

Wave am I? Identification aveugle par apprentissage de l'empreinte radio-fréquence de dispositifs sensibles

Directeur de thèse : Matthieu Gautier (IRISA - Equipe Granit)

Co-encadrement : Robin Gerzaguet (IRISA - Equipe Granit)

Tuteur DGA : Erwan Nogues

Mots-clefs : Attaque TEMPEST, identification d'empreinte RF, classification, radio logicielle, architecture reconfigurable

1 Contexte

Les systèmes d'informations font désormais partie intégrante du fonctionnement des administrations publiques, des entreprises et plus généralement du mode de vie de tout un chacun. De fait, la sécurité des systèmes d'informations est un enjeu crucial à de multiples échelles et la protection des données sensibles (mécanisme de défense) comme l'interception de données (mécanisme d'attaque) présentent des intérêts stratégiques.

Ces systèmes échangent donc de l'information par des supports de transmissions différents et en particulier via des transmissions sans fil. Ainsi, la question de la protection des données transmises entre un nœud d'intérêt et un point d'accès réseau (station de base, récepteur ...) se pose. Il y a deux manières distinctes de protéger les données i) en sécurisant la couche physique, c'est à dire en rendant l'interception des signaux délicate (système TRANSEC) ii) en cryptant les données transmises, c'est à dire en rendant le décodage des données interceptées difficile. Les données cryptées sont qualifiées de « noires » en opposition à des données « rouges » non cryptées. La première technique s'appuie sur la sécurisation (et une complexification) de la couche physique et est toutefois plus difficile (et plus coûteuse) à mettre en œuvre pour des réseaux classiques du fait de la spécificité et du coût de déploiement associé (standardisation, circuit dédié, déploiement, ...). La seconde approche s'appuie sur les couches plus hautes du modèle OSI et définit une protection cryptographique.

Lorsqu'un signal est transmis par le nœud d'intérêt, sa détection n'implique donc pas *a priori* une fuite d'information sensible car l'information contenue dans le message est protégée (données « noires »). Cependant, il peut arriver que ce signal « noir » soit accompagné d'un signal « rouge » compromettant dû à une émission non légitime. C'est le contexte de canaux cachés TEMPEST [14] où un signal non protégé (rouge) est transmis sur une porteuse légitime de manière volontaire (on parle alors de *air gap bridging* [12]) ou involontaire (par couplage électromagnétique du fait de la proximité spatiale des composants électroniques) [2]. Le synoptique d'un tel scénario est représenté sur la Figure 1, où un nœud d'intérêt (Device 0) transmet un signal « noir » légitime à un autre composant (Device 1) et un signal « rouge » sensible par un canal caché (signal compromettant).

Ainsi, s'il peut être illusoire d'accéder à l'information échangée entre un nœud d'intérêt et son point d'accès réseau par l'intermédiaire du canal légitime « noir », il peut être intéressant d'identifier la présence de ce nœud d'intérêt afin d'intercepter ensuite les informations compromettantes présentes dans un éventuel canal caché. Il s'agit donc d'être capable d'authentifier la présence de ce nœud dans un réseau (via son canal légitime), sans avoir une connaissance exhaustive de la couche physique utilisée (i.e. sans décoder les informations « noires » présentes). Dans ce but, l'approche proposée est de s'appuyer sur les caractéristiques physiques de la partie radio fréquence (RF) du nœud d'intérêt. En effet, la partie RF est basée sur des éléments analogiques qui présentent des imperfections (gigue de fréquence, non-linéarités des composants d'amplifications ...) qui à la manière d'une empreinte digitale, marque de manière unique la transmission [22, 5]. On parle alors d'*empreinte RF*. Dans le cadre de cette thèse, on se propose donc d'utiliser des estimations de cette empreinte RF afin de discriminer et d'identifier un nœud d'intérêt dans un réseau.

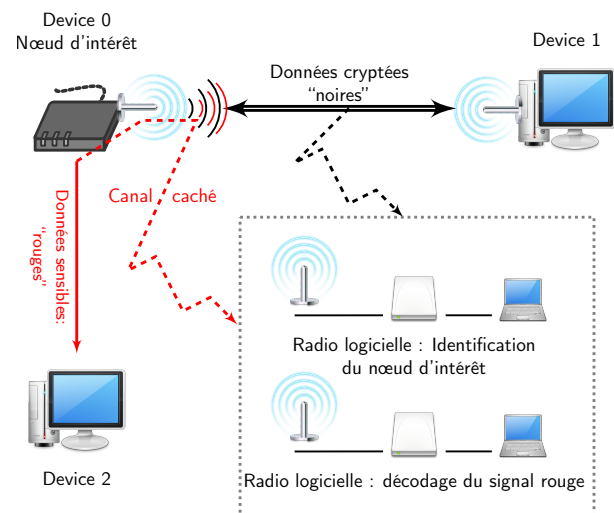


FIGURE 1 – Schéma du scénario d'intérêt et du dispositif d'interception.

Cette thèse est complémentaire des travaux actuels de Corentin Lavaud, thèse du pôle d'excellence cyber commencée en 2018. Cette dernière porte sur la détection et le décodage de canaux électro-magnétiques cachés et considère effective la présence du nœud d'intérêt. L'objectif de cette nouvelle thèse est donc de se placer en amont pour proposer un moyen d'identifier la présence et l'activité du nœud d'intérêt au sein d'un réseau.

2 Positionnement

La problématique de l'authentification de systèmes d'information par l'identification de leur couche physique n'est pas récente et a fait l'objet de plusieurs travaux de la littérature dans des contextes différents [10, 25]. Plusieurs éléments marquants rendent cependant la problématique de la thèse particulièrement actuelle et pertinente : l'avènement de radios logicielles large bande fournissant des données massives, des méthodes d'identification par apprentissage adaptées à ces données massives, et des capacités de calculs intégrées dans ces radios permettant de réaliser rapidement ces méthodes.

Tout d'abord, le dispositif d'interception peut bénéficier des capacités de traitement importantes dues aux avancées récentes des radios logicielles. Une radio logicielle (ou *Software Defined Radio* (SDR) en anglais) est un composant visant à réaliser une opération de transmission et/ou de réception d'un signal [13]. Contrairement aux solutions classiques où ces étapes sont réalisées sur un composant matériel dédié, (*hardware*) une SDR réalise ces opérations par une approche logicielle (*software*) qui fait abstraction des composants analogiques [21]. Les avantages sont nombreux : une grande flexibilité par l'utilisation d'une description *software* des fonctions, une réduction des coûts via des plateformes génériques et large bande, et un temps de conception plus court (*fast prototyping*) [1]. Si les premières générations de radios logicielles étaient limitées en termes de capacité de traitement, rendant délicate l'interface avec des systèmes réels, les dernières générations sont capables d'échantillonner une bande très large (100 à 200 MHz) avec une très bonne résolution (12 à 16 bits) tout en adressant une large gamme de fréquence porteuse (100 MHz - 6 GHz). Ainsi, une approche d'interception à base de SDR permet aujourd'hui d'avoir accès à l'intégralité de la bande où la transmission du signal « noir » peut apparaître. Cette caractéristique modifie radicalement les techniques d'interception, où la problématique consiste à traiter une quantité très importante d'information et non plus à accéder directement au signal ciblé.

Ensuite, la discrimination des différents utilisateurs sera effectuée par des techniques d'intelligence artificielle [23, 27, 16, 4]. La plupart des techniques d'identification par classification des empreintes RF reposent sur un algorithme d'extraction d'un ensemble de descripteurs à part d'un signal RF, plutôt bande étroite. Ces descripteurs sont ensuite associés à un algorithme de classification reposant sur une modélisation par mélanges de gaussiennes (GMM), à l'aide de séparateurs à vaste marge (SVM) ou plus récemment avec l'utilisation de réseaux de neurones. L'approche proposée dans ces travaux reposera sur ce schéma d'identification par empreinte RF en deux étapes. La première étape consistera en la collecte du signal large bande et en l'extraction des caractéristiques nouvelles d'empreintes RF (e.g. les non-linéarités de l'amplificateur de puissance). Dans la deuxième étape, les fonctionnalités d'apprentissage et la génération de modèles de décision sont réalisées.

Enfin, ces traitements peuvent être intégrés sur des architectures temps réel avec des co-processeurs ou des accélérateurs matériels. Comme énoncé précédemment, les SDR actuelles sont capables de gérer une bande instantanée très large, et donc doivent mécaniquement traiter une grande quantité de données. Ainsi, les capacités de traitement matériel ont augmentées avec les générations successives de SDR afin d'accélérer la quantité de traitements des données. La Figure 2 représente l'évolution en débit et capacité de traitement matériel des différentes générations des SDR de Ettus Research. Elle illustre parfaitement la nécessité de déporter une partie du traitement en hardware pour supporter les cadences de traitement.

Ces trois aspects ouvrent de nouvelles perspectives pour le développement de méthodes efficaces, temps réel, et flexibles permettant l'identification d'un nœud d'intérêt au sein d'un réseau légitime.

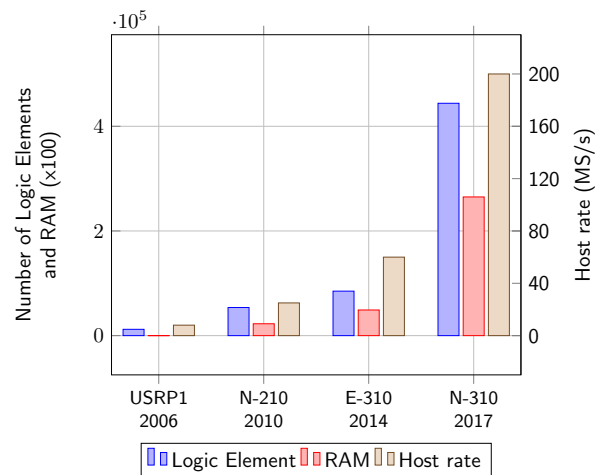


FIGURE 2 – Débit et ressources Hardware accessible en fonction des générations des radios logicielles (ici de Ettus research) [7]

3 Objectifs de la thèse

Ainsi, un certain nombre de verrous méthodologiques subsistent qu'il convient d'adresser. L'objectif de la thèse de doctorat est ainsi d'apporter une réponse aux questions suivantes :

1. **Quelles sont les éléments RF permettant de discriminer une transmission par rapport à une autre ?**

L'objectif de la thèse est de proposer une identification passive d'un nœud présent dans un réseau en s'appuyant sur son empreinte RF. La première question est donc de pointer les éléments RF à estimer qui permettent de discriminer un nœud par rapport à un autre. Dans le contexte classique de la détection d'*empreintes RF*, la plupart des méthodes s'appuient sur une estimation de la puissance du signal reçu [11, 19], ou par une métrique annexe telle que la mesure d'entropie [6]. D'autres familles de méthodes exploitent plutôt les défauts RF pour segmenter les utilisateurs via l'estimation des imperfections des oscillateurs [17] ou via une extraction de la statistique du bruit de phase [26].

Dans ces travaux de doctorat, on se propose d'étudier une autre source d'imperfection RF qui permettra a priori une excellente discrimination des utilisateurs : la non-linéarité de l'amplificateur de puissance (ou *Power Amplifier* en anglais). Du fait des fortes contraintes des amplifications, ces éléments sont fortement non-linéaires et ont une signature unique. Toutefois, la modélisation de leur comportement est très difficile, et passe par des modèles paramétriques simplifiés (comme le modèle de Rapp [18]). Les modèles plus complets, qui prennent notamment en compte les effets mémoires offrent de meilleurs modèles mais restent très complexes à l'image des modèles de Volterra ([28, 24]).

2. **Comment discriminer un utilisateur à partir de ces métriques RF ?**

Ces travaux reposent dans un premier temps sur la définition de l'empreinte RF et l'utilisation de la non-linéarité de l'amplificateur de puissance est la piste envisagée. Le choix de ce type d'empreinte implique l'utilisation de modèles suffisamment complets pour garantir une bonne identification d'un nœud d'intérêt. Dans cet objectif, des techniques de classification issues de l'intelligence artificielle peuvent être un atout précieux à cette modélisation comme la méthode très récemment proposée dans [20]. Il s'agit tout d'abord de s'appuyer sur une bonne connaissance de l'utilisateur à identifier avec une phase d'entraînement réalisée à partir de l'empreinte de cet utilisateur. Il pourra alors être intéressant de comparer différentes méthodes d'apprentissage et notamment de comparer le taux de détection avec des méthodes paramétriques de la littérature.

3. **Comment construire un système qui permet de discriminer en temps réel ces utilisateurs ?**

Les techniques de discrimination du nœud d'intérêt demanderont ainsi de nombreuses données issues de la partie RF qu'il va falloir identifier. Par ailleurs, ces traitements devront se réaliser dans un temps court et restreint de manière à garantir une identification quasi temps réel. Il est donc nécessaire d'utiliser les ressources matérielles présentes sur les radios et en particulier les ressources reconfigurables (de type FPGA) qui permettront d'avoir une architecture flexible pour la détection (approche de prototypage rapide).

4 Équipe Granit du laboratoire IRISA

Les travaux proposés dans cette thèse tirent profit de la complémentarité entre les compétences de la DGA et de l'équipe Granit. La DGA a une expertise reconnue des attaques TEMPEST et des algorithmes de détection associés. De son côté, l'équipe Granit s'intéresse à l'adaptativité des systèmes de transmission sans fil et apporte les compétences suivantes :

- Définition d'algorithmes adaptatifs [3][8],
- Prototypage rapide de traitements haut-débit sur cible matérielle FPGA [15],
- Portage d'algorithmes sur des plate-formes radio logicielle [9].

Cette complémentarité permet actuellement d'encadrer conjointement les travaux de thèses de Corentin Lavaud. Cette thèse est financée par le pôle d'excellence cyber et a commencé en 2018. Le sujet de thèse est « Systèmes reconfigurables pour l'interception de signaux sporadiques compromettants ». Les travaux proposés dans cette nouvelle thèse sont dans la continuité de celle-ci et reposent notamment sur l'expertise actuellement développée sur les radios logicielles hautes performances pour l'interception des systèmes compromettants.

Références

- [1] Asad A Abidi. The path to the software-defined radio receiver. *IEEE Journal of Solid-State Circuits*, 42(5) :954–966, 2007.

- [2] D. Agrawal, B. Archambeault, R. Josyula., and P. Rohatgi. The EM Side-Channel(s). In *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, pages 29–45, 2 2003.
- [3] Fayçal Ait Aoudia, Matthieu Gautier, and Olivier Berder. Learning to Survive : Achieving Energy Neutrality in Wireless Sensor Networks Using Reinforcement Learning. In *IEEE International Conference on Communications (ICC)*, Paris, France, May 2017.
- [4] Songlin Chen, Hong Wen, Jinsong Wu, Aidong Xu, Yixin Jiang, Huanhuan Song, and Yi Chen. Radio Frequency Fingerprint-Based Intelligent Mobile Edge Computing for Internet of Things Authentication. *Sensors*, 19(16), 2019.
- [5] Chanakya Damarla, James Ivers, Mark Pollard, Andrew J Kompanek, and Brian H Trammell. Method for RF fingerprinting, March 18 2008. US Patent 7,346,359.
- [6] Shouyun Deng, Zhitao Huang, Xiang Wang, and Guangquan Huang. Radio frequency fingerprint extraction based on multidimension permutation entropy. *International Journal of Antennas and Propagation*, 2017, 2017.
- [7] Ettus Research. Universal Software radio platform (USRP), 2017. <https://www.ettus.com/>.
- [8] R Gerzaguët, L Ros, F. Belveze, and J-M Brossier. Performance of a digital transmitter leakage LMS-based cancellation algorithm for multi-standard radio-frequency transceivers. *Digital Signal Processing*, 51 :35 – 46, 2016.
- [9] R Gerzaguët, L Ros, J-M. Brossier, and F. Belveze. Compensation numérique de spurs multiples avec estimation conjointe des décalages de fréquences dans le contexte OFDM. In *Proc. 25eme colloque Grets*, pages 1–4, 2015.
- [10] O. Gungor and C. E. Koksäl. On the Basic Limits of RF-Fingerprint-Based Authentication. *IEEE Transactions on Information Theory*, 62(8) :4523–4543, Aug 2016.
- [11] David A Knox and Thomas Kunz. AGC-based RF fingerprints in wireless sensor networks for authentication. In *Proc. IEEE International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, pages 1–6. IEEE, 2010.
- [12] M. G. Kuhn and R. Anderson. Soft Tempest : Hidden Data Transmission Using Electromagnetic Emanations. In David Aucsmith, editor, *Information Hiding (IH)*, pages 124–142. Berlin, Heidelberg, 4 1998.
- [13] Joseph Mitola. Software radios : Survey, critical evaluation and future directions. *IEEE Aerospace and Electronic Systems Magazine*, 8(4) :25–36, 1993.
- [14] NSA. *NACSIM 5000 : Tempest Fundamentals*. National Security Agency, February 1982. Partially declassified transcript : <http://cryptome.org/nacsim-5000.htm>.
- [15] Ganda Stephane Ouedraogo, Matthieu Gautier, and Olivier Sentieys. A Frame-Based Domain-Specific Language for Rapid Prototyping of FPGA-Based Software Defined Radios. *EURASIP Journal on Advances in Signal Processing*, page 13, November 2014.
- [16] L. Peng, J. Zhang, M. Liu, and A. Hu. Deep Learning Based RF Fingerprint Identification Using Differential Constellation Trace Figure. *IEEE Transactions on Vehicular Technology*, 69(1) :1091–1095, Jan 2020.
- [17] Adam C Polak and Dennis L Goeckel. Wireless device identification based on RF oscillator imperfections. *IEEE Transactions on Information Forensics and Security*, 10(12) :2492–2501, 2015.
- [18] Raviv Raich, Hua Qian, and G Tong Zhou. Orthogonal polynomials for power amplifier modeling and predistorter design. *IEEE transactions on vehicular technology*, 53(5) :1468–1479, 2004.
- [19] Saeed Ur Rehman, Kevin Sowerby, and Colin Coghil. RF fingerprint extraction from the energy envelope of an instantaneous transient signal. In *Proc. IEEE Australian Communications Theory Workshop (AusCTW)*, pages 90–95. IEEE, 2012.
- [20] Jinlong Sun, Wenjuan Shi, Zhutian Yang, Jie Yang, and Guan Gui. Behavioral modeling and linearization of wideband RF power amplifiers using BiLSTM networks for 5G wireless systems. *IEEE Transactions on Vehicular Technology*, 68(11) :10348–10356, 2019.
- [21] Walter HW Tuttlebee. *Software defined radio : enabling technologies*. John Wiley & Sons, 2003.
- [22] Oktay Ureten and Nur Serinken. Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering*, 32(1) :27–33, 2007.
- [23] Zhou Y., Wang X., Chen Y., and Tian Y. Specific Emitter Identification via Bispectrum-Radon Transform and Hybrid Deep Model. *Mathematical Problems in Engineering*, 2020.
- [24] Chao Yu, Lei Guan, Erni Zhu, and Anding Zhu. Band-limited volterra series-based digital predistortion for wideband rf power amplifiers. *IEEE Transactions on Microwave Theory and Techniques*, 60(12) :4198–4208, 2012.
- [25] P. L. Yu, J. S. Baras, and B. M. Sadler. Physical-Layer Authentication. *IEEE Transactions on Information Forensics and Security*, 3(1) :38–51, March 2008.

- [26] Caidan Zhao, Minmin Huang, Lianfen Huang, Xiaojiang Du, and Mohsen Guizani. A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks. *Computer Networks*, 128 :164–171, 2017.
- [27] X. Zhou, A. Hu, G. Li, L. Peng, Y. Xing, and J. Yu. Design of a Robust RF Fingerprint Generation and Classification Scheme for Practical Device Identification. In *2019 IEEE Conference on Communications and Network Security (CNS)*, pages 196–204, June 2019.
- [28] Anding Zhu and T.J. Brazil. Behavioral modeling of RF power amplifiers based on pruned volterra series. *IEEE Microwave and Wireless Components Letters*, 14(12) :563–565, 2004.