Soutenance de thèse

Khaled TALEB soutiendra sa thèse de doctorat préparée au sein de l'ISAE-ONERA SCANR et intitulée «*Sécurité de La couche physique: codes polaires wiretap pour des communications sécurisées*»

Le 19 mai 2022 à 10h00, Salle des thèses - ISAE-SUPAERO

devant le jury composé de

M. Jérôme LACAN	Professeur ISAE-SUPAERO	Directeur de thèse
Mme Meryem BENAMMAR	Enseignante-chercheuse ISAE-SUPAERO	Co-directrice de thèse
M. Charly POUILLAT	Professeur ENSEEIHT	
M. Christophe JÉGO	Professeur Bordeaux INP	Rapporteur
Mme Elsa DUPRAZ	Maîtresse de conférences IMT Atlantique	
M. Pierre LOIDREAU	Chercheur Université de Rennes 1	
M. Jean-Marie GORCE	Professeur INSA Lyon	Rapporteur

Résumé : Dans cette thèse, nous examinons le canal wiretap de Wyner dans la pratique, pour atteindre la sécurité en terme de théorie de l'information. Ce type d'approche de la sécurité a longtemps été écarté des applications pratiques. Ceci est principalement dû à une définition légèrement différente de la sécurité (Sécurité forte vs sécurité sémantique), en plus du fait que ces méthodes sont étudiées de manière asymptotique, donc pas en pratique. Les spécialistes ont donc préféré des solutions cryptographiques sur les couches supérieures du réseau afin d'assurer la sécurité. Cependant, il a été montré que ces définitions de la sécurité sont en fait équivalentes les unes aux autres. De plus, nous montrons que le comportement asymptotique des codes polaires, utilisés sur un canal wiretap, appelés codes polaires wiretap, est compatible avec son comportement asymptotique, ce qui rend les codes polaires wiretap utiles pour des applications pratiques. Un autre avantage principal de l'utilisation de la sécurité de la couche physique est que les types de réseaux émergents tels que les réseaux de capteurs, les réseaux ad hoc qui passent par plusieurs intermédiaires de la source à la destination, ou les réseaux d'identification par radiofréquence (RFID), sont de faible complexité, sur lesquels la gestion des clés cryptographiques, ainsi que la complexité de calcul rendent l'utilisation des techniques cryptographiques typiques difficile. Nous nous appuyons principalement sur les schémas présentés par Vardy et al. pour obtenir un secret faible et fort. Étant donné que nous utilisons ces schémas dans des longueurs de bloc finies, des fuites d'informations peuvent se produire. Il existe des méthodes dans la littérature pour calculer et estimer cette fuite d'information, mais nous montrons comment ces méthodes sont soit infaisables en pratique, soit simplement inexactes. De plus, nous introduisons une nouvelle méthode, pour estimer cette fuite, qui s'avère être très précise et plus légère en calcul que les méthodes connues. D'autre part, nous étudions également la construction pratique de codes polaires wiretap à longueur de bloc finie et examinons l'impact des principaux paramètres de construction sur le taux de code réalisable et la fuite d'information. Enfin, nous présentons notre banc d'essai, utilisé pour mettre en œuvre les codes polaires wiretap en pratique, en utilisant un émetteur et deux récepteurs, simulant le récepteur légitime et l'espion. Nous montrons que plus l'espion est éloigné de l'émetteur, plus il y a de bruit, et donc une moins bonne capacité de décodage, et qu'au-delà d'une certaine distance, il est incapable de décoder quoi que ce soit, et reçoit une image très bruyante, de laquelle aucune information utile ne peut être extraite.

Mots-clés : codes polaires, théorie de l'information, codage correcteur d'erreurs, communication, canal wiretap

Summary: this thesis will focus on the construction of physical layer security schemes for realistic communication scenarios.This will be done through a combination of some tools inspired from information theoretic security in order to characterize optimal theoretic schemes, along with design criteria from error correction coding. Finally, the main goal is to construct error correcting codes which approach these theoretic limits and validate them with system level simulation based on realistic specifications

Keywords: Computer vision, Deep learning, Video analysis, Autonomous vehicles