Proposition de stage de fin d'études niveau M2

Chiffrement multi-senseurs pour sécuriser les communications tactiques

Mots clés : Sécurité, Intelligence Artificielle (IA), Communications numériques tactiques

Face à la croissance exponentielle des attaques sur les systèmes télécoms, la sécurité est devenue un sujet vital pour le fonctionnement des sociétés. Le triptyque CIA (Confidentialité, Intégrité, Authentification), assuré par des algorithmes informatiques de cybersécurité au niveau des couches supérieures, est particulièrement vulnérable à des attaques au niveau physique (écoutes, brouillage). C'est pourquoi la sécurité de la couche physique des communications numériques est en plein essor, tout particulièrement pour les liaisons satellites (guerre des étoiles) et les flottes de drones. A cet égard, le cryptage multi-senseurs par masquage spatial est particulièrement attractif grâce à sa capacité à éviter les attaques par écoute illicite sans coordination a priori entre l'émetteur et le récepteur [1]. Récemment, plusieurs techniques ont été proposées dans la littérature pour faire face à cette problématique [2,3,4]. Cependant, elles souffrent de différents inconvénients et notamment, une complexité élevée, une faible efficacité énergétique avec un grand rapport entre la puissance crête et moyenne (PAPR).

L'objectif de ce stage est donc de concevoir une stratégie de masquage qui permette de façon optimale la génération d'un chiffrement spatial afin d'assurer un niveau de sécurité maximal. Pour ce faire, plusieurs approches seront étudiées, notamment celle basée sur la capacité d'apprentissage des réseaux de neurones du processus de maximisation des interférences dans les directions des récepteurs illégitimes. Ce chiffrement doit garantir la confidentialité des communications tactiques dans des conditions hostiles, et ce en particulier dans le cas où l'attaquant a une connaissance complète des algorithmes utilisés et cherche à neutraliser le signal de masquage du système de défense en opérant des attaques coordonnées. Nous chercherons aussi à concevoir des algorithmes pour permettre la bonne réception de ces signaux furtifs par les récepteurs légitimes.

Contexte : Ce stage niveau M2 se déroulera au laboratoire U2IS de l'ENSTA-Institut Polytechnique de Paris. Il peut déboucher sur une thèse de doctorat (rémunération attractive niveau CIFRE déjà acquise) à l'IPP dont les résultats intéresseront l'AID (Agence Innovation Défense), la DGA (Direction Générale de l'Armement) et un acteur industriel majeur du déploiement des futurs réseaux tactiques.

Profil recherché : L'étudiant devra posséder une solide formation en mathématiques appliquées ; en particulier des compétences dans plusieurs des domaines suivants seront appréciées : traitement statistique du signal, communications numériques, intelligence artificielle, réseaux sans fil, sécurité et crypto. Il devra être motivé pour le monde de la recherche et posséder une nationalité européenne.

Contacts : tarak.arbi@ensta-paris.fr, benoit.geller@ensta-paris.fr

Références :

1. A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” Communications Surveys Tutorials, IEEE, vol. 16, no. 3, pp. 1550–1573, Third 2014.
2. Y. Ding and V. Fusco, “Establishing metrics for assessing the performance of directional modulation systems,” IEEE Transactions on Antennas and Propagation, vol. 62, no. 5, pp. 2745–2755, May 2014.
3. E. Tollefson, B. R. Jordan and J. D. Gaeddert, "Out-phased array linearized signaling (OPALS): A practical approach to physical layer encryption," *IEEE Military Communications Conference*, Milcom, USA, Oct. 2015.
4. S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” Wireless Communications, IEEE Transactions on, vol. 7, no. 6, pp. 2180–2189, June 2008.

M2 training period

Securing tactical digital communications with multi-sensor encryption

Keywords: Cybersecurity, Artificial Intelligence, Tactical Wireless Digital Communications

Considering the exponential growth of attacks on telecom systems, security has become a vital society subject. The triptych CIA (Confidentiality, Integrity, authentication), provided by computer cybersecurity algorithms at the upper layer, is particularly vulnerable to attacks at the physical level (eavesdropping, jamming). This is why the subject of digital communications security at the physical layer grows exponentially, especially for satellite links (Star Wars) and drone fleets. Multi-antenna physical encryption through spatial masking is particularly attractive thanks to its high capacity to avoid eavesdropping attacks with no a priori coordination between the transmitter and the receiver [1]. Recently, several techniques have been proposed in the literature [2,3,4]. However, they suffer from different drawbacks: high computational complexity and low energy efficiency with large Peak to Average Power Ratio (PAPR).

The purpose of this internship is therefore to design a masking strategy that optimally allows the generation of a spatial encryption in order to ensure a maximum level of security. To reach this goal, several approaches will be studied, in particular the one based on the neural networks learning capacity of the process of maximizing interference in the directions of illegitimate receivers. This encryption must guarantee the confidentiality of tactical communications in hostile conditions, in particular when the attacker has a complete knowledge of the defense algorithms and seeks to neutralize the masking signal of the defense system by carrying out coordinated attacks. We will also design algorithms that allow high quality reception of these furtive signals by legitimate receivers.

Context: This M2 research internship will take place at the U2IS laboratory of ENSTA- Institut Polytechnique de Paris (IPP). It can lead to a PhD thesis (attractive remuneration at the CIFRE level already acquired) at the IPP, the results of which will be of interest to the AID (Defence Innovation Agency), the DGA (Direction Générale de l'Armement) and a major industrial player in the deployment of future tactical networks.

Requirements: The ideal candidate must have a solid background in applied mathematics; in particular, good ability in several of the following areas will be appreciated: statistical signal and data processing, digital communications, artificial intelligence, wireless networks, security and cryptography. He must be motivated for the research world and have a European nationality.

Contacts: tarak.arbi@ensta-paris.fr, benoit.geller@ensta-paris.fr

References:

1. A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” Communications Surveys Tutorials, IEEE, vol. 16, no. 3, pp. 1550–1573, Third 2014.
2. Y. Ding and V. Fusco, “Establishing metrics for assessing the performance of directional modulation systems,” IEEE Transactions on Antennas and Propagation, vol. 62, no. 5, pp. 2745–2755, May 2014.
3. E. Tollefson, B. R. Jordan and J. D. Gaeddert, "Out-phased array linearized signaling (OPALS): A practical approach to physical layer encryption," *IEEE Military Communications Conference*, Milcom, USA, Oct. 2015.
4. S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” Wireless Communications, IEEE Transactions on, vol. 7, no. 6, pp. 2180–2189, June 2008.