

# Design and Performance Evaluation of Intrusion Detection Systems for Voice over IP networks

## Mots clés :

- **Directeur de thèse** : ahmed MEHAOUA
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire d'Informatique PARIS DEscartes
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

## Résumé du projet de recherche (Langue 1)

Ce travail de recherche vise à apporter un élément de réponse à la problématique de la sécurisation des services audiovisuel (VoIP, Visio, IPTV, ...) dans les réseaux IP et en particulier à la détection et à la prévention d'intrusions dans les réseaux. De nombreuses menaces touchent ces infrastructures et les services audiovisuels (DOS, DDOS, SPIT, ...). Il est important de concevoir des modèles de détection et de prévention (IDS/IPS) efficaces, robustes et capables de monter à l'échelle (scalability). Cette thèse de doctorat consistera à déterminer les principales vulnérabilités des réseaux et des services de Voix-Vidéo sur IP par rapport aux attaques internes et externes au réseau, en proposant des solutions de détection et de prévention contre ces attaques.

## Résumé du projet de recherche (Langue 2)

Les travaux de recherche pourront s'organiser autour de ces points : 1. Etude bibliographique sur les différents modèles et stratégies des IDS/IPS proposé dans la littérature pour confiner tout trafic anormale (détection, réaction et reprise). Cette étude doit déterminer les vulnérabilités et les menaces, ainsi que les aspects de protection de l'infrastructure et des services en mettant l'accent sur les outils formels informatiques et mathématiques employés. 2. Proposition d'un modèle de détection d'anomalies répondant aux contraintes et spécificités de ces réseaux et services audiovisuels. 3. Evaluation et analyse des performances de ce modèle permettant de mettre en évidence les vulnérabilités et l'efficacité du modèle proposé pour la protection des systèmes de voix-vidéo sur IP. Ces validations seront réalisées autant d'un point de vue théorique que pratique, au moyen de modélisation analytique, simulations et l'extension d'un outil de détection d'intrusion (préprocesseur dans SNORT).