De la radio matérielle à la radio logicielle: impact sur l'étude de la sécurité des réseaux sans fil

Chaouki Kasmi, Arnaud Ebalard et Pierre-Michel Ricordel

Agence Nationale de la Sécurité des Systèmes d'Information
51, Boulevard de la Tour-Maubourg
75700 Paris 07 SP
prenom.nom@ssi.gouv.fr

Résumé Pour des besoins de mobilité ou de coût, les systèmes d'information utilisent des moyens de communications "sans-fil" comme le Wi-Fi, le Zigbee, le Bluetooth, ou les réseaux de téléphonie cellulaires (DECT, 2G/3G). Ces réseaux sont aujourd'hui largement déployés pour l'échange de données privées ou professionnelles.

La transition progressive d'équipements radiofréquences dits matériels vers des technologies de radio logicielle ont permis de profiter du haut niveau d'intégration et de la flexibilité de ces technologies.

Ces équipements commercialisés à des prix parfois très faibles peuvent être détournés – logiciellement ou matériellement – de leurs fonctions premières, pour être ensuite utilisés comme des outils d'analyse. Ces derniers ont ainsi permis de réaliser des études protocolaires de nombreux réseaux "sans-fil" jusqu'alors difficiles ou très coûteuses à mettre en œuvre.

Keywords: Radio logicielle, SDR, USRP

1 Introduction

La multiplication en nombre et en type des réseaux sans-fil a fortement fait évoluer les technologies et les méthodes utilisées pour leur développement. L'apparition de la radio logicielle a ainsi entrainé la réduction des temps et des coûts de développement des produits radios.

Ces évolutions ont également permis à la communauté scientifique de développer plus simplement des outils d'analyse efficaces, notamment pour évaluer leur sécurité.

Après une introduction aux réseaux sans-fil, le document s'attarde dans un second temps sur le concept de radio logicielle pour ensuite présenter son utilisation dans l'analyse de protocoles radio. Enfin, les évolutions envisagées dans le domaine font l'objet d'une section spécifique.

2 Introduction aux réseaux sans-fil

Il existe différents types de réseaux radios qui se distinguent par leurs caractéristiques physiques et protocolaires. Les premières dépendent grandement

des fonctionnalités attendues du réseau radio (débit et portée par exemple), des capacités physiques des émetteurs et terminaux (puissance, consommation) mais également de la date de conception de la technologie. Les caractéristiques protocolaires sont fortement liées à la complexité des services fournis par le réseau radio.

2.1 Aspects radios

Les aspects radios dimensionnants au niveau des couches physiques (PHY) et de contrôle d'accès au media (MAC) sont :

- ***la fréquence de travail***, qui impacte la portée, les antennes et les premiers étages analogiques ;
- ***les sauts de fréquence*** éventuels d'un canal à un autre. Certains standards, comme le Bluetooth, nécessitent une très grande agilité en fréquence, qui impacte les modules de traitement du signal et notamment les fonctions de conversion analogique/numérique.
- ***la bande passante*** de travail, qui impacte les performances du système. Plus la bande passante est élevée, plus la capacité de traitement de la radio doit être élevée, et plus le débit binaire utile est élevé ;
- ***le parallèlisme des communications*** : simplex (un seul sens de communication), alternat (half-duplex), bidirectionnel simultané (full-duplex), voire MIMO [1], qui impacte l'architecture de la radio ;
- ***la modulation et le codage employés***, qui peuvent être simples (OOK [2], FSK [3]) ou très complexes à mettre en oeuvre (OFDM [4], DSSS [5], modulation d'amplitude en quadrature haute densité, codage en treillis) ;
- ***les codes détecteurs et correcteurs d'erreurs***, qui peuvent aller du simple CRC [6] aux codes les plus complexes (Reed-Solomon, Turbo Codes) ;
- ***la méthode d'accès au media (MAC)*** peut nécessiter des temps de réponse très courts (synchronisation avec les autres émetteurs pour éviter les collisions, acquittements des paquets reçus) ou des adaptations spécifiques des étages de décodage (détection de collision). Ceci accroît les besoins de traitement temps réel ;

En pratique, la complexité à interagir au niveau physique avec un type de réseau radio donné dépend de la capacité du matériel à supporter ces différentes caractéristiques. Mais celle-ci dépend également de la capacité à reprogrammer ou contrôler le matériel à une vitesse compatible avec la fréquence de fonctionnement du réseau.

---

1. Multiple Input and Multiple Output, pour réception et émission multiple
2. On-Off Keying
3. Frequency Shift Keying
4. Orthogonal Frequency-Division Multiplexing
5. Direct-Sequence Spread Sprectrum
6. Cyclic Redundancy Check

2.2 Aspects protocolaire

Certains réseaux radios simples transportent des données brutes, parfois dans un seul sens de communication. D'autres, plus complexes, utilisent des mécanismes de signalisation pour supporter diverses fonctionnalités : partage du spectre radio entre différentes ressources, négociation de fonctionnalités ou de paramètres de sécurité comme l'authentification ou le chiffrement du canal de communication.

Les réseaux de téléphonie mobile intègrent ainsi un grand nombre de fonctionnalités nécessitant le maintien d'états au niveau des récepteurs et des émetteurs. Ils supportent au final le transport d'information de voix, de données et de signalisation.

La maîtrise des aspects protocolaires des réseaux radios étudiés et la capacité à contrôler des éléments logiciels et matériels de manière à interagir avec ceux-ci sont des éléments clés dans leur étude. La complexité des protocoles et l'accès aux documents de spécification sont bien évidemment des aspects dimensionnants dans leur étude.

2.3 Analyse

Les interactions avec un réseau radio dépendent donc initialement de la complexité à reproduire sa couche physique soit par un développement de matériel spécifique soit en détournant/réutilisant un matériel dédié. La difficulté est ici inhérente aux éléments physiques cités précédemment : fréquence, largeur de bande, modulation et utilisation potentielle de saut de fréquence ...

De plus, en fonction du scénario envisagé, la capacité à émuler les couches physiques et donc à réaliser les premières interactions avec le réseau radio n'est pas l'unique obstacle à considérer. Ainsi, la compréhension de la couche protocolaire transportée est généralement nécessaire dans de nombreux scénarios ; une trame donnée n'ayant par exemple une signification qu'à un instant donné, pour une ressource radio donnée et en fonction des échanges précédents. Pour illustrer cet exemple, l'émission d'une trame de désauthentification sur un réseau Wi-Fi nécessite une authentification préalable d'un client au point d'accès et la présence des identifiants spécifiques à ce client dans la trame de désauthentification construite.

3 Présentation de la radio logicielle

Issue de la recherche militaire américaine à la fin des années 70 sur les radios multimodes opérant en bandes VHF et UHF, la radio logicielle aboutit au début des années 90 par la famille de projets SPEAKeasy Phase I et Phase II aux premières implémentations de radios logicielles émulant des radios tactiques. Elle rejoint en 1991 [1] la communauté scientifique dans le cadre des applications de télécommunications civiles. En 1995, un RFI[7] sur la radio logicielle pour

7. Request For Information

des applications de téléphonie mobile marque le point de départ d'une activité accrue dans ce domaine. En 1996 apparait le Modular Multifunctional Information Transfer System Forum qui devient en 2009 le Wireless Innovation Forum [8]. Il s'agit d'une coopération entre chercheurs et industriels internationaux dont l'objectif est de promouvoir et de développer la technologie radio logicielle.

3.1 Le principe de radio logicielle

Une radio logicielle – en anglais Software Defined Radio ou SDR – est un système de radiocommunication configurable utilisant des techniques de traitement numérique du signal sur des circuits numériques programmables. Sa flexibilité lui permet de s'adapter à différents protocoles de radiocommunication, et de répondre au besoin croissant de performance et d'interopérabilité entre systèmes. L'objectif de la radio logicielle consiste en une dématérialisation complète de l'interface radio. Elle participe à la tendance globale des circuits électroniques à devenir des circuits à haute densité d'intégration [36].

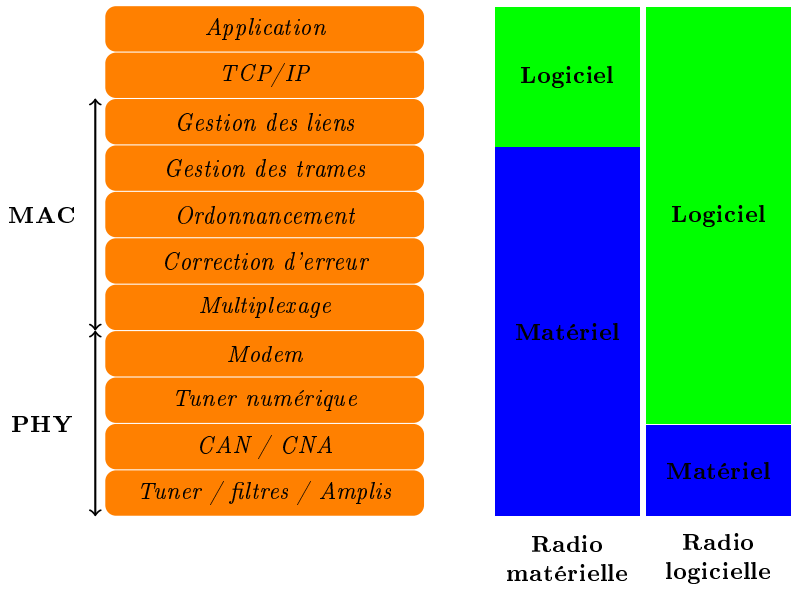

Figure 1. Evolution de la radio matérielle à la radio logicielle

L'évolution ultime de la radio logicielle est la radio intelligente ou radio cognitive [1,2]. Une radio intelligente est une radio logicielle dans laquelle les éléments de communication évoluent en fonction des conditions de propagation et de son

8. http://www.wirelessinnovation.org/

état interne, ce qui se traduit par une modification de sa couche physique : utilisation de différentes modulations, différents types de codes correcteurs pour répondre aux stress du canal de propagation.

Les radios logicielles permettent l'utilisation de multiples formes d'ondes, éventuellement dans différentes bandes spectrales, pour différents usages, voire même de façon simultanée. Dans une radio logicielle, les propriétés de la fréquence porteuse, de la bande passante du signal, de la modulation et de l'accès au réseau sont définies par logiciel. Celles-ci ont donc vocation à être portables sur tout plate-forme ; ceci explique la nécessité des recherches actuelles dans le développement de standards ouverts [22].

Les radios logicielles modernes mettent également en œuvre des codes de correction d'erreurs, des modules d'encodage de la voix, de la vidéo ou des données et des fonctions cryptographiques. Ces équipements sont aujourd'hui éprouvés [8] et font partie de notre quotidien, que ce soit pour la conception de modem 3G+ [34,35] dans les terminaux mobiles ou les équipements des réseaux radios comme les stations de base.

3.2 Architectures de la radio logicielle

Il existe différentes architectures intermédiaires de la radio dite matérielle à la radio intelligente. Le niveau d'intégration des fonctions numériques résulte de l'augmentation des performances des composants utilisés pour ces traitements [44]. Du DSP au FPGA [27] ou par l'utilisation de cartes multi-processeurs, la capacité de traitement temps réel a fortement progressé. Il est ainsi possible d'ajouter à l'équipement les capacités liées à la prise de décisions sur des modifications des paramètres de la couche physique en fonction de capteurs externes (bruit électromagnétique, surcharge de la bande de fréquence utilisée...).

Ces différentes évolutions [37] ainsi que la multiplication des capacités des terminaux se traduisent par une classification de ces systèmes :

Catégorie	Dénomination	Degré de reconfiguration
0	Radio matérielle	Radio qui ne peut pas être modifiée par logiciel ; reconfiguration par échange de composant.
I	Radio contrôlée par logiciel	Reconfiguration limitée à un jeu prédéfini de paramètres (niveau de puissance, interconnexions, ...)
II	Radio définie par logiciel	Contrôle logiciel et reconfiguration des formes d'ondes, fréquence, bande passante, (dé)modulation, détection du signal, paramètres de sécurité, etc.
III	Radio logicielle idéale	Conversion analogique au niveau de l'antenne, du haut-parleur et du microphone ; tout le reste est logiciel.
IV	Radio logicielle ultime	Comprend tout type de trafic et d'informations de contrôle, et supporte la plupart des applications et circuits d'antenne.

Figure 2. Classification des systèmes radio logicielle selon le Wireless Innovation Forum

Les plates-formes et bancs d'essai de radios logicielles "libres" offrent aux chercheurs et développeurs la possibilité de concevoir leurs propres applications radios logicielles. Au vu de la complexité croissante des systèmes à concevoir, une plate-forme de prototypage est choisie en fonction de critères multiples : flexibilité, rapidité de calcul, communications entre composants et présence d'interfaces externes. Bien que la radio logicielle restreinte offre de multiples avantages aux concepteurs de systèmes radio, il reste de nombreuses questions ouvertes sur la façon de mettre en œuvre et de gérer la flexibilité dans un système de transmission sans fil.

Dans le cadre de projets de recherche, plusieurs plates-formes radios logicielles expérimentales ont pu voir le jour. La liste des radios logicielles réalisées, en développement ou à l'état de prototype [19] est très étendue.

3.3 Exemples de plates-formes spécifiques

On distingue différentes catégories de dispositifs à base de SDR. Les dispositifs spécifiques, conçus et développés pour répondre à un besoin particulier, relativement peu flexibles, sont souvent coûteux ; cependant ces systèmes sont optimaux pour l'application visée. On retrouve notamment dans cette catégorie les équipements de test et de métrologie ainsi que de nombreuses plates-formes de recherche, mais aussi certaines fabrications artisanales dédiées à une norme de radiocommunication ou un protocole particulier. Les applications visées par ces plates-formes sont très diverses :

- BEE2, Berkeley Emulation Engine 2 est une plate-forme de radio logicielle utilisée pour des applications nécessitant des capacités de calcul importantes, notamment en radioastronomie [7,9,10].
- CalRadio est un programme de recherche et de développement d'émetteur/récepteur sans-fil mettant en œuvre des plates-formes de test [11].
- Chameleonic Radio est un prototype expérimental de radio multibande et multimode, élaboré par Virginia Tech [12].
- VT-CORNET, Virginia Tech Cognitive Radio Network Testbed est une plate-forme de test de radio intelligente [13].
- FPGA4U, FPGA4U est une carte développée par l'école polytechnique fédérale de Lausanne (EPFL) à des fins pédagogiques [14].
- HPSDR, HPSDR (High Performance Software Defined Radio) est un projet matériel et logiciel "libre" de récepteur SDR [15].
- KNOWS, Kognitiv Networking Over White Spaces issu de l'alliance de Microsoft et de Dell est une radio intelligente détectant et exploitant de façon adaptative les bandes libres TV [16].
- KUAR, la plate-forme Kansas University Agile Radio est une plate-forme expérimentale "low-cost" [17].
- MARS, le système Maynooth Adaptable Radio System, finalisé en 2007, est une SDR où toutes les opérations de traitement du signal sont implémentées sur des processeurs à usage généraux [18].
- Le Japanese National Institute of Information and Communications Technology (NICT) a réalisé une plate-forme SDR pour tester des réseaux mobiles de dernière génération [19].
- SDR4ALL, Software Defined Radio For All, projet de recherche né de la collaboration entre le CEA et l'école d'ingénieurs SUPELEC, consiste en la mise en œuvre d'outils pour tester, en conditions réelles, des algorithmes et schémas de transmission radio [20].
- WARP, Wireless Open Access Research Platform est une plate-forme de radio logicielle communautaire évolutive, extensible et programmable, à vocation académique et de recherche, développée par l'université RICE de Houston (Texas, Etats-Unis) [45].

En ce qui concerne les modules logiciels, plusieurs standards ont été spécifiés : Ham Radio Control Libraries [23], Software Communications Architecture [21,22], Object Management Group Model-Driven Architecture [24] IEEE Standards Coordinating Committee et la GNU Radio [39].

3.4 Sécurité et sûreté de fonctionnement

Des travaux portant sur la fiabilité et la sécurité de ces équipements ont été réalisés. Le Wireless Innovation Forum a élaboré un ensemble d'exigences de sécurité [25] visant à prévenir un comportement indésirable d'une radio logicielle dans le cas d'une action malveillante. La cause de ces comportements anormaux peut être un virus, un vers ou tout autre code malveillant, qui provoquerait la génération d'interférences, des risques sur la santé des personnes (rayonne-

ment électromagnétique), la divulgation (de secrets industriels ou informations classifiées) ou des fraudes en tout genre sur des réseaux à accès payant.

3.5 Des approches matérielles pures et SDR

La réalisation de plates-formes à faible coût est maintenant possible et nombreuses sont les réalisations de SDR radioamateur. Ces équipements offrent la possibilité au plus grand nombre d'étudier le spectre radioélectrique, et notamment les protocoles de transmission radiofréquence. Divers projets universitaires emploient ces radios logicielles à des fins d'étude et de recherche dans des bandes de fréquences autorisées (bandes ISM[9] par exemple), mais aussi l'utilisation de ces équipements sur d'autres parties du spectre, pour par exemple étudier des réseaux sans fil (GSM, GPS, DECT ...).

L'émergence des radios logicielles au sein des équipements de radiocommunication apporte de la souplesse de fonctionnement, une grande évolutivité et permet de réaliser des économies d'échelle aux industriels du secteur. Cependant, la migration logicielle des fonctions de traitement du signal radio a aussi des inconvénients. En effet, de nombreuses normes de radiocommunication sont soumises à licence et/ou restrictions d'emploi. Les équipements conventionnels sont censés respecter ces contraintes de fonctionnement.

4 Analyse de protocoles radios

4.1 Capacité d'analyse d'un modem reconfigurable : le dongle

Les limitations décrites précédemment [10], associées à l'utilisation d'un équipement matériel dédié, notamment en terme de complexité de développement, ont poussé de nombreux chercheurs à utiliser certains matériels dédiés mettant en oeuvre un logiciel reconfigurable.

Ces matériels prennent souvent la forme d'un *dongle* utilisant différents types d'interface de communication avec la machine hôte (USB, PCI, PCIe, ...).

La généralisation de l'utilisation de ce type d'équipement remonte aux débuts de l'étude pratique des réseaux Wi-Fi à la fin des années 90. A cette époque, certaines cartes PCMCIA mettant en oeuvre des chipsets particuliers permettaient le scan, l'écoute voire l'injection de trames sur les réseaux wifi. Celles-ci ont permis la mise en oeuvre des premières preuves de concepts (PoC) visant à démontrer les nombreuses attaques sur la première version du protocole 802.11 (désauthentification, attaque sur le WEP ...).

Ces études ont été rendues possibles car les couches basses des matériels n'étaient pas figées mais reconfigurables logiciellement. Par la suite, de nombreux autres protocoles ont été étudiés par l'intermédiaire de matériels dédiés utilisant un logiciel reconfigurable :

---

9. *Industrial, Scientific and Medical*, bandes radio fréquences réservées pour utilisation par les applications industrielles, médicales et scientifiques.
10. protocole à saut de fréquence, bande passante importante, ...

- ***Bluetooth***
  L'explosion des possibilités offertes par le protocole Bluetooth pour les communications à faible distance a engendré la production en masse de chipsets intégrés directement aux équipements terminaux (PC, téléphones, terminaux de paiement, ...) mais également de *dongles* (généralement USB).
  La grande majorité de ces équipements fournissent le support matériel des couches basses du protocole, nécessité par l'utilisation d'une technique de saut de fréquence assez poussée (jusqu'à 1600 sauts par seconde) et une largeur de spectre importante (79 canaux de 1 Mhz répartis de 2.402 Ghz à 2.480 Ghz). En pratique, ces spécificités du Bluetooth rendent difficile le développement d'un support sur une plate-forme de radio logicielle comparativement aux gains obtenus par rapport à l'utilisation d'un *dongle*.

- ***DECT***
  Créé en 1992, le protocole DECT est aujourd'hui utilisé par plusieurs centaines de millions de périphériques, parmi lesquels principalement des téléphones.
  L'analyse du protocole par la communauté a débuté vers 2006 et a rapidement mené à plusieurs résultats, mettant notamment au jour des faiblesses dans les primitives cryptographiques et les implémentations [3,4].
  Même si les travaux initiaux d'analyse cryptographique du protocole ont nécessité une rétroingéniérie matérielle et logicielle, la démonstration des possibilités d'écoute et d'émission sur des réseaux DECT a été simplifiée par l'utilisation d'une simple carte PCMCIA DECT de type ComOnAir.

- ***Zigbee***
  Basé sur le protocole IEEE 802.15.4, les avantages en matière de simplicité protocolaire, de consommation électrique et de coût de Zigbee en ont fait un protocole de choix pour le contrôle sans-fil dans le milieu industriel et la gestion de bâtiment : climatisation, vannes, alarmes, serrures.
  Des *dongles* voire des kits de développement complets sont disponibles pour des sommes dérisoires. Des projets comme KillerBee[11] permettent de transformer certains de ces *dongles* pour capturer et émettre des trames à bas niveau.

- ***NFC***
  L'apparition de la technologie NFC, notamment sur les téléphones portables, pour des utilisations comme le paiement sans contact ou la récupération de contenu (URL, coupons de réductions, ...) a poussé le développement de projets [6,5] visant à supporter les principaux matériels. Cette technologie ouvre des portes vers l'émulation native de cartes sans contact, ce qui était auparavant difficile à mettre au point matériellement.

11. http://code.google.com/p/killerbee/

4.2 Capacité d'analyse d'une radio logicielle type USRP

Les performances des équipements de type radio logicielle et l'ouverture de ces plates formes dans des projets dits "libres" ont permis aux chercheurs du domaine d'analyser les signaux électromagnétiques qui nécessitaient auparavant des équipements coûteux. Les problèmes d'ordre matériel sont devenus des problèmes logiciels bien moins difficiles à résoudre car les processus de conception, de mesure et de test sont associés à une mise à jour logicielle au lieu d'une conception matérielle.

Les projets "libres" USRP [46] et GNURadio [39] sont des exemples de l'essor de l'utilisation de la radio logicielle. Ces projets ont permis aux spécialistes de la sécurité de s'intéresser aux protocoles radios.

- ***Systèmes champs proche : RFID et NFC***

  En 2006, Henryk Plötz a utilisé un USRP [46], le projet GNU Radio [39] et un outil de visualisation pour capturer et analyser le signal d'identification d'une carte RFID pour déclencher l'ouverture d'une porte dotée d'un système de contrôle d'accès 125 kHz. Ces travaux ont été suivis par l'analyse des technologies à 13.56 MHz ayant abouti aux attaques sur Mifare Classic [47].

- ***Réseaux de données : Bluetooth, ZigBee et Wi-Fi***

  Les protocoles Bluetooth, ZigBee et Wi-Fi ont fait l'objet d'une analyse de leurs mécanismes de sécurité. L'acquistion d'un transfert de données Bluetooth à l'aide d'une radio logicielle de type USRP n'est pas chose aisée du fait de certaines particularités de ce protocole. L'évasion en fréquence impose à l'équipement de mesure une agilité en fréquence ou une bande d'acquisition importante. Ces deux approches consistent au choix :

  – à acquérir tous les canaux Bluetooth en parallèle ce qui nécessite un équipement à bande-passante importante et capable de numériser un grand nombre de données ;
  – à reconfigurer la fréquence de l'USRP à chaque saut de fréquence.

  Celles-ci ne sont en pratique ni satisfaisantes ni suffisantes.

- ***Réseaux cellulaires : DECT et GSM***

  Les réseaux cellulaires ont également fait l'objet d'études ayant permis l'analyse de trames de réseau de téléphonie mobile existants [42]. L'implémentation de la pile protocolaire est d'ailleurs disponible sur Internet depuis 2004. L'analyse du GSM à l'aide d'une radio logicielle permet l'étude et l'analyse des mécanismes cryptographiques présents dans les couches

physiques. Sans implémentation des couches bas niveaux, il est impossible d'étudier en pratique la sécurité de ces réseaux.
En ce qui concerne le DECT un projet d'implémentation a échoué en raison des difficultés rencontrés [41]. Les ressources matérielles pour le traitement des données des couches 3 et 4 du protocole étaient trop importantes pour être gérées pas l'USRP. Les chercheurs se sont alors intéressés à l'utilisation d'un *dongle* dédié [12].
L'implémentation SDR de ces différents protocoles n'a donc pas toujours abouti. Les difficultés rencontrés ainsi que l'attrait du protocole pour la communauté de recherche sont des éléments déterminants pour la réussite du projet.
Des travaux sont en cours dans la communauté sur les réseau PMR-TETRA [43] et les réseaux de téléphonie satellite [42].

4.3 Comparaison des approches SDR et *dongle*

L'analyse de réseaux radio est utile afin de vérifier la conformité de l'implémentation vis-à-vis des spécifications techniques. Les travaux réalisés par différents chercheurs en sécurité ont, avec le temps, démontré le besoin d'auditer les différentes couches de ces protocoles. L'implémentation des mécanismes de sécurité dans certains protocoles comme le GSM ont poussé les chercheurs à s'intéresser à de nouvelles méthodes d'analyse. La radio logicielle est rapidement devenue le moyen efficace pour la compréhension du protocole et des échanges de données entre les différents équipements. Cependant l'audit de ces couches de sécurité nécessite la réimplémentation du protocole dans son intégralité.

La radio logicielle offre les possibilités suivantes lors de l'étude de réseaux sans-fil :

- analyse en disponibilité du canal radio ;
- analyse protocolaire ;
- analyse des données sur l'interface air.

Néanmoins, ces possibilités sont à modérer en fonction :

- de la capacité et les performances des équipements utilisés ;
- de la robustesse du protocole ;
- de la disponibilité des spécifications techniques ;
- des mécanismes de sécurité mis en œuvre.

A contrario l'utilisation de *dongles* ayant une architecture optimisée pour un protocole donné permet une étude simplifiée, notamment dans les cas suivants :

- le saut en fréquence est utilisé par le protocole étudié (Bluetooth) ;
- la largeur spectrale est importante (Wi-Fi) ;

12. carte PCMCIA ComOnAir citées précédemment

– la spécification du protocole est indisponible (DECT) ;
– les mécanismes de sécurité sont mis en oeuvre dans les couches hautes du protocole (Wi-Fi).

5 Evolutions envisagées

L'intégration des nouvelles technologies de transmission radiofréquence dans une plate-forme SDR nécessite une augmentation des performances des interfaces de communication, de la puissance des processeurs et des capacités de traitement du signal par les composants embarqués. L'USRP2 (FPGA de nouvelle génération, interface Gigabit Ethernet) est un premier pas vers des SDR de nouvelle génération. Voici quelques axes d'amélioration possibles des SDR actuelles :

- ***Le défi de la numérisation haut débit***
  Les défis de la numérisation sont aujourd'hui en passe d'être relevés. Cependant, le traitement de ces données est encore lié à l'utilisation de processeurs multi-coeur. Pour contourner cette contrainte, des travaux de conception portant sur un composant analogique ont été réalisé ; le SASP [13] est inséré entre l'amplificateur faible bruit et le CAN [14]. Il a pour rôle d'effectuer un prétraitement analogique du signal RF afin d'abaisser la fréquence de travail du CAN à 10 MHz.

- ***Amélioration des performances des interfaces entre la plate-forme et l'ordinateur hôte***
  L'utilisation de cartes multi-processeur impose au contrôleur principal de pouvoir traiter un grand nombre de données. Afin de transmettre ces données du module radio vers le module principal (utilisation d'un PC hôte pour le module protocolaire) la liaison de donnée doit être la plus efficace possible :
  – Une liaison PCI Express version 2.0 est optimisée pour le transfert de données en streaming et offre un débit utile de 1 Go/s par sens de transmission. La combinaison de plusieurs voies PCI Express pourrait augmenter significativement le débit global. La plupart des ordinateurs disposent d'au moins deux voies par port d'extension. Un accès au bus graphique offre une disponibilité de 32 voies, soit 16 Go/s de données bidirectionnelles en PCIe 32x 2.0. Les spécifications de la version 3.0 de PCI Express prévue pour une commercialisation en courant 2011 prévoient de doubler ces débits ;
  – Une liaison Gigabit Ethernet dernière génération offre jusqu'à 100 Gigabit/s de débit, ce qui est également suffisant pour la plupart des applications. On notera l'évolution de la radio logicielle USRP sur ces aspects permettant le passage d'une bande passante de 8 MHz à 25 MHz ;

13. Sampled Analog Signal Processor
14. Convertisseur Analogique Numérique

  - Une liaison USB 3.0 permettrait par ailleurs d'augmenter les débits de communications ; ce standard n'est cependant pas encore apparu sur des systèmes temps-réel embarqués.

- ***Augmentation des capacités de traitement embarqués***
  Le concept d'intégration de la majorité des traitements in situ est motivé par le fait que les schémas de communication nécessitent des temps de réponse de plus en plus courts. La réalisation d'opérations de traitement du signal par des circuits embarqués spécialisés type DSP et FPGA de plus en plus performants, permet d'envisager la mise en œuvre d'applications temps réel pour des réseaux de communications haut-débits.

- ***Divers types de processeurs au sein d'une même plate-forme***
  Une implémentation typique de SDR contient un processeur général, un DSP ou un FPGA, voire un FPGA embarquant des cœurs DSP. Les systèmes à base de FPGA offrent des performances intéressantes mais au prix d'une augmentation de la complexité de conception. Les processeurs à usage généraux dits GPP sont moins efficaces pour le traitement de la couche physique, mais excellents pour les couches supérieures et paraissent plus accessibles aux développeurs. Aucune solution n'est optimale, c'est pourquoi les processeurs dédiés aux applications de radio logicielle possèdent généralement une architecture hétérogène multicœur composée de FPGA(s), DSP(s) ou GPP(s). L'exploration des capacités des puces graphiques GPU pour des traitements parallèles est en cours ; ces processeurs ayant démontré leurs capacités pour des calculs distribués.

L'apparition de nouveaux standards de communication pour la gestion de transfert de données entre le contrôleur général et les modules de traitement ainsi que les hausses en performance de composants dédiés permettra une amélioration non négligeable des équipements radio logicielle.

En ce qui concerne les projets "libres", plusieurs évolutions prouvent l'impact signicatif sur les techniques d'acquistion et de traitements des échantillons. La numérisation large bande ne peut à elle seule améliorer les débits d'acquisition car le traitement des données est bridé par les capacités des processeurs dédiés ainsi que par le contrôleur principal devant absorber des masses importantes de données.

6 Conclusion

L'utilisation de radio logicielle dans les systèmes de radiocommunication est en plein essor. Cette technologie possède des avantages économiques significatifs : elle permet de réaliser rapidement et à moindre coût les développements nécessaires au support des nombreux protocoles existants ainsi que de ceux en cours de spécification.

L'amélioration des architectures matérielles dédiées aux applications de radio logicielle ainsi que la mise en place de standards internationaux promet à cette

technologie un vaste champ d'utilisation (outils de métrologie, équipement de télécommunications, systèmes tactiques ...).

Les mécansimes de sécurité spécifiés aux niveaux des différentes couches des modèles protocolaires imposent aux chercheurs en sécurité d'adapter les moyens d'analyse aux protocoles testés. L'apparition de périphériques reprogrammables ainsi que la radio logicielle deviennent ainsi des solutions complémentaires pour l'analyse de ces modèles.

La pertinence de l'un ou de l'autre de ces outils d'analyse dépend en pratique des spécificités du protocole considéré, aussi bien au niveau des couches physiques que protocolaires. Une des contraintes résiduelle forte sur l'utilisation de la radio logicielle pour évaluer la robustesse de certains protocoles réside ainsi dans la disponibilité de spécifications techniques.

La disponibilité pour la communauté scientifique et le grand public de ces outils d'analyse a permis de mettre en évidence les limites de certains protocoles et d'améliorer la sécurité de leurs successeurs. Malgré tout, le détournement à des fins malveillante [15] de ces outils d'analyse permet d'envisager la récupération par un attaquant de données personnelles.

Les évolutions à venir de la radio logicielle prenant en compte les limitations des plates-formes actuelles en feront certainement un outil de plus en plus incontournable dans l'analyse des réseaux sans-fil.

15. En France, ces systèmes sont soumis à règlementation dès lors qu'ils deviennent des outils dits d'interception [48]

Références

1. J. Mitola. **"Software Radio Architecture : Object-Oriented Approaches to Wireless Systems Engineering"**. Editions Wiley, 2000. 543 pages. ISBN 0471384925.
2. J. Mitola. **"Cognitive Radio : An Integrated Agent Architecture for Software Defined Radio"**. Ph.D. dissertation, Royal Institute of Technology (KTH), Sweden, 2000, Disponible à http://web.it.kth.se/~maguire/jmitola/Mitola_Dissertation8_Integrated.pdf
3. Andreas Schuler, Erik Tews, Ralf-Philipp Weinmann, **"deDECTed.org"**, 29 Décembre 2008, Disponible à https://dedected.org/trac/raw-attachment/wiki/25C3/talk-25c3.pdf
4. Karsten Nohl, Andreas Schuler, Erik Tews, Ralph-Philipp Weinmann, Mathias Wenzel **"DECT (part II)"**, 29 Décembre 2009. Disponible à https://dedected.org/trac/raw-attachment/blog/slides-for-the-26c3-talk/DECT%20%28Part%20II%29.pdf
5. Projet de boite à outils NFC basé sur libnfc, Disponible à http://code.google.com/p/nfc-tools/
6. Bibliothèque fournissant le support pour l'interaction avec des périphériques NFC. Disponible à http://code.google.com/p/nfc-tools/
7. **"Berkeley Emulation Engine 2"**, Disponible à http://bee2.eecs.berkeley.edu/
8. Dr James E. Gunn, **SDR Market studies Overview**
9. C. Chang, J. Wawrzynek, et R. Brodersen. **"BEE2 : a high-end reconfigurable computing system. IEEE Design & Test of Computers**, IEEE, vol. 22, no. 2, pages 114 à 125, mars-avril 2005. Disponible à http://bee2.eecs.berkeley.edu/papers/BEE2_chang_ieee.pdf
10. S. Mishra, D. Cabric, C. Chang, D. Willkomm, B. Van Schewick, S. Wolisz et B. Brodersen. **"A real time cognitive radio testbed for physical and link layer experiments"**. IEEE International Symposium Dynamic Spectrum Access Networks (DySPAN), novembre 2005, [en ligne]. Disponible à http://www.tkn.tu-berlin.de/publications/papers/dyspan05_cr-testbed2.pdf
11. **"Calit2 Wireless Communications Research and Development Platforms"** Disponible à http://calradio.calit2.net/
12. **Gumstix packs**. Disponible à http://www.gumstix.com/store/catalog/packs.php
13. **"Cognitive Radios and Networks"**. Bradley Department of electrical & Computer Engineering. Virginia Tech, Disponible à http://wireless.vt.edu/research/Cognitive_Radios_Networks/
14. **USB-powered FPGA-based development board**. School of Computer and Communication Sciences of EPF. Disponible à http://fpga4u.epfl.ch/wiki/Main_Page
15. **HPSDR Wiki : Community Portal**. Disponible à http://openhpsdr.org/wiki/index.php?title=HPSDRwiki:Community_Portal
16. P. Bahl, R. Chandra, T. Moscibroda, R. Murty, et M. Welsh. **White space networking with Wi-Fi like connectivity**. SIGCOMM '09, New York, États-Unis

2009, pages 27 à 38. Disponible à http://www.eecs.harvard.edu/~mdw/papers/whitefi-sigcomm09.pdf

17. G. J. Minden, J. B. Evans, L. Searl, D. Depardo, V. R. Petty, R. Rajbanshi, T. Newman, Q. Chen, F. Weidling, J. Guffey, D. Datla, B. Barker, M. Peck, B. Cordill, A. M. Wyglinski et A. Agah. **"KUAR : A Flexible Software-Defined Radio Development Platform"**. Information Technology and Telecommunications Center. Université du Kansas. 2007. Disponible à http://www.ittc.ku.edu/publications/documents/minden2007_dyspan07.pdf
18. R. Farrell, M. Sanchez et G. Corley. **"Software-Defined Radio Demonstrators : An Example and Future Trends"**. 30 septembre 2008. Disponible à http://www.hindawi.com/journals/ijdmb/2009/547650.html
19. H. Harada. **"Software defined radio prototype for multi-mode and multi-service radio communication systems"**. National Institute of Information and Communications Technology (NICT). Disponible à http://www.sdrforum.org/pages/sdr05/4.6%20Special%20Applications%202/4.6-04%20Harada.pdf
20. **Software Defined Radio For All**. Disponible à http://sdr4all.org/index.html
21. **SCA : Support for "Three Category" Approach for Software Communications Architecture (SCA) Standards**
22. **SCA : SCA Implementation Opensource FM3TR Reference Waveform – Developed by Mercury Computer Systems under contract to the Wireless Innovation Forum, this reference implementation provides an open source implementation of an SCA enabled test waveform Link opens Mercury website**
23. **Ham Radio Control Libraries**. Disponible à http://hamlib.sourceforge.net/
24. **Object Management Group Model-Driven Architecture**. Disponible à http://www.omg.org/mda
25. **Security of SDR study**. Disponible à http://srg.cs.uiuc.edu/swradio/
26. D. Spill et A. Bittau. BlueSniff : Eve meets Alice and Bluetooth. First USENIX Conference on Offensive Technologies (WOOT'07), **USENIX, 6 aout 2007**
27. M. Cummings and S. Haruyama., **"FPGA in software radio"**, IEEE Comms. Mag., pp. 108–112, 2 1999.
28. S. Gultchev, K. Moessner, and R. Tafazoli, **"Management and control of reconfiguration procedures in software radio terminals"** in Proc. 2nd Workshop on Software Radios, Karlsruhe, Germany, March 2002, pp. 125–129.
29. R. Hoshyar, S. Gultchev, K. Seo, and R. Tafazolli, **"Software reconfigurability - algorithm level approach"**, in Proc. 4th International Conference on 3G Mobile Communication Technologies, London, UK, June 2003.
30. A. Kountouris and C. Moy, **"Reconfiguration in software radio systems"** in Proc. 2nd Workshop on Software Radios, Karlsruhe, Germany, March 2002, pp. 119–124
31. M. Mehta, N. Drew, and C. Niedermeier, **"Reconfigurable terminals : an overview of architectural solutions", IEEE Comms. Mag., pp. 82–88, 8 2001.**
32. S. Srikanteswara, J. Reed, P. Athanas, and R. Boyle, **"A soft radio architecture for reconfigurable platforms"** IEEE Comms. Mag., vol. 38, pp. 140–147, 2 2000.

33. W. Bennet, J. R. MacLeod, J. P. McGeehan, **"Broadband High Dynamic-Range RF Transmitter Technology for Flexible Multi-Standard radios"**, ACTS, Mobile Communications Summit, Rhodes, June 8-11, 1998.
34. C. Bonnet, G. Caire, A. Enout, P. Humblet, G. Montalbano, A. Nordio, D. Nussbaum, T. Höhne, R. Knopp, B. Rimoldi, **"An open software-radio architecture supporting adavanced 3G+ systems"**, Annales des télécommunications, Tome 56, n^o5-6, mai-juin 2001.
35. A. Ciochocki, R. Unbehauen, **"Neural Networks for Optimization and Signal Processing"**, Wiley and sons, New York, 1993.
36. N. J. Drew, P. Tottle, **"IC Technologies and Architectures to Support the Implementation of Software Define Radio Terminals"**, ACTS, Mobile Communications Summit, Rhodes, June 8-11, 1998.
37. D. Efstathiou, J. Fridman Z. Zvonar, **"Recent Developments in Enabling Technologies for Software Defined Radio"**, IEEE Communications Magazine, August 99, pp. 112-117.
38. H. Harada, M. Fujise, **"Multimode Software Radio System by Parameter Controlled and Telecommunication Toolbox Embedded Digital Signal Processing Chipset"**, ACTS, Mobile Communications Summit, Rhodes, June 8-11, 1998.
39. **"GNU Radio : Introduction and Computational Capabilities of the Open Source GNU Radio Project"**, Wireless Innovation Forum Tom Rondeau (Center for Communications Research, USA), Decembre 2010
40. **Universal Software Radio Peripheral Architectures and Products Lists,** http://www.ettus.com
41. **Research and experimentation with the DECT,** http://dect.osmocom.org/trac/dect
42. **Research and experimentation with the GSM network,** http://misterhac.appspot.com/airprobe.org
43. **Research and experimentation with the TETRA trunked radio system,** http://tetra.osmocom.org/trac/
44. **"The Future is Not the Past ; Watch the Trends"**, Paul Kolodzy (Kolodzy Consulting) , Decembre 2010
45. http://warp.rice.edu/trac/wiki/Projects/UCI_NIJ-SDR
46. http://www.ettus.com/
47. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia **A Practical Attack on the MIFARE Classic**, Disponible à http://www.proxmark.org/documents/mifare_weakness.pdf
48. http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/legislation-en-matiere-d-outils-d-espionnage.html