Institut FARMAN

Projet DECORR

Evaluation de la **DECORR**élation entre canaux : application à la sécurisation des réseaux sans fil

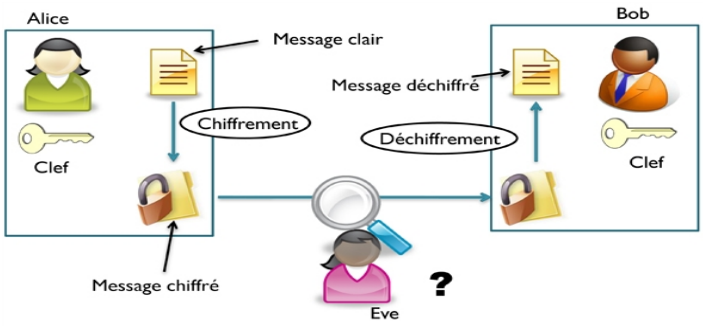
Porteurs du projet : Jean-Pierre Barbot (SATIE) - Laurent Fribourg (LSV)

Objet général de l'étude :

L'utilisation de réseaux sans fil (WiFi, 3G, …) pour acheminer des données s'est très rapidement et très largement répandue. Si cette mutation facilite grandement la mobilité et l'échange d'informations, celle-ci s'est malheureusement opérée au détriment de la sécurité et de la protection des données. La presse spécialisée s'inquiète de cette nouvelle faille dans nos modes de transmission de données, particulièrement quand il s'agit de données sensibles professionnelles et/ou stratégiques [1].
En effet, si l'acheminement de données peut être efficacement sécurisé dans des réseaux filaires (blindage électromagnétique, accès contrôlés, …), ce n'est plus le cas dès lors que ces réseaux sont « sans fils ». Certes la mise en œuvre de clefs de cryptage rend possible une relative protection, mais le caractère facilement détectable et observable de ces réseaux les rendent, ainsi que les données qu'ils transportent, très vulnérables.

La problématique de ce projet est donc : **comment sécuriser l'acheminement de données sensibles à l'aide de réseaux « sans fil »**, et ceci de façon inviolable ?

Afin de protéger les données qu'ils véhiculent, les systèmes contemporains de sécurité des réseaux sans fil se basent sur l'échange de clefs de cryptage. Ces clefs de cryptage doivent nécessairement être connues des seuls utilisateurs licites du réseau et inconnues de tout utilisateur illicite. Comme il d'usage dans le domaine de la cryptographie, nous appellerons par la suite « Bob » et « Alice » les utilisateurs licites du réseau, et « Eve » l'observateur illicite espionnant les échanges de données de Bob-Alice.



Afin d'encrypter leurs échanges, Bob et Alice peuvent utiliser des clefs de cryptage connues d'eux seuls. Deux configurations existent : soit Bob et Alice ont convenu d'une clef statique avant transmission, comme c'est le cas par exemple pour les clefs WAP-2 des réseaux wifi, soit Bob et Alice ont une gestion de clef dynamique. S'il est clair que ce dernier schéma dynamique offre un pouvoir d'encryptage renforcé, des failles de sécurité subsistent car ces systèmes nécessitent une phase de distribution des clefs. Renforcer la sécurisation de ces réseaux impose donc d'encrypter dynamiquement les données numériques échangées à partir d'informations que seuls Bob et Alice peuvent connaître, et ceci sans les transmettre.

S'appuyer sur la physique est un moyen bien connu pour générer un aléa non cassable par des méthodes mathématiques. Parmi les liens qui unissent Bob et Alice et connus d'eux seuls, le candidat idéal est le canal de propagation radioélectrique réciproque qui les relie. D'une part c'est le caractère aléatoire de la propagation électromagnétique dans un réseau sans fil qui fixe les « limites fondamentales du secret » telles que définies par C. Shannon [2]. De plus, le canal de propagation réciproque entre deux nœuds fixes du réseau, par exemple Bob

et Alice, est totalement **décorrélé** du canal de propagation Bob-Eve si Alice est distante d'une centaine de longueur d'onde d'Eve (soit environ 15 mètres à 2 GHz). Ainsi, Alice et Bob observe un processus aléatoire : le canal de propagation réciproque qui les lie, différemment de celui observé par Eve. Il est alors aisé de percevoir le pouvoir renforcé d'un système d'encryptage des données qui, en plus d'exploiter des clefs de cryptage publics ou privées, exploiterait des **clefs de cryptage dynamiques** générées à partir de la seule observation du canal de propagation réciproque. Par ce procédé, Bob et Alice disposeraient d'une clef d'encryptage connue d'eux seuls, générée dynamiquement sans échanger d'informations car établie à partir de l'observation du canal qui les relient. Eve, espionnant les transmissions entre Bob et Alice à travers un canal différent, sera incapable d'accéder à cette clef. Expliquons maintenant comment il est possible de réaliser l'observation et la caractérisation d'un canal de propagation réciproque.

Le canal de propagation entre deux nœuds fixes et dans les bandes de fréquence utilisées par les réseaux sans fil : bande UHF (300 MHz à 3 GHz), peut être considéré comme linéaire et invariant. Comme tous systèmes linéaires et invariants, il est entièrement caractérisé par sa réponse impulsionnelle complexe, ou par sa fonction de transfert (transformée de Fourier de la réponse impulsionnelle). Connaître le canal de propagation nécessite donc d'en mesurer la réponse impulsionnelle, c'est le processus d'**identification**. Il se trouve que ce processus d'identification est déjà réalisé par tous les systèmes de télécommunications sans fil. La phase d'identification est en effet indispensable pour régler l'égaliseur numérique présent dans tous les systèmes de télécommunication. L'étude proposée ici vise à exploiter cette phase d'identification pour mesurer la décorrélation des canaux et garantir ainsi une sécurisation de transmission. Cette mesure de décorrélation reposera essentiellement sur l'utilisation d'un **sondeur de canal large bande** (voir dans le paragraphe étude proposée).

L'état de l'art de ce champ scientifique indique ces dernières années un très fort et très naturel regain d'intérêt, tant théorique qu'applicatif. Deux catégories d'articles se distinguent. Une première catégorie regroupe des articles développant des algorithmes d'encryptage fondés sur une modélisation théorique du canal de propagation. L'apport de ces algorithmes est établi théoriquement ou à l'aide de logiciels de simulation [3][4]. Une seconde catégorie d'articles présente des approches plus expérimentales et exploite pour cela des réseaux sans fils existant (IEEE 802.11, …). Divers schémas d'encryptage sont testés, généralement en milieu de propagation « indoor » [5], avec une perception très limitée du canal de propagation.

Etude proposée :

Nous proposons d'étudier la décorrélation entre canaux de propagation séparés spatialement, en d'autres termes la décorrélation entre les canaux Bob-Alice et Bob-Eve ou Alice-Eve. Pour cela nous proposons d'utiliser des mesures de canaux de propagation déjà disponibles et d'en réaliser de nouvelles. De telles mesures nécessitent l'utilisation d'un appareil de mesure original : un **sondeur de canal** large bande [6]. Nous proposons pour cela d'utiliser le sondeur du laboratoire LTCI dans le cadre d'une collaboration entre les laboratoires SATIE et LTCI de Télécom Paris Tech.

Ce travail expérimental sera confronté avec les résultats théoriques concernant les **«limites fondamentales du secret»** énoncées par Shannon [2]. De ce travail pourrait également découler des applications portant sur l'encryptage dynamique des communications numériques.

Types d'Analyse Envisagés :

- Approche expérimentale : SATIE dispose déjà d'une large base de données mesurées comportant plusieurs dizaines de milliers de réponses impulsionnelles complexes dans une riche variété d'environnements de propagation. La collecte d'autre mesures sera effectuée en utilisant le sondeur de canal du LTCI. Cet ensemble de mesure servira à évaluer la décorrélation entre canaux. Ces données seront exploitées en faisant une analyse statistique. Ces mesures de décorrélation nous serviront comme élément de base pour quantifier le degré de sûreté de la communication.

- Simulation par chaîne de communication numérique : Parallèlement nous procéderons à la simulation d'un environnement de propagation prototype. Nous avons à notre disposition différents programmes informatiques permettant d'effectuer les simulations qui seront comparées aux données expérimentales effectuées avec le sondeur de canal.

- Simulation symbolique par model-checking : Le model-checking est une méthode formelle de vérification qui a déjà été utilisée avec succès pour analyser la performance et la sûreté de procédés correcteurs d'erreurs [9][10]. La méthode consiste, dans un premier temps, à construire un modèle formel du système à analyser (ici, un émetteur, canal entaché de bruit, récepteur,…) sous forme d'un automate probabiliste, c'est-à-dire, un système de transitions enrichi avec de l'information probabiliste. L'automate vise à représenter toutes les configurations possibles dans lesquelles peut se trouver le système étudié, ainsi que toutes les transitions le faisant passer d'une configuration à l'autre. Trois types de modèles probabilistes sont couramment utilisés : les chaînes de Markov à temps discret, à temps continu ainsi que les Processus de Décision Markoviens combinant indéterminisme et probabilités. Une fois le système modélisé, l'outil de vérification (model-checker) répond automatiquement à une question concernant, par exemple, la probabilité minimale/maximale ou le taux moyen d'occurrence d'une erreur dans le système, en ramenant cette question à un problème d'optimisation linéaire. Nous allons dans ce cadre formel réfléchir à une modélisation à la propriété de décorrélation dans l'espoir d'obtenir une quantification formelle de sécurité de l'environnement considéré. Des comparaisons avec les résultats de la simulation numérique détaillée ci-avant ainsi qu'avec les données expérimentales.

Déroulement de l'étude :

Premier temps : Exploitation des données expérimentales SATIE (6 mois : T_0-T_0+6)
L'énorme jeu de données dont dispose SATIE servira à établir le degré de décorrélation d'un environnement de propagation et son impact sur le degré de sécurité d'une communication numérique.

Deuxième temps : Simulations numériques d'environnements de communication (18 mois : T_0+6 -T_0+24)

Les critères dégagés seront exploités pour reproduire des expériences soit physiquement, soit numériquement, soit symboliquement et des analyses comparées seront conduites.

Moyens et délivrables :

L'étude est prévue sur une durée de deux ans.

Outre les outils PRISM du LSV et la chaîne de communications numériques du laboratoire SATIE, les laboratoires utiliseront les moyens humains suivants :

- LSV (3 personnes) : Laurent Fribourg (DR, 20%, porteur du projet pour le LSV), Claudine Picaronny (MC, 20%), Romain Soulat (Doct, 40%).

- SATIE (2 personnes) : Jean-Pierre Barbot (MC, 20%, porteur du projet pour SATIE), Thi Huyen Trang NGUYEN (Doct 40%).

Délivrables : Un rapport de mi-parcours (T_0+12) et un rapport final (T_0+24).

Objectif : Deux communications dans des congrès internationaux et au moins une revue internationale, toutes rédigées en commun.

Moyens financiers demandés : 12 k€

LSV : 6 k€ visant à soutenir :

- Une conférence internationale sur la modélisation, évaluation de performance et vérification probabilistes (QEST,RANDOM,…) : 2 k€,
- Un séjour d'un mois à Oxford (UK), dans le groupe de Marta Kwiatkowska développant PRISM (dans le but de maîtriser les dernières optimisations de cet outil en constante évolution, pour les appliquer spécifiquement à la modélisation des échanges sur réseau sans fil) : 4 k€.

SATIE : 6 k€ répartis de la façon suivante :

- Une conférence internationale sur le codage et la sécurisation des réseaux, type IEEE ICC : 2 k€,
- Un ordinateur : 2 k€,
- achat de matériel lié à l'utilisation du sondeur de canal (antennes, câbles, …) : 2 k€

Références :

[1] Dossier Sécurité : les nouvelles menaces à la porte des entreprises, Le Monde Informatique, 2 Novembre 2011. http://www.lemondeinformatique.fr/les-dossiers/sommaire-lire-securite-les-nouvelles-menaces-a-la-porte-desentreprises-106.html

[2] C. E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol. 29, pp. 656–715, 1949.

[3] P.C. Pinto, J. Barros, M.Z. Win, "Secure Communication in Stochastic Wireless Networks Part I: Connectivity" IEEE Trans. On Information Forensics and Security, Vol. 7, N°1, pp. 125-138, Feb 2012.

[4] M. Bloch et al., "Wireless Information-Theoretic Security," IEEE Trans. Info. Theory, 2008, pp. 2515–34.

[5] J.W. Wallace, R.K. Sharma, "Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis" IEEE Trans. in Information Forensics and Security, Vol. 5, N° 3, pp. 381-392, Sept 2010.

[6] J.-P. Barbot, "Propagation radioélectrique avec les mobiles pour les communications personnelles à l'intérieur des bâtiments dans la bande 1-3 GHz", Thèse de Doctorat de l'Université Paris-Sud 11, Orsay, 22 juin 1995.

[7] E. J. Candès and T. Tao. Near-optimal signal recovery from random projections: universal encoding strategies. *IEEE Trans. Inform. Theory*, **52** 5406-5425.

[8] Bajwa W.U., Haupt J., SayeedA.M., and Nowak N. *Compressed Channel Sensing: A New Approach to Estimating Sparse Multipath Channel,* Proceedings of IEEE, vol. 98, no 6, pp. 1058-1076, 2010.

[9] M. Duflot, L. Fribourg, Th. Hérault, R. Lassaigne, F. Magniette, S. Messika, S. Peyronnet and C. Picaronny, «Probabilistic Model Checking of the CSMA/CD Protocol Using PRISM and APCM », In Proceedings of the 4th International Workshop on Automated Verification of Critical Systems, ENTCS 128(6), pages 195-214. Elsevier Science Publishers, 2005.

[10] G. Norman, D. Parker, M. Kwiatkowska and S. Shukla, « Evaluating the reliability of NAND Multiplexing with PRISM, » IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems, vol. 24 no 10, Oct. 2005, pp. 1625-1637.