Codage de source avec contraintes de sécurité

Joffrey Villard
(joffrey.villard@supelec.fr)

SUPÉLEC, Dpt. Télécommunications, Gif-sur-Yvette, France.

Encadrants de thèse : Pascal Bianchi (Télécom ParisTech) et Pablo Piantanida (Supélec)
Correspondant DGA : Albin Dunand (DGA IP/TSI/TTS)

Contexte : les réseaux de capteurs sans fil

Cette thèse est consacrée aux problèmes d'estimation-détection dans les réseaux de capteurs, dont les applications concernent les domaines militaire, industriel, environnemental, sanitaire et commercial. On suppose qu'un phénomène physique est observé par le biais de capteurs, qui communiquent leurs observations à un centre de fusion distant. Les canaux de transmission sont supposés sans fil, donc de capacité finie et « publics » : les informations doivent être compressées avant leur transmission et peuvent être interceptées par un adversaire (appareil étranger au réseau ou capteur corrompu). Il s'agit alors de déterminer des bornes théoriques sur les performances du système et d'en déduire des principes pour la réalisation pratique de solutions efficaces.

Théorie de l'information et sécurité

La sécurité, dans l'approche traditionnelle de la cryptographie, est assurée sous l'hypothèse que l'adversaire ne peut pas résoudre (en temps raisonnable) certains problèmes complexes, comme la factorisation de grands nombres entiers. Cependant, dans certains cas (pour des données très sensibles, par exemple), on peut souhaiter une sécurité inconditionnelle, qui ne dépende ni du temps ni de la puissance de calcul dont dispose l'adversaire. La théorie de l'information fournit des outils permettant une définition quantitative du niveau de sécurité d'un système. En particulier, l'entropie définie par Shannon mesure l'incertitude à propos d'une variable aléatoire. En utilisant les propriétés statistiques du système, on peut alors concevoir des méthodes de compression et de transmission de l'information qui maximisent l'incertitude de l'adversaire à propos des données à protéger.

Un problème à 4 utilisateurs

Nous avons étudié en particulier un problème à quatre utilisateurs, où deux capteurs souhaitent transmettre leurs observations à un centre de fusion, en assurant un certain niveau de sécurité par rapport à un capteur espion. Dans ce contexte, les utilisateurs légitimes souhaitent à la fois diminuer les débits nécessaires à la transmission, augmenter la précision avec laquelle le centre de fusion reconstruit l'information, et augmenter la sécurité de la communication. Ces trois objectifs ne peuvent être réalisés simultanément et les utilisateurs doivent trouver un compromis. En décrivant un schéma de codage particulier, nous avons obtenu des bornes théoriques sur les performances générales d'un tel système. Sous certaines hypothèses, celles-ci permettent de déterminer l'ensemble des performances conjointement atteignables.

Perspectives

Dans le précédent problème, les canaux de communication sont supposés à débit limité et sans erreur. L'étude du cas plus général où ces canaux sont bruités est en cours. A plus long terme, considérer plusieurs adversaires permettrait de prendre en compte la connaissance imparfaite de la situation du capteur espion. D'autre part, des résultats récents proposant des schémas pratiques de codage sous contraintes de sécurité pourraient être adaptés au contexte étudié dans cette thèse.

Publications

L'ensemble des publications liées à ces travaux est disponible sur internet à l'adresse suivante : http://perso.telecom-paristech.fr/~villard/.