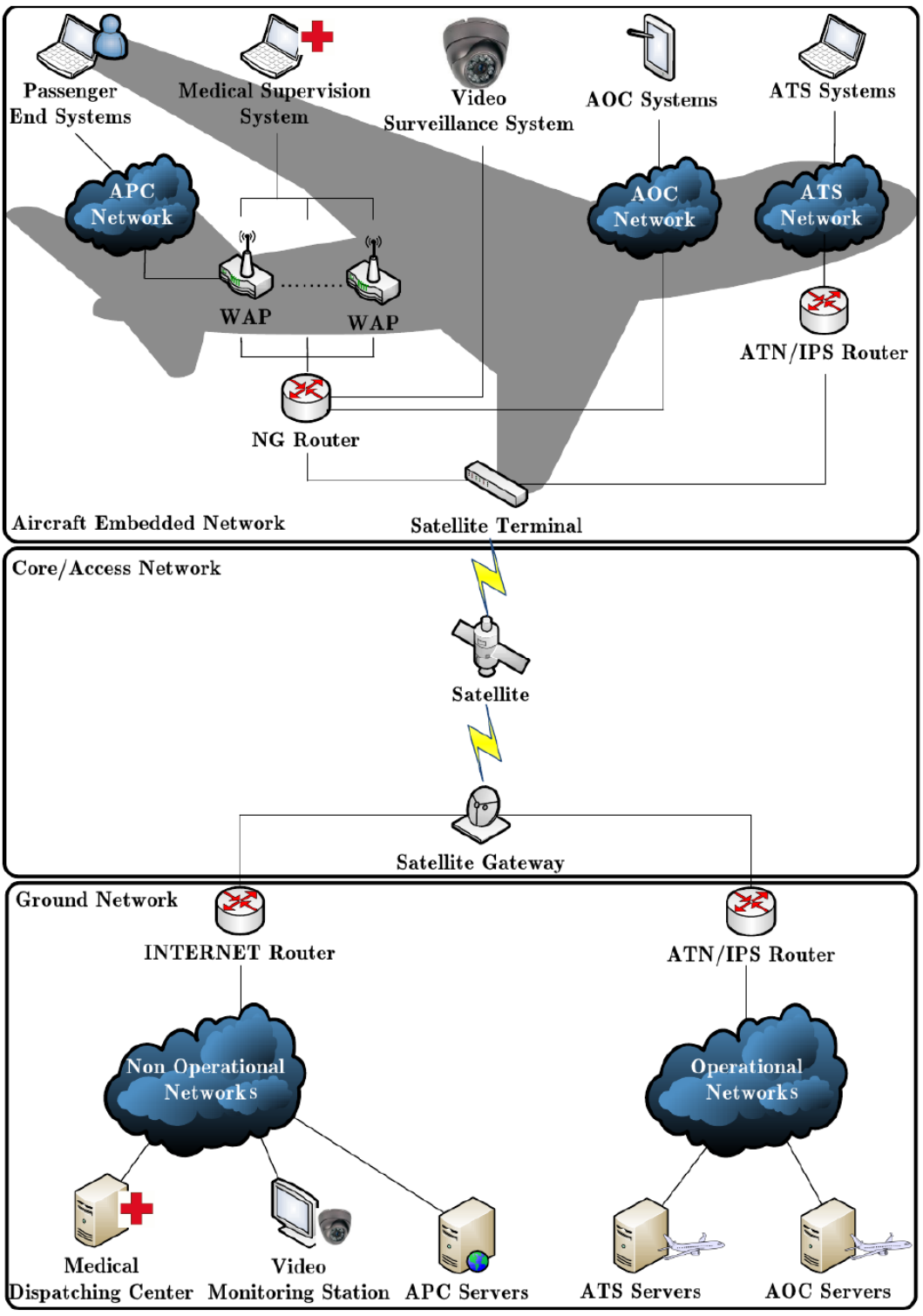


Figure 2 : exemple de mutualisation des communications au travers d'un lien satellite unique

Le DO-178B définit 5 niveaux d'assurance concernant le développement des logiciels avioniques, appelés Design Assurance Level ou DAL. Le DAL-A est le niveau le plus exigeant en termes de contraintes et est utilisé pour les applications critiques dont les dysfonctionnements pourraient être catastrophiques, tandis que le DAL-E est un niveau non contraignant réservé aux applications ne pouvant pas avoir d'incidence sur la « safety » de l'appareil. Pour être embarqué et utilisé dans l'appareil, un logiciel doit être auparavant évalué suivant des critères de « safety » ; cette vérification appelée « certification » est

effectuée par des organismes nationaux indépendants des développeurs. En France, la DGAC[3] est l'organisme de certification pour les systèmes aéronautiques.

A l'origine, seule la « safety » était prise en compte de manière approfondie par les avionneurs. Ceux-ci considéraient que la complexité des systèmes embarqués et la fermeture des réseaux avioniques garantissaient leur « security ». Depuis les attentats du 11 septembre 2001, la « security » est désormais devenue une préoccupation majeure pour la conception des systèmes et introduit de nouvelles contraintes et de nouvelles pratiques dans le monde aéronautique. Les produits sensibles doivent être validés d'un point de vue sécuritaire, cette validation de la « security » est appelée « évaluation ». Les exigences de « security » peuvent être regroupées dans des «paquetages» d'exigences permettant leur « évaluation » dans le produit final. Il existe ainsi 7 paquetages constitués uniquement d'exigences d'assurance et appelés «Niveaux d'assurance d'évaluation» («Evaluation Assurance Level» ou EAL). Ces paquetages d'exigences sont numérotés de 1 à 7. L'EAL-2 reprend l'ensemble EAL-1 et y ajoute des exigences supplémentaires. Il en est de même jusqu'à l'EAL-7, le plus haut niveau d'assurance de sécurité que peut recevoir un produit dans la nomenclature CC ITSEC «Common Criteria for Information Technology Security Evaluation». Cette norme ISO référencée sous le numéro ISO CEI 15408, souvent appelée en abrégé les «Critères Communs» ou « CC », permet d'évaluer un système complet vis-à-vis d'exigences de sécurité. Elle est publiée en quatre parties : *(cc1, 2009 ; cc2, 2009 ; cc3, 2009 & cc4, 2009).*

Cependant, malgré l'existence de ces deux standards (DAL vs EAL), les processus de certification (pour garantir la « safety » du système) et d'évaluation (garantissant sa « security ») sont actuellement traités de manière parallèle et indépendante, certaines vérifications similaires étant ainsi effectuées deux fois. Nous reviendrons sur cet aspect dans la section 2.3 relative à notre contribution sur les approches orientées modèles en aéronautique.

1.2.2- Le contexte UAS (Unmaned Aerial Systems)

- **Les principaux types de réseaux sans fil**

Un réseau sans fil ad hoc (Mobile ad hoc Network - MANET) est une collection de nœuds mobiles qui communiquent les uns avec les autres sans avoir recours à une infrastructure préexistante. Il se forme de manière non planifiée et imprévisible. Il constitue un système autonome dynamique qui peut avoir plusieurs hôtes et interfaces de communication. Ces derniers communiquent avec des liaisons sans fil, sans l'utilisation d'une infrastructure fixe et sans administration centralisée. Les nœuds sont libres de bouger aléatoirement sans contraintes et s'organisent arbitrairement. Les nœuds étant mobiles et communicant sans fil, ils peuvent à tout moment quitter ou joindre le réseau. De fait, à mesure que les connexions entre les nœuds se créent et se détruisent, la topologie du réseau évolue de façon dynamique. Ainsi, les chemins empruntés par les paquets peuvent rapidement être modifiés au cours du temps *(Corson & Macker, 1999)*.

Les réseaux VANETs[4] constituent un nouvel aspect des réseaux ad hoc mobiles MANET. Ils apparaissent depuis quelques années comme un moyen effectif d'améliorer la sécurité routière. Ils permettent d'établir des communications entre véhicules ou avec une infrastructure située aux bords des routes. Comparativement à un réseau ad hoc classique, les réseaux VANET sont caractérisés par une forte mobilité des nœuds due à la vitesse des véhicules et rendant la topologie du réseau fortement dynamique *(Liu & He, 2010)*.

[3] DGAC: Direction Générale de l'Aviation Civile
[4] VANETs : réseaux ad hoc véhiculaires (Vehicular Ad hoc Network)

La problématique de la gestion de ces environnements fortement contraints par définition va être présentée dans la suite. La question du routage dans ce type d'environnement doit être considérée comme un enjeu particulièrement important. Elle fera l'objet d'un paragraphe spécifique dans la suite de cette section. De plus, il nous semble important de considérer également les problématiques de gestion de la qualité de service dans ces environnements ainsi que la sécurisation des échanges, c'est la raison pour laquelle des sections spécifiques sont dédiées à ces deux enjeux à la fin de cette section.

- **Réseaux ad hoc à base d'UAVs (UAANET – UAv Ad hoc Network)**

Un réseau UAANET est un réseau ad hoc entre un groupe d'UAVs. Nous considérons dans ce travail les UAVs dit « légers » (ou mini-drônes). Un exemple des caractéristiques d'un UAV commercial (société Delair Tech) sera donné plus loin dans ce chapitre (cf. Tableau 7). Ils possèdent une petite taille, un faible poids et vole à une altitude proche du sol *(Bento, 2008)*. Les MANET qui incluent traditionnellement les réseaux d'UAV, possèdent des limites en termes de capacité de transfert, sécurité ou encore consommation d'énergie. La mobilité des nœuds du réseau rajoute de la complexité à ce type de réseau. En effet, les UAVs sont libres de se déplacer arbitrairement (dans la limite des trajectoires planifiées pour leurs opérations). Dès lors, la topologie du réseau peut changer de façon aléatoire et parfois très rapidement ce qui peut induire des perturbations dans la connectivité du réseau à cause des modifications fréquentes des liens entre les différents nœuds du réseau. De plus, l'utilisation de systèmes de communications sans fil induit des problématiques supplémentaires (perturbations par exemple) qui ne sont pas présentes dans les communications filaires.

Si l'on compare les UAANET aux autres types de réseaux MANET : VANET ou encore AANET (Aeronautical Ad hoc network), ils possèdent des particularités au niveau des spécificités de leur environnement. En effet, les UAANET doivent prendre en compte des besoins nouveaux. Par exemple, un UAV a de très faibles ressources énergétiques si on le compare à un véhicule (VANET) ou un avion (AANET). Ainsi, dans la définition des systèmes pour UAV, il est très important de prendre en compte dès le départ le critère de consommation de l'énergie afin de rendre la solution proposée optimale pour l'environnement final.

Une autre différence porte sur les trajectoires suivies par les nœuds d'un réseau UAANET. Pour un VANET l'ensemble des nœuds suivent la même trajectoire et se déplace dans le même sens. Ceci a pour conséquence de créer moins de perturbation dans le réseau. Les modèles de mobilité utilisés dans les VANET ne peuvent donc pas être utilisés tel quel pour les UAANET. En effet, dans un UAANET, un UAV a la possibilité de se déplacer librement en fonction des besoins de la mission qu'il s'est vu assigner.

De plus, les UAANET permettent à leurs entités (UAV) d'avoir un comportement semi autonome voire complètement autonome. Pour cela, ils doivent échanger des messages de façon fiable étant donné que ces informations peuvent être utilisées pour réaliser un processus de décision propre et local à chaque UAV. C'est une grosse différence avec d'autres types de réseaux ad hoc sans fil tel que les réseaux de capteurs (WSN pour Wireless Sensor Network) où les informations vont la plupart du temps dans un seul sens : c'est-à-dire du capteur vers la station de contrôle. De plus, les capteurs n'échangent pas d'informations entre eux ce qui n'est pas le cas dans les UAANET.

Ainsi, les UAANET possèdent des particularités (topologie du réseau fortement variable par exemple) que nous devons prendre en compte pour proposer des solutions de gestion de la QdS et de la sécurité adaptées à leur environnement. Dans la suite, nous allons nous attacher à décrire les principaux mécanismes qui sont à l'étude à l'heure actuelle pour les UAANET et dont nous nous sommes inspirés pour présenter une partie des

contributions recherches de ce chapitre. Ces mécanismes s'articulent autour des fonctions de routage, de gestion de la QdS ou encore de la sécurité.

- **Nouveaux mécanismes de routage pour les UAANET**

Il existe plusieurs critères pour la conception et la classification des protocoles de routage dans les réseaux ad hoc : la manière dont les informations de routage sont échangées, quand et comment les routes sont calculées, etc. Ainsi, il est possible de distinguer quatre grandes catégories de protocoles de routage qui sont listées ci-après.

Les protocoles de routage proactifs

Le principe de base des protocoles proactifs est de maintenir à jour les tables de routage en continu. Dans le contexte des réseaux ad hoc, les nœuds peuvent apparaître ou disparaître de manière aléatoire et la topologie même du réseau peut changer. Les tables sont donc maintenues grâce à des paquets de contrôle, et il est possible d'y trouver directement et à tout moment un chemin vers les destinations connues en fonction de divers critères. Parmi les protocoles proactifs les plus étudiés dans la littérature, nous pouvons citer par exemple : DSDV (Destination Sequenced Distance Vector) *(Bhagwat, 1994)* et OLSR (Optimized Link State Routing) *(Jacquet, 2003)*. Dans ce type de mécanisme de routage, chaque nœud diffuse à ces voisins des messages de contrôle par anticipation, pour maintenir les informations des tables de routage à jour.

Les protocoles de routage réactifs

Les protocoles de routage réactifs ou à la demande comme par exemple AODV (Ad Hoc On Demand Distance Vector) *(Chakeres et al., 2004)* ou DSR (Dynamic Source Routing) *(Maltz, 1996)*, créent et maintiennent les routes selon les besoins des agents présents dans le réseau. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information spécifique et inconnue au préalable. Pour cela, ils nécessitent de transmettre des données supplémentaires à cause des trafics de signalisation générés ce qui peut avoir pour conséquence d'augmenter le délai de transmission dans le réseau *(Royer, 1999)*. Dans ce type de mécanisme de routage, chaque nœud source diffuse des requêtes de route pour chercher son destinataire mais ces échanges sont réalisés uniquement à la demande, lorsqu'une route doit être établie.

Les protocoles de routage hybrides

Ils combinent les principes des protocoles proactifs et réactifs. Ils utilisent un protocole proactif, pour connaître le plus proche voisin, ainsi ils disposent des routes immédiatement dans le voisinage. Au-delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques des protocoles réactifs pour chercher des routes. Citons le protocole ZRP (Zone Routing Protocol) *(Haas, 1997)* qui est un des premiers protocoles de routage hybride dédié aux réseaux ad hoc classiques.

Les protocoles de routage géographiques

Les protocoles de routage géographiques ont comme caractéristique commune deux étapes distinctes. Dans la première phase, dite de localisation d'un nœud destinataire, le nœud source détermine la position géographique du nœud destinataire avant d'envoyer des paquets d'information et dans ce cas un service de localisation doit être utilisé. La deuxième phase est l'acheminement ou le routage des paquets vers ce nœud. Dans un protocole de routage géographique, un nœud est supposé aussi connaître sa position géographique en utilisant par exemple les données de positionnement issues du système GPS. Les positions

des voisins sont généralement connues puisque chaque nœud envoie périodiquement sa position à ses voisins immédiats. En d'autres termes, la connaissance du voisinage est périodiquement mise à jour à l'aide de messages échangés entre les nœuds voisins. Quand un nœud ne dispose pas des coordonnées géographiques d'un autre nœud destinataire, il envoie une requête de positionnement au service de localisation en demandant ces informations. Parmi les protocoles de routage géographiques les plus utilisés pour les MANET, nous pouvons citer par exemple GPSR *(Karp, 2000)*, LAR (Location-Aided Routing) *(Vaidya, 1998)* et DREAM (Distance Routing Effect Algorithm for mobility) *(Basagni et al., 1998)*.

Avantages et inconvénients des différentes solutions de routage

A titre de comparaison, les protocoles proactifs n'optimisent pas l'utilisation de la bande passante alors que les protocoles réactifs sont très coûteux en temps de transmission de données à cause des trafics de signalisations générés, ce qui a pour conséquence d'augmenter le délai de transmission des informations utiles. Les protocoles hybrides peuvent cumuler les inconvénients des protocoles réactifs et proactifs : messages de contrôle périodique engendrant un « overhead » ainsi qu'un coût de couverture élevé lors de la procédure de découverte d'une nouvelle route. Pour les protocoles géographiques, la difficulté repose dans la nécessité de disposer d'un système de localisation des nœuds qui n'est pas forcément disponible dans le type de systèmes embarqués utilisés pour les réseaux UAANET.

- **Garantie de la QdS**

La topologie fortement variable d'un réseau MANET peut nécessiter le développement de mécanismes spécifiques de gestion et de garantie de la QdS dans le cadre où les applications qui utilisent ce réseau ont des besoins spécifiques en termes de délai, débit ou de perte qu'un simple service Best Effort ne peut pas garantir. En effet, les modifications topologiques induites par les déplacements des nœuds dans le réseau peuvent fortement pénaliser les performances des mécanismes réseaux traditionnels (i.e. non orientés QdS).

Ainsi, si des solutions comme IntServ *(Braden et al., 1994)* ou DiffServ *(Blake et al., 1998)* existent pour les réseaux filaires, il reste beaucoup de travail à faire dans les réseaux sans fil pour proposer un niveau de performance équivalent en matière de gestion de la QdS. En effet, il existe peu de contributions permettant de faire de la différenciation de service en fonction des besoins utilisateurs ou applicatifs dans ce type d'environnement. Deux propositions principales ont été faites dans le domaine des MANET : INSIGNIA *(Lee & Campbell, 1998)* et SWAN *(Ahn et al., 2002).*

INSIGNIA ("In-band Signalling Support for QoS In Mobile Ad hoc Networks") est la première architecture protocolaire de gestion de la signalisation pour les MANET permettant de fournir de la QdS dans ce type d'environnement. Il s'appuie sur un mécanisme de signalisation « In-Band ». Cette approche utilise les entêtes des paquets IP pour rajouter des informations sur la signalisation de la QdS en même temps que les paquets transportent de l'information. Ces informations de signalisation sont utilisées pour faire les réservations de ressources dans le réseau. Ainsi, INSIGNA en collaboration avec des mécanismes de contrôle d'admission réserve les ressources pour apporter de la QdS au trafic acheminé dans l'environnement MANET en temps réel. Il permet aux paquets prioritaires de spécifier leur besoin de bande passante en ajoutant à chaque paquet IP une option dans l'entête IP. Cette option permet d'établir, de restaurer et d'adapter les ressources entre un couple émetteur et récepteur. INSIGNA nécessite pour fonctionner dans le réseau MANET une modification de l'entête IP pour permettre son déploiement effectif.

Le second modèle proposé pour les MANET pour gérer la QdS est SWAN : « Stateless Wireless Ad hoc Network ». Il s'agit d'une architecture protocolaire de gestion de la QdS avec une approche sans état permettant de fournir de la QdS de bout en bout pour les réseaux ad hoc. Il est capable de traiter deux classes de service différentes : « Best Effort » et « Real Time ». SWAN utilise un mécanisme de contrôle du débit pour les trafics « Best Effort » et un mécanisme de contrôle d'admission chez l'émetteur pour la gestion du trafic temps réel. Le contrôle d'admission est géré par le nœud source après avoir estimé le niveau de ressources réseaux disponibles entre l'émetteur et le récepteur.

D'autres solutions différentes de SWAN et INSIGNIA existent dans la littérature mais elle traite la gestion de la QdS au niveau de la couche MAC. Il est évident que la prise en compte des interférences réseaux ainsi que l'occupation du canal de transmission permet d'augmenter le niveau de performances. Néanmoins, cela nécessite des logiciels (« drivers » des interfaces prenant en compte ces besoins de QdS au niveau MAC) et des matériels réseaux (carte Wifi paramétrable par exemple) qui ne sont pas forcément disponibles sur le marché des mini drones. Un des objectifs de notre travail étant de pouvoir proposer une solution à faible cout déployable sur des systèmes simples et légers, nous n'avons donc pas privilégié cette solution au niveau des contributions que nous présenterons dans la suite de ce chapitre.

- **Axes de sécurisation d'un réseau UAANET**

La flexibilité offerte grâce à l'auto-organisation et aux communications sans fil ou encore la mobilité des nœuds rendent les réseaux ad hoc particulièrement vulnérables à des nouvelles attaques de sécurité. Dans la suite de cette partie, nous présentons une description des principales attaques pour lesquelles ils sont vulnérables.

Les attaques sur les protocoles de routage

Les protocoles de routage sont définis au niveau de la couche réseau, ils servent à étendre la connectivité d'un saut à tous les nœuds dans le réseau. C'est donc à ce niveau que fonctionnent ces derniers ainsi que le mécanisme de retransmission des paquets de données. Un simple détournement du fonctionnement normal de ces protocoles provoque une perturbation des communications, et l'ensemble du réseau peut être bloqué. La sécurité de la couche réseau est donc primordiale dans la mesure où le but du réseau est avant tout de mettre en relation des nœuds et d'acheminer leurs données. L'étude des protocoles de routage présentée dans la littérature montre que de nombreux protocoles existants ne sont pas sécurisés. En effet, Les nœuds de ce réseau sont particulièrement vulnérables aux différentes attaques connues dans les réseaux ad hoc classiques types MANETs ou VANETs. Ces principales attaques sont les suivantes : « Select Forwarding », « Sybil Attack », « Sink Hole » ou encore « Impersonation ».

Select Forwarding

Le routage multi-sauts suppose que tous les nœuds participant au routage acheminent les messages qu'ils reçoivent avec succès. Dans les attaques par transmission sélective (« Select Forwarding »), un nœud refuse de transmettre certains messages et les suppriment. En particulier dans les réseaux de drones l'attaque « Select Forwarding » peut provoquer des pertes de données comme les informations géographiques critiques pour chaque drone si un protocole géographique est utilisé pour le routage des informations. Ce type d'attaque peut aussi porter sur les informations de contrôle échangées entre les drones pour permettre de mener à bien leur mission.

Sybil Attack

Cette attaque se déroule lorsqu'un nœud malicieux présente des identités multiples dans le réseau. Ce type d'attaque a un effet majeur sur les algorithmes de routage géographique qui nécessitent la localisation d'un nœud pour router l'information. Étant donné que l'attaquant peut réaliser l'attaque sur différents nœuds du réseau et ainsi apparaître de façon malicieuse à plusieurs endroits du réseau, la plupart des paquets pourront être routés vers lui ce qui peut lui permettre ensuite de réaliser l'attaque « Select Forwarding ».

Sink Hole

Dans ce cas, le nœud malveillant achemine tout le trafic vers lui afin de contrôler et voler la plupart des données. Avec des mécanismes de routage géographique ou proactif, toutes les données sont diffusées dans le réseau. De ce fait le nœud malveillant peut facilement voler ces données en changeant la direction du trafic vers un autre chemin.

Spoofing ou Impersonation (usurpation d'identité)

Dans cette attaque, l'entité malveillante utilise une fausse identité comme de fausses lettres de créance souvent utilisés dans les MANETs pour se faire passer pour une entité légitime ou pour jouir des privilèges de cette dernière. Cela a pour conséquence de produire un changement dans les routes suivies par les informations, la perte de données ou encore des boucles dans le réseau

Quelques protocoles de routage sécurisés pour MANETs

A partir des différentes attaques identifiées précédemment pour les réseaux MANET, un certain nombre de propositions de mécanismes de routage sécurisés ont été faites dans la littérature. Nous détaillons les plus importantes dans les paragraphes suivants. Le Tableau 1 résume les différentes solutions de sécurité (et les mécanismes de sécurité utilisés) présentées dans cette sous-section.

OLSR sécurisé

Il existe plusieurs extensions de sécurité pour le protocole OLSR qui ont été proposées dans la littérature. Leur point commun réside dans l'utilisation de signature numérique pour assurer l'authentification et l'intégrité des messages de contrôle. Une telle authentification peut être réalisée soit de saut en saut, soit de bout en bout. Dans Secure OLSR, Hafslund et al. *(Hafslund et al., 2004)* ont proposé une approche d'authentification de saut en saut dans laquelle chaque nœud signe les paquets OLSR au fur et à mesure de leur retransmission. Ainsi, à la réception d'un paquet OLSR, un nœud intermédiaire vérifie la signature du nœud précédent, la retire, puis appose sa propre signature. Cependant, la signature assure seulement que le nœud qui a transmis le trafic est bien celui qui a signé le paquet, mais n'apporte aucune garantie sur l'intégrité du paquet original. Ici, les auteurs suggèrent l'utilisation de clés symétriques et d'une fonction de hachage telle que SHA-1 pour la génération des signatures numériques. De manière similaire à Secure OLSR, Adjih et al. ont proposé dans *(Adjih et al., 2003)* une extension de sécurité pour le protocole OLSR basée sur l'utilisation de signatures numériques. Dans leur approche, une signature numérique est associée pour chaque message de contrôle OLSR et non plus à chaque paquet de données OLSR. Ensuite, les auteurs proposent une approche d'authentification de bout en bout selon laquelle un nœud récepteur authentifie le nœud d'origine avec lequel il est amené à échanger de l'information.

ARAN

Sanzgiri et al. *(Sanzgiri et al., 2002)* ont présenté le protocole sécurisé ARAN (Authenticated Routing for Ad hoc Networks) qui prévoit l'utilisation de la cryptographie à clé

publique pour sécuriser la construction des chemins des protocoles réactifs tels qu'AODV. Cette contribution suppose l'existence d'un serveur d'authentification dont le rôle est de gérer la distribution des certificats pour les nœuds autorisés dans le réseau. Chaque nœud doit, au préalable, récupérer un certificat auprès du serveur qui lui servira à signer les messages de contrôle avant de rejoindre le réseau. ARAN offre des services d'authentification, d'intégrité et de non-répudiation. Néanmoins, en termes de sécurité, une limitation vient du fait que dans la phase de maintenance, l'authenticité d'une information de rupture de lien n'est pas vérifiée. Ceci offre l'occasion à un attaquant interne d'agir sur le réseau en envoyant de fausses ruptures pour invalider les chemins. Par conséquent, un déni de service peut apparaitre ce qui peut entraîner une surconsommation de ressources puisque la procédure de recherche de route devra se dérouler à nouveau. Enfin, il utilise la cryptographie à clé publique pour authentifier les nœuds de saut en saut, ce qui entraine des coûts de calcul importants.

SAODV

Zapata et Asokan *(Zapata & Asokan, 2002)* ont proposé une extension de sécurité pour le protocole AODV nommée SAODV (Secure Ad hoc On-Demand Distance Vector Routing). Contrairement à l'extension ARAN pour laquelle les données variables des messages de contrôle sont retirées, l'idée principale de SAODV consiste à faire usage d'une signature numérique (créée par cryptographie à clé publique) pour protéger les données statiques des messages de contrôle, puis de recourir à des chaînes de hachage pour protéger l'intégrité de la partie non statique qu'est le compteur de sauts. Cependant, l'utilisation des chaînes de hachage pour empêcher une entité malveillante d'attaquer le compteur de sauts reste limitée, car même s'il est vrai que des chemins plus courts qu'ils ne le sont en réalité ne peuvent pas être annoncés, rien n'empêche un attaquant d'augmenter le nombre de sauts ou de le laisser inchangé. En outre, dans le cas où plusieurs attaquants sont en collusion, une attaque de type « Wormhole » peut être menée. Par conséquent, l'attaquant parvient à manipuler le compteur de sauts et à raccourcir la longueur d'un chemin, ceci de manière transparente pour les autres nœuds.

SRP

Papadimitratos et Haas *(Papadimitratos & Haas, 2003)* ont proposé SRP (Secure Routing Protocol), une extension de sécurité pour les protocoles de routage réactif à la source, dont en particulier DSR. Cette approche se produit par l'ajout d'une séquence qui permet de sécuriser les messages de recherche d'un chemin entre une source et une destination. Selon cette approche, le nombre d'opérations cryptographiques est énormément réduit puisque seule une authentification des nœuds de bout en bout entre la source et la destination est requise. Plus spécifiquement, ces nœuds utilisent un code d'authentification de message MAC (Message Authentication Code). La destination est capable de détecter toute modification sur les données statiques d'un message de demande de chemin. Du point de vue de la source, le MAC lui permet de vérifier l'intégrité du chemin découvert inclus dans le message sur lequel il porte, et d'en authentifier son origine. En revanche, il présente certains défauts qui limitent son utilisation. Premièrement, SRP ne sécurise pas la phase de maintenance des chemins. Ensuite, il ne permet pas d'empêcher les attaques menées par des nœuds internes et qui portent des changements sur les informations de routage lors de multiples retransmissions. Ceci est dû à l'absence d'authentification des messages de saut en saut.

Différentes versions pour sécuriser GPSR

Dans la littérature, plusieurs extensions de sécurité pour le protocole GPSR ont été proposées *(Samundiswary & Dananjayan, 2010) (Hao & Chao, 2007) (Liu & He, 2010)*. Dans *(Samundiswary & Dananjayan, 2010)*, les auteurs ont proposé une nouvelle extension de

GPSR appelée S-GPSR (Secured Greedy Perimeter Statless Routing Protocol) Ce protocole utilise le système de confiance en conjonction avec les distances géographiques qui sont incorporées dans la table de voisinage pour créer un chemin plus court et plus stable. Cette nouvelle approche S-GPSR, assure l'authentification et l'intégrité par rapport à GPSR non sécurisé. En revanche, il affiche des faiblesses face aux attaquants car cette approche est incapable de détecter tous les nœuds malveillants. Ainsi, elle peut même considérer des nœuds en panne qui ne fonctionnent pas à cause d'un manque d'énergie ou de ressources comme des nœuds malveillants, ceci peut donc engendrer des perturbations au niveau du fonctionnement optimal réseau.

Dans le but de sécuriser et empêcher les attaquants de pénétrer le réseau, les auteurs de *(Hao & Chao, 2007)* ont proposé une solution de cryptographie symétrique pour éviter le « Sybil Attack » (une attaque qui permet aux nœuds malveillants de manipuler et usurper les identités des nœuds illégalement) ainsi que le mécanisme Multi Path Routing pour éviter l'attaque de « Select Forwarding ». Cette nouvelle approche de GPSR est connue sous le nom de Improved-GPSR (Improved-Greedy Perimeter Stateless Routing). En revanche, la méthode proposée pour remédier aux problèmes de sécurité présente l'inconvénient majeur de ne pas être optimale pour la gestion du réseau. En effet, elle produit une surcharge dans le réseau car elle affiche des coûts plus importants en termes de nombre de messages de signalisation échangés que d'autre solution de sécurisation.

Dans le protocole Trust-Aware GPSR (Trust-Aware-Greedy Perimeter Stateless Routing), les auteurs de *(Liu & He, 2010)* ont proposé une méthode pour sécuriser le protocole GPSR. Cette solution consiste à utiliser un mécanisme de confiance. Chaque nœud possède sa propre valeur de confiance $T_i(t)$ (Trustiness) qui indique la crédibilité globale du nœud i selon un temps t. Ainsi, il conserve une table de voisinage locale contenant un état supplémentaire appelé « Neighbor R » (réputation) qui enregistre la position des voisins par rapport au nœud source. La réputation est déterminée en fonction de la valeur Trustiness $T_i(t)$. Cette dernière est calculée par un algorithme utilisant la distance géographique. Dans ce protocole, le prochain voisin est celui qui a la plus grande valeur de réputation et la plus courte distance géographique. Cette nouvelle approche présente certains défauts qui limitent son utilisation. Ce protocole ne permet pas de contrer les attaques de déni de service. De plus, il ne permet pas d'empêcher les attaques qui sont menées par les nœuds qui existent dans la zone de localisation et qui visent à modifier les données. Ceci est dû à l'absence d'authentification des messages de saut en saut. Les extensions de sécurité proposées pour GPSR couvrent un grand nombre de problèmes distincts. Mais toutes ces solutions restent des mécanismes partiels et jusqu'à aujourd'hui, il n'existe pas de solution complète pour faire face à toutes les vulnérabilités du protocole GPSR.

GSPR

GSPR (Geographical secure path routing protocol) est une version totalement différente de la version du protocole GPSR. Les auteurs de *(Pathak & Yao, 2008)* ont proposé un nouveau protocole de routage géographique sécurisé nommé GSPR. Ce protocole est dédié aux réseaux VANETs. Il achemine les messages vers des zones bien localisées tout en détectant les zones contenant des nœuds malicieux. De plus, il authentifie le chemin grâce à l'utilisation de clés publiques.

Tableau 1 : techniques de sécurité utilisées pour les principaux mécanismes de routage sécurisés pour les réseaux ad hoc

Protocole	Routage	Mécanisme de sécurité
S-OLSR	Proactif	MAC
S-OLSR	Proactif	Signature à clé publiques
SAODV	Réactif	Signature à clé publiques , chaîne de hachage
SAP	Réactif	MAC
ARAN	Réactif	Signature à clé publiques
S-GPSR	Géographique	Système de confiance
Improved-GPSR	Géographique	Cryptographie à clé publiques
Trust-Aware GPSR	Géographique	Système de confiance(Réputation)
GSPR	Géographique	Cryptographie à clé publiques

Nous arrivons à la fin de la partie relative à l'état de l'art des solutions de routage, gestion de la QdS et sécurité pour les environnements contraints. Nous avons fait le choix de ne développer dans un premier temps que ces aspects pour les réseaux aéronautiques et pour les réseaux de flottes de drones. Ceci afin de ne pas surcharger inutilement l'introduction de ce chapitre. Par la suite, nous reviendrons ponctuellement sur les solutions existantes dans la littérature pour les différents domaines scientifiques connexes auxquels nous nous sommes intéressés pour mener à bien notre travail de recherche. Pour conclure cette introduction, nous présentons, dans la sous-section suivante, la structure de la contribution d'HDR que nous allons détailler par la suite (cf. section 2).

1.3- STRUCTURATION DE LA CONTRIBUTION D'HDR

La contribution de ce manuscrit vise à illustrer comment les mécanismes de sécurité et de QdS sont liés et peuvent être traités de façon partiellement conjointe pour permettre une meilleure utilisation des ressources réseaux dans le type d'environnement spécifique que représente un réseau contraint.

Ainsi, nous commencerons cette sous-section par présenter les principaux résultats de recherche qui ont été introduits pendant mon expérience de doctorant puis de post-doctorant au LAAS-CNRS et au KAIST (Korean Advanced Institute of Science et Technology). L'objectif de ce travail a été de proposer de nouveaux mécanismes de niveau transport permettant l'optimisation de la QdS et dans un deuxième temps d'étudier comment ces mécanismes peuvent être utilisés dans le domaine de la sécurité réseau pour faire face à des comportements anormaux (attaques de déni de service par exemple). Ces mécanismes reposent sur l'utilisation de mécanismes de mesures en temps réel qui permettent d'augmenter le niveau de connaissance du fonctionnement du réseau et proposer des ajustements au plus près des variations de ressources que l'on peut mesurer dans ce réseau. Ces contributions ont été réalisées pour le réseau Internet qui n'est pas à proprement parlé un réseau contraint. Néanmoins, ces résultats de recherche préliminaires m'ont permis de structurer ma réflexion et d'apporter, dans un deuxième temps, une contribution pour le domaine plus spécifique des réseaux contraints : réseau satellite, réseaux ad hoc de drones, réseaux sans fil aéronautiques… Ainsi, la période de mes travaux avant 2006 (cf. sous-section 1.3.1) représente un résumé des contributions que j'ai pu réaliser dans le domaine de la gestion de la QdS et de la sécurité avec comme réseau d'application l'Internet. La période de mes travaux à partir de 2006 (cf. sous-section 1.3.2 et section 2) représente la suite de ce travail mais adapté à un environnement plus spécifique : celui des réseaux contraints.

Il est important pour le lecteur de noter que les résultats présentés dans la sous-section 1.3.1 ne représentent pas directement le cœur de ma contribution permettant la

soutenance de mon HDR. Néanmoins, ils constituent le point de départ de ma réflexion intellectuelle qui m'a amené, dans un second temps, à m'intéresser à la problématique des réseaux contraints et ainsi proposer diverses solutions de gestion de la QdS et de la sécurité pour ces environnements spécifiques : réseau aéronautique ou encore réseau de drones.

C'est la raison pour laquelle, dans la suite de cette introduction, je m'attache à résumer le fil directeur de mes recherches suivies au travers de ces deux phases. Je détaillerai par la suite, dans les sections suivantes (section 2 et suivantes), les principales contributions que j'ai réalisées visant à améliorer le niveau de QdS et de sécurité pour des systèmes communicant spécifiquement en environnement contraint.

1.3.1- Travail de thèse et de post-doctorat : septembre 2002 – aout 2006

Pendant la période de septembre 2002 à août 2006, j'ai eu la possibilité de travailler tout d'abord en tant que doctorant puis post-doctorant dans le groupe OLC (Outils et Logiciels pour la Communication) du LAAS-CNRS. Dans le même temps, entre août 2005 et février 2006, j'ai mené une expérience de post doctorat dans une équipe de recherche internationale située en Corée du Sud, au sein du KAIST (Korean Advanced Institude of Science and Technologie) dans le laboratoire Advanced Network sous la direction du professeur Sue B. Moon. Les thématiques de recherche que j'ai abordées ainsi que les projets de recherche supports dans lesquels j'ai été investi sont détaillés ci-après.

J'ai eu la possibilité en particulier pendant ma thèse puis mon activité de post-doctorat de pouvoir travailler sur différents projets de recherche français et européens dont le dénominateur commun était l'utilisation des techniques de métrologie réseaux pour améliorer les services de l'Internet. L'objectif a été, dans un premier temps, de favoriser la compréhension des phénomènes complexes qui régissent le réseau Internet et dans un deuxième temps, de pouvoir proposer des modifications pour les mécanismes qui sont déployés dans ce réseau. L'objectif final a été d'améliorer le fonctionnement global de l'Internet et d'augmenter ainsi le niveau de service fourni par ce dernier.

En effet, l'Internet est en train de devenir le réseau universel pour tous les types d'informations, du transfert simple de fichiers binaires jusqu'à la transmission de la voix, de la vidéo ou d'informations interactives en temps réel. L'Internet se doit donc de fournir de nouveaux services adaptés pour ses applications et les données qu'elles transmettent. De plus, l'Internet croît très rapidement, en taille (nombre d'utilisateurs, d'ordinateurs connectés, etc.) et en complexité, en particulier à cause de la nécessité d'offrir de nouveaux services et d'optimiser l'utilisation des ressources de communication pour améliorer la qualité de service offerte aux utilisateurs. A cause de cette complexité grandissante de l'Internet, l'évolution de ce réseau global est indissociable d'une parfaite connaissance et compréhension des caractéristiques de son trafic. Bien que la métrologie ne soit appliquée dans la recherche, l'ingénierie et la conception des réseaux Internet que depuis le début des années 2000, cette approche est de plus en plus populaire et devrait tendre à se généraliser. Ses principes consistent à étudier, caractériser, analyser et modéliser le trafic existant sur les liens de l'Internet, afin de comprendre les mécanismes qui régissent le comportement du réseau par rapport à un trafic qui s'avère méconnu. En particulier, garantir la qualité de service (QdS) dans l'Internet est un problème essentiel aujourd'hui. La métrologie du trafic Internet, et notamment son analyse montre que les mécanismes de transport actuels (TCP) introduisent des propriétés de LRD (Long Range Dependence) qui se traduisent par une grande variabilité du trafic et obligent à sur-dimensionner les ressources de communication.

Un des objectifs de mon travail de thèse a été de trouver des protocoles de transport qui réduisent cette LRD afin d'optimiser l'utilisation des ressources de communication. Ainsi, les nouveaux mécanismes protocolaires et architecturaux de l'Internet pourront être parfaitement adaptés aux besoins des utilisateurs et aux contraintes du trafic. Finalement,

c'est le processus de recherche et d'ingénierie des réseaux qui peut être modifié en lui ajoutant une phase métrologique en amont permettant de collecter des données et des connaissances sur l'existant, qui permettront ensuite de concevoir et mettre en oeuvre de nouveaux réseaux optimisés. Ainsi, mon travail de thèse a présenté une nouvelle approche pour l'Internet, dont l'objectif a été d'améliorer la gestion du trafic, la QdS et plus généralement, les services réseaux. Cette approche, appelée MBN (Measurement Based Networking), repose principalement sur l'utilisation de techniques de métrologie actives et passives qui permettent de mesurer en temps réel différents paramètres du réseau et de son trafic pour ainsi réagir très rapidement et très précisément à des évènements spécifiques (apparition de congestion par exemple). J'ai illustré en particulier l'approche MBN au travers du développement d'un mécanisme de contrôle de congestion orienté mesures intitulé MBCC (Measurement Based Congestion Control) et je l'ai évalué au travers de simulations NS-2. Mes résultats ont ainsi montré, en particulier, comment ce nouveau mécanisme permet d'améliorer les caractéristiques du trafic ainsi que la QdS dans l'Internet, malgré la complexité et la variabilité du trafic actuel. Enfin, dans la dernière partie de mon travail de thèse j'ai présenté comment l'approche MBN et le mécanisme MBCC, en particulier, peuvent garantir une QdS robuste, i.e. capable de fournir la QdS demandée en toutes circonstances, notamment en présence d'attaques de DdS (Déni de Service). En effet, j'ai utilisé l'architecture MBA (Measurement Based Architecture) basée sur des mesures du trafic en temps réel pour s'adapter aux ruptures légitimes ou illégitimes du trafic s'y produisant en continu. En particulier, j'ai démontré que le mécanisme de contrôle de congestion MBCC associé à MBA, conçu pour générer des trafics réguliers et optimaux, rend l'Internet plus robuste que TCP face aux attaques de DdS.

Ce résultat a permis d'orienter la suite de mes travaux de recherche. En effet, il existe un lien fort entre mécanismes d'amélioration (et a fortiori de garantie) de la QdS dans un réseau et le niveau de sécurité qui peut être offert par ce dernier. L'exemple MBCC de cette section montre comment un mécanisme de contrôle de congestion alternatif à TCP peut apporter plus de stabilité et donc plus de robustesse (d'un point de vue de la sécurité du service réseau rendu). Ainsi, dans la suite de ce manuscrit, nous allons revenir sur le lien qui unit ces deux aspects de la gestion du réseau (gestion de la QdS et gestion de la sécurité) et voir comment nous pouvons améliorer conjointement le niveau de satisfaction des usagers pour ces deux indicateurs.

Par la suite, dans le cadre du séjour post-doctoral réalisé au KAIST, j'ai appliqué mes résultats de caractérisation du trafic à la prédiction de matrices de trafic pour ainsi pouvoir réaliser un dimensionnement et une interconnexion optimaux dans le cadre d'une topologie multi-domaines comme celle présente dans l'Internet. En parallèle, j'ai poursuivi mon travail de développement d'outils de caractérisation du trafic initié au cours de mon doctorat en l'orientant plus spécifiquement vers la conception d'outils de détection d'intrusion reposant sur l'analyse des caractéristiques spécifiques du trafic qui sont présentes dans ces cas particuliers.

A l'issue de ces travaux de recherche j'en pressenti que les travaux de sécurité que j'avais initié au cours de cette période (2002-2006) pouvaient être approfondis et offraient un champ d'application très important. C'est dans ce cadre que j'ai eu la possibilité d'intégrer l'ENAC de Toulouse et son laboratoire TELECOM afin d'étudier dans quelles mesures mes travaux de recherche définis pour le réseau Internet pouvaient s'appliquer à des réseaux plus spécifiques tels que les réseaux aéronautiques ou encore les réseaux de drones. C'est ainsi que la problématique du lien qui existe entre sécurité et QdS pour optimiser l'utilisation des ressources en environnement contraint m'est apparu comme un sujet de recherche à part entière. Le premier type de réseau contraint auquel je me suis intéressé dans mes travaux de recherche a donc été le réseau aéronautique. Il s'agit de l'ensemble des systèmes qui permettent aux aéronefs de pouvoir échanger différents types d'informations

pendant leurs différentes phases de vol. Par la suite, j'ai considéré des réseaux contraints plus traditionnels tels que les réseaux de drones collaboratifs.

1.3.2- Activités de recherche au sein de l'ENAC : depuis septembre 2006

Ainsi, les travaux que je mène, depuis 2006, à l'ENAC dans le domaine aéronautique ou encore dans le domaine des réseaux de drones impliquent le plus souvent des ressources réseaux limitées et donc l'utilisation de mécanismes permettant d'optimiser l'utilisation de ces ressources. De plus, la nécessité de durcir vis-à-vis de comportements internes ou externes illicites ces environnements en ajoutant diverses solutions de gestion de la sécurité complexifie l'utilisation optimale des ressources réseaux disponibles.

Dès lors, le dénominateur commun des travaux qui seront présentés dans une deuxième partie de ce chapitre repose sur le lien fort qui existe entre mécanismes de QdS et mécanismes de sécurité dans des environnements réseaux contraints et hétérogènes. Ainsi, dans le cadre du projet FAST[5] et de la thèse de M. Slim Ben Mahmoud, nous avons proposé un mécanisme de gestion adaptatif de la sécurité qui prenait en compte l'état des ressources des différents liens sur le chemin pour pouvoir garantir un niveau de service aux usagers du système. En pratique, le goulot d'étranglement réseau se situait sur le lien avec le moins de capacité à savoir le lien satellite et c'est donc ce dernier sur lequel les mesures de performances se concentraient. De plus, pour pouvoir déployer ces mécanismes de sécurité, il était important de considérer l'architecture support de sécurité à déployer également dans le réseau. Pour cela, il a été nécessaire de définir une PKI (Public Key Infrastructure) adaptée au contexte aéronautique. Cette proposition a été prototypée et testée en environnement d'émulation. Pour pouvoir confronter les mécanismes à un trafic réaliste, un premier travail de modélisation des divers trafics aéronautiques (ATSC[6], AOC[7], AAC[8] et APC[9]) a été réalisé. Ce premier niveau de réalisation pratique a soulevé diverses questions sur la suite à donner à nos recherches si l'on souhaitait pouvoir aller plus loin dans ce domaine et pouvoir, par exemple, certifier un tel système.

Ainsi, je me suis intéressé par la suite à la problématique de la certification de système ayant des fonctionnalités nouvelles pour l'aéronautique : en l'occurrence l'interconnexion sécurisée de différents domaines avioniques et aéronautiques. Ce travail a été rendu possible par le partenariat que j'ai initié avec la société Thales Avionics (Toulouse) qui nous a permis de définir un prototype pré-industriel de routeur embarqué de nouvelle génération. La collaboration avec l'entreprise Thales Avionics et l'encadrement de la thèse de M. Antoine Varet nous ont amené à considérer au plus tôt la phase de certification du système final pour le développement du prototype. Ainsi, nous nous sommes intéressés au domaine des approches de conception et développement orientées modèles (DO-331 *(DO-331, 2011)* et DO-178C *(DO-178C, 2011*) qui au moment du lancement projet et du travail de thèse (septembre 2010) commençait à apparaitre comme une des pistes futures pour permettre la vérification de tels systèmes complexes. Ce travail s'est traduit par la réalisation d'une maquette et de tests en environnement grandeur nature. Pour cette dernière phase du travail, il a été possible d'enrichir le travail de modélisation du trafic aéronautique initié dans le projet FAST pour le rendre plus réaliste grâce notamment à l'intégration de processus de génération basé sur des sources on-off et de modèles stochastiques à queue lourde.

Ces deux projets ont permis de concevoir et tester des briques réseaux indépendantes. Néanmoins, pour pouvoir contribuer à l'amélioration des performances d'un

[5] FAST : Fiber-like satellite Telecommunications
[6] ATSC : Air Traffic Service Communication
[7] AOC : Aeronautical Operational Communication
[8] AAC : Aeronautical Administrative Communication
[9] APC : Aeronautical Passenger Communication

réseau (type aéronautique ou encore de drones), il est nécessaire d'avoir en parallèle une approche plus globale de gestion de l'architecture de communication. Nous avons donc contribué à définir une méthode d'analyse de risque dans le cadre du projet européen SESAR[10]. Cette méthode a permis de donner des orientations dans la définition d'une architecture de communication multi-liens avec prise en compte conjointe des aspects QdS et sécurité pour le futur réseau de communication déployé par l'intermédiaire du projet SESAR. Ces problématiques de communication et sécurité ont pu ainsi être fédérées au travers du sous-projet SESAR 15.2.4 dont l'objectif est la définition et la conception d'une architecture de communication de bout en bout multi-liens tenant compte des problématiques de QdS et de sécurité.

En parallèle de l'aspect purement aéronautique, j'ai eu la possibilité de m'intéresser également à la définition d'une architecture de QdS mais pour un domaine connexe : les flottes de mini drones collaboratifs. Ce travail se déroule dans le cadre de la thèse de Melle Ouns Bouachir. Cette application repose sur l'utilisation de réseaux ad hoc de drones disposant, par construction, de faibles ressources (autonomie, CPU, capacité de transmission) et pour lesquels il a été nécessaire de définir l'architecture de communication, valider les concepts en simulation et finalement tester la solution logicielle proposée par l'intermédiaire de cibles matérielles réelles.

Ce travail m'a ouvert la voie à une collaboration avec une entreprise toulousaine « Delair Tech », spécialisée dans la conception de drones. Dans ce cadre, nous nous intéressons actuellement à la définition d'une architecture générique embarquée proposant des fonctionnalités de sécurité pour tout type d'application : vidéo surveillance, communication en environnement critique, etc. La cible matérielle de ce nouveau projet (démarré en novembre 2013) est un drone industriel. Ainsi, les objectifs de certification qui avait été envisagés dans la thèse d'Antoine Varet reviennent au cœur de la problématique car ces drones pourraient à terme voler dans le même espace aérien que les avions civils.

Dans ce travail, la conception des mécanismes de sécurité adaptés au domaine des drones est le cœur de la contribution. Néanmoins, nous avons souhaité intégrer l'aspect certification de la solution proposée dans ce projet de façon à pouvoir capitaliser sur les méthodes et outils proposés pendant notre collaboration avec l'entreprise Thales Avionics afin de pouvoir proposer une solution qui serait intégrable à moindre coût dans l'espace aérien civil. Dans ce contexte, il sera nécessaire de fournir, à terme, un dossier de certification aux organismes de standardisation. Ainsi, si cette problématique de certification n'avait pas été considérée dès le départ du projet, les coûts de certification de la solution logicielle finale deviendraient exorbitants. Dès lors, les pistes de conception orientée modèle et la réutilisation partielle de la méthode de prototypage logiciel rapide proposée dans la thèse d'Antoine Varet constituent un projet de recherche intéressant que nous sommes en train d'approfondir au travers de la thèse de M. Jean Aimé Maxa qui a débutée en novembre 2013 avec l'entreprise Delair Tech.

Ainsi, la suite du manuscrit (section 2) présente les différentes contributions introduites précédemment en développant de façon conjointe les 4 thématiques de recherche ci-dessous :

- Architecture de communication sécurisée,
- Architecture de communication pour les réseaux de communication contraints (satellite, MANET),
- Caractérisation et modélisation du trafic et des attaques,
- Problématiques conjointes de sureté et de sécurité pour la certification dans les systèmes aéronautiques.

[10] SESAR : Single European Sky for ATM Research

Par la suite, un résumé des activités d'encadrement réalisées au cours de ces travaux de recherche (section 3) ainsi que la liste des développements logiciels (section 4) qui ont été nécessaires pour réaliser ces contributions scientifiques sont également fournis en guise de récapitulatif. Enfin, à la fin de ce chapitre, la section 5 synthétisera les travaux de recherche présentés pour ce manuscrit d'habilitation à diriger les recherches et présentera un certain nombre de perspectives scientifiques que nous envisageons pour la suite de nos travaux. Pour information, le lecteur trouvera dans le chapitre 5 la bibliographie de ce manuscrit d'HDR et dans le chapitre 6 la liste des différentes publications de l'auteur.

2- CONTRIBUTION A L'AMELIORATION DES COMMUNICATIONS DE DONNEES EN ENVIRONNEMENT RESEAU CONTRAINT

Mon expérience de doctorant et de post-doctorant m'a permis de m'intéresser, dans un premier temps, aux problématiques de gestion de la qualité de service de l'Internet puis de considérer certaines applications de mes travaux à un domaine plus spécifique qu'est la détection d'attaque et la sécurité du trafic de l'Internet. Ainsi, en intégrant l'ENAC et le laboratoire TELECOM courant 2006, j'ai eu la possibilité de considérer ces mêmes problématiques mais dans un domaine réseau connexe à l'Internet : les réseaux de communications aéronautiques puis les réseaux de flottes de drones. Mes travaux de recherche ont ainsi pu être étendus à ce nouvel environnement tout en considérant des problématiques qui sont fondamentales pour mon travail : la gestion de la qualité de service, l'analyse du trafic et des attaques ainsi que les architectures de sécurité.

2.1- CARACTERISATION DU TRAFIC AERONAUTIQUE

Dans un premier temps, je me suis intéressé à la caractérisation du trafic aéronautique. En effet, pour pouvoir agir de façon efficace sur un environnement il faut être capable de connaitre avec précision les caractéristiques du trafic qui transite dans cet environnement. Ainsi, nous avons effectué une étude pour déterminer les types de flux susceptibles de transiter à travers des équipements embarqués à bord des avions. Trois classes principales de trafic sont susceptibles de transiter sur les réseaux liés au domaine aéronautique : les flux ATSC, AOC+AAC et APC.

Ces flux sont respectivement ceux des systèmes hautement critiques nécessaires au vol (Air Traffic Services Communications), des systèmes embarqués gérés par la compagnie pour les aspects commerciaux, de sécurisation, de régulation et d'optimisation du vol (Aeronautical Operational Control + Aeronautical Administrative Communication) et enfin ceux des futurs flux « passagers » (Aeronautical Passenger Communication) constitués des données échangés par les passagers vers les réseaux au sol via les infrastructures embarquées dans l'avion (par exemple, le Wifi fourni à bord par la compagnie).

Pour ces classes de flux, nous avons modélisé, selon les types de protocoles employés (TCP ou UDP), les délais entre paquets (appelés Doff, en secondes) et les tailles de flux (appelés Don, en octets), ainsi que leurs distributions mathématiques et leurs paramètres. Ainsi, Doff désigne la distribution des intervalles de temps entre les débuts de flux et Don désigne la distribution des durées des flux.

2.1.1- Trafics ATSC, AOC et AAC : modélisation à l'aide de machines à état

Les flux ATSC, AOC et AAC existent déjà, ils utilisent exclusivement le protocole de transport UDP *(Ben Mahmoud, 2012)*. Nous avons déterminé à partir d'un document de référence, le COCR *(COCR, 2007),* les tailles minimales et maximales des paquets IPv4 échangés. Étant donné qu'il a été prouvé que le choix de la distribution a un impact négligeable sur les résultats *(CNES, 2009)*, nous avons choisi d'utiliser des distributions uniformes pour les Don et les Doff. De plus, nous avons modélisé ces flux, à l'aide de machines à états représentées Figure 3. Chaque état représente un type de message qui peut être généré en fonction des phases de vol de l'avion. Les transitions sont calculées en fonction de la probabilité de ce message d'être généré ou reçu par l'avion en fonction de la phase de vol dans laquelle il se trouve et des échanges précédents qu'il a eus avec le sol. Le résultat de l'enveloppe de caractérisation obtenu est décrit dans le Tableau 2.

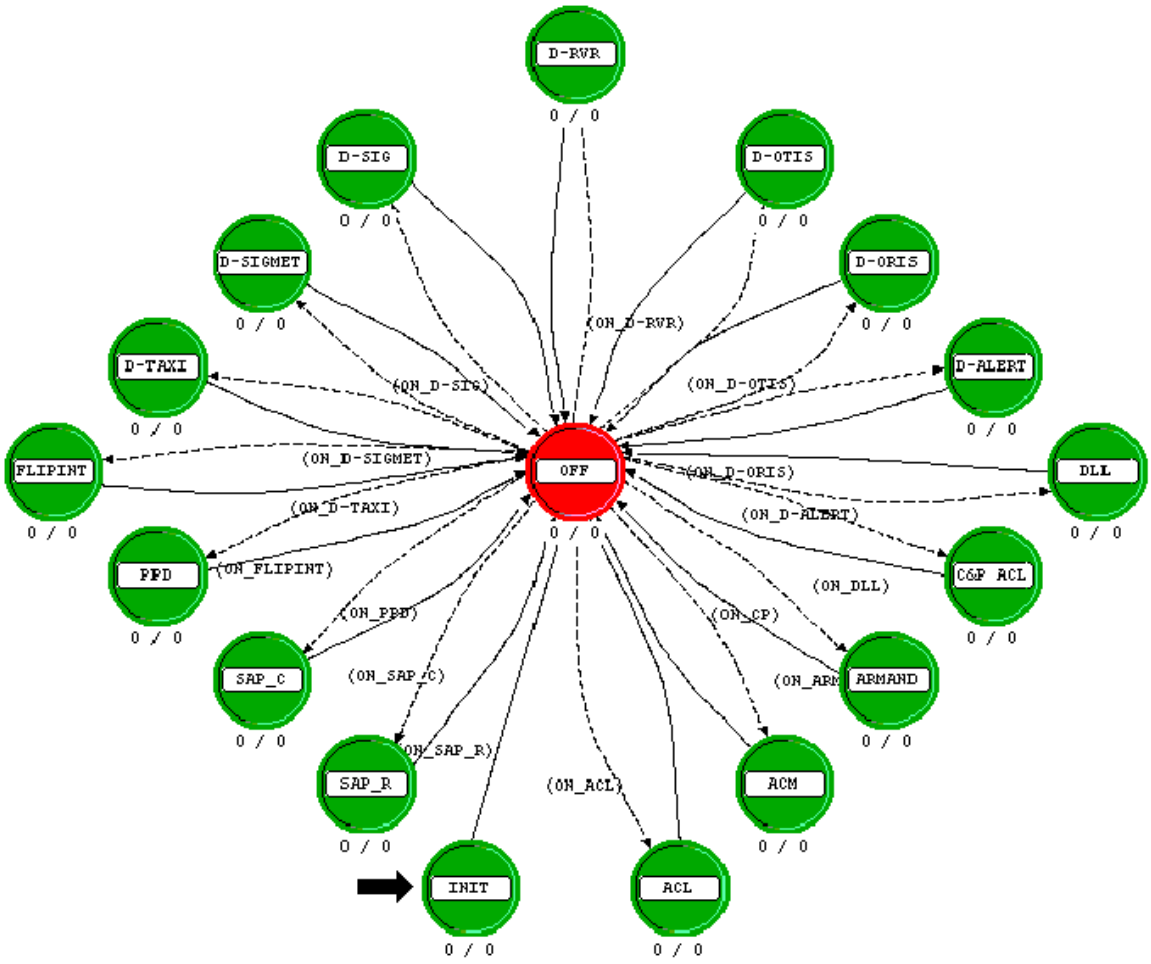


Figure 3 : modélisation à l'aide de machines à états (exemple du trafic ATSC)

Tableau 2 : modélisation par distributions mathématiques des flux ATSC, AOC et AAC

Flux UDP		Paramètres	Air vers Sol	Sol vers Air
ATSC	Don : Uniforme [octets]	Min	88	88
		Max	2500	4000
	Doff : Uniforme [seconde]	Min	0	0
		Max	2	2
AOC+AAC	Don : Uniforme [octets]	Min	90	90
		Max	5000	125
	Doff : Uniforme [seconde]	Min	0	0
		Max	2	2

2.1.2- Trafic APC : modélisation à l'aide de sources ON-OFF

Le cas des flux passagers est plus complexe, Bien qu'il existe quelques cas de services Internet embarqués, par satellite, peu de données publiques quantitatives existent et elles sont inadaptées aux moyens de communications et aux débits envisagés (bien plus important que ce qui est utilisé à l'heure actuelle dans les avions). Ainsi, nous ne pouvions pas mener le même type de modélisation à base de machine à états et de caractéristiques précises des messages échangés (cf. document COCR *(COCR, 2007)*). Nous nous sommes donc appuyés sur divers résultats de modélisation du trafic Internet, basé sur l'utilisation de processus appelés « sources ON-OFF ». Le principe de génération d'une source ON-OFF est rappelé Figure 4.

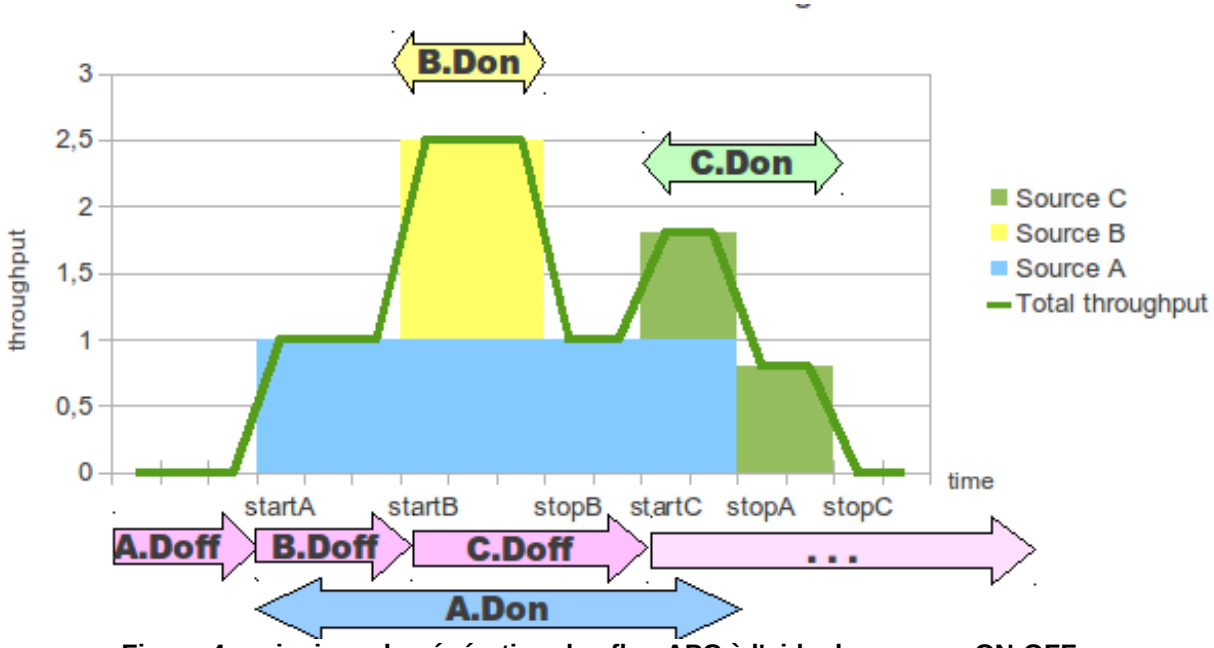


Figure 4 : principes de génération des flux APC à l'aide de sources ON-OFF

Ainsi, nous avons modélisé les Doff (temps entre flux) à l'aide de lois de Weibull (λ, k, max), jugées aujourd'hui les plus réalistes pour ce type de trafic *(Olivier & Benameur, 2000)*. Nous avons cependant ajusté les valeurs de plafond « max » pour que le débit total soit conforme à ce qui est attendu. La loi de Pareto (X_m, α , max) a été utilisée pour modéliser les Don (durées des flux).

Cette modélisation à base de loi à queue lourde *(Leland et al., 1994) (Olivier & Benameur, 2000)* pour le trafic APC a donné de très bon résultats. Nous avons comparé les caractéristiques de trafic collecté sur le réseau Internet[11] avec celui généré à partir du processus à base de sources ON-OFF décrit dans cette section. Les résultats sont très encourageants. La Figure 5 et Figure 6 représentent la correspondance entre les caractéristiques du trafic généré par l'intermédiaire du processus ON-OFF et les caractéristiques du trafic réel collecté sur le réseau Internet. On peut observer une très bonne superposition le long de la première bissectrice pour les différents diagrammes QQ-Plot, signe que la loi générée est conforme à la loi observée dans le trafic réel.

Ces résultats de caractérisation de trafic nous ont permis par la suite de pouvoir valider les contributions scientifiques que nous avons faites pour améliorer les performances des systèmes en environnement contraint. En effet, la phase d'évaluation de performance est bien plus efficace lorsque le trafic auquel sont confrontés les nouveaux mécanismes (de gestion de la sécurité et de la QdS dans notre cas) comporte des propriétés que l'on peut retrouver dans un trafic réel. Le travail de caractérisation et de modélisation pour le trafic aéronautique présenté dans cette section a rendu possible cette démarche.

Dans la suite, nous allons donc nous intéresser aux différentes contributions permettant de gérer la QdS et la sécurité pour un premier environnement contraint : le milieu aéronautique.

[11] Ce trafic a été collecté sur le routeur de sortie de l'ENAC et représente l'ensemble de communications entrantes et sortantes échangées par le personnel et les étudiants sur la base d'une journée.

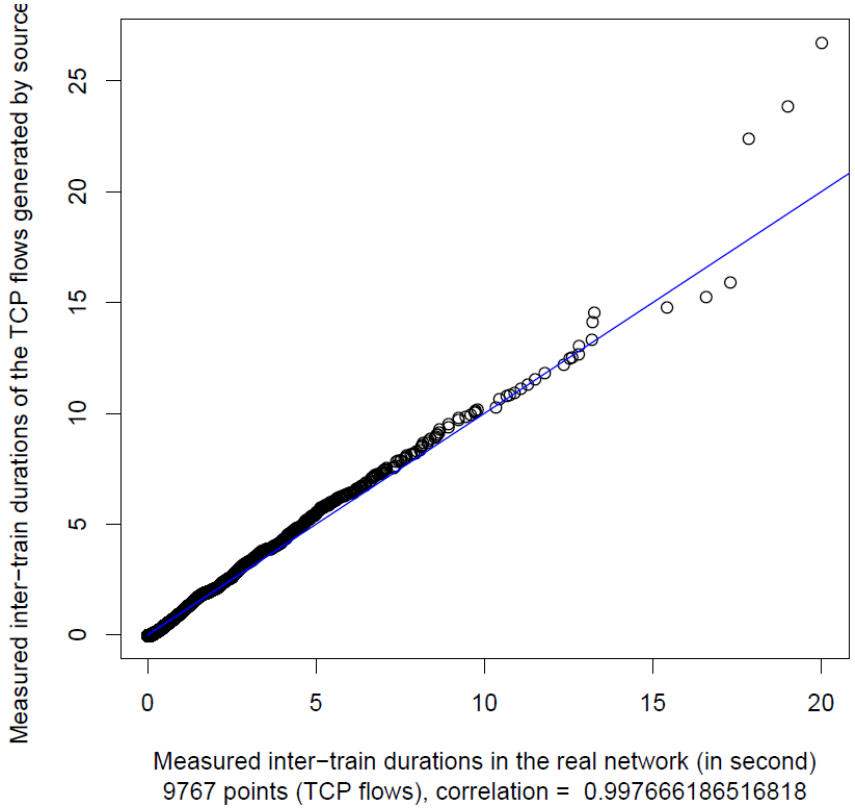


Figure 5 : QQPlot pour la série des Doff (trafic réel vs trafic généré)

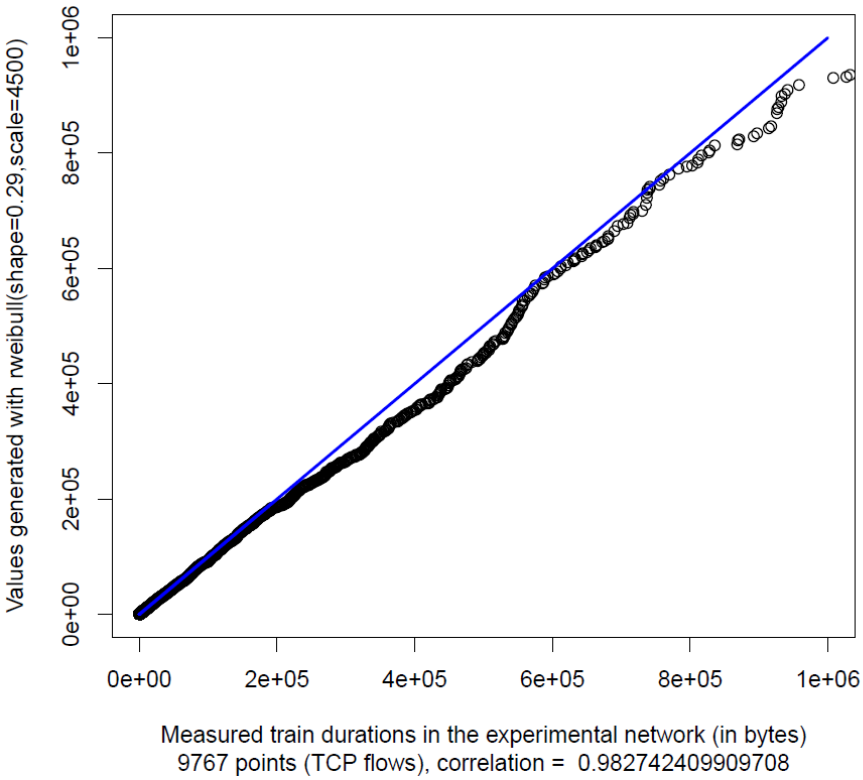


Figure 6 : QQPlot pour la série des Don (trafic réel vs trafic généré)

2.2- EXEMPLE DE LIEN ENTRE GESTION DE LA QDS ET DE LA SECURITE POUR LES ENVIRONNEMENTS AERONAUTIQUES

Le contexte aéronautique a, depuis plusieurs années, mis en évidence le besoin croissant de technologies de sécurité permettant d'éviter des utilisations malveillantes des matériels ou services installés à bord des avions par les compagnies pour leurs usagers et leurs besoins propres.

Avec l'apparition prochaine d'un service d'accès à l'Internet cabine pour le plus grand nombre, ce besoin de sécurisation va devenir une priorité. A l'heure actuelle, il n'existe pas de solution de sécurité permettant, d'une part, de gérer ce nouveau type de trafic air-sol (appartenant à la famille de l'APC pour Aeronautical Passenger Communication) et d'autre part, de l'intégrer parmi les autres types de trafic échangés entre l'avion et le sol (trafics AOC pour Aeronautical Operational Control ou ATC pour Air Traffic Control par exemple) tout en maximisant le niveau de robustesse offert.

En effet, la plupart des approches de sécurisation « avion » se concentrent sur des méthodes et techniques permettant de sécuriser les échanges au sein de l'avion (réseau avionique de type AFDX par exemple) ou sur un lien dédié aux seules communications du contrôle aérien (flux ATC principalement). Cette problématique bien que nécessaire ne suffit plus à l'heure où l'interconnexion du réseau avionique avec le reste des réseaux de communication (réseau Internet par exemple) apparaît de jour en jour comme une étape incontournable. En effet, la demande des passagers pour accéder à leurs outils de travail (classiques pour les réseaux terrestres traditionnels) depuis leur siège en cabine devient de plus en plus pressante.

2.2.1- Projet FAST (septembre 2008 – mars 2012) : définition d'une architecture de communication sécurisée pour les communications sol-bord dans le contexte aéronautique

Ainsi, en septembre 2008, j'ai initié au sein du groupe de recherche ResCo du laboratoire TELECOM de l'ENAC une codirection officielle de thèse (avec Alain Pirovano, responsable du groupe ResCo) pour la définition d'une architecture de sécurité pour les communications sol-bord dans le contexte aéronautique. Ces travaux trouvent un support financier et technique dans le cadre d'un projet national labellisé « Aerospace-Valley » intitulé FAST (Fiber-like Aeronautical Satellite Telecommunication). Ce financement nous a ainsi permis de financer Slim Ben Mahmoud qui a soutenu sa thèse en février 2012.

Ce travail de thèse a porté sur le thème « Sécurisation des applications avion dans un système de communication intégrant un segment sol bord par satellite ». L'objectif de ce travail de thèse était de répondre à ce manque en proposant une architecture de sécurité permettant l'échange sécurisé des différents types de trafic générés par les applications aéronautiques classiques, l'Internet cabine ou encore des applications plus spécifiques nécessaires dans des contextes d'urgence (télé médecine par exemple).

Ce travail s'est donc inscrit pour partie dans le cadre d'un projet industriel intitulé FAST qui a permis de proposer une infrastructure de communication aéronautique par satellite à haut débit. L'architecture de sécurité qui a été proposée dans ce travail de thèse a donc pris en compte les spécificités techniques de la solution réseau proposée dans le projet FAST. En effet, la présence du lien satellitaire devait être analysée comme un sous-élément de l'architecture globale de sécurité avec pour objectif de fournir un service sécurisé de bout en bout optimal. De plus, les applications étudiées dans le projet FAST présentaient une forte hétérogénéité en termes de contenus et d'usages qui a ainsi imposé des solutions architecturales de sécurité à définir spécifiquement.

Enfin, le contexte aéronautique dans lequel s'est inséré ce projet a nécessité de considérer les problématiques de mise à l'échelle pour ce qui est de la gestion des échanges

en environnement sécurisé. A titre d'exemple, dans le ciel français, le nombre moyen d'avions à un instant T approche les 400 avec plusieurs services (passagers et/ou compagnie) pouvant opérer en même temps dans chaque avion. Le nombre élevé des échanges qui en résultent nécessite de proposer des solutions permettant par exemple une gestion optimisée des clés de session entre usagers.

2.2.2- Contribution à l'amélioration de la QdS et de la sécurité pour les environnements aéronautiques

Ce travail de recherche a donc comporté trois phases. Une première a porté sur l'étude des architectures de sécurité existantes (tout d'abord généralistes mais également orientées aéronautique) pour permettre d'en isoler les fonctionnalités importantes en vue de proposer dans un deuxième temps une architecture de sécurité originale permettant de répondre aux besoins et contraintes spécifiques du domaine étudié. Cette phase de conception a été complétée par une évaluation des performances de la solution retenue. Dans un troisième temps, cette architecture a été développée sous forme de maquette puis testée et validée dans un environnement réel mis à notre disposition dans le cadre du projet FAST.

- **Architectures de sécurité existantes pour l'aéronautique**

Lorsque le projet FAST a démarré, les problématiques d'architecture de sécurité pour l'aéronautique étaient encore à un niveau d'avancement très faible. En effet, il existait, dans la littérature, quelques solutions permettant de sécuriser des applications spécifiques de l'aéronautique (par exemple les messages ACARS : Aircraft Communication Addressing and Reporting System) au travers du système AMS (ACARS Message Security) *(ARINC823P1, 2007)*. Néanmoins, ce type de solution ne permet pas de sécuriser de façon globale l'ensemble des informations qui sont émises et reçues par un avion : communications ATC, AOC et APC. Nous avons donc dû nous tourner vers différentes solutions de sécurité initialement introduites pour le réseau Internet comme par exemple les solutions de sécurisation de niveau réseau (IPSec) ou encore transport (TLS). L'utilisation de ces mécanismes et leur adaptation au domaine spécifique de l'aéronautique est détaillée dans la sous-section qui suit.

- **Gestion adaptative de la sécurité : système SecMan**

Pour permettre de gérer de façon optimisée à la fois la QdS et la sécurité dans le cadre des échanges entre le bord et le sol, un module de gestion de la sécurité adaptative a été proposé (SecMan : Security Manager). Cette pièce fonctionnelle additionnelle a permis d'adapter l'ensemble des mécanismes de sécurité à utiliser pour échanger les différents types de communication émis par l'avion en fonction des ressources disponibles sur le lien sol-bord. Ce lien sol-bord était constitué d'un lien satellite en bande K. Le faible niveau de ressources disponibles (au regard des différents trafics à générer : APC, AOC et ATS) a nécessité de s'inspirer des approches de gestion orientée mesures. En effet, un module déployé sur le lien satellite permettait de connaitre le niveau de ressources disponibles et par un mécanisme de « cross-layer » de pouvoir choisir les bons algorithmes de sécurité à appliquer aux applications en fonction de leur besoins. Ce choix se faisait en privilégiant différents facteurs d'optimisation pour le choix de ces algorithmes de sécurité, par exemple leur niveau de robustesse mais aussi de consommation réseau.

La Figure 7 représente le déploiement du module SecMan dans le cadre de la topologie réseau envisagée pour le projet FAST. Il faut préciser que ce nouveau composant SecMan doit pouvoir s'interfacer avec les architectures existantes permettant un traitement de la QdS sur le lien sol-bord. La Figure 8 résume notamment l'interfaçage qu'il a fallu réaliser entre les systèmes SatCom existant et notre contribution SecMan. Dans ce contexte,

il a été nécessaire de prioriser et traiter de façon différenciée les différents types de flux (ATC, AOC et APC) échangés par l'avion et le sol.

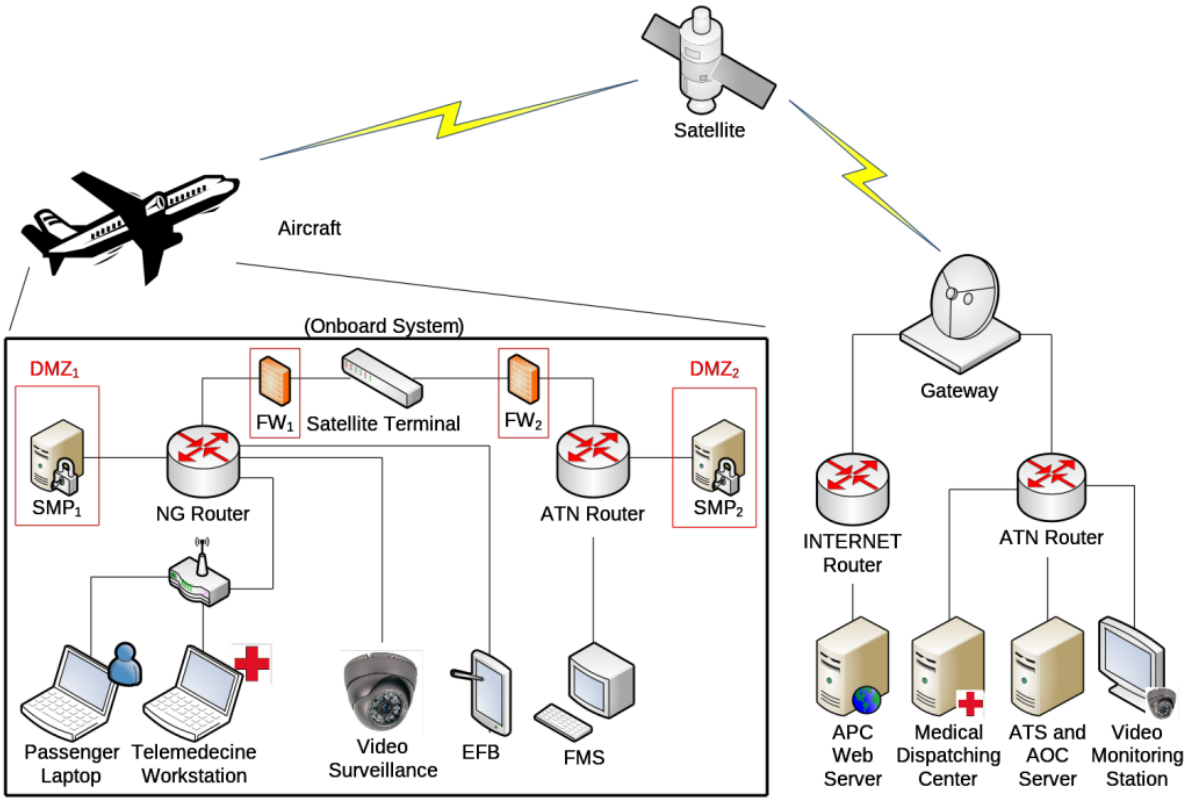


Figure 7 : déploiement du module SecMan (SMP) dans le cadre du projet FAST

La Figure 9 présente le principe de fonctionnement de l'architecture interne du module SecMan. Ce dernier, en s'appuyant sur les besoins de sécurité des différents flux qu'il doit sécuriser, active les mécanismes de sécurité adéquats en contrôlant en temps réel le niveau et l'état des ressources réseaux et systèmes disponibles pour permettre le déploiement de la politique de sécurité. Le choix du mécanisme de sécurité à activer se fait en prenant en compte différents paramètres. Il repose sur un algorithme adaptatif qui permet de proposer le meilleur service de sécurité en fonction du niveau de ressources disponibles sur le réseau. Les détails de ce mécanisme décisionnel sont abordés ci-après.

Principes de fonctionnement de l'algorithme décisionnel de la sécurité pour le module SecMan

L'un des objectifs du Security Manager Proxy consiste, à l'établissement d'un nouveau flux, à sélectionner la politique de sécurité optimale à appliquer, en fonction des paramètres suivants : les ressources système et réseau occupées, les besoins du flux et les capacités de sécurisation exploitables entre les différentes entités du réseau.

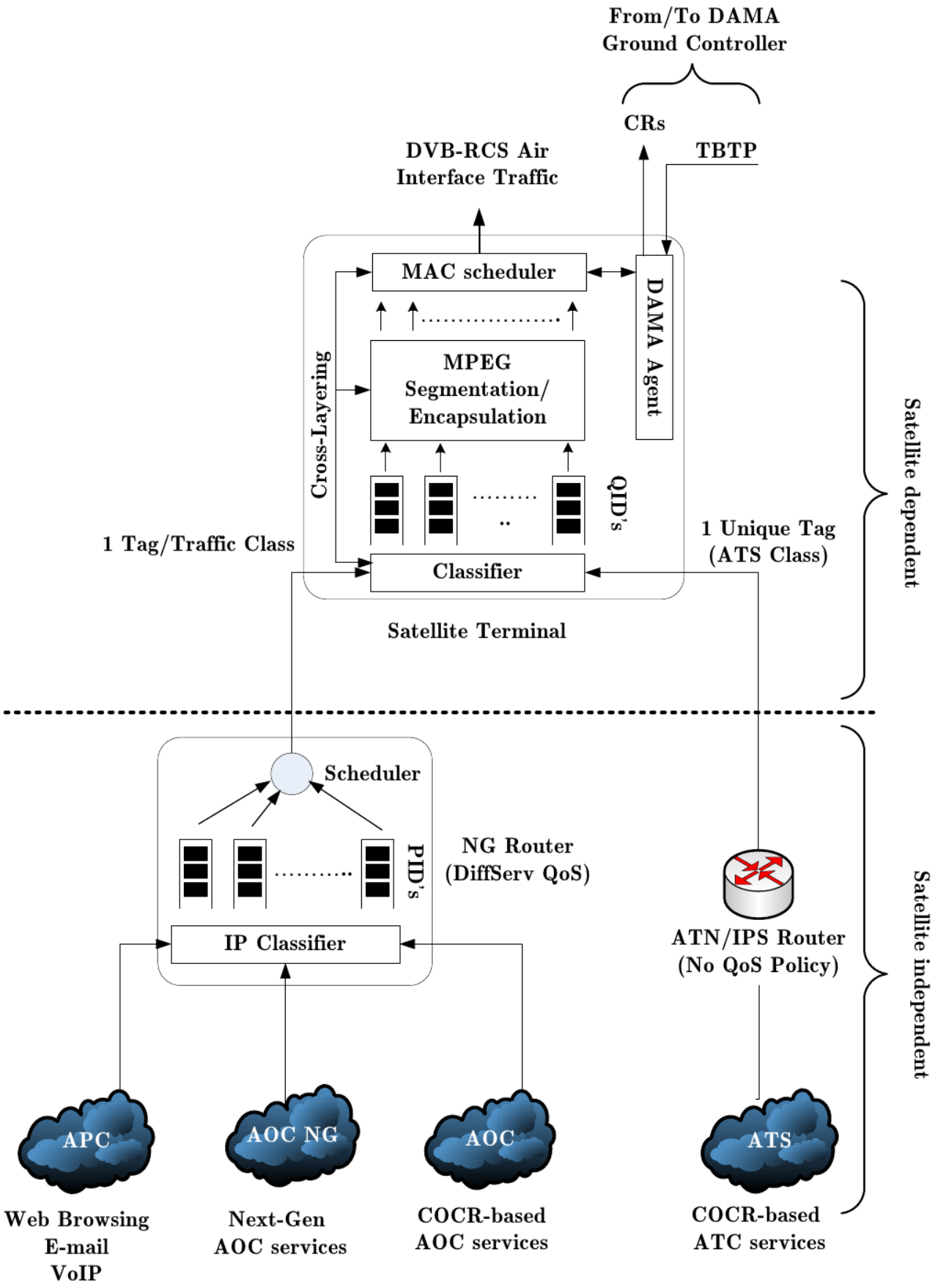


Figure 8 : gestion de la QdS dans le projet FAST

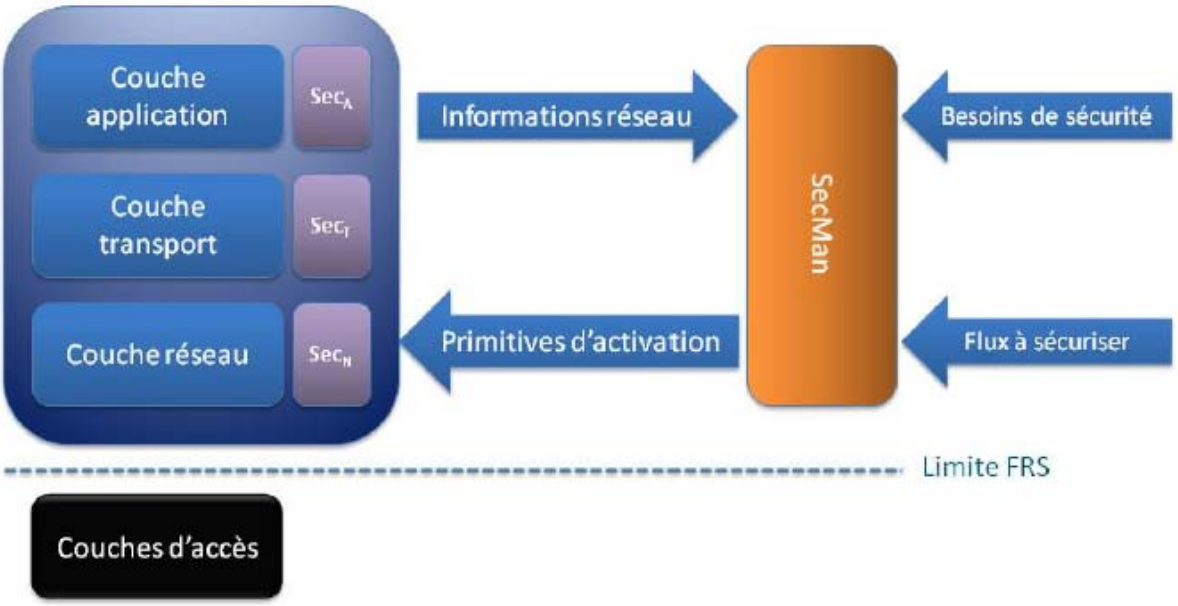


Figure 9 : principes de fonctionnement de SecMan

Etant donné que le SecMan est destiné à établir une politique de sécurité pour un réseau aéronautique basé sur le protocole IP, il est conçu pour être indépendant des couches inférieures à la couche Réseau (niveau 3 du modèle OSI). Les données, les exigences de sécurité et l'état en temps réel des systèmes et du réseau sont les entrées de l'algorithme décisionnel qui retourne un sous-ensemble de mécanismes et d'algorithmes de sécurité à appliquer aux données. Le protocole Simple Network Management Protocol (SNMP) est utilisé pour récupérer les informations d'états sur les systèmes distants et la charge réseau, transmises par des agents localisés sur les différents routeurs du réseau. Les informations telles que ifSpeed pour la bande passante réseau disponible et tcpCurrentEstab pour les connexions TCP actives sont issues des Management Information Bases (MiBs) et envoyées au Network Management Systems (NMS). L'utilisation de la version 3 du protocole SNMP permet de sécuriser les requêtes et les réponses SNMP, empêchant ainsi des intrus d'exploiter ou d'altérer les informations échangées.

A partir de ces entrées (illustrées dans la Figure 10), un algorithme d'optimisation sur plusieurs critères (« Multi-Criteria Decision Making Algorithm », MCDMA) est utilisé pour déterminer la politique optimale à associer au flux au moment de son établissement, c'est-à-dire quel(s) mécanisme(s) de sécurité appliquer avec quel(s) algorithme(s) pour sécuriser la communication IP. Les MCDMA désignent des algorithmes déjà éprouvés dans des domaines divers tels que les décisions économiques, politiques, sociales et managériales. Ils permettent d'établir le meilleur compromis parmi de nombreuses alternatives suivant des critères potentiellement contradictoires et sont basés sur des séries de calculs mathématiques pour classer les alternatives et finalement en extraire la meilleure.

L'« Analytic Hierarchy Process » (AHP *(Bhushan, 2004) (Saaty, 2008)*) est un processus de décision multi-critères reconnu pour son approche simple et hiérarchique de modélisation de systèmes complexes. La première étape consiste à établir un arbre ayant pour racine le but à optimiser et à le ramifier en critères d'évaluation des alternatives à comparer. Ensuite, pour chaque critère, les alternatives doivent être quantifiées à l'aide de métriques numériques ; dans le cas d'une évaluation non numérique, une comparaison deux à deux des alternatives permet d'établir cette métrique. Dans un troisième temps est associé à chaque critère un poids relatif aux critères ayant le même père dans l'arbre AHP.

Finalement, des calculs matriciels permettent de classer les alternatives en fonction de leur capacité à répondre au but ultime recherché (qui est la racine de l'arbre AHP).

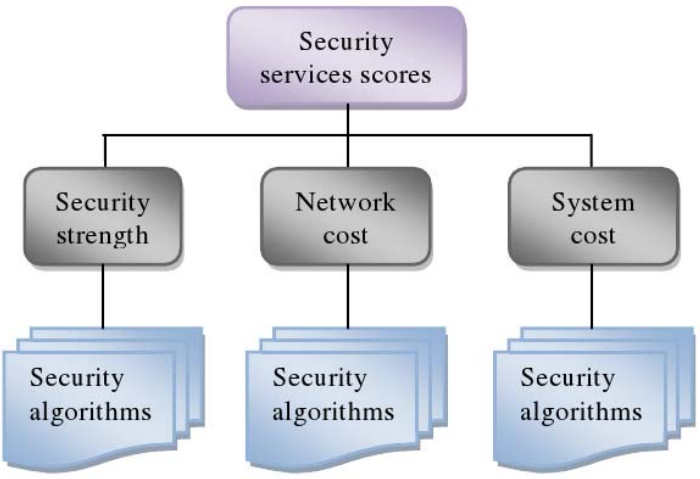


Figure 10 : ensemble des critères étudiés par l'algorithme AHP

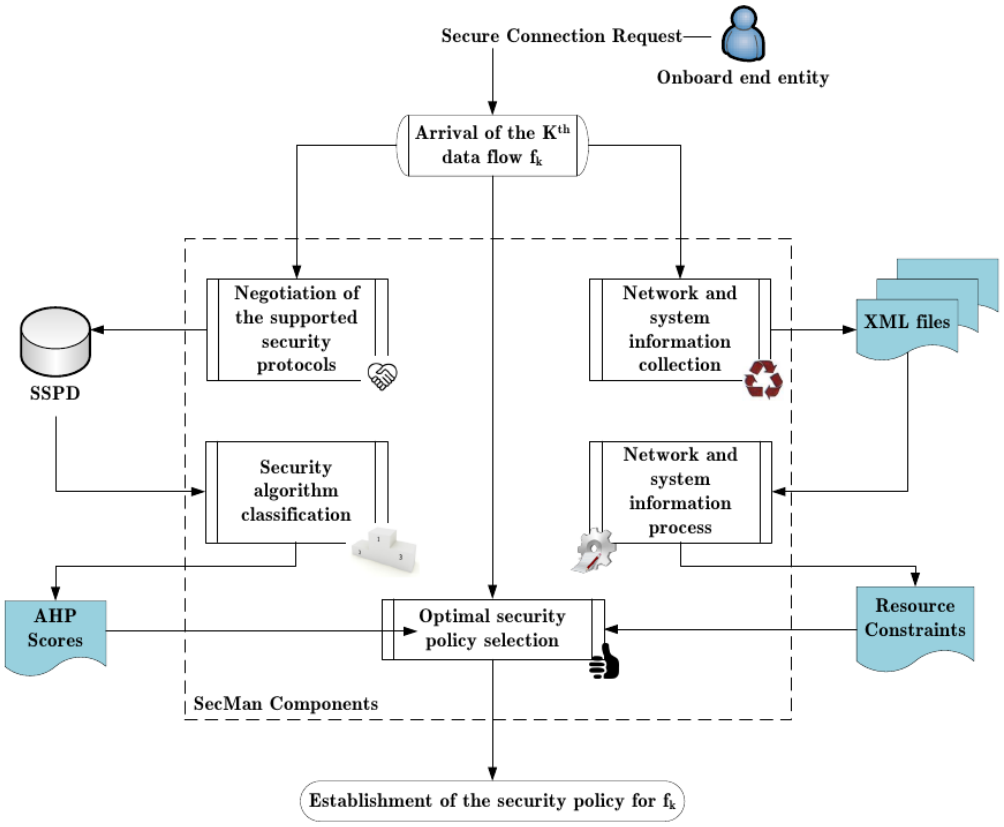


Figure 11 : algorithme de sélection de la politique de sécurité optimale du SecMan

Dans le cadre du SecMan, l'un des buts recherchés est la robustesse de la sécurité offerte. Celle-ci est mesurée en fonction des services offerts par la politique de sécurité, c'est-à-dire de la confidentialité, de l'intégrité et de l'authenticité, chacun de ces services étant évalués en fonction de critères spécifiques : taille de la clef cryptographique, taille du bloc de chiffrement utilisé, délai de bout en bout de l'authentification... Les alternatives sont les mécanismes et les algorithmes de sécurité utilisables simultanément par le SecMan et le serveur distant contacté, l'ensemble des alternatives étant établi suite à une négociation via le protocole sécurisé « Supported Security Protocols » (SSP) que nous allons détailler dans la suite.

Cependant, se baser uniquement sur la robustesse est insuffisant pour déterminer la politique optimale. Un surplus de charge réseau est engendré par l'application des mécanismes de sécurité, de même qu'une augmentation de la charge processeur ; ces éléments sont aussi pris en compte pour déterminer la politique optimale.

Ainsi, lorsqu'un premier flux arrive et que le système est peu chargé, une politique de robustesse maximale mais coûteuse pourra être sélectionnée. A l'arrivée d'un deuxième flux, cette même politique pourra être rejetée au profit d'une autre politique moins robuste et moins coûteuse si le système est chargé.

L' algorigramme de la Figure 11 représente donc le principe de fonctionnement du SecMan, elle illustre l'algorithme de sélection qui est appliqué par SecMan pour proposer le meilleur service de sécurité en fonction du niveau de ressources disponibles sur le réseau.

Cette figure présente les différentes étapes effectuées depuis l'arrivée d'un flux jusqu'à l'établissement de la politique optimale. Rappelons que la politique optimale est celle maximisant la robustesse tout en minimisant les charges système et réseau. Une politique de sécurité est le sous-ensemble des mécanismes de sécurité activés (SSL, IPSec...) et de leurs algorithmes sélectionnés.

SSP : protocole de négociation des mécanismes de sécurité disponibles pour le décideur SecMan

Pour permettre la sélection parmi un ensemble de mécanismes de sécurité entre les différentes entités du réseau, il est nécessaire de connaître l'ensemble des mécanismes de sécurité qui sont supportés par ces derniers. Pour cela, un protocole de négociation intitulé SSP (Supported Security Protocols) a été introduit. Ce dernier a fait l'objet, dans un premier temps, d'une analyse de risque qualitative pour le rendre robuste aux attaques de type rejeu de message ainsi que pour garantir l'authenticité des agents et l'intégrité des messages échangés. Dans un deuxième temps, il a été modélisé formellement par l'intermédiaire du logiciel AVISPA[12] (Automated Validation of Internet Security Protocols and Applications) *(Abadi & Cortier, 2005)*. Cet outil a permis par l'intermédiaire d'un langage de haut niveau de formaliser le comportement du protocole SSP et de le confronter à différents paradigmes d'attaques réseaux (le plus important étant le modèle d'intrusion Dolev-Yao). Cet outil permet en particulier de vérifier que le protocole ne possède pas d'erreur de conception qui le rendrait sensible à des intrusions potentielles. A l'issue de cette formalisation, nous pouvons affirmer que le protocole SSP (détaillé dans la Figure 12) ne comporte pas d'erreurs de conception qui le rendrait vulnérable aux principales attaques réseaux traditionnelles : rejeu des messages, authentification des entités et intégrité des messages.

Résultats de l'utilisation de SecMan en environnement aéronautique

Le dispositif SecMan a été validé par l'intermédiaire d'un environnement réseau émulé réalisé conjointement par l'ENAC et la société ASTRIUM (responsable du développement de l'émulateur SATEM). La topologie réseau de cet environnement est représentée dans la Figure 13.

La Figure 14 résume les résultats obtenus lors du déploiement de SecMan dans cet environnement satellite émulé. En particulier, on observe que le niveau de sécurité maximal est conservé pour les flux les plus prioritaires (flux ATS #1 et #2) et ce, même en présence d'une perturbation des ressources disponibles sur le lien satellite (cf. l'évènement « Satem Fading »). Notre système est capable de choisir de façon adaptative les mécanismes de

[12] Site du projet AVISPA : http://www.avispa-project.org/<

sécurité en temps réel pour s'adapter au niveau de ressource disponible tout en garantissant une priorité et un niveau de QdS donné pour les flux qu'il sert.

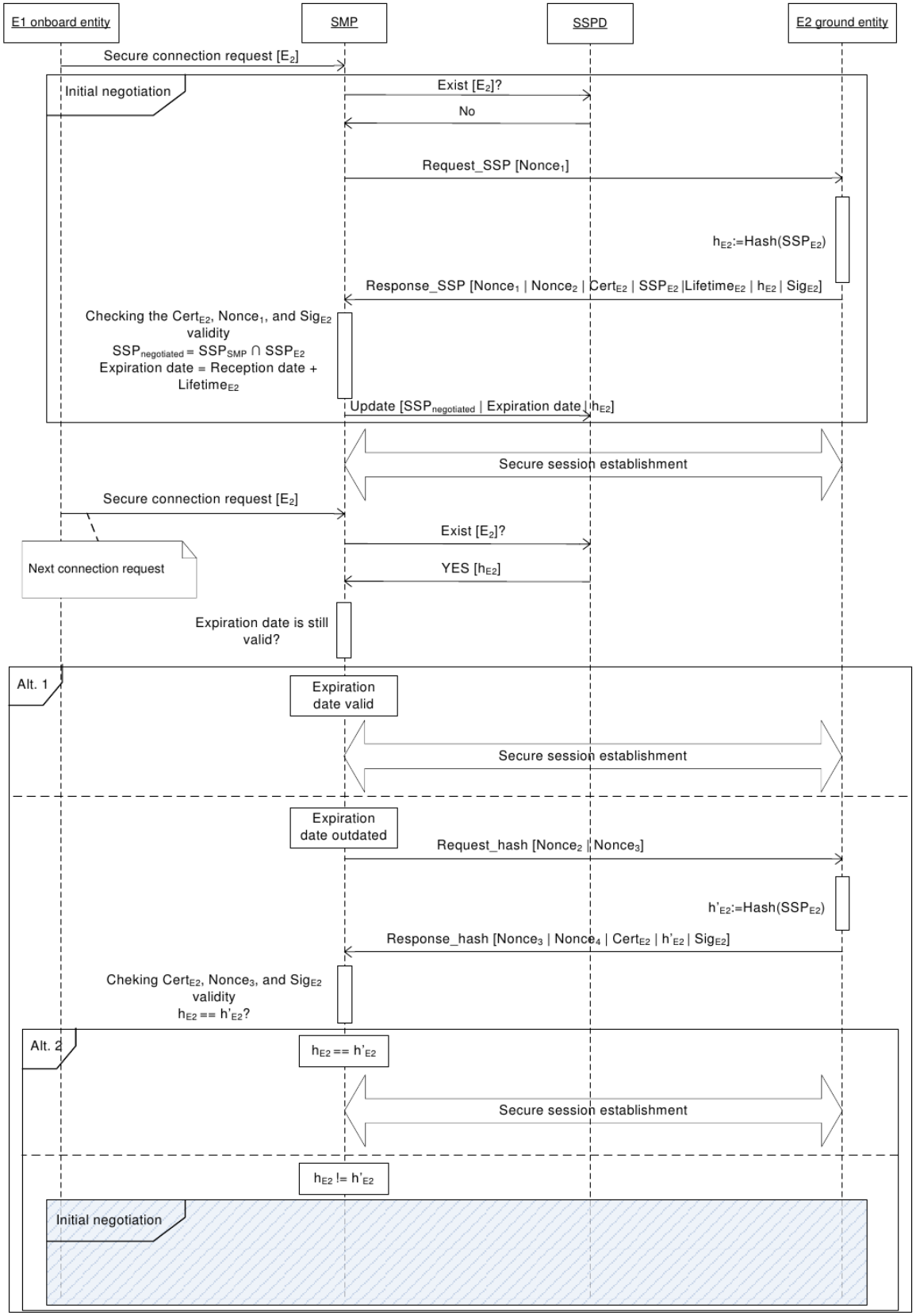


Figure 12 : fonctionnement du protocole SSP

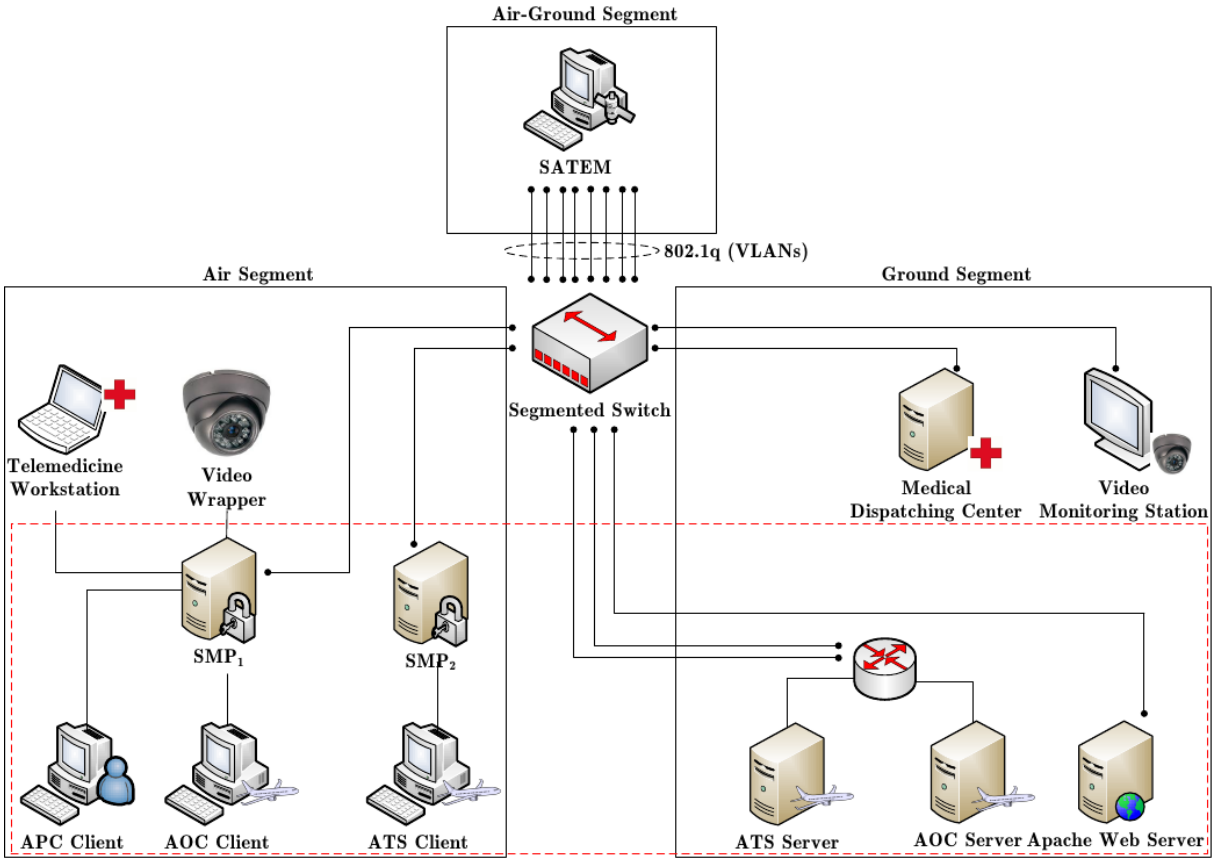


Figure 13 : environnement aéronautique émulé

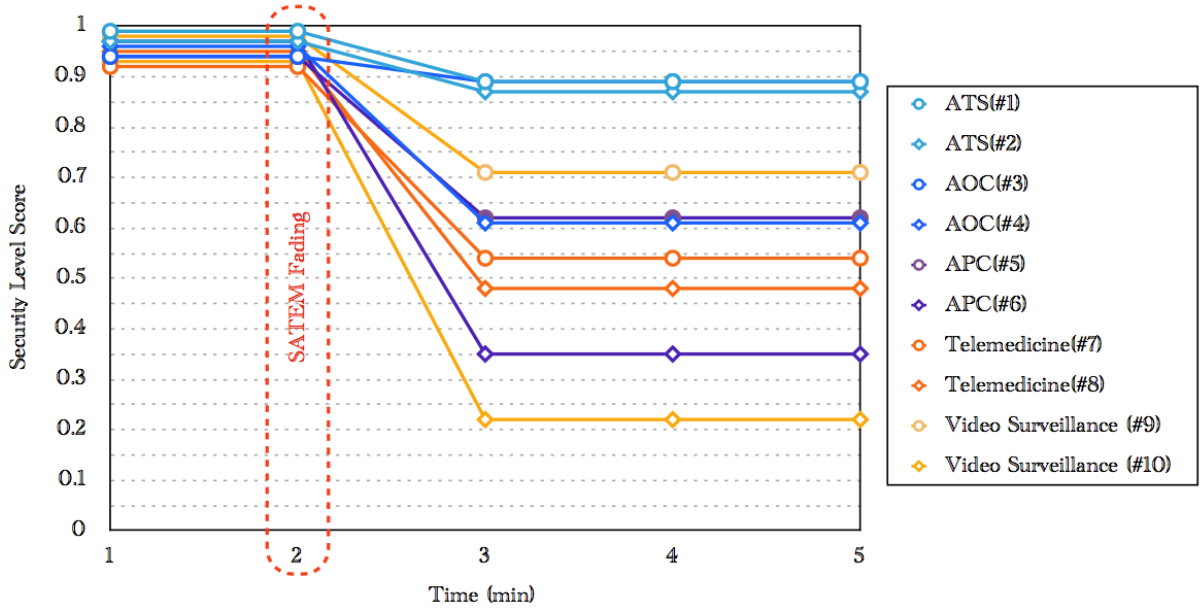


Figure 14 : utilisation de SecMan en environnement émulé

- **Proposition d'une PKI pour le domaine aéronautique**

Il est nécessaire de préciser que pour pouvoir déployer les mécanismes de sécurité à bord de l'avion pour les différents types de flux précédemment listés, une PKI (Public Key Infrastructure) spécifique pour l'aéronautique a été proposée. Cette dernière limite les échanges entre le bord et le sol afin de pouvoir tirer partie du faible niveau de ressources offert par l'environnement contraint aéronautique.

Comparaison des principales solutions de PKI existantes

Il existe différents types de PKI dans la littérature pour les domaines filaire et non filaire. Les principaux modèles sont résumés dans le Tableau 3. Le modèle hiérarchique avec plusieurs entités racines est celui qui offre les meilleurs avantages en termes de mise à l'échelle, interopérabilité et robustesse. Nous nous sommes donc orientés vers une proposition reposant sur cette architecture (cf. Figure 15). Le principe de cette architecture est de déléguer les mécanismes de sécurité (authentification, révocation, etc.) par domaine à une entité dédiée. Ce principe nous a semblé intéressant pour l'adapter au monde aéronautique et pouvoir ainsi déléguer la gestion des mécanismes de sécurité à chacune des compagnies aériennes présentes dans ce domaine. En effet, leur concurrence permanente laisse peu d'espoir dans la mise en commun d'une autorité racine de base. Ce principe nécessite néanmoins l'échange d'information entre les entités de certification de plus bas niveau. Pour cela, les CA « racines » des différentes compagnies doivent pouvoir échanger des informations pour établir une liste de CA dans lesquelles elles ont confiance (cf. « trusted CA list » de la Figure 15).

Tableau 3 : comparaison des avantages et inconvénients des différents modèles de PKI

PKI Model	Scalability	Interoperability	Robustness
Bridge model	high	medium	low
Mesh model	low	high	medium
Single-rooted model	low	high	low
Multi-rooted model	high	medium	medium
Anarchy model	low	low	medium

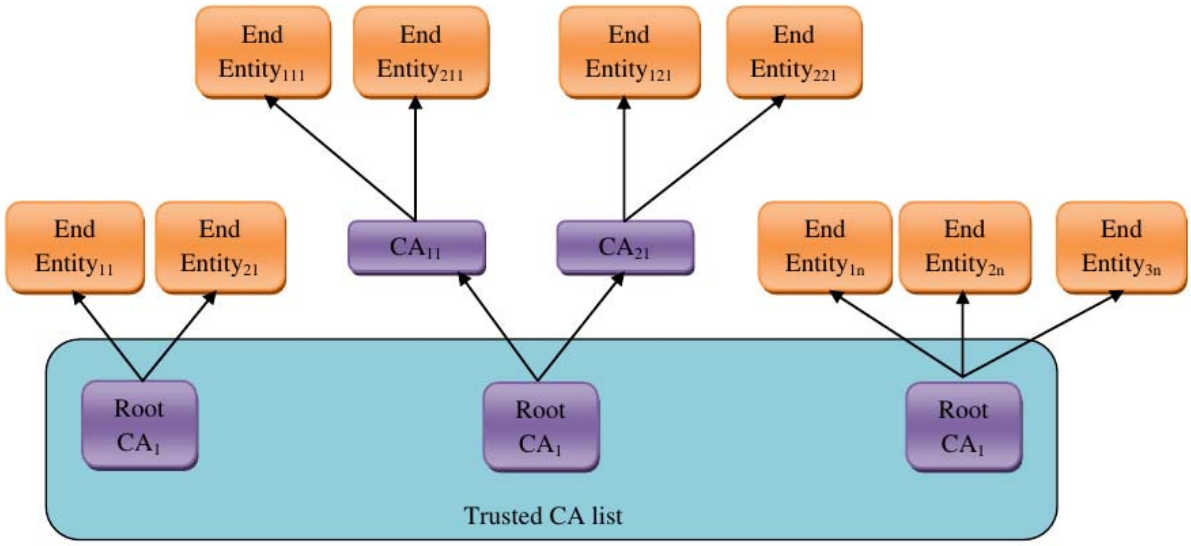


Figure 15 : modèle générique de PKI hiérarchique comportant plusieurs racines

Ce principe d'architecture est instancié dans le cadre de la Figure 16. Les CA racine (cf. Root CA de la partie droite de la Figure 16) doivent maintenir à jour entre elles une liste de confiance de toutes les CA racines. Cet équipement étant situé au sol, il ne consomme pas de ressources sol-bord embarqués. Pour les échanges sol-bord, différentes configurations ont été étudiées, l'objectif étant de limiter la quantité d'informations échangées entre l'avion et le sol dans le cadre des fonctions gérées par la PKI aéronautique (échanges entre les entités Sub-CA et Root CA de la partie droite de la Figure 16). Dans cette figure, vous pouvez observer la solution qui offre les meilleurs résultats en termes d'échanges de

données entre le sol et l'avion par rapport au modèle de référence utilisé traditionnellement dans une approche classique de type Internet. Elle permet en particulier d'économiser les ressources réseaux qui sont peu disponibles dans l'environnement contraint que représente le milieu aéronautique. Cette solution de PKI a ainsi été intégrée dans l'environnement aéronautique complet sur la base du principe de PKI hiérarchique comportant plusieurs racines et trois niveaux différents d'accréditation (cf. Figure 17).

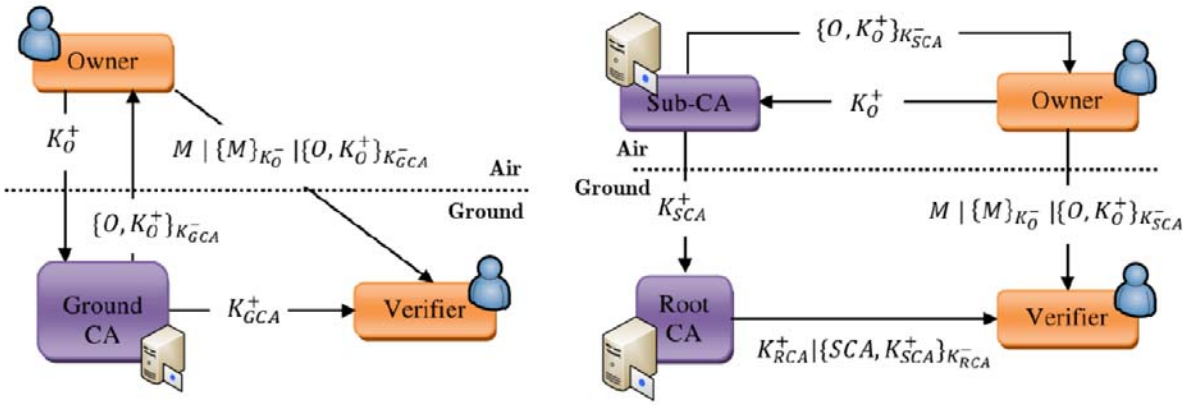


Figure 16 : architectures de PKI: référence Internet (à gauche) vs. PKI aéronautique hiérarchique (à droite)

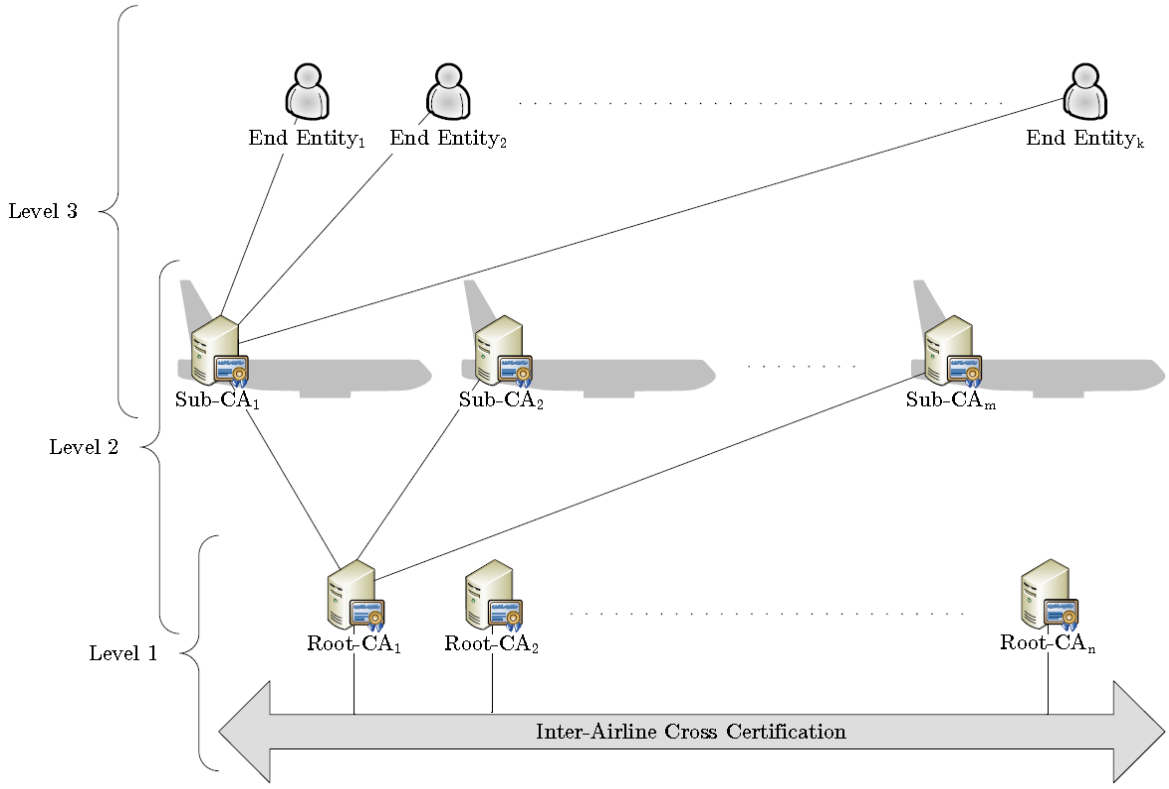


Figure 17 : PKI aéronautique hiérarchique complète comportant plusieurs racines

Tableau 4 : détails des données de vol (DSNA-DTI)

Hour of Flight	Aircraft Label	ICAO Code
08:00:12	A320	GBL5MT
11:02:54	A319	AAF421
12:42:00	A321	MON954
14:00:01	C550	FYG583B
14:30:44	A320	JET327

Evaluation de la PKI aéronautique

Pour permettre de valider cette proposition de nouvelle PKI dans un contexte se rapprochant du contexte aéronautique français, nous avons choisi d'utiliser les enregistrements des vols (différentes positions des avions au cours du temps) mis à notre disposition par le site de la DSNA-DTI (Direction Supérieur de la Navigation Aérienne – Direction de la Technique et de l'Innovation). Il s'agit de l'organisme de la DGAC chargé de la conduite des actions de recherche et développement pour l'aéronautique française. Dans ce cadre, nous avons pu récupérer plusieurs traces de trafic aéronautique réel nous renseignant sur le nombre d'avions présents dans le ciel français à un moment donné. Un exemple des données collectées pour cette étude est présenté dans le Tableau 4.

Nous avons pu en déduire dans un second temps, l'évolution du nombre d'avions et de passagers par compagnie dans le ciel français. La Figure 18 illustre l'évolution de ces données pour la compagnie Air France.

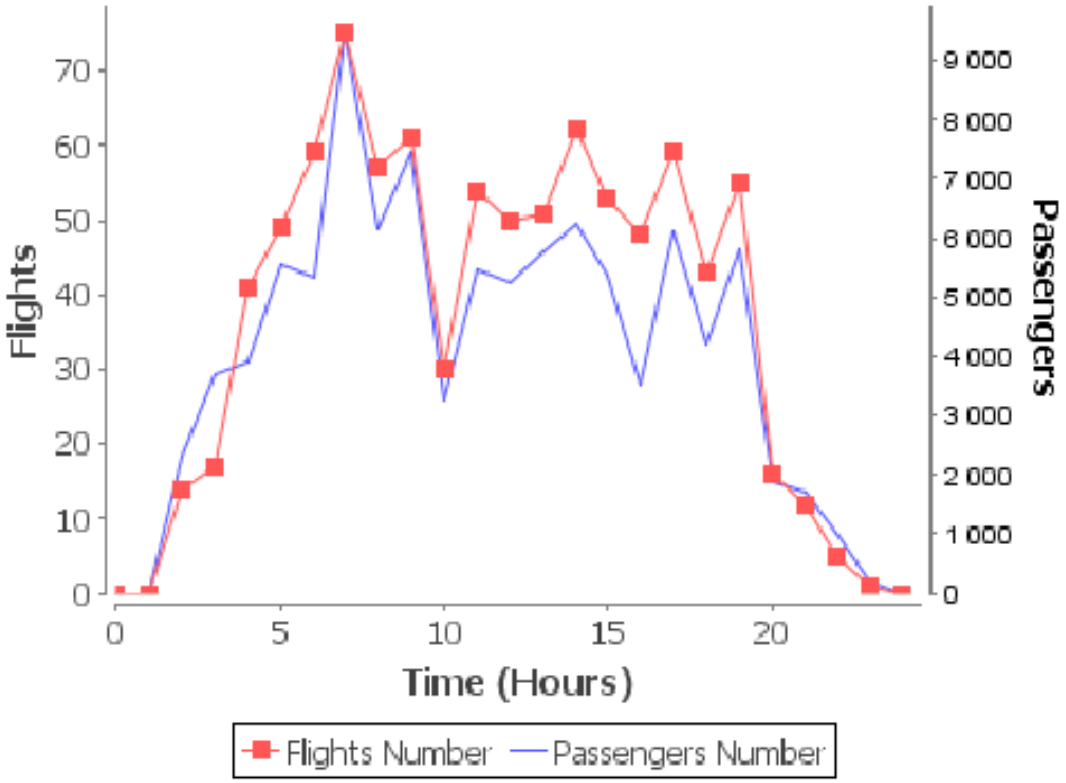


Figure 18 : statistique journalière du nombre d'avions AIR FRANCE en vol

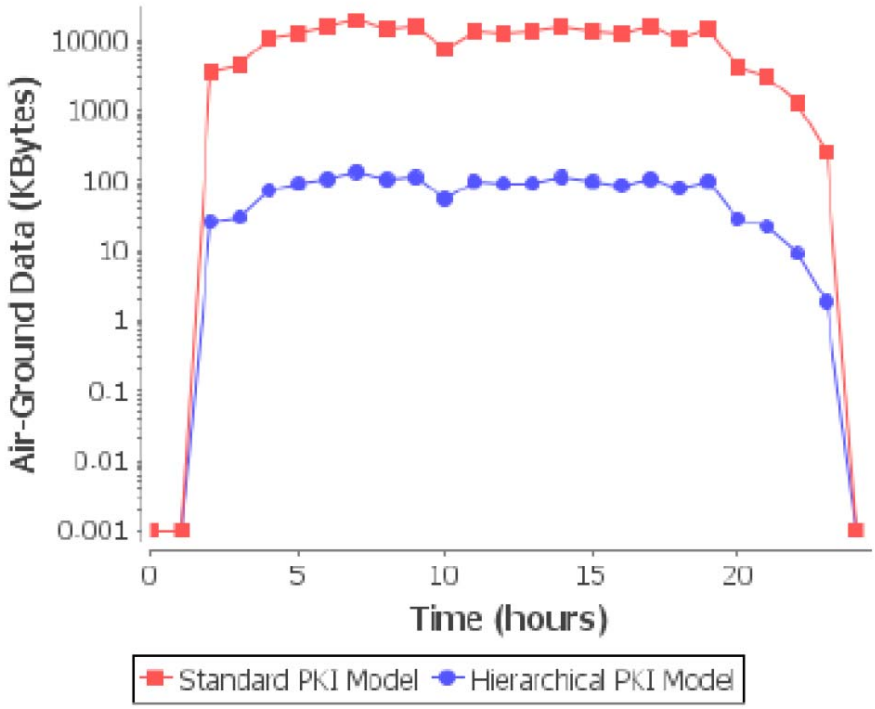


Figure 19 : utilisation des ressources du lien sol-bord

La Figure 19 permet de quantifier le volume de ressources réseau sauvegardées en utilisant cette nouvelle PKI aéronautique (cf. courbe « hierarchical PKI model » en bleue). En effet, en maximisant le nombre d'échanges entre le CA embarqué (cf. Sub-CA de la partie droite de la Figure 16) à bord de l'avion et les entités présentes dans l'avion il est possible d'alléger de façon très importante le nombre d'information qui dans une PKI traditionnelle (cf. courbe « standard PKI model » en rouge) sont échangées entre la CA sol (cf. Ground CA de la partie gauche de la Figure 16) et les entités à bord de l'avion. Il est important de noter qu'il reste toujours des échanges entre le bord et le sol (cf. Sub-CA et Root CA de la partie droite de la Figure 16) mais ces échanges sont bien moins importants que dans une PKI traditionnelle ce qui permet d'optimiser l'utilisation du lien sol-bord dans cet environnement contraint.

Ces travaux représentent ainsi un premier niveau de contribution pour traiter de façon conjointe les problématiques de sécurité et de QdS dans un même composant aéronautique et faire face aux caractéristiques spécifiques de l'environnement aéronautique. Par la suite, nous allons développer plus en détails cet aspect sécurité ainsi que la problématique de la certification de tels systèmes aéronautiques.

2.3- DE L'INGENIERIE ORIENTEE MODELE POUR LA CERTIFICATION DE SYSTEMES COMPLEXES

2.3.1- De l'intérêt des approches orientées modèles pour la conception aéronautique

Le travail de recherche initié dans le cadre du projet FAST et la thèse de Slim Ben Mahmoud a pointé du doigt le besoin de pouvoir prendre en compte, dès le départ, dans la définition de nouvelles solutions de sécurité pour le trafic aéronautique, les problématiques de certification du système final que l'on souhaite concevoir. Ainsi à l'issue du projet FAST, je me suis intéressé au processus de génie logiciel qui permettrait de pouvoir améliorer la

vitesse de développement d'un système aéronautique et le niveau de confiance que l'on pourrait avoir dans son fonctionnement (par rapport au niveau de confiance de référence que l'on peut avoir dans un logiciel développé de façon classique). En effet, aussi performant soit le module SecMan développé dans le cadre du projet FAST il serait quasiment impossible (c'est-à-dire à un coût financier acceptable) de pouvoir certifier un tel système pour une utilisation industrielle future.

Ainsi, le sujet abordé dans cette section porte sur les méthodes de génie logiciel qui permettent de concevoir et mettre en œuvre de façon efficace (vis-à-vis du temps et du coût financier) un système complexe dans un environnement où les contraintes de certification, de sécurité et de sûreté de fonctionnement sont omniprésentes. En effet, le domaine de la conception des systèmes complexes pour l'avionique est en mutation depuis la publication en 2012 des standards DO-178C et DO-331, 20 ans après la publication des versions précédentes. Ainsi, il est maintenant possible de pouvoir utiliser les techniques de prototypage rapide de système héritées du génie logiciel généraliste et de les appliquer au domaine de l'aéronautique. Ce changement des outils de conception, de développement et de validation doit s'accompagner d'un support méthodologique car l'utilisation d'approches orientées modèles pour la conception et la validation de systèmes est profondément différente de ce qui pouvait se faire jusqu'à présent dans le domaine de l'aéronautique.

2.3.2- Les techniques de validation formelle basées sur les modèles

Les modèles permettent de décrire précisément l'intégralité du comportement d'un système et de la solution logicielle qui lui est associée. Ainsi, il est possible de générer à partir de ceux-ci tout ou partie du code logiciel dans un langage intermédiaire (langage C, C++, Ada…). Mais les modèles initiaux sont aussi suffisamment précis pour vérifier et valider (ou invalider) certaines propriétés du logiciel.

Les modèles peuvent en effet permettre de vérifier à une phase précoce de la conception si un logiciel ou certaines de ses fonctions ne peuvent jamais bloquer (pas de boucle infinie indésirable), si les calculs numériques risquent d'échouer (pas de dépassement des limites matérielles de codage des entiers), si certains états ont été spécifiés mais sont inaccessibles (ces états et le code associé sont dit « morts »).

Les méthodes de vérification de telles propriétés sur les modèles sous-jacents des logiciels peuvent être classées en trois catégories, décrites ci-dessous : les méthodes de « Model Checking », de preuves formelles de théorèmes et d'assertion de code.

Quel que soit la méthode, trois résultats sont possibles en sortie de l'outil de vérification : propriété vérifiée et validée, propriété fausse (résultat potentiellement accompagné du contre-exemple ayant invalidé la propriété), propriété ni validée ni invalidée (lorsque la vérification prend trop de temps ou ne peut aboutir faute de données suffisantes).

- **Model Checking**

La première catégorie de méthodes, appelée « Model Checking », consiste à établir l'ensemble des états par lequel peut passer le programme, puis à parcourir cet ensemble pour valider la propriété à vérifier.

Un bon outil de « Model Checking » maintient ainsi l'espace d'état le plus réduit possible durant la construction pour pouvoir vérifier en un temps raisonnable les propriétés qu'on lui demande. A noter que l'aspect « raisonnable » de l'exécution de l'outil est un paramètre humain variant d'un projet logiciel à un autre, pouvant aller de l'ordre de la seconde à l'ordre du mois dans la pratique.

Les outils de « Model Checking » utilisent l'espace d'états d'une fonction. Cet espace peut être représenté sous la forme d'un diagramme UML à états-transitions. De manière réciproque, il existe des outils de « Model Checking » qui prennent en entrée un diagramme UML à états-transitions et valide les propriétés directement sur celui-ci. Ainsi, le modèle à états-transitions qui sert aux développeurs à concevoir les fonctionnalités et à générer automatiquement une partie du code source du logiciel sert aussi à valider ce code source.

- **Preuve Formelle**

Parallèlement aux méthodes de « Model Checking », le monde de la recherche universitaire s'est intéressé à un autre axe de recherche pour garantir des propriétés sur des blocs logiciels. Cet axe consiste à extraire un théorème du bloc et à valider formellement ce théorème, d'où le nom de « Preuve Formelle de Théorème » qui lui est associé.

Les preuves formelles de théorèmes sont complémentaires du Model Checking : certaines propriétés invérifiables avec l'une des méthodes sont parfois triviales à vérifier avec l'autre et vice-versa.

En interne, les algorithmes de preuves formelles sont souvent des algorithmes complexes de réécriture de la propriété pour montrer l'équivalence de cette propriété jointe aux données d'entrées avec le résultat.

D'autres approches de la preuve formelle de théorème consistent à écrire initialement les théorèmes, abstraits, puis à les raffiner de manière successive en les complétant pour arriver après plusieurs itérations au code source, concret et pouvant être compilé puis exécuté sur une machine réelle. L'outil de preuve formelle garantit alors l'équivalence du théorème avec tous les raffinements successifs. Ces approches utilisent des langages textuels tels que Coq *(Bertot, 2011)* et le langage B *(Abrial, 1996)* et sont utilisables pour le développement en aéronautique suite à la parution en 2012 du DO-333 *(DO-333, 2012)* relatif à la certification de logiciel avec des méthodes formelles. Toutefois, ces approches s'éloignent de celles appliquées dans le cadre de notre cas d'étude présenté plus loin, le routeur SNG. Ces approches sortent donc du périmètre de ce manuscrit.

- **Assertion de code**

La troisième et dernière catégorie de méthodes formelles garantissant le fonctionnement correct de logiciel aéronautique est l'assertion de code. Alors que le « Model Checking » et la preuve de théorèmes sont tous deux issus principalement des milieux académiques, les industriels leur demandèrent dans les années 1990 des solutions pour valider des codes existants sans avoir besoin de réécrire les modèles ni de recommencer le développement de ces logiciels.

La solution choisie passe par l'ajout de propriétés à valider sous forme d'annotations directement dans le code source du logiciel. Ces propriétés, inscrites dans des blocs de commentaires pour ne pas changer l'exécution du compilateur, respectent un formalisme particulier qui est reconnu par l'outil validant formellement les propriétés à vérifier. Cet outil ne modifie pas le code, les validations sont effectuées de manière statique, sans exécuter dynamiquement le code sur le système réel; la terminologie parle donc d'analyse statique du code source.

Les propriétés couramment vérifiées passent par l'ajout aux fonctions à valider de pré-conditions, de post-conditions et de clauses d'invariance, sur le modèle de la logique de Hoare définie en 1969 (Hoare, 1969). Les pré-conditions sont des données fournies à l'outil de vérification pour le guider dans son évaluation et le renseigner sur l'état de l'environnement de la fonction. De la même manière, les clauses d'invariance indiquent ce

que la fonction ne devrait pas modifier. Enfin, l'outil vérifie formellement que l'ensemble des pré-conditions, des clauses d'invariance et du code de la fonction à tester implique systématiquement l'ensemble des post-conditions. Dans le cas contraire, la propriété est invalidée et l'outil l'indique au testeur en le guidant sur les raisons de l'échec.

L'approche par assertion de code a ainsi permis aux industriels de se familiariser avec les concepts des méthodes formelles et d'intégrer plus sereinement des outils tels que ceux de « Model Checking » et de preuve de théorème. Cette approche s'inscrit comme un interfaçage entre l'informatique fondamentale développée dans les milieux académiques et l'informatique très appliquée résultant des besoins immédiats des industriels.

Ainsi, la conception, la mise en œuvre et la validation de systèmes avioniques et aéronautiques sont devenues des tâches extrêmement complexes de part l'augmentation des fonctionnalités qui sont déployées dans les systèmes avioniques actuels et la nécessité de pouvoir les certifier avant leur mise en production. Dans le cadre de nos travaux, nous avons donc proposé une méthodologie qui permet de prototyper rapidement un tel système en considérant dès le départ les aspects de certification de la solution produite. Cette méthode tire parti des approches de conception orientée modèle ainsi que de l'utilisation des méthodes formelles (principalement les outils de « Model Checking ») pour la validation de ces systèmes. De plus, l'utilisation d'outils de génération automatique de code logiciel à partir de modèles permet de réduire la phase de développement mais aussi de tests de la solution finale.

2.3.3- Projet MILSAvion : définition d'un routeur avionique sécurisé de nouvelle génération (septembre 2010 – septembre 2013)

Cette problématique a pu être abordée par l'intermédiaire d'un projet mené en collaboration avec la société Thalès Avionics à Toulouse. Dans le projet MILSAvion, il s'agissait de proposer une architecture de sécurité pour l'ensemble des communications aéronautiques qui viendrait en complément de l'architecture de sécurité utilisée dans le réseau avionique et qui permettrait de plus une interconnexion sécurisée entre le monde « avion » et le monde extérieur (réseau Internet par exemple). L'enjeu de ce travail était de prendre en compte les problématiques de standardisation adoptées dans le monde avionique, les intégrer comme pré requis et proposer une solution architecturale adaptée et compatible avec l'approche actuelle. En effet, une solution globale de sécurité intégrant le segment avion, le segment sol-bord et le segment sol n'aura de pérennité scientifique et industrielle que si elle prend en compte l'ensemble des critères de sécurité qui caractérisent les divers environnements traversés et considère dès le départ les divers principes de standardisation retenus pour ces derniers.

Ce projet m'a permis de pouvoir encadrer la thèse d'Antoine Varet dont l'objectif a été de concevoir, développer et tester en environnement réaliste un routeur sécurisé pour l'aéronautique de nouvelle génération (appelé routeur SNG dans la suite).

2.3.4- Méthodologie de développement rapide pour systèmes embarqués critiques

Dans le cadre du développement du logiciel embarqué de notre routeur SNG, certifier un routeur existant aux niveaux exigibles par les avionneurs se serait avéré très coûteux. C'est pourquoi nous avons cherché des solutions afin de développer un routeur de nouvelle génération en optimisant les coûts. Cela nous a conduit à créer une méthodologie de développement de logiciel aéronautique et à l'appliquer au cas de notre routeur SNG. Les objectifs de notre méthodologie sont la minimisation des durées de modélisation, de développement et de validation du routeur ainsi que la minimisation des efforts à fournir pour

la certification (« safety ») et l'évaluation (« security ») tout en maximisant les niveaux de « safety » et de « security » apportées par le routeur SNG.

On suppose pour pouvoir appliquer cette méthodologie que la phase de spécification logicielle a été effectuée antérieurement. Ainsi, avant d'appliquer la méthodologie, l'architecte logiciel dispose d'un ensemble d'exigences spécifiant l'ensemble des services que le logiciel doit fournir ainsi que l'ensemble des contraintes qu'il doit respecter. Dans le cas de notre routeur SNG, cet ensemble d'exigences comprend notamment des exigences concernant le routage des paquets, leur sécurisation mais aussi sur les performances attendues du système final.

La méthodologie peut être résumée par l'application successive des sept étapes suivantes illustrées par la Figure 20.

Dans un premier temps, l'architecte logiciel effectue une partition de l'ensemble des exigences : il scinde cet ensemble en différents sous-ensembles disjoints tels que l'union des sous-ensembles donne l'ensemble initial d'exigences. Chaque sous-ensemble est alors associé à ce que l'on appelle une « partition logicielle ». C'est l'étape de **partitionnement**. Dans le cadre du routeur SNG, trois partitions logicielles ont été extraites:

- les exigences de routage et de filtrage (Pfr4),
- les exigences de sécurisation des données (Pse),
- les exigences d'interfaçage du logiciel avec le matériel (Piface).

Ensuite, le comportement de chaque « partition logicielle » est représenté à l'aide de modèles graphiques de systèmes dynamiques et de machines à états. Ces modèles permettent aux développeurs de tester et valider dès la conception le fonctionnement du logiciel et de ses sous-parties. C'est l'étape de **modélisation**. Nous avons modélisé le routeur SNG à l'aide des outils Simulink *(MathWorks, 2013b)* et Stateflow *(MathWorks, 2013c)*, deux toolkits fonctionnant avec Matlab *(MathWorks, 2013a)*.

Dans un troisième temps, les modèles sont convertis en code source à l'aide d'un générateur automatique qualifié de code. C'est l'étape de **transformation**. Nous avons généré le code source en langage C du routeur SNG à l'aide de l'outil Gene- geneauto *(Toom et al., 2008)*, un transformateur de modèles en code source libre et Open-Source.

Afin de fonctionner au sein d'une cible spécifique, le code généré doit être lié à un système d'exploitation. Pour cela, du code additionnel appelé « glue code » est généré. Il contient notamment les liaisons entre les entrées/sorties du modèle et celles de la partition logicielle du système d'exploitation, ainsi que les informations d'ordonnancement des différentes partitions et le point d'entrée du code généré à l'étape précédente. C'est l'étape de **collage**. Dans le domaine de l'embarqué, certains systèmes temps-réel certifiables et évaluables existent, tels que PikeOS *(PikeOS, 2011),* commercialisé par Sysgo, que nous utilisons pour faire fonctionner les blocs logiciels du routeur SNG.

La cinquième étape est l'étape de **compilation** : les codes sources générés par les étapes 3 (transformation) et 4 (collage) sont compilés et liés ensemble en un code binaire par partition. L'usage d'un compilateur qualifié dans cette étape permet de réduire le coût de la certification du produit logiciel final.

Dans un sixième temps, l'architecte logiciel décrit la structure globale du produit logiciel en y précisant pour chaque partition logicielle le nombre d'instances devant s'exécuter simultanément, leur configuration, leur ordonnancement... Il regroupe dans une « image finale » ces informations, le noyau du système d'exploitation et l'ensemble des codes binaires de partition (générés à l'étape précédente). C'est l'étape d'**intégration**. Cette

étape est souvent simplifiée par les outils de développement fournis avec le système d'exploitation, tel que le plugin Eclipse CODEO fourni avec Sysgo PikeOS.

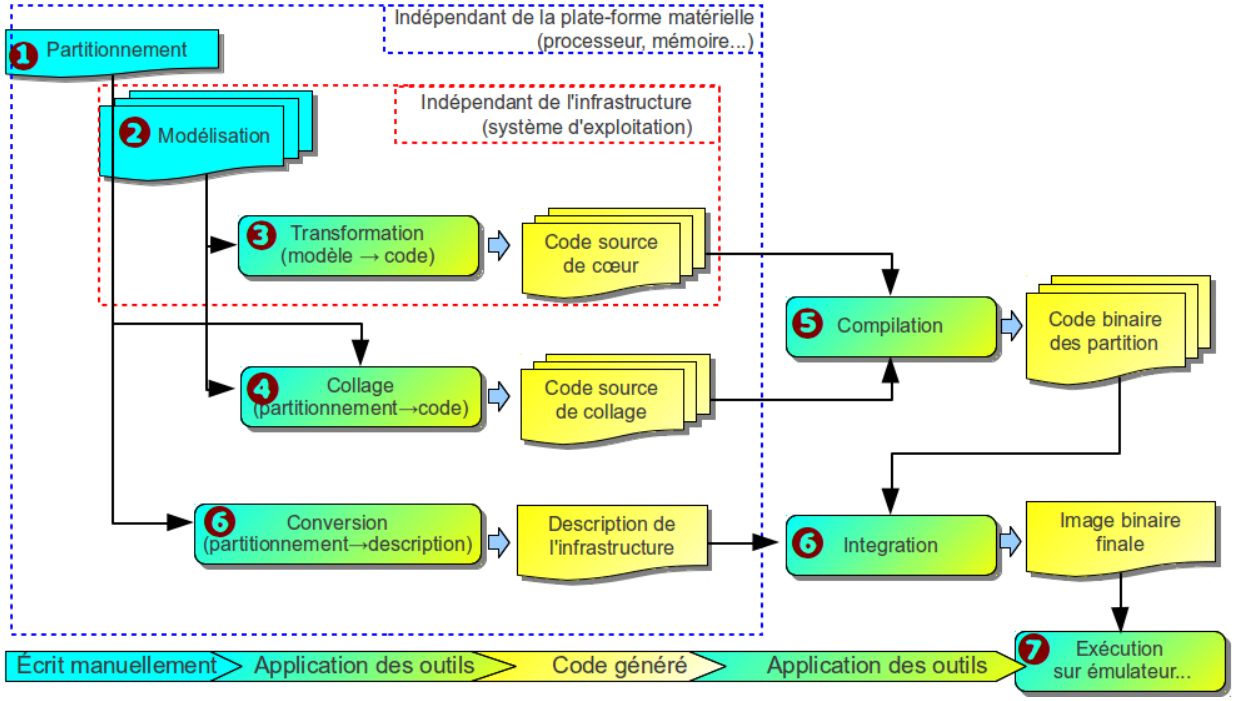


Figure 20 : méthodologie de développement orientée modèle pour les systèmes embarqués complexes

Enfin, les développeurs peuvent télécharger cette image finale sur le matériel embarqué ou encore l'exécuter à l'aide d'un émulateur afin de vérifier son fonctionnement et valider ses performances grâce, par exemple, à l'émulateur qemu-*x86 (QEMU, 2011)* : c'est l'étape d'**exécution**.

Dans cette section, nous présentions les résultats que nous avons obtenus pour le processus de développement à appliquer à un environnement logiciel embarqué complexe. Les contraintes de sûreté et de sécurité y sont critiques. Nous avons ainsi fait le choix d'un système d'exploitation (Sysgo PikeOS) compatible MILS (Multi Independant Level of Security) *(Rushby, 1981)* et IMA (Integrated Modular Avionics) IMA *(Gardise et Pighetti, 2009)*. Ces contraintes nous ont aussi poussés vers l'utilisation d'outils de modélisation pour pouvoir vérifier le système au plus tôt et vers des générateurs de codes automatisés pour éviter les fautes de traduction d'un langage de haut niveau vers des langages plus proches de notre cible matérielle embarquée. Ces outils nous ont aussi permis d'accélérer la phase de développement et de fabriquer rapidement un prototype fonctionnel pour les tests et la validation du logiciel embarqué critique (routeur SNG) que nous allons présenter dans la section suivante.

2.4- CONTRIBUTION A LA SECURISATION DU TRAFIC EN ENVIRONNEMENT AERONAUTIQUE

La thèse d'Antoine Varet qui s'adossait au projet MILSAvion nous a permis de proposer en s'appuyant sur la méthodologie de conception orientée modèle introduite précédemment un routeur de nouvelle génération pour l'avionique. Ce dernier représente un élément de contribution supplémentaire (par rapport au SecMan précédemment introduit) pour la sécurisation du trafic en environnement aéronautique.

2.4.1- Un routeur sécurisé pour la gestion du trafic aéronautique

Ce travail de thèse a reposé sur des principes de gestion de la sécurité indépendants (MILS pour Multi Independent Levels of Security) introduits récemment dans le monde avionique en complément de l'approche plus traditionnelle IMA (pour Integrated Modular Avionics). La spécificité de l'approche que nous avons suivie a été d'associer les différents niveaux de sécurité aux différents domaines de communication qui peuvent être rencontrés dans les communications aéronautiques (ATC, AOC ou APC). L'utilisation de la technologie MILS a permis de proposer une nouvelle génération de routeur embarqué (routeur « nouvelle génération ») permettant de multiplexer de façon sûre et sécurisée l'ensemble des communications sur un lien sol-bord unique tout en gérant leur spécificité et notamment leur différent niveau de criticité. Par exemple, la ségrégation entre des flux de niveaux de criticité différents sera garantie au même titre que l'impossibilité d'écouter des flux de trafic dont on ne serait pas le propriétaire.

La solution architecturale proposée dans ce travail repose principalement sur un composant central de routage, de filtrage et de sécurisation des flux de données aéronautiques. Grâce à la méthode d'ingénierie logicielle orientée modèle présentée précédemment, un travail de conception et de développement a pu être mené. Cela a abouti à la proposition d'un composant avionique central appelé Routeur Sécurisé de Nouvelle Génération (routeur SNG). Les fonctionnalités mises en œuvre par le routeur SNG sont résumées dans la Figure 21.

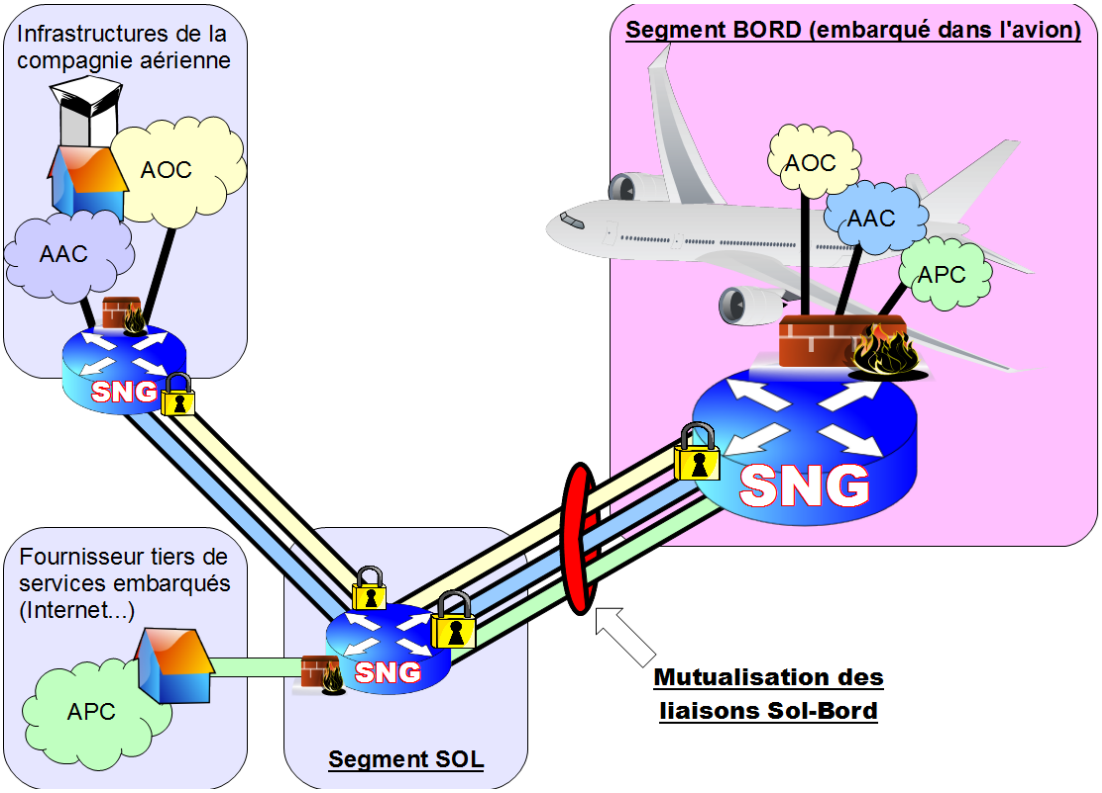


Figure 21 : exemple de déploiement du routeur SNG dans le contexte aéronautique

De plus, cette approche a permis d'étendre les principes de sécurité traditionnellement considérés dans le réseau avionique aux différents réseaux extérieurs. Ce travail a été rendu possible par la définition de nouveaux « middlewares » de communication sécurisés (de type « partitioning communications system » par exemple) qui se sont positionnés en complément des solutions MILS de définition des systèmes communicants.

Ce travail s'est traduit par une phase de validation formelle des solutions protocolaires proposées (des méthodes de « model-checking » ont été utilisées dans ce

contexte). En effet, les critères de certification dans le monde aéronautique sont très stricts et tout logiciel (système ou réseau) embarqué doit au préalable avoir fait l'objet d'une validation complète et formelle de l'ensemble des cas d'exécution qui pourrait l'amener à la faute. Il en va de même pour l'ensemble des scénarios qui pourrait occasionner une attaque de ces systèmes par un tiers malintentionné. Ainsi, afin de traiter du problème de la certification des solutions proposées, des méthodes de validation formelle ont été utilisés pour permettre la prise en compte des besoins spécifiques de certification et de validation des communications aéronautiques entre le (ou les) réseau(x) « avion » et le reste du monde. Ces méthodes ont été en particulier utilisées sur les modèles de haut niveau (Simulink et Stateflow) proposés lors de la phase de conception

Les différentes étapes du travail de thèse ont été :

- Expression du besoin de sécurité et analyse de risque du système à concevoir (routeur « nouvelle génération ») ;
- Design de l'architecture du système dans le contexte MILS ;
- Ecriture du code logiciel pour les différentes entités du système (principalement les fonctions de routage, filtrage et qualité de service) dans le contexte MILS ;
- Validation formelle du fonctionnement de différentes entités logicielles du système ;
- Réalisation d'une maquette du routeur « nouvelle génération » intégrant les différentes entités du système par l'intermédiaire d'une plateforme commerciale MILS (solution retenue Sysgo PykeOS).

- **Architecture logicielle détaillée du routeur SNG**

Le routeur doit assurer plusieurs fonctions, illustrées au travers de la Figure 21. Le routeur doit filtrer et router les paquets IPv4 et IPv6 entre ses différentes interfaces réseau. Ces fonctions « routage» et «filtrage» forment le premier groupe de fonctionnalités.

Ensuite, le routeur doit pouvoir assurer la sécurité des communications en garantissant la confidentialité et l'intégrité des échanges via des canaux sécurisés, après avoir authentifié les nœuds d'extrémités de ces canaux. Pour limiter une prolifération de canaux sécurisés peu utilisés et donc un gaspillage des ressources réseaux, le routeur peut être configuré pour mutualiser ces canaux et ainsi sécuriser plusieurs flots de données dans un même canal. Le deuxième groupe de fonctionnalités est constitué de ces fonctions de multiplexage et de sécurisation des données.

Un troisième groupe de fonctionnalités est relatif au contexte avionique pour lequel est destiné le routeur. En effet, les interfaces réseau du routeur sont des interfaces AFDX, donc des interfaces Ethernet auxquelles certaines exigences fonctionnelles ont été ajoutées pour garantir un meilleur déterminisme.

Enfin, les exigences non fonctionnelles telles que la sûreté et la sécurité du système « routeur SNG » concernent tout le système et toutes les fonctionnalités. Bien que formant un quatrième groupe, elles impactent toutes les autres fonctionnalités et les processus de conception et de mises en œuvre. Elles ne se traduisent pas forcément par du code ou des modèles et sont donc traitées d'un point de vue méthodologique.

La Figure 22 présente l'architecture du routeur SNG. Celle-ci formalise et « fige » la décomposition des fonctionnalités en trois classes, détaillées ci-dessous. Cette décomposition fonctionnelle préconisée dans la première étape de notre méthodologie permet de se concentrer pour chaque classe sur le sous-ensemble de fonctions à modéliser en faisant abstraction des sous-ensembles associés aux autres classes, ce qui permet de simplifier la modélisation.

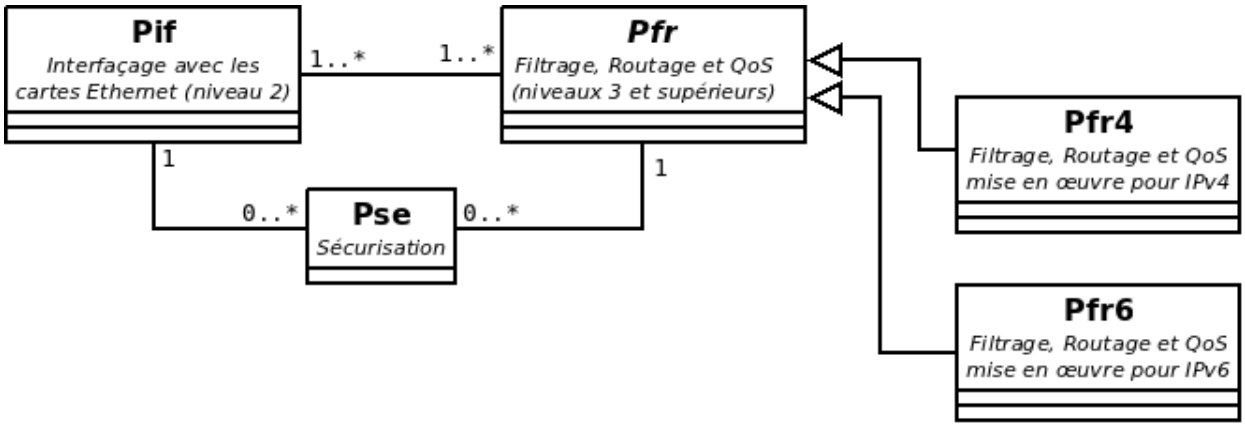


Figure 22 : diagramme de classes du routeur SNG

La classe Pfr est associée aux fonctionnalités de routage et de filtrage des paquets, elle est donc fortement liée au protocole de niveau réseau. Étant donné que le routeur est destiné à interagir avec le protocole IPv4 mais aussi avec le protocole IPv6, deux variantes ont été modélisées, l'une pour IPv4 appelée Pfr4 puis son dual Pfr6 pour le protocole IPv6.

Ces deux classes Pfr4 et Pfr6 présentent une interface commune vis-à-vis des autres classes de partition du système. Ainsi, la classe de partition abstraite Pfr définit une interface commune liant les entrées et sorties de la classe de partition de routage et de filtrage Pfr avec celles de la classe de partition d'interfaçage Piface présentée plus loin. Le mécanisme d'héritage est utilisé pour dériver les deux classes Pfr4 et Pfr6 de la classe-mère abstraite Pfr ; ces deux classes héritent donc d'une interface d'entrées/sorties unifiée.

Cependant, bien qu'IPv6 soit spécifié comme le remplaçant d'IPv4, ces protocoles sont trop différents pour mutualiser les mises en œuvre des classes Pfr4 et de Pfr6. L'héritage n'a donc pas été utilisé ici pour mutualiser plus encore la conception de ces deux classes de partition.

La classe Piface permet de lier les classes gérant les données (Pfr4 et Pfr6) aux entrées/sorties matérielles. Cette liaison consiste en pratique à réceptionner les trames Ethernet reçues par les cartes réseau, à désencapsuler les données de ces trames et à les transmettre à la classe adaptée (une instance de Pfr4 pour les paquets IPv4, une instance Pfr6 pour les paquets IPv6 ou encore rejeter les trames invalides et de protocoles inconnus). Cette liaison est bidirectionnelle, c'est-à-dire que Piface assure aussi l'émission des paquets IP sur le réseau physique.

La Figure 23 illustre le lien qui existe entre les différents outils qui ont été présentés dans la section 2.3.4 relative à la méthodologie de prototypage rapide. Les diagrammes Simulink et Stateflow permettent d’avoir une modélisation de haut niveau des fonctions de la partition Pfr4. La représentation à l’aide de ces modèles permet de tirer parti des fonctions de « Model Checking » disponibles dans les applications Simulink et Stateflow afin de vérifier que les modélisations ne comportent, par exemple, ni exécution bloquante ni code mort.

L'approche graphique des modèles utilisés avec notre méthodologie est synthétique et complète. En effet, l’intégralité de l'algorithme de routage présenté Figure 24 tient sur une page. Notre approche permet ainsi une relecture de modèle rapide. Dès lors, le modèle de la Figure 24 résume visuellement l'ensemble des cas de routage de paquets et des traitements effectués pour le système SNG.

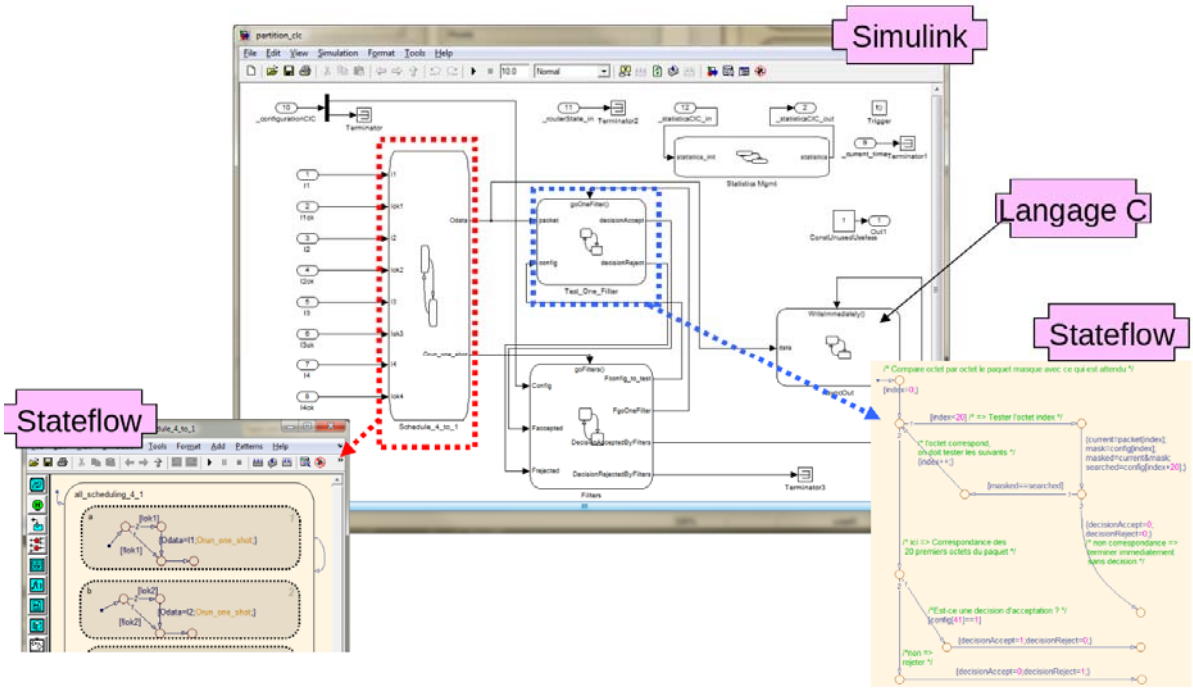


Figure 23 : modélisation de la classe Pfr4 du routeur SNG à l'aide de diagrammes Simulink et Stateflow

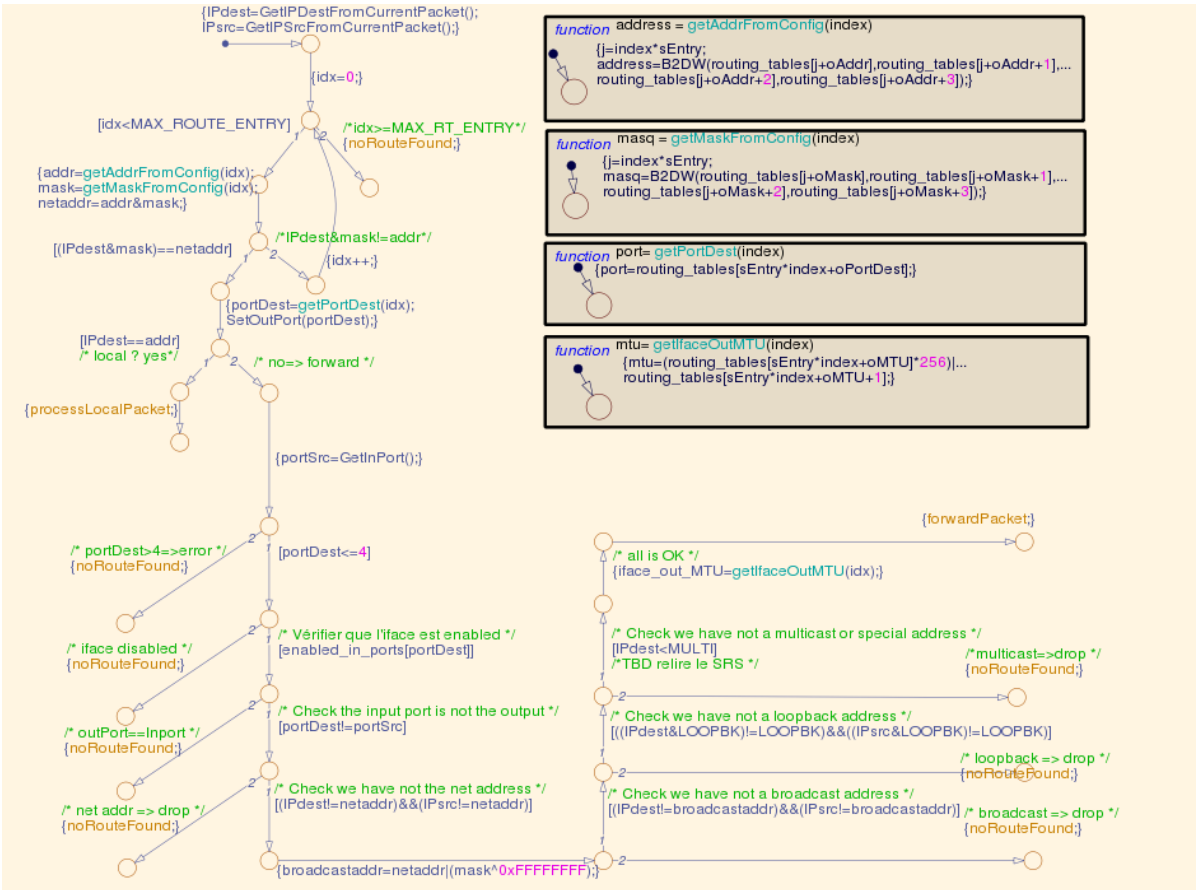


Figure 24 : diagramme à états-transitions de routage des paquets IPv4

Enfin, les fonctionnalités spécifiques à la sécurisation des données par le routeur sont mises en œuvre par une classe de partition dédiée, la classe Pse (« Partition de SÉcurisation »).

Le protocole IKEv2 a été mis en œuvre par des modèles Simulink et Stateflow pour le routeur SNG. Bien que des modèles formels aient déjà été utilisés pour valider la spécification ou le code source du protocole, à notre connaissance, c'est la première fois que ce protocole est mis en œuvre par l'intermédiaire d'une approche orientée modèle.

Ces modèles permettent de contrôler la mise en œuvre dès le stade de conception, pour s'assurer notamment de l'absence de blocage et prouver ainsi la terminaison des algorithmes. L'automatisation de la chaîne de transformation et de compilation, du modèle au code source puis au code binaire, apporte des garanties de conformité du code binaire vis-à-vis des spécifications du protocole. De plus, cela limite les phases d'évaluation et de certification à la validation des modèles et des transformateurs, évitant d'avoir à valider le code source intermédiaire complexe.

L'ensemble des classes de partition communiquent via des associations représentées sur le diagramme de classe de la Figure 22. Ces associations se traduisent à la mise en œuvre par des files de messages («Message Queues»), gérées par le système d'exploitation compatible IMA. Nous avons choisi arbitrairement d'utiliser des files dimensionnées à 1 message maximum par file avec un ordonnancement de processus par priorité statique préemptif pour que les instances de la classe Pfr soient prioritaires sur les instances de la classe Pif. Ainsi, les paquets sont traités dès leur arrivée par la partie logicielle du routeur SNG et mis éventuellement en attente dans la file d'attente matérielle de la carte Ethernet (cette dernière étant imposée à 256 trames Ethernet par le constructeur). Ces choix permettent de valider les exigences du routeur SNG, comme démontré dans la sous section suivante.

- **Résultats de l'évaluation des performances du routeur SNG**

Le logiciel embarqué produit à partir de la méthode de prototypage rapide présentée précédemment a été testé dans un environnement aéronautique émulé et confronté à du trafic aéronautique réaliste.

Les performances globales du système SNG sont résumées dans la Figure 25. Les deux paramètres principaux que nous avons considérés pour ce type de système embarqué sont la capacité globale minimum de traitement offerte par le routeur et le délai maximum de traitement qu'il induit pour chaque paquet qu'il transmet. Ce système a été stressé par l'intermédiaire du modèle de trafic présenté dans la section 2.2 qui permet de générer du trafic aéronautique réaliste pour l'ensemble de ses composantes : ATSC, AOC+AAC et APC.

La Figure 25 illustre sur sa partie gauche que la capacité globale minimum de traitement du routeur SNG se situe autour de 48 Mbps. Ce débit est suffisant pour permettre de transmettre les trafics générés par l'intermédiaire des technologies actuelles disponibles dans l'industrie aéronautique pour transférer les informations de l'avion vers la station sol. Cela signifie que notre système est capable de supporter les caractéristiques de l'ensemble des systèmes de communication aéronautique actuels ainsi que les évolutions à venir en matière d'interconnexion entre l'avion et les différents services sols disponibles.

De plus, en analysant la métrique délai maximum de traitement, nous pouvons observer sur la partie droite de la Figure 25 le routeur SNG induit un délai bien inférieur à tous les systèmes de communication air-sol avec lesquels il pourrait être interfacé. En effet, le routeur SNG induit un délai maximum de traitement d'une milliseconde alors que les recommandations des communications air-sol spécifient un délai minimum d'acheminement situé dans l'intervalle [100 ms ; 1 s] pour la plupart des services aéronautiques (voir pour détails *(COCR, 2007)*).

Pour conclure sur ces résultats d'évaluation des performances du routeur SNG, nous pouvons affirmer que la méthode de prototypage rapide orientée modèle présentée dans ce papier permet d'atteindre les objectifs de performances recherchés par les systèmes embarqués aéronautiques actuels et futurs. D'autre part, comme cela a été mentionné dans les sections précédentes, l'amélioration des performances du système final s'accompagne également d'un raccourcissement du temps de développement de ce système par rapport aux méthodes d'ingénierie logicielle traditionnelle. Ce gain de temps repose sur l'utilisation de méthodes de vérification à partir des modèles et sur l'intégration d'outils certifiés permettant d'autogénérer le code pour le système final. Cette utilisation permet ainsi aux développeurs de s'affranchir d'un grand nombre de tests unitaires longs et fastidieux et de privilégier à la place des méthodes de vérification formelle.

La thématique abordée au travers de ces travaux de recherche a donc concerné la définition d'une architecture de sécurité et de communication pour un routeur de nouvelle génération permettant l'échange des communications sol-bord dans le contexte aéronautique. Ce travail constitue une contribution supplémentaire à la thématique de la gestion de la QdS et de la sécurité dans les environnements contraints. Ce travail vient en complément du travail présenté au travers du projet FAST, il permet en particulier d'ajouter un volet méthodologique pour la partie conception et contribuer également à la mise à la disposition de la communauté d'un système de communication sécurisé certifiable (routeur SNG) pour l'aéronautique.

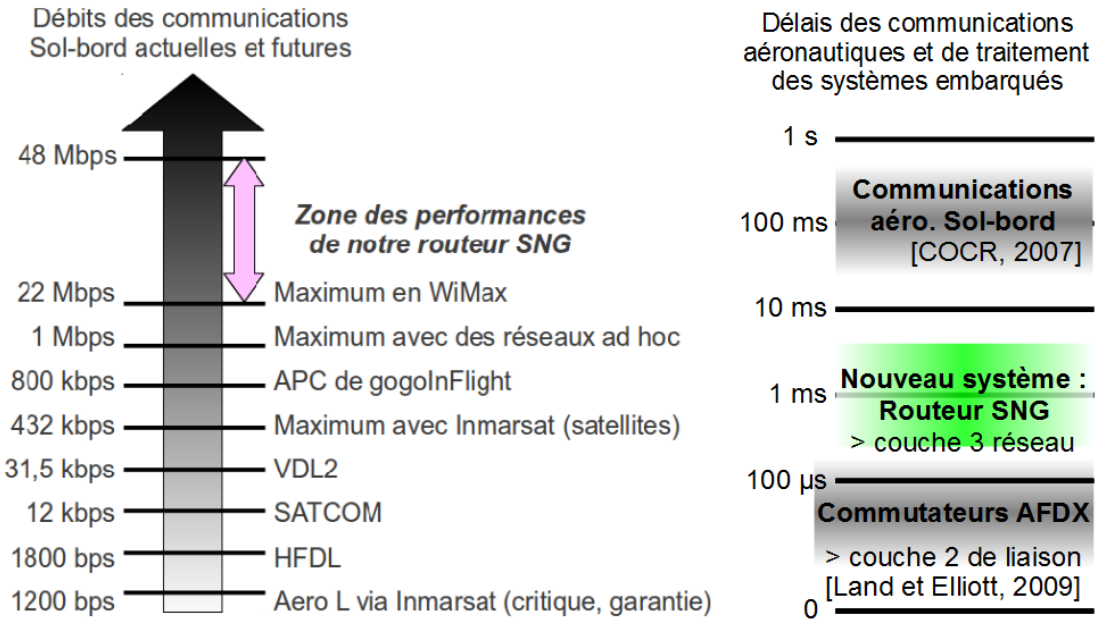


Figure 25 : performances globales du système SNG

Les résultats de ces travaux de recherche ont intéressé l'éditeur anglo-saxon ISTE Wiley qui, après étude par son comité de sélection scientifique, a accepté de publier ces travaux dans l'ouvrage référencé *(Varet & Larrieu, 2014b)*. Cet ouvrage est en cours de finalisation au moment où nous finissons la rédaction de ce manuscrit d'HDR et sera disponible à la fin du premier semestre 2014.

Ce travail n'est néanmoins pas suffisant pour traiter de l'ensemble des problématiques liées à la sécurisation dans les environnements contraints. C'est pour cela que nous allons maintenant présenter un autre volet de notre contribution à ce domaine : la

définition d'une méthode quantitative d'analyse de risque pour les environnements aéronautiques.

2.4.2- Analyse de risque quantitative pour les environnements aéronautiques

Ce travail s'adosse à un projet européen, SESAR[13] (Single European Sky for Atm Research) dont la vocation est de proposer une solution complète et intégrée pour la gestion du trafic aérien dans le ciel européen. Différents axes de recherche sont abordés au travers de ce projet. Je suis investi dans des activités de définition de l'architecture de communication du projet SESAR mais aussi dans la définition des mécanismes de sécurité pour cette architecture.

Dans le cadre du projet européen SESAR, j'ai été amené à diriger les activités de deux groupes de travail pour le laboratoire TELECOM/ResCo de l'ENAC.

- **Projet européen SESAR WP SESAR 15.2.7 : système AeroMACS (débuté en janvier 2010)**

Depuis janvier 2010, tout d'abord dans le cadre de la thèse de Slim Ben Mahmoud puis à l'issue de sa soutenance dans le cadre d'un contrat de post doctorat de 18 mois, nous avons été amenés à travailler sur le futur système de communication sans fil utilisé dans les aéroports pour faire communiquer avions, véhicules au sol, tour de contrôle et compagnies aériennes. Ce système fortement dérivé du système WIMAX a tout de même nécessité des ajustements en termes de mécanismes de sécurité pour permettre d'éviter tout comportement malicieux de la part d'un usager du système ou d'un pirate potentiel.

Pour cela, nous avons été amenés à définir une méthodologie d'analyse de risque quantitative qui nous a permis de faire des recommandations sur les fonctions et les suites logicielles à déployer dans la configuration finale de façon à minimiser le niveau de risque d'un point de vue sécurité pour les utilisateurs du système. Les travaux sont en cours de finalisation et de standardisation auprès de deux organismes : Eurocontrol et l'OACI (International Civil Aviation Organization).

- **Projet européen SESAR WP SESAR 15.2.4 : architecture de communication de bout en bout pour les communications aéronautiques (débuté en septembre 2013)**

Le travail réalisé dans le cadre du 15.2.7 est une sous partie d'un projet plus vaste qui consiste à développer une architecture de communication pour l'ensemble des phases de vols d'un avion. Ainsi, le sous-projet 15.2.4 s'intéresse aux différents segments de la communication sol bord : AeroMACS[14], L-DACS[15] (pour les communications continentales) et satellite (pour les communications océaniques). L'objectif de notre travail est de réaliser, dans un premier temps, une analyse de risque sécurité pour l'ensemble des segments de communication présentés précédemment et, dans un deuxième temps, de faire des recommandations sur les mécanismes de sécurité à déployer pour offrir une continuité du service de bout en bout.

Ce travail se complète par des aspects en rapport direct avec la définition d'une architecture de communication car il est nécessaire de pouvoir déployer des services de « hand off » entre segments de communication hétérogènes mais aussi des services de

[13] Site web du projet SESAR : http://www. Sesarju.eu
[14] AeroMACS : Aeronautical Mobile Airport Communications System
[15] L-DACS : L-band Digital Aviation Communications System

gestion de la qualité de service de façon à pouvoir prioriser et véhiculer différents types d'informations aéronautiques qui n'ont pas nécessairement la même importance.

Ce travail a débuté en septembre 2013 sous la forme d'un deuxième contrat de post doctorat pour Slim Ben Mahmoud et devrait s'achever fin 2015.

- **Définition d'une méthode d'analyse de risque quantitative pour le système AeroMACS**

Etat de l'art des différentes méthodes d'analyse de risque SSI (Sécurité des Systèmes d'Information)

Il existe deux grandes familles de méthodes d'analyse de risque : les méthodes qualitatives (principalement utilisées pour la gestion de la sécurité informatique et réseau en entreprise) et les méthodes quantitatives (développées la plupart du temps par la communauté recherche en sécurité). Les méthodes qualitatives (dont les principales sont listées dans le Tableau 5) permettent une évaluation du niveau de risque mais nécessite une expertise de la part de l'utilisateur de la méthode pour pouvoir, positionner le niveau de risque pour une menace donnée au sein d'une échelle de risque prédéfinie. A titre d'exemple, considérons une échelle de risque comportant trois niveaux : faible, moyen, grand. Dès lors, deux menaces obtenant le même niveau de risque (par exemple niveau moyen) ne sont pas directement différentiables en terme d'impact pour la sécurité globale du système d'information (SI).

Tableau 5 : principales méthodes d'analyse de risque utilisées pour la SSI

Standards and Methods	Security oriented	Risk oriented	Aeronautical oriented	Quantitative based approach
CRAMM	✓	✓	×	≈ ✓
OCTAVE	✓	✓	×	×
EBIOS	✓	✓	×	×
MEHARI	✓	✓	×	×
CORAS	✓	✓	×	×

C'est pour cette raison qu'un grand nombre de travaux ont été menés pour définir des algorithmes permettant de définir de façon automatique et avec précision le niveau de risque global auquel un SI est exposé. C'est l'objectif de toute méthode d'analyse de risque quantitative. Nos travaux se positionnent dans cette mouvance et se propose d'intégrer un concept spécifique, la propagation du risque, dans un domaine pour lequel aucun travaux n'ont été menés : les architectures réseaux aéronautiques.

Pour cela, nous avons étudié les différents travaux qui ont utilisé le concept de propagation du risque pour les réseaux traditionnels (principalement les réseaux d'entreprises et le réseau Internet) (Frigault & Wang, 2008) (Kondakci, 2010) (Zhang et al., 2004) (Yau & Zhang, 1999) et nous nous sommes intéressés à l'application de ce concept pour les réseaux spécifiques aéronautiques.

Principes de l'analyse de risque quantitative

Ainsi, dans le cadre du projet SESAR 15.2.7 nous avons été amenés à définir une méthodologie d'analyse de risque quantitative. Cette méthodologie repose sur l'utilisation du concept de propagation du risque au sein d'un réseau (ce concept est illustré au travers de

la Figure 26). Ce concept permet de modéliser les attaques complexes qui utilisent successivement plusieurs vecteurs d'attaque pour pénétrer le système cible final.

En modélisant les différentes relations qui existent entre les entités du réseau et en introduisant cette notion de propagation du risque entre ces dernières lors de la réalisation d'une attaque, nous avons pu quantifier le niveau de risque global auquel s'expose le SI dans son ensemble. L'algorithme que nous avons défini pour réaliser cette évaluation est présentée dans l'ouvrage *(Ben Mahmoud et al., 2013)* et dans la publication *(Ben Mahmoud et al., 2011b).* Etant donné le caractère volumineux de la présentation de la démonstration de cette méthodologie et des algorithmes de calcul associés, nous avons jugé inutile de mettre l'intégralité de la démonstration dans le corps de ce manuscrit. Les principaux résultats de cette démonstration sont présents en annexe A du manuscrit. Le lecteur souhaitant obtenir plus de détails peut également se référer aux références précédentes.

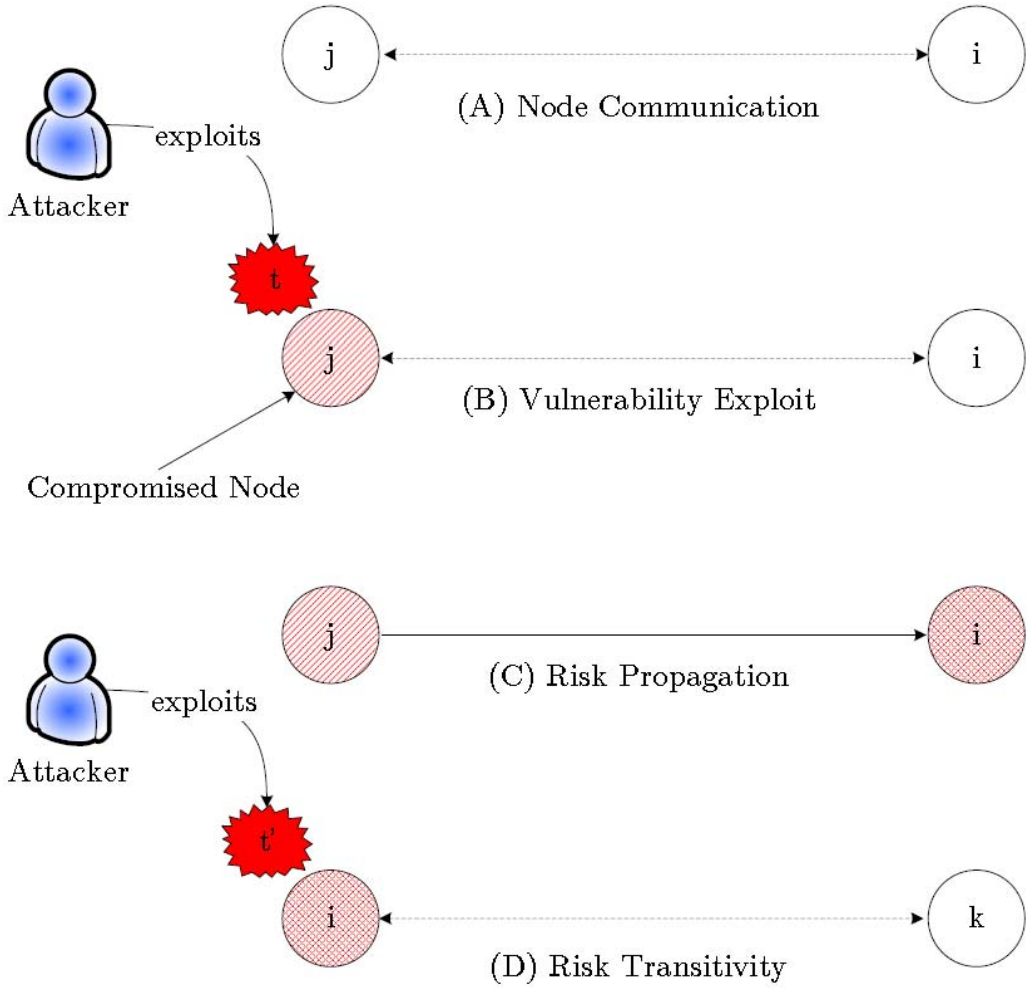


Figure 26 : principe de la propagation du risque entre deux nœuds

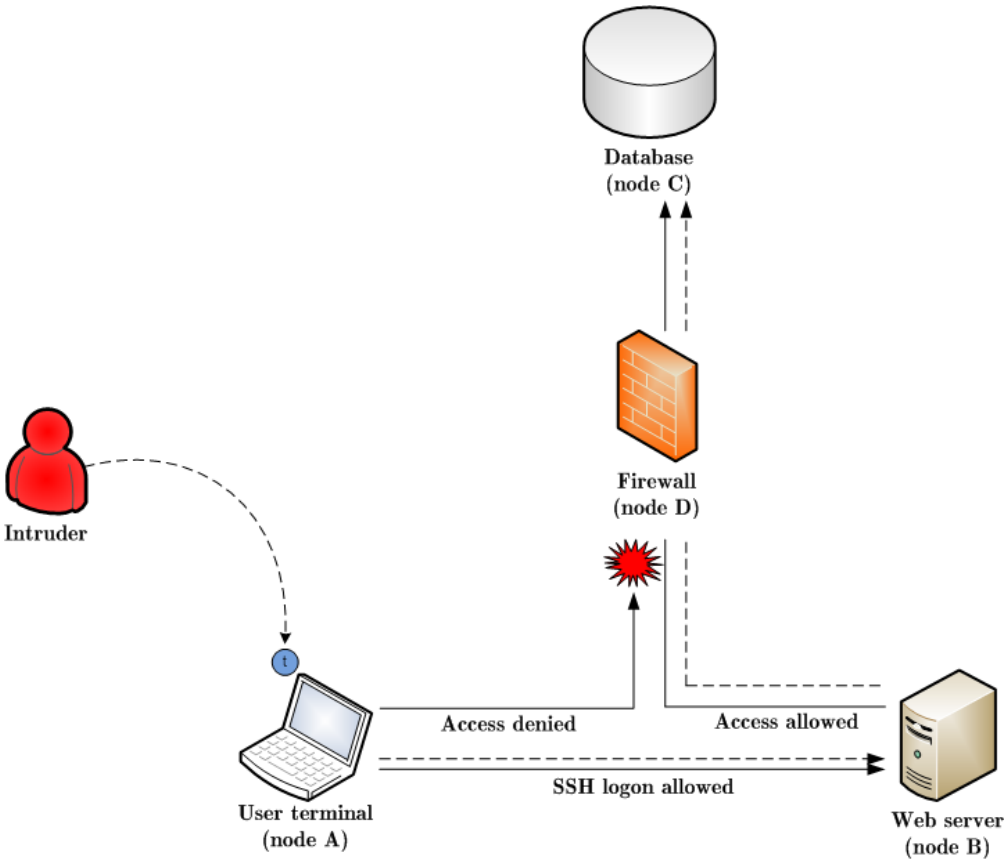


Figure 27 : exemple de scénario d'attaque

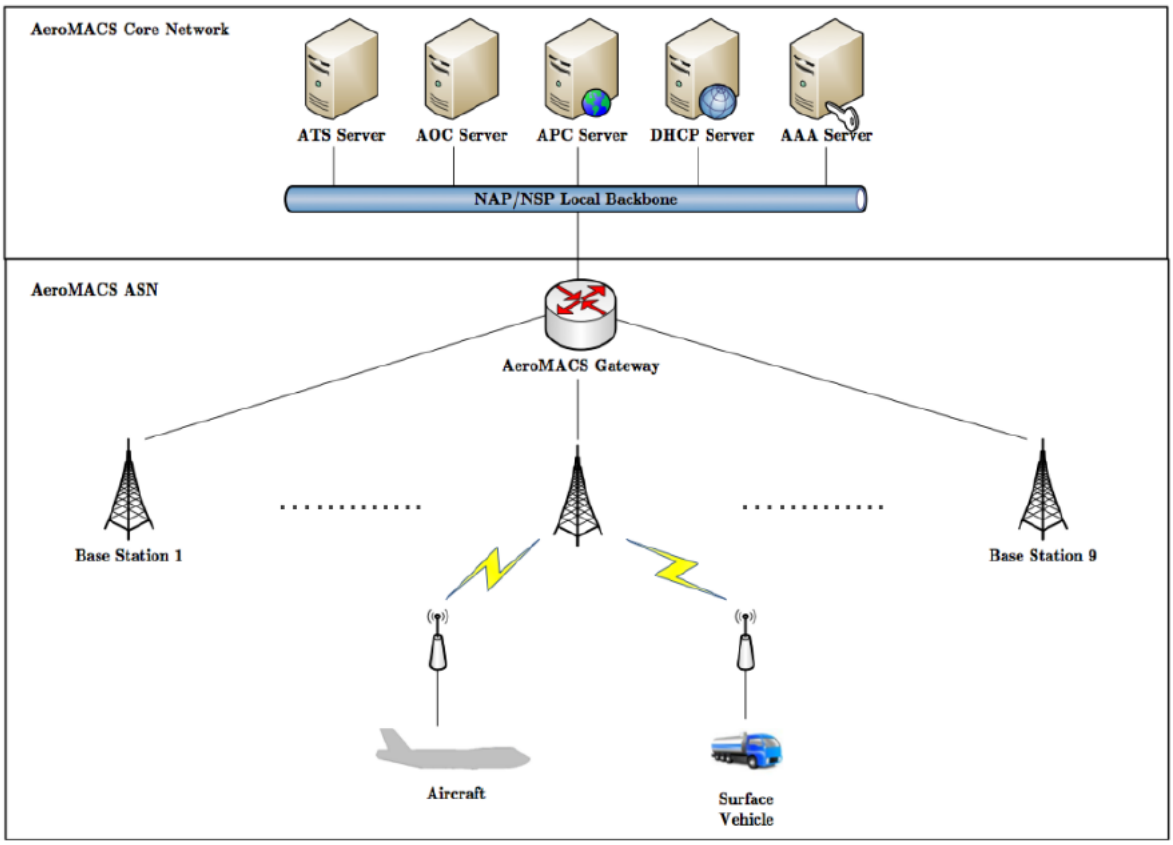


Figure 28: topologie du réseau AeroMACS (topologie #1)

Utilisation de la méthode d'analyse de risque quantitative pour augmenter le niveau de sécurité du réseau AeroMACS

En s'appuyant sur ce concept de propagation du risque, nous pouvons définir différents scénarios d'attaque reposant sur la notion de propagation du risque en rapport avec la plateforme AeroMACS qui nous intéresse précisément dans ce projet. Un exemple de scénario d'attaque est présenté dans la Figure 27. Dans ce dernier, le nœud vulnérable C n'est pas directement attaquable depuis la machine A en raison de la politique de sécurité et des règles de sécurité configurées sur le coupe-feu du nœud D. Néanmoins, l'attaquant en réalisant, dans un premier temps, une intrusion sur le système distant B, peut, dans un deuxième temps, accéder à la machine cible C ; la politique de sécurité étant plus permissive pour le nœud B que pour le nœud A. Dès lors, l'attaque a pu avoir lieu en se propageant du nœud A au nœud B, puis du nœud B au nœud C. Notre méthodologie rend possible la modélisation de ces scénarios d'attaque complexes et permet d'estimer le niveau de risque auquel s'expose les différentes entités du réseau dans le cas de ces attaques.

Notre travail a porté spécifiquement sur l'analyse du futur réseau AeroMACS (la Figure 28 présente une topologie générale de ce système). A l'aide de la méthode d'analyse de risque que nous avons définie dans le cadre de ces activités, nous avons été capables de lister les différentes vulnérabilités présentes dans ce système, de les quantifier, et de déduire à l'aide des résultats de calcul du niveau de risque que nous avons obtenus, une architecture alternative permettant de diminuer le niveau de risque du système final et atteindre le niveau requis pour un déploiement opérationnel.

La proposition de cette architecture alternative (plus robuste aux attaques et offrant un niveau de risque global plus faible) s'est faite en isolant les entités du réseau concentrant le plus haut niveau de risque et en les remplaçant, par d'autres entités moins sensibles aux mêmes attaques comme l'illustre la Figure 29. L'isolation de ces entités a été rendu possible en analysant les résultats de notre méthode d'analyse de risque qui donne pour chaque entité sa contribution au niveau de risque global de l'architecture que l'on souhaite sécuriser.

En effet, nos différents calculs ont démontré que l'entité possédant le plus haut risque de compromission (i.e. avec le niveau de risque le plus élevé dans le réseau) est la passerelle AeroMACS (« AeroMACS gateway » dans la Figure 29). Il s'agit du point de passage obligé pour le trafic échangé entre les véhicules de surface, les avions et les réseaux privés aéronautiques (type AAC ou AOC). Dès lors, elle représente l'entité la plus sujette aux attaques réseaux et pour laquelle le niveau de risque s'est retrouvé le plus haut dans notre méthode de calcul (cf. niveau = 1.875 pour la passerelle dans la topologie initiale de la Figure 30). En appliquant notre méthodologie, nous avons donc décidé de dupliquer cet équipement en le remplaçant par deux équipements de constructeurs différents. Cela a eu pour conséquence de mécaniquement diminuer la probabilité de réalisation d'une attaque pour chacun des nouveaux équipements et de plus en choisissant les équipements affichant le moins de vulnérabilités réseaux connues de diminuer également le niveau risque de la passerelle (cf. Figure 30, niveau = 0.451 pour la passerelle de la nouvelle topologie présentée Figure 29).

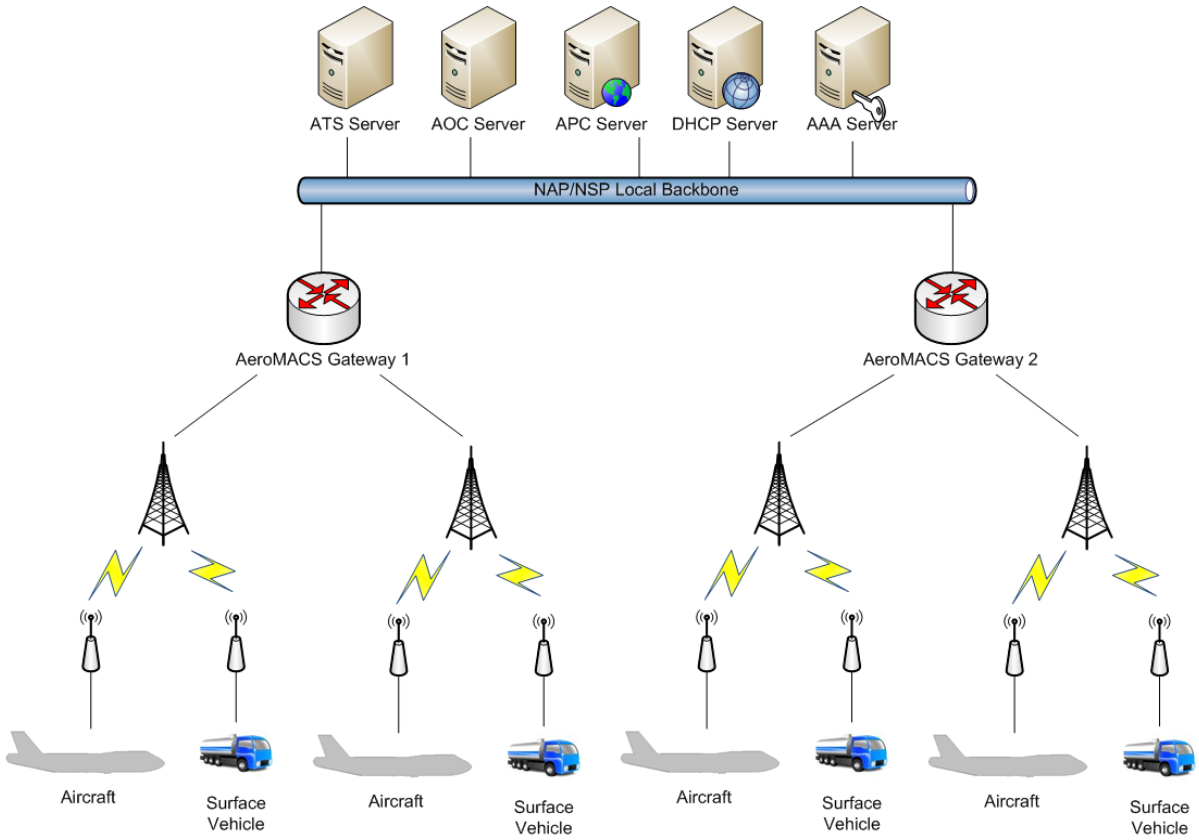


Figure 29 : proposition d'évolution de la topologie réseau AeroMACS (topologie #2)

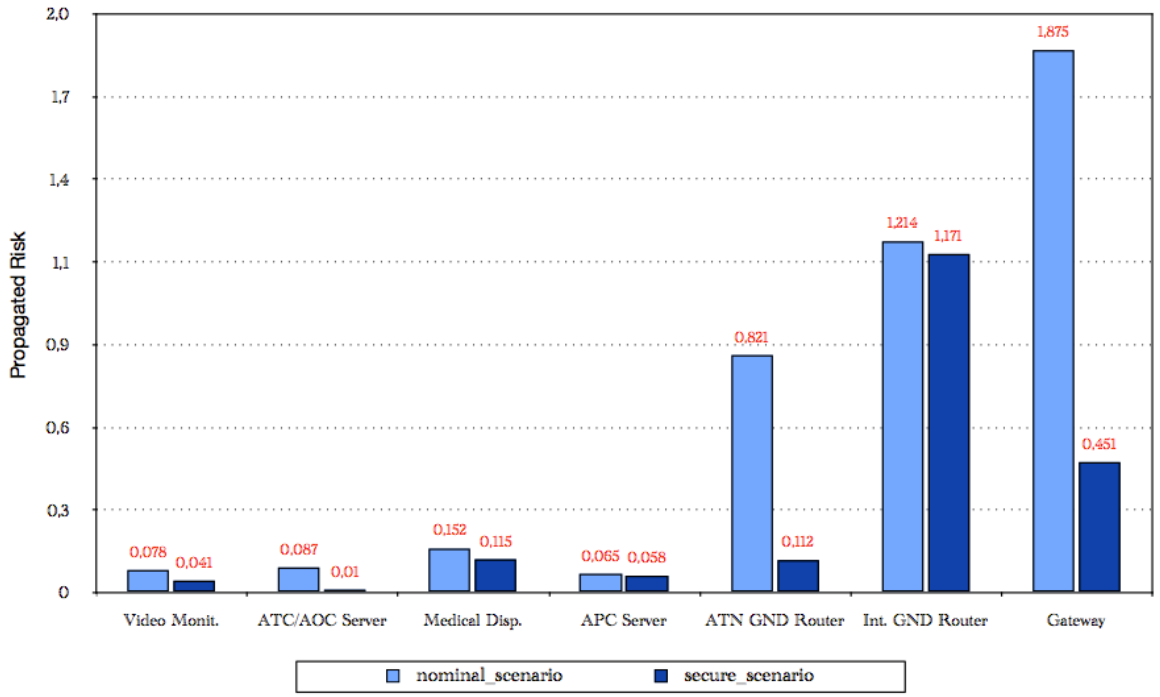


Figure 30 : niveau de risque des différentes entités présentes dans le réseau AeroMACS : topologie initiale #1 vs. topologie évoluée et plus sécurisée #2

Les résultats de ces travaux de recherche ont intéressé l'éditeur anglo-saxon ISTE Wiley qui après étude par son comité de sélection scientifique a accepté de publier en 2013 ces travaux dans l'ouvrage référencé *(Ben Mahmoud et al., 2013).*

Ces résultats démontrent comment il est possible de contribuer à l'amélioration de la QdS puis de la sécurité dans un environnement contraint de type aéronautique. Dans la suite de ce chapitre nous allons maintenant considérer un autre type d'environnement réseau contraint : les flottes de drones.

2.5- CONTRIBUTION A LA ROBUSTESSE DES COMMUNICATIONS POUR LES FLOTTES DE DRONES

Depuis plusieurs années, le développement des thématiques de recherche autour des réseaux ad hoc mobile (MANET : Mobile Ad Hoc Network) *(Camp et al., 2002)* concerne les différents domaines des transports terrestres, maritimes ou encore aériens. On peut citer en particulier le développement de nouveaux réseaux de communication pour permettre l'échange d'informations entre voitures ou trains (VANET : Vehicular Ad Hoc Network). Les réseaux ad hoc aériens sont également en pleine évolution. Une des raisons est l'évolution très importante des capacités de calcul et d'autonomie embarquées directement dans ces aéronefs. Ce travail de recherche s'intéresse à un sous ensemble de ces aéronefs que sont les aéronefs autonomes (UAV : Unmaned Aerial Vehicule ou "drone") pour lesquels les nouvelles fonctionnalités de calcul permettent d'envisager des applications nouvelles en matière de communication et de sécurisation de ces communications. Un état de l'art a été présenté pour les réseaux UAANET en introduction de ce chapitre dans lequel les principaux enjeux de routage et de sécurité ont été énoncés.

Dans la suite de cette section deux contributions vont être introduites : la première (cf. section 2.5.1) au travers du projet D3COS permettant de garantir de la QdS dans le cadre de la communication d'agents UAV collaboratifs et la seconde (cf. section 2.5.2) permettant de sécuriser une infrastructure de communication pour une flotte de drones au travers du projet SUANET.

2.5.1- Architecture de qualité de service pour agents coopératifs

- **Projet européen D3COS : définition d'une architecture de communication pour agents collaboratifs (démarré en novembre 2011)**

Le projet européen D3COS[16] (Designing Dynamic Distributed COoperative human-machine Systems) s'intéresse à la définition de moyens de communication pour les agents collaboratifs de plusieurs types (avions, voitures, trains, bateaux…). Dans ce cadre le groupe ResCo doit contribuer à la définition d'une architecture de communication garantissant la qualité de service (QdS) pour les agents collaboratifs amenés à communiquer entre eux via des réseaux de communication ad hoc.

- **Définition d'une architecture de communication à QdS garantie pour les drones**

Ainsi depuis septembre 2011, je participe au co-encadrement d'Ouns Bouachir, étudiante à l'Université Paul Sabatier de Toulouse. Ce co-encadrement est assuré également par MM. Fabien Garcia (enseignant chercheur au laboratoire TELECOM de l'ENAC) et Thierry Gayraud (professeur à l'Université Paul Sabatier de Toulouse et chercheur au LAAS-CNRS).

L'objectif du travail comporte trois phases :

1. Tout d'abord, la définition d'une architecture de communication pour les réseau de drones ad hoc offrant des garanties en termes de différenciation de services.

[16] Site web du projet D3COS : http://www.d3cos.eu/.

2. Ensuite, la mise en œuvre de ces nouveaux services dans le simulateur OMNET++ afin de valider le gain apporté par cette solution par rapport aux solutions existantes dans le domaine. Cette mise en œuvre par simulation devra se traduire par une « implémentation » sur cible réelle par l'utilisation de système Rasberry Pi.
3. Enfin, le déploiement de cette solution sera testé en configuration grandeur nature par l'intermédiaire des drones qui sont quotidiennement utilisés au sein de l'ENAC par l'intermédiaire du programme transverse « drones » de l'ENAC et le système d'autopilotage Paparazzi.

Etat de l'art des solutions de QdS pour les flottes de drones

Comme présenté en introduction de ce chapitre, il existe, dans la littérature, deux principales architectures de garantie de la QdS précédemment développées au niveau réseau pour les drones : SWAN et INSIGNIA. Nous faisons volontairement le choix d'écarter les travaux qui portent sur la modification des mécanismes de la couche MAC car ils sortent de notre domaine de compétence.

INSIGNIA possède le principal inconvénient de devoir modifier l'entête IP des paquets qui sont échangés dans le réseau (cf. principe de signalisation « inband »). C'est la raison pour laquelle nous ne l'avons pas retenu pour la solution finale. SWAN ne nécessite pas de sauvegarde de l'état des différents flux présents dans le réseau ce qui peut aider au passage à l'échelle de la solution mais diminue grandement la finesse de traitement en matière de QdS de la solution finale. Ce paramètre de passage à l'échelle ne nous a pas semblé déterminant pour justifier de sélectionner ce type de différenciation de service. En effet, le nombre de nœuds dans une flotte de drones (et donc de flux générés par ces derniers) reste relativement bas (par rapport à une approche QdS dans l'Internet). Ainsi, la gestion de la différentiation par flux peut être réalisée de façon satisfaisante dans ce type de contexte UAANET.

Dès lors, nous avons décidé de retenir les principes de traitements par flux de l'approche INSIGNIA mais de modifier son principe de gestion de la signalisation pour proposer un système qui ne nécessite pas la modification de l'entête IP. La principale raison à ce choix est la facilité de développement et la portabilité de la solution logicielle développée car cette dernière peut être traitée uniquement au niveau utilisateur du système (« Linux user level ») et ne nécessite aucune nouvelle primitive de traitement de niveau noyau (« Linux kernel level »).

Mécanismes de l'architecture DAN

L'architecture DAN (DCoS Ad hoc Network) que nous avons définie est présentée dans la Figure 31. Son objectif est de proposer aux agents collaboratifs différents niveaux de QdS en fonction du type d'application qu'ils souhaitent utiliser. En effet, trois classes de flux (Urgent, Premium et Best-Effort) ont été introduites. Les flux Urgent (trafics sporadiques) sont les plus prioritaires et les flux Best-Effort les moins prioritaires. Les flux Premium représentent les trafics possédant des besoins en termes de faible taux de perte et faible latence (i.e. trafic vidéo temps réel). Pour pouvoir traiter ces différents types de flux, un ensemble de mécanismes a été proposé pour permettre de faire de la différentiation de service au sein du réseau ad hoc. La Figure 32 résume le lien qui existe entre les différentes fonctions introduites par DAN : contrôle d'accès, classification et différentiation des flux.

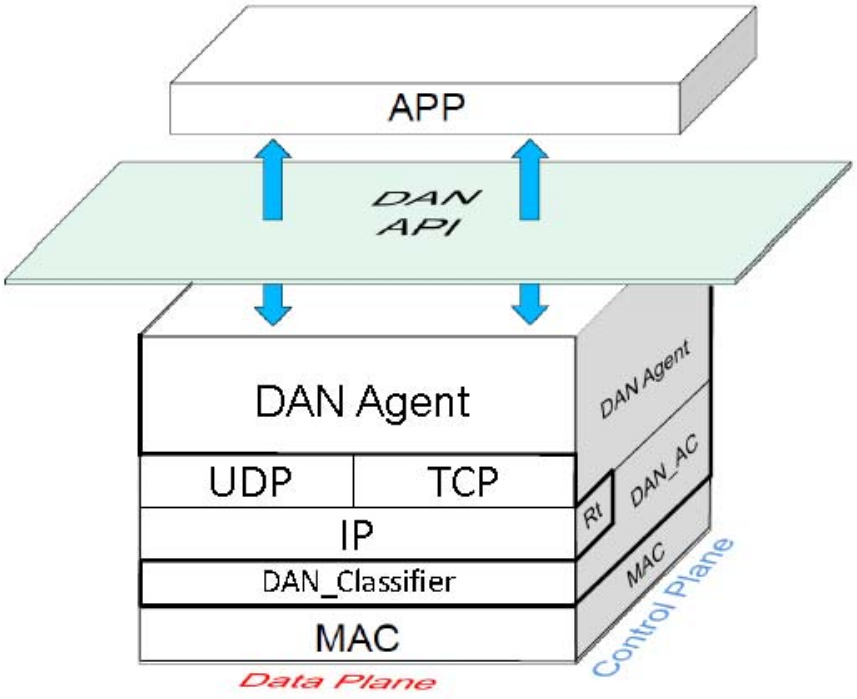


Figure 31 : architecture DAN

Les principaux mécanismes qui ont dû être définis pour le contexte UAANET sont :

- Module « DAN_agent » : il s'agit du point de contact de l'application qui souhaite exploiter les fonctionnalités de QdS de cette architecture. Il gère l'ensemble des autres modules et il maintient la liste des flux prioritaires (flux Premium) ;
- Module « Admission Controller » : il est conscient des ressources localement disponibles et fait le choix de réserver ou non les ressources pour une nouvelle demande de flux ;
- Module « Classifier » : en mettant en œuvre des mécanismes d'ordonnancement et de mise en file d'attente, il peut traiter les priorités entre les différents paquets qui doivent être émis.

La réservation de ressource dans le réseau se fait par une mise à jour progressive des états des nœuds sur le chemin suivi par les paquets de réservation : Chaque nœud ayant la possibilité d'informer le module « DAN_agent » émetteur qu'il n'est pas à même de pouvoir offrir les ressources nécessaires pour la demande de réservation d'un nouveau flux.

- **De la pertinence de l'utilisation d'un modèle de mobilité pour les simulations de drones**

La finalité de l'architecture DAN est d'être testée en environnement réel par l'intermédiaire des drones Paparazzi[17]. Néanmoins, avant de viser une intégration sur cible réelle, il a été nécessaire de valider la solution en simulation. Afin d'augmenter le niveau de réalisme de ces simulations nous avons proposé une étude comparative entre les différents modèles de mobilité traditionnellement utilisés et un nouveau modèle que nous avons défini pour permettre de valider les nouvelles solutions (architecture DAN précédemment décrite) en simulation de façon la plus réaliste possible.

[17] Site web du projet Paparazzi : **http://*paparazzi.enac.fr/***

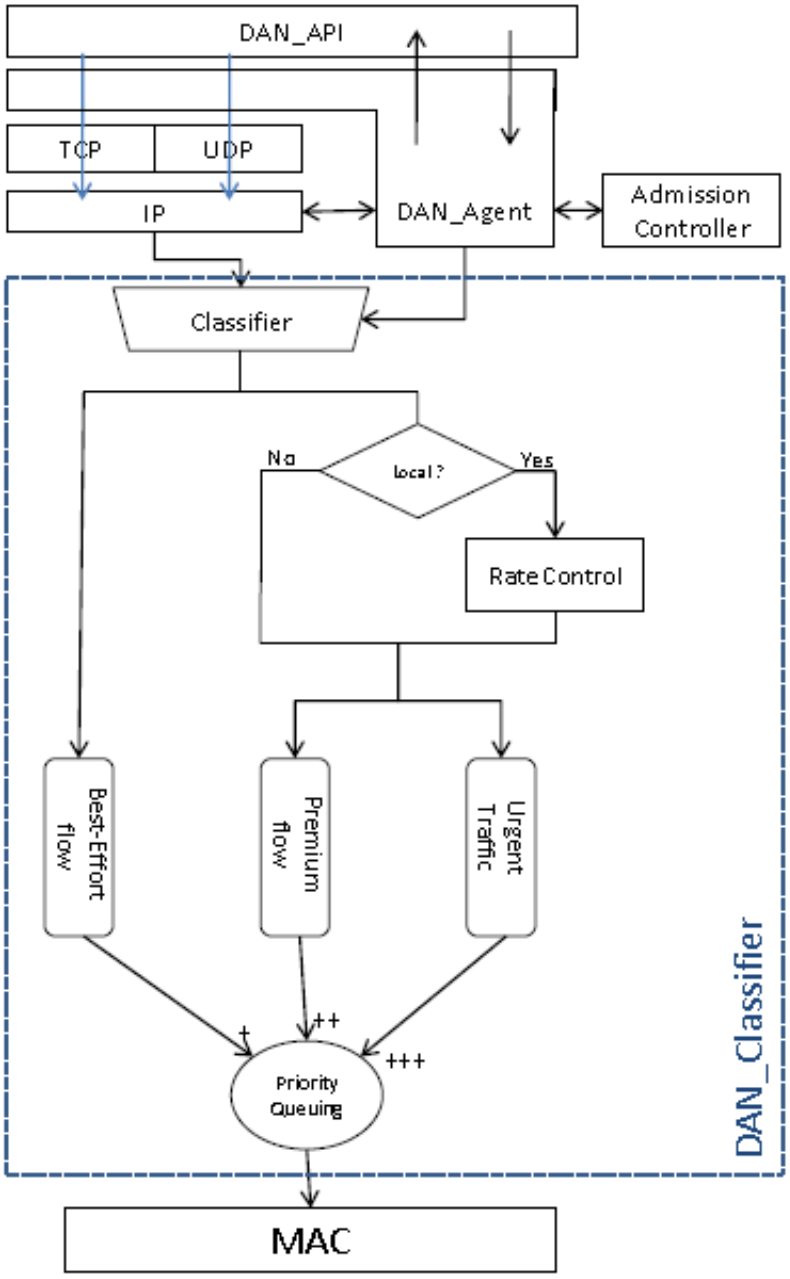


Figure 32 : mécanismes déployés dans l'architecture DAN

Principes des modèles de mobilités utilisés pour la simulation de drones

La plupart des modèles de mobilité se basent sur des mouvements simples permettant de représenter les plans de vol des drones en simulation :

- se déplacer vers un point de destination spécifique,
- tourner à droite,
- tourner à gauche.

Certains modèles peuvent ajouter des mouvements supplémentaires comme par exemple voler de façon circulaire au dessus d'un point spécifique pour, par exemple, permettre la collecte d'information sur ce dernier.

Le modèle de mobilité Random Way Point (RWP) est le plus souvent utilisé dans ce domaine par la simplicité de sa mise en œuvre. Néanmoins, les déplacements basiques qu'il

émule peuvent être fortement améliorés pour se rapprocher d'un comportement réel de drone. C'est la raison pour laquelle nous avons défini un nouveau modèle de mobilité dérivé des comportements des drones Paparazzi. Le comportement du modèle Paparazzi (PPRZM) est résumé dans la Figure 33. Il est le résultat de la concaténation de différents mouvements de base : « scan », « oval », vol stationnaire, vol en huit ou déplacement vers un point spécifique.

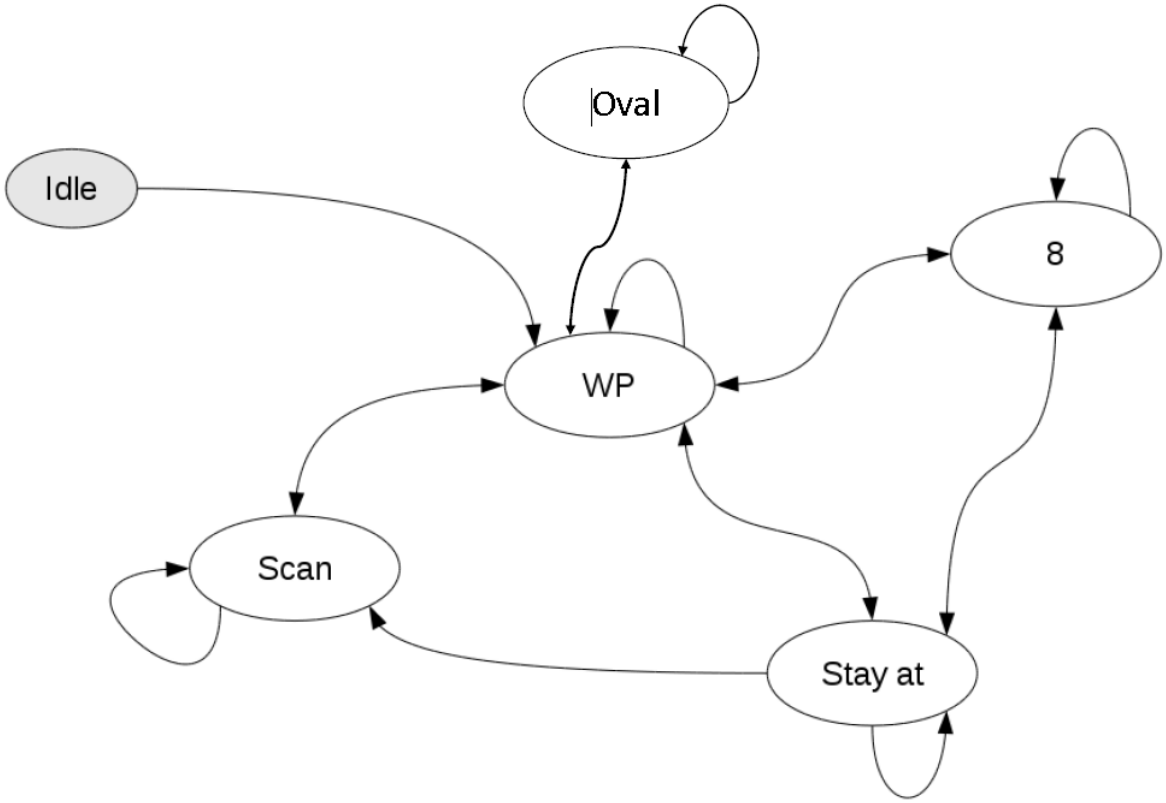


Figure 33 : principes de déplacement pour le modèle Paparazzi (PPRZM)

Pour permettre l'instanciation de ce modèle, il est nécessaire de quantifier la probabilité de passage d'un état à l'autre. Pour cela, nous avons étudié différentes traces de vols Paparazzi afin de pouvoir paramétrer les probabilités de passage d'un état à l'autre. Lorsque le drone est dans un état spécifique, son comportement est déterministe jusqu'à ce qu'il quitte cet état pour un autre. Le modèle PPRZM que nous avons proposé est donc semi stochastique.

Evaluation du modèle de mobilité PPRZM

Dès lors, nous avons décidé de comparer ce nouveau modèle au modèle de mobilité de référence dans la littérature (RWP) et de comparer également ces résultats à des déplacements simulés mais directement basés sur des traces réelles. L'objectif est double : pouvoir quantifier la précision de notre modèle par rapport au modèle RWP mais aussi pouvoir quantifier l'erreur introduite par l'utilisation de modèles par rapport à l'injection directe de traces réelles en simulation. Pour réaliser ces travaux nous avons utilisé le simulateur OMNET++.

La Figure 34 résume les comparaisons que nous avons faites sur la base des modèles de mobilité présents dans la littérature (PPRZM et RWP). Pour illustrer cette comparaison, nous avons utilisé un diagramme de représentation Kiviat. Ce diagramme permet de représenter différents paramètres sur chaque branche du diagramme. On obtient donc une signature spécifique pour le modèle PPRZM, le modèle RWD et les traces réelles.

Ces différentes signatures facilitent grandement la comparaison de ces différents paramètres. Dans ce travail, nous avons fait l'hypothèse que tous les paramètres ont le même niveau d'importance dans la construction de la signature. Chaque valeur des paramètres est normalisée : l'objectif étant de comparer la valeur d'un même paramètre pour les différents modèles et les traces réelles considérées.

Les paramètres que nous avons considérés dans cette étude sont de deux types :

- Structure géométrique du réseau construit pendant la simulation : nombre de voisins pour chacun des nœuds UAV, « clustering » des UAV dans les différentes zones du réseau, distribution des UAV dans l'espace de simulation, etc.
- Performances des mécanismes réseau étudiés en simulation : taux d'acheminement des paquets, délai de bout en bout, débit, etc.

On observe dans la Figure 34 que pour la majorité des paramètres présents sur les branches du diagramme Kiviat, c'est le modèle PPRZM qui se rapproche le plus des résultats obtenus à l'aide de données de vols réelles injectées dans le simulateur. Ainsi, nous recommandons fortement l'utilisation de ce modèle pour la validation de nouveaux mécanismes en simulation.

Il est important d'ajouter qu'un des constats de cette étude (cf. Figure 34) est que les différents modèles probabilistes utilisés pour simuler le déplacement des drones en simulation sont toujours imprécis en comparaison des déplacements qui peuvent être réalisés lors d'expérimentations réelles.

Dès lors, nous avons fait le choix d'injecter dans nos simulations OMNET++, des plans de vols tirés de nos expérimentations réelles avec les drones Paparazzi. En effet, c'est le moyen le plus précis de pouvoir reconstituer des trajectoires qui soient observables dans la réalité et ainsi confronter dès la phase de simulation nos nouveaux mécanismes (architecture DAN) à des comportements réalistes. Cette étape de simulation réaliste est fondamentale afin de pouvoir passer, dans un second temps, à l'expérimentation en conditions réelles et avoir un degré de confiance suffisant dans la solution testée en simulation afin d'aborder le cas réel sereinement.

Néanmoins, nous sommes conscients que tous les travaux sur la mobilité des drones n'ont pas forcément accès à des traces réelles comme c'est le cas pour nous au sein de l'ENAC. Dans ce cas, nous pouvons recommander grâce à l'étude dont les résultats sont résumés dans la Figure 34 que le modèle de mobilité Paparazzi (PPRZM) est le plus adapté pour la validation de mécanismes réseaux avec le simulateur OMNET++. En effet différents paramètres de comparaison ont été considérés pour mettre en concurrence le modèle PPRZM, le modèle RWP et les traces réelles. Sur les deux types de comparaisons réalisées (structure géométrique du réseau simulé et performances des mécanismes de routage réseau simulés), le modèle PPRZM démontre de meilleures qualités de représentations que le modèle RWD par rapport aux traces réelles qui peuvent être utilisées en simulation.

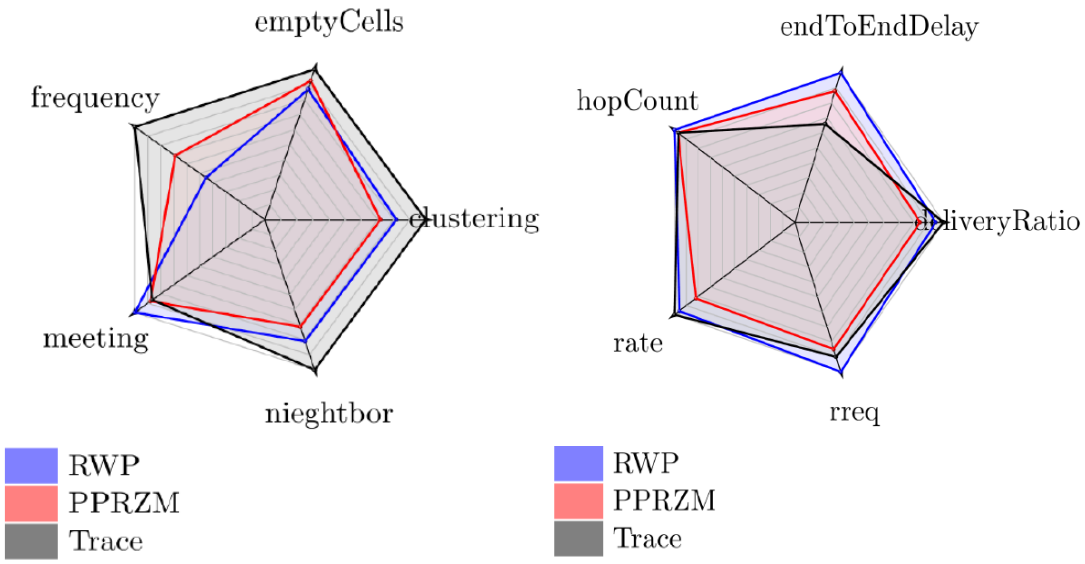


Figure 34 : comparaison des différents modèles de mobilité (PPRZM et RWP) utilisés pour la simulation de drones par rapport à l'utilisation de traces réelles en simulation (partie gauche structure géographique du réseau simulé vs. partie droite performances des mécanismes de routage réseau

- **Validation en simulation de l'architecture DAN**

Dans la suite de ces travaux, par l'intermédiaire des simulations dont les paramètres sont détaillées dans le Tableau 6, nous avons pu valider que les critères de QdS étaient garantis par l'architecture DAN qui a été développée et présentée au début de cette section. En effet, la Figure 35 illustre que le délai de bout en bout est maintenu au minimum pour le trafic le plus critique (« Urgent traffic ») et qu'il augmente en fonction de la criticité des trafics : « Premium traffic » est plus critique que « Best-Effort traffic » et nous pouvons observer que le délai augmente également pour ces deux types de trafic de façon inverse au niveau de criticité représenté. Les mêmes commentaires peuvent être réalisés pour le paramètre taux de perte, tel que l'illustre la Figure 36.

Tableau 6 : paramètres de simulation (architecture DAN)

UAV number	10
routing protocol	AODV
MAC protocol	802.11
Transmission range	250m
Channel capacity	54 Mbps
Premium Capacity in Admission Control	11 Mbps (about 20% of the channel capacity)
Urgent traffic /node	500 Bytes sent randomly every [1s,3s]
Premium traffic /node	760Kbps : 950 Bytes every 10ms
Best effort traffic /node	4Mbps: 500Bytes every 1ms

Il est important de préciser que ces simulations avaient pour objectif de valider le fonctionnement et la garantie de QdS de l'architecture DAN. C'est la raison pour laquelle un protocole de routage standard très utilisé dans la littérature (i.e. le protocole AODV) a été utilisé pour cette étude. Une des perspectives de ce travail abordée à la fin de ce chapitre porte sur l'utilisation de protocole de routage plus évolué intégrant, dans leurs mécanismes d'établissement des routes, la gestion de la QdS ou encore des approches multi chemins qui sont une composante très importante de la topologie des réseaux ad hoc de flottes de drones.

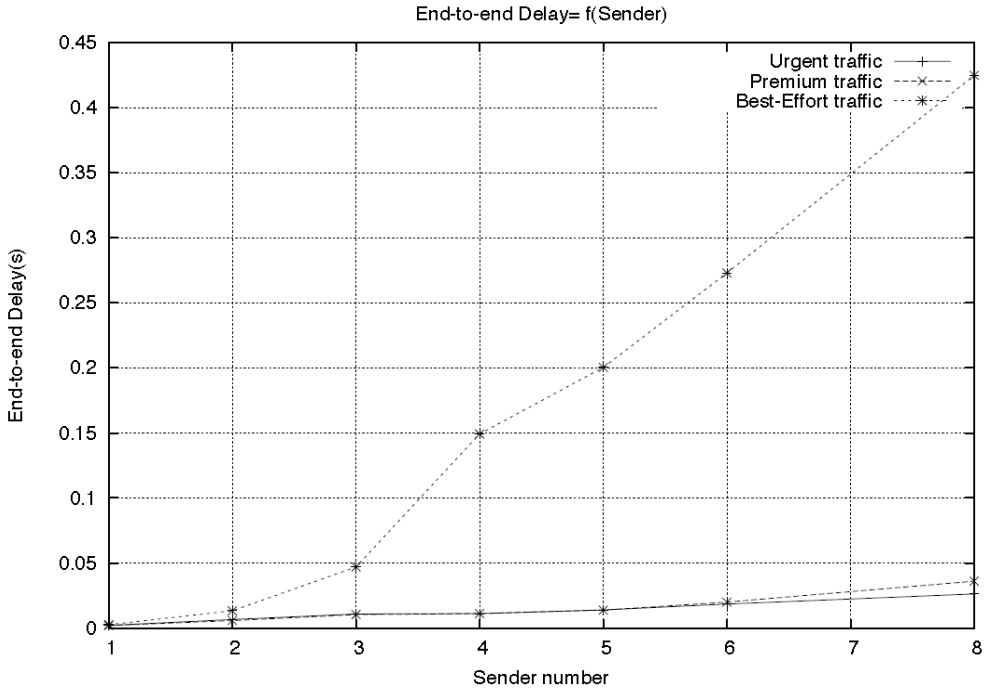


Figure 35 : délai de bout en bout en fonction du nombre d'émetteurs par type de service

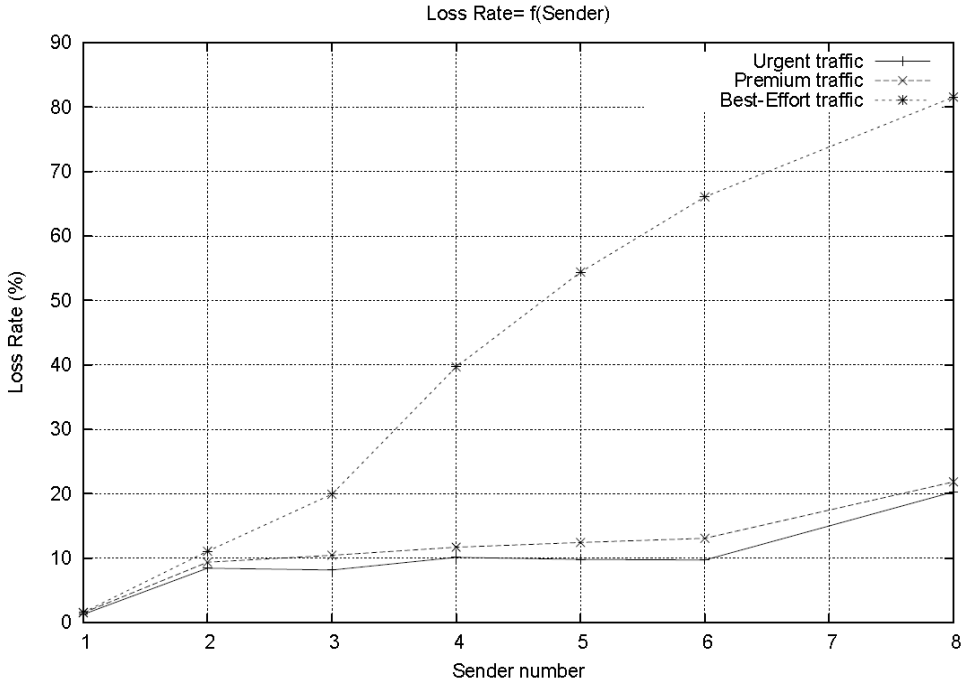


Figure 36 : taux de perte en fonction du nombre d'émetteurs par type de service

De plus, la suite de ce travail porte sur la validation en environnement réel de cette solution de gestion de la QdS. Pour cela, nous sommes en train de mettre en œuvre sur une architecture matérielle Rasberry Pi cette solution logicielle (architecture DAN). Dans un deuxième temps, nous allons réaliser des essais en vol par l'intermédiaire de drones quadri-rotors Paparazzi développés au sein de l'ENAC. Les expérimentations ont lieu pendant le premier trimestre 2014. Les résultats de cette expérimentation réelle ne sont pas encore disponibles au moment où nous rédigeons ce manuscrit, c'est la raison pour laquelle nous ne pouvons les consigner par écrit.

Ce travail s'est focalisé dans un premier temps sur l'aspect gestion de la QdS dans le cadre d'une flotte de drones. Il est néanmoins intéressant de pouvoir rajouter des problématiques de sécurité lorsque l'on traite de communication en environnement contraint comme une flotte de drones. Cet aspect de la problématique a pu être abordé dans le cadre du travail qui est présenté dans la section qui suit.

2.5.2- Architecture sécurisée pour une flotte de drones

L'objet de ce dernier domaine de recherche est de définir, concevoir et mettre en œuvre une architecture de sécurité pour les réseaux ad hoc d'UAV (également appelé flotte de drones).

Nous avons identifié trois grandes pistes de contribution pour ce travail de recherche :

- Infrastructure de gestion des clés ;
- Mécanismes de routage sécurisés ;
- Mécanismes de communication de données sécurisés.

Le premier axe concerne la définition des mécanismes nécessaires pour permettre le déploiement au sein du réseau ad hoc de l'ensemble des clés nécessaires à la mise en œuvre des mécanismes d'authentification, de confidentialité et d'intégrité qui représentent la clé de voûte pour permettre d'augmenter le niveau de robustesse de cet environnement.

Le deuxième axe consiste à réfléchir à de nouveaux mécanismes de routage sécurisés permettant l'acheminement des données au sein du réseau ad hoc. Actuellement des protocoles de routage spécifiquement développés pour les MANET ont déjà été proposés mais peu ont pris en compte la composante sécurité. Ce travail s'appuiera particulièrement sur le protocole de distribution de clés présenté dans le point précédent. En effet, le mécanisme de routage sécurisé qui sera proposé mettra en œuvre des techniques d'authentification et de vérification de l'intégrité qui reposeront sur l'utilisation de clés partagées ou de clés asymétriques (couple clés publiques/privées). Un point important de ce travail consistera à proposer un mécanisme de routage faiblement consommateur en matière de ressources réseaux afin de pouvoir garantir la meilleure utilisation du canal de communication représenté par les liaisons inter UAVs.

Enfin, le dernier axe de recherche s'intéresse à définir de nouveaux mécanismes d'échange de données sécurisées entre UAVs. Il sera en particulier intéressant de pouvoir prendre en compte la notion de groupe de drones qui peut être introduit lors de la mise en place de mission complexe. Dans ce cas précis, il faut que l'architecture de gestion de clés prenne en considération les problématiques d'entrée/sortie d'un nœud dans un groupe. Une option serait par exemple de changer la clé de chiffrement utilisée dans le groupe que le nœud a quitté afin d'éviter qu'il ne puisse accéder à des informations auxquelles il ne peut plus prétendre vu qu'il a quitté le groupe. De plus, ce mécanisme de ré-allocation de clés doit être léger et efficace et nécessiter le moins d'échange de messages possibles.

La phase de test va passer par la réalisation d'une maquette grandeur nature permettant de mettre en évidence la faisabilité des concepts proposés pendant ce travail de thèse. Afin de s'approcher d'un cas d'utilisation le plus réaliste possible, nous avons défini en partenariat avec la société DELAIR TECH un scénario d'application qui représenterait à long terme l'objectif final pratique du travail de recherche développé dans le cadre de cette thèse.

- **Projet SUANET : Sécurisation des échanges dans le cadre d'un réseau ad hoc de drones (démarré en novembre 2013)**

Dans le cadre du partenariat envisagé avec la société Delair Tech[18], spécialiste dans le développement de drones, nous envisageons de décliner les concepts de recherche présentés précédemment au contexte d'application spécifique d'un réseau de drones produit par cette société. En effet, le domaine des drones est en pleine évolution et les compétences acquises par la société Delair Tech dans le cadre du développement de différents produits commerciaux (par exemple le DT-18) nous permettent d'envisager une application industrielle réaliste des concepts de sécurité pour les réseaux ad hoc définis dans ce travail de thèse. En particulier, il semble envisageable de viser une implémentation de la solution technique proposée dans cette thèse au travers de la plateforme de développement que propose la société Delair Tech. Pour cela, il sera nécessaire de développer un prototype logiciel compatible avec la cible embarquée SABRE™ Lite (i.MX 6 quadcore). Le Tableau 7 présente un résumé des caractéristiques techniques de la cible embarquée visée dans ce travail : le DT-18.

Tableau 7 : caractéristiques techniques du DT-18

Characteristic	Value
Model	DT-18
MTOW	< 2kg
Payload	250g
Range	100km
Cruise speed	50km/h
Wind	up to 45km/h
Photo	5 to 10cm resolution
Video	20cm resolution
Infra-red video	30cm resolution
Real-time transmission	Up to 15km. Extension to 100km
Autopilot	Delair-Tech technology
Onboard computer	payload and communication control, 1GHz
Field deployment	< 10 minutes
Price	15 k€

De plus, le partenariat avec un spécialiste des drones de surveillance nous permet d'envisager des cas d'utilisation réalistes adaptés à ce domaine en pleine évolution. En effet, les drones sont pilotés par l'intermédiaire d'une station sol qui permet de collecter les informations d'un ou plusieurs drones en vol. Il est donc intéressant d'envisager une hiérarchie entre les différents équipements (drone(s) en vol et station(s) sol(s)). Cette hiérarchie permettrait de faire apparaître différents rôles dans le réseau ad hoc ainsi constitué. Chacun de ces rôles pourrait permettre de décliner et spécifier de façon adéquate chacun des mécanismes de sécurité envisagés dans la section précédente. D'autre part, dans le cadre de l'échange d'information au sein du réseau ad hoc de drones, il serait intéressant dans ce travail de thèse d'envisager une solution pour permettre d'interfacer les informations échangées par la flotte de drone vers d'autres réseaux notamment le réseau opérationnel de la DGAC. Cette application pourrait faciliter l'intégration future des drones dans l'espace aérien national voire international. Ce besoin passe là aussi par la déclinaison de mécanismes de sécurité adaptés permettant de garantir que le système actuel ATM ne soit pas impacté par l'intégration de ces nouveaux équipements.

- **Scénario d'application (expérimentation réelle) : télésurveillance distribuée d'une zone géographique sinistrée à l'aide d'un réseau de drones ad hoc sécurisé**

[18] Site web de la société Delair-Tech : http://www.delair-tech.com

Dans ce travail de recherche, nous avons défini un cas d'utilisation qui représente une situation d'urgence où un réseau de drones ad hoc va être utilisé pour couvrir par télésurveillance (i.e. images en rafale, films vidéo en temps réel) une zone géographique dévastée suite à une catastrophe naturelle (séisme par exemple). Le réseau ad hoc sera constitué de 3 agents coopératifs autonomes communiquant ensemble de manière sécurisée par le réseau ad hoc de communication.

L'utilisation du réseau ad hoc formé par les drones peut se justifier par la topologie du terrain qui rend impossible la communication directe entre la station sol de contrôle et les différents drones. Ces problèmes peuvent s'expliquer par la présence d'obstacles sur la trajectoire entre la station sol et les différents drones ou de vol des drones à trop faible altitude. Il est donc nécessaire d'utiliser un drone spécifiquement comme relais de communication au sein du réseau de drones pour acheminer l'information entre tous les drones et la station au sol de contrôle. Le schéma Figure 37 explicite cette configuration.

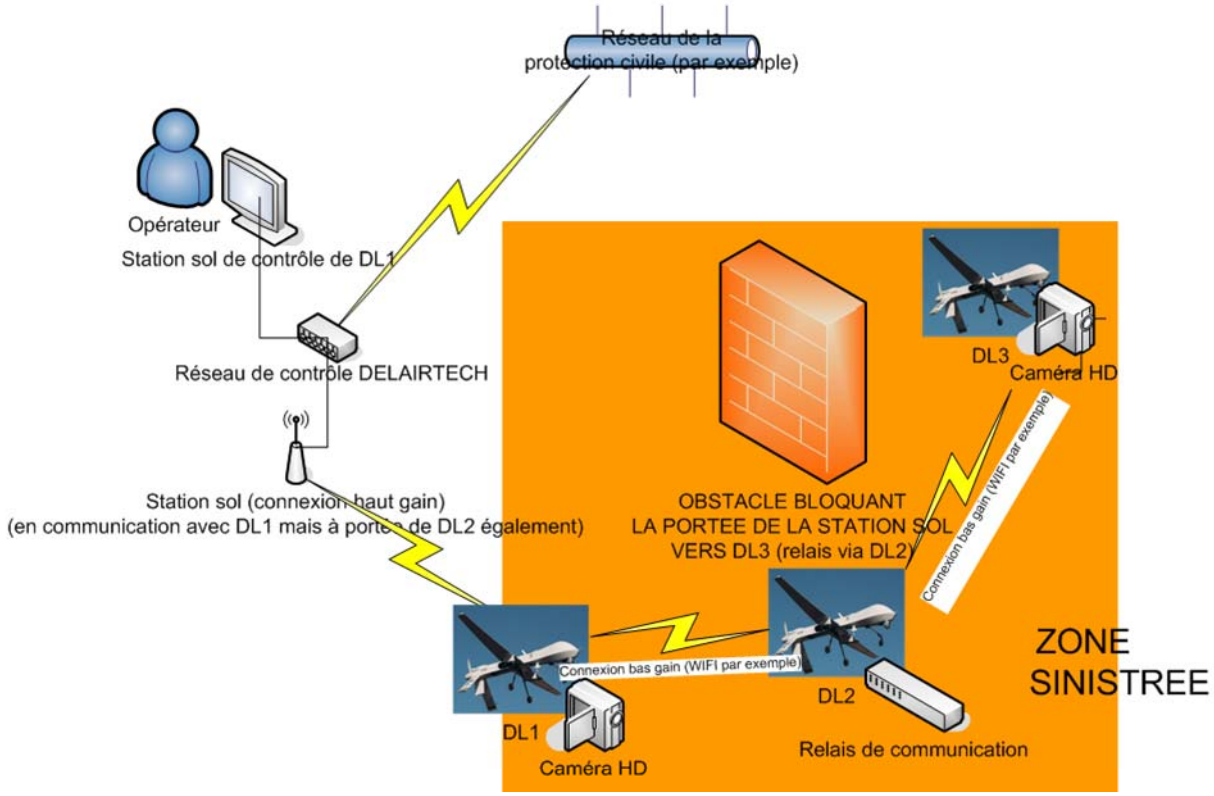


Figure 37 : scénario d'application (télésurveillance distribuée)

- **Contribution à la sécurisation des communications dans une flotte de drones**

Le travail précédemment développé va donc se découper en trois étapes :

- Conception de l'architecture de communication sécurisée ;
- Validation de la proposition ;
- Test en environnement réel de cette solution.

Ainsi, dans ce cadre et depuis novembre 2013, je suis directeur officiel de thèse[19] de Jean Aimé Maxa qui travaille sur ce projet dans le cadre d'une bourse de thèse CIFRE.

[19] Dans ce cadre, je suis titulaire d'une dérogation de l'Université Paul Sabatier de Toulouse.

Les problématiques d'optimisation de l'utilisation du réseau seront illustrées par l'utilisation d'un protocole de routage et d'acheminement de l'information (les flux images et/ou vidéos) basé sur l'émission multicast par exemple. Enfin la problématique de sécurité des communications sera abordée de façon duale :

- tout d'abord à travers l'objectif de fournir un réseau ad hoc protégé de tout problème de sécurité (authentification des agents ou encore confidentialité des données échangées) pour éviter qu'un tiers malintentionné puisse mettre à mal le service rendu par cette solution de télésurveillance distribuée ;
- ensuite, dans sa capacité à s'interfacer de façon sécurisée avec d'autres réseaux existants, au travers de la station sol de façon à pouvoir acheminer ces informations de supervision de façon sécurisée vers un réseau tiers (réseau DGAC par exemple, ministère de l'intérieur, réseau d'urgence, etc…). Dans ce dernier cas, les problématiques de négociation des paramètres de communication sécurisée seront en particulier mis en évidence.

Nous arrivons au terme de la description des travaux de recherche que nous avons mené depuis 2006 au sein du laboratoire TELECOM de l'ENAC en tant qu'enseignant-chercheur. La section suivante résume les activités d'encadrement que j'ai réalisées au cours de cette expérience professionnelle. Ensuite, la section 4 fait un récapitulatif des développements logiciels qui ont été réalisés pour répondre aux problématiques recherche décrites dans ce chapitre et qui ont été mis à la disposition de la communauté recherche et industrie par l'intermédiaire d'une licence Open Source. Enfin, la section 5, récapitulera les différents axes de recherche que je me suis attaché à développer dans ce manuscrit et présentera les différentes perspectives de recherche que j'envisage pour la suite de mes activités de recherche dans le domaine de l'amélioration de la QdS et de la sécurité en environnement contraint.

3- ACTIVITES D'ENCADREMENTS (DEPUIS 2002)

Je résume dans cette section les différents encadrements dont j'ai eu la charge (étudiants de deuxième cycle et de troisième cycle) au travers des différents projets de recherche que j'ai menés au LAAS-CNRS puis à l'ENAC de Toulouse. Ces encadrements sont répartis entre un niveau deuxième cycle (stage ingénieur, master professionnel ou master recherche) et un niveau troisième cycle (étudiant en thèse de doctorat).

3.1- ETUDIANTS DE DEUXIEME CYCLE EN STAGE INGENIEUR, MASTER PROFESSIONNEL OU MASTER RECHERCHE

3.1.1- Encadrement pendant mon travail de doctorat (2002 – 2006)

Pendant la période *mars 2004 - septembre 2005*, j'ai encadré **Yu ZHANG**, stagiaire ENSEEIHT, pour un stage de DEA de 6 mois réalisé dans le groupe OLC. Le sujet de ce stage, en rapport avec la thématique de mon travail de thèse, était « Métrologie dans les réseaux IP : Caractérisation du trafic Internet ».

J'ai, en outre, participé aux co-encadrements (avec mon directeur de thèse P. Owezarski) des stages suivants :

- Stage de fin de 4ème année, stagiaire IUP STRI UPS (2003) sur le sujet : « Utilisation de la métrologie pour le réalisme des émulations » ;
- Stage de fin de 5ème année, stagiaire DEA UPS (2003) sur le sujet : « Métrologie et Sécurité : nouvelles méthodes pour la détection d'attaques ».

3.1.2- Encadrement en tant qu'enseignant-chercheur au sein de l'ENAC (depuis septembre 2006)

- Stages validant le cursus **Master 2 recherche** :

- **Hassna LOUADAH**, étudiante en Master 2 Recherche à l'Université Paris Descartes : « contribution aux mécanismes de sécurité pour un routeur embarqué sécurisé » ;
- **Amira MAKHLOUF**, étudiante ENSEEIHT en M2R IT : « définition d'une architecture de gestion de la sécurité pour les réseaux ad hoc aéronautiques » ;
- **Antoine VARET**, étudiant INSA en M2R IA : « mise en œuvre d'une architecture de gestion de la sécurité pour les communications aéronautiques du futur » ;
- **Hamza HAIMEUR**, étudiant UPS en M2R RT : « méthodologie de gestion et d'analyse du risque pour la sécurité des réseaux aéronautiques ».

- Stages validant le cursus **ingénieur** :

- **Alinoé ABRASSART**, étudiant en 3ème année ENAC : « application d'une méthode MDD pour le développement de mécanismes de sécurité pour la communication de mini-drones »;
- **Gilles ROUDIERE**, étudiant en 5ème année INSA : « mise en œuvre d'une architecture de communication embarqué pour mini-drones »;

- Stages étudiant intégrés au cursus **ingénieur ENAC** :

  - **IENAC 2ème année filière L** (projets réalisés en binôme sur une période de 3 mois) :

- Vérification formelle d'un protocole de sécurité à l'aide d'un outil d'analyse automatique des failles de sécurité ;
- Proposition d'une infrastructure à clés publiques originale adaptée au contexte aéronautique ;
- Développement d'un module de décodage logiciel WIRESHARK pour le trafic radar au format ASTERIX (version 2) rapport au format PDF ;
- Développement et déploiement d'une application distribuée d'administration pour le parc de machines de la subdivision ELR.

    - **IENAC 3eme année option Télécom et Réseaux** (projets réalisés en binôme sur une période de 2 mois) :

- Etude d'un système de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire ;
- Prise en main, configuration et évaluation des performances d'un "framework" logiciel de gestion de la sécurité d'un SSI dans le cadre d'un réseau d'entreprise privé ;
- Etude de l'impact d'un déploiement d'une architecture de sécurité multi-domaines dans un contexte aéronautique : prise en compte de la problématique de mise à l'échelle pour ce qui est de la gestion des échanges en environnement sécurisé aéronautique ;
- Etude des faiblesses des mécanismes de sécurité du protocole « Wifi ».

    - Stages étudiant intégrés au cursus **ingénieur INSA** :

- **Benoit Sainct**, étudiant INSA Toulouse en 4ème année du département GMM : « caractérisation et analyse de trafic à l'aide d'outils statistiques » ;

- **Léo Sartre**, étudiant INSA Toulouse en 4ème année du département GEI : « développement d'un outil pour l'analyse de code : METRIX » ;

- **Julien Marchand**, étudiant INSA Toulouse en 3ème année du département GEI : « modélisation sous Stateflow et Simulink d'un processus de requêtes/réponses pour les options Neighbor Discovery et Router Alert du protocole IPv6 » ;

- **Antoine Varet**, étudiant INSA Toulouse en 4ème année du département GEI : « développement d'un décodeur ASTERIX pour le logiciel Wireshark ».

3.2- ETUDIANTS DE TROISIEME CYCLE EN THESE DE DOCTORAT

    - Thèses soutenues :

- **Slim Ben Mahmoud**, « sécurisation des applications avion dans un système de communication intégrant un segment sol bord par satellite », soutenue en février 2012, co-encadrement avec Alain Pirovano (groupe ResCo/TELECOM/ENAC), INSA de Toulouse.
- **Antoine Varet**, « définition, conception, mise en œuvre et validation d'un routeur sur et sécurisé pour l'avionique de nouvelle génération », soutenue en octobre 2013, encadrement, INSA de Toulouse.

    - Thèses en cours :

- **Ouns Bouachir**, « conception et mise en œuvre d'une architecure à qualité de service pour les réseaux de drones collaboratifs », débutée en novembre 2011, co-encadrement avec Fabien Garcia (groupe ResCo/TELECOM/ENAC) et Thierry Gayraud (Université Paul Sabatier de Toulouse), Université de Toulouse.
- **Jean Aimé Maxa**, « définition et mise en œuvre d'une architecture de communication sécurisée pour les réseaux de drones », débutée en novembre 2013, encadrement, dérogation HDR de l'Université de Toulouse.

4- DEVELOPPEMENTS LOGICIELS

Les différents projets dans lesquels j'ai été impliqué depuis 2002 m'ont permis de produire différents logiciels qui sont des supports pour mes travaux de recherche. Cette partie de mon travail est indissociable des contributions recherches qui ont été présentées tout au long de ce chapitre. En effet, pour mener à bien les phases de validation et de tests abordées dans les différents projets de recherche pour lesquels j'ai été partie prenante, il a été nécessaire à plusieurs reprises de combler un manque en matière de logiciels libres spécifiques.

Ces travaux se sont donc traduits par la production d'un certain nombre de logiciels qui ont été mis à la disposition de la communauté scientifique pour la plupart en licence « Open Source ». Les différents projets logiciels qui ont été développés sont présentés ci-après :

- **METRIX** : outil d'analyse qualitatif et quantitatif de code :
  - Ce logiciel développé dans le cadre du partenariat avec Thales Avionics permet d'analyser la qualité du code généré par un système d'auto-génération de code.
  - Il est disponible en version open source sur la page suivante : **http://www.recherche.enac.fr/~avaret/metrix**

- **SCOUT** : protocole permettant l'auto-configuration de différents nœuds réseau dans le cadre de la mise en œuvre d'une communication sécurisée
  - Ce logiciel développé dans le cadre du partenariat avec Thales Avionics permet d'accélérer le déploiement de tunnels sécurisés dans un environnement réseau ouvert (type réseau Internet) pour lesquels les phases de configuration sont trop lourdes pour être réalisées de façon manuelle.
  - Il est disponible en version open source sur la page suivante : **http://www.recherche.enac.fr/~scout6**

- Décodeur **ASTERIX** pour le logiciel **Wireshark** :
  - Le logiciel Wireshark est un analyseur réseau provenant du monde « Open Source ». Ses capacités de décodage et ses performances en capture en font l'un des meilleurs analyseurs réseaux, devant bon nombre de logiciels du même type dits propriétaires.
  - L'objectif de notre travail a été de permettre l'exploitation des fonctionnalités d'analyse réseau du logiciel Wireshark dans le cadre du décodage des trames ASTERIX (All purpose STructured Eurocontrol Radar Information eXchange).
  - La version que nous avons utilisée ici est la 1.0.7, disponible sur clef USB ou via un installeur et fonctionne sous Windows (2000, XP, Vista) et sous Linux. Elle contient un plugin additionnel fournissant la prise en charge de la dissection et de l'interprétation des paquets contenant des données au format ASTERIX.
  - Le code source et la documentation développeur sont disponibles sous licence open source : **http://www.recherche.enac.fr/leopart/~asterix/**.

- **ZOO** : développement d'un logiciel d'analyse de traces permettant une décomposition du trafic en fonction du type de flux considéré (**http://www.laas.fr/~owe/ZOO/index.htm**).

- Développement du **site Web** du projet **METROSEC** : système de stockage de traces de métrologie passive et de récupération de ces traces : technologies PHP/MySQL et HTML (**http://www.laas.fr/METROSEC**).

5- CONCLUSIONS ET PERSPECTIVES DES TRAVAUX DE RECHERCHE

Nous arrivons à la fin du chapitre dédié à la présentation de mes travaux de recherche en vue de l'obtention de l'habilitation à diriger les recherches. Dans ce chapitre, j'ai articulé mes différentes contributions autour de la problématique de la gestion de la QdS et de la sécurité en environnement réseau contraint. Deux grands types de réseaux ont été analysés : les réseaux de flotte de drones et les réseaux aéronautiques.

Au travers de mes travaux j'ai mis en évidence 4 axes de contributions différents pour ces environnements :

- Tout d'abord, la proposition d'une architecture de sécurité adaptative pour les communications aéronautiques sol-bord a permis une gestion conjointe des paramètres de QdS mais aussi de sécurité.
- Dans un deuxième temps, je me suis attaché à définir une méthode de génie logiciel permettant de concevoir et mettre en œuvre de façon efficace un système complexe dans un environnement où les contraintes de certification de sécurité et de sûreté de fonctionnement sont critiques. Une application aux systèmes aéronautiques embarqués a été présentée pour illustrer les avantages de cette méthodologie.
- Par la suite, j'ai proposé une méthode quantitative d'analyse de risque pour les environnements critiques. En particulier, un cas d'application aux réseaux aéronautiques (réseau aéroportuaire AeroMACS) a été présenté et utilisé pour valider l'applicabilité de cette méthode et illustrer les améliorations en matière de robustesse pour le système final (i.e. l'architecture de communication AeroMACS) sur lequel cette méthode est appliquée.
- Enfin, la dernière contribution porte sur l'amélioration de la robustesse des communications pour les flottes de drones. Une architecture de communication d'agents collaboratifs garantissant la QdS a été proposée et validée par simulation en s'appuyant sur un nouveau modèle de mobilité plus proche des conditions réelles d'un environnement de drones communiquant.

Ces différentes contributions ont permis de rendre les systèmes évoluant en environnement réseau contraint auxquels je me suis intéressé (système aéronautique et flotte de drones) plus robustes à la fois en terme de QdS mais aussi de sécurité. Le trait d'union que j'ai souhaité réaliser au niveau de mes travaux de recherche entre les concepts de gestion de la qualité de service et de la sécurité pour ces systèmes apparait, à l'heure actuelle, comme de plus en plus important à mesure que les systèmes développés par les ingénieurs deviennent plus complexes. En effet, il est maintenant très difficile de pouvoir suivre des approches de conception disjointes pour ces deux thématiques (i.e. développer en parallèle des solutions traitant de la QdS et de la sécurité), le résultat final risquant d'être sous optimal et relativement complexe à fusionner étant donné le caractère variable et dépendant des ressources disponibles dans les environnements contraints.

Dans la suite de mes travaux de recherche, je souhaite continuer à exploiter le lien qui existe entre ces deux domaines de recherche de façon à pouvoir proposer des solutions architecturales originales, optimales et adaptées au plus prêt des caractéristiques des futurs réseaux contraints à étudier. Ainsi, les travaux présentés précédemment ouvrent naturellement un certain nombre de perspectives qui peuvent être résumées autour des quatre axes de recherche suivants :

- Méthodologie de prototypage pour systèmes complexes critiques ;
- Application des contributions en matière de gestion de la QdS et de la sécurité au contexte de l'architecture de communication SESAR ;
- Extension des travaux sur la sécurisation des flottes de drones ;
- Application des contributions en matière de sécurité au domaine des réseaux ad hoc aéronautiques.

5.1- METHODOLOGIE DE PROTOTYPAGE RAPIDE DE SYSTEMES COMPLEXES

Différentes pistes s'offrent à nous concernant l'aspect génie logiciel de notre travail. Nous envisageons à court terme d'étudier les optimisations à apporter aux processus et aux outils utilisés pour la mise en œuvre de notre méthodologie de prototypage rapide.

Une des pistes étudiées consiste à employer d'autres langages pour le code source. Ainsi, nous avions pensé initialement utiliser une chaîne «outils de programmation fonctionnelle» basée sur le langage CaML mais nous n'avions pas approfondi cette piste faute de besoin associé à notre projet du routeur SNG. Pourtant, une chaîne fonctionnelle pourrait s'avérer bien plus adaptée que notre chaîne «programmation impérative» pour les projets de recherche basés, par exemple, sur les mathématiques fondamentales ou issus du domaine de la recherche opérationnelle. D'autre part, nous avons testé la méthodologie sur le routeur SNG en utilisant le langage C. Bien que nous disposions des outils pour utiliser le langage Ada comme langage intermédiaire, nous nous sommes contentés d'évaluer les performances sur une version générée en langage C. Pourtant, le langage Ada présente potentiellement de nombreux avantages, aussi bien en termes de performances et d'optimisation qu'en termes de sûreté et de sécurité de fonctionnement logiciel. Il mériterait aussi un complément d'étude pour évaluer l'impact du langage intermédiaire sur l'application de la méthodologie.

De plus, notre méthodologie effectue un découpage fort entre les classes de partition et les instances de partition, découpage analogue à une classe d'objet et une instance d'objet dans l'approche MDD (Model Driven Development). Ce découpage a été prévu notamment pour préparer la mutation prochaine d'architectures basées sur des processeurs monocore et gérant de manière séquentielle les fils d'exécution à des architectures futures multicore ou multiprocesseurs, voir massivement multicore (GPGPU[20]), où chaque instance peut être associée à son cœur. Les systèmes multicore ont montré leur efficacité dans différents domaines, mais le monde aéronautique semble encore frileux à les intégrer en raison de considérations de sûreté de fonctionnement. Les projets de développement de logiciels avioniques ayant suivi notre méthodologie devraient être adaptables facilement et à moindre coût aux futures architectures parallèles dès que les GPGPU seront disponibles sur le marché des plateformes matérielles pour l'aéronautique. Ceci sera rendu possible en évitant de recommencer l'ensemble du processus de développement et de validation du logiciel.

5.1.1- Développement d'un axe certification pour la safety des logiciels : exemple du système ACAS-X

De nombreux systèmes aéronautiques évoluent pour tirer partie des améliorations des principes de conception actuels pour les systèmes complexes. En particulier, nous souhaitons dans un futur proche pouvoir investiguer des pistes d'application de notre méthodologie de prototypage rapide présentée dans ce manuscrit à d'autres domaines que l'amélioration des communications en environnement contraint. En effet, cette méthodologie peut s'appliquer facilement à d'autres problématiques du monde aéronautique : par exemple, les futurs systèmes de navigation.

Nous souhaiterions en particulier analyser comment cette méthodologie peut faciliter le développement, le test et la certification du futur système d'évitement entre aéronefs qui est en train d'être défini conjointement par la FAA (Federal Aviation Administration) et l'Europe au travers du projet SESAR (WP 9.47). Ce système intitulé ACAS-X (Aircraft Collision Avoidance System) est une évolution du système TCAS (Traffic Alert and Collision

[20] GPGPU : General-purpose computing on graphics processing units

Avoidance System.) qui est utilisé depuis le milieu des années 70 dans les avions commerciaux. Ce nouveau système remplace un algorithme d'évitement classique qui est le fruit d'évolutions successives par une nouvelle conception orientée méthode formelle qui le rendra plus facilement validable à grande échelle. Dans ce contexte, notre méthodologie pourra permettre tirer partie de ce cœur de modélisation formelle pour extraire un modèle de haut niveau qui permettra à l'aide de la chaine d'outils présentée dans ce chapitre de pouvoir dériver rapidement le code logiciel embarqué. Les phases de tests et donc de certification seront également allégées ce qui permettra une accélération du cycle de développement industriel.

5.1.2- Application de cette méthodologie au contexte des drones pour faciliter une certification de ces systèmes

Une autre piste d'application de notre méthodologie concerne les futures évolutions de l'architecture de gestion de la QdS et de sécurité que nous envisageons de définir pour l'environnement UAANET. En effet, un des enjeux pour les années à venir dans le développement des drones et de pouvoir justifier de leur intégration dans tout ou partie de l'espace aérien traditionnel. Pour cela, il sera nécessaire de pouvoir passer les étapes de certification de ces systèmes auprès des organismes de certification (DGAC pour la France ou encore EASA[21] pour l'Europe). Pour cela, l'utilisation de modèles de haut niveau couplés aux méthodes de vérification à base de méthodes formelles permettront de viser un objectif de certification beaucoup plus rapidement et de façon plus efficace qu'avec les méthodes de développement logiciel traditionnelles qui sont utilisées à l'heure actuelle dans le domaine des drones.

5.2- TRAITEMENT CONJOINT DE LA QDS ET DE LA SECURITE DANS LE CADRE DE L'ARCHITECTURE DE COMMUNICATION SESAR

Le travail réalisé dans le cadre de l'AeroMACS (WP 15.2.7), est inscrit dans un cadre plus large d'une architecture de communication de bout en bout. Ce travail est mené dans le cadre du WP 15.2.4. Le travail initié dans le WP 15.2.7 sur l'analyse de risque quantitative représente un point de départ de la contribution que nous envisageons dans le cadre du 15.2.4. En effet, ce travail porte sur la définition de l'architecture de communication qui doit conjointement pouvoir fournir à la fois un niveau de QdS mais aussi un niveau de sécurité satisfaisant. Ce travail a démarré à la fin de l'année 2013 et représente une application intéressante pour nos travaux de gestion conjointe de la QdS et de la sécurité en environnement contraint.

En effet, dans le cadre de ce projet nous seront amenés à définir des mécanismes capables de tirer partie des différentes ressources mises à disposition par la future architecture de communication du projet SESAR. Cette dernière offrira aux aéronefs différents segments de communication disponibles : AeroMACS, L-DACS et SatCom. L'idée de chaque technologie de communication est de couvrir un périmètre spécifique : par exemple, la zone aéroportuaire pour le système AeroMACS, le continent européen pour le système L-DACS ou encore les communications transocéaniques dans le cadre de communications SatCom. Ces segments de communication peuvent potentiellement être disponibles en parallèle au cours d'un même vol. Il s'agit du concept de communication « multilink ». Dès lors, ce concept nécessite de spécifier et de concevoir un système sécurisé qui permettent de proposer différents niveaux de qualité de service (QdS) et qui tire parti du principe « multilink » de l'architecture de communication.

[21] EASA : European Aviation Safety Agency

Il est à noté que le travail qui est mené dans ce projet est encore à la phase de spécification du système final. Ainsi, le travail de définition d'une architecture de bout en bout intégrant des fonctionnalités de gestion de la QdS et de la sécurité dans un contexte multi-lien doit être continué. En particulier, il est nécessaire de finaliser la conception et la mise en œuvre des mécanismes qui ont été introduits de façon partielle dans ce manuscrit. Une autre étape de ce travail portera sur la phase de validation de ces mécanismes en environnement réel.

5.3- NOUVELLES FONCTIONNALITES POUR LES RESEAUX DE DRONES COMMUNIQUANTS

Un certain nombre de fonctionnalités nouvelles ont été introduites pour optimiser les mécanismes de gestion de la QdS et de sécurité à l'environnement contraint que représente un réseau UAANET. Néanmoins, des évolutions à ces travaux peuvent être envisagées à court terme.

5.3.1- Routage basé sur la QdS

L'architecture à gestion de la qualité de service qui a été présentée dans le projet D3COS est un premier niveau de contribution intéressant pour le domaine des UAANET. Néanmoins, de nombreuses pistes d'amélioration méritent d'être investiguées. La plus naturelle à court terme consiste à introduire un nouveau protocole de routage orientée QdS pour permettre de tirer parti des mécanismes de gestion de la QdS qui ont été introduits dans le cadre de l'architecture DAN. Ce mécanisme de routage orienté QdS pourra en particulier tirer parti des études de routage multi chemin qui existent dans la littérature et faire le lien entre la caractéristique hautement maillée d'un réseau UAANET et les mécanismes de gestion de la QdS maintenant disponibles dans cet environnement au travers des propositions qui ont été faites dans ce manuscrit.

5.3.2- Interconnexion avec l'environnement extérieur : intégration dans l'espace aérien classique

Dans le cadre du projet SUANET, nous souhaitons étudier la possibilité d'interconnecter l'environnement UAANET avec des environnements extérieurs. Dans ce projet, un premier niveau d'interfaçage avec des réseaux tiers (type réseau de la sécurité civile par exemple) va être considéré. Néanmoins, à plus long terme, il serait intéressant d'étudier la faisabilité d'une interconnexion avec l'espace aérien traditionnel. En effet, les différentes informations qui y sont échangées permettraient d'augmenter le niveau de performances des systèmes UAVs. En contre partie, il va être nécessaire de pouvoir garantir que cet interfaçage ne nuit pas à la sûreté et à la sécurité du système aérien existant. Pour cela, de nouveaux mécanismes de sécurité à base de proxy sécurisés devront être proposés pour permettre le transit sans risque de compromission des données entre le réseau UAANET et le réseau aérien classique. Les approches orientées modèles permettront de faciliter le développement de ces nouvelles solutions telles que la perspective de la section 5.1.2 l'a déjà mentionné.

5.4- CONTRIBUTION A LA SECURISATION DES COMMUNICATIONS POUR LES RESEAUX AD HOC AERONAUTIQUES

Le domaine de l'aéronautique s'intéresse lui aussi depuis peu à la possibilité de faire communiquer des avions entre eux sans nécessairement utiliser un relais sol ou satellite *(Besse et al., 2010)*. Ce nouveau type de MANET est appelé AANET pour Aeronautical Ad Hoc Network. La caractéristique de sûreté (résistance aux événements accidentels ou involontaires) propre au domaine aéronautique nécessite le développement de techniques

nouvelles de communication qui ne sont pas nécessairement transposables directement depuis le domaine des VANET « traditionnels » (voiture, train ou bateau). En particulier, les AANET mettent en évidence des caractéristiques nouvelles en terme de topologie, vitesse de déplacement, connectivité ou encore trajectoire des nœuds *(Medina et al., 2008)*. De plus, la caractéristique de sécurité (résistance aux événements volontaires malveillants) spécifique à ce type de réseau nécessite la définition de nouvelles solutions de gestion de la sécurité. La sécurisation des communications doit donc être un élément fondamental de l'infrastructure de sécurité des AANET afin d'éviter qu'une attaque visant le lien de communication ne puisse mettre en péril la sureté du vol (on parle dans ce cas de « security for safety »).

Dès lors, l'objet de ce travail de recherche serait de considérer spécifiquement la problématique de la sécurité aéronautique appliquée au contexte des communications dans le cas des réseaux ad hoc aéronautiques. Ce nouveau domaine de communication représente une solution alternative aux techniques de communication plus coûteuses qui font intervenir de nombreuses stations sols ou satellites. En effet, l'utilisation de l'avion comme relais direct de la communication inter aéronefs représente à la fois une technique nouvelle mais aussi moins coûteuse à mettre à œuvre que les techniques traditionnelles de communication utilisées jusqu'alors (infrastructure de communication par satellite par exemple).

Néanmoins, la problématique de la sécurité de ce nouveau système ne peut pas être écartée car dans tous les cas, il faut s'assurer qu'un individu malveillant ne puisse pas tirer partie des vulnérabilités du système de communication pour dégrader ses performances ou pire entraîner une avarie qui pourrait impliquer la perte de vies humaines. L'objet de ce travail de thèse est donc de réfléchir à une solution complète de gestion de la sécurité dans le contexte des réseaux ad hoc aéronautiques.

Le premier axe concerne la définition des mécanismes nécessaires pour permettre le déploiement au sein du réseau ad hoc aéronautique de l'ensemble des clés nécessaires à la mise en œuvre des mécanismes d'authentification, de confidentialité et d'intégrité qui représentent la clé de voûte pour permettre d'augmenter le niveau de robustesse (en termes de sûreté et de sécurité) de cet environnement réseau spécifique. Il sera notamment question de réfléchir et proposer une solution adaptée au contexte des AANET, c'est-à-dire légère par rapport à ce qui peut se faire dans un contexte plus classique de type réseau Internet. En effet, un aéronef constitue un système embarqué dont l'énergie, la puissance de calcul ainsi que l'interopérabilité avec l'environnement extérieur sont, par définition, limitées. Une des pistes de réflexion portera sur la définition de nouveaux protocoles de distribution des clés. En effet, une infrastructure de gestion de clés type LKH (Logical Key Hierarchy) *(Harney & Harder, 1999)* reposant sur une entité centralisée n'est pas adaptée à un réseau AANET qui est distribué par conception.

Le deuxième axe consistera à réfléchir à de nouveaux mécanismes de routage sécurisés permettant l'acheminement des données au sein du réseau AANET. Actuellement des protocoles de routage spécifiquement développés pour les AANET ont déjà été proposés tels que DASR (Delay Aware Multipath Doppler Routing in Aeronautical Ad hoc Networks) *(Gu et al., 2011)*, mais aucun n'a pris en compte la composante sécurité. Ce travail s'appuiera particulièrement sur le protocole de distribution de clés présenté dans le point précédent. En effet, le mécanisme de routage sécurisé qui sera proposé mettra en œuvre des techniques d'authentification et de vérification de l'intégrité qui reposeront sur l'utilisation de clés partagées ou de clés asymétriques (couple clés publiques/privées). Un point important de ce travail consistera à proposer un mécanisme de routage faiblement consommateur en matière de ressources réseaux afin de pouvoir garantir la meilleure utilisation du canal de communication représenté par les liaisons inter-aéronefs dans le cadre d'un AANET. De plus, de nombreux travaux ont été initiés sur l'utilisation de la position

géographique des entités du réseau AANET dans le protocole de routage (lors de l'établissement de la route par exemple). L'information étant facilement accessible à travers les systèmes GPS (Global Positioning system) embarqués à bord, cette piste sera notamment investiguée de façon approfondie. De plus, la notion de groupe sera une composante majeure dans la définition des deux contributions précédentes. Le travail pourra en particulier porter sur des algorithmes de « clustering » dynamique appliqués à la distribution des clés et au mécanisme de routage.

Enfin, le dernier axe de recherche s'intéressera à définir de nouveaux mécanismes d'échange de données sécurisées entre avions. En effet, des avions appartenant à la même compagnie pourront avoir accès aux informations utiles acheminées par l'intermédiaire du réseau AANET alors que des compagnies commercialement concurrentes refuseront certainement de mutualiser leur accès à ces informations sensibles. Dans ce dernier cas de figure, il sera nécessaire de réfléchir à des mécanismes originaux permettant de garantir la confidentialité des échanges inter-compagnies aériennes.

En ce concerne les outils scientifiques qui seront utilisés pour mener à bien ce travail de recherche, il semble important de mentionner que le modèle de mobilité qui sera utilisé pour valider l'ensemble des contributions ci-dessus représentera la pierre angulaire de l'étape de validation. En effet, à l'heure actuelle peu de travaux se sont intéressés à la définition d'un tel modèle spécifiquement dédié à l'environnement aéronautique. En particulier, on peut citer qu'une des caractéristiques spécifiques de déplacement d'un avion est d'avoir une trajectoire à trois dimensions et non pas simplement dans un plan à deux dimensions. De plus, le savoir faire de l'ENAC en matière de contrôle du trafic aérien lui confère un accès privilégié à des traces de trafic aéronautique réelles qui permettraient de développer un modèle de mobilité adapté à ce nouveau trafic et nécessaire pour cette communauté scientifique.

L'utilisation de ces traces réelles représentera donc une possibilité de validation très intéressante pour les travaux portant sur les mécanismes de routage sécurisés ou encore sur la sécurisation des communications de données. De plus, nous envisageons d'utiliser des outils de vérification formelle pour la validation du protocole de distribution des clés mentionné précédemment comme AVISPA (Automated Validation of Internet Security Protocols and Applications). Enfin, la plupart des travaux que nous avons pu lire valident les solutions sous forme de simulations (à l'aide d'outils comme NS-2, OMNET++, QualNet ou encore OPNET) mais les modèles de communication de la couche d'accès utilisés reposent sur des systèmes sans fil de type 802.11 (i.e. WIFI) qui possèdent des caractéristiques (e.g. portée des nœuds, vitesse de déplacements des agents, taille de la zone de couverture géographique) inexploitables dans un environnement aéronautique type AANET. Il faudra donc réfléchir à la technique d'accès qui sera utilisée lors de la phase de validation en simulation et qui permettrait d'obtenir des résultats conformes à un environnement réel.

CHAPITRE 3- ACTIVITE EN MATIERE DE RESPONSABILITES COLLECTIVES

Ce chapitre renseigne sur les différentes activités en matière de responsabilités collectives que j'ai en charge. Elles permettent d'attester de mon implication pour le rayonnement scientifique de la communauté de recherche en réseaux et sécurité des réseaux.

1- ORGANISATION DU WORKSHOP WAS'COM 2014 : IEEE WORKSHOP ON ADAPTIVE TECHNIQUES FOR COMMUNICATION NETWORKS

En 2014, je serai coorganisateur du Workshop IEEE WAS'COM (Workshop on Adaptive Techniques for Communication Networks). Ce colloque sera organisé dans le cadre de la conférence IEEE COMPSAC 2014[22]. Nous sommes deux personnes (Slim Ben Mahmoud et moi-même) responsables de la définition du domaine scientifique visé par ce Workshop, de la communication autour du Workshop, de la sélection des papiers ainsi que du déroulement de ce Workshop. La thématique abordée au cours de ces deux jours de Workshop est en rapport avec les mécanismes adaptatifs qui sont actuellement définis pour les environnements réseaux complexes (et notamment les systèmes intelligents).

2- MEMBRE DU GROUPE DE TRAVAIL EUROCAE WG 82 : « NEW AIR-GROUND DATALINK TECHNOLOGIES »

Depuis 2011, je fais partie du groupe EUROCAE 82. J'ai notamment contribué à la définition et la standardisation du futur système de communication AeroMACS en environnement aéroportuaire.

3- PARTICIPATION AUX COMITES DE RELECTURE

Je suis membre des différents comités de relecture suivants.

- **Revues internationales :** IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Parallel and Distributed Systems, Compuper Communications Journal, Elsevier Ad Hoc Networks Journal.
- **Revue nationale :** Techniques et Sciences Informatiques.
- **Conférences internationales :** Workshop on Protocols for Fast Long-Distance Networks, Workshop on Quality of Future Internet Services, Workshop on Multimedia Interactive Protocols and Systems, International Conference on Internet & Information Technology in Modern Organizations.
- **Conférence nationale :** Colloque Francophone de l'Ingénierie des protocoles.

4- ADMINISTRATION PEDAGOGIQUE AU SEIN DE L'ENAC

- **Enseignant référent** pour le domaine sécurité des réseaux à l'ENAC : dans ce cadre depuis 2006, je dirige **la mise en place et le développement** des activités d'enseignement dans le domaine de la **« sécurité des réseaux »** pour l'ENAC (cursus ingénieur IENAC et IESSA)**.**

[22] Site web de la conférence COMPAC'2014 : http:// ***compsac****.cs.iastate.edu/*

- **Responsable** des **stages de formation continue** (gestionnaire de ressources pédagogiques) : dans ce cadre, je réalise un travail de gestion des intervenants et de planification des cours pour les stages de formation continue suivant : NARCI, SECRE et SECRE++

5- CHARGES COLLECTIVES AU SEIN DE L'ENAC

Depuis 2010, je suis représentant suppléant au Conseil des Etudes de l'ENAC, dans ce cadre, j'assiste aux réunions trimestrielles de ce conseil et contribue aux discussions sur les orientations pédagogiques au sein de l'ENAC.

CHAPITRE 4- ACTIVITE EN MATIERE D'ENSEIGNEMENT

Ce chapitre renseigne sur les différentes activités en matière d'enseignement que je mène en parallèle de mes activités de recherche décrites de façon détaillée dans le chapitre 2 de ce document.

Depuis le début de mes activités d'enseignement (octobre 2002), ma charge d'enseignement se découpe entre les différents domaines :

- **Sécurité dans les réseaux** : cours, TP et projet ;
- **Réseaux informatiques** : cours, TD, TP et projet ;
- **Administration système et réseau** : TP ;
- **Algorithmique** : cours, TD, TP et projet ;
- **Programmation système** : TP ;
- **Programmation réseau** : TD et TP ;
- **Génie Logiciel** : TD, TP et projet ;
- **Informatique** : cours et TP.

Ces activités se répartissent entre deux établissements : l'ENAC et l'INSA de Toulouse. Une première phase (jusqu'à août 2006) représente mes activités d'enseignement réalisées en tant que moniteur puis ATER. La deuxième phase à partir de septembre 2006 représente mon activité d'enseignement en tant qu'enseignant-chercheur.

1- PERIODE 10/2002-08/2006 : MONITEUR PUIS ATER A L'INSA DE TOULOUSE

J'ai, tout d'abord, réalisé 3 années d'enseignement (**192 heures équivalent TD au total**) en tant que moniteur à l'INSA de Toulouse. Mon volume horaire était de 64 heures équivalent TD par année et se détaillait comme suit.

Remarque :

- *Pour l'ensemble des enseignements détaillés ci-après, les heures de « Cours » ont été dispensées à des groupes de 48 étudiants, les « TD » à des groupes de 24 étudiants et les « TP » à des groupes de 12 étudiants.*
- *Les enseignements de spécialité ont été dispensés dans le département Génie Electrique et Informatique (GEI), dans les filières **Automatique Electronique et Informatique** (AEI), **Génie Informatique et Industriel** (GII), **Réseaux et Télécommunications** (RT) et **Temps Réel et Systèmes** (TRS).*

***Première année de monitorat** – 64 H eq. TD (octobre 2002 - septembre 2003)*

- **Introduction à l'algorithmique** (langage ADA) – 1ère année INSA (premier cycle - PC) – étudiants sportifs de haut niveau : *14 H TD + 33 H TP*
- **Perfectionnement en algorithmique** (langage ADA) – 2ème année INSA (PC) : *54 H TP + 18 H projet TP*

***Deuxième année de monitorat** – 64 H eq. TD (octobre 2003 - septembre 2004)*

- **Perfectionnement en algorithmique** (langage ADA) – 2ème année INSA (PC) : *7,5 H TD + 18 H TP*

- **Algorithmique avancée** (langage ADA) – 3ème année INSA (département GEI – filière GII) : *48 H TP + 18 H projet TP*
- **Caractérisation du trafic et métrologie de l'Internet** (langage C, programmation réseau, Matlab, évaluation de performances) – 5ème année INSA (département GEI – filière RT) : *6 H TD*

***Troisième année de monitorat** – 64 H eq. TD (octobre 2004 - septembre 2005)*

- **Introduction à l'algorithmique** (langage ADA) – 1ème année INSA (PC) – étudiants étrangers asiatiques (ASINSA) : *10 H Cours + 6 H TD*
- **Introduction au langage C** (langage C – Linux) – 3ème année INSA (département GEI – filière GII) : *6 H TP*
- **Programmation système** (langage C – Linux) – 4ème année INSA (département GEI – filière GII): *21 H TP*
- **Conception orientée objet** (UML – programmation objet) – 4ème année INSA (département GEI – filière GII) : *12 H TP*
- **Programmation réseau** (langage C – programmation Socket – Linux) – 5ème année INSA (département GEI – filière TRS) : *6 H TP*
- **Caractérisation du trafic et métrologie de l'Internet** (langage C – programmation réseau – langage de script – Matlab) – 5ème année INSA (département GEI – filière RT) : *16 H TD*
- **Evaluation de performances** (simulateur réseau NEST – langage C – calculs statistiques) – 5ème année INSA (département GEI – filière RT) : *12 H TP*

***ATER** – 96 H eq. TD (mars 2006 - août 2006)*

J'ai ensuite dispensé un mi-temps d'enseignement en tant qu'ATER à l'INSA de Toulouse entre mars et août 2006 soit un total sur 6 mois de 96 heures équivalent TD d'enseignement.

- **Perfectionnement en algorithmique** (langage ADA) – 3ème année INSA (département GEI – filière GII / RT) : 4 *H TD + 33 H TP*
- **Conception orientée objet** (UML – programmation objet) – 4ème année INSA (département GEI – filière AEI) : *6,25 H TD*
- **Programmation orientée objet** (programmation objet – langage JAVA) – 4ème année INSA (département GEI – filière RT) : 8,25 *H TP*
- **Programmation réseau** (langage C – programmation Socket – Linux) – 4ème année INSA (département GEI – filière GII) : 1*8 H TD*
- **Analyse du trafic réseau** (TCPDUMP – programmation Socket – Linux) – 4ème année INSA (département GEI – filière RT) : 20 *H TD*

2- PERIODE A PARTIR DE 09/2006 : ENSEIGNANT-CHERCHEUR

***ENAC** – 1424 H eq. TD (depuis septembre 2006)*

Depuis septembre 2006, **je suis enseignant-chercheur en réseaux informatiques, spécialité sécurité dans les réseaux,** à l'ENAC de Toulouse où je dispense les mêmes

fonctions d'enseignement qu'un Maître de conférences. Pour cela je réalise une charge d'enseignement d'environ **200 h eq. TD / an.**

En particulier, **je suis en charge de la mise en place des nouveaux enseignements de « sécurité dans les réseaux »** pour le département SINA de l'ENAC**.** Pour cela, j'ai **défini, conçu et dispensé** l'ensemble des enseignements suivants :

- **Sécurité dans les réseaux** : 350 H de cours, 324 H de TP et 130 H de projet,
- **Réseaux informatiques** : 90 H de cours, 147 H de TP et 70 H de projet,
- **Administration système et réseau** : 36 H de TP,
- **Génie Logiciel** : 70 H de projet.

J'ai, de plus, dispensé des enseignements déjà existants dans les cursus ENAC dans les domaines ci-après :

- **Réseaux informatiques** : 60 H de cours et 136 H de TP,
- **Informatique** : 20 H de cours et 66 H de TP.

Chaque enseignement mentionné dans cette section (cours ou TP) a nécessité la définition et la rédaction de supports de cours de taille variable en fonction du volume horaire de l'enseignement.

La plupart des supports de cours de l'ENAC sont soumis à des droits de non diffusion à l'extérieur de l'établissement. Pour cette raison, ils ne se trouvent pas sur un site web téléchargeable, néanmoins dans le cadre de la rédaction de cette habilitation à diriger les recherches, je pourrai fournir sur demande une copie papier des différents supports de cours qui pourront s'avérer nécessaires pour l'évaluation de mon dossier de candidature (pour toute demande merci de me contacter par mail nicolas.larrieu@enac.fr ou téléphone 0628070519). Les examinateurs de ma candidature peuvent également consulter le site http://www.nicolas-larrieu.com/, ils y trouveront un certain nombre de documents pédagogiques mis en ligne et libres de droit.

Le détail des enseignements que j'ai dispensés est présenté ci-dessous.

Interventions en formation initiale :

Technicien Supérieur de l'Etude et l'Exploitation de l'Aviation Civile (niveau BAC+2) :

- **Introduction aux réseaux informatiques** (42 H de cours et 72 H de TP) : module de vulgarisation où sont abordées les notions fondamentales d'interconnexion de réseau, d'administration de réseau, d'application client-serveur pour l'Internet et de sécurité informatique et réseau.

Ingénieur du Contrôle et de la Navigation Aérienne (niveau BAC+5) :

- **Introduction aux réseaux informatiques** (18 H de cours) : module de vulgarisation où sont abordées les notions fondamentales d'interconnexion de réseau dans le contexte spécifique des réseaux de la navigation aérienne.

Ingénieur Electronicien des Systèmes de Sécurité Aérienne - IESSA (niveau BAC+4/5) :

- **Techniques et mécanismes de sécurité réseau** (72 H de cours + 100 H de TP) : voir descriptif détaillé section suivante ;
- **Introduction aux techniques de caractérisation de trafic pour l'Internet** (9 H de cours + 6 H de TP) ;
- **Techniques d'accès réseau à distance** : protocole d'accès à distance, tunneling sécurisé, NAT, PAT et mobilité (9 H de cours + 24 H TP) ;

- **Applications du monde Internet** (9 H de cours + 36 H de TP) : module d'introduction au fonctionnement des principales applications client-serveur de l'Internet ;
- **Mise en œuvre des techniques de Voix sur IP** (8 H de TP) ;
- **Services réseaux : NTP et DNS** (36 H de TP) ;
- **Supervision réseau : SNMP** (24 H de TP) ;
- **Fonctionnement des protocoles TCP/UDP** (8 H de TP).

Ingénieur ENAC (niveau BAC+4/5)

- **Techniques et mécanismes de sécurité réseau** (70 H de cours + 28 H de TP) ;
- **Techniques et outils de métrologie pour l'Internet** (21 H de cours + 24 H de TP) ;
- **Introduction aux réseaux locaux** (24 H de TP) ;
- **Introduction à la programmation d'applications client-serveur pour l'Internet** (36 H de TP) ;
- **Projets** en binôme d'étudiants d'une durée de 12 à 24 semaines (soit un volume de 70 H eq. TD par projet) permettant d'illustrer des points particuliers des enseignements comme par exemple :
  - *Etude des faiblesses des mécanismes de sécurité du protocole « Wifi » ;*
  - *Réalisation et déploiement d'une plateforme de configuration et d'administration d'un parc de machines linux pour une salle de TP* ;
  - *Développement d'un module de décodage du trafic radar ASTERIX pour le logiciel Wireshark*.

Master « Cooperative Avionics » (niveau BAC+5 cours dispensé **en langue anglaise**)

- **Overview of datalink security techniques: notions for secure aeronautical datalink systems** (24 H de cours) : cours avancés sur les futures techniques et architecture de sécurité des communications sol-bord aéronautiques

Master « Air Trafic Management » (niveau BAC+5 cours dispensé **en langue anglaise**)

- **Security and QoS for Networking** (24 H de cours) : introduction pour une vulgarisation des principales notions de sécurité informatique et réseau pour un public d'étudiant en master non spécialiste du domaine.

Interventions en formation continue :

J'interviens par ailleurs dans différents stages de formation continue sur site ou à l'ENAC dispensés aux fonctionnaires IESSA en poste dans les différents organismes de la DGAC[23] (aéroports, centre de contrôle en route, approches…). La description de ces stages est disponible sur le site de l'ENAC, les intitulés sont les suivants : **NARCISSE** (Nouvelle ARChitecture d'Interconnexion SécuriSéE), **SECRE** (SECurité des Reseaux), **SECRE++** (SECurité des Reseaux avancées) et **MESANGE** (MESsagerie Aéronautique de Nouvelle GEnération) et représentent au total une charge d'enseignements (cours et TP) d'environ 8 semaines à temps plein (soit 150 H de cours et 333 H de TP), les thématiques abordées vont des principes fondamentaux des réseaux de communication jusqu'aux fonctionnalités avancées des réseaux de l'aviation civile (par exemple les nouvelles architectures de sécurité ou encore les mécanismes de détection d'intrusion et d'audit).

[23] DGAC : Délégation Générale de l'Aviation Civile

***Vacataire à l'INSA de Toulouse** – 113 H eq. TD (depuis septembre 2007)*

Depuis septembre 2007, j'ai repris en tant que vacataire certains des enseignements que j'ai dispensés au cours de mon monitorat et de mon poste d'ATER à l'INSA de Toulouse.

- **Perfectionnement en algorithmique** (langage ADA) – 2ème année INSA (filière IMACS) : *20 H TD + 36 H TP*
- **Algorithmique avancée** (langage ADA) – 3ème année INSA (filière IMACS) : *20 H TD + 24 TP*
- **Structure de données avancées** (langage ADA) – 3ème année INSA (filière MIC) : *18 TP*
- **Caractérisation du trafic et métrologie de l'Internet** (langage C – programmation réseau – langage de script – simulateur NS – calcul statistiques) – Bureau d'étude 5ème année INSA (département GEI – filière RT) : *32 H TP*

3- RECAPITULATIF DES ENSEIGNEMENTS

A titre d'information synthétique, je fournis le recensement des enseignements par thématique et de façon chronologique que j'ai pu réaliser au travers de mon parcours de doctorant, ATER et enseignant-chercheur depuis 2002.

Récapitulatif thématique de l'ensemble des enseignements dispensés

	Cours (H)	*TD (H)*	*TP (H)*	*Projet (H)*	**Total (H eq. TD)**
Sécurité dans les réseaux	350		324	130	*935*
Réseaux informatiques	150	22	283	70	*436*
Administration système et réseau			70		*46*
Algorithmique	10	72	192	36	*239*
Programmation système			21		*14*
Programmation réseau		38	6		*42*
Génie Logiciel		6	20	70	*66*
Informatique	80		66		*74*
Total	**590**	**138**	**982**	**306**	**1853**

Récapitulatif chronologique de l'ensemble des enseignements dispensés

	Cours (H)	*TD (H)*	*TP (H)*	*Projet (H)*	**Total (H eq. TD)**
INSA (1ère année monitorat)		14	87	18	*64*
INSA (2ème année monitorat)		18	66	18	*64*
INSA (3ème année monitorat)	10	22	57		*64*
ATER		48	41		*96*
ENAC formation initiale	250		340	270	*782*
ENAC formation continue	330		262		*670*
INSA (vacations)		40	110		*113*
Total	**590**	**138**	**982**	**246**	**1853**

CHAPITRE 5- BIBLIOGRAPHIE DU MANUSCRIT D'HDR

(Abadi & Cortier, 2005) M. Abadi and V. Cortier, Deciding knowledge in security protocols under (many more) equational theories. In Proc. 18th IEEE Computer Security Foundations Workshop (CSFW'05), Aix-en-Provence, France, June 2005, pages 62-76. IEEE Comp. Soc. Press, 2005.

(Abrial, 1996) Jean-Raymond Abrial. The b-book, assigning programs to meanings. Cambridge University Press, 1996.

(Adjih et al., 2003) Cedric Adjih, Thomas Clausen, P. J. & Raffo, D., 'Securing the olsr protocol', In Proceedings of the 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop, Mahdia, Tunisia, June 25, 27, 2003.

(Ahn et al., 2002) G.-S. Ahn, A. Campbell, A. Veres, and L.-H. Sun, "Swan: service differentiation in stateless wireless ad hoc networks," in INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol. 2, pp. 457–466 vol.2, 2002.

(ARINC811, 2005) Airlines Electronic Engineering Committee (AEEC) ARINC811. ARINC Standards 811 Commercial Aircraft Information Security Concepts of Operation and Process Framework, 12/2005.

(ARINC821, 2008) Airlines Electronic Engineering Committee (AEEC) ARINC821. ARINC Standards 821 Aircraft Network Server System (NSS) Functional Definition, 12/2008.

(ARINC823P1, 2007) Digital Security Committee (DSEC), ARINC Specification 823P1 823P1 DataLink Security, Part 1 - ACARS Message Security, 2007

(Basagni et al., 1998) S.Basagni, I.Chlamtac, V. R. & B.a.Woodward, 'A Distance ROUTING E_ect Algorithm for mobility (DREAM)', the fourth annual ACM/IEEE international Conference on Mobile computing and networking (MobiCom '98), Pages 76-84, 1998.

(Ben Mahmoud, 2012) Mohamed S. Ben Mahmoud. Addressing Security Challenges in Emerging Data-based Aeronautical Communications. PhD thesis, Institut National des Sciences Appliquées de Toulouse (INSA Toulouse), February 2012.

(Bento, 2008) M. de Fatima Bento, «Unmanned Aerial Vehicles» wo18.15 GNSS, January/February 2008, available in : http://www.insidegnss.com/auto/janfeb08-wp.pdf

(Bertot, 2011) Yves Bertot et Pierre Castéran. Le Coq'Art (v8). http://www.labri.fr/perso/casteran/CoqArt/coqartF.pdf vu en 01/2014.

(Besse et al., 2010) Frédéric Besse, Alain Pirovano,Fabien Garcia, José Radzik, "Aeronautical Ad Hoc Networks : a new Datalink for ATM", INO 2010, 9th Innovative Research Workshop & Exhibition, 7-9 Dec. 2010, EUROCONTROL Experimental Center, Brétigny-sur-Orge, France.

(Bhagwat, 1994) Bhagwat, C. E. P. &. P. (1994), 'Highly dynamic destination sequenced distance-vector routing (dsdv) for mobile computers', 94 Conference on Communications Architectures, Protocols and Applications, p. 234_244.bhagwat

(Blake et al., 1998) S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services." RFC 2475 (Informational), Dec. 1998. Updated by RFC 3260.

(Braden et al., 1994) R. Braden, D. Clark, and S. Shenker, "Integrated Services in the Internet Architecture: an Overview." RFC 1633 (Informational), June 1994.

(Bhushan, 2004) Kanwal Rai Bhushan. Strategic Decision Making : Applying the Analytic Hierarchy Process. Springer-Verlag, London, 2004.

(Camp et al., 2002) T. Camp, J. Boleng, and V. Davies, “A survey of mobility models for ad hoc network research,” WIRELESS COMMUNICATIONS & MOBILE COMPUTING (WCMC): SPECIAL ISSUE ON MOBILE AD HOC NETWORKING: RESEARCH, TRENDS AND APPLICATIONS, vol. 2, pp. 483–502, 2002.

(cc1, 2009) cc1. Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model, July 2009.

(cc2, 2009) cc2. Common Criteria for Information Technology Security Evaluation Part 2 : Security functional components, July 2009.

(cc3, 2009] cc3. Common Criteria for Information Technology Security Evaluation Part 3 : Security assurance components, July 2009.

(cc4, 2009) cc4. Common Methodology for Information Technology Security Evaluation Evaluation methodology, July 2009.

(Chakeres et al., 2004) D. Chakeres, I, M. Belding, E. Royer, (2004), 'AODV Routing Protocol Implementation Design', Proceedings of the International Workshop on Wireless Ad Hoc Networking(WWAN), Tokyo, Japan, March 2004.

(CNES, 2009) CNES. SATCOM for ATM : Estimation of Capacity Required for AMS(R)S Communications Around 2020 Over European Area, 07 2009.

(COCR, 2007) Communications Operating Concept and Requirements for Future Radio System, Released: 01/05/2007 Edition: 2.0., EUROCONTROL.

(Corson & Macker, 1999) S. Corson and J. Macker, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, University of Maryland, Naval Research Laboratory Request for Comments: 2501, January 1999

(DO-178B, 1992) SC-167 DO-178B. Software considerations in airborne systems and equipment certification. Radio Technical Commission for Aeronautics, 12/1/1992.

(DO-178C, 2011) SC-205 DO-178C. “Software considerations in airbone systems and equipment certification”. Radio Technical Commission for Aeronautics, 12/13/2011

(DO-331, 2011) SC-205 DO-331. “Model-based development and verification supplement to DO-178C and DO-278A”. Radio Technical Commission for Aeronautics, 12/13/2011

(DO-333, 2012) SC-205 DO-333. “Formal Methods Supplement to DO-178C and DO-278A”. Radio Technical Commission for Aeronautics, 01/05/2012.

(Frigault & Wang, 2008) M. Frigault and Lingyu Wang. Measuring network security using bayesian network-based attack graphs. In Proc. 32nd Annual IEEE Int. Computer Software and Applications COMPSAC '08, pages 698-703, 2008.

(Garside et Pighetti, 2009) R. Garside and F. Pighetti. Integrating modular avionics : A new role emerges. Aerospace and Electronic Systems Magazine, IEEE, 24(3) :31 –34, march 2009.

(Gu et al., 2011) Wenzhe Gu; Jinglin Li; Maohui Lv; Qibo Sun; Fangchun Yang, "Delay Aware Multipath Doppler Routing in Aeronautical Ad hoc Networks," 14th IEEE International Conference on Computational Science and Engineering (CSE), 2011.

(Haas, 1997) Haas, Z. J., 'A new routing protocol for the reconfigurable wireless networks', dans Proc. 6th IEEE Int'l Conf. on Universal Personal Communications(ICUPC'97) (San Diego, CA, USA) vol. 2, p. 562_566, 1997.

(Hafslund et al., 2004) Andreas Hafslund, Andreas Tonnesen, Roar Bjorgum, Jon Andersson and Oivind Kure. (2004), 'Secure extension to the olsr protocol', In OLSR Interop and Workshop, August 2004.

(Hao & Chao, 2007) Wu Hao & Cheng Chao, L. C.-s., 'Research on One Kind of Improved GPSR Secure Routing Protocol', IEEE 2007 International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2007.

(Harney & Harder, 1999) Hugh Harney, Eric Harder, "Logical Key Hierarchy Protocol", IETF Internet Draft, 1999.

(Hoare, 1969) C.A.R.Hoare. An Axiomatic Basis for Computer Programming. Communications of the ACM, 12(10):576–585, October 1969. Disponible à http://www.spatial.maine.edu/~worboys/processes/hoare%20axiomatic.pdf. Lien vérifié en 01/2014.

(Jacquet, 2003) Jacquet, T. C. &. P. (2003), 'Optimized Link State Routing Protocol (OLSR)', RFC 3626.

(Karp, 2000) Karp, H. T. K., 'GPSR: Greedy perimeter stateless routing for wireless networks', 6th ACM/IEEE Int'l Conf. on Mobile Computing and Networking (MobiCom 2000) (Boston, MA, USA), ACM Press, p.243-254, 2000.

(Kondakci, 2010) S. Kondakci. A causal model for information security risk assessment. In Proc. Sixth Int Information Assurance and Security (IAS) Conf, pages 143-148, 2010.

(Land et Elliott, 2009) Ian Land and Jeff Elliott. Architecting ARINC 664, Part 7 (AFDX) Solutions. Xilinx, May 2009.

(Lee & Campbell, 1998) S. Lee and A. Campbell, “Insignia: In-band signaling support for QoS in mobile ad hoc networks,” in Proc of 5th International Workshop on Mobile Multimedia Communications (MoMuC), (Berlin, Germany), October 1998.

(Leland et al., 1994) Leland W. E., Taqqu S. M., Willinger W. and Wilson D. V., On the Self-Similar Nature of Ethernet Traffic, (Extended Version) IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 2, NO. 1, FEBRUARY 1994

(Liu & He, 2010) Yanheng LIU, Junting HE, J. W., 'Enhancing GPSR's Credibility Using Experienced Trustiness for VANET', Journal of Computational Information Systems 6:8(2010), 2537-2544. 2010.

(Maltz, 1996) Maltz, D. B. J. 'Dynamic source routing in ad hoc wireless networks', Mobile Computing (T. Imielinski & H. Korth, eds), Kluwer Academic Publishers vol. 353, p. 153-181,1996.

(MathWorks, 2013a) The MathWorks. Matlab R2012b. http ://www.mathworks.fr/, 04 2013.

(MathWorks, 2013b) The MathWorks. Simulink, logiciel de modélisation système multiphysique. http ://www.mathworks.com/products/simulink/, 04 2013.

(MathWorks, 2013c) The MathWorks. Stateflow, logiciel de modélisation de diagrammes à états. http ://www.mathworks.com/products/stateflow?s_cid=wiki_stateflow_2, 04 2013.

(Medina et al., 2008) Medina, D.; Hoffmann, F.; Ayaz, S.; Rokitansky, C.-H., "Topology characterization of high density airspace aeronautical ad hoc networks," 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008.

(Olivier & Benameur, 2000) Olivier P. and Benameur N., Flow Level IP traffic characterization, France Télécom, 2000

(Papadimitratos & Haas, 2003) Papadimitratos, P. & Haas, Z. J., 'Secure message transmission in mobile ad hoc networks. Ad Hoc Networks', Ad Hoc Networks, 193-209, 2003.

(Pathak & Yao, 2008) Vivek Pathak, Danfeng Yao, L. I., 'Securing Geographical Routing in Mobile Ad hoc Networks', Technical report, Rutgers University CCC Pervasive Computing Intiative Grant and by the NSF grant CNS-0520123, 2008.

(PikeOS, 2011) Sysgo PikeOS Real-Time Operating System, December 2011. http ://www.sysgo.com/products/pikeos-rtos-and-virtualization-concept/.

(QEMU, 2011) QEMU, a generic and open source machine emulator and virtualizer, December 2011. http ://wiki.qemu.org/.

(Royer, 1999) Royer, C. E. P., 'Ad hoc on-demand distance vector routing', 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99) (New Orleans, Lousiana, USA), 1999, p.90-100.

(Rushby, 1981) J. M. Rushby. Design and verification of secure systems. SIGOPS Oper. Syst. Rev., vol. 15, no. 5, pages 12–21, December 1981.

(Saaty, 2008) Thomas L. Saaty. Relative Measurement and its Generalization in Decision Making : Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors - The Analytic Hierarchy/Network Process. RACSAM, 2008.

(Samundiswary, & Dananjayan, 2010) P. Samundiswary, D. & Dananjayan, P., 'SECURED GREEDY PERIMETER STATELESS ROUTING FOR WIRELESS SENSOR NETWORKS', International Journal of Ad hoc, Sensor & Ubiquitous Computing(IJASUC) Vol.1, No.2., June 2010.

(Sanzgiri et al., 2002) Kimaya Sanzgiri, Bridget Dahill, B. & Belding-Royer, E. M. (2002), 'A secure routing protocol for ad hoc networks', In ICNP, IEEE Computer Society, 78,89. 2002.

(Toom et al., 2008) Andreas Toom and al. Gene-auto : An automatic code generator for a safe subset of simulink/stateflow and scicos. In 4th European Congress ERTS Embedded Real Time Software, 2008.

(Vaidya, 1998) Vaidya, Y.-B. K., 'Location-aided routing (Lar) in mobile ad hoc networks', 4th ACM/IEEE Int'l Conf. on Mobile Computing and networking (MobiCom'98) (Dallas, TX, USA), ACM Press, p. 66_75, 1998.

(Yau & Zhang, 1999) S. S. Yau and Xinyu Zhang. Computer network intrusion detection, assessment and prevention based on security dependency relation. In Proc. Twenty-Third Annual Int. Computer Software and Applications Conf. COMPSAC '99, pages 86-91, 1999.

(Zapata & Asokan, 2002) Zapata, M. G. & Asokan., N. (2002), 'Securing ad hoc routing protocols', Workshop on Wireless Security, pages 1,10. 2002

(Zhang et al., 2004) Yong-Zheng Zhang, Bin-Xing Fang, and Xiao-Chun Yun. A risk assessment approach for network information system. In Machine Learning and Cybernetics, 2004. Proceedings of 2004 International Conference on, volume 5, pages 2949-2952 vol.5, aug. 2004.

CHAPITRE 6- LISTE DES PUBLICATIONS DE L'AUTEUR

La liste des publications qui suit renseigne sur les différentes publications réalisées par l'auteur de ce manuscrit d'HDR.

La catégorie ouvrage fait référence à des ouvrages rédigés par l'auteur et ses collègues directs (laboratoire TELECOM de l'ENAC) de façon intégrale alors que la catégorie contribution à ouvrage représente un chapitre d'un ouvrage plus général (qui peut être une compilation de travaux d'équipes différentes) où l'auteur n'a contribué qu'à un chapitre de l'ouvrage. Les publications de type ouvrage sont le résultat d'un processus de sélection réalisé par l'éditeur lui-même (éditions ISTE Wiley dans les deux cas) alors que pour les contributions à ouvrage il s'agit de chapitres de livre qui ont été rédigés sur invitation des rédacteurs en chef des ouvrages mentionnés (Bernard Reber et Claire Brossaud).

Ouvrage International (livre intégral) :

(Ben Mahmoud et al., 2013) S. BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, Risk Propagation Assessment for Network Security Application to Airport Communication Network Design, ISTE, Wiley, 2012, 144 pages, mars 2013, ISBN: 9781848214545.

Contribution à Ouvrage International (chapitre de livre) :

(Larrieu & Owezarski, 2010) **N. LARRIEU**, P. OWEZARSKI, "Metrology of Internet networks", Digital Cognitive Technologies. Epistemology and Knowledge Society, Wiley Editions, 24 pages, septembre 2010, ISBN: 9781848210738.

Revues Internationales avec Comité de Lecture :

(Varet & Larrieu, 2013) A. VARET, **N. LARRIEU**, "How to assess the quality of source codes in a model driven software design approach - Application to aeronautical embedded system design", AIAA Journal of Aerospace Information Systems, submitted, under review, 2013.

(Bouachir et al., 2013a) O. BOUACHIR, F. GARCIA, **N. LARRIEU**, T. GAYRAUD, "Survey of Communication Architectures In UAV Ad hoc Networks: Toward Cooperative Operations", IEEE Communications Magazine, submitted, under Review. 2013.

(Ben Mahmoud et al., 2012a) M. S. BEN MAHMOUD, A. PIROVANO, **N. LARRIEU**, "Aeronautical Communication Transition From Analog to Digital Data: A Network Security Survey", Elsevier Computer Science Review Journal, accepted for publication, fall 2014.

(Varet & Larrieu, 2014a) A. VARET, **N. LARRIEU**, "How to generate realistic network traffic profiles in theory and practice?", Computer and Information Science, Canadian Center of Science and Education, accepted for publication, Volume 8, April 2014.

(Scherrer et al., 2007a) A. SCHERRER, **N. LARRIEU**, P. OWEZARSKI, P. BORGNAT, P. ABRY, "Non Gaussian long memory model for Internet traffic : Application to DDoS detection", Annals of Telecommunications, juillet 2007.

(Scherrer et al., 2007b) A. SCHERRER, **N. LARRIEU**, P. OWEZARSKI, P. BORGNAT, P. ABRY, "Non Gaussian and long memory statistical characterisations for internet traffic with

anomalies", Rapport LAAS N°05303, août 2007, 12 pages, IEEE Transactions on Dependable and Secure Computing.

(Owerzarski et al., 2005a) P. OWEZARSKI, **N. LARRIEU**, L. BERNAILLE, W. SADDI, F. GUILLEMIN, A. SOULE, K. SALAMATIAN, "Distribution of traffic among applications as measured in the French METROPOLIS project", Rapport LAAS, octobre 2005, 13 pages, revue Annals of Telecommunications, special issue "Analysis of traffic and usage traces on the Internet - From network engineering to sociology of uses".

(Larrieu & Owezarski, 2005a) **N. LARRIEU**, P.OWEZARSKI, "Towards a measurement based networking approach for internet QoS improvement", LAAS report N°04193, Computer Communications Journal, Issue 3, Vol.28, pp.259-273, février 2005, 29p.

(Owezarski & Larrieu, 2003) P. OWEZARSKI, **N. LARRIEU**, "Coherent charging of differentiated services in the internet depending on congestion control aggressiveness", Computer Communications Journal, Issue 13, Vol.26, pp.1445-1456, août 2003.

Ouvrage Francophone (livre intégral) :

(Varet & Larrieu, 2014b) A. VARET, **N. LARRIEU**, « Méthodologie de prototypage rapide de logiciels pour les systèmes avioniques - Contribution des approches orientées modèles pour la certification de systèmes complexes », ISTE, Wiley, 100 pages, accepté pour publication, mai 2014.

Contribution à Ouvrage Francophone (chapitre de livre) :

(Larrieu & Owezarski, 2007) **N. LARRIEU**, P. OWEZARSKI, « Métrologie des réseaux de l'internet », Humanités numériques Tome 1, Hermès Science, Traité IC2 Information-Commande-Communication, mai 2007, pp.131-145, ISBN : 9782746216617.

Revues Nationales avec Comité de Lecture :

(Larrieu & Varet, 2014) **N. LARRIEU**, A. VARET, Méthodologie orientée modèle pour le prototypage rapide de systèmes complexes - Application à l'avionique embarquée de nouvelle génération « Techniques et outils de métrologie pour l'Internet et son trafic », janvier 2014, en cours de relecture.

(Owezarski & Larrieu, 2007) P. OWEZARSKI, **N. LARRIEU**, « Techniques et outils de métrologie pour l'Internet et son trafic », réf TI-R1090, publiée en juin 2007, 46 pages, revue Techniques pour l'Ingénieur, série « Mesures des Telecommunications ».

(Larrieu & Owezarski, 2004) **N. LARRIEU**, P. OWEZARSKI, « De la métrologie pour l'ingénierie des réseaux de l'Internet », « Technique et Sciences Informatiques » journal, numéro spécial « Réseaux et Protocoles », vol. 23, n°5-6/2004, septembre 2004, 33 p.

Conférences Internationales avec Comité de Lecture :

(Larrieu, 2014) **N. LARRIEU**, "How can model driven development approaches improve the certification process for UAS?", IEEE ICUAS 2014, submitted, under review.

(Varet & Larrieu, 2014c) A. VARET, **N. LARRIEU**, ”A new tool to generate realistic network traffic”, IEEE COMPSAC 2014, submitted, under review.

(Bouachir et al., 2013b) O. BOUACHIR, F. GARCIA, **N. LARRIEU**, T. GAYRAUD, “Ad hoc Network QoS Architecture For Cooperative Unmanned Aerial Vehicles (UAVs)”, Wireless Days Conference, Barcelone, 2013.

(Ben Mahmoud & Larrieu, 2013a) M. S. BEN MAHMOUD, **N. LARRIEU**, “An ADS-B based Secure Geographical Routing Protocol for Aeronautical Ad Hoc Networks”, IEEE 36th Annual Computer Software and Applications Conference (COMPSAC), 2013

(Varet et al., 2013) A. VARET, L. SARTRE, **N. LARRIEU**, ”METRIX: a new tool to evaluate the quality of software source codes”, AIAA Infotech 2013.

(Varet & Larrieu, 2012a) A. VARET, **N. LARRIEU**, ” Security capability discovery protocol over unsecured IP-based topologies”, 8 pages, SAR (Security in Network Architectures) – SSI (Security in Information Systems) 2012, Cabourg, May 2012

(Varet & Larrieu, 2012b) A. VARET, **N. LARRIEU**, C. MACABIAU, ”Design and development of an embedded aeronautical router with security capabilities”, ICNS 2012, Avril 2012.

(Ben Mahmoud et al., 2012b) M. S. BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, ”Quantitative Risk Assessment to Enhance AeroMACS Security in SESAR”, 12 pages, ICNS 2012, Avril 2012.

(Ben Mahmoud et al., 2011a) M. S. BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, ”A Quantitative Risk Analysis of AeroMACS Security in SESAR”, SAE Aerotech 2011, Toulouse, November 2011, oral presentation only.

(Varet & Larrieu, 2011) A. VARET, **N. LARRIEU**, ”New Methodology To Develop Certified Safe And Secure Aeronautical Software”, 14 pages, Digital Avionics Systems Conference (DASC-2011), Seattle, USA, October 2011.

(Ben Mahmoud et al., 2011b) M. S. BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, ”A Risk Propagation Based Quantitative Assessment Methodology for Network Security”, 16 pages, SAR (Security in Network Architectures) – SSI (Security in Information Systems) 2011, La Rochelle, May 2011

(Ben Mahmoud et al., 2010a) M. S. BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, A. VARET, ”An adaptive security architecture for future aircraft communications”, 15 pages, Digital Avionics Systems Conference (DASC-2010), Utah, October 2010.

(Ben Mahmoud et al., 2010b) M. S. BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, ”A Performance-aware Public Key Infrastructure for Next Generation Connected Aircrafts”, extended abstract, 15 pages, Digital Avionics Systems Conference (DASC-2010), Utah, October 2010.

(Ben Mahmoud et al., 2010c) M. S. BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, ”Security architecture design for satellite aeronautical data link communications”, 12 pages, AIAA SPACE 2010 Conference & Exposition/28th AIAA International Communications Satellite Systems Conference (ICSSC-2010), California, September 2010.

(Ben Mahmoud et al., 2009a) M. S. BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, ”An Aeronautical Data Link Security Architecture Overview”, 8 pages, 28th Digital Avionics Systems Conference (DASC’09), 25-29 October 2009, Orlando, Florida.

(Scherrer et al., 2006a) A. SCHERRER, **N. LARRIEU**, P. OWEZARSKI, P. BORGNAT, P. ABRY, “Non Gaussian and Long Memory statistical characterisations for Internet traffic”, 12 pages, décembre 2005, soumis à la conférence IPS-MoMe 2006.

(Larrieu & Owezarski, 2005b **N. LARRIEU**, P. OWEZARSKI, “Measurement based networking approach applied to congestion control in the multi-domain Internet”, LAAS report

N°04256, 9p., publié dans les actes de la conférence IFIP/IEEE International Symposium on Integrated Network Management (IM 2005), mai 2005, Nice, France.

(Larrieu, 2005a) **N. LARRIEU**, “Monitoring based approach for congestion control aiming at improving Internet QoS”, Rapport LAAS N°04260, 3 p., January 2005, publié dans les actes de la conférence IEEE INFOCOM 2005, Student Workshop, mars 2005, Miami, FL, USA.

(Labit et al., 2005) Y. LABIT, P. OWEZARSKI, **N. LARRIEU**, “Evaluation of active measurement tools bandwidth estimation in real environnement”, Rapport LAAS N°04548, février 2005, 10p., publié dans les actes de la conference IM 2005 – End to End Monitoring Workshop.

(Owezarski & Larrieu, 2004a) P. OWEZARSKI, **N. LARRIEU**, "Measurement Tools and Techniques for traffic and QoS management", International Mediterranean Modeling Multiconference / Integrated Modeling & Analysis in Applied Control & Automation (I3M/IMAACA, 2004), Genoa, Italy, 28-31 octobre, 2004.

(Larrieu, 2004) **N. LARRIEU**, “A measurement based networking approach for improving Internet congestion control”, IFIP World Computer Congress (WCC’04), Student Forum, Toulouse (France), 22-27 août 2004.

(Owezarski & Larrieu, 2004b) P. OWEZARSKI, **N. LARRIEU**, "Internet traffic characterization – An analysis of traffic oscillations", IEEE International Conference on High Speed Networks and Multimedia Communications (HSNMC’2004), Toulouse, France, 30 juin – 2 juillet, 2004.

(Owezarski & Larrieu, 2004c) P. OWEZARSKI, **N. LARRIEU**, "A trace based method for realistic simulation", IEEE International Conference on Communication (ICC’2004), Paris, France, 20-24 juin, 2004.

(Larrieu & Owezarski, 2003a) **N. LARRIEU**, P .OWEZARSKI, "TFRC contribution to Internet QoS improvement", Proceedings of the fourth COST 263 international workshop on Quality of Future Internet Services (QoFIS’2003), Suède, 1 – 3 octobre 2003

Conférences Francophones avec Comité de Lecture :

(Varet & Larrieu, 2012c) A. VARET, **N. LARRIEU**, « Le protocole de découverte de sécurisation SCOUT », CFIP 2012.

(Aussibal et al., 2007) J. Aussibal, P. Borgnat, Y. Labit, G. Dewaele, **N.LARRIEU**, L. Gallon, P. Owezarski, P. Abry, K. Boudaoud, « Base de traces d'anomalies légitimes et illégitimes », Joint Conference SAR (Security in Network Architectures) – SSI (Security in Information Systems), juin 2007, Lyon, France.

(Borgnat et al., 2006) P. Borgnat, **N. LARRIEU**, P. Owezarski, P. Abry, J. Aussibal, L.Gallon, G. Dewaele, K. Boudaoud, L. Bernaille, A. Scherrer, Y.Zhang, Y. Labit, « Détection d'attaques de Dénis de Service par un modèle non gaussien multirésolution », Colloque Francophone sur l'Ingénierie des Protocoles, novembre 2006, Tozer, Tunisie.

(Scherrer et al., 2006b) A. SCHERRER, **N. LARRIEU**, P.OWEZARSKI, P.BORGNAT, « Une caractérisation non gaussienne et à longue mémoire du trafic Internet et de ses anomalies », Rapport LAAS N°06076, Janvier 2006, 15p., 5ème conférence sur la Sécurité et les Architectures Réseaux (SAR’06), juin 2006, Seignosse.

(Larrieu et al., 2005) **N. LARRIEU**, Y. ZHANG, P. OWEZARSKI, « Caractérisation et analyse du trafic Internet en fonction du type d’application », Rapport LAAS, septembre 2005, 4 p., conférence GRETSI 2005.

(Borgnat et al., 2005) P. BORGNAT, **N. LARRIEU**, P. ABRY, P. OWEZARSKI, « Détection d'attaques de « Déni de Services » : ruptures dans les statistiques du trafic», Rapport LAAS, septembre 2005, 4 p., conférence GRETSI 2005.

(Owezarski & Larrieu, 2005a) P. OWEZARSKI, **N. LARRIEU**, « Un mécanisme de contrôle de congestion orienté mesures pour une QdS robuste dans l'Internet », Rapport LAAS N°05010, 10p., 4ème conférence sur la Sécurité et les Architectures Réseaux (SAR'05), juin 2005, Batz sur Mer.

(Larrieu & Owezarski, 2005c) **N. LARRIEU**, P.OWEZARSKI, « Contrôle de congestion et gestion du trafic à partir de mesures », LAAS report N°04609, mars 2005, 17p., Colloque Francophone sur l'Ingénierie et les Protocoles (CFIP 2005), Bordeaux, France.

(Larrieu & Owezarski, 2003b) **N. LARRIEU**, P. OWEZARSKI, « Une extension du modèle de tarification "smart market" pour l'Internet basé sur le contrôle de congestion », LAAS report N°03220, 10ème Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'2003), Paris (France), 7-10 octobre 2003, pp.377-392.

Présentations en tant qu'orateur invité

(Larrieu, 2013) Conférence Ingénierie des Systèmes Complexes à Logiciels Prépondérants (ISCLP) 2013 – session méthodologies et technologies innovantes pour les systèmes embarqués, « Méthodologie pour le prototypage rapide de solutions logicielles pour l'aéronautique (prise en compte des aspects conjoints de certification et d'évaluation) », Toulouse (France), 5-6 novembre 2013.

(Larrieu, 2004) Journées Télécoms et Réseaux 2004 (JTR'04), "Traffic characterization and analysis", Montpellier (France), 4-6 octobre 2004.

Rapports de Contrat :

(Ben Mahmoud & Larrieu, 2013b) M. Slim BEN MAHMOUD, **N. LARRIEU**, "AeroMACS Security Analysis", livrable de fin de projet SESAR 15.2.7, 101 pages, Octobre 2013.

(Ben Mahmoud et al., 2011c) M. Slim BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, "Rapport technique de fin de projet", livrable de fin de projet, FAST, 56 pages, Juin 2011.

(Ben Mahmoud et al., 2011d) M. Slim BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, "Rapport de test du démonstrateur FAST", comité techniques "applications", rapport de projet intermédiaire, FAST, Janvier 2011.

(Ben Mahmoud et al., 2010d) M. Slim BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, "Définition du décideur SecMan (Security Manager)", comité techniques "applications", rapport de projet intermédiaire, FAST, 4 pages, Avril 2010.

(Ben Mahmoud et al., 2010e) M. Slim BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, "La gestion de la sécurité des Communications dans le projet FAST", rapport d'avancement, FAST, Février 2010.

(Ben Mahmoud et al., 2009b) M. Slim BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, "Campagne de simulation permettant un dimensionnement du lien satellite FAST", comité techniques "applications", rapport de projet intermédiaire, FAST, Décembre 2009.

(Ben Mahmoud et al., 2009c) M. Slim BEN MAHMOUD, **N. LARRIEU**, A. PIROVANO, “Caractérisation des flux ATS et AOC”, comité techniques “applications“, rapport de projet intermédiaire, FAST, Mars 2009.

(Ben Mahmoud et al., 2009d) M. Slim BEN MAHMOUD, **N. LARRIEU**, Alain PIROVANO, “Recensement et caractérisation des flux applicatifs du projet FAST”, Projet FAST, Comité technique “Applications”, 7 pages, avril 2009.

(Ben Mahmoud et al., 2009e) M. Slim BEN MAHMOUD, **N. LARRIEU**, Alain PIROVANO, “Définition des besoins de sécurité relatifs aux flux applicatifs du projet FAST”, Projet FAST, Comité technique “Applications”, 4 pages, mars 2009.

(Owezarski & Larrieu, 2005b) P. OWEZARSKI, **N. LARRIEU**, “Definition of monitoring equipment and software and location points”, EuQoS project, Work Package n°2, Delivrable 2.1.1, 86 p., mars 2005.

(Owezarski et al., 2005b) P. OWEZARSKI, F. RACARU, G. AURIOL, **N. LARRIEU**, “Technical requirements for the trial, tasks and scheduling”, EuQoS project, Work Package n°5, Delivrable 5.1.1, 161 p., mars 2005.

(Owezarski et al., 2005c) P. OWEZARSKI, F. RACARU, G. AURIOL, **N. LARRIEU**, “Connectivity and performance tests report for local and pan-European (across GEANT) testbed design for the Trial”, EuQoS project, Work Package n°5, Delivrable 5.1.2, 96 p., mars 2005.

(Owezarski & Larrieu, 2005c) P. OWEZARSKI, **N.LARRIEU**, “Definition of monitoring equipment and software and location points”, Rapport LAAS N°05106, EuQOS Project IST 004503, Février 2005, 86p.

(Owezarski et al., 2004) P. OWEZARSKI, **N. LARRIEU**, L. BERNAILLE, W. SADDI, F. GUILLEMIN, A. SOULE, K. SALAMATIAN, “Distribution of traffic among applications as measured in the French METROPOLIS project”, LAAS report N°04628, contrat RNRT METROPOLIS, octobre 2004, 13p.

(Larrieu et al., 2004) **N. LARRIEU**, P. OWEZARSKI, K. SALAMATIAN, A. SOULE « Rapport intermédiaire du sous-projet 3 : Analyse du réseau », contrat RNRT METROPOLIS, janvier 2004, 56 p.

(Friedman et al., 2004) T. FRIEDMAN, K. SALAMATIAN, P. OWEZARSKI, **N. LARRIEU**, G. YONNET, E. DA COSTA, F. X. ANDREU, « Rapport intermédiaire du sous-projet 6 : Tarification et SLA », contrat RNRT METROPOLIS, janvier 2004, 51 p.

(Owezarski & Larrieu, 2004d) P. OWEZARSKI, **N. LARRIEU**, « Rapport intermédiaire du sous-projet 7 : Conception et mise en place de la plate-forme de mesures passives », contrat RNRT METROPOLIS, janvier 2004, 10 p.

Rapports Techniques

(Varet et al., 2009a) Antoine VARET, **Nicolas LARRIEU**, Jean-Marie FONTAINE, “How to improve Wireshark dissector design with C-code autogenerator methodology?”, 21 pages, septembre 2009.

(Varet et al., 2009b) Antoine VARET, **Nicolas LARRIEU**, Jean-Marie FONTAINE, “GUIDE DU CONCEPTEUR DU PLUGIN ASTERIX POUR WIRESHARK SOUS ENVIRONNEMENTS WINDOWS ET LINUX”, 12 pages, août 2009.

(Varet et al., 2009c) Antoine VARET, **Nicolas LARRIEU**, Jean-Marie FONTAINE, “GUIDE DE MODIFICATION DE L'AUTOGENERATEUR DE CODE C POUR WIRESHARK SOUS ENVIRONNEMENTS WINDOWS ET LINUX”, 17 pages, août 2009.

(Varet et al., 2009d) Antoine VARET, **Nicolas LARRIEU**, Jean-Marie FONTAINE, “GUIDE DE L’UTILISATEUR DU PLUGIN ASTERIX POUR WIRESHARK SOUS ENVIRONNEMENT WINDOWS”, 24 pages, juillet 2009.

Mémoire de Thèse :

(Larrieu, 2005b) **N. LARRIEU**, “Contrôle de congestion et gestion du trafic à partir de mesures pour l'optimisation de la QdS dans l'internet“, Rapport LAAS N°05229, Doctorat, Institut National des Sciences Appliquées, Toulouse, 4 Juillet 2005, 184 p., Président: O.FESTOR, Rapporteurs: S.FDIDA, G.LEDUC, Examinateurs: C.CHASSOT, F.GUILLEMIN, Directeur de thèse: P.OWEZARSKI

ANNEXE A : PRINCIPES DE FONCTIONNEMENT DE LA METHODE D'ANALYSE DE RISQUE QUANTITATIVE POUR L'AERONAUTIQUE

Chapter 1

A Quantitative Network Risk Assessment Methodology based on Risk Propagation

This appendix introduces an original risk assessment approach based on risk propagation for network security. The proposed approach measures quantitatively the network risk level based on critical aspects such as the impact of a successful attack on a node and the risk propagation of that attack within the network. The experiments have been conducted using real dataset and vulnerability databases. Each parameter involved in the risk assessment process is quantified then the overall approach is described in detail.

1.1 Quantifying Methodology Parameters

This section explains how every involved network parameter in the risk assessment process are computed. First, it is necessary to clarify how the risk is decomposed in the model, then every parameter are ointroduced and its respective formula.

1.1.1 Network Risk Decomposition

In the proposed methodology, there are 4 types of risks, namely:

1. **The risk per node** is computed for each node depending on its own vulnerabilities and its connections with correlated nodes. As a node is connected to other nodes in the network, the total risk for a given node i is evaluated as the product of node value $Value_i$ and the sum of its individual and propagated risks (respectively denoted $Risk_i^+$ and

$Risk_i^-$):

$$Risk_i = Value_i * (Risk_i^+ + Risk_i^-) \tag{1.1}$$

2. **The individual risk** is the intrinsic risk computed for each node, meaning it takes into account only the vulnerabilities associated with the node itself. The individual risk $Risk_i^+$ is computed as the sum on the number of existing vulnerabilities T_i of the product between the likelihood of occurrence of a threat $P_t(i)$ and its impact $I_t(i)$, which is fully compliant with the basic expression of the risk mentioned in formula 1.2:

$$Risk = Likelihood * Impact \tag{1.2}$$

$$Risk_i^- = \sum_{t=0}^{T_i} P_t(i) * I_t(i) \tag{1.3}$$

3. **The propagated risk** is the risk inherited from the dependency between correlated nodes (*e.g.* data flow exchanges, client-server architectures, etc). The propagated risk $Risk_i^+$, is estimated as the following:

$$Risk_i^+ = \sum_{j=0}^{n_i} \sum_{t=0}^{T_j} P_t(i,j) * I_t(i,j) \tag{1.4}$$

   Compared to equation 1.3, the idea is quite the same except the difference that the propagated likelihood $P_t(i,j)$ and the propagated impact $I_t(i,j)$ are induced by all the vulnerable nodes connected with node i (where n_i denotes the total number of nodes connected to the node i).

4. **The network risk** is the total risk computed for all the nodes composing the network. It is calculated as the sum of all the risks relevant to each node in the network (where n denotes the total number of hosts on the network):

$$Risk_{net} = \sum_{i=0}^{n} Risk_i \tag{1.5}$$

The next section explains how the node value used in the formula 1.1 is computed.

1.1.2 Node Value

Considering that network nodes have not the same functionalities, it can be considered that their degree of importance in the network may vary. Thus, the value of a node i is given by:

$$Value_i = n_i * FunctionValue_i \tag{1.6}$$

Indeed, the node functionality $FunctionValue_i$, which reflects the importance of a host from a security point of view, is taken into consideration. For instance, it is clear that a firewall is more critical for the security of the network than a user terminal. Besides, the value of a node increases when it is connected to a large number of nodes (*i.e.* when the node correlation is high). For instance, server nodes (*e.g.* email servers, web servers, DNS servers, etc) or proxies are highly connected to other nodes in the network.

This node value expression could be sufficient if the risk assessment is dedicated to an intra-network domain perimeter where only the node functionality may vary from a host to another one. Nevertheless, the node value expression presented equation 1.6 is certainly unsatisfactory to introduce the priority between network domains.

1.1.3 Enhanced Node Value

In order to introduce the priority between network domains, the equation 1.6 is slightly modified :

$$Value_i = n_i * FunctionValue_i * ClassValue_i \tag{1.7}$$

where $ClassValue_i$ expresses the class value of a node, depending on the network domain it belongs to. May the reader notice that both node function and class values are the only parameters requiring a *"human in the loop"* since there are no means to quantify them in practice. It is usually the duty of the administrator to assign these values depending on his needs and objectives. For instance, if the monetary value is an important parameter in the risk evaluation process, he could instantiate the function values to the cost of each host. For such a purpose, the risk assessment tool must give enough freedom to the user that he can assign the node values as he wants before initiating the evaluation process. In the model, both functions and class values have been ranged between 0.0 and 1.0 (which is an arbitrary choice and could be modified). For the aeronautical case studies, $ClassValue_i$ and $FunctionValue_i$ will be instantiated later for the specific needs of the SESAR project.

In the following section, the individual and propagated impact of threat on network nodes will be quantify .

1.1.4 Impact of Threats

As seen in equations 1.3 and 1.4, two types of impact of threats have been defined:

1. $I_t(i)$ is the impact of threat caused by the exploit of a specific vulnerability t to the node i. For each node, the estimated impact $I_t(i)$ is retrieved from the CVE public vulnerability database. To be more specific, $I_t(i)$ is referred to the CVSS severity (*i.e.* impact) score associated to each vulnerability occurring on that node, which is basically a numerical score ranged between 1.0 and 10.0. Practically, this information can be obtained by accessing manually the CVE database or by scanning the network using the NESSUS[1] vulnerability scanning tool: as far NESSUS is connected to the CVE database, the results remain the same. The number of vulnerabilities T_i, used in both equations 1.3 and 1.4, is a simple addition on the existing vulnerabilities for that node;

2. $I_t(i,j)$ is the propagated impact of a threat caused by the exploit of a vulnerability t from a node j to a node i:

$$I_t(i,j) = Value_i * I_t(j) * \sigma(i,s) \tag{1.8}$$

The propagated impact depends on the affected node value, namely $Value_i$ (as expressed in formula 1.7), the impact of t on the issuing node j (*cf.* CVSS score as defined above), and the targeted service s. $\sigma(i,s)$ is a scalar value deduced as the following:

$$\sigma(i,s) = SPV_i * (SOV_s)^{tr} \tag{1.9}$$

where SPV_i is a binary *Security Protection Vector* that defines the security features provided by security mechanisms and countermeasures used to protect the node i. The dimension of the vector depends on how many security services are provided. For instance, if confidentiality, integrity, and authentication are considered, SPV_i would be a 3-dimension vector. Moreover, let's assume that only confidentiality is provided for the data flows issued from the node i, the associated binary indicator vector will be equal to [0 1 1]. It could seem meaningless to associate the zero binary value to express a *"YES"*, but this is done in order to respect the impact function behavior. Indeed, the impact grows when less security features are available. Thus, mapping the one binary value to a *"YES"* is inadequate. In this specific case, the more security features is, the bigger would be the propagated impact,

[1]Note that any scanning tool providing the same features as NESSUS can be used.

which would not be logical regardi ng the impact function previously defined.

The second part of the equation 1.9 is the *Security Objective Vector* SOV_s that defines the security objectives per service (note that the transpose of the vector is used here in order to obtain a scalar result). For instance, if the example of a service s provided by the node i is chosen again where high security objectives are expressed for the the confidentiality, integrity, and authentication security services, the SOV_s vector could be equal to [5 5 5], where the value 5 expresses the highest security requirement. These values depend on the security objectives expressed beforehand at a previous step of the ISSRM process.

The SOV_s vector has to be instantiated according to the security objectives expressed in the COCR document for the aeronautical operational services.

In the following section, explanations are given on how to quantify the occurrence likelihood and threats propagation.

1.1.5 Likelihood of Threats

Similarly to the threats impact, two types of threats likelihood are defined:

1. $P_t(i)$ is the occurence likelihood of a threat caused by the exploit of a specific vulnerability t to the node i. $P_t(i)$ represents the possibility that an attack associated with a specific vulnerability t is conducted. The occurence likelihood evaluation is driven by the TYPHON (Telecommunications and Internet Protocol Harmonization Over Networks) threat analysis methodology proposed by the ETSI. However, as the likelihood values are qualitative, this part of the existing ETSI methodology is extended in order to quantify the involved parameters. Indeed, the likelihood evaluation is based on two behavioral factors:

   - ◇ The technical difficulties that an attacker may face in order to achieve his goal;
   - ◇ The motivation for an attacker to carry out a given attack.

   Thus, the likelihood of threats can be:

   (a) *Unlikely*: if the motivation for conducting an attack is low (*e.g.* no financial interest or technical challenges) and there are strong technical difficulties to overcome (*e.g.* insufficient knowledge to conduct the attack);

(b) *Possible*: if the motivation is moderate (*e.g.* reasonable financial gains) and the technical difficulties are solvable (*e.g.* information required to exploit the vulnerability are available);

(c) *Likely*: if there is a high attacker motivation (*e.g.* inducing a denial of service on the network, important financial gains) and technical difficulties are almost nonexistent (*e.g.* no security protection).

Despite the fact that these behavioral factors seem adapted and should be logically considered to evaluate the likelihood associated to an attack, they can not be used directly in the model as quantitative values are needed. Besides, the ETSI methodology does not explain how the technical difficulties and motivation factors are combined together in order to deduce the likelihood of occurrence of a threat. To address these issues, some modifications are brought in order to use these behavioral factors in the risk assessment process. First, the likelihood is computed using the motivation and technical difficulties values (respectively denoted $Motivation_t(i)$ and $TechnicalDifficulty_t(i)$) as shown in the following formula:

$$P_t(i) = \frac{Motivation_t(i)}{TechnicalDifficulty_t(i)} \tag{1.10}$$

In fact, $P_t(i)$ should increase when the motivation get higher; otherwise, $P_t(i)$ decreases when the technical difficulties that must be overcome increase.

The motivation for an attacker to exploit a vulnerability t on a node i is:

$$Motivation_t(i) = Value_i * T_i \tag{1.11}$$

Equation 1.11 shows that the motivation increases as the node value or the number of known vulnerabilities increases. Technical difficulties becomes more significant when security features (*e.g.* Firewalls) are reinforced (*e.g.* increasing their number or enhancing the security policies) or the amount of information required to exploit a vulnerability t is high:

$$TechnicalDifficulty_t(i) = S_i + B_t \tag{1.12}$$

In equation 1.12, S_i expresses the number of security mechanisms used to protect the node i. B_t is the amount of elementary informations needed by an attacker to exploit the vulnerability t. The assumption

that $B_t > 0$ is done, meaning that at least one elementary information has to be available to in order to conduct an attack exploiting t. Indeed, the attacker will be probably unable to exploit a vulnerability if a minimum of data is not available to start the attacking process (*e.g.* opened port IDs, user logins, target addresses, etc). As the resulting probability value must be ranged between 0.0 and 1.0, both motivation and technical difficulties values have been normalized between 0.0 and 1.0;

2. $P_t(i,j)$ is the likelihood of propagation of a threat caused by the exploit of a vulnerability t on a node j to node i given by:

$$P_t(i,j) = P_t(j) * P(i,j) \tag{1.13}$$

In fact, the likelihood of propagation depends on the likelihood of vulnerability t on the issuing node j and the likelihood of correlation $P(i,j)$ between the two nodes, given by:

$$P(i,j) = \frac{f_{ij}}{F_{ij}} \tag{1.14}$$

$P(j,j)$ depends on ratio between the number of detected and total data flows exchanged (*i.e.* the sum of all detected data flows) between two nodes i and j and relative to the attacked service. Practically, f_{ij} and F_{ij} can be directly deduced using some network statistics tools like NETSTAT[2] or raw data from */proc/net/dev*.

All the parameters discussed above are resumed in table 1.1:

[2] `http://linux-ip.net/html/tools-netstat.html`

Table 1.1: Risk Parameter Notations

Notation	Description
$Risk_i$	Node risk evaluated on node i
$Risk_i^-$	Individual risk evaluated on node i
$Risk_i^+$	Propagated risk evaluated on node i
$Risk_{net}$	Network risk
$Value_i$	Value of node i
$FunctionValue_i$	Function value of node i
$ClassValue_i$	Class value of node i
t	An exploitable vulnerability
n	Total number of nodes in the network
n_i	Number of nodes connected with node i
T_i	Number of vulnerabilities exploitable on node i
S_i	Number of security features deployed to protect i
B_t	Number of information needed to exploit t
$P_t(i)$	Likelihood of occurrence of a threat exploiting t
$I_t(i)$	Impact of threat exploiting t
$P_t(i,j)$	Likelihood of propagation of a threat exploiting t
$I_t(i,j)$	Propagated impact of a threat exploiting t
f_{ij}	Number of flows detected between nodes i and j
F_{ij}	Total number of flows exchanged between i and j
$Motivation_t(i)$	Motivation of an attacker to exploit t
$TechnicalDifficulty_t(i)$	Technical difficulty level to exploit t
$\sigma(i,s)$	Scalar value as the product of SPV_i and SOV_s
SPV_i	Security protection vector for the node i
SOV_s	Security objective vector for the service s

Finally, since all the parameters involved in the network risk computation process are now defined, the risk assessment algorithm can be proposed. Each step of the overall network risk assessment process is explained regarding the relevant pseudo-code algorithm.

1.2 Network Security Risk Assessment Process

In this section, 6 steps are described leading to the final network risk evaluation based on the proposed approach. In each step, the corresponding pseudo-code algorithm is given:

1. *Initiation step*: first, a set of vulnerable nodes and a set of processed nodes to null are initiated. All risk values (individual, propagated,

and node risks) are initiated for each node in the network. Also, a set of correlated nodes for each node is created;

Algorithm 1 Variables Initiation

```
1: V ← {∅}; //initiate a set of vulnerable nodes
2: NV ← {∅}; //initiate a set of processed nodes
3: for all i ∈ network do
4:     Risk_i^- ← 0;
5:     Risk_i^+ ← 0;
6:     Risk_i ← 0;
7:     C_i ← {∅}; //initiate a set of correlated nodes with node i
8: end for
```

2. *Scan and identify vulnerable nodes*: the second step is to identify all the vulnerabilities specific to each node in the network. If any vulnerability is detected, the node is marked as vulnerable and added to V. The node values are also computed and the corresponding CVSS severity scores are stored for a later use in the algorithm (see algorithms 3 and 4);

Algorithm 2 Scan and identify vulnerable nodes

```
9: for all i ∈ network do
10:     identify vulnerabilities;
11:     Value_i ← n_i * FunctionValue_i * ClassValue_i;
12:     if any vulnerability is detected then
13:         add node i to V;
14:     end if
15:     for all vulnerability t do
16:         store t and associated CVSS score;
17:     end for
18: end for
```

3. *Compute the individual risk for each vulnerable node*: for each vulnerable node identified in the previous step, tracks of the nodes that could be impacted by the network correlation are kept. The obtained set of correlated nodes will be used in the following step. Then for each vulnerable node, its individual risk is computed according to the formula 1.3;

4. *Compute the propagation risk for nodes correlated with vulnerable nodes*: for each vulnerable node, nodes are considerer one by one, and the propagated risk of the targeted node is incremented. The infected node is then tested: if it was not considered as vulnerable, the set of vulnerable nodes and the occurence likelihood of threat are updated;

Algorithm 3 Compute the individual risk for each vulnerable node

for all node $i \in V$ **do**
  store correlated nodes with node i in C_i;
  for all vulnerability t **do**
    $TechnicalDifficulty_t(i) \leftarrow S_i + B_t$;
    $Motivation_t(i) \leftarrow Value_i * T_i$;
    $P_t(i) \leftarrow Motivation_t(i)/TechnicalDifficulty_t(i)$;
    $Risk_i^- \leftarrow Risk_i^- + (P_t(i) * I_t(i))$;
  end for
end for

Algorithm 4 Compute the propagation risk for nodes correlated with vulnerable nodes

while $V \neq \{\varnothing\}$ **do**
  for all $j \in V$ **do**
    for all $i \in C_j$ **do**
      for all vulnerability t **do**
        $\sigma(i,s) \leftarrow SPV_i * (SOV_s)^{tr}$;
        $I_t(i,j) \leftarrow Value_i * \sigma(i,s) * I_t(j)$; *//s is the targeted service by t*
        $P(i,j) \leftarrow f_{ij}/F_{ij}$;
        $TechnicalDifficulty_t(j) \leftarrow S_j + B_t$;
        $Motivation_t(j) \leftarrow Value_j * T_j$;
        $P_t(i) \leftarrow Motivation_t(i)/TechnicalDifficulty_t(i)$;
        $P_t(i,j) \leftarrow P_t(j) * P(i,j)$;
        $Risk_i^+ \leftarrow Risk_i^+ + (P_t(i,j) * I_t(i,j))$;
        $P_t(i) \leftarrow P_t(i) + P_t(i,j)$; *//update the likelihood of threat*
        if $P_t(i) > 1$ **then**
          $P_t(i) \leftarrow 1$; *//the likelihood of threat should not exceed 1*
        end if
      end for
      if node $i \notin V and \notin NV$ **then**
        store node i in V; *//the node is now vulnerable*
      end if
    end for
    copy node j to NV and remove it from V; *//this node has been processed*
  end for
end while

5. *Compute the risk for each node in the network*: at this phase, the output of algorithms 3 and 4 are considered and the risk per node is

computed according to the expression 1.1;

Algorithm 5 Compute the total risk for each node in the network

52: **for all** node $i \in network$ **do**
53: $Risk_i \leftarrow Value_i * (Risk_i^- + Risk_i^+)$;
54: **end for**

6. *Compute the whole network risk level*: finally, the total network risk is estimated according to formula 1.5;

Algorithm 6 Compute the whole network risk level

55: **for all** node $i \in network$ **do**
56: $Risk_{net} \leftarrow Risk_{net} + Risk_i$;
57: **end for**

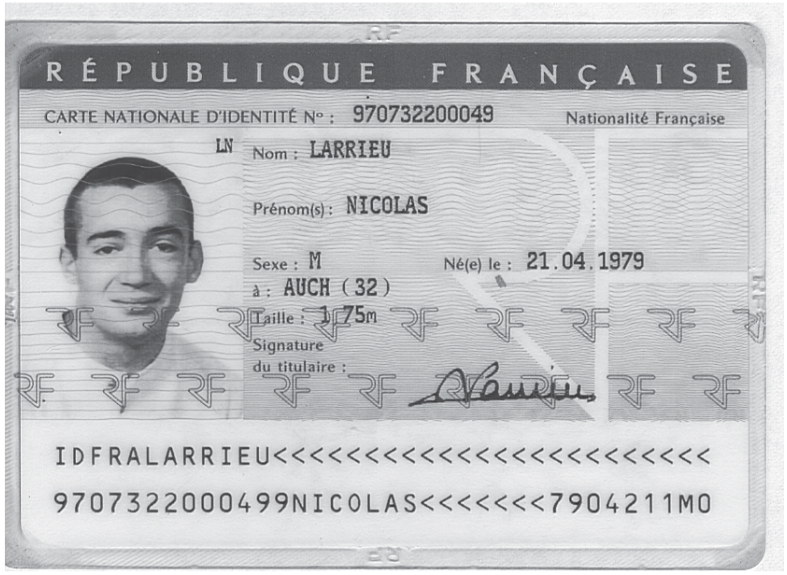
ANNEXE B : DOCUMENTS ADMINISTRATIFS

- Photocopie de ma **carte d'identité**
- Photocopie de mon **diplôme de doctorat**

- Document attestant **des qualifications précédemment obtenues** (CNU 27 et 61) lors de la campagne de 2006
- Document attestant **des qualifications précédemment obtenues** (CNU 27 et 61) lors de la campagne de 2010
- Document attestant **des qualifications précédemment obtenues** (CNU 27 et 61) lors de la campagne de 2014

- **Autorisation officielle** de co-encadrement de thèse de Slim Ben Mahmoud délivrée par **l'INSA de Toulouse**
- **Autorisation officielle** de co-encadrement de thèse d'Antoine Varet délivrée par **l'INSA de Toulouse**
- **Attestation de co-encadrement de thèse** d'Ouns Bouachir délivrée par l'école doctorale EDSYS
- **Dérogation officielle** d'encadrement de thèse de Jean Aimé Maxa à compter du 1er janvier 2013 délivrée par **l'Université Paul Sabatier de Toulouse**

- **Attestation du responsable de mon département d'enseignement à l'ENAC (Mathy GONON)** attestant de la charge d'enseignement réalisée depuis septembre 2006 en tant qu'en enseignant chercheur au sein de l'ENAC
- **Contrat de travail en CDI de l'ENAC** attestant de ma fonction actuelle d'enseignant chercheur à l'ENAC



RÉPUBLIQUE FRANÇAISE

CARTE NATIONALE D'IDENTITÉ N° : 970732200049 Nationalité Française

LN

Nom : LARRIEU

Prénom(s) : NICOLAS

Sexe : M Né(e) le : 21.04.1979

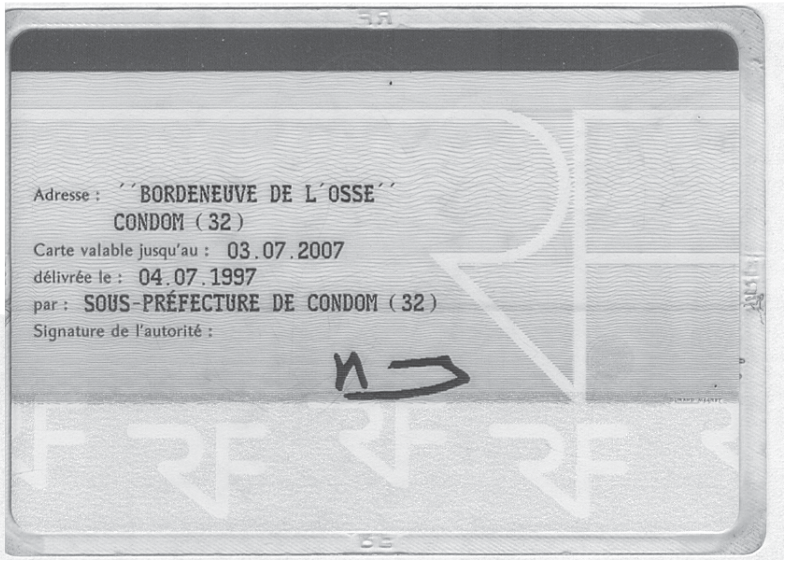
à : AUCH (32)

Taille : 1,75m

Signature du titulaire :

IDFRALARRIEU<<<<<<<<<<<<<<<<<<<<<<<<

9707322000499NICOLAS<<<<<<<7904211MO



Adresse : ''BORDENEUVE DE L'OSSE''
CONDOM (32)

Carte valable jusqu'au : 03.07.2007

délivrée le : 04.07.1997

par : SOUS-PRÉFECTURE DE CONDOM (32)

Signature de l'autorité :

INSA TOULOUSE

ATTESTATION DE DOCTORAT

(arrêté du 25 avril 2002)

Le Directeur de la Recherche de l'Institut National des Sciences Appliquées de Toulouse certifie que

Monsieur LARRIEU Nicolas

Né le 21 avril 1979

à Auch (GERS)

Inscrit à l'Institut National des Sciences Appliquées de Toulouse,

A OBTENU LE 4 JUILLET 2005

Le Diplôme de Docteur ce qui lui confère le GRADE DE DOCTEUR de l'Institut National des Sciences Appliquées de Toulouse

SPECIALITE : RESEAUX ET TELECOMMUNICATIONS

AVEC LA MENTION Très Honorable

Toulouse, le 5 juillet 2005

Institut National des Sciences Appliquées TOULOUSE

Jacques ERSCHLER

Il ne peut être délivré de duplicata de la présente attestation.

Institut National des Sciences Appliquées de Toulouse - 135, avenue de Rangueil - 31077 Toulouse cedex 4 (France)
Tél. : 05 61 55 95 13 - Télécopie : 05 61 55 95 00 - Web : www.insa-toulouse.fr

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE

Secrétariat général
Direction générale des ressources humaines

Service des personnels enseignants de l'enseignement supérieur et de la recherche
Sous-direction du recrutement et de la gestion des carrières

RECAPITULATIF DES QUALIFICATIONS OBTENUES
au 27/02/2009

Par M. LARRIEU NICOLAS

Né(e) le 21/04/1979 à AUCH

CORPS	SECTION	N° QUALIFICATION	DATE	CAMPAGNE
MCF	27	06227163110	27/01/2006	2006
MCF	61	06261163110	02/02/2006	2006

Le directeur général des ressources humaines

Thierry LE GOFF

Authentification : 7473fcf59f85a9b5e634b43b59a1a7a9 (1235724671094)

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE

Secrétariat général
Direction générale des ressources humaines

Service des personnels enseignants de l'enseignement supérieur et de la recherche
Sous-direction du recrutement et de la gestion des carrières

RECAPITULATIF DES QUALIFICATIONS VALIDES
publiées au 25/11/2013*

Par M. NICOLAS LARRIEU

Né(e) le 21/04/1979 à AUCH

CORPS	SECTION	N° QUALIFICATION	DATE	CAMPAGNE	DATE EFFECTIVE PEREMPTION
MCF	61	10261163110	20/01/2010	2010	31/12/2014
MCF	27	10227163110	21/01/2010	2010	31/12/2014

(*)Attention, les qualifications obtenues au titre de la campagne de qualification en cours ne sont mentionnées sur ce document que si leur résultat a déjà été communiqué à l'administration par le CNU et publié sur GALAXIE. En cas de doute, veuillez consulter la rubrique "Résultats qualification" pour vérifier si tous vos résultats sont connus

Authentification : c3c8833d15cdcdf361ff4c86f434d115 (1385376840543)

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE

Secrétariat général
Direction générale des ressources humaines

Service des personnels enseignants de l'enseignement supérieur et de la recherche
Sous-direction du recrutement et de la gestion des carrières

RECAPITULATIF DES QUALIFICATIONS VALIDES
publiées au 15/05/2014*

Par M. NICOLAS LARRIEU

Né(e) le 21/04/1979 à AUCH

CORPS	SECTION	N° QUALIFICATION	DATE	CAMPAGNE	DATE EFFECTIVE PEREMPTION
MCF	61	10261163110	20/01/2010	2010	31/12/2014
MCF	27	10227163110	21/01/2010	2010	31/12/2014
MCF	27	14227163110	31/01/2014	2014	31/12/2018

(*)Attention, les qualifications obtenues au titre de la campagne de qualification en cours ne sont mentionnées sur ce document que si leur résultat a déjà été communiqué à l'administration par le CNU et publié sur GALAXIE. En cas de doute, veuillez consulter la rubrique "Résultats qualification" pour vérifier si tous vos résultats sont connus

Authentification : d63ff63e2c2d992afd98fc4cb07493bf (1400146539787)

INSA TOULOUSE — ToulouseTech Technologies & Management — Service Recherche — Université de Toulouse

Toulouse, le 20 novembre 2008

Direction de la Recherche
Tél. : 05 61 55 99 75
Secrétariat
Tél. : 05 61 55 95 32
Fax : 05 61 55 95 00
Mèl : valerie.perraut-bertrand@insa-toulouse.fr

M. Alain PIROVANO
ENAC – Laboratoire LEOPART
7, avenue Edouard Belin
31055 TOULOUSE Cedex 4

SR.CS. 2008. 78/RF.VPB
Objet : Demande d'autorisation à diriger une thèse

Cher Monsieur,

J'ai le plaisir de vous informer que le Conseil Scientifique, lors de sa séance du 6 novembre dernier, a donné un avis favorable à votre demande d'autorisation à co-diriger la thèse de M. Mohamed Slim BEN MAHMOUD à 50 %.
La co-direction de cette thèse se fera avec M. Nicolas LARRIEU

Veuillez recevoir, Cher Monsieur, l'expression de mes sincères salutations.

Le Président du Conseil Scientifique

Institut National des Sciences Appliquées TOULOUSE

M. Louis CASTEX

CC : Ghislaine MARTINEZ – Responsable du Service Enseignement

Université de Toulouse

Année universitaire 2010-2011

Etablissement d'inscription :

Institut National des Sciences Appliquées de Toulouse (INSA Toulouse)

Ecole doctorale :

Systèmes (EDSYS)

DOSSIER DE CANDIDATURE EN 1ère ANNÉE DE DOCTORAT

Mme ☐ Melle ☐ M. ☒

NOM (marital) : VARET **PRÉNOMS** : Antoine, Bernard

Nom de jeune fille :

Nationalité : Française

N° I.N.E : 1898032251J N° étudiant **INSA** : 1 2500295

Né(e) le : 04/07/1987 à : Blois (41) Pays : FRANCE

Adresse : App 994 Résidence 7 6, allée des Sciences Appliquées
31400 TOULOUSE

Tél. : Portable : 06 32 47 93 49

Courriel: avaret@gmail.com

PROJET DE THÈSE

Discipline ou spécialité du doctorat : EDSYS - Informatique

Titre de la thèse : Définition, mise en oeuvre et validation d'une architecture de gestion adaptative de la sécurité pour les communications aéronautiques

Unité de recherche (n° UMR ou UPR...) : laboratoire LEOPART affilié EDSYS

Directeur(trice) de thèse : Nicolas LARRIEU Fonction (Professeur, Mcf, DR, CR...) : Enseig/Cherche

Titre (Docteur ou HDR ou DE) : Docteur Date et lieu d'obtention HDR :

Adresse professionnelle : ENAC, Département CNS, laboratoire LEOPART Téléphone : 05 62 17 43 64
7, avenue Edouard Belin, 31055 Toulouse Cedex 4 Courriel : nicolas.larrieu@enac.fr

Co-directeur(trice) *(s'il y a lieu)* : Christophe MACABIAU Fonction (Professeur, Mcf, DR, CR...) : Enseignant/Chercheur

Titre (Docteur ou HDR ou DE) : HDR Date et lieu d'obtention HDR : DEC 2002, TOULOUSE

Adresse professionnelle : ENAC, Département CNS, laboratoire LTST Téléphone : 05 62 17 42 77
7, avenue Edouard Belin, 31055 Toulouse Cedex 4 Courriel : macabiau@recherche.enac.fr

Dans le cadre d'une co-tutelle de thèse, préciser :

- le nom de l'établissement partenaire :
- le pays :

Année Universitaire 2011-2012
Etablissement : INSA Institut National des Sciences Appliquées de Toulouse
Renouvellement de l'inscription:
2° année de thèse

cadre réservé à l'établissement
Dossier transmis le : .....

Université de Toulouse

DEMANDE DE RENOUVELLEMENT D'INSCRIPTION EN DOCTORAT

Etat Civil

Numéro national étudiant : 1898032251J
N° étudiant : 12500295
Monsieur VARET
Prénoms : Antoine Bernard
Nom (marital) : .....
Nationalité : Française
Né le 4 juillet 1987 à Blois Loir et Cher - Pays : FRANCE

Adresse pour l'année universitaire 2011/2012 :
App 994 Résidence 7 6, allée des Sciences Appliquées 31400 TOULOUSE
Tel : 06 32 47 93 49

Adresse professionnelle 2011/2012 :
Laboratoire LEOPART Ecole Nationale de l'Aviation Civile (ENAC) 7 av Edouard Belin 31055 TOULOUSE cedex 4
Tel : 05 62 17 47 48

Tel .....
Portable :
E-mail : avaret@gmail.com avaret@recherche.enac.fr

THESE

Ecole Doctorale : ECOLE DOCTORALE SYSTEMES
Spécialité : Informatique et Systèmes Embarqués

Directeur de thèse Christophe MACABIAU Avis: FAVORABLE Signature :	**Directeur de l'unité de recherche** Alain PIROVANO Avis: Favorable Signature et cachet :
Directeur de l'Ecole Doctorale Caroline BERARD Proposition : ☒ favorable ☐ défavorable Date : 6/07/2011 Signature :	**DECISION DU PRESIDENT OU DIRECTEUR DE L'ETABLISSEMENT (sauf UT3)** **Nom:** **Autorisation :** ☐ **Accordée** ☐ **Refusée** **Date :** **Signature et cachet :**

ECOLE DOCTORALE SYSTEMES INSA TOULOUSE

Université de Toulouse

Année universitaire **2012-2013**
Établissement :
INSA- Institut National des Sciences Appliquées de Toulouse
École doctorale :
SYSTEMES
Discipline ou Spécialité de la thèse :
Informatique et Systèmes Embarqués

Cadre réservé à l'établissement
Dossier transmis le : .....

DEMANDE DE RENOUVELLEMENT D'INSCRIPTION EN DOCTORAT 3° Année

N°I.N.E. : 1898032251J **N° étudiant** : 12500295

Monsieur VARET **PRENOMS** : Antoine Bernard
NOM (marital) : .....
Né le 4 juillet 1987 à Blois Loir et Cher - Pays : FRANCE

Adresse pour l'année universitaire 2012/2013 :
App 994 Résidence 7 6, allée des Sciences Appliquées 31400 TOULOUSE

Tél. : 06 32 47 93 49 Mobile : 06 32 47 93 49
Courriel : avaret@recherche.enac.fr

RENOUVELLEMENT D'INSCRIPTION EN: 3°A

Directeur de thèse: Christophe MACABIAU

Co-Encadrant de thèse: Nicolas LARRIEU

Titre de la thèse : Définition, mise en oeuvre et validation d'une architecture de gestion adaptative de la sécurité pour les communications aéronautiques

Unité de recherche et n° : Laboratoire d\'Étude et d\'Optimisation des architectures des Réseaux de Télécommunication

Thierry Gayraud
Professeur UPS
Directeur de Thèse de Ons Bouachir

Objet : attestation encadrement thèse de doctorat de Ons Bouachir

Je soussigné Thierry Gayraud atteste que Monsieur Nicolas LARRIEU participe activement à l'encadrement de Mme Ons Bouachir depuis le 1er octobre 2011.

Cette thèse fait l'objet d'un triple encadrement nécessité par les compétences multiples sollicitées par le sujet de thèse proposé financé dans le cadre d'une action contractuelle européenne.

Il n'est pas possible de co-encadrer à 3 et de ce fait nous avons décidé en ensemble que les co-encadrants officiels sont Mr Fabien Garcia, car il est le responsable des activités scientifiques afférentes au contrat annoncé précédemment qui finance donc le doctorat de Mme Bouachir, et moi même car je suis pour l'instant le seul titulaire d'une HdR.

Si ce choix est dicté par le contexte, je tiens tout particulièrement à affirmer que l'apport de Mr Nicolas Larrieu à l'encadrement de ces travaux est indéniable et équivalent à celui des autres encadrants. La production scientifique ci-dessous peut en attester :

- O. BOUACHIR, F. GARCIA, **N. LARRIEU**, T. GAYRAUD, "Survey of Communication Architectures In UAV Ad hoc Networks: Toward Cooperative Operations", IEEE Communications Magazine, submitted, under Review. 2013.

- O. BOUACHIR, F. GARCIA, **N. LARRIEU**, T. GAYRAUD, "Ad hoc Network QoS Architecture For Cooperative Unmanned Aerial Vehicles (UAVs)", IFIP Wireless Days Conference, Valencia, Espagne, 2013.

La soutenance de ce doctorat est prévue dans le courant du second semestre 2014.

Pour faire valoir ce que de droit.

Toulouse, le 06/01/2014

Thierry Gayraud
Professeur des Universités

Formulaire CNIL

3 ème année de Thèse 2013 - 2014

Ouns BOUACHIR

Née le 2 septembre 1987

1ère inscription en Thèse : Novembre 2011

Etablissement : UT3 - Université de Toulouse 3 Paul Sabatier

Ecole Doctorale : SYSTEMES

Spécialité : Informatique

N° INE : 06O9KL02P80 **Nationalité :** Tunisienne **N° Etudiant :** 0310021112597

Adresse E-mail : ons.bouachir@gmail.com ons.bouachir@recherche.enac.fr

Adresse : 13 Rue du General Bares App 28 31400 Toulouse FRANCE

Tél. : 0660922382

Sujet de thèse : Conception et implémentation d'une architecture de communication pour agents mobiles coopératifs

Laboratoire : - RESCO- RESeaux de COmmunication de données -ENAC

Encadrement de la thèse : Thierry GAYRAUD - Fabien GARCIA - Nicolas LARRIEU

Financement 1 : Financement pour étudiants étrangers (EGIDE, ...)

Organisme : ENAC

de septembre 2011 à septembre 2014

Financement 2 : Financement pour doctorants étrangers

Organisme : Bourse Campus France

de septembre 2011 à août 2014

Diplômes et spécialités : Ingénieur - Télécommunications

Etablissement : Ecole supérieure des communications de Tunis

obtenu en octobre 2011

2011	Ingénieur National	Télécommunications	Ecole supérieure des communications de Tunis	TUNISIE
2008	Diplome des études universitaire du 1er cycle	Maths/Physique	Institut préparatoire des études d'ingénieur de Nabeul	TUNISIE
2006	baccalauréat	Mathématiques	Lycée secondaire de Beni Khiar	TUNISIE

Je soussignée Ouns BOUACHIR certifie être en accord avec les informations ci-dessus et m'engage à mettre à jour régulièrement mes données dans la base de l'école doctorale pendant la durée de ma thèse et pendant 5 ans après l'obtention de mon diplôme.

A ....., le 4 décembre 2013 SIGNATURE :

Année universitaire **2013-2014**
Établissement :
UT3 - Université de Toulouse 3 Paul Sabatier
École doctorale :
SYSTEMES
Discipline ou Spécialité de la thèse :
Systèmes embarqués et Informatique

Cadre réservé à l'établissement
Dossier transmis le : .....

DOSSIER DE CANDIDATURE EN 1ère ANNEE DE DOCTORAT

N°I.N.E. : 5SRSUK00F64 **N° étudiant** :

Monsieur MAXA **PRENOMS** : Aimee Jean Jean
NOM (marital) : MAXA
Nationalité : Malgache
Né le 13 octobre 1990 à Toamasiina - Pays : MADAGASCAR

Adresse actuelle :
Chez ENAC-Résidence Léopold Galy - 7 AVENUE EDOUARD BELIN CS 54005 - Toulouse 31055 Toulouse

Tél. : 0752776583 Mobile : 0752776583
Courriel : maxajeanaime@gmail.com

PROJET DE THESE

Titre de thèse : Sécurité des réseaux ad hoc aéronautiques : application aux réseaux de drones

N° et Unité de recherche : RESCO- RESeaux de COmmunication de données -ENAC

Directeur de thèse : M. Nicolas LARRIEU
Titre : EC - Fonction : -
Tel : 05 62 17 43 64 Courriel : nicolas.larrieu@enac.fr
HDR : en cours obtenue le : ..... à .....
Adresse professionnelle : ENAC 7 avenue Edouard Belin BP 4005 31055 Toulouse Cedex4 FRANCE

Co-tutelle : non

Direction des études et de la
vie de l'étudiant

UNIVERSITÉ
TOULOUSE III
PAUL SABATIER
Université de Toulouse

DIRECTION DES ÉTUDES ET DE LA VIE
DE L'ÉTUDIANT

CERTIFICAT DE SCOLARITE

La Directrice Générale des Services de l'Université Paul Sabatier - Toulouse III
certifie que

MAXA JEAN AIMÉ

Id. National : 5SRSUK00F6 4
N° Etudiant : 21312078

Né le 13 octobre 1990
à TAMATAVE (MADAGASCAR)

est régulièrement inscrit pour l'année universitaire 2013/2014

Diplôme : DOC. U. SYSTEMES EMBARQUES ET INFORMATIQUE
Année : DOC. U. SYSTEMES EMBARQUES ET INFORMATIQUE
Composante : Faculté des Sciences et d'ingénierie

Fait à TOULOUSE, le 20 janvier 2014

Par délégation, D. Loustau

D. Loustau

Université Toulouse III
Bât. administratif central
118 route de Narbonne
31062 Toulouse cedex 9
Tél. : + 33 5 61 55 66 11
www.univ-tlse3.fr

ENAC
ECOLE NATIONALE DE L'AVIATION CIVILE

Département Sciences et Ingénierie
de la Navigation Aérienne

ATTESTATION

Je sous-signé Mathy Gonon, chef de Département SINA à l'ENAC, atteste que Monsieur Nicolas Larrieu, Enseignant-Chercheur au sein du Groupe de Recherche RESCO du Laboratoire TELECOM de l'ENAC depuis 2006 assure, conformément au Règlement Intérieur de l'établissement, une charge d'enseignement correspondant à 50% de la charge annuelle, soit 200 heures de contact-élève, pour les enseignements de son domaine de compétence.

Fait pour valoir ce que de droit.

Fait à Toulouse , le 18 octobre 2013

Mathy GONON
Chef du Département Sciences et
Ingénierie de la Navigation Aérienne

7, avenue Edouard Belin - BP 54005 - 31055 Toulouse Cedex 4
Tél. + 33 (0) 5 62 17 40 00 - Fax + 33 (0) 5 62 17 40 23
www.enac.fr

ENAC
ECOLE NATIONALE DE L'AVIATION CIVILE

CONTRAT DE TRAVAIL DE DROIT PUBLIC A DUREE INDETERMINEE

Entre les soussignés :

L'Ecole nationale de l'aviation civile,
7, avenue Edouard Belin,
BP 54005
31055 TOULOUSE cedex 4

d'une part,

ET

Monsieur Nicolas LARRIEU
Né le 21 avril 1979, à Auch (32)
Demeurant : 4, rue Georges Brassens
31320 CASTANET TOLOSAN

N° de sécurité sociale : 1 79 04 32 013 080 (47)

d'autre part,

Vu la loi n° 84-16 du 11 janvier 1984 modifiée portant dispositions statutaires relatives à la Fonction Publique de l'Etat, notamment son article 4 (2ème alinéa) ;

Vu le décret n° 85-1148 du 24 octobre 1985 modifié relatif à la rémunération des personnels civils et militaires de l'Etat, des personnels des collectivités territoriales et des personnels des établissements publics d'hospitalisation, notamment ses titres III et IV ;

Vu le décret n° 86-83 du 17 janvier 1986 modifié relatif aux dispositions générales applicables aux agents non titulaires de l'Etat pris pour l'application de l'article 7 de la loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat ;

Vu le décret n° 2007-651 du 30 avril 2007 modifié, portant statut de l'Ecole Nationale de l'Aviation Civile ;

Vu le décret en date du 27 novembre 2008 portant nomination de Monsieur Marc HOUALLA dans l'emploi de directeur de l'Ecole Nationale de l'Aviation Civile,

ARTICLE 8 : IMPUTATION DE LA DEPENSE

La dépense correspondant à la rémunération de **Monsieur Nicolas LARRIEU**, imputée sur les crédits du budget de l'Ecole Nationale de l'Aviation Civile Civile (compte 643 - action 50) assurée par le bureau des traitements et salaires de l'Ecole Nationale de l'Aviation Civile dont relève l'intéressé.

Fait à Toulouse, le 1 AOUT 2012
(en trois exemplaires)

Le Contrôleur Financier
en région Midi-Pyrénées

Sous le n° 127 du 31/07/2012

L'adjointe au Contrôleur Budgétaire Régional,
DRFiP de la Région MIDI-PYRENEES
et du département de la Haute-Garonne

Christiane RIELLO

Le Directeur de l'Ecole Nationale
de l'Aviation Civile

M. HOUALLA
Le Directeur des Etudes et de la Recherche
P.O.

Gilles PERBOST

Signature de l'intéressé
(Précédé de la mention " Lu et approuvé ")

Lu et approuvé