

Fiche de demande de soutien Com2I

Nom du projet : MoSAIC (Mobile Systems Availability Integrity and Confidentiality)

Responsable LAAS : Marc-Olivier Killijian

Groupe(s) concerné(s) : TSF

Chercheurs impliqués et pourcentage d'implication :

Permanents : Marc-Olivier Killijian : 50%

David Powell 30%

Yves Deswarte 30%

Doctorants et autres : Doctorant1 à définir: 100% (au LAAS)

Doctorant2 à définir: 100% (à Eurécom)

Objectifs du projet:

Le projet proposé vise l'étude de nouveaux mécanismes de tolérance aux fautes et de sécurité pour les dispositifs mobiles sans-fil dans des applications d'intelligence ambiante (l'informatique ubiquitaire, le support tactique pour les champs de bataille ou la sécurité civile, la domotique, etc.). Nous nous focaliserons sur les réseaux éparés auto organisés, utilisant de façon prédominante des communications sans-fil à un seul saut, c'est-à-dire des réseaux composés d'un faible sous-ensemble d'une population importante de mobiles, réseaux qui se créent spontanément par le fait d'une certaine proximité et la découverte mutuelle, et qui cessent d'exister dès que la communication n'est plus possible.

Nous explorerons le problème peu étudié jusqu'à présent de la tolérance aux fautes dans ces réseaux. Le premier objectif consiste à définir un service de sauvegarde et de restauration automatique de données, basé sur la coopération entre mobiles n'ayant aucune relation de confiance pré-établie. Un tel service vise à assurer la disponibilité des données critiques gérées par des mobiles qui sont particulièrement vulnérables à l'épuisement des batteries, aux dommages physiques, au vol, ... L'idée de base est de permettre à un mobile d'exploiter des pairs accessibles afin de gérer la sauvegarde de ses données critiques. L'implémentation d'un tel service par coopération entre mobiles n'ayant aucune relation de confiance préalable est loin d'être triviale du fait des nouvelles menaces introduites : (a) des mobiles « égoïste » peuvent refuser de collaborer, (b) les mobiles qui servent de sauvegarde peuvent également défaillir ou attaquer l'intégrité ou la confidentialité des données, (c) des mobiles malveillants peuvent chercher à provoquer un déni de service par l'inondation des pairs avec de fausses requêtes de sauvegarde, etc. Traiter ces menaces est le second objectif du projet. Nous avons l'intention d'étudier des mécanismes de gestion de la confiance dans les services collaboratifs entre mobiles mutuellement suspicieux. Dans ce contexte, des mécanismes basés sur la notion de réputation (pour une évaluation de la confiance a priori et une imputabilité a posteriori) et de récompense (pour l'incitation à collaborer) sont de premier intérêt. Dans les réseaux éparés et éphémères que nous considérons, les mécanismes ne peuvent se baser ni sur l'accès à des tiers de confiance ni sur la présence d'une majorité des mobiles considérés, la réputation et la récompense autoportées semblent par conséquent particulièrement bien adaptées.

Positionnement du projet dans la prospective scientifique du laboratoire :

La sûreté de fonctionnement des systèmes mobiles est un nouvel axe de recherche du groupe TSF. Il rencontre un succès certain au sein de la communauté puisque le projet proposé à l'ACI Sécurité et Informatique a reçu d'excellentes évaluations et sera amené à se développer dans le laboratoire avec le démarrage prochain de deux thèses sur le sujet.

Fiche de demande de soutien Com2I

Contexte et partenaires externes (académiques ou industriels) éventuels :

Dans le cadre du projet MoSAIC, accepté et partiellement financé par l'ACI Sécurité et Informatique, les partenaires sont l'équipe ACES (Michel Banâtre) de l'IRISA et la Network Security Team (Refik Molva, Yves Roudier) à Eurecom.

Financement (montant et origine)

Montant total du projet : 258k€
Montant LAAS : 92k€

Planning :

Date de début : 01/10/2004
Date de fin : 31/09/2007

Principales étapes :

18 mois: rapport sur la sûreté de fonctionnement et la sécurité des réseaux éphémères auto-organisés de systèmes mobiles
36 mois: plate forme expérimentale illustrant les mécanismes de sûreté de fonctionnement et de sécurité définis dans le projet

Soutien technique demandé :

Nous demandons 1 ingénieur à mi-temps à partir de janvier 2005, et ce jusqu'à la fin du projet.

Description succincte des travaux confiés au service

- Mise en place des environnements de développement (a priori Java embarqué, J2ME) pour les dispositifs mobiles (assistants numériques, laptops, dispositifs de captures, téléphone 3eme génération, etc.),
- Mise en place et exploitation d'outils de simulation et d'expérimentation en situation réelle de dispositifs mobiles à grande échelle,
- Développement d'un intergiciel pour la tolérance aux fautes et de sécurité des dispositifs mobiles

Structure de la demande	
Compétence	Volume en % de temps plein
Java Réseaux mobiles (802.11) Systèmes embarqués (linux/winCE/embedded)	} 50%

Développement système

Contact préalable avec le service 2I ?

OUI

Fiche de demande de soutien Com2I

Effort demandé en % de temps plein

Total : 50%

Répartition sur la durée du projet :

1ere année : 3 h.m.

2eme année : 6 h.m.

3eme année : 6 h.m.