Caractérisation de l'environnement électromagnétique transport pour la reconnaissance de conditions électromagnétiques critiques

Souheir Mili

N° d'ordre : 41494

THESE

Présentée à

L'Université des Sciences et Technologies de Lille

Pour obtenir le titre de

DOCTEUR DE L'UNIVERSITE

Spécialité : ELECTRONIQUE

Par

Souheir MILI

CARACTÉRISATION DE L'ENVIRONNEMENT ÉLECTROMAGNÉTIQUE TRANSPORT POUR LA RECONNAISSANCE DE CONDITIONS ÉLECTROMAGNÉTIQUE CRITIQUES

Soutenue le 21 octobre 2014 devant la Commission d'Examen :

Rapporteurs :	Françoise PALADIAN, Professeur à l'Université de Clermont-Ferrand 2
	Marc HELIER, Professeur à l'Université Pierre et Marie Curie
Examinateurs :	Olivier COLOT, Professeur à l'Université de Lille 1
	Philippe POULIGUEN, Responsable du domaine scientifique ondes, DGA
	Chaouki KASMI, Inspecteur des systèmes de sécurité, ANSSI
Directeur de thèse :	Marc HEDDEBAUT, Directeur de recherche, IFSTTAR
Encadrants :	Virginie DENIAU, Chargée de recherche, IFSTTAR
	David SODOYER, Chargé de recherche, IFSTTAR
Invité :	Philippe MASSY, Chef de la section Réseaux radio d'entreprise, SNCF.

Thèse préparée au sein du laboratoire LEOST-COSYS de l'IFSTTAR

Remerciements

Quand on désire savoir, on interroge, quand on veut être capable on étudie. Renvoyez sans arrêt ce que vous savez déjà, étudiez sans cesse du nouveau. Alors vous deviendrez maître.
Confucius
Dis-moi et j'oublierais. Montre-moi et je me souviendrais. Implique-moi et je comprendrais.
Confucius

Ces pages du mémoire sont consacrées aux remerciements. Je les utilise en tout premier lieu pour évoquer ma gratitude envers toutes les personnes qui ont participé à ce travail, que ce soit de près ou de loin. Tant de personnes ont rendu possible l'achèvement de cette thèse qu'il est difficile de toutes les citer. J'espère par avance qu'elles ne m'en voudront pas pour tout oubli.

J'exprime tout d'abord mes plus vifs remerciement aux membres du Jury d'avoir accepté de rapporter et d'examiner ce travail de thèse.

Merci à Madame Françoise PALADIAN et à Monsieur Marc HELIER pour avoir accepté d'être rapporteurs de ce travail. Je tiens également à remercier Monsieur Philippe MASSY, Monsieur Olivier COLOT, Monsieur Chaouki KASMI et Monsieur Philippe POULIGUEN de m'avoir fait l'honneur de participer à ce jury de thèse.

J'adresse également de chaleureux remerciements à mon directeur de thèse Marc HEDDEBAUT pour m'avoir conseillé, encouragé et soutenu. Il a toujours été attentif et disponible malgré ses nombreuses charges. Ses compétences, sa rigueur scientifique et sa clairvoyance m'ont beaucoup appris tel un ange gardien ces qualités professionnelles et humaines m'ont aidé à aller au bout de ce travail dans la confiance et la sérénité.

Merci également à mes encadrants, Virginie DENIAU et David SODOYER.

Merci à toi David, cette dernière année a été particulièrement prenante; mais tu m'as soutenu (jamais deux sans trois), tu as su m'écouter et me motiver en permanence et je t'en suis très reconnaissante.
Je te remercie aussi pour toutes nos discussions scientifiques et nos débats statistiques. Tu es une personne rare et unique et j'ai appris beaucoup grâce à toi.

Virginie, que dire pour t'exprimer ma gratitude, tu es plus qu'une encadrante pour moi et je ne pourrais jamais te remercier pour tout ce que tu as fait pour moi. A toi et à ta famille merci, aussi bien sur le plan professionnel que personnel. Tu es devenue plus qu'une amie pour moi, un mentor. J'ai beaucoup appris et évolué sur le plan scientifique; tu as su me guider tout au long de ces trois années et tu n'as jamais douté de moi.

Je tiens à remercier encore une fois l'équipe qui m'a encadré et dirigé, merci de m'avoir donné une chance de collaborer avec vous, d'avoir cru en moi de m'avoir encouragé et d'avoir participé à ma formation doctorale.

Je remercie également l'école doctorale EDSPI 072 pour son implication dans la vie doctorale et ses multiples efforts afin de nous assurer une formation doctorale de qualité.

Merci à toi Sébastien AMBELLOUIS, nos conversations et débats m'ont permis d'avancer sur divers sujets tant professionnels que personnels. Je serais heureuse à l'avenir de poursuivre ces échanges sur nos thèmes d'intérêt scientifique commun.

Je tiens également à remercier tous les participants au projet européen « SECRET » dans le cadre duquel s'est effectuée cette thèse. Les travaux des différents groupes, les réunions de travail et les discussions ont toutes été très constructives pour moi.

Je tiens à remercier également Jean Pierre GHYS et Henri PHILIPPE (SNCF) pour leurs soutiens technique majeur lors des expérimentations menées ensemble sur site.

Je tiens également à remercier Monsieur Charles TATKEU, directeur du laboratoire, tu as été d'une grande aide pour moi à un moment où j'en avais besoin.

Merci à tout le personnel du site IFSTTAR de Villeneuve d'Ascq, amis et collègues, en particulier à toi Stephen, qui a été ma première rencontre au labo et qui est devenue une grande amie, à toi Julien pour nos grands fous-rires, et merci à toi Nadjah, tu es une amie précieuse. Je pense également à mes amis Christophe, Nesrine, Jean-luc, Aurelien, Bilal et Amine pour le soutien qu'ils m'ont apporté.

Merci à toi ma sœur adorée que ferais-je sans toi. Merci à tes deux petits anges AYDAN et IRIS qui ont toujours su me redonner le sourire.

J'ai tenu parole Papa et comme tu le souhaitais, toi qui ne voulais pas assister à une simple soutenance d'ingénieur, te voilà obligé d'assister à ma soutenance de doctorat. L'élève est en train de rejoindre le maître. Merci papa de m'avoir poussé et soutenu.

Et enfin merci à toi Maman, je ne serais pas là sans toi. J'espère que tu es fière car c'est autant ma réussite que la tienne.

Je remercie également mon frère et le reste de ma famille ainsi que les personnes qui m'ont aidé dans la réalisation de ce travail.

Je dédie ce travail à la mémoire de ma grande tante, je t'ai perdu il y a de cela un an
mais j'espère que de là ou tu es, tu es fière de moi.

SOMMAIRE

LISTE DES FIGURES

LISTE DES TABLEAUX

GLOSSAIRE

2G : Système de radio téléphonie cellulaire de deuxième génération
3G : Système de radio téléphonie cellulaire de troisième génération
4G : Système de radio téléphonie cellulaire de quatrième génération
AC : Alternating current
ANFR : Agence Nationale des Fréquences
ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
ATP : Automatic Train Protection
BBAG : Bruit Blanc Additif Gaussien
BBC : British Broadcasting Corporation
BER : Bit Error Rate
BSC : Base Station Controller
BTS : Base Transceiver Station
CEM : Compatibilité électromagnétique
CRI : Radio Chine Internationale
DC : Direct current
dsp : Densité spectrale de puissance
DW : Deutsche Welle
EIRENE : European Integrated Railway Radio Enhanced NEtwork project
EM : Electromagnétique
ERA : Agence ferroviaire européenne – European Railway Agency
ERTMS : European Rail Traffic Management System
ETCS : European Train Control System
ETSI : Institut européen de normalisation des télécommunications
EVM : Error Vector Magnitude (module de l'erreur vectorielle)
FAR : False Alarme Rate
FB : Fractional Bandwidth
GIA : Groupe Islamique Armé.
GSM : Global System for Mobile communications
GSM-R : Global System for Mobile communications – Railways
IEM HA : High altitude Electromagnetic impulse (HEMP)
HIRF : High Intensity Radiated Fields
HPM : High Power Microwave

IEMI : Interférences électromagnétiques intentionnelles
KI : Kol Israël
KVB : Contrôle de vitesse par balise
LBR : Largeur de bande relative
PAMR : Public Acces Mobile Radio.
PMR : Private Mobile Radio
QoS : Quality of Service
RBC : Radio Block Center
RFE : Radio Free Europe
RL : Radio Liberty
RN : Radio Netherlands
RV : Radio Vatican
SACEM : Système d'Aide à la Conduite, à l'Exploitation et à la Maintenance
SHF : Supra-haute fréquence
SJR : Signal to Jammer Ratio
SNCF : Société Nationale des Chemins de fer Français
SNR : Signal to Noise Ratio
STI : Spécification techniques d'interopérabilité
TDMA : Time Division Multiple Access
TETRA : TErrestrial Trunked Radio
TGV : Train à Grande Vitesse
UHF : Ultra Hautes Fréquences
UIC : Union Internationale des Chemins de fer
ULB : Ultra large bande
URSS : Union des Républiques Socialistes Soviétiques
UWB : Ultra Wide Band
VACMA : Veille Automatique par Contrôle du Maintien d'Appui.
VOA : Voice of America

Introduction

Le système ferroviaire dans son ensemble a été techniquement amené à évoluer fortement ces dernières années, non seulement dans un but d'augmentation globale des performances, avec notamment le fort développement de la grande vitesse, mais également dans le but de réduire certaines nuisances générées, telles que sonores.

Le développement de l'interopérabilité ferroviaire en Europe constitue un autre élément majeur de cette évolution accélérée. L'interopérabilité ferroviaire possède pour objectif de permettre aux trains de traverser les frontières européennes sans contraintes techniques et participe de ce fait à la libre circulation des citoyens et des biens en Europe. En effet, pendant longtemps, chacun des réseaux ferroviaires européens a mis en œuvre ses propres techniques, certes dérivées de concepts communs, mais menant à des réalisations pratiques distinctes. Ces réalisations propres ont conduit à une situation ne permettant plus aux trains de franchir les frontières des Etats, la signalisation ferroviaire en particulier n'étant plus comprise au-delà par les trains ou le sol.

Fin 1990, sous l'égide de la Commission Européenne, le European Railway Research Institute (ERRI), disparu depuis, a créé un groupe d'experts ferroviaires nommé A200 en vue de regrouper et d'écrire les exigences liées à l'émergence d'un système de contrôle commande ferroviaire interopérable en Europe pour les trains à grande vitesse. Ce futur système est baptisé European Train Control System ou ETCS. En juin 1991, les industriels de la signalisation ferroviaire travaillant au sein du consortium européen EUROSIG et les réseaux ferroviaires regroupés dans l'Union Internationale des Chemins de fer, l'UIC, se sont mis d'accord afin de définir les spécifications des trois sous-ensembles techniques bien cernés à savoir :

- un nouvel équipement de communication interne fondé sur une architecture informatique ouverte nommé EUROCAB ;
- un nouveau système de communication ponctuelle train-sol interopérable nommé EUROBALISE ;
- un nouveau moyen de communication continu train-sol interopérable appelé EURORADIO.

ETCS et ces sous-ensembles techniques s'inscrivent plus largement dans le nouveau concept de gestion de trafic ferroviaire baptisé European Rail Traffic Management System ou ERTMS. Fin 1993, l'Europe décide une Directive sur l'interopérabilité ferroviaire à grande vitesse et crée une structure destinée à préparer les spécifications techniques d'interopérabilité ou STI. EUROBALISE se fonde sur une variante du système KVB, initié par l'industriel Ericsson, de contrôle de vitesse par balise opérant dans la gamme des 27 MHz. EURORADIO trouve une solution technique par le biais d'une variante du protocole de radiocommunication cellulaire initialement appelé Groupe Spécial Mobile puis, rebaptisé Global System for Mobile communication et, dès lors nommé GSM-Railway ou plus simplement GSM-R dans le monde ferroviaire. Ces travaux se sont poursuivis et amplifiés depuis ; ils se sont en particulier étendus aux lignes à vitesse conventionnelle.

Dans EURORADIO, GSM-R assure une liaison continue entre le train et les centres de contrôle selon un mode de communication connecté. Il fournit au train et au sol les informations de signalisation requises afin de participer à assurer la circulation en sécurité des trains. GSM-R est désormais déployé largement le long de corridors ferroviaires transeuropéens et s'avère un élément clé de la gestion du trafic ferroviaire européen et au-delà de ses frontières.

Il faut donc s'assurer de son bon fonctionnement afin de garantir le bon acheminement des transmissions entre les différents acteurs du système. Ce bon fonctionnement est assuré par le respect d'exigences écrites dans les spécifications techniques d'interopérabilité.

Par ailleurs, l'environnement radioélectrique ferroviaire s'avère très complexe, sujet aux interférences électromagnétiques de tous ordres. Ces interférences peuvent être imputables au système ferroviaire lui-même. Elles peuvent ainsi émaner du matériel roulant, de l'alimentation électrique, de l'électronique de puissance, de la caténaire ou du pantographe... ou encore être imputables à des sources externes au système, tels que les impacts de foudre, les sources d'émission radiofréquence de puissance à proximité de la voie… Ces interférences peuvent également être intentionnelles afin de nuire délibérément aux échanges de données.

Dans le cadre de cette thèse, nous considérons ce dernier type de perturbations électromagnétiques, d'origines intentionnelles. Au même titre que l'emploi de brouilleurs de radiocommunications mobiles opérant dans des conditions très strictes d'utilisation en certains lieux fermés, nous considérons l'existence potentielle de brouilleurs radiofréquences opérant en gamme GSM-R qui perturberaient ces communications et ainsi pourraient conduire à une dégradation consécutive des performances du système de gestion de trafic.

Habituellement, lorsqu'il s'agit d'interférences électromagnétiques, les experts se réfèrent aux normes ferroviaires de compatibilité électromagnétique ou CEM. A ce jour cependant, les normes existantes ne traitent pas encore des situations de brouillages électromagnétiques intentionnelles pour les

systèmes de transmission mobile et peu d'éléments de référence s'avèrent disponibles afin de traiter ce problème.

Cette thèse se propose de contribuer à apporter des éléments scientifiques de réponse à celui-ci, notamment en évaluant la faisabilité de techniques permettant d'identifier la présence de signaux de brouillage se superposant à un environnement électromagnétique ferroviaire habituel, que nous qualifions de « normal ».

Cette caractérisation se fonde sur certains paramètres caractéristiques du protocole GSM-R et intègre une part de la grande diversité des environnements électromagnétiques ferroviaires en mesure d'être rencontrés, en voies, en gares, à bord des trains… Nous établirons ainsi des liens entre ces caractéristiques représentatives et la qualité des transmissions effectuées.

Lors de ces travaux, nous serons amenés à créer des modèles représentatifs du système dans ce mode de fonctionnement « normal », assurant une qualité de transmission satisfaisante et à les confronter à d'autres, représentant diverses situations de brouillage, en mode « attaqué ». Nous créerons ainsi, à partir de brouilleurs disponibles prêtés par un opérateur ferroviaire, des bases de données de signaux de brouillage électromagnétiques en mesure d'effectuer leurs détections ultérieures voire, de permettre l'identification de ces brouilleurs. Des mesures effectuées en simulation puis en laboratoire nous permettront d'établir initialement ces modèles. Elles seront par la suite enrichies par d'autres données issues d'expérimentations réalisées in situ.

La finalité de ce travail et des méthodes développées consiste à être en mesure de mettre en place un système de détection et, ou de classification de ces attaques dans les terminaux GSM-R placés dans les trains ou le long de la voie ferroviaire permettant d'anticiper les dégradations critiques des liaisons et de mettre en œuvre ensuite des contremesures permettant de les pallier.

Dans la perspective de restituer le travail effectué lors des trois années écoulées, ce mémoire de thèse est organisé en quatre chapitres et des annexes, proposés de la manière suivante :

Le chapitre 1 vise à mettre en avant l'intérêt et les objectifs de la thèse. Il décrit dans un premier temps la notion d'infrastructure critique et aborde plus particulièrement celle ferroviaire. Le système ERTMS et ses composantes sont rappelés pour les points qui concernent notre étude. Nous pointons en outre les entrées du système potentiellement vulnérables aux brouillages électromagnétiques. Nous mentionnons ensuite les différents systèmes de brouillages radioélectriques intentionnels référencés avant de passer en revue différentes attaques perpétrées par le passé contre le système ferroviaire. Nous expliquons par la suite les conséquences potentielles générées par ces brouillages électromagnétiques sur le système ferroviaire. Nous concluons ce chapitre par une synthèse des

normes ferroviaires mises en place auxquelles nous pouvons nous référer afin d'établir un fonctionnement GSM-R « normal ».

Le chapitre 2 propose initialement d'approfondir certains de ces éléments. Il décrit les interférences perturbant la communication GSM-R avant de rentrer plus en détails dans la description des brouilleurs électromagnétiques et des formes d'ondes générées. Nous présentons par la suite une architecture de communication GSM-R typique et effectuons une première analyse de l'impact des perturbations selon la localisation du brouilleur au sein de cette architecture. Nous passons ensuite à la présentation de l'ensemble des outils qui seront exploités par l'étude. Nous introduisons dans un premier temps les méthodes d'analyse que nous emploierons. Puis, le banc de mesure utilisé afin de mettre en œuvre ces analyses sera décrit. Son utilisation permettra d'acquérir les résultats initiaux nécessaires à l'alimentation des bases de données nécessaires aux méthodes sélectionnées. De premiers résultats expérimentaux seront discutés permettant de fournir des ordres de grandeur réalistes de niveaux de brouillage critiques. Enfin, nous présenterons la chaîne de communication employée. Celle-ci sera modélisée en précisant les informations qui seront prélevées et scrutées le long de cette chaîne proposant une représentation simplifiée mais réaliste pour notre étude d'un récepteur GSM-R.

Le chapitre 3 est consacré aux méthodes de détection et de classification des perturbations produites par les brouilleurs électromagnétiques. Nous décrivons les éléments théoriques exploités afin de mettre en place le système de détection et de classification supervisé envisagé. Une représentation des formes des signaux est introduite ainsi que les organigrammes régissant le fonctionnement du système de détection. Nous commençons par les modèles quadratiques permettant uniquement la détection des signaux de brouillage. Nous poursuivons et concluons ce chapitre avec les modèles fréquentiels en mesure d'assurer à la fois la détection et la classification des signaux de brouillage.

Le chapitre 4 présente les résultats de détection et de classification obtenus durant nos travaux. Nous exploitons nos modèles à l'aide des différentes bases de données et selon les différents scénarios de perturbation générés par simulation, sur le banc de mesure réalisé au laboratoire et en environnement réel. Nous concluons ce chapitre en faisant le point quant à l'applicabilité des méthodes de détection et de classification employées dans le contexte ferroviaire particulier considéré. Pour ce faire, nous prenons en compte en particulier la robustesse des résultats obtenus vis-à-vis de la complexité de l'environnement électromagnétique pris en compte.

Nous dressons finalement quelques perspectives permettant de poursuivre ce travail de recherche initial.

Le travail mené dans le cadre de cette thèse entre dans le cadre du projet européen SECRET «SECurity of Railways against Electromagnetic aTtacks» du septième programme cadre de recherche

et développement. Ce projet vise à développer des solutions innovantes afin d'améliorer la résilience électromagnétique des systèmes radio ferroviaires.

Chapitre 1 : Objectif et contexte du travail

SOMMAIRE

I. Objectif de la thèse

En raison de son déploiement très vaste et de son accès relativement aisé, l'infrastructure ferroviaire apparaît susceptible de subir d'éventuelles attaques, menées sous différentes formes. Celles-ci peuvent avoir des conséquences significatives sur l'économie ainsi que sur la sécurité du mode de transport. Ces dernières années, des efforts considérables ont été déployés en vue de développer un système de gestion du trafic ferroviaire paneuropéen interopérable. Ces systèmes sont de ce fait bien documentés et leurs caractéristiques techniques sont également largement diffusées et disponibles, les rendant ainsi, peut-être, plus vulnérables à grande échelle en cas d'actions malveillantes. Des communications radio de différentes natures sont largement employées pour gérer ce trafic ferroviaire.

Ces dispositifs de communication interviennent à de nombreux niveaux, contrôle-commande embarqué, communication entre trains et infrastructure (voix et données de signalisation) et services aux voyageurs. Leurs mises en défaut à l'aide de signaux de brouillage radioélectrique intentionnels pourraient potentiellement conduire à de sérieuses anomalies de fonctionnement.

Dans ce contexte, le travail mené dans cette thèse possède pour objectif principal de détecter efficacement des attaques électromagnétiques intentionnelles et de les identifier. Ce travail se focalise sur la radio sol-trains, composante importante du système de gestion de trafic ferroviaire. Nous développerons des méthodes de surveillance de l'environnement radioélectrique afin de détecter des signaux de brouillage visant à mettre en défaut cette radio sol-trains. Ces méthodes nous permettent d'obtenir une représentation des caractéristiques globales de l'environnement radioélectrique ferroviaire dans la bande de fréquence d'intérêt.

Pour cette entrée en matière constituée par ce premier chapitre, nous proposons de présenter le cadre général de cette étude en abordant successivement la notion d'infrastructures critiques et, en particulier celle de transport ferroviaire. Nous poursuivrons en rappelant les composantes de l'interopérabilité ferroviaire tout en nous focalisant sur la radio sol-trains qui constitue l'objet d'étude de ce travail de thèse. Nous montrerons que la radio-sol-trains pourrait être potentiellement brouillée par des signaux radio opérant dans les bandes allouées à l'aide de systèmes de brouillage radioélectriques intentionnels existants. Nous proposerons ensuite une classification des attaques déjà subies par le système ferroviaire ainsi qu'un bref historique des agressions les plus marquantes. La conséquence d'un brouillage radio pouvant être la perte de la liaison radio sol-trains, nous envisageons ce cas de figure ainsi que ses conséquences sur l'exploitation. Nous identifierons enfin les spécifications techniques

disponibles imposées afin de garantir le fonctionnement correct de cette radio sol-trains constituées des normes existantes pertinentes pour notre étude.

II. Les infrastructures critiques

La commission européenne décrit les infrastructures critiques comme suit : "Les infrastructures critiques sont les installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements des États membres. Les infrastructures critiques se trouvent dans de nombreux secteurs de l'économie, y compris les secteurs bancaire et financier, les transports et la distribution, l'énergie, les services de base, la santé, l'approvisionnement en denrées alimentaires et les communications, ainsi que certains services administratifs de base" [1.1].

Comme on peut le constater, ces infrastructures critiques sont nombreuses et occupent une place importante dans notre quotidien, que ce soit directement, ou indirectement. Nous pouvons les classer selon leurs impacts à l'aide de la figure 1.1 [1.2].

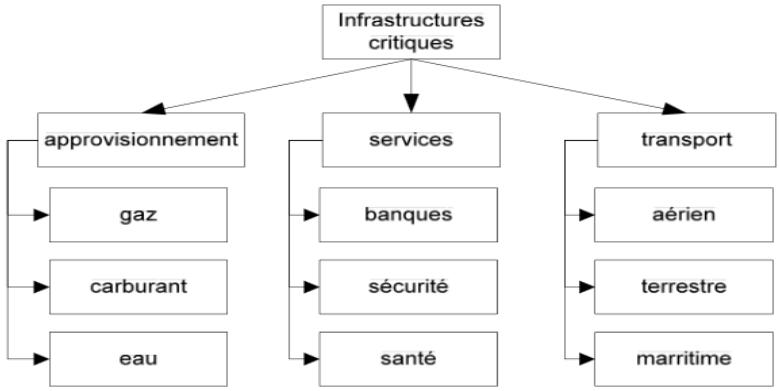


Figure 1.1. Classement des infrastructure critiques

Considérons plus particulièrement deux de ces infrastructures.

L'infrastructure de télécommunication assure simultanément les échanges de données et la communication entre individus. Elle s'avère également capitale et sa mise en défaut aurait des effets catastrophiques. Historiquement, les télécommunications représentent la première infrastructure critique. Ceci vient de la gestion de la crise qui opposait les présidents Kennedy et Khrouchtchev lors de l'installation de missiles à Cuba en 1962 [1.3] et des échanges vitaux et critiques qui se sont à l'époque déroulés, à distance, entre ces deux présidents.

Celle liée à l'énergie représente également une des infrastructures essentielles de notre quotidien. Composée de l'ensemble des moyens de production de transport et de distribution, elle s'avère parmi les plus importantes d'une nation car, de son bon fonctionnement, dépend celui de nombreuses autres infrastructures critiques. Sa défaillance provoquerait ainsi par effet domino la mise en défaut de nombreuses autres infrastructures critiques comme les transports.

III. L'infrastructure critique ferroviaire

La mobilité constitue un des besoins fondamentaux de l'homme dans nos sociétés modernes. Pour cela, une autre entrée aussi importante que les précédentes est constituée par les infrastructures de transport. Le bon fonctionnement de celles-ci autorise notamment l'acheminement quotidien de centaines de millions de voyageurs. Les infrastructures de transport sont réparties en trois grandes catégories : transport terrestre (route et rail), transport par voie d'eau (fluvial et maritime) et transport aérien (aviation civile). Le transport peut également être subdivisé entre transport de passagers et transport de marchandises qui, bien souvent, exploitent les mêmes grandes infrastructures. Une dégradation de ces systèmes génèrerait un ensemble de répercussions en chaîne ayant un impact économique et social majeur.

Lors de ce travail, nous nous focalisons sur l'infrastructure de transport ferroviaire couvrant plus de 152 000 km de corridors prioritaires en Europe. Ces lignes de chemin de fer constituent un moyen de transport vital assurant tant le transport de voyageurs que celui de marchandises, En France, le réseau représente 53 452 km de lignes, 1 875 km sont des lignes à grande vitesse et 15 164 km des lignes électrifiées [1.4]. Ce réseau conséquent assure l'acheminement annuel de plus de 105 milliards de voyageurs.

En France, les chemins de fer sont apparus en 1827. Ils ont représenté depuis ce jour un défi technologique et une révolution culturelle en évoluant en quelques dizaines d'années de la machine à vapeur au train à grande vitesse alimenté en courant industriel. En phase avec l'évolution de la motorisation, celle des systèmes de commande et de régulation du trafic a pris également un essor considérable [1.5]. Cet essor s'est effectué de façon parallèle mais non concertée dans chacun des états européens. Ceci a conduit rapidement à des solutions proches sur le plan des principes mis en jeu mais cependant souvent incompatibles techniquement. Par conséquent, les trains ne pouvaient pas franchir les frontières nationales.

Chacun des réseaux européens se caractérise dès lors par sa propre signalisation, parfois par une tension d'alimentation de la caténaire particulière, un écartement des rails distinct, des limitations de vitesse, ou encore des règles de sécurité et de freinage spécifiques.

Le passage des trains aux frontières demande donc des procédures et des normes complexes afin de s'adapter. Pendant longtemps, le choix a été fait de changer de locomotive et de conducteur à la

frontière. Plus récemment, certains trains ont été adaptés (Thalys, Eurostar…) et sont équipés d'autant de systèmes de signalisation et d'électronique de puissance que de pays à traverser. Cette multiplicité d'équipements augmente le risque de mauvaises interprétations de la signalisation par le conducteur et provoque aussi une perte de temps qui se répercute sur la gestion du trafic. Ceci engendre des conséquences non seulement financières mais humaines [1.6].

Pour pallier ce problème et autoriser la libre circulation des citoyens et des biens dans l'espace européen, des travaux ont été entrepris qui ont permis l'arrivée de la directive 96/48/CE [1.7] du Parlement européen décrivant et ouvrant la voie vers l'interopérabilité ferroviaire. Nous reprenons cette définition : « L'interopérabilité est l'aptitude du système ferroviaire transeuropéen à grande vitesse à permettre la circulation sûre et sans rupture de train à grande vitesse en accomplissant les performances spécifiées. Cette aptitude repose sur l'ensemble des conditions réglementaires, techniques et opérationnelles qui doivent être remplies pour satisfaire aux exigences essentielles. » Cette directive européenne a permis l'émergence puis le déploiement du système ERTMS (European Railway Traffic Management System) afin de permettre l'harmonisation nécessaire, d'assurer la bonne circulation et d'éviter la rupture de charge des trains sur les lignes. Ce nouveau système de gestion du trafic ferroviaire possède pour but la standardisation des différents systèmes coexistant à ce jour en Europe et d'autoriser une interopérabilité des systèmes de contrôle commande ferroviaires.

III.1. ERTMS / ETCS

ERTMS constitue le nouveau système de gestion du trafic ferroviaire paneuropéen mis en place dans le but d'assurer l'interopérabilité ferroviaire. ERTMS permet de gérer le contrôle de vitesse des trains en assurant la sécurité grâce notamment à un échange d'informations entre le sol et les trains. Il est constitué de deux éléments de base. ETCS (European Train Control System) remplace le grand nombre de systèmes de contrôles de vitesse et de signalisation actuellement utilisés sur les différents réseaux par un nouvel équipement. GSM-R (Global System for Mobile communications – Railways), le standard de communication adapté aux spécifications ferroviaires remplace progressivement les différentes radios analogiques exploitées depuis la généralisation de l'emploi de la radio sol-trains. Entre 2007 et jusqu'à présent, l'Union européenne a favorisé par des financements la mise en place et la migration des différents systèmes en service dans les Etats membres par ERTMS [1.8]. Le déploiement d'ERTMS se poursuit suivant trois niveaux. Le premier niveau exploite une communication ponctuelle par balises au sol, les deuxième et troisième niveaux exploitent une radio sol-trains continue fondée sur le déploiement d'un réseau de communication GSM-R déployé spécifiquement le long des lignes [1.9].

Les informations échangées avec le sol permettent de planifier la stratégie de circulation des trains, de définir des courbes de vitesse maximales autorisée. ETCS intervient automatiquement si elles ne sont pas respectées et prend la main au conducteur pour assurer le respect des vitesses imposées [1.10].
ETCS possède trois composantes de communication afin d'assurer son bon fonctionnement. Elles apparaissent figure 1.2 et sont constituées d'une architecture informatique de communication interne au train appelée EUROCAB, d'une communication ponctuelle notée EUROBALISE par balises et d'une communication sol-trains continue EURORADIO, portée par GSM-R.

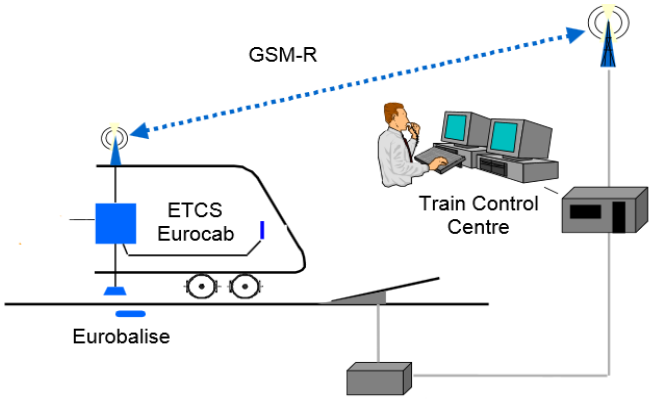


Figure 1.2. Infrastructure ERTMS / ETCS

III.1.1. Eurocab

L'équipement ETCS de contrôle des trains se décompose en fonctions installées à bord du train et en fonctions disposées sur la voie. Eurocab représente la partie disposée à bord des trains. Celui-ci gère la protection automatique des trains (Automatic Train Protection – ATP) en assurant la compatibilité avec tous les systèmes ATP européens préexistants, par un système ouvert, intégrant ETCS.

III.1.2. Eurobalise

Les balises sont des éléments fixes placés sur la voie, fixés sur les traverses, tels que représentées figure 1.3. Elles communiquent de loin en loin avec le train grâce aux lecteurs de balises montés sous les trains. Les eurobalises permettent l'échange d'informations entre sols et trains. Elles assurent également la fourniture d'un top précis de localisation lors du passage du train au droit de celle-ci, effaçant la dérive des capteurs proprioceptifs de localisation. La balise est activée par un signal émis depuis l'antenne du lecteur de balise du train. L'eurobalise est télé alimentée à une fréquence de 27 MHz (lien descendant). En retour la balise émet vers l'antenne (lien montant) un signal portant les données dans une gamme de fréquences centrée sur 4,23 MHz [1.11].

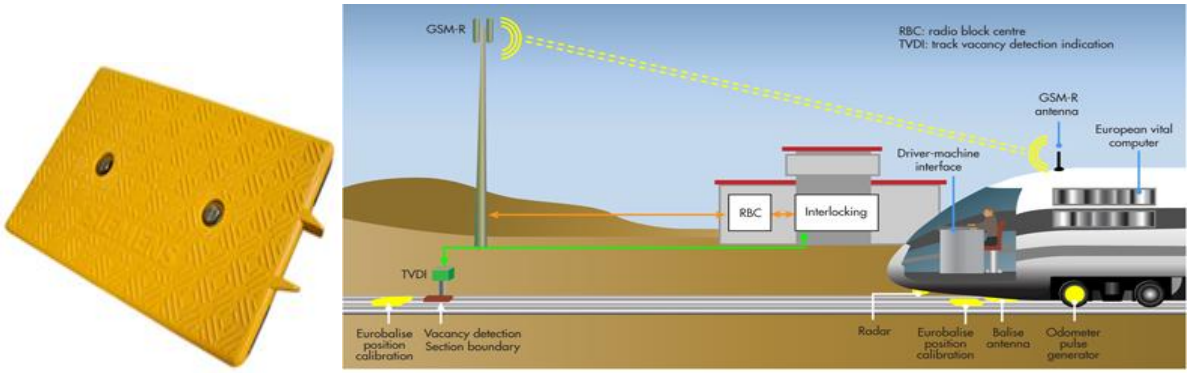


Figure 1.3. Eurobalise.

III.1.3. Euroradio

Euroradio est le système sélectionné pour réaliser le système de communication dédié au ferroviaire. Cette interface assure la sécurité des communications entre le train et les Radio Block Center (RBC) au sol via un réseau spécifique. L'euroradio utilise un protocole spécial qui permet d'encoder et de décoder les messages reçus et envoyés par les RBC [1.12].

III.1.3.1. TETRA

Au cours des dernières années, lorsque des évènements majeurs sont survenus, les équipes d'intervention d'urgence de plusieurs pays européens ont connu des problèmes d'interopérabilité de communication, en partie en raison de l'absence de normalisation de leurs équipements radio mobile. Afin de pallier ce problème, le système TETRA (TErrestrial Trunked RAdio) a été spécialement mis en place dès 1995. Il propose et présente une infrastructure commune à tous les services officiels en Europe afin d'assurer ces besoins spécifiques de communication [1.13]. TETRA est utilisé par les services de sécurité publique comme les forces de polices et les pompiers mais aussi sur certains sites industriels, ou par tout autre groupe fermé d'utilisateurs. TETRA assure des fonctionnalités de protection et de confidentialité des communications sensibles. Ce système est construit de telle manière à garantir un transfert des données à des vitesses plus rapides que celles observées dans les communications mobiles.

Il a été décidé entre 1985 et 1989 par l'Union Internationale des Chemins de fer (UIC) d'acquérir certaines fréquences afin de les utiliser en emprise ferroviaire pour des besoins opérationnels. Quelques études ont été menées pour évaluer les besoins en fréquences ainsi que pour mesurer en parallèle les avantages et les inconvénients de deux systèmes émergents à l'époque, TETRA et GSM. Finalement la décision a été prise de choisir une variante du système GSM pour assurer les communications radio [1.13]. Les raisons de ce choix ont été l'emploi d'une radio numérique cellulaire de seconde génération bénéficiant déjà de développements considérables menés par

l'industrie des télécommunications et à laquelle peu de modifications seraient à apporter afin de satisfaire le cahier des charges ferroviaire.
TETRA reste cependant utilisé par certains opérateurs tels que la SNCF afin d'assurer tous les services de communication radio en gares.

III.1.3.2. GSM-R

Afin d'assurer les communications sol-trains, le protocole de communication GSM-R s'est progressivement imposé. La connexion s'établit par une liaison radio entre la station mobile présente dans le train et les antennes-relais installées le long des voies.
GSM-R fournit aux opérateurs ferroviaires des services pour les communications vocales. Il permet également des échanges d'informations de signalisation, des appels d'urgence, des communications de maintenance et des appels de groupes (VGCS : Voice Group Call Services). GSM-R autorise également le transfert des données de diagnostic, celui de l'information aux passagers via les annonces ou appels diffusés (VBS : Voice Broadcast Services).
GSM-R reprend les principes de base du standard de communication cellulaire. Une gamme de fréquences lui a été attribuée spécialement, partout en Europe, afin de couvrir les besoins ferroviaires. Deux fois 4 MHz de bande sont disponibles comme le représente la figure 1.4. Ces deux gammes servent pour le lien montant, de 876 à 880 MHz et, le lien descendant, de 921 à 925 MHz. Chacune de ces bandes est divisée en canaux de 200 kHz de large.

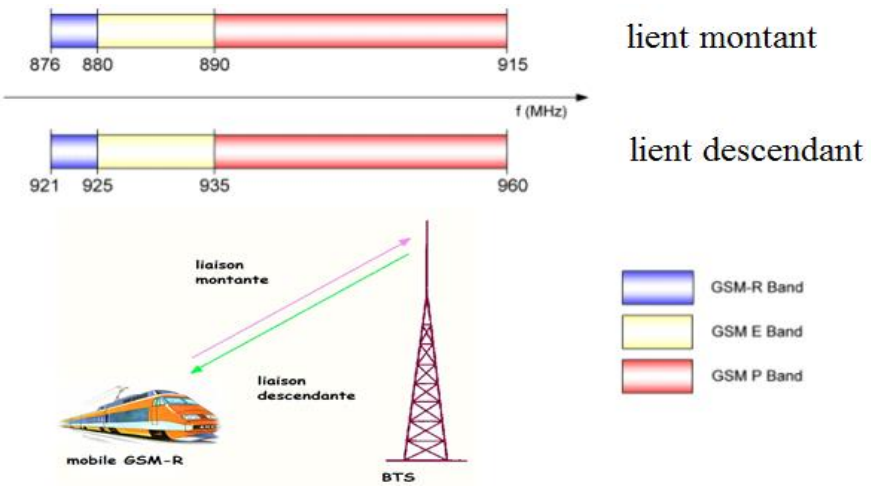


Figure 1.4. Fréquences GSM-R.

Plusieurs éléments composent un système GSM-R.

- ***GSM-R CABRADIO***

Le Cabradio est l'équipement de communication qui se trouve à bord du train. Il représente le moyen de communication vers l'extérieur principal des conducteurs. Il ne se limite pas aux échanges téléphoniques mais sert également au transfert de données. L'émetteur développe une puissance maximale de 8 W dans les bandes de fréquences paneuropéennes allouées. Une ou plusieurs antennes sont montées, généralement au-dessus de la cabine de conduite. Ceci permet de limiter la longueur des câbles coaxiaux acheminant les signaux de et vers les antennes. Le Cabradio supporte les communications sol-trains à des vitesses qui peuvent dépasser 500 km/h.

- ***Radio block center***

Le RBC, installé au sol, reçoit et envoie des messages électroniques vers les équipements ETCS à bord des trains. Un RBC couvre une zone géographique particulière correspondant à plusieurs cellules consécutives GSM-R. Chaque message électronique peut contenir un ou plusieurs paquets de données. Ces paquets de données possèdent la même structure que ceux transmis par les balises à la voie.

- ***Les stations de base***

Les stations de base ou BTS – Base Transceiver Stations sont constituées des antennes et des équipements radio installés en bordure des voies qui assurent la couverture radio. La portée radio d'une BTS est limitée à quelques kilomètres, les signaux sont focalisés au moyen d'antennes directives vers l'amont et l'aval de la voie afin de couvrir au mieux l'infrastructure ferroviaire. La BTS est un ensemble d'émetteurs-récepteurs qui gère localement la transmission radio (modulation, démodulation, égalisation, codage correcteur d'erreur…). Les BTS réalisent aussi des mesures de puissances reçues et de qualité radio afin de vérifier que les communications en cours se déroulent efficacement.

- ***Les contrôleurs de stations de bases***

Ainsi que sur un réseau GSM standard, un contrôleur de stations de base GSM-R ou BSC - Base Station Controller gère un ensemble de BTS. Ce contrôleur constitue un nœud de communications vers et en provenance des BTS. Le BSC assure la gestion des ressources radio pour la zone couverte par les différentes stations de base qui y sont connectées. Il commande l'allocation des canaux radio et exploite les mesures effectuées par les BTS afin de contrôler les puissances d'émission du mobile. Cette dernière est fonction de la distance mobile-émetteur de telle manière que la liaison soit toujours de bonne qualité.

Ainsi que nous venons de le rappeler, GSM-R est le support utilisé pour les transmissions de la voix et de données indispensables à la signalisation ferroviaire. Ceci fait de lui un système vital lié à

l'infrastructure critique ferroviaire. Un des points vulnérables de l'architecture ferroviaire que nous pouvons identifier serait ainsi ce système de communication sol-trains.

Dans ce qui suit, nous nous concentrons sur cet aspect du problème. Cependant, avant de traiter de façon plus approfondie celui-ci, évaluons quels sont les points d'entrée possibles de brouilleurs électromagnétiques intentionnels dans le système.

IV. Points d'entrée potentiels des signaux de brouillage dans le système

La figure 1.5 représente les points d'entrée potentiels des signaux de brouillage dans ERTMS/ETCS, tels qu'ils ont été identifiés dans [1.14]. On retrouve sur ce schéma les éléments critiques évoqués précédemment :

- Les eurobalises et leurs éventuelles extensions euroloop[1] permettant d'accroître la portée de la communication par balises.
- L'odométrie train, fondée sur l'utilisation de capteurs proprioceptifs de type radar et roue phonique, associés aux balises pour la relocalisation, lorsque la dérive intrinsèque aux capteurs proprioceptifs devient problématique.
- GSM-R, représente à la fois par les mobiles et par le réseau installé à l'infrastructure qui constitue le point d'entrée que nous considérons.

[1] Câble rayonnant monté entre les rails qui permet d'étendre la portée de la communication par balise et dont l'installation reste optionnelle.

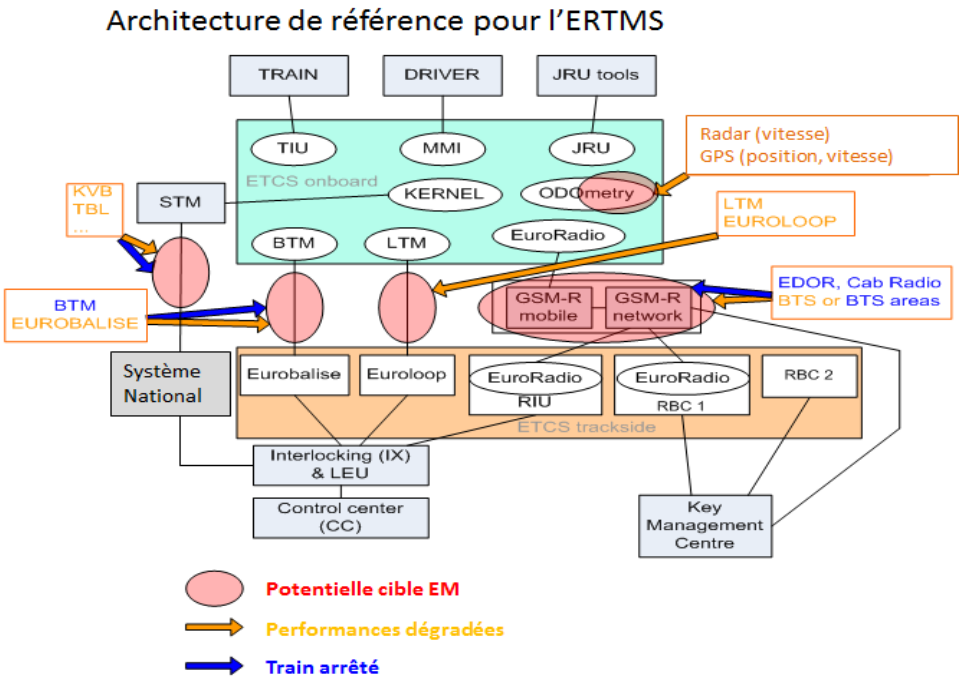


Figure 1.5. Points d'entrée potentiels des signaux de brouillage (source ALSTOM).

V. Les systèmes de brouillage radioélectriques intentionnels

V.1. Introduction

Les systèmes de brouillage intentionnels ont vu le jour pour des besoins militaires afin de perturber les communications tactiques. Ils sont apparus pratiquement dès l'utilisation de la radio par les forces armées.

Le principe du brouillage réside dans le fait d'envoyer un signal de bruit à une forte puissance, couvrant ainsi le signal utile et le rendant inutilisable. L'apparition de ces signaux peut avoir comme conséquence une perturbation du système, voire l'empêcher complètement de fonctionner temporairement ou définitivement.

Actuellement, les dispositifs de brouillage, dont la détention et l'utilisation sont interdits, leurs importations étant strictement contrôlées et leurs utilisations réprimées, restent cependant accessibles sur certains marchés internationaux. Ils peuvent constituer de petits équipements discrets et autonomes délivrant une puissance de brouillage déjà significative, de l'ordre du watt, voire plus.

L'effet du brouillage se manifeste sous la forme d'interférences dues à l'interaction entre équipements et à la dégradation de l'information reçue liée à l'introduction d'une énergie de brouillage non désirée.

Différentes catégories de brouillages ont été répertoriées selon leurs causes, leurs effets et les caractéristiques du brouillage radioélectrique.

V.2. Blocage de réception pour des signaux hors bande

Il est important de distinguer ici les notions de brouillage et de blocage. A l'inverse du brouillage, le blocage du récepteur repose sur des interférences dues à de puissantes émissions hors bandes qui provoquent une désensibilisation des étages d'entrée du récepteur, entrainant une dégradation de la communication. Ce genre de problèmes est souvent résolu en ajoutant des filtres supplémentaires à l'émission comme à la réception, rejetant les signaux hors bande. A titre d'exemple, les récepteurs GSM-R se dotent actuellement sur certains réseaux de filtre additionnels afin de se prémunir de l'arrivée de signaux de radiotéléphonie cellulaire 3G et 4 G hors bande, parfois puissants. Ces sources peuvent être proches avec des infrastructures 2 G, 3 G et GSM-R presque co-localisées ou utilisées par les passagers en embarqué à bord de trains, tramways, métros…

V.3. Quelques utilisations effectives de signaux de brouillage

V.3.1. Brouillages volontaires de la radiodiffusion

Certains brouillages intentionnels apparaissent lorsqu'un opérateur transmet délibérément sur une fréquence occupée. Ce type de brouillage peut être utilisé pour empêcher l'information d'être acheminée. Il s'agit d'un moyen courant de censure dans les régimes totalitaires, où les stations radios étrangères situées à proximité du pays sont brouillées, pour qu'elles ne puissent pas être reçues par les habitants [1.15].

Le premier radio-brouillage militaire a été enregistré contre le télégraphe au début du vingtième siècle. Les russes et les allemands ont été initiateurs dans ce domaine. Berlin a commencé à brouiller le programme radio de Kominterm. En 1931, l'URSS brouille la radio roumaine. En 1934, la radio allemande est brouillée par l'Autriche puis, en 1940, l'URSS brouille les communications radio du Vatican. La majorité des brouillages radio fut entrepris par l'union soviétique, qui a contribué à développer ces systèmes [1.16]. Lors de la seconde guerre mondiale, les allemands ont entrepris de brouiller les transmissions de la BBC et d'autres stations alliées pour empêcher les citoyens et la résistance d'écouter les diffusions de messages codés.

Durant la guerre froide, les soviétiques ont eu recourt aux brouillages des communications occidentales, cela a abouti à augmenter les puissances de transmission. La Radio Free Europe et son service jumelé Radio Liberty furent les cibles principales des brouilleurs soviétiques, suivies par la Voice of America (VOA) et la BBC World Service. Ces opérations ont commencé en 1948 par le brouillage de VOA et de la BBC puis, a évolué jusqu'en 1988 pour inclure Radio Chine Internationale (CRI), Deutsche Welle (DW), Kol Israël (KI), Radio Corée, Radio Vatican (RV), Radio Netherlands (RN), et d'autres. Lorsque les deux Radio Free Europe (RFE) et Radio Liberty (RL) ont commencé leurs émissions en 1951 et 1953, dédiées uniquement à l'Europe de l'Est et l'Union soviétique, elles

furent également les cibles des interférences avec quelques interruptions occasionnelles de services linguistiques de l'Est jusqu'à ce que le brouillage cesse complètement en 1988.
Durant l'année 2009, différents cas de brouillage ont été constatés en Iran, sur la télévision par satellite ainsi que sur les accès internet, ces perturbations ont coïncidé avec les élections présidentielles et ont eu pour but de contrôler le flux d'actualités, réduisant ainsi la liberté d'expression. Par la suite, le gouvernement iranien a indiqué que ces brouillages ont été utilisés dans le but de protéger les citoyens contre les valeurs non islamiques [1.17].
Sur internet, la BBC chinoise a été bloquée en Chine depuis son lancement en 1999. La BBC Perse a été perturbée par intermittence à partir de 2006, et régulièrement depuis 2009 [1.18]. Aujourd'hui encore la Chine bloque les services en langue chinoise de Radio Moscou, ainsi que toute la programmation de Radio Free Asia en Asie du Sud et d'autres services de radiodiffusion de l'Ouest.

Au fil du temps, les techniques de brouillage ont évolué et ne sont plus cantonnées au domaine militaire. Ses principes se sont améliorés en fonction du développement technologique et des nouvelles cibles à toucher. Dès 1976, une autre étape dans la réalisation de brouilleurs a débuté par l'envoi de signaux de perturbation similaires à ceux attendus par le récepteur mais, portant des informations erronées ouvrant la voie aux systèmes de leurrage.

V.3.2. Brouillage de la navigation aérienne

L'une des premières cibles de brouillage a également été l'aviation militaire. Des brouilleurs de radars ont été utilisés dès la seconde guerre mondiale. Ils se sont avérés très efficaces pour empêcher la détection des cibles.
En 1992, un accident aérien majeur dû à un type de brouillage est survenu en France. Une catastrophe aérienne causée par un écart dans le sens longitudinal entre la hauteur affichée par les appareils de mesure et la hauteur réelle de l'avion par rapport à la piste a entrainé l'écrasement d'un avion civil sur le mont Sainte-Odile. La défaillance des systèmes de navigation constitue la cause la plus probable de l'accident et il a été diagnostiqué qu'elle était due à un brouillage non intentionnel des signaux de radionavigation.
L'automatisation des systèmes de contrôle aérien représente un risque et entraine la vulnérabilité du système de transport. Des études ont récemment été effectuées sur la vulnérabilité de ces systèmes de contrôle de nouvelle génération, qui démontrent qu'il serait possible de modifier la trajectoire virtuelle d'avions actuellement en vol, voire de retirer un aéronef entièrement des moniteurs de contrôle. Ceci perturbe la capacité du système à fournir aux pilotes des informations précises sur l'emplacement, la vitesse et la direction des autres aéronefs. Bien que de telles interférences n'entraînent pas directement

des accidents car les pilotes conservent un contrôle direct sur le mouvement de leurs avions, leurs impacts potentiels restent considérables [1.20].

V.3.3. Attaques par des organisations criminelles

À ce jour, différents cas d'attaques ont été perpétrés [1.21].
Au Japon, des criminels ont utilisé un générateur électromagnétique pour interférer avec le processeur d'une machine à sous.
A Moscou, le bon fonctionnement d'un central téléphonique a été interrompu par une injection à distance d'une tension dans une ligne téléphonique, ceci a laissé deux cent mille personnes sans service téléphonique pendant toute une journée [1.19].
Un criminel russe a désactivé l'alarme d'une bijouterie en utilisant un générateur de signaux artisanal.

De façon plus générale, en brouillant le système de communication reliant un lieu à surveiller aux services de surveillance à distance, certains malfaiteurs neutralisent aisément la transmission à distance, par radiotéléphonie cellulaire, de signaux d'alarmes.

Durant notre travail, nous nous focalisons sur les brouillages radio susceptibles de perturber le système ferroviaire. Retraçons un bref panorama des attaques qu'a pu subir ce mode de transport.

VI. Attaques du système ferroviaire

Des attaques ont été perpétrées contre le système ferroviaire dès le début de son exploitation [1.22]. Dans ce paragraphe nous en rappelons les moyens et objectifs. Ces problèmes ferroviaires ont tous en commun des dégâts causés sur l'infrastructure et le matériel roulant, mais possèdent des sources et des objectifs différents. De ce fait, on peut les regrouper dans les catégories suivantes :

- Attaques terroristes : ces attaques sont dues à des actions terroristes dans un but religieux politique ou bien idéologique.
- Attaques anti systèmes : ces attaques ne présentent pas de répercussions immédiates. Elles peuvent être considérées en tant que signes de protestation contre le système.
- Attaques liées au chantage : ces attaques ont pour but de prouver la capacité des auteurs à causer des dégâts afin de pouvoir obtenir des avantages.
- Attaques criminelles : ces attaques sont des actions indépendantes, ayant pour but d'assouvir un intérêt personnel.

Associons quelques exemples à chacune de ces catégories.

VI.1. Attaques terroristes

Le 4 août 1974, en Italie, à San Benedetto Val di Sambro, le train de nuit « Italicus » qui reliait Rome à Munich a subi une explosion due à une bombe placée dans un de ses wagons par une organisation néo-fasciste Ordine Nuovo. Cet incident a causé la mort de douze personnes et a fait quarante-huit blessés. Selon un schéma proche, en 1977, à Moscou, une organisation nationaliste arménienne a été inculpée suite à des explosions dont l'une d'elles a touché le métro reliant les gares d'Izmailovskaya et de Pervomaiskaya. A Moscou, le 6 février 2004, les séparatistes tchétchènes on fait exploser une bombe à bord d'un train causant cent vingt blessés et la mort de quarante et une personnes.

En 2002, à Godhra en Inde, le train express Sabarmati, transportant de nombreux pèlerins hindous a subi un freinage d'urgence qui a permis à des individus de monter à bord afin d'y mettre le feu, cinquante-neuf personnes ont été tuées dans l'attaque.

En mars 2004, en Espagne, plusieurs bombes ont explosé dans le train atteignant la gare d'Atocha, cet incident a été très meurtrier, faisant cent quatre-vingt-onze morts et mille huit cents blessés.

L'année suivante, en juillet 2005, lors d'une attaque terroriste contre la capitale britannique, trois bombes ont explosé à bord du métro londonien, causant la mort de cinquante-six personnes et sept cents blessés. Ces attaques ont été revendiquées par Al-Qaïda et les brigades Abou Hafs al-Masri contre le gouvernement britannique.

A la même époque, à Jaunpur en Inde, le train express Shramijvi, voyageant entre Jaunpur et Delhi a subi une explosion causant treize morts et cinquante blessés. Durant l'année qui a suivi, une série de sept attentats a frappé le chemin de fer de banlieue à Mumbai. L'engin explosif a été disposé à l'intérieur d'un four micro-ondes, causant deux cents neuf morts et sept cents blessés. Le mouvement des étudiants islamiques de l'Inde, et le groupe Mujahideen Indien ont été identifiés comme responsables de l'attaque. En 2007, le train Samjhauta express, reliant Delhi à Lahore au Pakistan a explosé, causant la mort de soixante-huit personnes et faisant plus de cinquante blessés.

En France, en 1995 à Paris, entre le 25 juillet et le 17 octobre, une série d'attaques terroristes a frappé la France, trois bouteilles de gaz ont été utilisées contre le système ferroviaire. La première a explosé à la gare Saint-Michel, la seconde à la station Maison Blanche et la troisième entre Musée d'Orsay et Saint-Michel. Huit personnes ont été tuées dans ces attaques et cent vingt-deux blessés, les assaillants étaient des membres du groupe islamique armé (GIA).

VI.2. Attaques anti-système

Contrairement aux attaques terroristes, le nombre d'attaques anti système menaçant le trafic ferroviaire n'est pas aussi important. On en compte seulement deux à ce jour. En 1995, au Japon, du gaz sarin a été diffusé sur plusieurs lignes de métro de Tokyo. Les auteurs ont transporté plusieurs petits sacs de

sarin à bord de cinq trains différents. Treize personnes ont été tuées, cinquante ont été blessés, et plus de mille ont souffert de problèmes de vision temporaires. Les assaillants ont été identifiés comme membres d'Aum Shinrikyo (aujourd'hui connu sous le nom d'Aleph), une secte japonaise.
En 2008, une série coordonnée d'attaques a eu lieu sur des lignes ferroviaires dans le nord de la France. Des barres métalliques ont été attachées aux lignes électriques à haute tension qui alimentent les trains à grande vitesse; lorsque les barres ont été accrochées au passage des locomotives, il y a eu destruction des lignes hautes tension. Un groupe d'anarchistes, le "neuf de Tarnac" composé de jeunes gens issus de la classe moyenne, a été identifié comme l'organisateur de l'attaque. Ces agressions ont provoqué le retard de plus de cent soixante trains à grande vitesse.

A ces attaques anti-systèmes, on peut ajouter les nombreuses actions menées par des organisations pacifiques qui consistent à s'opposer aux transports de certaines matières dangereuses et qui conduisent au dérangement du réseau.

VI.3. Attaques liées au chantage

Jusqu'à ce jour, une seule attaque de cette nature a été identifiée, en 1984, à San Benedetto Val di Sambro, Italie. Elle s'est opérée dans la même zone touchée par la catastrophe du train Italicus en 1974. Des terroristes ont réussi à faire exploser une bombe cachée dans un autocar de passagers lorsque le train était au milieu d'un tunnel, maximisant ainsi les effets de l'explosion et rendant difficile l'intervention de l'équipe d'urgence. Quinze personnes ont été tuées et deux cent soixante-sept ont été blessées. Cette seconde attaque a été attribuée à la mafia italienne, déçue par les dernières lois adoptées par le gouvernement italien. La mafia a décidé d'envoyer "un message" politique par cette attaque.

VI.4. Attaques criminelles

La première attaque criminelle contre le système ferroviaire remonte à 1908 à Bezdany en Russie. Un train de l'Empire russe transportant deux cent mille roubles russes, soit la recette fiscale allant de Varsovie à Saint-Pétersbourg a été attaquée par une bande de vingt personnes décidées à les voler. Deux groupes ont été ciblés, le personnel sur le train et les agents de sécurité en gare. Plusieurs bombes ont été utilisées par les voleurs et un soldat russe a été tué. En 1925, à Lucknow en Inde, le train transportant l'argent du gouvernement britannique a été volé, les assaillants sont montés à bord du train, ont activé le frein d'urgence, maîtrisé les gardes et se sont enfuis avec l'argent.

En 1963, à Ledburn en Angleterre, le train postal roulant de Glasgow à la gare d'Euston à Londres transportait l'équivalent de quarante-trois millions de livres pour être détruits à la banque

d'Angleterre. Pour stopper le train, les voleurs ont interrompu le signal vert d'un feu de circulation en utilisant une batterie portable, et actionné le signal rouge. Une fois le train arrêté, les bandits ont sauté à bord pour détacher la locomotive des deux premières voitures du train et se sont emparés de l'argent.

Cette attaque du train postal, restée très célèbre dans les annales, est très illustrative de ce qu'une modification de la signalisation ferroviaire peut introduire en termes d'arrêt du train « à la demande ».

Dès lors, une question qui se pose est de déterminer si un brouillage électromagnétique de la radio sol-trains pourrait, par exemple développer un tel scénario entrainant l'arrêt du train à une localisation prédéterminée. Etudions ainsi l'impact d'une perte de communication sol-trains.

VII. Conséquences d'une absence de capacité de communication

La radio sol-trains GSM-R possède un rôle important dans le fonctionnement de la signalisation ferroviaire telle qu'implémentée dans ERTMS/ETCS. Des règles ont été édictées afin d'assurer la sécurité de circulation des trains. Une règle importante au regard de notre étude précise que le train doit s'arrêter automatiquement si la communication GSM-R est perdue. Cette règle permet d'assurer que le train ne continue pas à circuler avec des informations de signalisation qui ne sont pas actualisées. [1.23] précise ainsi qu'en France, une perte de connexion d'une durée de 20 secondes sur le réseau TGV entraîne l'arrêt du train. L'immobilisation en voie du train engendrée par cet arrêt d'urgence et causée par les perturbations du lien GSM-R génère des perturbations en cascade sur le trafic ferroviaire, car chaque train est lié aux autres sur le réseau. Cela met en défaut le système ETCS, ce qui force le système de gestion du trafic ERTMS à arrêter l'exploitation pour une durée indéterminée. Après restauration de la connexion, des procédures particulières s'appliquent afin de redémarrer l'ensemble de l'exploitation de la ligne. Les réactions du système présentent donc un impact économique et des conséquences sur la qualité de service du système de transport (QoS).
GSM-R permet de gérer différentes fonctions ferroviaires critiques qui seraient dès lors interrompues en cas de pertes de connexion. Il s'agit de :

L'alerte radio : ce système est spécialement dédié aux conducteurs, il permet de réagir dans des situations dangereuses afin d'alerter les agents au sol ainsi que les trains se trouvant dans une zone proche. Le dispositif exploite un signal sonore qui retentit dans toutes les cabines de conduite des trains de la zone afin de les arrêter. Pour assurer ce service, 95 % des alertes émises doivent être reçues en moins de deux secondes, 99 % en moins de trois secondes [1.23]. A la réception de ce signal, un appel de conférence téléphonique est automatiquement établi entre les conducteurs concernés et les agents au sol responsables de la cellule où se trouve le train émetteur de l'alerte ainsi que dans les cellules voisines. Le système ferroviaire réagit à cette alerte par l'arrêt du train concerné ainsi que

celui des trains circulant sur des lignes proches, dépendantes de celle où s'est produit l'incident. Cet arrêt est établi pour une durée indéterminée. La circulation des trains non concernés par l'alerte n'est pas modifiée.

L'alarme VACMA : le système de Veille Automatique par Contrôle du Maintien de l'Appui couplé avec la radio constitue le système qui veille à ce que le conducteur ne perde pas sa vigilance. En cas de détection de pertes de vigilance, le train est arrêté. Le service radio permet de transmettre les informations et les coordonnées du train au régulateur de la ligne pour faciliter l'arrivée des secours. Pour des raisons de sécurité, le lien de transmission avec le train en circulation doit être maintenu en permanence avant le déclenchement d'un arrêt d'urgence. Pour cela, la durée maximale de perte de connexion est de 20 secondes. Le développement des niveaux de l'ETCS tend à améliorer ce fonctionnement en doublant la couverture radio afin d'assurer au maximum 52 minutes de perte de service par année glissante.

VIII. Description des normes EIRENE

GSM-R implémente certaines spécificités ferroviaires. Afin d'assurer des besoins de mobilité et de couverture radio, le réseau est constitué de cellules assurant une couverture au plus près de l'emprise ferroviaire. Chaque cellule couvre approximativement une longueur de 6 à 7 km selon une couverture latérale voisine de 800 mètres [1.24].

Les spécificités du système GSM-R ont fait l'objet de travaux et notamment ceux du projet EIRENE, qui regroupe les niveaux requis pour une exploitation opérationnelle de GSM-R. Les spécifications EIRENE complètent celles du GSM et de l'ETSI afin de garantir l'interopérabilité du GSM-R entre les différents réseaux ferroviaires européens. Ces spécifications EIRENE, écrites par l'UIC, ont été reprises par la normalisation ferroviaire.

Selon celles-ci, le protocole de communication doit gérer un certain nombre d'exigences. Nous en présentons dans la section suivante certaines, d'intérêt pour ce travail.

VIII.1. Couverture réseau

Les spécifications EIRENE traitent notamment de la couverture réseau, elles permettent de définir les niveaux de couverture comme étant les niveaux de puissance reçus par l'antenne du train disposée à 4 m au-dessus des voies, lorsque ce dernier circule. Une antenne de rayonnement isotrope est utilisée. Les niveaux minimums de puissance requis à l'entrée du récepteur en fonction de la vitesse ou de type de communication sont indiqués dans le tableau suivant [1.25].

Tableau 1.1 Niveaux de couverture.

Système de communication	Vitesse km/h	Niveau de puissance minimum requis
Voix et donnée critiques	-	-98 dBm
Lignes avec ETCS niveaux 2/3	> 220	-95 dBm
Lignes avec ETCS niveaux 2/3	> 280	-92 dBm
Lignes avec ETCS niveaux 2/3	220-280	entre -95 dBm et -92 dBm

Comme on peut le constater, pour des vitesses élevées et pour les lignes exploitant les niveaux 2 et 3 du système ETCS, -95 dBm s'avère être le niveau de puissance minimum requis afin de maintenir la communication. Ce niveau de puissance reçu est faible. De ce fait, il devient probablement possible de générer un signal en provenance d'une source de brouillage disposée dans l'environnement proche de l'antenne de réception GSM-R pouvant atteindre, voire dépasser cette valeur.

VIII.2. Handover

Le handover représente l'opération permettant la transition de la communication depuis une cellule vers la suivante. Il s'effectue sans interrompre la communication mais en perdant les informations transmises durant la période de quelques centaines de millisecondes de basculement d'une cellule à l'autre. Afin d'assurer cette opération, les spécifications EIRENE stipulent les exigences regroupées dans le tableau 1.2 [1.26].

Tableau 1.2 Handover

Spécifications du Handover	
Taux de réussite	99.8 %
Temps d'exécution	± 300 ms
Distance de chevauchement	600 m

Le handover est décidé par le BSC et commandé par les BTS aux mobiles. Afin de limiter l'impact de l'interruption de communication liée au handover, certains opérateurs utilisent les équipements de CABRADIO de tête et de queue du train en basculant de l'un à l'autre pour pallier la brève période de perte de données. Un brouillage de la communication durant cette phase pourrait perturber, voire faire échouer cette opération de basculement d'une cellule à la suivante.

VIII.3. Qualité de service

Il existe différentes exigences qui ont été mises en place afin de définir des valeurs requises en termes de QoS. Le tableau 1.3 précise les temps d'établissement des communications en fonction du type d'appel [1.26].

Tableau 1.3 Durée d'établissement d'appels pour les différentes classes.

Class	Type d'appel	Durée d'établissement
Class I	Appel d'urgence ferroviaire	$\leq$ 1s
Class la	Appel de groupe urgent mobile-à-mobile	$\leq$ 2s
Class II	Toute opération couverte par le handover	< 5s
Class III	Tous les appels de priorité faible	< 10 s

Le temps d'établissement correspond à la durée entre la requête d'établissement et l'indication du succès de la connexion. Tout délai supérieur au temps précisé est considéré comme une erreur de connexion et correspond à une défaillance du système. Ces éléments sont récapitulés dans le tableau 1.4 [1.24].

Tableau 1.4 Paramètres de QoS du système

Paramètres QOS	valeurs
Délai d'établissement de la connexion pour un appel d'origine	< 8.5 s (95%), $\leq$ 10 s (100%)
Taux d'erreur pour l'établissement des connexions	$< 10^{-2}$
Temps de transfert maximum (end-to-end) de 30 bits de données	$\leq$ 0.5 s (99%)
Taux de perte de connexion	$\leq 10^{-2}$ / h
Période de transmission d'interférences	< 0.8 s (95%), < 1 s (99%)
Période de retransmission de la donnée erronée	> 20 s (95%), > 7 s (99%)
Délai d'enregistrement sur le réseau	$\leq$ 30 s (95%), $\leq$ 35 s (99%), $\leq$ 40 s (100%)
Taux d'erreur binaire BER	$< 10^{-4}$ sur 90% du temps
Temps sans connexion	< 300 ms
Probabilité de perte de la connexion	$<10^{-4}$
Vitesse de transmission	> 2.4 kbps
Probabilité d'erreur d'appel	$< 10^{-3}$

Ce tableau établit un récapitulatif des exigences requises pour une bonne transmission. Le non-respect de ces valeurs signifie l'apparition d'un défaut. Le système admet cependant une certaine probabilité d'échec d'appel de perte de connexion, ainsi qu'une probabilité d'erreur binaire de la communication tout en assurant des délais de transfert et de retransmission corrects.

Lorsque ces valeurs attendues et mesurées lors de la recette de la ligne ne sont plus respectées, ceci peut vouloir indiquer la présence de perturbations, dont des brouillages intentionnels.

VIII.4. Niveau de puissance

Différentes études de planification du réseau cellulaire sont menées afin d'optimiser les niveaux de puissance présents le long de l'infrastructure ferroviaire. Les BTS sont disposées le long des voies de manière à assurer les communications sur plus de 95 % de la zone de couverture. Pendant son trajet et en fonction des positions des stations de base rencontrées sur son itinéraire, la puissance du signal reçu par l'antenne train ou par celle de l'antenne BTS varie entre -95 et -20 dBm [1.24].
La figure 1.6 fournit un enregistrement de puissance reçue à bord d'un train lors de son déplacement. Dans ce cas particulier de couverture radioélectrique, à proximité de la BTS, la puissance croît jusque -30 dBm au point kilométrique repéré par la valeur 9.10. Celle-ci décroît de façon dissymétrique de part et d'autre de ce maximum. Cette dissymétrie est liée à l'utilisation d'une antenne directive de type Yagi présentant un rapport avant arrière significatif. La valeur de puissance reçue reste au-dessus de -95 dBm jusqu'au point kilométrique repéré par la valeur 10.80, soit 1.7 km plus loin. Des baisses ponctuelles du niveau de réception en dessous de -95 dBm peuvent être tolérées dès lors qu'elles ne concernent pas plus de 5% du temps et de l'espace.

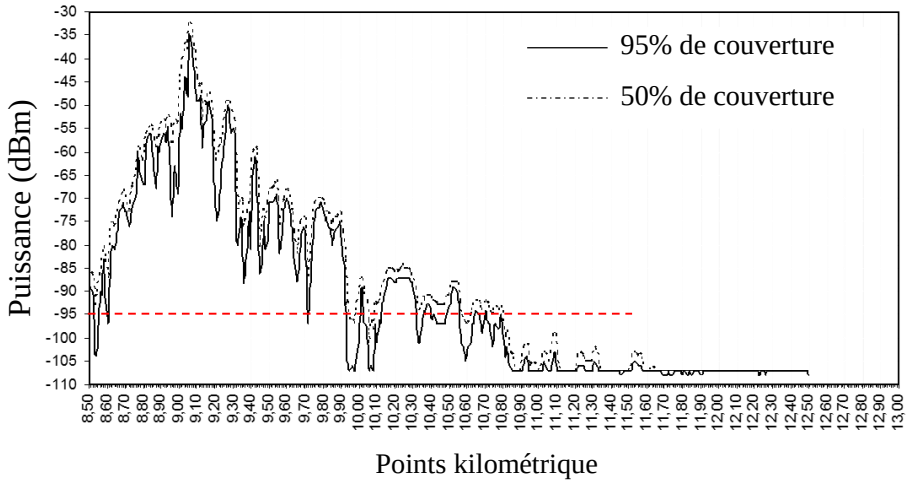


Figure 1.6. Puissance reçue sur un canal GSM-R en fonction de la distance à la BTS (source SNCF).

IX. Conclusion du chapitre 1

Dans ce premier chapitre du mémoire, nous avons souhaité présenter successivement les objectifs de la thèse puis positionner ce travail dans son contexte.

L'objectif de notre travail consiste à détecter rapidement des signaux de brouillage intentionnels perturbant une liaison radio nécessaire au bon fonctionnement du contrôle commande ferroviaire ainsi qu'à en évaluer l'impact, en fonction de ses caractéristiques.

Pour cette entrée en matière, nous avons tout d'abord rappelé ce que sont les infrastructures critiques ainsi que leurs rôles dans l'activité économique des états.

Parmi ces infrastructures critiques, celle de transport ferroviaire possède des caractéristiques particulières, en lien notamment avec son déploiement géographique considérable, son rôle majeur pour la mobilité des citoyens et des biens, et sa nécessaire interopérabilité inter états.

Nous avons ensuite rappelé les composantes de cette interopérabilité ferroviaire en nous focalisant sur la radio sol-trains qui constitue l'objet d'étude de ce travail de thèse. Cette radio-sol-trains pourrait ainsi être brouillée par des signaux radio intentionnels opérant dans les bandes allouées.

Nous avons poursuivi ce premier chapitre en présentant quelques systèmes de brouillage radioélectriques intentionnels existants puis, en proposant une classification des attaques déjà subies par le système ferroviaire ainsi qu'un bref historique des plus représentatives.

La conséquence d'un brouillage radio pouvant être la perte de la liaison radio sol-trains, nous avons envisagé ce cas de figure et ses conséquences sur l'exploitation.

La radio sol-trains interopérable obéissant à des spécifications précises, nous avons rappelé les normes EIRENE les plus pertinentes au vu de cette étude.

Ces éléments étant rappelés, situés et établis, nous proposons dans le chapitre 2 de nous focaliser sur ces problèmes d'interférences et sur les brouilleurs qui les génèrent. Partant d'une architecture de radio sol-trains GSM-R typique, nous analyserons a priori l'impact de la présence de brouilleurs au sol ou en embarqué. Des mesures préliminaires menées sur un banc de test permettront de cerner les paramètres des signaux de brouillage significatifs et d'évaluer quantitativement leurs impacts dans quelques cas de figure réalistes de communication. Partant de ce cadre de travail précisé, nous introduirons finalement dans ce chapitre 2, le modèle de chaîne de transmission qui nous servira par la suite dans notre étude.

X. Références du chapitre 1

[1.1] I. Cochran, «Vulnérabilité au changement climatique et possibilités d'adaptation», 2009.
[1.2] A. Baina, Contrôle d'accès pour les grandes infrastructures critiques. Application au réseau d'énergie électrique, Toulouse: Doctorat de l'Université de Toulouse, 2009.
[1.3] T. G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, John Wiley & Sons, 2006.
[1.4] R. Pleikys, radio jamming in soviet union. antentop, 2006.
[1.5] P. Delacroix, J. Falaize et H. Girod-Eymer, 150 ans de trains de voyageurs en France, La Vie Du Rail, 1983.
[1.6] «ERTMS pour un trafic ferroviaire fluide et sûr» Brochure publiée par: Commission européenne, DG Énergie et transports, 2005.
[1.7] Journal officiel des communautés Européennes, «Directive 96/48/CE du conseil relative à l'intéroperabilité du système ferroviaire transeuropéen à grande vitesse», 1999.
[1.8] [En ligne]. Available: http://ertms.uic.asso.fr/2_etcs.html. Dernier accès, mai 2014.
[1.9] «From trucks to trains how ertms helps making rail freight more competitive» Bruxelles, 2010.
[1.10] D. De Neef, «Le système ERTMS / ETCS», 2008. [En ligne]. Available: http://www.belrail.be/F/infrastructure/signalisation/index.php?page=ertms. Dernier accès avril 2014.
[1.11] The European Commission's Directorate-General for Energy and Transport, «ERTMS – Delivering Flexible and Reliable Rail Traffic Office for Official Publications of the European Communities», 2006.
[1.12] UNISIG, «Subset-037 ERTMS/ETCS - Class 1 Euroradio Functional Interface Specifications, Issue 2.3.0», 2005.
[1.13] ETSI TR 102 300-2, «Terrestrial Trunked Radio Part 2: Radio channels, network protocols and service performance», 2013.
[1.14] «Catalogue of public domain devices, their assemblies and classification in terms of EM threat Submission» Deliverable D1.1 , projet SECRET, 2013.
[1.15] Agence Nationale des fréquences, «étude de la cce sur l'ingénierie des sites radioélectriques», 2001.
[1.16] A. Moabit, «Protection d'infrastructures critiques, concept de base de protection» Berlin, 2006.
[1.17] [En ligne]. Available: http://fr.wikipedia.org/wiki/Brouillage radio. Dernier accès, avril 2014.
[1.18] «Satellite and internet jamming rises as broadcast industry seek to uphold UN Article 19» [En ligne]. Available: http://www.bbc.co.uk/mediacentre/latestnews/2012/201112wsjammingconference.html. Dernier accès, janvier 2014.
[1.19] G. Lugrin, «La vulnérabilité des réseaux électriques en cas d'attaques électromagnétiques,» 2013.
[1.20] A. Becker, «Interference technology,» [En ligne]. Available: http://www.interferencetechnology.com/next-gen-flight-control-system-vulnerable-jamming-attacks/. Dernier accès janvier 2014.
[1.21] F. Sabath, «Threat of electromagnetic terrorism leassons learned from documented IEMI attacks,» EuroEm, p. 17, juillet 2012.
[1.22] A. Zanassi, «Attaques du système ferroviaire», projet SECRET, 2012.
[1.23] J. Cellmer, «Le réseau GSM-R de RFF L'automatisation des transports publics,» REE, n° 13, pp. 45-52, 2012.
[1.24] UNISIG, «Subset-093 ERTMS/ETCS Class 1 Euroradio Functional Interface Specifications, Issue 2.3.0», 2005.
[1.25] ETSI TR 103 134 V1.1.1, «Railway Telecommunications (RT) GSM-R in support of EC Mandate M/486 EN on Urban Rail», 2013.
[1.26] UIC Project EIRENE, «Functional Requirements Specification», 2006.

Chapitre 2 : Brouillages électromagnétiques et impacts sur la communication GSM-R

SOMMAIRE

I. Interférences et radio communication GSM-R

Nous entamons ce deuxième chapitre par un rappel portant sur la description de quelques sources de perturbations électromagnétiques que l'on peut trouver dans l'environnement ferroviaire.

I.1. Interférences d'origines naturelles et industrielles

Les interférences électromagnétiques représentent l'une des premières causes perturbant le lien entre les stations de base et les stations mobiles GSM-R à bord du train. Ces interférences sont définies comme toute perturbation qui dégrade les communications ou interrompt de manière répétitive un service de télécommunication. Certaines interférences peuvent être d'origines naturelles (foudre, décharges orageuses, décharges électrostatiques…). D'autres interférences sont d'origines industrielles. L'ensemble du système ferroviaire, matériel roulant, infrastructure ferroviaire et équipements assurant l'alimentation en énergie électrique (caténaire, pantographe) peut en effet générer de fortes perturbations électromagnétiques par lui-même.
Différentes sources de perturbations en résultent. Une première catégorie correspond à celles en mesure de générer des signaux à des fréquences allant jusqu'à quelques dizaines de kHz. Il s'agit plus particulièrement :

Des harmoniques de courant et de tension dus aux redresseurs en sous station électrique ;
De l'électronique de puissance montée sur véhicule ;
De l'amplitude du courant de traction ;
Des transitoires dans le circuit d'alimentation ;
De l'interaction entre véhicules et sous-stations ;
Des courants de signalisation ;
Des distorsions du courant de traction.

Une seconde catégorie peut produire de l'énergie à des fréquences plus élevées. Ainsi, des signaux de perturbation à des fréquences proches de 1 GHz ont été mesurés et analysés [2.1]. Il s'agit des perturbations associées aux arcs électriques générés par le contact glissant entre le fil de caténaire et le pantographe. Ces arcs proviennent de l'imperfection du contact et sont souvent accentués pour les trains qui possèdent plusieurs pantographes connectés à la caténaire.
Ces perturbations d'origines naturelles et industrielles sont non-intentionnelles. Bien qu'elles peuvent affecter la qualité des communications GSM-R, elles ne font pas l'objet de notre étude. Notre travail traite spécifiquement des perturbations électromagnétiques intentionnelles pouvant entrainer des perturbations de la communication sol-trains.

I.2. Brouillages externes IEMI

Les interférences électromagnétiques intentionnelles portent généralement le nom d'IEMI (Intentional ElectroMagnetic Interference). Ce type d'interférences présente une menace particulière car elles peuvent être dimensionnées à la demande et de ce fait présenter des caractéristiques plus efficaces que les interférences d'origines naturelles et industrielles pour brouiller les systèmes.

Les normes internationales ont décrit les attaques IEMI comme étant "toute source d'énergie électromagnétique malicieuse introduisant un bruit ou un signal qui viendrait perturber ou endommager le système à des fins criminelles ou bien terroristes."

Différentes sources d'attaques intentionnelles ont été recensées à ce jour.

Les brouilleurs militaires sont des dispositifs conçus et dimensionnés de telle manière à dégrader ou bien à détruire le fonctionnement d'un système au sol ou bien aérien grâce à leurs portées significatives, liées à leur forte puissance. Il s'agit en particulier des armes micro-ondes de forte puissance. Ces armes sont capables de générer, sur des portées de quelques kilomètres, des champs électromagnétiques supérieurs ou égaux à ceux produits par une explosion nucléaire en haute altitude (IEM-HA). Elles peuvent avoir une fréquence de répétitions atteignant quelques kHz [2.2].

D'autres dispositifs de brouillages, destinés à un usage non militaire sont visibles notamment sur internet. Ils peuvent être utilisés de manière plus facile, ces dispositifs étant d'encombrement réduit et de ce fait discrets. Leur efficacité est moindre que les dispositifs militaires mais ils ciblent certaines bandes de fréquences radio largement employées. Les puissances radio fréquences délivrées sont plus faibles et les portées sont réduites en proportion.

Nous étudions plus particulièrement cette gamme de perturbateurs et décrivons maintenant le fonctionnement de certains de ces équipements.

❖ Brouilleurs GSM-R

Il existe différents dispositifs de brouillage des systèmes de communication. Ces dispositifs sont actifs sur de larges gammes de fréquence et sont en mesure de perturber différents systèmes de radio communication et de radio navigation couvrant en particulier les bandes de fréquence attribuées au GSM-R. Ces brouilleurs peuvent délivrer aux récepteurs des niveaux de puissance comparables ou supérieurs à ceux en provenance des émetteurs souhaités. La figure 2.1 illustre un brouilleur particulier de faible encombrement disposé à proximité d'un train. Le brouilleur possède quatre antennes distinctes permettant des opérations dans quatre bandes UHF et SHF de fréquences différentes.

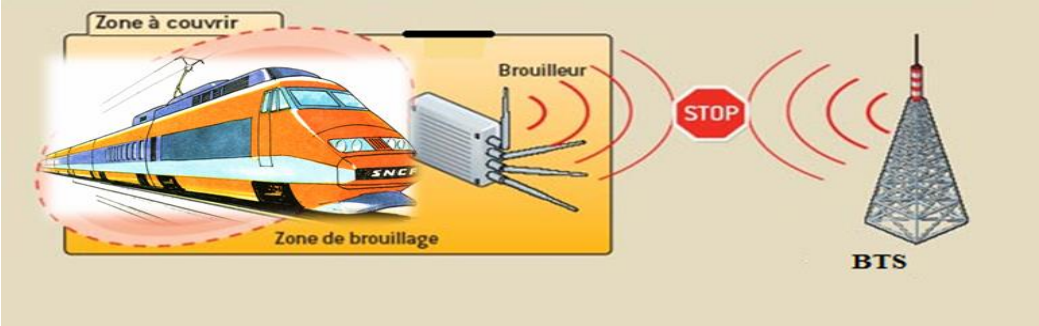


Figure 2.1 Brouilleur GSM-R.

Plus généralement, une analyse des systèmes de brouillage a permis de les répertorier selon leurs effets et leurs caractéristiques principales en cinq classes différentes notées A à E [2.3].

Type "A" brouilleurs

Ce premier type de brouilleur, illustré sur la figure 2.1 précédente, est constitué de plusieurs oscillateurs indépendants balayant rapidement une gamme de fréquence et transmettant de ce fait un signal de brouillage capable de perturber de nombreux services. Ces appareils empêchent les dispositifs radio-mobiles aux alentours de recevoir et de développer un dialogue efficace avec les stations de base ou d'autres équipements normalement à portée radio.

Type "B" brouilleurs intelligents

Ce type de brouilleurs ne transmet pas de signal d'interférences. Ces équipements de brouillage possèdent un numéro d'identification reconnu par les stations de bases. Ils fonctionnent tels des détecteurs. Lorsqu'ils sont situés à proximité de dispositifs radio-mobiles, ils empêchent l'établissement des autorisations d'appels avec ces stations de base.

En captant les signaux émanant de la station de base et en détectant les mobiles, ces systèmes préviennent les stations de base que le mobile ne possède par exemple pas d'autorisation de connexion.

Lorsque le mobile signale se trouver en situation d'urgence, l'effet du brouilleur peut être inhibé et la connexion être rétablie.

Type "C" balises de brouillage intelligent

Ces dispositifs ne transmettent pas non plus de signaux d'interférence sur le canal de communication. Le brouilleur fonctionne comme une balise permettant de désactiver les opérations et les sonneries du mobile à l'intérieur de la zone de couverture de celle-ci. Les utilisateurs préenregistrés pour les appels

d'urgence utilisent une séquence spécifique afin d'inhiber le brouillage. A la sortie de la zone de couverture du brouilleur, le mobile retrouve un fonctionnement nominal.

❖ ***Type "D" récepteurs directs***

Ces dispositifs de brouillage fonctionnent à l'instar d'une station de base portable et interagissent avec les mobiles. Le brouilleur fonctionne en mode réception et sélectionne certains mobiles afin de bloquer les communications s'ils se trouvent à proximité. Cette technique de brouillage sélectif nécessite un récepteur pour détecter les mobiles à proximité. L'avantage d'une telle sélectivité est de minimiser la pollution électromagnétique et de ne mettre en jeu que des puissances réduites.
Le signal émis par la station portable de brouillage essaye d'établir le lien avec la station de base simultanément et en utilisant les mêmes canaux et slot time que le mobile. La technique mise en œuvre consiste donc à empêcher toute tentative d'établissement de communication avec la station de base recherchée.

Type "E" bouclier EMI-brouilleur passif

Cette technique supprime les signaux et les interférences électromagnétiques en générant l'équivalent d'une cage de Faraday afin d'atténuer ou de bloquer les rayonnements EM entrants ou sortants du volume couvert. Il serait possible de mettre en œuvre cette technique dans les nouvelles architectures des bâtiments pour concevoir des pièces "calme". Les appels d'urgence sont bloqués, sauf s'il est possible de les décoder et de reconnaitre leur caractère d'urgence, et cela à travers un câble coaxial rayonnant disposé dans la pièce.

Une étude effectuée par l'Agence Nationale des Fréquences (ANFR) a permis de recenser les appareils de brouillage actuellement utilisés et facilement disponibles sur le marché [2.4]. Un dispositif de détection et de blocage des téléphones mobiles peut ainsi émettre une puissance allant jusque 30 W. Ce dispositif permet le renvoi systématique des appels sur messagerie. Il représente un système puissant car il atteint des niveaux de puissance équivalents à ceux d'une BTS. Un second système de brouillage large bande affectant la signalisation d'appel quant à lui, émet une puissance d'environ 300 mW, durant quelques secondes. Cette configuration reste suffisante pour empêcher le mobile de répondre à la signalisation. Dans ce document, une classification des systèmes de brouillage en deux catégories distinctes apparait [2.4] :

- Les brouilleurs émettant du bruit en continu et couvrant un large spectre.

– Les systèmes à filtres impliquant une analyse du signal et du protocole de communication utilisé qui envoient un message forçant une fin de communication pendant une phase d'établissement d'appel.

Ces deux catégories correspondent respectivement aux catégories A et D précédentes. Durant notre travail nous nous focalisons sur les brouilleurs de type A, les plus rencontrés. Ce type de dispositif émet continuellement du bruit couvrant une large bande de spectre, ayant des caractéristiques fréquentielles et temporelles que nous détaillons dans la section suivante.

II. Brouilleurs électromagnétiques

Une classification de ces brouilleurs selon leur niveau de complexité a également été établie afin de les différentier en fonction de leurs formes d'onde (puissance, durée…). Celle-ci apparaît figure 2.2 [2.5].

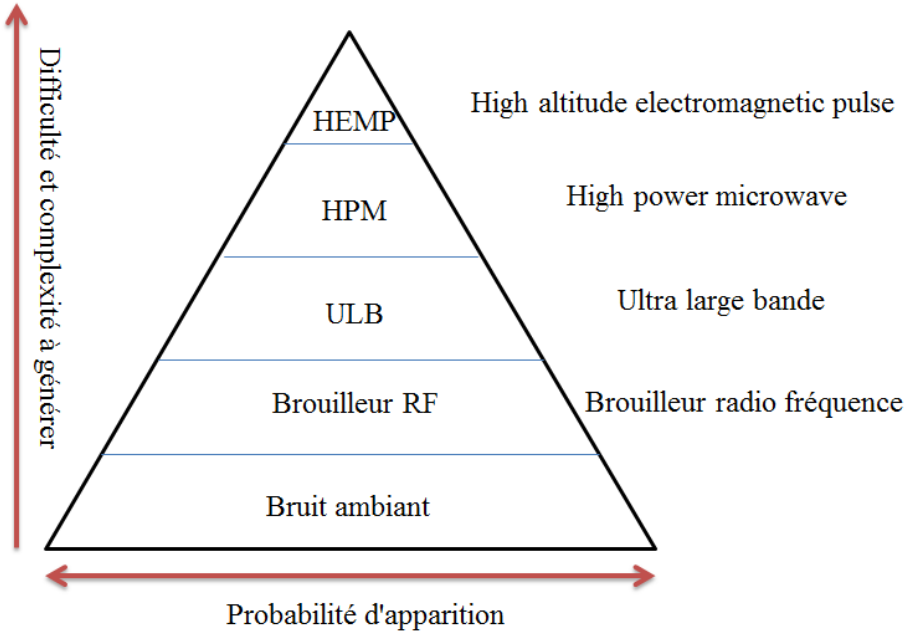


Figure 2.2 Classification des attaques EM.

La capacité de génération d'une impulsion à haute énergie est rapidement limitée par la technologie. Il devient ainsi plus probable de considérer un système soumis à un brouillage radiofréquence ciblé dans une bande de fréquence limitée qu'à une perturbation haute puissance HPM ou Ultra Large Bande.
Différentes études ont été menées à ce jour afin de traiter les attaques électromagnétiques perpétrées contre le système GSM-R de manière intentionnelle ou non [2.5]. GSM-R utilise un protocole standard public similaire à celui employé par le GSM. Il devient donc aisé de s'informer sur ses paramètres et ses spécificités et de pouvoir en déduire une source de perturbation efficace en se focalisant sur certaines de ses caractéristiques publiées. On peut donc concevoir un brouilleur radiofréquence

bas-coût, dimensionné de manière à obtenir l'impact désiré visant ce protocole particulier et ses bandes allouées.

Dans une nouvelle section, nous proposons une description des formes d'onde qui sont considérées en mesure de perturber la signalisation ferroviaire. Ces formes d'ondes, pouvant être générées à l'aide de composants sur l'étagère, sont classées en fonction de leurs caractéristiques temporelles et fréquentielles.

II.1. Brouilleurs ultra large bande

Ces brouilleurs sont réalisés à l'aide de générateurs de signaux ultra large bande. Ces sources produisent des impulsions transitoires d'une durée très brève ayant fréquemment un temps de montée aussi faible que 100 ps [2.5]. Cette impulsion brève génère une occupation spectrale très étendue couvrant une gamme comprise entre quelques mégahertz et plusieurs gigahertz. Par définition, un signal est ULB s'il satisfait les critères suivants :

- Une largeur de bande supérieure ou égale à 500 MHz ;
- une largeur de bande relative LBR (Fractional Bandwidth) à -10 dB supérieure ou égale à 0.25 fois la fréquence centrale, comme le montre la figure 2.3.
-

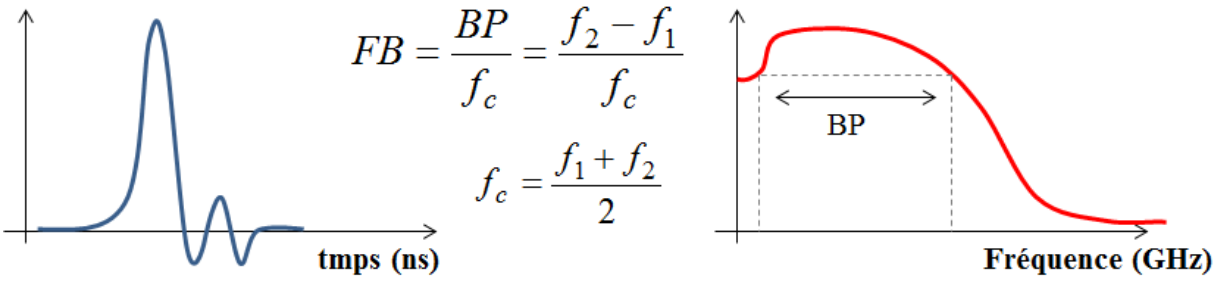


Figure 2.3 Signal ULB.

La figure 2.4 présente ainsi une forme d'onde ULB dans sa représentation en fonction du temps puis, dans le domaine des fréquences via sa densité spectrale de puissance (dsp), générée à partir des équations II.1 et II.2 suivantes :

$$g(t) = A(e^{-\alpha t} - e^{-\beta t}).u(t) \quad \text{(II.1)}$$

$$|G(f)| = \frac{A(\beta - \alpha)}{(\alpha + jw)(\beta + jw)} \quad \text{(II.2)}$$

Dans ces expressions A représente l'amplitude maximale, α et β, sont respectivement la largeur à mi-hauteur et le temps de montée, $u(t)$ correspond à l'échelon unitaire et w à la pulsation.

D'une durée très brève, l'énergie associée à l'impulsion est donc limitée. Pour cette raison, il est difficile de créer des dégradations permanentes avec ce type de perturbation. Néanmoins, celle-ci couvre une large gamme de fréquence et une augmentation de son amplitude lui permettrait de devenir une source de dégradation permanente du système.

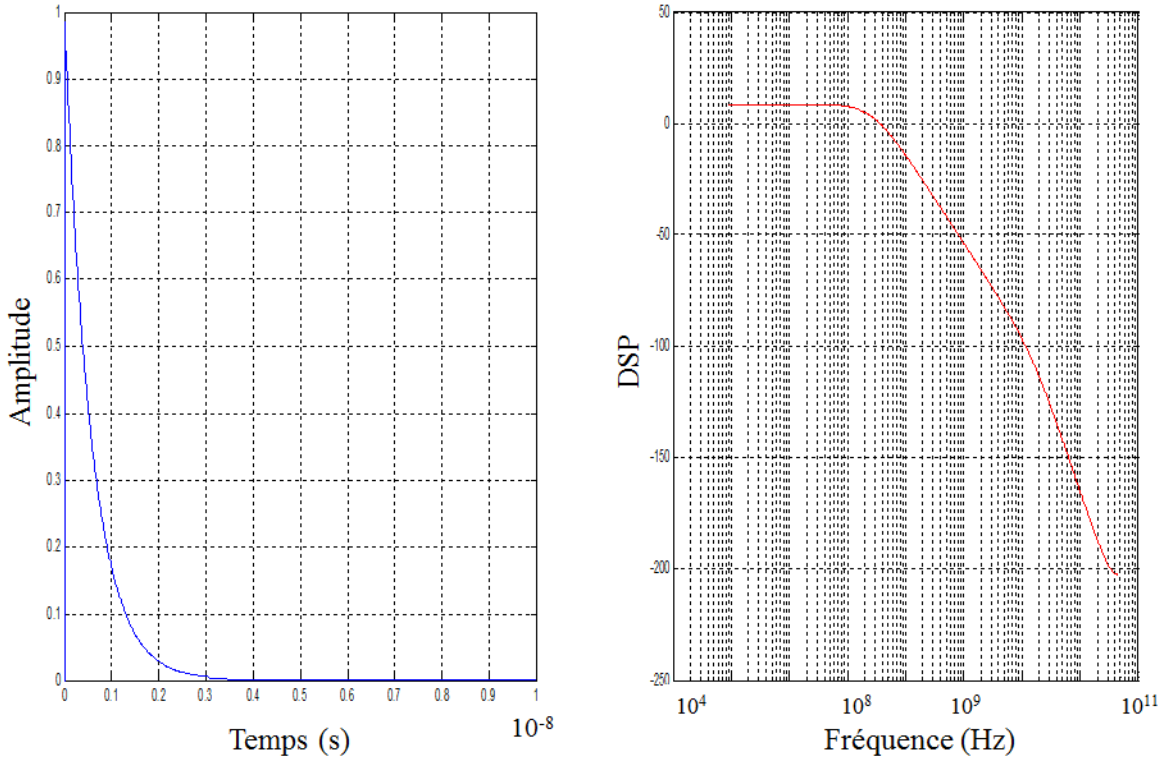


Figure 2.4 Représentations temporelles et fréquentielles d'un signal ULB.

Grâce à cette large bande de fréquences occupée la faisant ressembler à une augmentation du plancher de bruit, ces signaux ULB sont difficilement détectables par un récepteur non spécialisé.

II.2. Brouilleurs à bande étroite

Ces formes d'onde produisent un signal dont la largeur de bande relative est inférieure à 1.01. Contrairement aux signaux ULB, ils délivrent leur puissance dans une bande de fréquence étroite. Toute l'énergie du signal est concentrée dans cette gamme de fréquence. Leur impact est alors majeur si ces fréquences couvrent celles utilisées par le système.

La figure 2.5 illustre un tel brouillage à bande étroite. Un oscillateur à fréquence variable balaye rapidement et répétitivement, en quelques microsecondes, une gamme de fréquence couvrant quelques MHz, centrée sur une fréquence, par exemple voisine de 900 MHz. Les représentations temporelles et fréquentielles des signaux générés sont données par les équations II.3 et II.4 suivantes ou w_0 représente la pulsation centrale et A son amplitude.

$$g(t) = A\sin(w_0 t).u(t) \tag{II.3}$$

$$|G(f)| = Aj\pi(\delta(w+w_0) - \delta(w-w_0)) \tag{II.4}$$

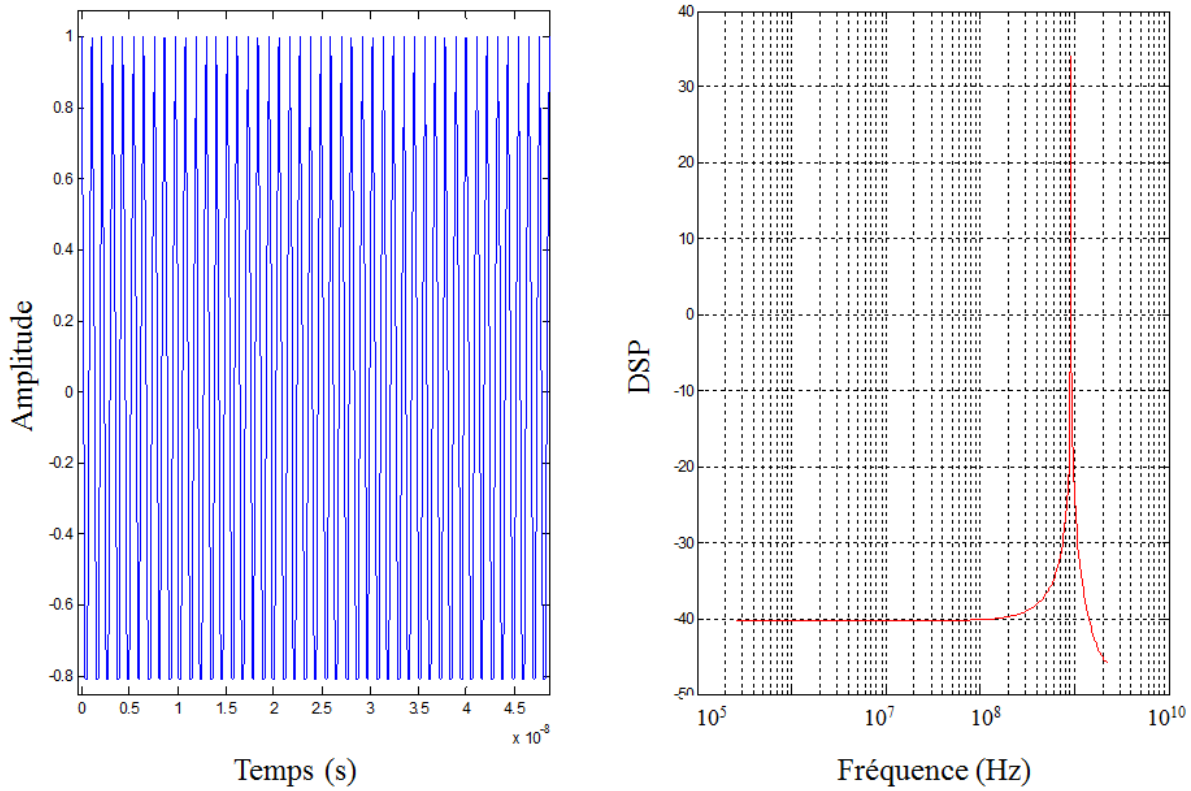


Figure 2.5 Représentations temporelles et fréquentielles d'un signal à bande étroite.

II.3. Brouilleurs à bande large par sinusoïde amortie

Les formes d'onde sinusoïdales amorties allient simultanément certaines caractéristiques de signaux ULB et de signaux sinusoïdaux entretenus. Ils présentent un temps de montée court, sont centrés sur une bande de fréquence déterminée et possèdent une énergie associée significative.

Les représentations temporelles et fréquentielles de ces signaux sont données par les équations suivantes II.4 et II.5, où τ constitue le facteur d'amortissement.

$$g(t) = Ae^{-\pi t}\sin(w_0 t).u(t) \tag{II.5}$$

$$|G(f)| = \frac{Aw_0}{\sqrt{(\tau^2 + {w_0}^2 - w^2)^2 + 4\tau^2 w^2}} \tag{II.6}$$

Ce type de formes d'onde représente un bon compromis pouvant couvrir toutes les fréquences allouées à un système radio et une énergie maximale concentrée autour de la fréquence centrale. Ce type

d'attaque représente des perturbations transitoires. La figure 2.6, représente l'évolution dans le temps d'un signal sinusoïdal amorti, centré à 900 MHz dont, le facteur d'amortissement τ est de 0.1 µs.

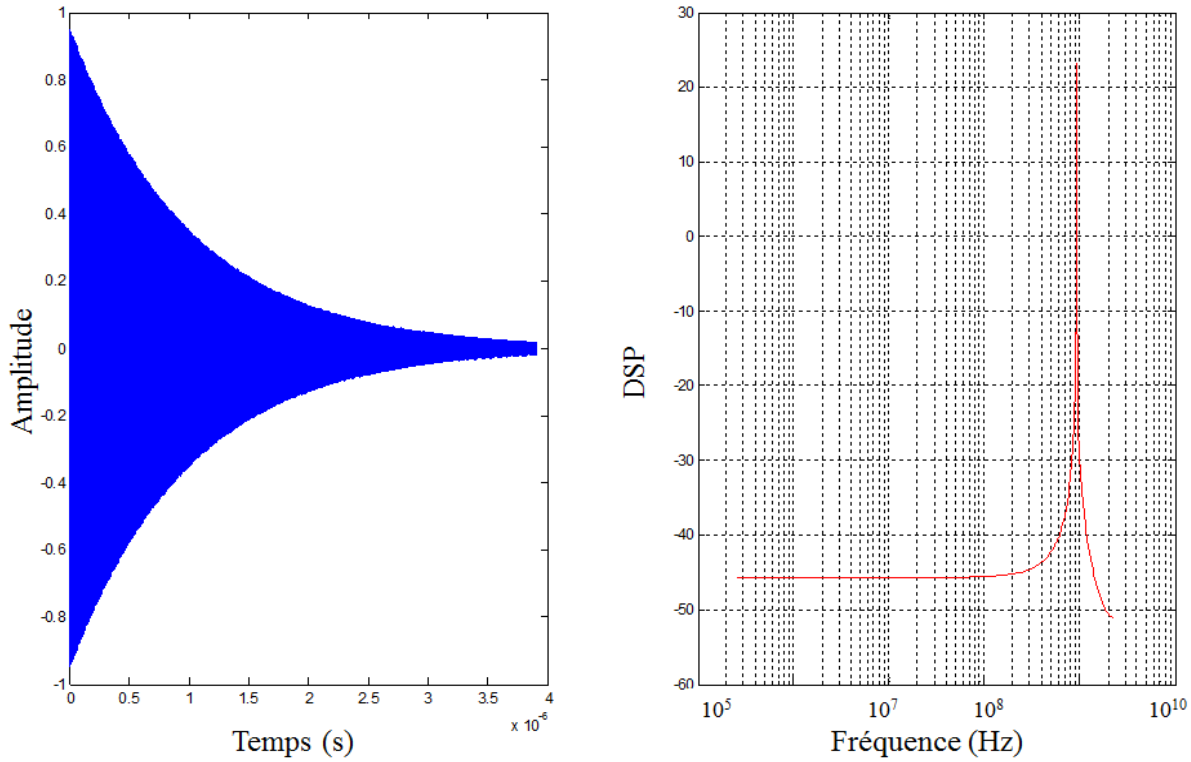


Figure 2.6 Représentations temporelles et fréquentielles d'un signal sinusoïdal amorti.

Cette figure illustre la combinaison de certaines caractéristiques de signaux ULB et de signaux sinusoïdaux entretenus mentionnée précédemment.

La figure 2.7, [2.6] présente une synthèse des densités spectrale d'énergie des différentes sources de perturbations que nous venons de rappeler, regroupées en fonction de leur pulsation *w*.
Le signal HEMP représente une explosion nucléaire à haute altitude. A échelle réduite, une impulsion électromagnétique peut être créée en utilisant des dispositifs non-nucléaires appelée micro-ondes de haute puissance (HPM) qui font partie des signaux ULB. Dans la même gamme, nous notons les dispositifs HIRF, qui délivre une énergie radiofréquence en champ fort.

Aux fréquences GSM-R les signaux large bande et bande étroite s'avèrent de ce fait les plus préoccupants.

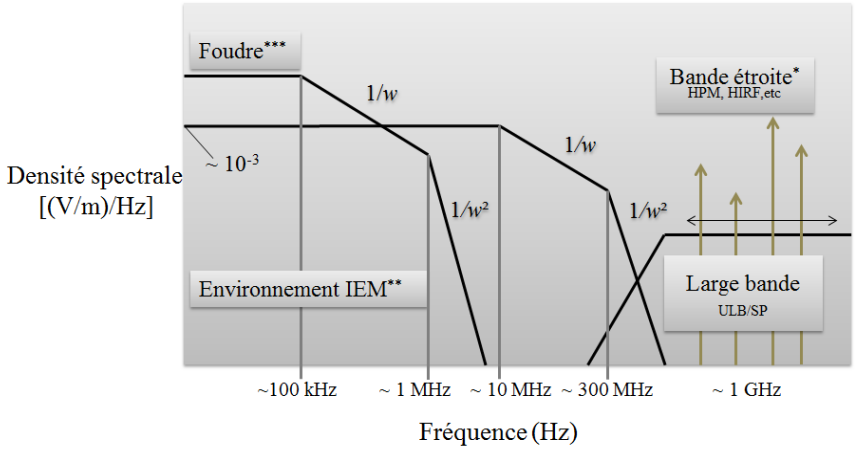


Figure 2.7 Comparaison spectrale des environnements électromagnétiques.

Apres avoir passé en revue ces différentes formes d'ondes de brouillage, nous présentons dans la section suivante les spécificités de l'architecture de communication GSM-R d'intérêt pour cette étude.

III. Architecture de communication GSM-R

Le contrôle à distance d'un grand nombre de trains à grande vitesse exige un transfert de données sans erreur et une transmission radio fiable disposant des ressources radio nécessaires. GSM-R est conçu pour permettre son exploitation y compris dans des conditions de propagation difficiles, dans les forêts denses, les tunnels, les tranchées profondes.

Une architecture simplifiée du système GSM-R est illustrée figure 2.8. Nous sommes en présence d'un réseau radio-mobile cellulaire dont une spécificité est de posséder des cellules disposées longitudinalement le long de la voie. Une couverture surfacique globale n'est en effet pas nécessaire comme ce serait le cas d'un réseau de radiotéléphonie cellulaire opéré par un opérateur de radiotéléphonie. Les BTS sont associées par deux pour couvrir deux cellules qui se chevauchent et placées dans une structure multi-boucle avec quatre BTS par BSC assurant la nécessaire redondance [2.7]. Le réseau reste cependant similaire à un réseau cellulaire mobile public bien que conçu pour répondre aux spécifications ferroviaires.

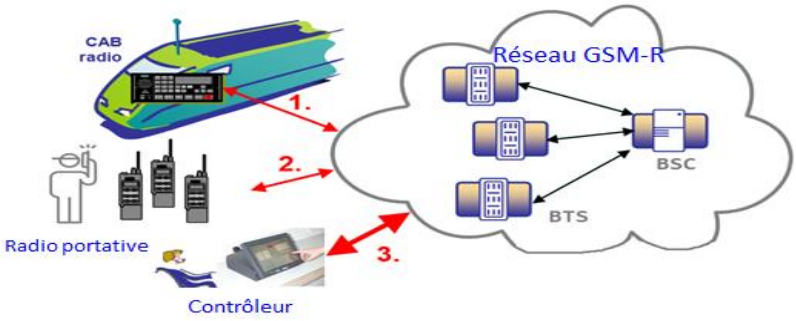


Figure 2.8 Architecture GSM-R.

Pour la planification du réseau, le niveau de couverture est défini en fonction de la superficie et de l'environnement afin que les critères des spécifications EIRENE soient respectés. Le niveau de couverture doit être d'au moins 95 % du temps, sur plus de 95 % de la zone de couverture.

La disposition des cellules des stations de base GSM-R détermine la couverture radio. Ainsi que nous l'avons vu précédemment, l'alignement des cellules est principalement linéaire, le long d'un axe ainsi que l'illustre la figure 2.9.

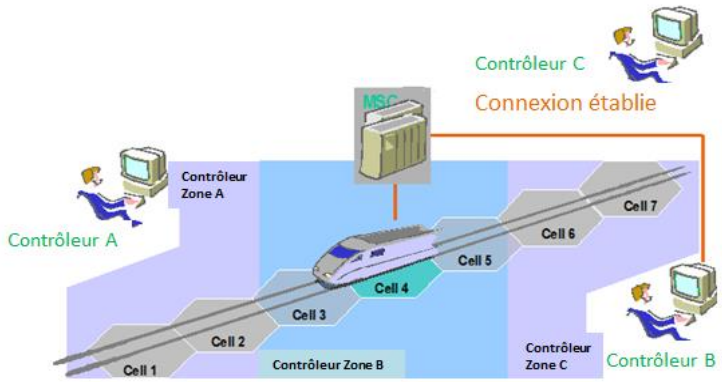


Figure 2.9 Implantation des cellules en GSM-R.

Néanmoins, une couverture de zones adjacentes à la voie peut exiger des cellules spécifiques supplémentaires afin d'assurer une couverture adéquate de l'ensemble de l'emprise ferroviaire.

Les contrôleurs et conducteurs de trains exploitent des terminaux fixes, le personnel de voie utilise des téléphones portable robustes à des fins d'exploitation. A usage général, des combinés sont remis à tous les autres membres du personnel.

Comme pour le GSM standard, l'écart entre un canal montant et un canal descendant est toujours de 50 MHz et chaque canal de fréquence utilisé pour une communication possède une largeur de bande de 200 kHz. Ceci détermine dans la bande allouée actuellement 20 canaux de fréquences dont seuls 18 sont utilisés pour éviter les problèmes d'interférences avec les autres réseaux de radiotéléphonie cellulaire.

Le principe de multiplexage utilisé afin d'étendre la capacité du système est un multiplexage temporel de type Time Division Multiple Access (TDMA), consistant à diviser chaque canal de communication en trames de 8 intervalles de temps ainsi que le représente la figure 2.10.

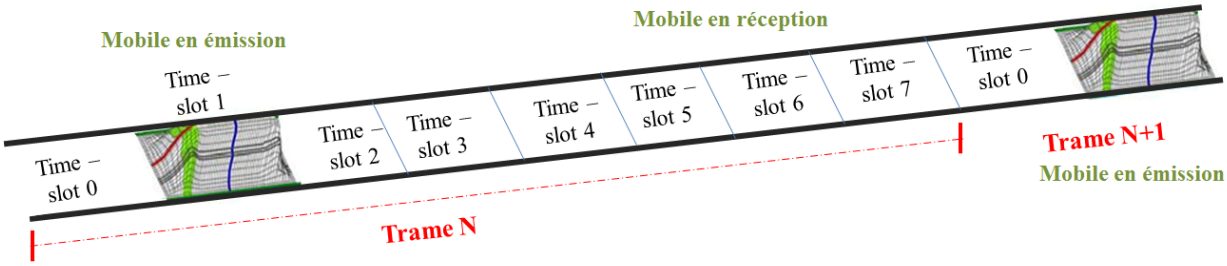


Figure 2.10 Trame TDMA.

Avec ce multiplexage, il devient possible de faire communiquer huit utilisateurs sur le même canal physique, ce qui permet de multiplier le nombre de canaux disponibles par unité de temps par huit comme l'illustre la figure 2.11.

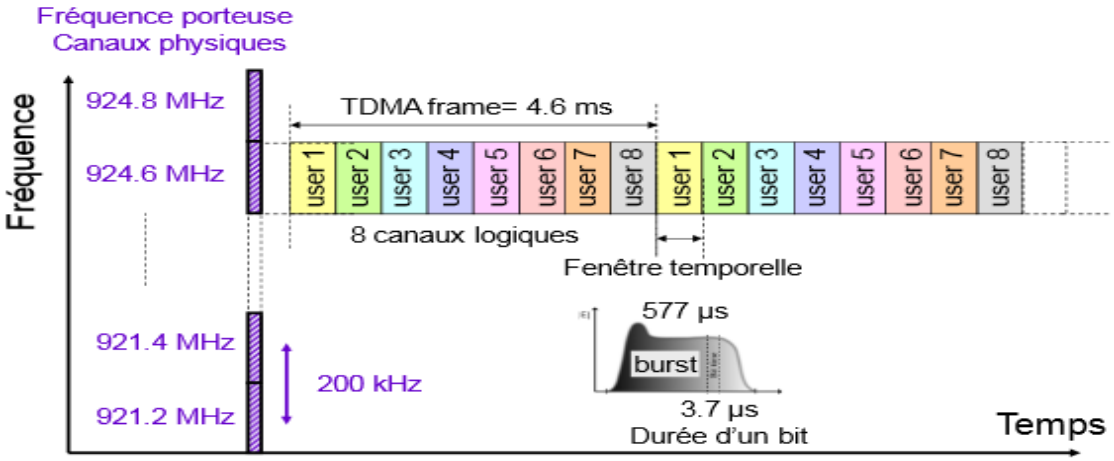


Figure 2.11 Multiplexage temps-fréquence.

Les informations de signalisation qui transitent via le GSM-R entre le train et les RBC utilisent les deux liens montant et descendant présentés. Un canal physique est attribué par le réseau pour la communication, auquel est associé un intervalle de temps également appelé time-slot d'une durée de 577 µs. Un même équipement devra attendre la fin des 7 time-slots suivants avant de pouvoir réémettre à nouveau, ce qui nous donne une durée de 4,615 ms avant une nouvelle transmission dans un time slot.

La figure 2.12, présente le format des trames transmises, chacune d'elles se composent de 157 bits d'une durée de 3,7 µs, appelé burst, ce qui correspond à une durée de 547,6 µs.

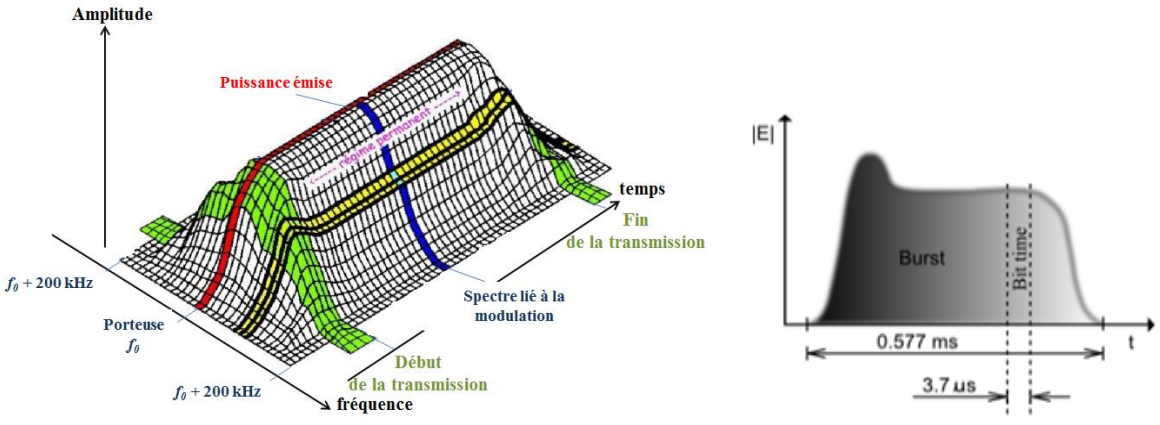


Figure 2.12 Burst GSM-R.

La trame est constituée en pratique d'une suite de 148 bits utiles suivis d'une interruption de la transmission appelée période de garde d'une durée de 30,46 µs dont le but est de bien séparer le contenu de 2 time slots successifs. Chacun des bursts est constitué des données à transmettre mais aussi de données d'information essentielles à la communication, ainsi que le schématise la figure 2.13.

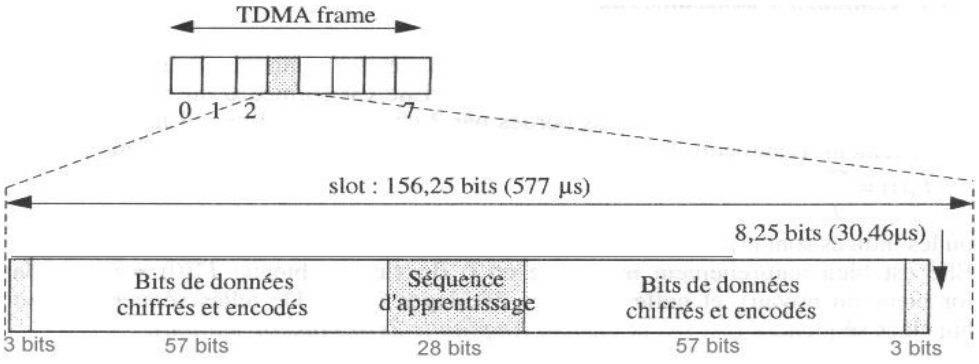


Figure 2.13 Structure d'un burst GSM-R.

La séquence d'apprentissage en particulier, est connue par l'émetteur et le récepteur afin que le récepteur puisse évaluer sur ces bits les distorsions introduites par le canal de propagation et les compenser pour le reste de la trame, ainsi qu'assurer la synchronisation et la compensation de l'effet Doppler. Le GSM-R bénéficie d'un égaliseur adaptatif spécifique afin de lui permettre de fonctionner jusqu'à des vitesses du train excédant 500 km/h.

Dans la section suivante, nous étudions qualitativement l'influence d'un brouilleur sur la communication GSM-R, selon sa position au sol ou en embarqué.

IV. Impact de la perturbation selon la localisation du brouilleur

Les différentes formes d'onde présentées au paragraphe II précédent constituent autant de sources de perturbation possibles pour le système GSM-R. Selon la localisation du brouilleur, au sol ou en embarqué, son impact peut s'avérer différent sur le système. Dans cette partie, nous traitons deux cas de figure où le brouilleur se trouve à proximité d'une station de base ou, à proximité de l'équipement Eurocab, à l'intérieur du train. Nous partons du principe que les brouilleurs de forte puissance sont plutôt utilisés au sol car ils s'avèrent volumineux et nécessitent une alimentation électrique souvent externe. En embarqué, des brouilleurs de puissance limitée à 1 W sont les seuls considérés. En référence à notre classification précédente, ils sont de type A et émettent de façon continue par balayage rapide des bandes allouées au GSM-R. Ces brouilleurs sont équipés d'antennes à faible gain constituées d'un élément rayonnant en quart d'onde au-dessus d'un boitier métallique.

Nous faisons également l'hypothèse, que nous vérifierons par la suite, que lorsque les puissances de signal utile et du brouilleur reçues par le récepteur sont du même ordre de grandeur, alors la communication est perturbée.

IV.1. Niveaux exploités par la communication

Les spécifications EIRENE [2.9] précisent que la dynamique de réception des signaux GSM-R doit être comprise dans la gamme comprise entre -20 dBm et -95 dBm. La figure 2.14 montre un relevé de puissance pratique effectué aux bornes d'une antenne de réception GSM-R d'un train sur une distance de 16 km. Sur cette figure, on observe quatre maximas correspondants au passage du train au plus près de quatre stations de base consécutives. La planification cellulaire mis en œuvre dans ce cas de figure permet d'atteindre des niveaux maximum ne dépassant pas -20 dBm et des niveaux minimum supérieurs à -95 dBm, bien en accord avec ces spécifications.

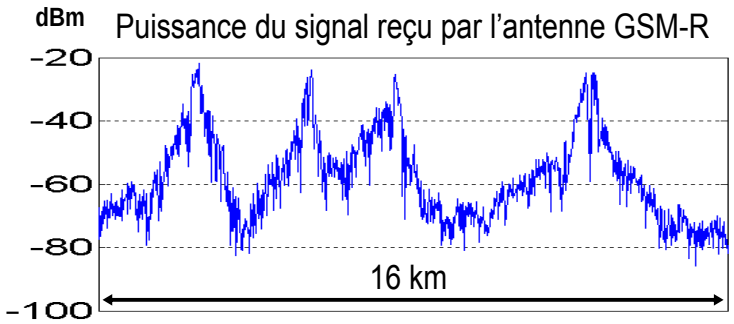


Figure 2.14 Evolution de la puissance reçue en fonction de la distance aux BTS

Ceci vaut pour la communication sol vers train (downlink). Pour la communication trains vers sol, les niveaux reçus par le récepteur de la BTS sont du même ordre de grandeur, les puissances délivrées par les équipements d'émission sol et trains étant identiques. Les puissances d'émission employées peuvent atteindre +39 dBm ou 8 W. Ceci représente une différence de niveau allant de 59 dB à 133 dB entre les niveaux émis et reçus. En conséquence, le signal d'émission ne subira vraisemblablement pas de perturbations, tandis que les signaux de réception pourraient être perturbés, surtout à distance des BTS, là où les signaux utiles reçus sont les plus atténués.

IV.2. Brouilleur disposé à l'infrastructure

La figure 2.15 montre un tel scénario. Ce type de brouilleur peut perturber le récepteur radio situé à l'infrastructure, que des trains soient présents ou non.

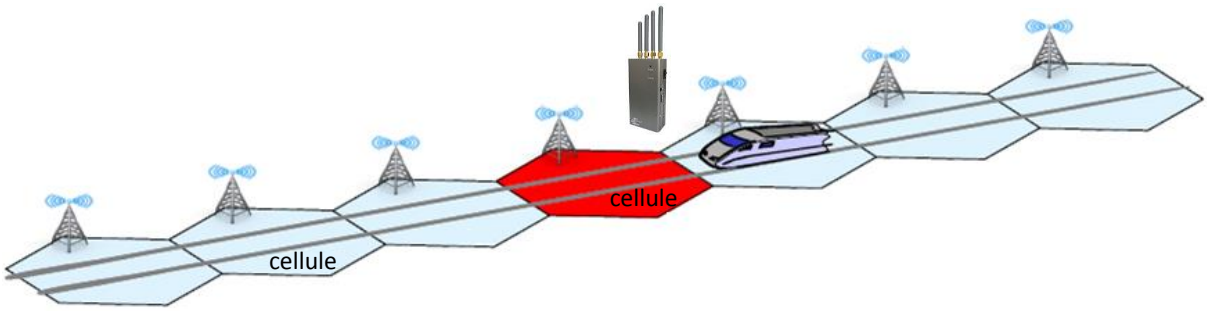


Figure 2.15 Brouilleur disposé à l'extérieur du train.

Les trains ont une vitesse qui peut dépasser 300 km/h ce qui les font traverser une cellule GSM-R en une minute environ. Deux scénarios peuvent être distingués :

(1) le brouilleur est placé le long des voies, à proximité immédiate d'une BTS ;

(2) le brouilleur est placé pratiquement à mi-chemin, entre deux BTS successives.

❖ *Hypothèse 1 :* Brouilleur à proximité d'une BTS

La figure 2.16 représente ce cas de figure où le brouilleur se trouve à proximité d'une BTS.

Figure 2.16 Brouilleur à proximité d'une BTS

Nous obtenons que :

- Le récepteur de la BTS situé à proximité du brouilleur sera le plus impacté. S'il est de puissance suffisante, le brouilleur pourrait empêcher la réception correcte des signaux en provenance du train. Tant que le train ne se trouve pas à proximité de la BTS, cette situation peut perdurer.
- Le signal de brouillage reçu par la BTS reste à un niveau constant, ce qui peut être utilisé afin d'identifier la localisation proche de la BTS du brouilleur.
- Les signaux de brouillage et GSM-R reçus par le train évoluent de façon similaire car les sources correspondantes sont pratiquement co-localisées.
- Si le brouilleur ne dépasse pas les 1 W, compte tenu des 8 W de la station de base et du meilleur dégagement radioélectrique de l'antenne de la station de base, son impact pourrait être négligeable à bord du train.
- Si le brouilleur développait une puissance excédant les 8 W, alors il pourrait être en mesure de brouiller continuellement la réception des signaux à bord du train.

❖ *Hypothèse 2 :* Brouilleur disposé entre deux BTS

La figure 2.17 représente ce second cas de figure où le brouilleur se trouve approximativement à mi-chemin entre deux BTS.

Figure 2.17 Brouilleur placé entre deux BTS.

Nous obtenons que :

- Les niveaux de brouillage seront pratiquement équivalents sur les deux BTS les plus proches.
- Entre deux BTS, le niveau reçu par le train est faible (cf. figure 2.14). L'impact du brouilleur sur la communication BTS vers le train peut être particulièrement important dans cette zone intermédiaire où s'effectue également l'opération de handover entre cellules consécutives.
- Si le brouilleur ne dépasse pas les 1 W, compte tenu des 8 W de la station de base et du meilleur dégagement radioélectrique de l'antenne située sur la station de base, son impact sera maximisé au moment du passage du train à proximité du brouilleur.
- Si le brouilleur développe une puissance importante, alors il pourrait brouiller continuellement la réception des signaux à bord du train.

IV.3. Brouilleur embarqué à bord du train

La figure 2.18 présente ce scénario où le brouilleur est présent cette fois à l'intérieur du train. Nous ne considérons plus cette fois que des brouilleurs de puissance limitée à 1 W, portables, autonomes et discrets.

Figure 2.18 Brouilleur disposé à l'intérieur du train.

Le signal reçu par l'antenne train en provenance du brouilleur sera stable si ce dernier ne se déplace pas à bord du train. Evaluons maintenant l'ordre de grandeur des signaux reçus par cette antenne train afin de déterminer sa capacité de brouillage.

IV.3.1. Evaluation du niveau de puissance reçu par l'antenne train

Considérons dans un premier temps uniquement une atténuation d'espace afin de représenter l'atténuation entre le brouilleur et l'antenne GSM-R du train. La puissance reçue par l'antenne GSM-R est alors uniquement fonction de la puissance d'émission et des gains d'antennes de l'émetteur et du récepteur. Avec notre hypothèse très simplificatrice, elle peut être calculée à partir de la formule de Friss suivante. Dans celle-ci, P_{rx} et P_{tx} représentent la puissance délivrée à l'antenne de réception et d'émission, G_{rx} et G_{tx} le gain linéaire de l'antenne de réception et d'émission, avec λ la longueur d'onde en mètres et d la distance séparant les deux antennes.

$$P_{rx} = P_{tx} \times G_{rx} \times G_{tx} \left(\frac{\lambda}{4\pi d} \right)^2 \qquad \text{(II.7)}$$

À une fréquence de 940 MHz, nous obtenons les pertes d'espace suivantes en fonction de la distance :

- 10 m de propagation en espace libre donnent une atténuation de -52 dB ;
- 100 m de propagation en espace libre donnent une atténuation de -72 dB.

10 m peut correspondre à la distance qui sépare un usager qui se situe sur le quai de l'antenne disposée au-dessus du train. 100 m peut correspondre à un usager à bord de la rame.

Des mesures menées dans le cadre du projet « SECRET » ont montré que la structure du train engendre une atténuation supplémentaire de 15 à 25 dB, ce qui nous donne, en prenant une valeur intermédiaire de 20 dB, les valeurs suivantes :

- A une distance de 10 m prenant en compte cette atténuation supplémentaire : -72 dB ;
- A une distance de 100 m prenant en compte cette atténuation supplémentaire : -92 dB.

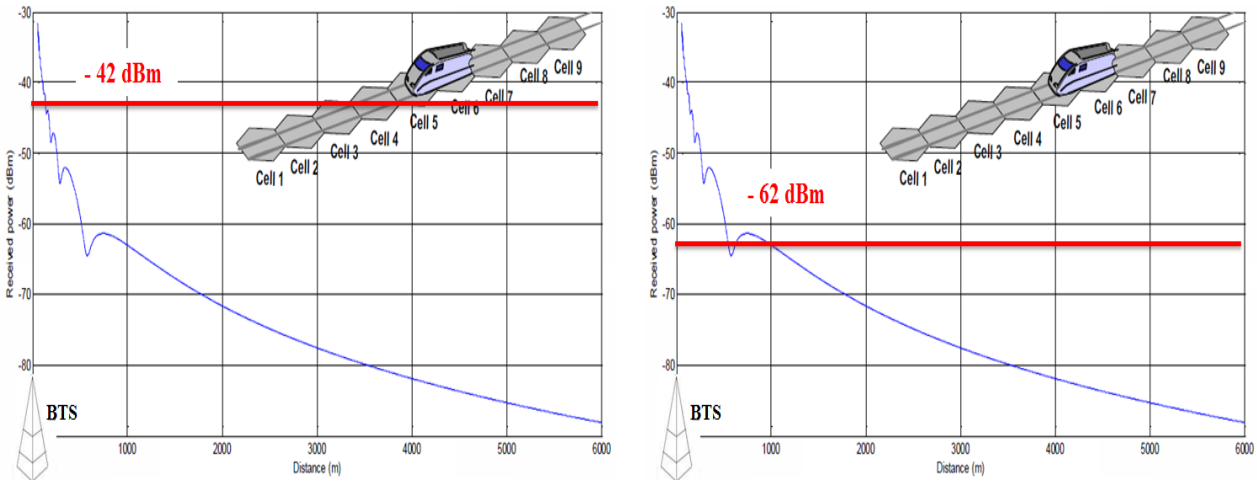
Nous faisons l'hypothèse que le brouilleur développe une puissance de +30 dBm, le niveau reçu en provenance de l'antenne du train devient :

- A 10 m le brouilleur développe avec ces hypothèses une puissance de : -42 dBm ;
- A 100 m, le brouilleur développe avec ces hypothèses une puissance de : -62 dBm.

Par rapport à notre dynamique de réception des signaux GSM-R à bord du train comprise entre -95 dBm et -20 dBm, le niveau de puissance reçu depuis le brouilleur pourra donc s'avérer être plus important que le signal utile. Regardons ce point plus en détails maintenant.

IV.3.2. Evaluation de la portée de brouillage

La figure 2.14 précédente représente les niveaux de réception GSM-R effectivement mesurés lors d'un parcours de 16 km du train. Afin d'obtenir une représentation plus pratique, nous avons modélisé un canal de propagation simplifié utilisant les pertes d'espace et la réflexion au-dessus d'un plan diélectrique considéré infini. Un premier chemin relie directement l'émetteur au récepteur. Ce chemin est affecté par les pertes d'espace. L'autre chemin subit une réflexion sur le sol avant de parvenir également au récepteur en étant également affecté par les pertes d'espace et l'atténuation liée à la réflexion. Le signal reçu par l'antenne s'écrit sous la forme de la somme des deux signaux reçus [2.10]. La figure 2.19 représente l'évolution de la puissance reçue par le train en s'éloignant d'une BTS, sur une distance de 6 km. Nous avons superposé sur cette courbe notée « a » la puissance constante reçue d'un brouilleur situé à 10 m (-42 dBm) et, sur la courbe notée « b », celle reçue par un brouilleur situé à 100 m (-62 dBm). Nous concluons que le brouilleur situé à 10 m impose une puissance supérieure à la puissance utile de communication de façon pratiquement permanente. Celui situé à 100 m développe une puissance supérieure à la puissance utile de communication à partir d'une distance à la BTS de 1000 m.



a : brouilleur à 10 m de l'antenne **b : brouilleur à 100 m de l'antenne**

Figure 2.19 Puissance reçue par l'antenne durant 6 km de trajet.

Ainsi, pendant 5 km, la radio sol-trains pourrait être brouillée, ce qui correspond, à la vitesse de 300 km/h, à un temps écoulé de 1 minute. Si une perte de communication s'effectue durant ce laps de temps due au brouillage, les données ne sont plus rafraichies et, ainsi que nous l'avons indiqué lors du chapitre I, paragraphe VII, nous pourrions avoir immobilisation du train après déclenchement du freinage d'urgence à une localisation ponctuellement prédictible.

Après avoir évalué de façon préliminaire les liens de communication les plus perturbés ainsi que les puissances de brouillage susceptibles d'être reçues, nous menons maintenant une étude préliminaire afin d'évaluer l'impact d'un brouillage sur une communication GSM-R en fonction du rapport de puissance entre la puissance utile de communication et celle fournie par le brouilleur.

V. Analyse de l'impact d'un brouillage sur une communication GSM-R

Dans cette dernière section du chapitre II, nous évaluons l'impact de signaux de brouillage sur le système de communication GSM-R. Pour cela, nous développons et utilisons un banc de mesure simulant le lien de communication entre un mobile GSM-R et une station de base et nous superposons des signaux de brouillage sur ce lien.

Afin d'évaluer le système de communication, nous étudions les paramètres caractéristiques de la communication. Durant cette étape, nous considérons deux paramètres particuliers :

- Le Bit Error Rate (BER) ou taux d'erreur binaire, représente le nombre de bits erronés sur la totalité des bits reçus durant la transmission. Ces bits erronés peuvent être imputés à la qualité de liaison en elle-même ainsi qu'aux brouillages ajoutés. Cette mesure représente généralement le paramètre de performance qui quantifie la fiabilité et la qualité de la liaison radio. L'équation II.8 fournit cette expression du BER.

$$BER = \frac{nombre\ \ de\ \ bits\ \ erronés}{nombre\ \ total\ \ de\ \ bits\ \ transmis} \times 100\% \qquad \text{(II.8)}$$

- Nous introduisons par l'équation II.9 également le paramètre Signal to Jammer Ratio (*SJR*) ou encore le rapport entre la puissance utile de communication et la puissance du brouilleur. Ce rapport est généralement utilisé pour évaluer l'impact d'un brouilleur sur un système.

$$SJR = \frac{puissance\ \ du\ \ signal}{puissance\ \ du\ \ brouilleur} \qquad \text{(II.9)}$$

V.1. Banc de mesures

Le banc de mesure développé au laboratoire dans le cadre de ce travail est présenté figure 2.20. Nous employons un simulateur de réseau GSM-R, CMU 200 de chez Rohde & Schwarz, qui établit et gère la communication avec un mobile de test GSM-R.

Le simulateur de réseau permet d'accéder directement aux valeurs de BER. Un générateur de brouillage associé à un coupleur permet de superposer les signaux de brouillage au signal utile.

Un analyseur de spectre est utilisé pour mesurer et régler les niveaux de puissance des signaux GSM-R et ceux fournis par le brouilleur à l'entrée du mobile. Un second équipement de mesure, FSIQ 7 de chez Rohde & Schwarz sera connecté par la suite afin d'effectuer les mesures de constellation.

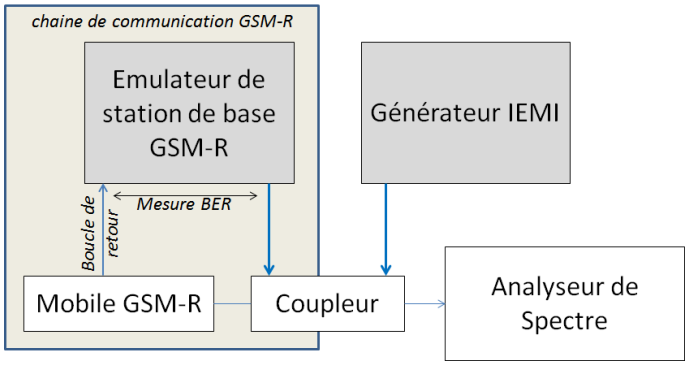


Figure 2.20 Banc de mesure GSM-R

Nous utilisons deux sources différentes de brouillage. La première source est constituée de brouilleurs de poche disponibles sur le marché. La seconde source est constituée d'un générateur de signaux modulable. Ces deux sources sont représentées par le bloc générateur IEMI de la figure 2.20.

Le principe consiste à simuler les transmissions et à introduire les signaux de perturbation durant une communication GSM-R. Il devient ainsi possible d'évaluer les BER en fonction des niveaux de puissance (*SJR*) fournis par le signal utile et pour les différents équipements de brouillage disponibles. Ces équipements étant reliés par câble coaxiaux, la perturbation reste confinée dans le banc de mesure.

V.1.1. Analyse fréquentielle des signaux de brouillage

Nous utilisons le banc de mesure afin de caractériser successivement les dispositifs de brouillage. Trois brouilleurs de poche différents sont utilisés successivement. La figure 2.21 montre un tel dispositif de brouillage avec ces quatre ports antennes de sortie, correspondants aux différentes bandes de fréquences couvertes.

Figure 2.21 Brouilleur de poche utilisé lors des essais.

L'analyse spectrale effectuée à partir de chacun d'entre eux à l'aide de l'analyseur de spectre fournit les résultats présentés sur la figure 2.22. Un atténuateur de 30 dB est inséré préventivement entre la sortie du brouilleur et l'analyseur de spectre afin de ne pas le saturer.

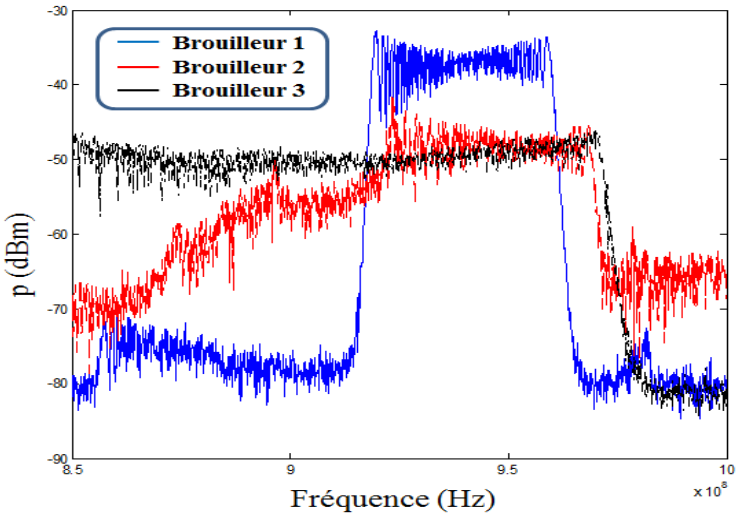


Figure 2.22 Densité spectrale de puissance des trois brouilleurs GSM.

Le brouilleur 1 génère des signaux de brouillage dans la bande de fréquences comprise entre 920 MHz et 970 MHz. Avec les bandes de résolution sélectionnées sur l'analyseur de spectre, dans la bande brouillée, les signaux présentent une ondulation qui peut atteindre pratiquement 10 dB. Cette caractéristique nous permettra, lors du chapitre 3, de faciliter l'identification des brouilleurs par analyse de cette signature.

Le brouilleur 2 couvre une bande plus large allant de 850 MHz à 970 MHz mais, avec une puissance plus réduite. Enfin, le brouilleur 3 couvre la bande de fréquences la plus étendue.

Ces expériences réalisées en laboratoire ont montré que le signal émanant de nos brouilleurs est typiquement généré par modulation d'un oscillateur commandé en tension (VCO). Le signal de modulation est une rampe. Ceci permet de balayer très rapidement une large bande de fréquence. Des

mesures complémentaires ont permis de montrer que la durée de balayage, quelle que soit la gamme balayée est voisine de 8 µs.

Ces oscillateurs n'étant pas stabilisés, ils dérivent en fréquence assez rapidement et leur puissance évolue également en fonction du temps et de la fréquence. Afin de s'affranchir de ces difficultés et disposer d'un signal de brouillage stable, nous considérons maintenant un signal de brouillage issu d'un synthétiseur de fréquence.

V.1.2. Impact d'une perturbation continue sur la communication GSM-R

En Europe, la numérotation des porteuses dans la gamme de fréquence paneuropéenne allouée suit l'ordre suivant :

GSM-R (876-880) MHz : pour $1 \leq n \leq 18$ $f = 876 + (0.2 \times n)$ MHz.

GSM-R (921-925) MHz : pour $1 \leq n \leq 18$ $f = 876 + (0.2 \times n)$ MHz.

Nous exploitons durant nos essais essentiellement le canal 18. Nous établissons une communication GSM-R sur ce canal via le CMU. Nous injectons ensuite les signaux de brouillage et nous évaluons leurs effets sur le *BER*, en faisant varier le *SJR*.

Deux signaux sont utilisés successivement, un signal sinusoïdal pur, centré dans le canal de communication et, un signal sinusoïdal modulé avec une excursion en fréquence de 75 kHz également centré sur le canal de fréquence exploité. La représentation spectrale de ces deux signaux apparaît sur la figure 2.23.

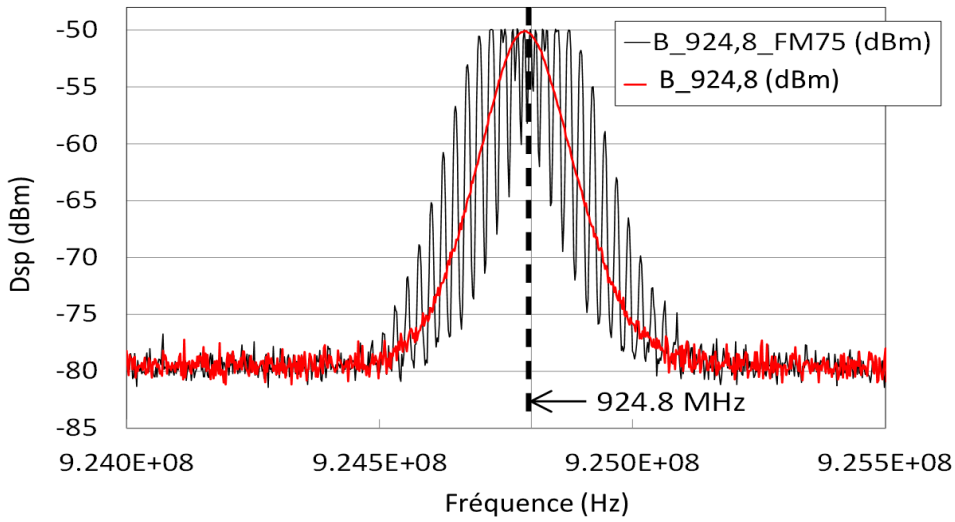


Figure 2.23 Densité spectrale de puissance des deux signaux de brouillage.

Pour effectuer ces mesures, nous travaillons à une puissance de communication constante comprise dans la gamme -95 dBm à -20 dBm. Nous avons sélectionné -38 dBm pour les mesures présentées, soit un rapport signal sur bruit confortable permettant d'obtenir un excellent BER en absence de

signaux de brouillage. La puissance de brouillage est modifiée progressivement et le BER correspondant est mesuré.

Les résultats de cette expérimentation sont représentés tableau 2.1. Les puissances de communication et de brouillage sont indiquées respectivement colonnes 1 et 2. Le *SJR* résultant de la différence entre ces deux puissances est donné colonne 3. Les BER mesurés par le CMU apparaissent colonnes 4 et 5, respectivement pour le brouillage sinusoïdal pur et, pour le brouillage modulé en fréquence.

Tableau 2.1 BER en fonction du *SJR* de la communication

P_GSM-R (dBm)	**P_JAM** (dBm)	**JSR** (dB)	**BER_*f1***	**BER_FM 75**
-38	-36	-2	Com. perdue	No conn.
-38	-37	-1	12,585	No conn.
-38	-38	0	5,564	No conn.
-38	-40	2	2,126	14,662
-38	-42	4	0,771	7,814
-38	-44	6	0,256	2,719
-38	-46	8	0,114	0,588
-38	-48	10	0,06	0,155
-38	-50	12	0,023	0,038

L'indication « com. perdu » signifie que la communication a été perdue après apparition de la perturbation. « No conn. » signifie qu'il est impossible d'établir la connexion dans cette configuration, lorsque le brouilleur est actif.

On peut conclure d'après ces résultats que si les puissances de communication et de brouilleur sont du même ordre de grandeur, alors les communications sont perturbées ou interrompues. Nous validons ainsi l'hypothèse effectuée en section IV de ce chapitre.

Un écart de 6 dB ou plus en faveur de la puissance de communication réduit fortement l'impact du brouillage.

Il est également important de noter qu'à puissance égale, le signal modulé en fréquence affecte plus la communication que le signal sinusoïdal pur centré dans le canal.

V.1.3. Brouillage et blocage de la communication GSM-R

Les récepteurs de communications mobiles peuvent également être perturbés par des signaux puissants situés hors bande, nous l'avons signalé qualitativement au paragraphe V.2 du premier chapitre. Il s'agit d'un effet de blocage de la réception lié aux phénomènes d'intermodulation puisque le réseau GSM-R jouxte les réseaux d'opérateurs de radiotéléphonie cellulaire à la fois dans l'espace et en ce qui concerne l'attribution des canaux de fréquences. Ce phénomène a été constaté à quelques reprises.

L'ETSI [2.9] a prévu cette situation et le tableau 2.2 résume les spécifications que le récepteur doit respecter en ce qui concerne la résistance aux signaux hors bande.

Tableau 2.2 Niveau de puissance perturbant la liaison GSM-R

Couverture des perturbations (MHz)	Puissance de la perturbation reçue (dBm)
$0.6 \leq \|fb\text{-}f0\| < 0.8$	-38
$0.8 \leq \|fb\text{-}f0\| < 1.6$	-33
$0.6 \leq \|fb\text{-}f0\| < 3$	-23
$3 \leq \|fb\text{-}f0\|$	-23

fb-f0 représente l'écart de fréquence entre la canal GSM-R et le canal hors bande. Sachant que la largeur d'un canal GSM-R est de 0.2 MHz, le récepteur doit être en mesure de résister à des niveaux de puissance de -38 dBm pour des signaux hors bande situés entre 3 et 4 canaux d'écart.
À plus de 3 MHz d'écart en fréquence, le récepteur ne doit pas être perturbé par des puissances d'entrée hors bande allant jusqu'à -23 dBm [2.11].

VI. Chaîne de transmission GSM-R

Durant notre travail, nous réalisons nos expérimentations à l'aide de deux plateformes différentes. La première utilise le banc de mesure introduit précédemment. La seconde exploite un modèle de simulation réalisé sous Matlab™ que nous décrivons maintenant plus avant. Nous considérons essentiellement la chaîne de modulation/démodulation GMSK. La modulation utilisée est une modulation de phase à déphasage minimal GMSK avec filtrage gaussien pour réaliser l'adaptation de la bande passante du signal à la largeur du canal attribué.

VI.1. Modélisation de la chaîne de communication GMSK

Nous modélisons dans un premier temps cette chaîne de modulation GMSK. La modulation à phase continue utilise un paramètre de largeur de bande avec un produit de modulation (BT_b) fixé à 0.3 ou T_b est la durée du bit. La chaîne de modulation simulée est représentée figure 2.24.

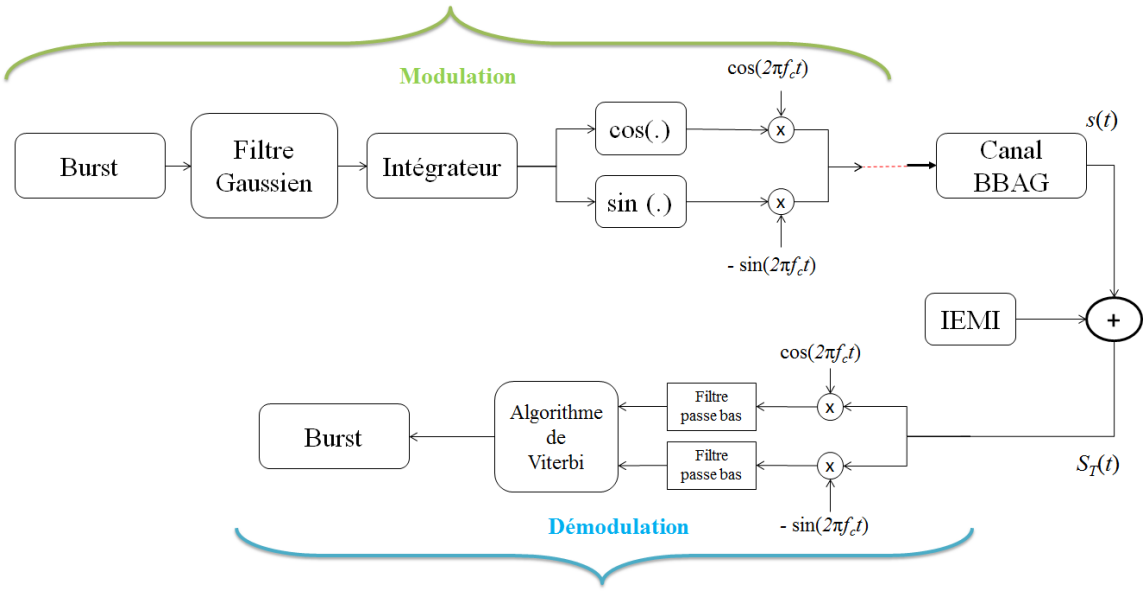


Figure 2.24 Chaîne de modulation / démodulation GMSK.

La chaîne de modulation génère une séquence de 148 bits correspondant à un burst GSM-R. La trame binaire de bits est modulée par un filtre gaussien afin de réduire l'énergie associée aux lobes secondaires. Cette modulation à phase continue effectue une intégration du signal filtré avant son passage dans un modulateur quadratique. A ce niveau, le signal correspond à celui transmis par l'émetteur. Nous introduisons à ce niveau un bruit blanc additif gaussien (*BBAG*). Nous superposons également à ce niveau le signal de brouillage.

Le signal $s(t)$ transmis par l'émetteur s'écrit sous la forme :

$$s(t) = \sqrt{\frac{2E_b}{T_b}}\left[\cos\phi(t,\alpha)\cos 2\pi f_c t - \sin\phi(t,\alpha)\sin 2\pi f_c t\right] + N_g(t) \qquad \text{(II.10)}$$

$N_g(t)$ représente l'effet du canal *BBAG*, E est l'énergie associée au bit d'une durée T_b, et f_c la fréquence de modulation. Les composantes cos $\phi(t, \alpha)$ et sin $\phi(t, \alpha)$ représentent respectivement les signaux en quadrature de phase, et où $\phi(t, \alpha)$ représente la phase instantanée (cf. annexe 1).

$$\phi(t,\alpha) = 2\pi\sum_{i<N}\alpha_i hq(t - iT_b) \qquad \text{(II.11)}$$

La séquence du signal binaire α_i est l'information du bit pour le i^{iéme} échantillon, avec h l'index de modulation et $q(t)$ la réponse de phase normalisée représenté par l'intégral du filtre utilisé par la modulation et qui est donnée par l'expression (cf. annexe 1):

$$q(t) = \int_{-\infty}^{t} g(\tau)d\tau \qquad \text{(II.12)}$$

Une expression plus simplifiée du signal reçu par l'antenne s'écrit sous la forme :

$$s(t) = \left[\cos(2\pi f_c t) i(t) + \sin(2\pi f_c t) q(t)\right] + N_g(t) \quad \text{(II.13)}$$

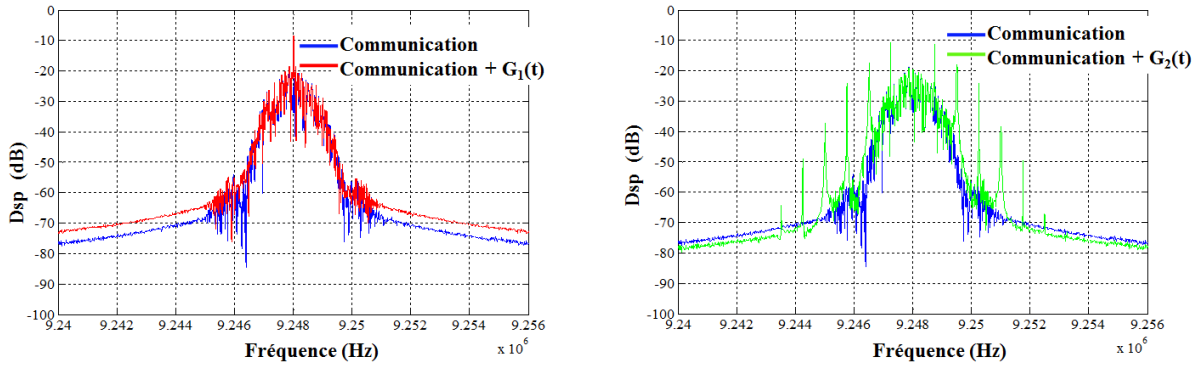
Ce qui donne :

$$s(t) = y(t) + N_g(t) \quad \text{(II.14)}$$

En rajoutant l'effet du brouillage notre signal s'écrit :

$$s_T(t) = s(t) + br(t) \quad \text{(II.15)}$$

Nous pouvons obtenir une représentation du signal à ce niveau de la chaîne de communication. Les résultats de la figure 2.25 montrent ainsi, sur la vue de gauche, le spectre du signal de communication avec et sans brouillage pour un signal sinusoïdal pur $G_1(t)$ et, sur la vue de droite, le spectre du signal de communication avec et sans brouillage pour le signal sinusoïdal modulé $G_2(t)$.



a : communication + brouillage $G_1(t)$ **a : communication + brouillage $G_2(t)$**

Figure 2.25 Spectre de communication GSM-R avec et sans brouillage.

On remarque qu'en ce qui concerne le spectre, la distinction sur cette représentation est forte entre la communication en mode de fonctionnement « normal » et la communication perturbée en présence de brouilleur, dès l'apparition du brouillage.

Cette remarque constitue un premier point d'entrée pour notre système de détection. Une méthode de détection possible consistera ainsi en une surveillance du spectre reçu par l'antenne de réception GSM-R. Les signatures en fréquences des brouilleurs apparaissant précédemment en figure 2.22 corroborent ce point.

Grâce au récepteur simplifié modélisé figure 2.24, l'antenne reçoit le signal et effectue la démodulation en utilisant une démodulation quadratique. Le signal est ensuite récupéré en utilisant un algorithme de Viterbi (VA) ainsi que le montre la figure 2.26.

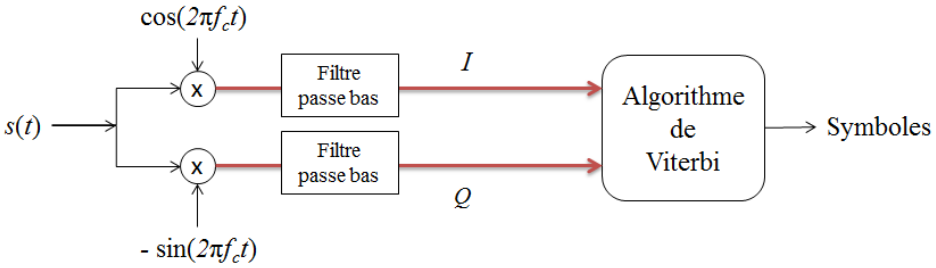


Figure 2.26 Chaîne de démodulation.

$I(t)$ et $Q(t)$ sont les signaux en phase et en quadrature donnés par les expressions suivantes :

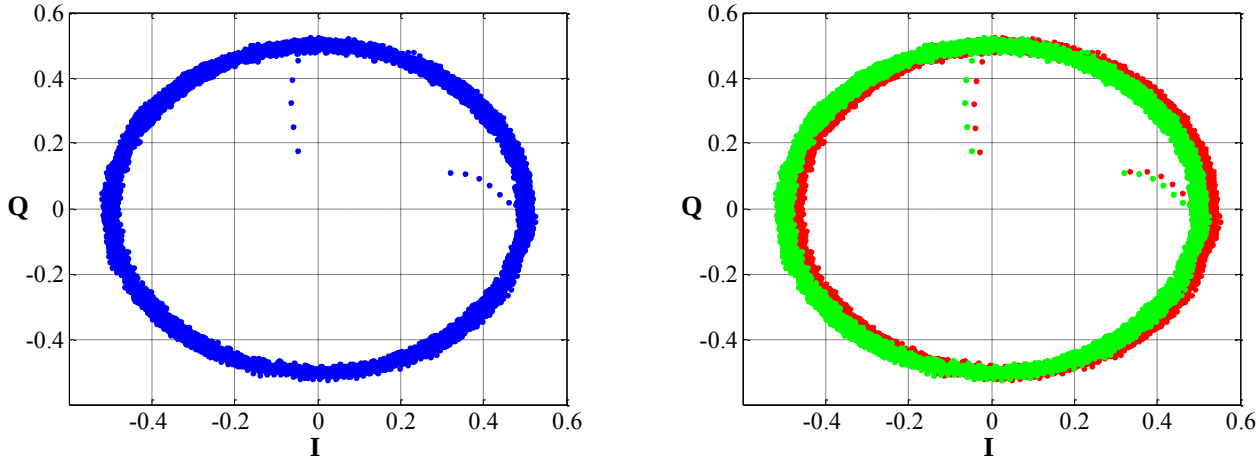
$$I(t) = g(t) * \left(\cos(2\pi f_c t) s(t)\right) \tag{II.16}$$

$$Q(t) = g(t) * \left(\sin(2\pi f_c t) s(t)\right) \tag{II.17}$$

VI.1.1. Constellation des signaux obtenus par simulation

Disposant de ces deux signaux en phase et en quadrature de phase, nous sommes maintenant en mesure de représenter la constellation décrivant le signal de communication reçu.

Les traitements sont effectués sur les données I et Q après filtrage. La figure 2.27 représente les deux modes de fonctionnement « normal » et « attaqué ». Dans cette représentation, le brouillage utilisé est modélisé par un signal sinusoïdal centré sur le canal avec superposition du *BBAG*.



a : signal de communication **b : communication + brouillage**

Figure 2.27 Représentation IQ avant filtrage pour les deux fonctionnements a : normal, b : normal + attaqué.

Nous obtenons qu'en fonction du *SJR*, l'étalement des signaux I et Q de la constellation évolue. Plus la puissance de brouillage est importante par rapport à la puissance de la communication utile, plus cet étalement s'avère prononcé.

Nous avons souhaité vérifier cette évolution obtenue par le modèle de simulation de façon expérimentale et nous avons reproduit ces conditions sur le banc de mesures.

VI.1.2. Constellation des signaux obtenus par le banc de mesures

Une variante du banc de mesure précédent figure 2.28 est utilisée lors de ces manipulations, à la différence de l'analyseur de spectre, nous utilisons cette fois un démodulateur de mesure de type Rohde et Schwarz FSIQ 7 afin d'afficher les constellations obtenues. L'émulateur de station de base est remplacé par un générateur de signaux GMSK afin d'obtenir une concordance avec notre modèle de simulation de chaîne de modulation / démodulation et de s'affranchir du caractère TDMA des signaux émis par le CMU 200.

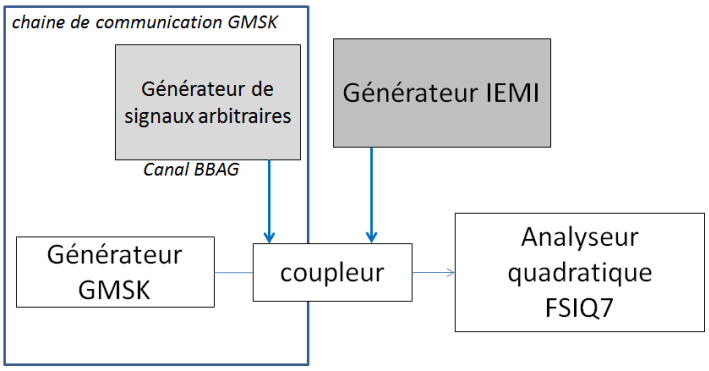


Figure 2.28 Banc de mesure quadratique.

Les résultats des mesures menées sur le banc de test GSM-R sont donnés figure 2.29. Les deux constellations représentent le signal de communication pur (a) et un signal GMSK en présence de brouillage avec un rapport signal sur bruit de 20 dB (b).

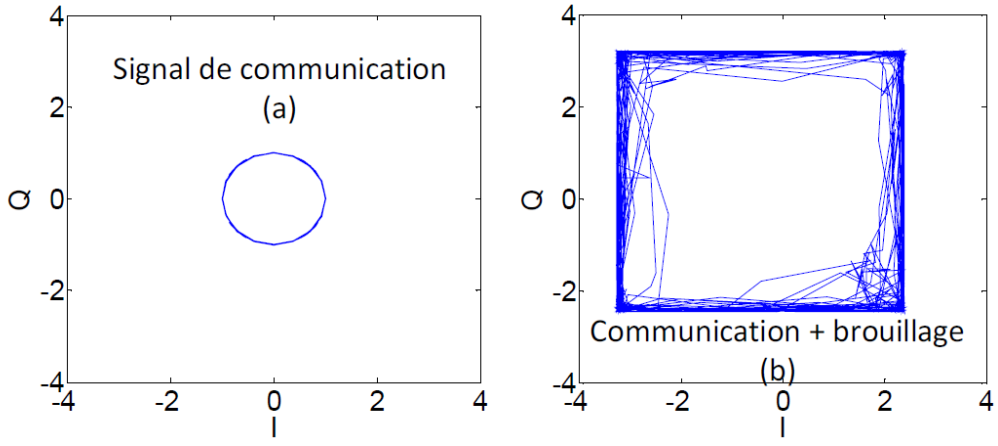


Figure 2.29 Constellation du signal GMSK a : sans brouillage, b : avec brouillage.

A travers ces constellations, on note la nette différence entre le signal de communication en mode de fonctionnement “normal” et le signal de communication en présence de brouillage.
Cette seconde représentation se base sur les principes de modulation de la chaîne de transmission GSM-R. Les caractéristiques quadratiques de cette modulation peuvent être utilisées afin de distinguer les situations avec brouillages et sans brouillages.

Avec cette seconde remarque, nous pouvons proposer de mettre en place une seconde méthode de détection se basant sur cette évolution de la constellation afin de créer un modèle de fonctionnement normal du système et de détecter des écarts par rapport à ce modèle normal.

A l’issue de ce chapitre, nous retenons donc les deux méthodes de détection repérées que nous proposons de développer dans le chapitre III.

VII. Conclusion du chapitre 2

Lors de ce deuxième chapitre nous avons analysé différents systèmes et différentes configurations pouvant perturber les communications GSM-R.
Dans une première partie, nous avons rappelé quelques sources d’interférences d’origines naturelles et industrielles en mesure de perturber les radiocommunications. Nous avons ensuite évoqué le cas plus particulier des brouilleurs électromagnétiques intentionnels ainsi que rappelé leur classification. Nous en avons identifié de trois types selon leur largeur de bande de brouillage : ultra large bande, à sinusoïde amortie et à bande étroite.
Les éléments pertinents pour l’étude d’une architecture de communication GSM-R ont ensuite été rappelés et nous avons considéré différentes dispositions de brouillage, le brouilleur étant disposé soit le long de l’infrastructure ferroviaire, soit à bord du train.
Nous en avons déduit les puissances de brouillage qu’il semble réaliste d’être reçues par les récepteurs des BTS et du train.
Nous avons également effectué une évaluation de la portée du brouilleur, qui peut être conséquente et avoir des conséquences sur l’exploitation ferroviaire.
Ce chapitre s’est poursuivi par une analyse de l’impact d’un brouillage sur une communication GSM-R effectuée à partir d’un banc de mesures. Nous avons obtenu que lorsque les puissances de communication et de brouillage sont du même ordre de grandeur, alors la communication peut être interrompue et devenir impossible.
Dans une dernière étape de ce chapitre nous avons modélisé une chaîne d’émission réception GSM-R simplifiée et avons mis en évidence deux méthodes possibles permettant de détecter voire d’identifier la présence de brouilleurs.

L'une considère l'analyse spectrale des signaux reçus par l'antenne. L'autre exploite les déformations de la constellation I et Q en présence de brouillage.
Le chapitre 3 se propose d'analyser maintenant en profondeur ces deux méthodes.

VIII. Références du chapitre 2

[2.1] S. Dudoyer, V. Deniau, S. Ambellouis, M. Heddebaut et A. Mariscotti, «Recherche de descripteurs adaptés à l'analyse du bruit EM agissant sur la qualité des transmission GSM-R» colloque CEM 2012, 2012.

[2.2] P. Degauque et A. Zeddam, compatibilité électromagnétique 1, des concepts de base aux applications, Paris: Lavoisier, 2007.

[2.3] Mobile & Personal Communications Committee, Use of Jammer and Disabler Devices for Blocking PCS, Cellular & Related Services of the Radio Advisory Board of Canada, RABC Publication 01.3, Ottawa, 2001.

[2.4] Autorité de régulation des télécommunications, « Utilisation en France d'appareils permettant d'empêcher le fonctionnement des téléphones mobiles», 2002.

[2.5] D. Månsson, Susceptibility investigations and classification of civilian systems and equipment, Uppsala: These de Master Université d' Uppsala, 2008.

[2.6] D. V. Giri et F. M. Tesche, Classification of intentional electromagnetic environments (IEME), *IEEE Transactions on Electromagnetic Compatibility*, pp. 322-328, 2004.

[2.7] R. Purnachandra, GSM - R (Global System for Mobile Communication - Railway) *CSI communications*, pp. 18-19, septembre 2012.

[2.8] Projet EIRENE, Functional Requirements Specification, 2006.

[2.9] ETSI TR 103 134 v1.1.1, «Railway Telecommunications (RT) GSM-R in support of EC mandate on Urban Rail», 2013.

[2.10] S. F. Mahmoud et J. R. Wait, Geometrical optical approach for electromagnetic wave propagation in rectangular mine tunnels, *Radio Science*, n°9, p. 1147–1158, 1974.

[2.11] Electronic Communications Committee (ECC) within the European Conference of Postal and Telecommunications Administrations (CEPT), Tactical mechanism to improve the compatibility between GSM-R and public mobile networks and guidance on practical coordination, ECC REPORT 162, Italy, 2011.

Chapitre 3 : Méthodes de détection et développement des outils associés

SOMMAIRE

I. Introduction

Ce troisième chapitre se concentre sur l'étude et le développement de systèmes automatiques de détection et, le cas échéant, d'identification d'attaques électromagnétiques visant les communications ferroviaires. Plus précisément, comme nous l'avons décrit au chapitre 2, nous nous intéressons spécifiquement aux brouillages électromagnétiques ciblant le réseau de radio sol-train par GSM-R.
Dans un premier temps nous nous intéressons à l'élaboration du système de détection. Basée sur une technique en mode supervisée, la détection consiste à identifier tous signaux (ou paramètres) s'écartant d'une représentation de l'environnement EM dit de fonctionnement « normal ».
Une étape d'apprentissage s'avère donc nécessaire afin de définir l'environnement EM « normal » dans lequel s'effectuent les communications GSM-R.

Considérant les deux méthodes repérées lors du chapitre précédent, nous procédons pour l'une de celles-ci à l'estimation de paramètres et à la caractérisation du fonctionnement « normal » à partir de signaux démodulés obtenus dans l'espace des temps, en quadrature, acquis dans ce contexte. Une fois les paramètres définis et le fonctionnement normal caractérisé et appris, nous procédons à la phase de détection.
Pour l'autre méthode repérée au chapitre II, nous étudions un système de détection et d'identification par classification spectrale des environnements électromagnétiques. Comme pour la détection utilisant des signaux démodulés en quadrature, nous utilisons une méthode supervisée. Une première étape est de décrire les paramètres capables de discriminer un signal d'attaque d'un autre. Une fois les paramètres identifiés et définis, nous passons à la phase d'apprentissage de modèle statistique en mesure de représenter ces divers signaux d'attaque. Enfin, nous présentons la procédure de détection et d'identification utilisant ces modèles et les relations statistiques de Bayes.

Pour résumer cette organisation, la figure 3.1 présente les différents blocs étudiés dans ce chapitre.

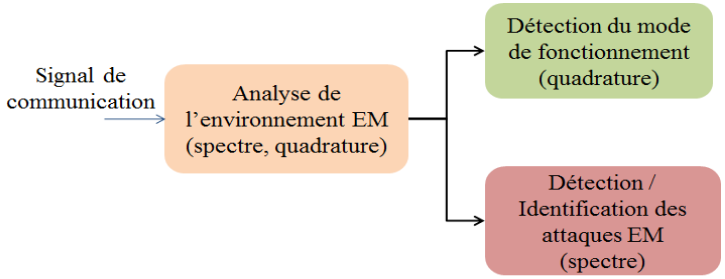


Figure 3.1. Architecture du système de détection.

Précisons que ces deux espaces quadratique et spectral de détection sont indépendants l'un de l'autre et correspondent également à des mises en œuvre très différentes que nous préciserons ultérieurement. La section suivante entame cette analyse en exploitant les signaux en quadrature.

II. Détection des attaques EM dans l'espace des signaux quadratiques *IQ*

II.1. Introduction

Nous nous intéressons dans cette section à l'élaboration d'un système de détection d'attaques EM exploitant directement l'estimation des signaux en bande de base. Nous exploitons les signaux en phase et en quadrature $I(t)$ et $Q(t)$ obtenus après le filtrage passe-bas de la chaîne de démodulation d'un récepteur GSM/GSM-R selon le schéma apparaissant figure 3.2.

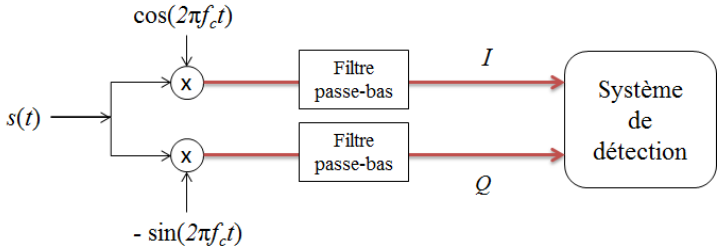


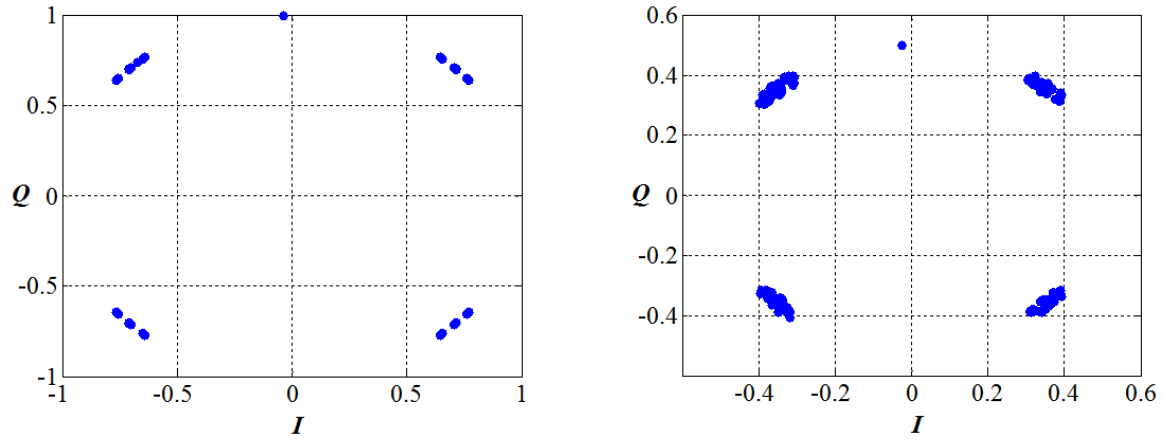
Figure 3.2. Système de détection quadratique

En considérant un canal de transmission *BBAG*, les expressions de $I(t)$ et $Q(t)$ sont données par les équations (II.16) et (II.17) présentées au chapitre précédent que nous rappelons ci-dessous.

$$I(t) = g(t) * \left(\cos(2\pi f_c t) s(t)\right)$$

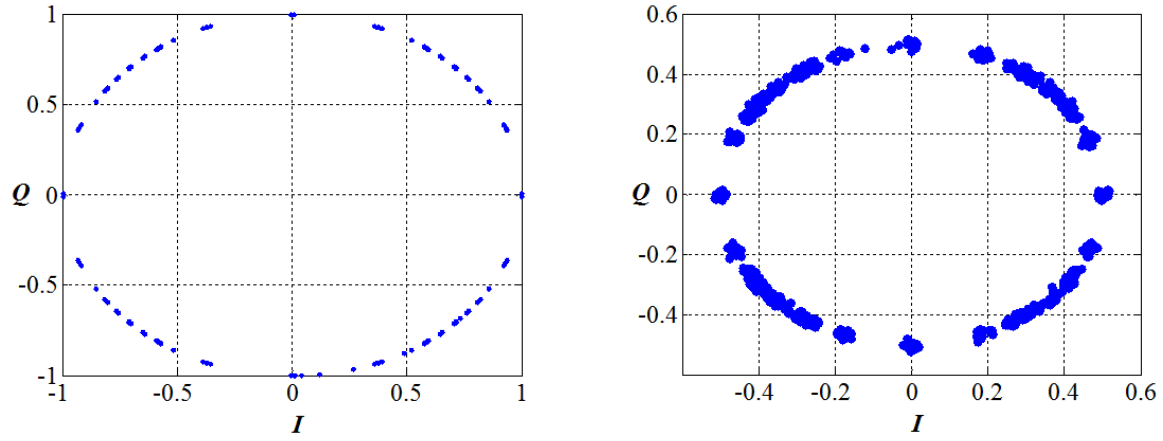
$$Q(t) = g(t) * \left(\sin(2\pi f_c t) s(t)\right)$$

$I(t)$ et $Q(t)$ sont les signaux estimés à la réception provenant des signaux en quadrature $i(t)$ et $q(t)$ élaborés à l'émission équation II.14, chapitre 2. Pour un pas d'échantillonnage T_e, correspondant à un échantillon par symbole, la représentation de $Q(nT_e)$ en fonction de $I(nT_e)$ est une constellation résultant des différents états des symboles à transmettre. La figure 3.3 présente une telle constellation pour des signaux $i(nT_e)$ et $q(nT_e)$ issues d'une modulation *GMSK* en utilisant un pas d'échantillonnage égale à un échantillon par symbole. Cette constellation représente un burst de 156 symboles avant et après passage dans un canal *BBAG* avec un *SNR* = 30 dB. En augmentant le nombre d'échantillons, la constellation se transforme en un cercle décrivant plus finement l'évolution temporelle de ces signaux en quadrature. La figure 3.4 présente ainsi les mêmes signaux avec un échantillonnage de 4 échantillons par symbole.



(a) (b)

Figure 3.3. Constellations des signaux en quadrature I(nTe) et Q(nTe), a : avant canal *BBAG*, b : après canal *BBAG* de *SNR* = 30 dB, avec un pas d'échantillonnage de 1 échantillon par symbole (en simulation).



(a) (b)

Figure 3.4. Constellations des signaux en quadrature I(nTe) et Q(nTe), a : avant canal *BBAG*, b : après canal *BBAG* de *SNR* =30 dB, avec un pas d'échantillonnage de 4 échantillons par symbole (en simulation).

L'effet du bruit du canal *BBAG* a pour conséquence de disperser les points de la constellation estimée autour de points de référence correspondant à la constellation avant canal, selon une variance fonction de la variance du bruit produit par le canal. Quelle que soit la puissance de ce bruit, le cercle reste cependant centré en zéro.

Partant de cette représentation en quadrature caractérisant l'environnement « normal » sous l'effet du canal *BBAG*, nous considérons qu'une éventuelle attaque EM portée sur les signaux *GMSK* déformera la représentation quadratique définie par un cercle de référence ainsi que nous l'avons déjà observé sur la figure 2.27 du chapitre II.

Suite à ces considérations, nous déterminons indépendamment deux descripteurs capables de caractériser et de discriminer efficacement cette représentation en quadrature, se trouvant soit dans un état « normal », soit dans un état « attaqué ».

II.1.1. Descripteur 1 : rayon du cercle $Q(t)$ en fonction de $I(t)$: $TT(t)$

Le rayon du cercle formé par $I(t)$ et $Q(t)$ est défini par :

$$TT(t) = I^2(t) + Q^2(t) \tag{III.1}$$

La moyenne de ce rayon au carré en fonctionnement normal est constante quel que soit le pas d'échantillonnage.

Le bruit blanc du canal tel que considéré n'implique sur la constellation qu'une variance de $TT(t)$ plus ou moins importante autour de sa moyenne, sans jamais déformer le cercle de référence, sous réserve bien entendu de ne jamais perdre la synchronisation.

A l'inverse, tout signal distinct de celui d'émission ou, ne correspondant plus à un bruit blanc gaussien, fait évoluer différemment ce rayon par translation, dilatation rapide,….

La démonstration théorique de ce résultat apparait en annexe 3.

La figure 3.5 et la figure 3.6 illustrent l'impact de perturbations « simples » sur la représentation en quadrature et par conséquent sur le rayon $TT(t)$. Elles présentent ces impacts pour une perturbation $G_1(t)$ définie par un signal sinusoïdal de fréquence égale à la fréquence de la modulation GMSK, pour deux taux de *SJR*. Dans le même cadre, la figure 3.6 présente les effets de $G_2(t)$ définie par un signal sinusoïdal modulé centré sur la fréquence de communication. La constellation définie par les signaux $I(nT_e)$ et $Q(nT_e)$ pour ces figures est estimée au niveau du récepteur après passage dans le canal *BBAG* avec un *SNR* de 30 dB. Un *SJR* = 26 dB est utilisé pour les figures 3.5 (a) et 3.6 (a) ainsi que pour les figures 3.5 (b) et 3.6 (b). Un *SJR* = 14 dB est employé pour les figures 3.5 (c) et 3.6 (c) ainsi que pour les figures 3.5 (d) et 3.6 (d). Des pas d'échantillonnage de T_e = 1 échantillon par symbole à T_e = 4 échantillons par symbole sont utilisés.

On remarque un décalage de la constellation perturbée par rapport à la constellation de référence. Ce décalage est dû à l'effet de la perturbation et s'avère fonction du *SJR* comme on peut le comparer entre les figures 3.5 (a, b) et les figures 3.5 (c, d). On note également que le pas d'échantillonnage permet d'obtenir une représentation plus fine de la déformation.

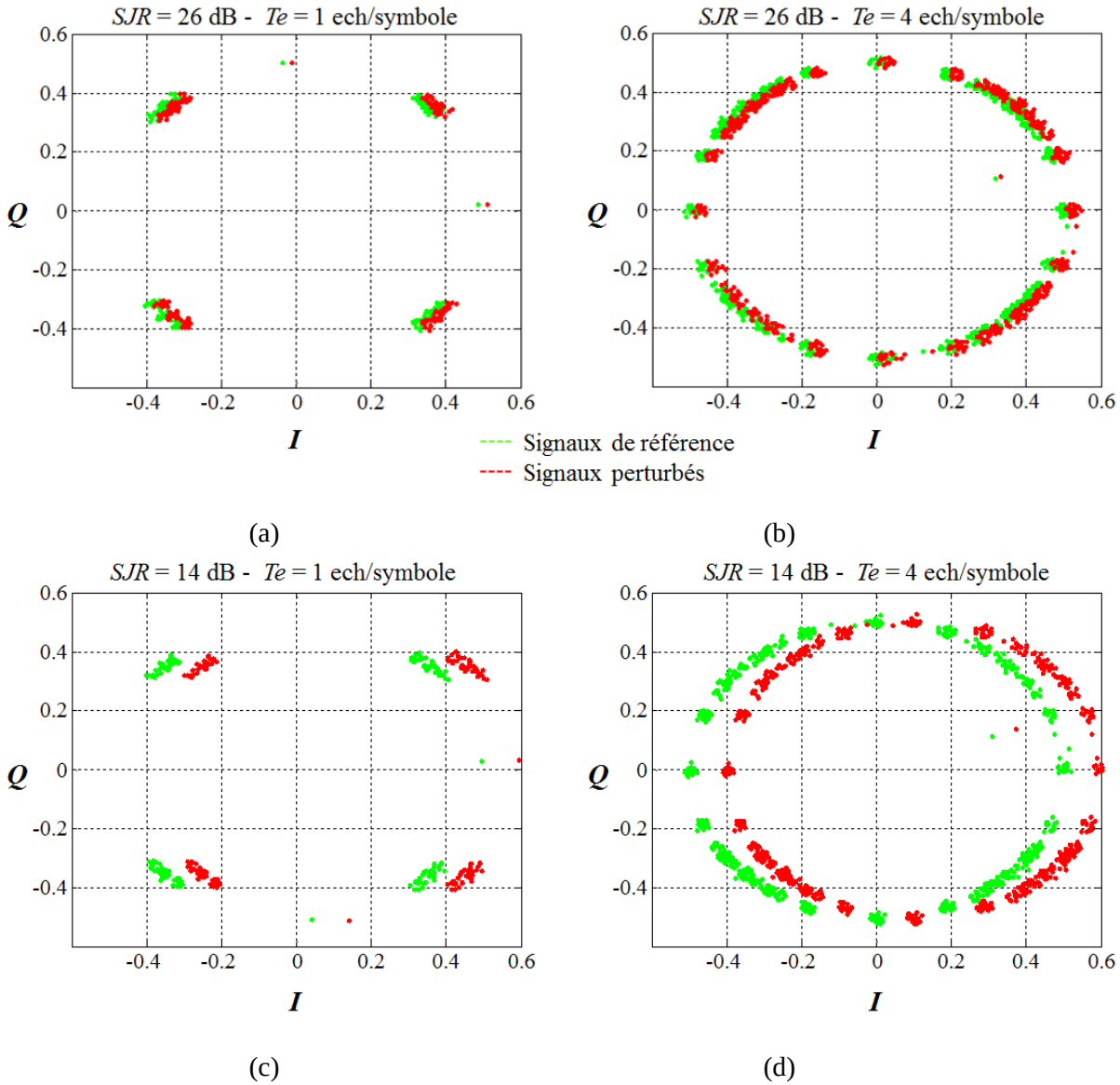


Figure 3.5. Constellations des signaux en quadrature $I(nT_e)$ et $Q(nT_e)$ perturbées avec G_1(t) a : SJR = 26 dB T_e = 1ech/symb, b : SJR = 26 dB T_e = 4ech/symb , c : SJR = 14 dB T_e =1ech/symb, d : SJR = 14 dB T_e = 4ech/symb, en vert le signal de référence et en rouge le signal perturbé (en simulation).

La figure 3.6 représente le même phénomène avec une perturbation différente notée G_2(t). Celle-ci est constituée d'un signal sinusoïdal de fréquence égale à la fréquence de la communication avec une excursion de fréquence de 75 kHz. Comme pour les constellations précédentes on remarque un décalage très significatif et un étalement de la variance des points autour de la référence qui dépend à la fois de la nature du signal de perturbation (dépend de la fréquence de modulation de la perturbation) et du *SJR*.

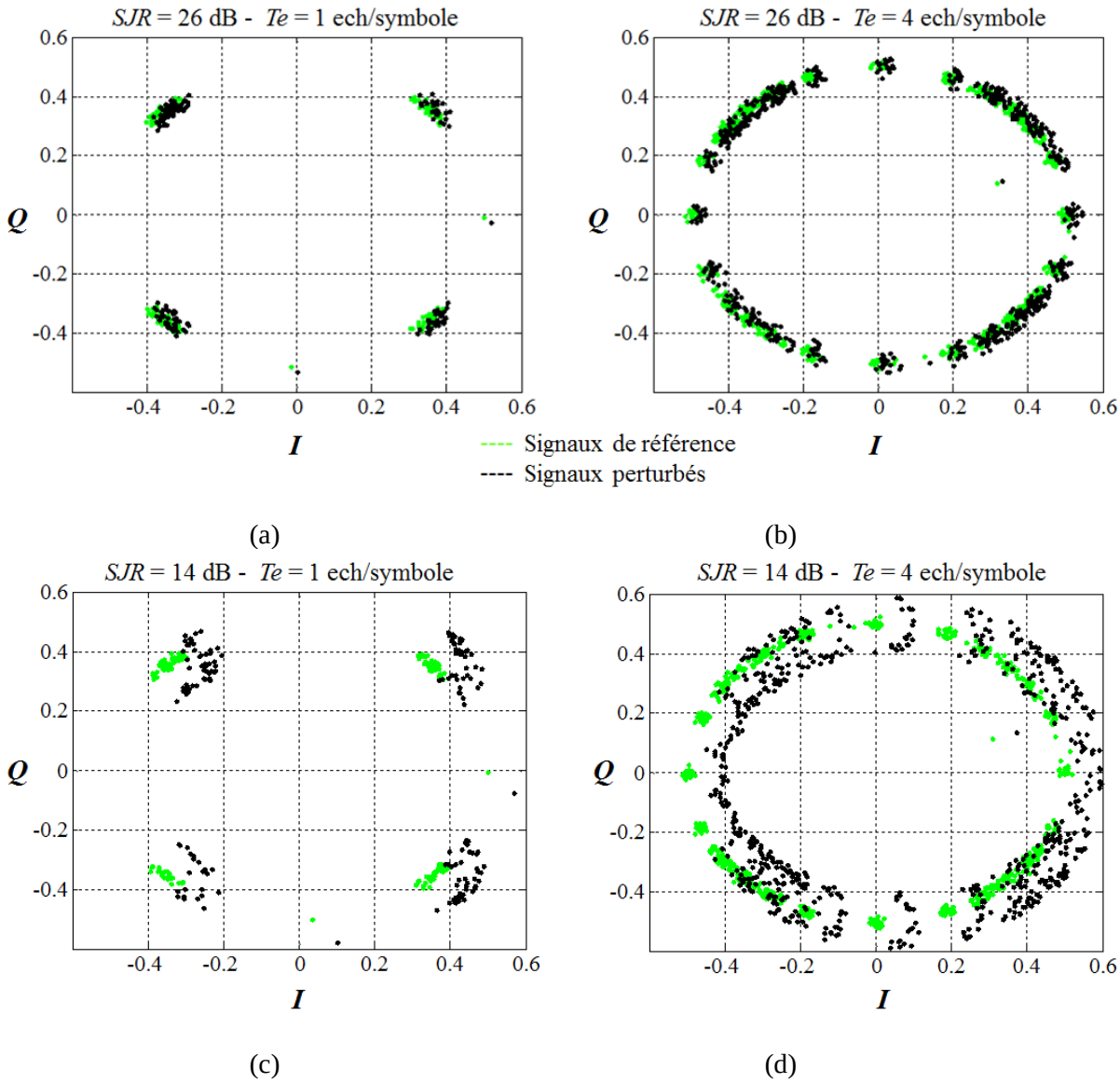


Figure 3.6. Constellations des signaux en quadrature $I(nT_e)$ et $Q(nT_e)$ perturbées avec $G_2(t)$ a : SJR = 26 dB T_e = 1ech/symb, b : SJR = 26 dB T_e = 4ech/symb , c : SJR = 14 dB T_e = 1ech/symb, d : SJR = 14 dB T_e = 4ech/symb, en vert le signal de référence et en noir le signal perturbé (en simulation).

II.1.2. Descripteur 2 : Module de l'erreur vectorielle (*EVM*)

L'*EVM* de l'anglais Error Vector Magnitude est un paramètre couramment utilisé dans les systèmes de communication modernes pour évaluer la qualité de modulation [3.1]. Ce paramètre a pour but de quantifier la qualité du signal de communication que d'autres mesures de performance telles que le diagramme de l'œil ou le taux d'erreur binaire (*BER*) ne couvrent pas.

Le vecteur d'erreur de magnitude mesure la variation entre la forme d'onde de référence et la forme d'onde mesurée. Pour cela, l'*EVM* correspond à la différence vectorielle entre un signal de référence et le signal reçu [3.2]. De cette façon, il représente donc la différence de position entre la représentation quadratique avant canal et après canal de transmission [3.1]. Ceci est illustré en figure 3.7.

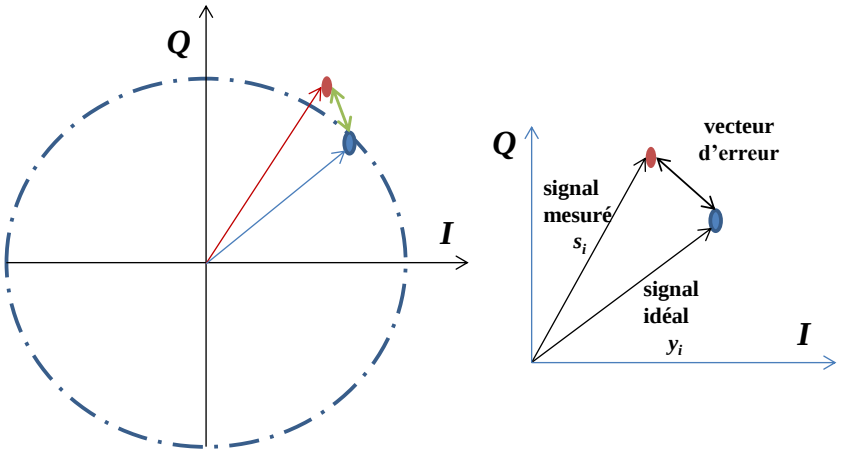


Figure 3.7. Constellation IQ et représentation de l'*EVM*.

L'expression de l'*EVM* est décrite comme suit :

$$EVM = \left|s_n - y_n\right| \text{ avec } \begin{cases} \left\|y_n\right\| = \sqrt{i^2(nT_e) + q^2(nT_e)} \\ \left\|s_n\right\| = \sqrt{I^2(nT_e) + Q^2(nT_e)} \end{cases} \quad \text{(III.2)}$$

où y_n et s_n représentent respectivement le vecteur défini par les composantes $i(nT_e)$ et $q(nT_e)$ pour le signal avant canal et le vecteur défini par les composantes $I(nT_e)$ et $Q(nT_e)$ pour le signal estimé après canal.

Afin de caractériser les propriétés de cette erreur vis-à-vis du signal de référence, on définit l'EVM_{rms}. Cette dernière correspond à la variance normalisée de l'erreur. Elle est estimée sur une durée temporelle équivalente à la durée d'un « *burst* » de 156 symboles pour le GSM-R :

$$EVM_{rms} = \sqrt{\frac{\sum_n \left|s_n - y_n\right|^2}{\sum_n \left|y_n\right|^2}} \quad \text{(III.3)}$$

De par la relation ci-dessous, l'EVM_{rms} caractérise l'état du canal et évolue directement en fonction du bruit superposé à la communication ([3.3][3.4]) :

$$EVM_{rms} \approx \sqrt{\frac{1}{SNR}} \quad \text{(III.4)}$$

Ce paramètre fournit donc une représentation quantitative de l'erreur physique introduite par les perturbations du canal, à la différence du *BER* qui fournit une mesure de qualité de communication.

Au vu de ces propriétés l'EVM_{rms} s'avère un second descripteur pertinent pour la détection d'une attaque électromagnétique vis-à-vis d'un fonctionnement normal d'un système communication, sous hypothèse de canal *BBAG*.

II.2. Modélisation du fonctionnement en mode « normal »

Que ce soit pour l'un ou l'autre des descripteurs étudiés, le principe de la modélisation reste le même. Dans chacun des cas, nous déterminons un modèle statistique génératif permettant de représenter l'environnement électromagnétique en état normal, au regard de différentes réalisations prises par le paramètre $TT(t)$ ou EVM_{rms}. Pour cela, nous posons l'hypothèse que pour un canal de communication *BBAG*, chacun des deux paramètres évolue selon une loi gaussienne régie par une moyenne μ_x et une variance σ_x.

$$p_x(x) = \frac{1}{\sigma_x \sqrt{2\pi}} \exp\left(-\frac{1}{2} \left(\frac{x - \mu_x}{\sigma_x} \right)^2 \right) \quad \text{(III.5)}$$

Pour $x = TT(t)$ la moyenne représente la valeur moyenne du rayon de la constellation et la variance est fonction du bruit du canal *BBAG*. Pour $x = EVM_{rms}$, la variance est également directement liée à la variance du bruit du canal (équation III.4).

Quel que soit le paramètre utilisé, la moyenne et la variance des modèles sont estimées selon le maximum de vraisemblance en utilisant les expressions :

$$\mu_x = E[x] \approx \frac{1}{N} \sum_{n=1}^{N} x(n) \quad \text{(III.6)}$$

$$\sigma_x^2 = E[x^2] \approx \frac{1}{N} \sum_{n=1}^{N} x^2(n) \quad \text{(III.7)}$$

A titre d'exemples, les figures 3.8 et 3.9 présentent respectivement les histogrammes de $TT(t)$ et de l'EVM_{rms} dans le cas de signaux *GMSK* en fonctionnement normal puis perturbé. Les perturbations sont les mêmes que celles définies précédemment pour la figure 3.5 et la figure 3.6, à savoir un signal sinusoïdal $G_1(t)$ (figure 3.8 (a et b) et figure 3.9 (a et b)), et un signal sinusoïdal modulé $G_2(t)$ (figure 3.8 (c et d) et figure 3.9 (c et d)). Pour chaque type de perturbation, deux taux de *SJR* sont appliqués.

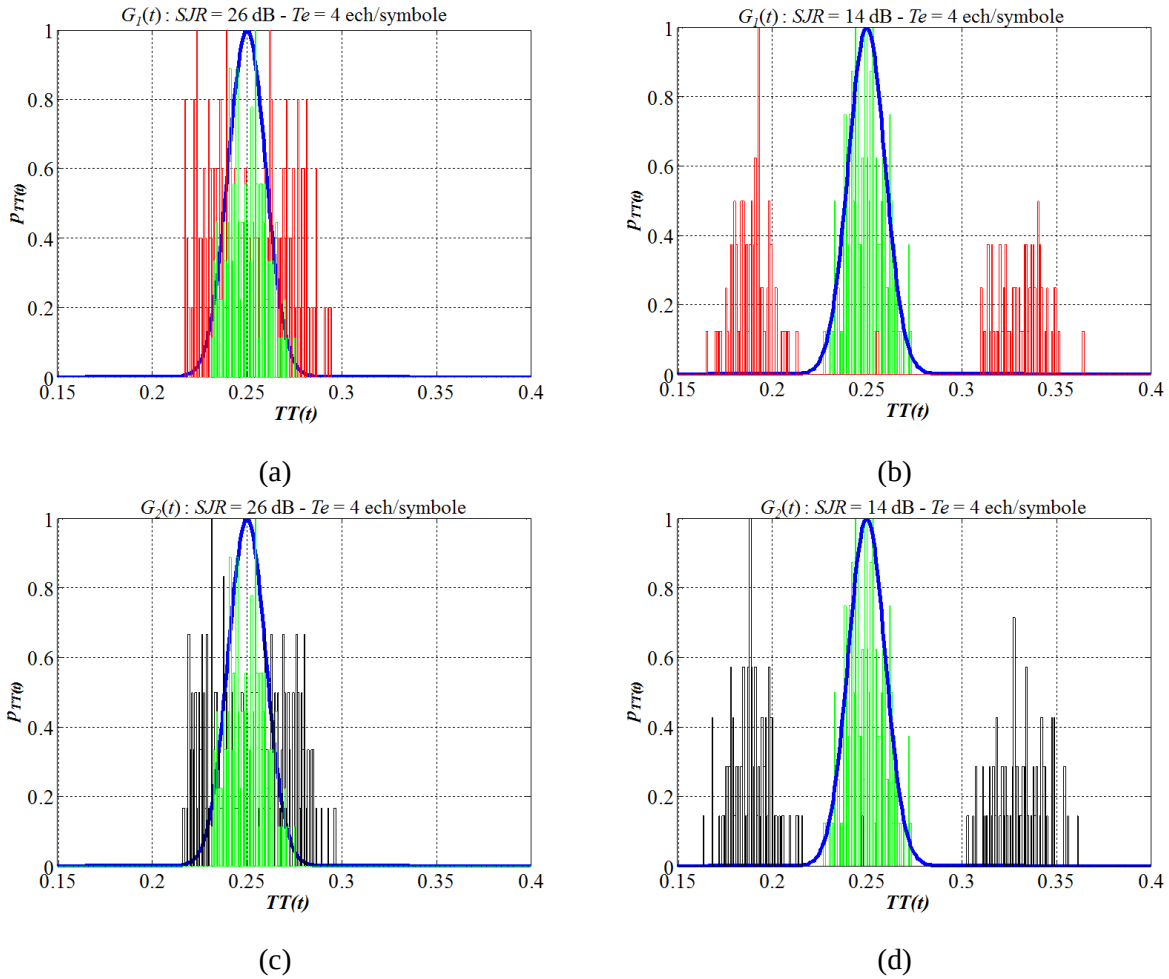


Figure 3.8. Histogrammes de *TT*(*t*) pour le signal de référence (en vert), pour le signal perturbé G_1(t) en rouge a : *SJR* = 26 dB, b : *SJR* = 14 dB, pour le signal perturbé G_2(t) en noir c : *SJR* = 26 dB, d : *SJR* = 14 dB, en bleu l'estimation de la distribution (en simulation).

Nous considérons à chaque fois un canal *BBAG* de *SNR* = 30 dB, avec un *SJR* = 26 dB pour les figures 3.8 (a) et 3.9 (a) et les figures 3.8 (c) et 3.9 (c) et un *SJR* = 14 dB pour les figures 3.8 (b) et 3.9 (b) et figures 3.8 (d) et 3.9 (d).

Comme attendu après la représentation de la constellation en figure 3.5, on note un décalage de l'histogramme des descripteurs perturbés par rapport à l'histogramme du fonctionnement normal. A nouveau le décalage est fonction du *SJR*.

Les deux perturbations affectent la représentation quadratique de la figure 3.3 et produisent des effets différents sur les deux descripteurs. La baisse du *SJR* augmente la variance de l'échantillon central de la constellation mais aussi de ces deux composantes latérales. On voit apparaitre à cause de ces perturbations un effet de décalage mais aussi un effet d'étalement sur les histogrammes. Le décalage est imputable à la puissance du signal perturbateur. L'étalement est lié à la fréquence de modulation.

Sur les histogrammes de la figure 3.8, on note l'apparition de deux modes distincts dont l'écartement est fonction du *SJR*, ceci est visible car le descripteur *TT*(*t*) se base sur un calcul linéaire, directement

sur les échantillons. En revanche l'EVM_{rms} nécessite un calcul plus complexe, supprimant le lien direct entre deux échantillons successifs.

Nous présentons ici les résultats pour des valeurs de *SJR* de 40 dB et 30 dB, car l'impact du brouillage sur ce descripteur est plus significatif, même pour des valeurs élevées de *SJR*.

On remarque sur la figure 3.9 un décalage important de l'histogramme en fonction du *SJR*. On constate pour G_2(t), que les histogrammes sont légèrement plus étalés que pour G_1(t), et légèrement moins décalés, ce qui est dû à la nature de la perturbation.

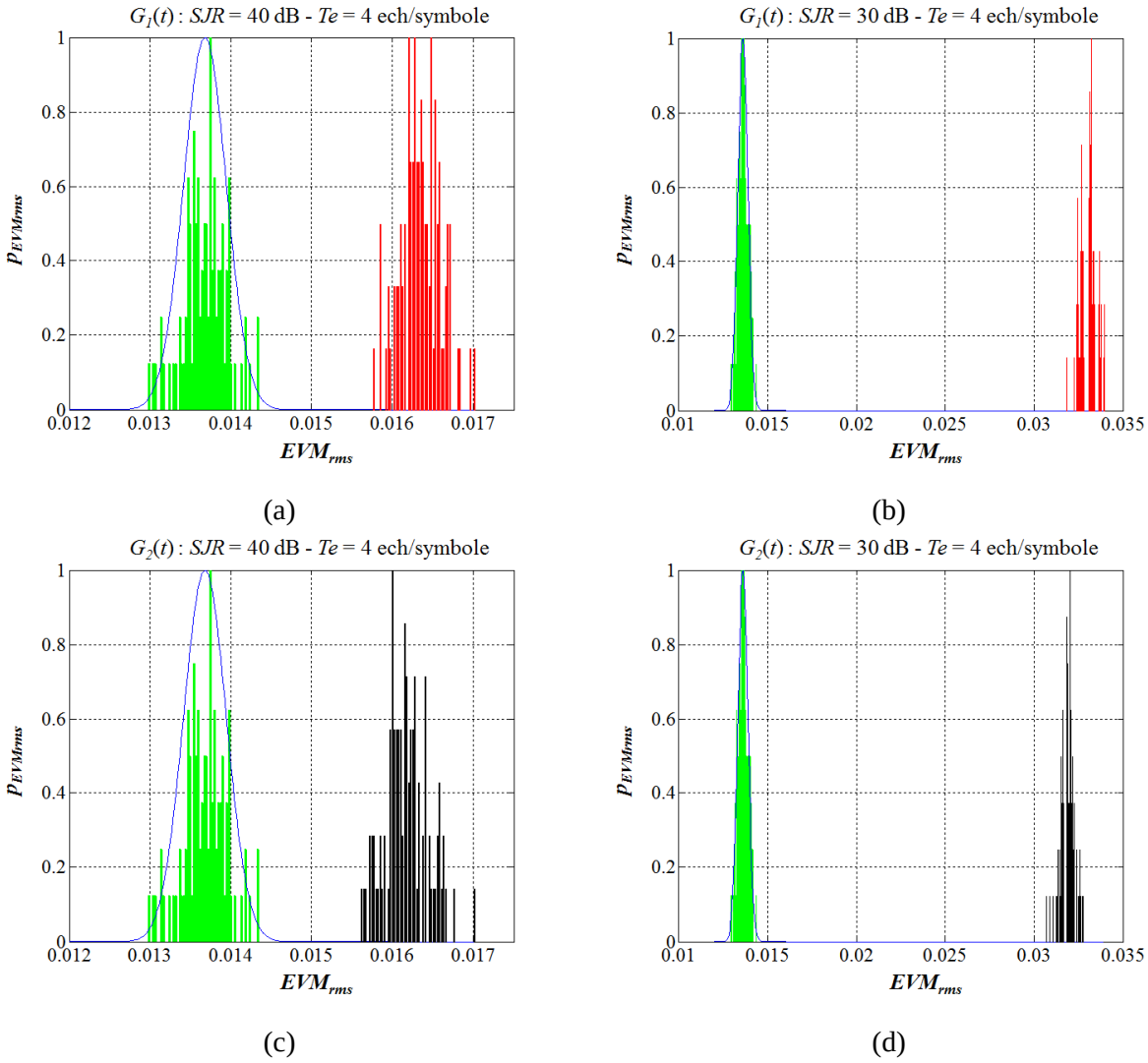


Figure 3.9. Histogrammes de l'EVM_{rms} pour le signal de référence (en vert), pour le signal perturbé G_1(t) en rouge, a : *SJR* = 40 dB, b : *SJR* = 30 dB, pour le signal perturbé G_2(t) en noir c : *SJR* = 40 dB, d : *SJR* = 30 dB, en bleu l'estimation de la distribution (en simulation).

II.3. Détection

Au vu de ces descripteurs et de leurs distributions, nous proposons d'effectuer une détection d'attaques EM en mode supervisé. Par conséquent, il est nécessaire dans un premier temps d'estimer

la distribution du descripteur à partir de bases de données acquises en fonctionnement dit « normal », préenregistrées. Une fois le modèle appris, la détection consiste à évaluer la distribution statistique de chaque nouveau descripteur observé.

Plus le descripteur observé appartient au modèle estimé, plus la valeur de la distribution est élevée. À l'inverse, un descripteur n'appartenant pas au modèle de normalité, fournit une valeur de distribution très faible. Il est donc nécessaire d'établir un seuil de valeur de densité statistique permettant de déterminer la limite de tolérance pour appartenir ou non au modèle. Dans le contexte d'une distribution gaussienne, il est possible de simplifier la mise œuvre de cette détection en déterminant la valeur de descripteur qui fournit cette valeur de seuil. Il suffit ensuite de comparer le descripteur observé à cette valeur de descripteur seuil. La distribution étant symétrique, ce seuil définit un intervalle centré autour de la moyenne de la distribution. En considérant que la valeur de seuil correspond au maximum, et au minimum par symétrie, du descripteur défini par la loi gaussienne estimée, la détection suivra l'expression suivante :

$$Si\ x \in \left[x_{seuilMIN}, x_{seuilMAX}\right] : \text{fonctionnement normal,}$$
$$\text{sinon détection d'attaque } E.M.$$

Avec :

$$\begin{cases} x_{seuilMIN} \approx \mu_x - 3\sigma_x \\ x_{seuilMAX} \approx \mu_x + 3\sigma_x \end{cases} \quad \text{(III.8)}$$

Les deux méthodes de détection qui viennent d'être présentées constituent un bon compromis pour un système de détection temps réel des attaques. Elles permettent intrinsèquement d'intervenir sur une durée très courte au niveau du burst (*EVM*), voire même en dessous de cette durée (*TT*).

La section suivante présente une approche différente de détection des perturbations fondée sur la représentation fréquentielle des signaux. Cette méthode ne requiert pas de synchronisation et utilise une détection des attaques par reconnaissance de forme (classification) de l'environnement EM. En plus de détecter les attaques, elle intègre un aspect de reconnaissance des signaux d'attaque, ce qui la différencie de la méthode précédente exploitant les signaux en quadrature.

III. Détection et reconnaissance d'attaques EM dans l'espace des fréquences

Dans cette seconde partie, nous mettons en place un système de détection d'attaque par reconnaissance de forme. Cette méthode exploite les informations apparaissant au niveau de l'antenne GSM-R et

acquises par l'intermédiaire d'un équipement de mesure associé, un analyseur de spectre par exemple. Elle a pour but d'observer et d'exploiter le contenu spectral dans le cadre de la détection de signaux perturbateurs en utilisant comme descripteur la densité spectrale de puissance (dsp).

Cette seconde approche se base sur les méthodes de classification supervisées utilisant des informations a priori sur l'environnement à étudier. Cela signifie que l'on doit disposer de données spectrales de l'environnement dit « normal » et également de données spectrales de l'environnement dit « attaqué » en présence de divers brouilleurs. L'objectif étant de faire de la détection par classification, ceci revient à reconnaitre un état EM parmi d'autres à partir du flux de données observé. La mise en œuvre d'un tel procédé peut se réaliser en estimant des modèles statistiques génératifs définis pour chaque état de l'environnement état non brouillé, état brouillé avec brouilleur 1, état brouillé avec brouilleur 2, état brouillé avec brouilleur 3. La décision finale se réalise ensuite par les relations statistiques de Bayes à partir de ces modèles.

III.1. Définition des descripteurs spectraux

Soit un signal $s(t)$ issu d'une observation de l'environnement électromagnétique acquis via une antenne GSM-R et l'équipement de mesure associé. Calculée sur une durée temporelle T, la dsp de $s(t)$ est définie par :

$$|s(f)|^2 = s(f)s^*(f) = \int_T s(t)\exp(-j2\pi ft)dt \int_T s(t)\exp(j2\pi ft)dt \qquad \text{(III.9)}$$

où $s(f)$ est la transformée de Fourier du signal $s(t)$ et * représente le conjugué d'une valeur complexe. Dans notre application, la dsp est observée sur une largeur de bande comprise entre une f_{min} et une f_{max}, correspondant à la bande de fréquence d'intérêt du GSM/GSM-R, ici centrée sur 923 MHz. Cette largeur de bande d'observation est obtenue soit directement par la sélectivité fréquentielle de l'antenne, de l'ordre de quelques pourcents de la fréquence centrale, soit par un paramétrage adéquat d'un appareil de mesure, tel qu'un analyseur de spectre fournissant directement la dsp. Cette dernière est communément exprimée en dBm, ce qui correspond au rapport de puissance en décibel entre la valeur mesurée et 1mW. Le descripteur permettant d'analyser au niveau fréquentiel l'environnement électromagnétique est donc un vecteur **S** de M composantes fréquentielles $S(f)$ uniformément réparties entre $f_{\min}$ et $f_{\max}$:

$$S(f) = 10\log_{10}1000|s(f)|^2 \text{ pour } f \in [f_{\min}, f_{\max}] \qquad \text{(III.10)}$$

La figure 3.10 présente des exemples de telles dsp pour M = 1501 avec $f_{\min}$ = 850 MHz et $f_{\max}$ = 1 GHz.

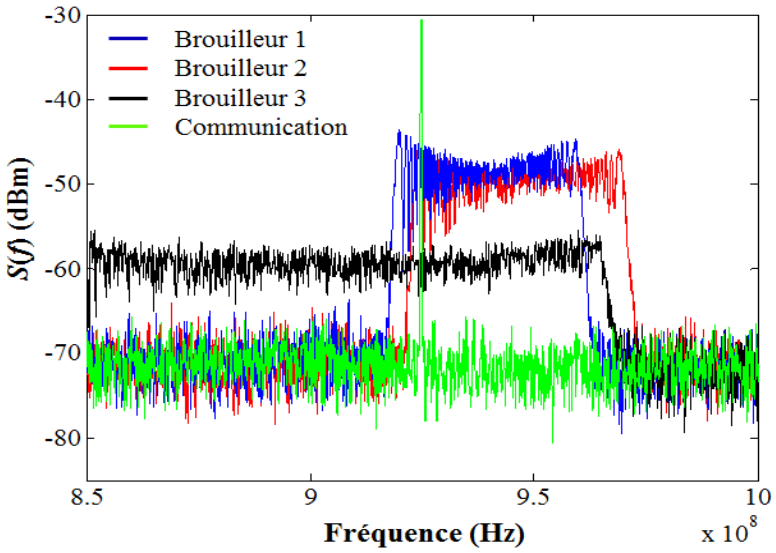


Figure 3.10. Dsp observées pour une communication en présence de trois brouilleurs différents (en mesure).

La figure 3.10 présente différentes allures de dsp de brouilleurs superposées à une communication *GMSK*. On représente en bleu, rouge et noir la dsp de trois brouilleurs distincts, et en vert on observe le signal de communication GSM-R centré dans son canal de 200 kHz. Ces observations sont issues du banc de mesure présenté au chapitre précédent.

Les brouilleurs que nous utilisons présentent la caractéristique d'occuper des bandes spectrales assez larges, ce qui leur permet d'affecter simultanément les liens montants et descendants dans les bandes GSM et GSM-R. Bien qu'appartenant au type A (cf. chapitre 2 section 2.1), ces brouilleurs présentent des caractéristiques fréquentielles différentes, tant par la largeur de bande occupée que par la répartition spectrale des puissances mises en jeu. D'une manière générale, l'allure spectrale des environnements brouillés est clairement différente de celle de l'environnement dit « normal » dans ce contexte d'observation obtenu depuis notre banc de mesure câblé.
En accord avec les mesures faites en laboratoire sur le banc de mesure, on observe les mêmes comportements fréquentiels pour des mesures effectuées cette fois en rayonné. La figure 3.11 montre l'évolution dans le temps de la dsp enregistrée lors d'expérimentations menées sur un quai de gare. Cette figure représente l'environnement EM ferroviaire aux abords de trains, avec le spectre des communications GSM et GSM-R où apparait clairement (observation 750) l'effet du brouillage.

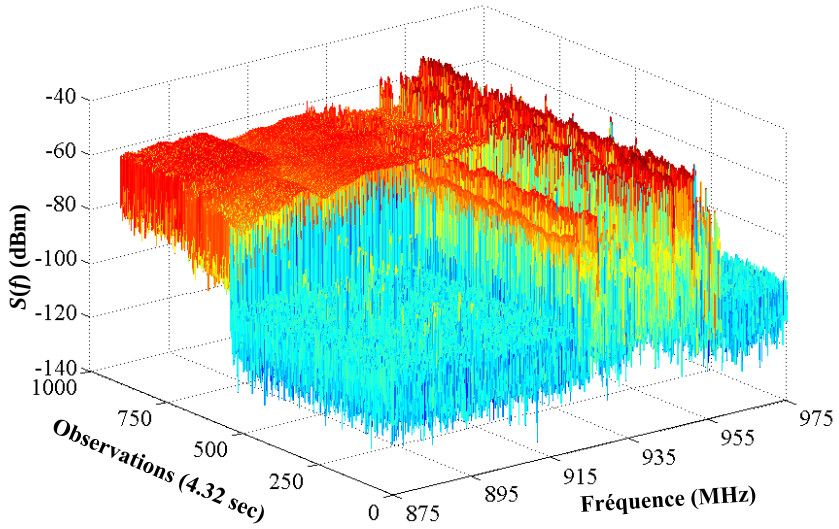


Figure 3.11. Représentations spectrales avec et sans brouillage menées sur un quai de gare (en mesure).

De ces observations, la dsp telle que définie par l'équation III.10 affiche des caractéristiques de discrimination claires entre un environnement brouillé et un environnement « normal », mais également entre différents états de brouillage. En tenant compte de ces propriétés, le descripteur **S** fournit la possibilité d'établir des processus de détection d'attaques EM, mais également de mettre en place des systèmes de reconnaissance des brouilleurs.

Au vu de la figure 3.10 puis, de la figure 3.11, on constate une diversité spectrale dans le sens où chacun des canaux spectraux sont régis par des modèles de distribution différents.

De plus, cette observation est également valable si l'on considère le même canal spectral pour différents environnements (différents brouilleurs) comme le montre la figure 3.12.

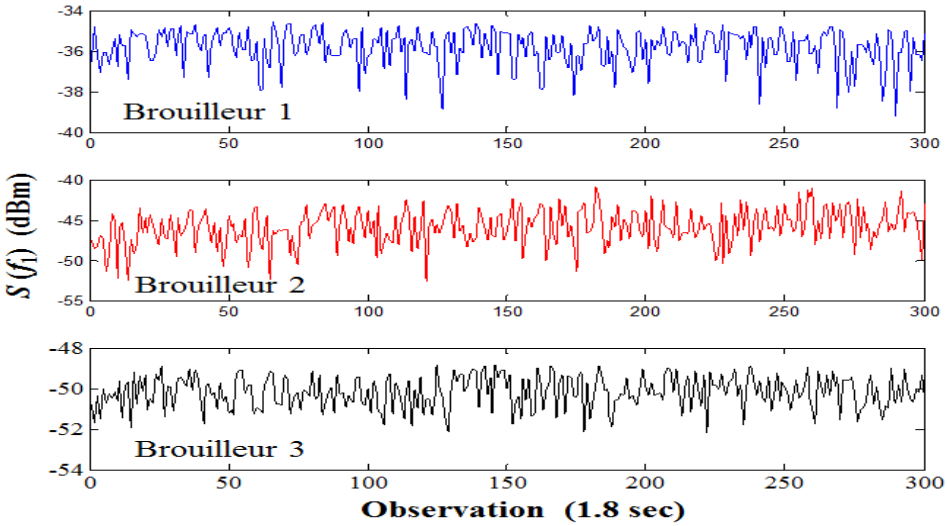


Figure 3.12. Evolution temporelle d'une fréquence observée sur banc de mesure avec f_1 = 924.8 MHz pour les 3 brouilleurs (1.8 sec) (en mesure).

Le descripteur considéré comme un processus stochastique est maintenant défini et brièvement analysé. Ainsi, définir un modèle de « forme » pour la classification revient à définir un modèle statistique pour chacun des environnements à reconnaitre, ce qui constitue l'objet de la section suivante.

III.2. Définition du modèle statistique de la dsp.

Soit **S** une dsp considérée comme un processus stochastique défini par une distribution statistique multi variables $p_s(\mathbf{S})$. En posant l'hypothèse que les M composantes de **S** sont décorrélées, la distribution statistique $p_s(\mathbf{S})$ peut s'exprimer comme étant le produit des distributions marginales de chacune de ces composantes $S(f)$:

$$p_{\mathbf{S}}(\mathbf{S}) = \prod_{f=f_{\min}}^{f_{\max}} p_{S_f}\left(S(f)\right) \tag{III.11}$$

Comme première approche, nous avons défini $p_{Sf}(f)$ par une distribution de loi gaussienne pour chaque fréquence f :

$$p_{S_f}\left(S(f);\mu_f,\sigma_f\right) = \frac{1}{\sigma_f\sqrt{2\pi}}\exp\left(-\frac{1}{2}\left(\frac{S(f)-\mu_f}{\sigma_f}\right)^2\right) \tag{III.12}$$

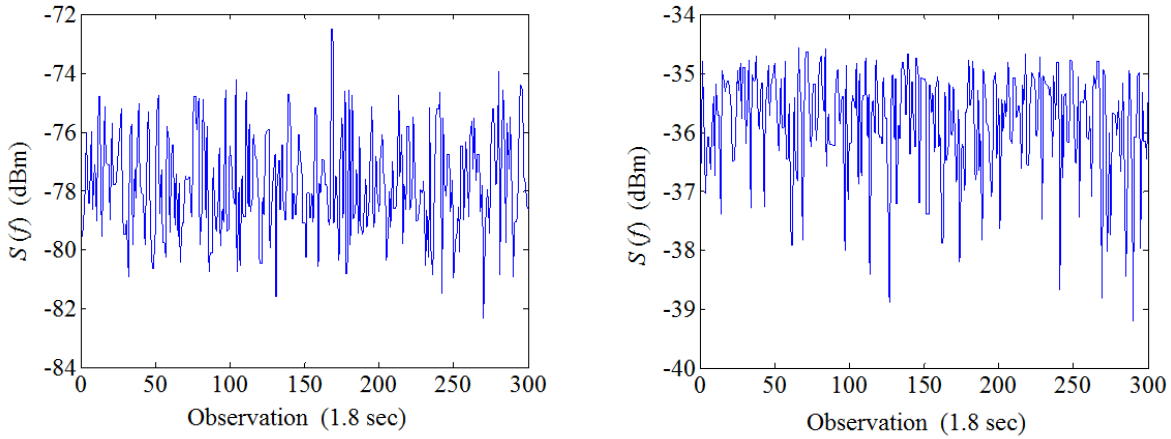
où μ_f et σ_f sont respectivement la moyenne et l'écart type du processus $S(f)$ [3.5].

Les figures 3.13 (a) et (b) présentent 300 réalisations pour deux fréquences respectivement de 912 MHz et de 924.8 MHz pour le brouilleur 1. À partir de la figure 3.10, 912 MHz se situe hors de la bande de brouillage de ce brouilleur 1, et 924.8 MHz dans sa bande. Les figures 3.14 (a) et (b) présentent les histogrammes associés à ces observations.

Considérant la figure 3.13 (a) puis, la figure 3.14 (a), les observations à f = 912 MHz semblent être distribuées selon une loi gaussienne, dans le bruit du canal; mais la figure 3.13 (b) puis, la figure 3.14 (b), montrent que cela n'est pas forcément le cas de toutes les autres fréquences dans les bandes des brouilleurs.

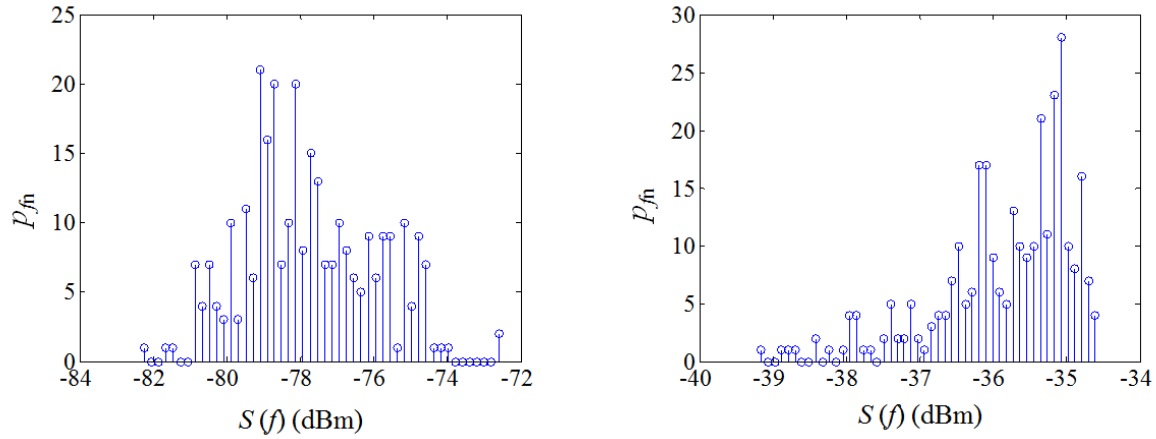
Les observations effectuées à f = 924.8 MHz présentent une répartition dissymétrique autour de leur moyenne. Par conséquent, on peut craindre que la distribution de loi gaussienne (par définition centrée) ne soit pas adaptée à ce type de processus. En effet, théoriquement, la distribution probabiliste définissant une transformée de Fourier (ou une dsp) est définie par une loi de Rayleigh à paramètre complexe (et réel pour une dsp) [3.6], [3.7], [3.8]. Il vient que la distribution d'une dsp exprimée en dB s'apparente alors théoriquement à une distribution de log Rayleigh [3.8]. Cette loi est

dissymétrique avec une queue de distribution plus longue pour les faibles valeurs vis-à-vis des plus grandes. Dans nos observations fortement bruitées (cf. figure 3.13 (a)), les différentes dsp ne suivent pas forcément cette théorie (selon la complexité du contenu de certains canaux et/ou certainement à la présence de non-linéarités existantes dans les appareils de mesure). Nous avons dès lors fait le choix de modéliser chaque canal spectral par une distribution de loi multi-gaussienne. Celle-ci, composée d'une somme de noyaux gaussiens pondérés permet, en fonction de l'estimation des noyaux et de leur poids, de s'adapter aux caractéristiques de chaque canal spectral.



(a) **(b)**

Figure 3.13. Evolutions temporelles de deux fréquences de la dsp S. observées sur banc de mesure, (a) : *S*(*f* = 912 MHz), (b) : *S*(*f* = 924.8 MHz) (en mesure).



(a) **(b)**

Figure 3.14. Histogrammes des 300 observations consécutives observées sur banc de mesure pour a : *S*(*f*=912 MHz), b : *S*(*f* = 924.8 MHz) (en mesure).

La définition de $p_{Sf}()$ dans ce contexte s'exprime par :

$$p_{S_f}(S(f)) = \sum_{g=1}^{G} p_g \mathcal{N}_g(S(f); \mu_{f(g)}, \sigma_{f(g)}) \quad \text{(III.13)}$$

où G désigne le nombre de noyaux gaussiens composant le mélange, $\mathcal{N}_g$ le noyau gaussien d'indice g suivant une loi normale de paramètre $\mu_{f(g)}$ et $\sigma_{f(g)}$ définie comme en équation III.5 et p_g le poids associé à chaque noyau gaussien $\mathcal{N}_g$ sachant que :

$$\forall g \ , p_g > 0 \ et \ \sum_{g=1}^{G} p_g = 1 \quad \text{(III.14)}$$

L'estimation des paramètres p_g, $\mu_{f(g)}$ et $\sigma_{f(g)}$, est réalisée par un algorithme itératif « *Expectation Maximisation* » [3.9] que l'on présentera dans le chapitre suivant, dédié à la mise en œuvre et à l'évaluation des algorithmes de détection, ainsi qu'en annexe 3.
La figure 3.15 présente un exemple de distribution engendrée par une loi multi-gaussienne pour une variable aléatoire arbitraire.

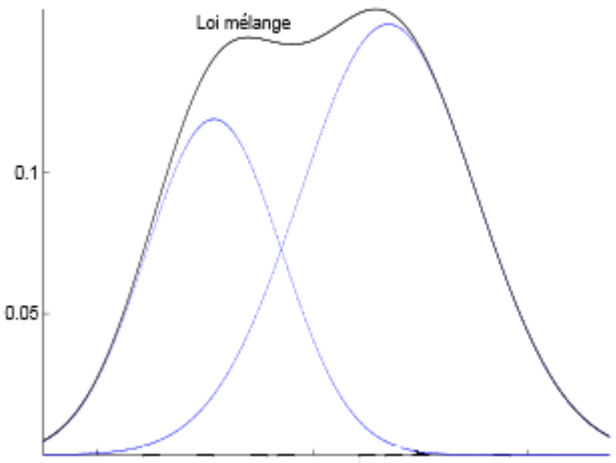


Figure 3.15. Mélange multi gaussien (2 gaussiennes).

Les définitions des paramètres et du modèle statique de la dsp étant maintenant posées, la section suivante présente la phase de détection par classification.

III.3. Détection par classification

Comme nous l'avons déjà vu dans l'espace d'observation IQ, la détection d'un évènement, consiste à détecter une évolution, soit un état particulier, à travers un flux d'observations. La classification consiste quant à elle à classifier, à reconnaitre à travers un flux d'observations des « motifs », des « formes » en essayant d'associer chaque observation à des processus déjà définis, « labellisés » et

connus (méthode supervisée). La méthode proposée ci-dessous exploite pour la détection les principes de la classification en définissant comme classes, les formes spectrales des différents états pris par les dsp. Ces états sont fonction de la présence de divers brouilleurs, mais également de l'état pris par une dsp quand celle-ci est mesurée dans l'état non attaqué, en absence de brouilleur. Ainsi, les processus de détection de brouillage et d'identification de brouilleur se font conjointement en identifiant la classe d'appartenance de la dsp observée.

Nous définissons le nombre de classes K égal au nombre d'états dans lequel peut se retrouver une dsp. K correspond au nombre B de brouilleurs que nous cherchons à reconnaitre, auquel s'ajoute l'état correspondant à l'environnement dit « normal ».

L'environnement normal est un environnement complexe dans le sens où la variation du niveau d'énergie des canaux spectraux est significative. Cette variation dépend de l'état d'exploitation des bandes de fréquence, du lieu et du temps (variation en puissance du bruit et de l'environnement).
Le choix du modèle multi-gaussien devient ici encore plus significatif puisque, outre le fait de pouvoir s'adapter aux diverses distributions des canaux spectraux, l'augmentation du nombre de noyaux gaussiens permettra également de modéliser les différentes variations de chacun des canaux spectraux pour une même classe d'environnement électromagnétique.

La modélisation des brouilleurs constitue une tâche particulièrement difficile au vu des diverses variations spectrales citées ci-avant. La première approche mise en œuvre consiste à modéliser simplement la signature spectrale de chaque brouilleur indépendamment du bruit de l'environnement. Cet exercice présente l'avantage de décrire simplement chaque brouilleur mais possède la faiblesse d'être moins robuste face aux variations de l'environnement. Dans un second temps, nous nous sommes proposée d'enrichir les modèles en apprenant les classes des différents brouilleurs en présence de l'environnement en y incorporant toutes les complexités décrites précédemment. Cette dernière définition des classes retenue présente l'avantage de prendre en considération le bruit environnant, mais aura le désavantage de complexifier les modèles au risque de réduire la capacité de discrimination entre les différentes classes.

Une fois les diverses classes définies et apprises, pour $K = B + 1$ environnement normal, la détection s'effectuera en utilisant un classificateur bayésien.
Soit la distribution conjointe de la dsp $\mathbf{S}$ et d'un état de brouillage k (k appartenant à $[0 : K-1]$, l'état $k=0$ étant posé comme l'état sans brouillage):

$$p(\mathbf{S},k) = p(k)\,p(\mathbf{S}/k) \tag{III.15}$$

où $p(k)$ est la probabilité d'être dans l'état k. La distribution statistique $p(\mathbf{S}/k)$ de **S** sachant l'état de brouillage k, correspond au modèle statistique k connu après un apprentissage des paramètres le définissant et est défini par les équations (équation III.11) et (équation III.12). En posant les équations ci-dessous :

$$p(\mathbf{S},k) = p(\mathbf{S})\,p(k/\mathbf{S}) \tag{III.16}$$

$$p(\mathbf{S}) = \sum_{K} p(\mathbf{S},k)dk \tag{III.17}$$

on aboutit à la probabilité d'être a posteriori dans l'état k sachant l'observation **S [3.10].**

$$p(k/\mathbf{S}) = \frac{p(k)\,p(\mathbf{S}/k)}{\sum_{l=0}^{K-1} p(l)\,p(\mathbf{S}/l)} \tag{III.18}$$

En considérant que chaque état est équiprobable (i.e. $p(k) = 1/K$, pour chacun des états k), le système de reconnaissance d'attaque E.M. maximise l'équation suivante :

$$\hat{k} = \arg\max_{i\in[0,K-1]} \frac{p(\mathbf{S}/i)}{\sum_{l=0}^{K-1} p(\mathbf{S}/l)} \tag{III.19}$$

Cette fonction représente le maximum a posteriori variant entre 0 et 1. A chaque nouvelle d.s.p **S** observée, l'équation III.19 ci-dessus sera évaluée ; l'état k maximisant l'équation III.19 permettra de déterminer si une attaque EM est présente ou non, tout en identifiant conjointement le type de brouilleur potentiellement présent.

III.4. Avantages et inconvénients des deux méthodes

Dans cette section, nous effectuons un récapitulatif portant sur les deux méthodes de détection considérées dans ce chapitre.

Dans une première partie, Nous développons une méthode de détection qui se fonde sur les paramètres quadratiques du système de réception GSM-R. Les deux descripteurs utilisés permettent de détecter la présence de perturbations. La différence de performance entre les deux descripteurs réside en particulier dans le temps de détection. En effet, la méthode basée sur le descripteur rayon $TT(t)$ permet

d'intervenir directement au niveau du bit (3.7 µs) mais notre système de détection peut être formulé afin de détecter la présence de perturbation si celle-ci est présente en analysant un ou plusieurs bits successifs. La méthode avec le descripteur EVM_{rms} quant à elle, ne peut prendre de décision que sur une durée supérieure ou égale à la durée d'un burst, soit 576.6 µs.

Ces deux variantes ont pour intérêt de pouvoir se greffer directement sur le terminal GSM-R en rajoutant seulement un bloc de détection et en traitant les informations en quadrature déjà disponibles dans celui-ci. Elles ne nécessitent donc pas de système annexe complexe. Néanmoins nous ne pourrons effectuer que la seule détection d'activité d'un brouilleur mais en aucun cas procéder à la reconnaissance du type de brouilleur détecté. L'hypothèse de travail forte retenue est également la seule contribution d'un bruit blanc additif gaussien.

De son côté, la seconde méthode développée, exploitant l'espace des fréquences centré dans la gamme d'intérêt, repose sur la détection par classification, ce qui lui permet de réaliser la reconnaissance des perturbations et par conséquent des brouilleurs. D'un point de vue applicatif, elle nécessite l'utilisation d'une antenne supplémentaire ou d'un coupleur et d'un matériel adéquat afin d'acquérir les densités spectrales de puissance dans la gamme de fréquence d'intérêt. Quant au temps nécessaire à la détection, celui-ci dépend du temps de traitement de l'appareil utilisé pour le calcul de la dsp qui peut s'effectuer en temps réel pour les appareils les plus récents.

Nous résumons les avantages et inconvénients des méthodes employées de façon qualitative au moyen du tableau 3.1. Nous avons sélectionné pour élaborer ce tableau les indicateurs Id1, Id2, Id3, Id4, Id5, Id6, Id7 décrits comme suit :

- Id1 : représente le besoin d'opérations supplémentaires nécessaire au calcul des descripteurs.
- Id2 : représente l'aspect complexité de la méthode de détection.
- Id3 : représente le besoin de synchronisation.
- Id4 : représente le besoin d'apprentissage.
- Id5 : représente la propriété de détection.
- Id6 : représente la propriété reconnaissance.
- Id7 : représente la fenêtre temporelle d'analyse.

Tableau 3.1 Avantages et inconvénients des méthodes de détection envisagées

Méthode		Id1	Id2	Id3	Id4	Id5	Id6	Id7
Domaine IQ	TT(t)	non	non	oui	oui	oui	non	3.7 µs (min.)
	EVM_{rms}	oui	non	oui	oui	oui	non	576.6 µs (min.)
Domaine spectral		oui	oui	non	oui	oui	oui	24 ms*

* temps de balayage de l'analyseur de spectre employé par le banc de mesure.

IV. Conclusion du chapitre 3

Durant ce chapitre nous avons décrit de manière approfondie les deux méthodes de détection que nous proposons pour traiter le problème posé. Nous avons commencé par introduire l'architecture du système de détection avant d'exposer les méthodes de détection et de reconnaissance retenues.

Dans un premier temps nous avons décrit le principe de détection dans l'espace des signaux en quadrature.

Nous avons détaillé les signaux extraits de la chaîne de communication GSM-R afin de mettre en avant la représentation en quadrature par les signaux *I* et *Q*. L'étape suivante nous a permis de définir deux descripteurs afin de mettre en œuvre la méthode de détection. Nous avons développé le principe du rayon *TT*(*t*) ainsi que celui de l'*EVM*. A partir de ces deux descripteurs, nous avons décrit le fonctionnement dit « normal ».

Nous avons validé la pertinence de ces descripteurs en présentant leurs histogrammes en situations normale et perturbée. Le processus de détection a été introduit en se basant sur les observations de ces histogrammes.

Dans une seconde partie nous avons introduit une seconde technique de détection fondée sur l'analyse des signaux dans le domaine des fréquences. Nous avons présenté le modèle statistique de détection et d'identification élaboré en utilisant les représentations spectrales des signaux de communication GSM-R en présence ou non de brouillage. Ce second aspect repose sur une modélisation statistique de la densité spectrale de puissance associée aux fréquences en utilisant un classifieur bayésien. Ce descripteur nous a permis de mettre en place la détection par classification. Nous faisons non seulement la comparaison par rapport au fonctionnement normal, mais aussi par rapport aux états appris qui représentent les différentes situations de brouillage.

Finalement, nous avons conclu ce chapitre en comparant les avantages et les inconvénients de chacune des méthodes utilisées.

La mise en œuvre de ces méthodes de détection et les résultats qu'ils procurent sont maintenant détaillés dans le dernier chapitre.

V. Références du chapitre 3

[3.1] T. L. Jensen et T. Larsen, Robust Computation of Error Vector Magnitude for Wireless Standards, *IEEE Trans. on Communications*, vol. 2, no 61, pp. 648-457, 2013.

[3.2] Y. Bayram, J. L. Volalis, S. K. Mayoung, S. J. Doo et P. Roblin , High-power EMI on RF amplifier and digital modulation schemes, *IEEE Trans. on EMC*, vol. 50, no 14, pp. 849-860, 2008.

[3.3] K. M. Gharaibeh, K. G. Gard et M. B. Steer, Accurate Estimation of Digital Communication System Metrics-SNR, EVM and ρ in a Nonlinear Amplifier Environment, *ARFTG Microwave Measurements Conference*, pp. 41-44, 2-3, Decembre 2004.

[3.4] R. A. Shafik, S. Rahman, R. Islam et N. S. Ashraf, On the Error Vector Magnitude as a Performance Metric and Comparative Analysis, *International Conference on Emerging Technologies (ICET)*, pp. 27–31, 13-14, November 2006.

[3.5] R. O. Duda, P. E. Hart et D. G. Stork , Pattern Classification– 2nd edition, John Wiley & Sons, 2000.

[3.6] B. Picinbono, Second-order complex random vectors and normal distributions, *IEEE Trans. on Signal Processing*, vol. 44, no 110, pp. 2637-2640, 1996.

[3.7] J. L. Massey et F. D. Neeser, Proper complex random processes with applications to information theory, *IEEE Trans. on Information Theory*, vol. 39, no 14, pp. 1293-1302, 1993.

[3.8] B. Rivet, L. Girin et C. Jutten, Log-Rayleigh Distribution: A simple and efficient Statistical Representation of Log-Spectral Coefficients, *IEEE trans. on audio, speech, and language processing*, vol. 15, no 13, pp. 796-802, 2007.

[3.9] A. P. Dempster, N. M. Laird et D. B. Rubin, Maximum likelihood from incomplete data via the EM algorithm, *Journal of the Royal Statistical Society, Series B*, vol. 39, no 11, pp. 1–37, 1977.

[3.10] C. P. Robert, The Bayesian Choice: From Decision-Theoretic Foundations to Computational Implementation, Paris: Springer Science+Business Media, LLC, 2007.

Chapitre 4 : Mise en œuvre des outils et évaluation des méthodes de détection

SOMMAIRE

I. Introduction

Dans ce chapitre nous mettons en œuvre les méthodes de détection et, le cas échéant, de reconnaissance de signaux de brouillage EM introduites lors du chapitre 2 puis, précisées lors du chapitre 3.

Pour chacune des méthodes, nous procédons à la mise en place des différentes phases qui nous permettront d'évaluer leur efficacité dans notre contexte de brouillage électromagnétique. Lors des premières sections de ce chapitre nous confrontons les résultats de simulation obtenus depuis nos modèles avec une partie des mesures réalisées en laboratoire sur le banc de test présenté à la fin du chapitre 2. Dans une dernière section, nous présenterons les résultats obtenus en environnement ferroviaire réel.

II. Mise en œuvre de la détection dans l'espace des signaux quadratiques *IQ*

Nous entamons ce chapitre avec la première méthode décrite précédemment qui met en œuvre une détection des attaques EM dans l'espace des signaux *I* et *Q*. Nous utilisons le descripteur $TT(t)$ puis, le descripteur EVM_{rms} afin de procéder aux tests de détection. Nous décrivons les différentes étapes qui nous permettent de mettre en place les tests.

II.1. Méthodologie de travail

Comme nous l'avons précisé dans le chapitre précédent, nous considérons un mode supervisé. Dans le cadre d'une détection supervisée, nous avons besoin de recourir à une première étape qui consiste en une phase d'apprentissage. Après le choix du descripteur, cette première partie du travail est essentielle à la mise en place des modèles décrivant la normalité. Tout descripteur calculé durant cette phase devra être représentatif de ce mode de fonctionnement dit « normal ». Par la suite, le travail de détection consistera à comparer les différents descripteurs obtenus à cet état de référence.

Nous décrirons ceci plus en détails dans la section suivante.

Ainsi qu'indiqué précédemment, pour les descripteurs $TT(t)$ et EVM_{rms}, deux contextes différents sont traités. Le premier concerne la simulation sous Matlab™, le second concerne les mesures réalisées sur banc de mesure. Il est important de noter que pour le second descripteur, les études faites en simulation restent fidèles à l'EVM_{rms} calculé théoriquement selon l'équation III.3 du chapitre 3. En revanche, en ce qui concerne les études faites sur banc, l'EVM_{rms} est estimé.

En effet, l'appareil utilisé pour mesurer l'EVM_{rms}, le FSIQ 7 présenté lors de la description du banc ne possède pas d'information sur le signal de référence. Ceci l'oblige à effectuer une estimation des constellations qu'il sélectionne par la suite comme référence pour toutes ses mesures. Il estime donc l'EVM_{rms} en comparant les valeurs de constellation reçues à celles qu'il a définies initialement en tant que référence. De plus, cette estimation calcule non pas la distance entre le symbole et sa référence mais, selon le processus implémenté par le constructeur, la distance minimale entre le symbole et les trois symboles de référence représentant la constellation *GMSK*. En outre, par comparaison avec l'EVM_{rms} théorique, les valeurs mesurées sur le FSIQ 7 n'intègrent pas de normalisation.

Puisque l'appareil utilise les constellations quadratiques pour le calcul des descripteurs $TT(t)$ et EVM_{rms}, les enregistrements pour la création des bases de données correspondantes peuvent être menés en parallèle, dans la même configuration de communication et, le cas échéant de brouillage.

Le principe de l'apprentissage utilisé dans cette partie de notre travail consiste à étudier la distribution des descripteurs afin de fixer des valeurs seuil délimitant au plus près l'environnement normal. Cet environnement normal est représentatif de conditions définies au départ. Pour définir ces conditions, une première étude est réalisée afin d'évaluer simultanément les effets du *SNR* sur le *BER* et sur l'EVM_{rms}. Cette étude nous permet de sélectionner une valeur de *SNR* réaliste dans l'environnement EM d'essai, que nous pourrons réemployer pour la suite de ce travail.

II.2. Evaluation des paramètres en fonction du *SNR*

Nous commençons par évaluer la variation de l'EVM_{rms} et du *BER* en simulation. Nous faisons varier le rapport signal sur bruit induit par le canal de communication et nous traçons figure 4.1 les courbes d'évolution du *BER* et de l'EVM_{rms}.

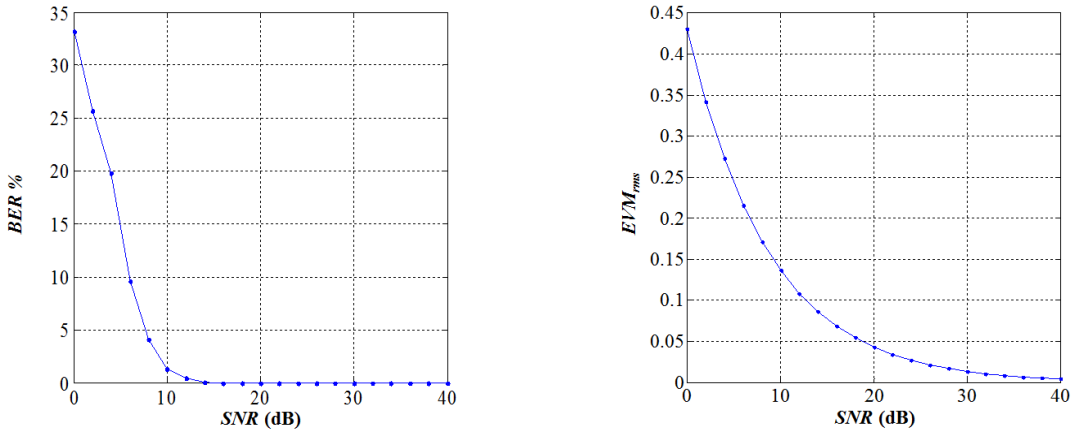


Figure 4.1. Variation du *BER* et de l'*EVM* en fonction du *SNR* (en simulation).

Sur cette figure le *BER* et l'EVM_{rms} sont les résultats d'une moyenne obtenue sur cent tirages. Chaque valeur est calculée en effectuant une moyenne sur les valeurs obtenues pour cent bursts successifs avec un *SNR* fixe.

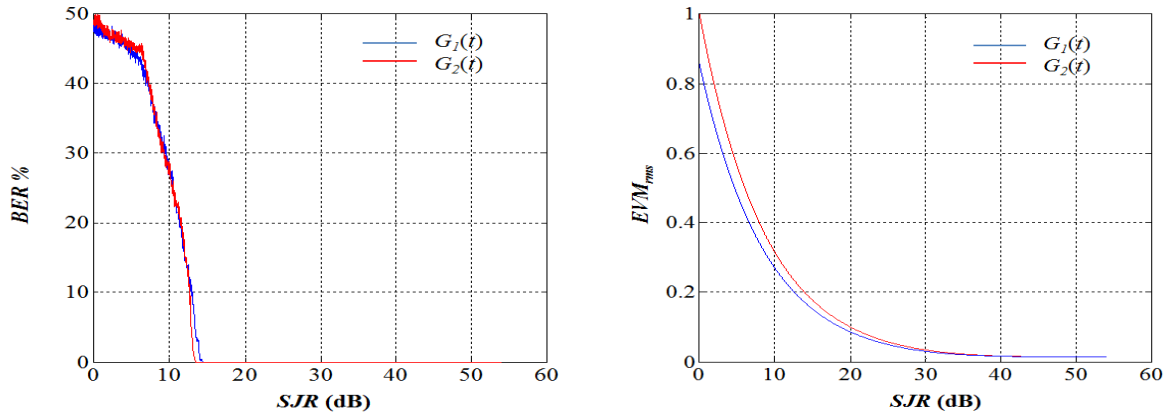
Selon les spécifications GSM, le rapport signal sur bruit minimum à assurer afin d'obtenir une communication efficace est de 9 dB, ce qui correspond, selon les spécifications EIRENE rappelées au chapitre 1, à un niveau minimum de puissance reçue par le récepteur de -95 dBm. Le niveau maximum reçu peut quant à lui atteindre -20 dBm, ce qui conduit à un rapport signal sur bruit atteignant cette fois la valeur importante de 84 dB. Au vu de ces éléments, nous sélectionnons un *SNR* de 30 dB en tant que condition de référence. Dans cette condition de *SNR*, le bruit n'affecte pas significativement la qualité des communications et le *BER* reste pratiquement à zéro. En mesure ou bien en simulation cette valeur de *SNR* nous sert désormais de référence. Afin d'aller au-delà de ce cas particulier représentatif, nous considèrerons toutefois également lors de certains de nos essais un *SNR* de 15 dB, plus proche d'une limite de portée GSM.

Dans la même optique, en fixant la valeur de *SNR* de référence, nous évaluons le *BER* et l'EVM_{rms} en faisant varier le *SJR*. Comme pour le chapitre précèdent, nous utilisons les deux signaux de perturbation $G_1(t)$ et $G_2(t)$ rappelés dans les équations suivantes.

$$G_1(t) = A_1 \cos(2\pi f_c t) \tag{IV.1}$$

$$G_2(t) = A_2 \cos(2\pi f_c t + k\cos(2\pi \Delta f t)) \tag{IV.2}$$

A_1 et A_2 représentent les amplitudes de ces deux perturbations, f_c est la fréquence de la communication *GMSK*, k le facteur de modulation qui est pris égal à un pour notre travail, et Δf la déviation en fréquence. Nous présentons ces résultats en figure 4.2.



(a) (b)

Figure 4.2. Variation du *SJR* avec *SNR* à 30 dB en présence des perturbation $G_1(t)$ et $G_2(t)$ pour a : le *BER*, b : l'EVM_{rms} (en simulation).

Chaque valeur représentée est le résultat d'une moyenne des valeurs calculées à partir de cent bursts successifs, avec un *SNR* de 30 dB et une valeur de *SJR* fixe. Cette évaluation nous servira par la suite pour établir les liens entre les valeurs d'EVM_{rms} et de *BER*. Le but est de pouvoir se référer à ces courbes pour les tests de détection sans avoir à recalculer le *BER*.

En ce qui concerne le *BER*, on constate pour les deux types d'interférence que pour des *SJR* équivalents, la variation du *BER* est similaire, hormis pour les faibles valeurs de *SJR* autour de 10 dB. Pour ce qui concerne l'EVM_{rms}, les courbes d'évolution sont similaires. L'EVM_{rms} de $G_2(t)$ est cependant un peu plus élevé. Rappelons que ce signal d'interférence $G_2(t)$ correspond à un signal modulé en fréquence présent dans le canal de communication. Celui-ci apparaissait déjà plus perturbateur que le signal $G_1(t)$ composé d'un signal sinusoïdal pur centré dans le canal de communication lors des essais expérimentaux initiaux présentés en fin de chapitre 2.
En utilisant ces résultats, nous pouvons établir un lien entre l'amplitude de la perturbation (*SJR*), l'EVM_{rms} et la qualité de la communication.
Après avoir fixé ces paramètres nous construisons maintenant les bases de données.

II.3. Construction des bases de données d'apprentissage

Dans une première étape nous effectuons les enregistrements de données servant à l'apprentissage. Elles nous permettent de fixer les valeurs seuil. Dans la section qui suit nous présentons successivement le travail effectué en simulation puis sur banc de mesure.

- **Simulation**

Nous utilisons le modèle de simulation réalisé sous Matlab™. Le schéma de la figure 4.3 représente la chaîne utilisée pour l'acquisition des données des descripteurs. Celle-ci est similaire à celle présentée lors du chapitre 3. Une trame de 156 bits modulés à la fréquence f_1 = 924.8 MHz est transmise à travers un canal *BBAG* avec un *SNR* de 30 dB (dans notre étude, nous considérons uniquement l'effet du bruit gaussien dans le canal de communication) avec une fréquence T_e de 4 échantillons par symbole.
Nous considérons les bases de données (C1, C'1) qui contiennent les valeurs d'EVM_{rms} et du rayon $TT(t)$, mesurées dans cet environnement de référence à *SNR* élevé.
Ces bases de données sont construites à partir des constellations $I(t)$ et $Q(t)$ recueillies au niveau du démodulateur.

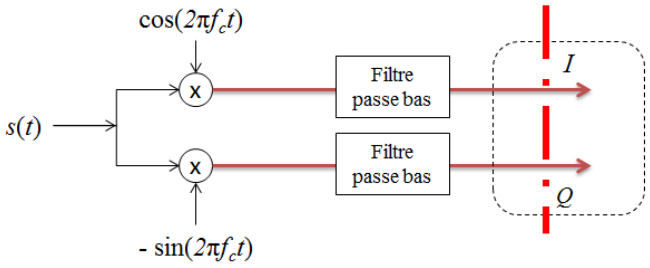


Figure 4.3. Chaîne de démodulation pour l'acquisition des données.

C'1 est constitué de N = 1000 enregistrements de bursts contenant N_a = 624 000 valeurs de rayon $TT(t)$. Cette valeur est obtenue par l'expression suivante : $N_a = (N*T_e)*N_b$, où N_b constitue le nombre de symboles par burst. Dans notre cas nous considérons N_b égal à 156 symboles et T_e égal à 4 échantillons par symbole.

Cela signifie que chaque échantillon de données I(t) et Q(t) contenu dans un burst possède N observations.

En parallèle, C1 contient également N enregistrements de bursts de communication *GMSK*, affectés par le même canal *BBAG* et un *SNR* de 30 dB. Chaque acquisition de cette base correspond à une valeur d'EVM_{rms} calculée sur un burst.

- **Mesures**

Dans cette partie nous utilisons le banc de mesure de la figure 4.4, présenté dans la section VI.1.2 du chapitre 2, où les trames GMSK sont constituées de 148 bits, ne contenant pas les bits de préambule du GSM.

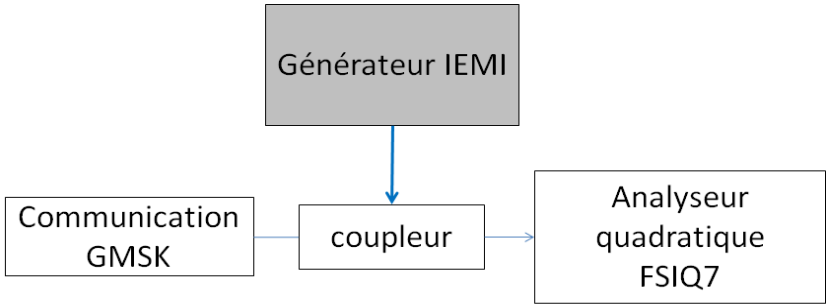


Figure 4.4. Banc de mesure quadratique.

Une trame *GMSK* centrée sur f_1 = 924.8 MHz est transmise en continu avec une fréquence d'échantillonnage de 4 échantillons par symbole. Elle est démodulée par un récepteur quadratique. Nous enregistrons en parallèle les constellations I(t) et Q(t) qui nous permettent de calculer les éléments correspondant aux valeurs de rayon TT(t) et aux valeurs d'EVM_{rms}.

Dans un premier temps nous considérons les données de communication intégrant l'effet du bruit du canal avec un *SNR* de 30 dB afin de créer la base de données de référence M1 pour les valeurs

d'EVM_{rms} et, M'1 pour les valeurs de rayon $TT(t)$. La base de données M1 contient les enregistrements de m = 600 bursts de données, soit m valeurs d'EVM_{rms}. De même M'1 contient les enregistrements de m = 600 bursts, ce qui donne (m*T_e)*N_b valeurs de $TT(t)$ (N_b = 148 bits).

Dans cette phase de travail, l'apprentissage consiste à évaluer les données contenues dans les bases C1 et M1 afin de déterminer l'EVM_{seuil} englobant tous les échantillons. Cette valeur seuil est calculée en utilisant l'équation III.8 présentée dans le chapitre 3.

$$\forall i = \{1, N\}, EVM_{seuil} = \mu_{EVM} + 3*\sigma_{EVM}$$

Pour les données des bases C'1 et M'1, la phase d'apprentissage consiste à déterminer les valeurs seuil des contours de rayon $TT(t)$ maximum et minimum.

$$\forall i = \{1, N\}, \begin{cases} TT_{seuil\min} = \mu_{TT} - 3*\sigma_{TT} \\ TT_{seuil\max} = \mu_{TT} + 3*\sigma_{TT} \end{cases}$$

$TT_{seuilmax}$ et $TT_{seuilmin}$ représentent le contour de rayon maximal et minimal englobant les enregistrements $TT(t)$ et sont utilisés afin de définir le mode de fonctionnement « normal ». Cela implique que tous les échantillons de données se trouvant à l'intérieur de ce contour appartiennent à ce mode de fonctionnement « normal ».

II.4. Construction des bases de données de test

Pour effectuer la phase de test nous considérons les deux signaux de perturbation $G_1(t)$ et $G_2(t)$ introduits précédemment.

- **Simulation**

Les enregistrements des deux descripteurs sont également menés en parallèle. C2 et C'2 correspondent respectivement au mode perturbé par le signal $G_1(t)$ pour les données d'EVM_{rms} puis, de rayon $TT(t)$. De même, C3 et C'3, correspondent respectivement au mode perturbé par le signal $G_2(t)$ pour les données d'EVM_{rms} puis, et de rayon $TT(t)$.
En plus de l'effet du *SNR* constant à 30 dB, les deux sources de perturbation $G_1(t)$ et $G_2(t)$, introduisent un *SJR* variant entre 0 dB et 55 dB, avec un pas de 0.05 dB.

N_1 = 1997 bursts sont utilisés pour chacune des perturbations pour les données de test, ce qui équivaut à N_1 valeurs d'EVM_{rms} pour C2 et également pour C3. Pour ce qui est de C'2 et C'3, chacune contient $N_t = (N_1 * T_e) * N_b$ échantillons de valeur pour $TT(t)$ où N_t = 1 246 128.

- **Mesures**

En laboratoire, nous utilisons un générateur permettant de créer les signaux $G_1(t)$ et $G_2(t)$ qui sont injectés en addition au bruit propre du canal. Chacune des bases de données M2 de $G_1(t)$ et M3 de $G_2(t)$ contient m1 = 1350 enregistrements, qui correspondent aux valeurs d'EVM_{rms} des m1 bursts, dont le *SJR* varie de 0 dB à 55 dB. De la même manière, M'2 et M'3 contiennent $N_m = (m1 * T_e) * N_b$ enregistrements d'échantillons de $TT(t)$ (N_m = 799 200).

Nous pouvons récapituler ces éléments associés aux bases de données dans le tableau 4.1 suivant.

Tableau 4.1 Base de données d'apprentissage et de test en simulation et en mesure.

		EVM_{rms}	$TT(t)$
Apprentissage			
Simulation		C1 (1000 valeurs)	C'1 (624 000 valeurs)
Mesure		M1 (600 valeurs)	M'1 (355 200 valeurs)
Test			
Simulation	$G_1(t)$	C2 (1997 valeurs)	C'2 (1 246 128 valeurs)
	$G_2(t)$	C3 (1997 valeurs)	C'3 (1 246 128 valeurs)
Mesure	$G_1(t)$	M2 (1350 valeurs)	M'2 (799 200 valeurs)
	$G_2(t)$	M3 (1350 valeurs)	M'3 (799 200 valeurs)

II.5. Résultats

En utilisant les bases de données enregistrées, nous réalisons maintenant les tests de détection afin d'évaluer les performances de nos modèles pour les deux descripteurs sélectionnés.

II.5.1. Détection basée sur l'*EVM*

- **Simulation**

Nous évaluons notre modèle de détection en utilisant les bases de données C 2 et C 3, en nous basant sur le fonctionnement de l'organigramme présenté en annexe 2 et, en satisfaisant également l'équation III.8 présentée au chapitre 3.

$$\forall i = \{1, N_1\}, EVM_{rmsi} < EVM_{seuil}$$

Le système de détection identifie l'échantillon et vérifie s'il appartient ou non à l'espace représentant le modèle, soit encore si l'EVM_{rms} calculé est supérieur à l'EVM_{seuil}.

Nous évaluons l'efficacité de détection en fonction du taux de détection. Le tableau 4.2 montre le résultat obtenu. Dans ce qui suit, l'absence de détection signifie qu'un brouilleur est présent mais n'est pas détecté.

Tableau 4.2 Taux de détection sur l'EVM_{rms} des perturbations $G_1(t)$ et $G_2(t)$ pour les bases C2 et C3

Mode	Détection	Absence de détection
C2	99.64 %	0.36 %
C3	99.7 %	0.30 %

Nous obtenons une détection efficace, sans pour autant être maximale pour les deux perturbations utilisées, sans aucune fausse alarme. Rappelons que ce taux de succès est atteint dans ces conditions de simulation optimales où le canal est stable et simplement affecté d'un faible bruit blanc gaussien.
Néanmoins, nous constatons une absence de détection dans certains bursts à partir d'un *SJR* supérieur ou égal à 54 dB, soit très en dessous du niveau de bruit du canal à 30 dB. Ces absences de détection interviennent pour des puissances de brouillage 24 dB en-dessous de celles du canal. $G_2(t)$ est plus perturbateur que $G_1(t)$ et est également un peu mieux détecté (cf. tableau 2.1).
Afin d'étayer ce résultat nous réitérons cet essai en considérant l'environnement de référence avec un *SNR* égal à 15 dB. Avec cette fois un peu plus de bruit présent dans le canal, notre modèle parvient à détecter tous les brouillages et cela pour des valeurs de brouillage 15 dB inférieures à celles du canal, contrairement aux 24 dB précédents.

- **Mesures**

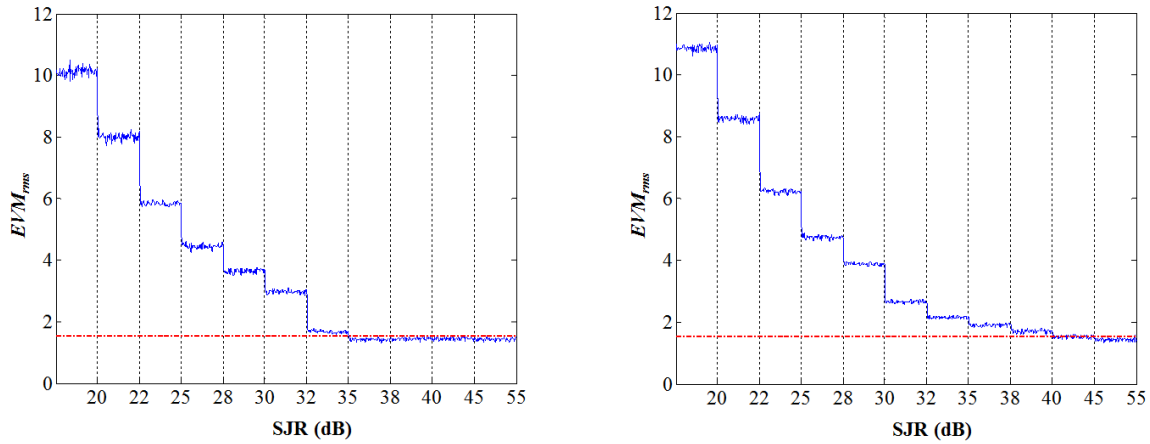
  - **Traitement sur un burst**

En utilisant le banc de mesure en laboratoire et de la même manière qu'en simulation nous testons les données en fonction de l'équation III.8 du chapitre 3. Un *SNR* égal à 30 dB est à nouveau utilisé.
Nous utilisons cette fois les bases de données M2 et M3 créées précédemment afin de déceler la présence des perturbations et d'analyser le fonctionnement du modèle de détection.
Chacune des bases est évaluée et le pourcentage de bonne détection et de non-détection est présenté dans le tableau 4.3. Nous travaillons sur un burst unique ainsi que nous l'avons pratiqué jusqu'à présent.

Tableau 4.3 Taux de détection sur l'EVM_{rms} des perturbations $G_1(t)$ et $G_2(t)$ pour les bases M2 et M3.

Base de données	Détection	Absence de détection
M2	73.33%	26.67%
M3	88.95 %	11.05 %

Pour M2, soit la perturbation $G_1(t)$ constituée d'un signal sinusoïdal pur, la détection est idéale pour des valeurs de *SJR* comprises entre 0 et 35 dB. Elle se dégrade à partir de 35 dB pour conduire à un pourcentage d'absence de détection de 26.67 % dans l'ensemble de la gamme 35 dB à 55 dB étudiée.
Pour M3, la détection s'avère meilleure car le système parvient à détecter les perturbations jusqu'à un *SJR* de 40 dB. Nous perdons pratiquement toute capacité de détection à partir de 40 dB.
Ces résultats sont illustrés figure 4.5. La ligne inférieure horizontale représente le seuil calculé pour la détection.



(a) (b)

Figure 4.5. Observations de l'EVM_{rms} en fonction du *SJR* pour les bases de données : a : M2, b : M3.

Pour $G_1(t)$ la capacité de détection est limitée à un *SJR* au plus égal à 35 dB. Pour ce qui est de $G_2(t)$, la capacité de détection est limitée à un *SJR* au plus égal à 45 dB.

- **Traitement multi bursts**

Afin de tenter d'améliorer la capacité de détection de notre modèle, nous décidons de procéder à la détection non plus sur un burst unique mais, sur plusieurs bursts successifs. Nous employons cinq bursts pour cet essai réalisé uniquement avec le brouilleur $G_2(t)$.
Nous observons les pourcentages des valeurs d'EVM_{rms} représentant 5 bursts successifs supérieures au seuil calculé précédemment.
La figure 4.6, présente les résultats obtenus dans cette configuration. Sur cette figure, nous indiquons par une ligne inférieure horizontale le taux nécessaire à la bonne détection.

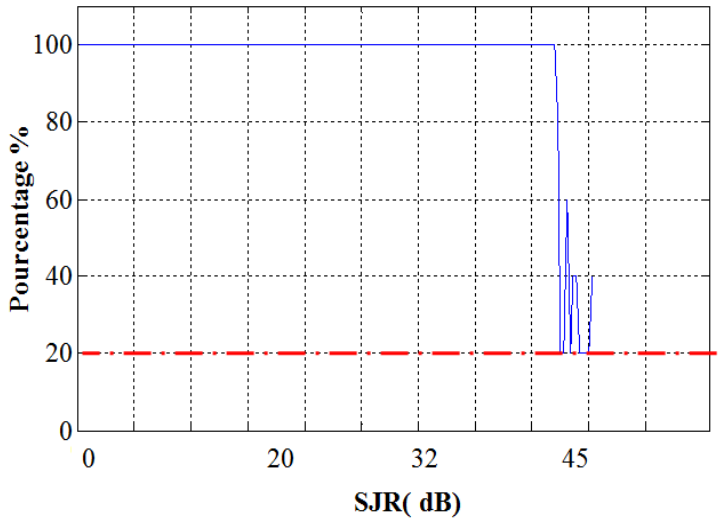


Figure 4.6. Taux de détection d'EVM_{rms} sur une fenêtre de 5 bursts successifs pour la base M3.

Pour cette durée de cinq bursts, on remarque que plus de 20 % des valeurs d'EVM_{rms} sont supérieures au seuil fixé par l'apprentissage. À l'inverse, pour les données de référence, moins de 20% des valeurs sont supérieures au seuil. Cette valeur de 20 % est prise comme limite pour distinguer la situation de référence de la situation brouillée.

Ceci nous permet d'obtenir une détection à 100 % pour un *SJR* allant jusqu'à 45 dB. Ceci améliore notablement les performances de détection de notre modèle.

- **Conclusion**

Dans les conditions de simulation favorables sélectionnées, notre système de détection par EVM_{rms} fonctionne efficacement. Expérimentalement, il révèle quelques limitations auxquelles nous remédions en augmentant le nombre de bursts d'analyse. Rappelons à nouveau la différence que nous avons mentionnée précédemment, concernant le calcul d'EVM_{rms} effectué par simulation et l'estimation mise en œuvre par l'appareil de mesure liée à l'absence de signal de synchronisation.

II.5.2. Détection basée sur le rayon *TT*(*t*)

- **Simulation**

  - **Traitement sur un burst**

Dans cette partie nous introduisons les résultats de détection obtenus en fonction des bases de données enregistrées C'2 et C'3. Le principe repose sur l'organigramme présenté en annexe 3. La détection consiste à satisfaire l'équation III.8 présentée au chapitre 3. Un burst est considéré perturbé si au

moins deux de ces échantillons, non nécessairement consécutifs, se situent à l'extérieur du contour délimité par ($TT_{seuilmin}$,$TT_{seuilmax}$).

$$\forall i = \{1, N_1\}, TT_{seuil\min} < TT_i < TT_{seuil\max}$$

Nous étudions les enregistrements de C'2 et C'3 et, pour chacune des bases, nous relevons le pourcentage de bonne détection et de non-détection. Nous évaluons également l'efficacité de notre modèle par le calcul du taux de fausses alarmes (FAR faux positifs).

Tableau 4.4 Taux de détection par *TT* (*t*) des perturbations $G_1(t)$ et $G_2(t)$ pour C'2 et C'3 si plus de deux échantillons se situent en dehors du modèle.

Base de données	Détection	Absence de détection
C'2	98.84 %	1.16 %
C'3	99.30 %	0.70 %

Les résultats présentés sur le tableau fournissent le taux de détection sur un burst. Dans ce cas, l'absence de détection apparait dans certain bursts à partir d'un *SJR* supérieur à 33 dB. Sachant que le *SNR* utilisé est de 30 dB, la puissance du brouilleur est alors plus faible de 3 dB que celle associée au bruit du canal. Lorsque le signal de brouillage est limité, son impact sur la communication est minime et le *BER* reste nul. Dans ce cas, le brouillage n'affecte pas la communication et l'on peut considérer cette capacité de détection suffisante.

A la différence du descripteur précédent, cette méthode induit plus de fausses alarmes, afin de vérifier cela nous utilisons la base de données C'1.
Comme on peut le noter sur le tableau 4.5, il est toujours possible d'avoir au moins un échantillon en dehors du modèle sans pour autant être en présence de brouillage.

Tableau 4.5 Taux de fausses détections par *TT* (*t*) pour des données d'apprentissages.

Base de données	Bonne détection	Fausses alarmes
C'1	98.5 %	1.5 %

Nous devons adapter le système pour éviter ces fausses alarmes, c'est l'objet de l'étape suivante.

- **Traitement sur les symboles**

Si nous raisonnons à l'échelle des échantillons, et non des bursts, nous obtenons les taux de détection présentés tableau 4.6. Ceux -ci représentent les taux de détection des échantillons perturbés calculés sur la somme des échantillons contenus dans les bases de données.

Tableau 4.6 Taux de détection par *TT* (*t*) des perturbations $G_1(t)$ et $G_2(t)$ pour C'2 et C'3, échantillon par échantillon.

Base de données	Détection	Absence de détection
C'2	86.75 %	13.25 %
C'3	82.56 %	17.44 %

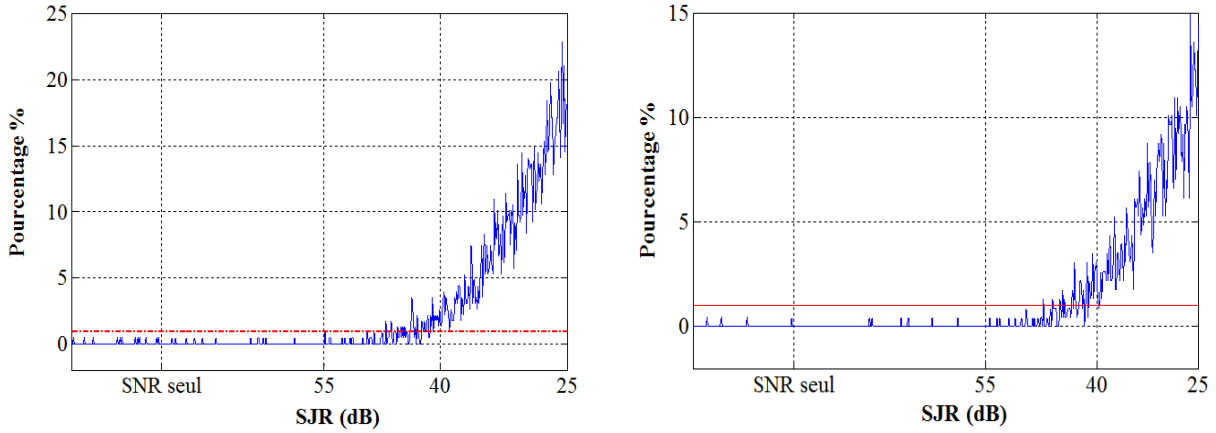
Le faible taux de détection signifie que la perturbation n'affecte pas forcément de la même manière tous les échantillons d'un même symbole.

Dans un premier temps, nous avons procédé à la détection sur un burst. Nous avons considéré que nous étions en présence de brouillage dans le cas ou plus de deux échantillons du burst étaient en dehors du modèle. Cela donne un bon taux de détection mais engendre des fausses alarmes. Par la suite, nous avons établi la détection directement au niveau des échantillons, ce qui a réduit l'efficacité de détection de notre système, mais réduit le taux de fausses alarmes.

Afin d'éviter les fausses alarmes et de perfectionner le système de détection, nous raisonnons maintenant non plus sur un échantillon mais sur un ensemble d'échantillons contenus dans un burst.
Nous avons progressivement augmenté le nombre de symboles pour atteindre une amélioration significative et arriver à une longueur de 57 symboles. Ceci représente le nombre de symboles de données chiffrés et encodés constituant la première partie du burst GSM (cf. figure 2.13).

Dans un mode de fonctionnement « normal », le taux de détection des échantillons représentant ces 57 symboles est inférieur à 1 %.
À partir de cette valeur, si le pourcentage de détection des échantillons sur 57 symboles est supérieur à 1 %, alors nous estimons être en présence d'une perturbation. Cette méthode s'avère applicable pour détecter des perturbations dont le *SJR* est supérieur ou égal à 38 dB pour $G_1(t)$ et 40 dB pour $G_2(t)$. Elle reste efficace car à ce niveau de *SJR* la perturbation demeure sans impact notable sur la communication.

La figure 4.7 représente le taux de détection des échantillons sur une fenêtre de 57 symboles. La ligne inférieure horizontale représente le taux nécessaire à la bonne détection fixé ici à 1%.



(a) (b)

Figure 4.7. Pourcentage de détection par échantillon sur une fenêtre de 57 symboles avec : a :la perturbation $G_1(t)$ et b : la perturbation $G_2(t)$.

Si nous considérons que le *SJR* du brouilleur à détecter est supérieur ou égal à 38 dB, alors nous obtenons une détection à 100% aussi bien pour $G_1(t)$ que pour $G_2(t)$.

- **Mesures**

  - **Traitement sur un burst**

De la même façon que nous avons procédé pour les tests en simulation, nous effectuons les tests de détection depuis les données fournies par le banc de mesure. Nous employons les bases de données M'2 et M'3 afin de déceler la présence des perturbations et d'en déduire le fonctionnement de notre modèle de détection.

Chacune des bases est évaluée et le pourcentage de bonne détection et de non-détection de brouillage résultant est présenté tableau 4.7.

Tableau 4.7 Taux de détection pat *TT*(*t*) des perturbations G_1(t) et G_2(I) pour les bases M'2 et M'3.

Mode	Détection	Absence de détection
M'2	86.28 %	13.72 %
M'3	95.30 %	4.70 %

Dans cette phase initiale, la détection n'est pas parfaite. Les pertes de détection sont obtenues pour des valeurs de *SJR* n'ayant cependant que peu ou pas d'impact sur le *BER*. Les pertes de détection apparaissent à partir d'un *SJR* de 32 dB pour $G_1(t)$, et de 40 dB pour $G_2(t)$.

Nous présentons maintenant dans le tableau 4.8 le taux de fausses alarmes obtenu par cette méthode.

Tableau 4.8 Taux de fausses détections par *TT* (*t*) pour des données d'apprentissage.

Base de données	Bonne détection	Fausses alarmes
M'1	49 %	51 %

En l'état du traitement, le taux de fausses alarmes relevé s'avère très élevé. Ceci signifie qu'il est fréquent d'avoir au minimum deux échantillons par burst en dehors des valeurs seuil. Pratiquer un traitement sur une durée plus longue pourrait améliorer les performances du système. Nous évaluons maintenant le potentiel d'amélioration associé à l'emploi d'une durée plus longue de traitement.

- **Traitement sur les symboles**

De la même manière qu'en simulation, nous présentons les résultats de détection effectués au niveau d'un échantillon. Le tableau 4.9 fournit les taux de détection calculés pour les deux perturbations considérées.

Tableau 4.9 Taux de détection par *TT*(*t*) des perturbations $G_1(t)$ et $G_2(t)$ pour les bases M'2 et M'3 échantillon par échantillon.

Mode	Détection	Absence de détection
M'2	44.58 %	55.42%
M'3	47.30 %	52.70 %

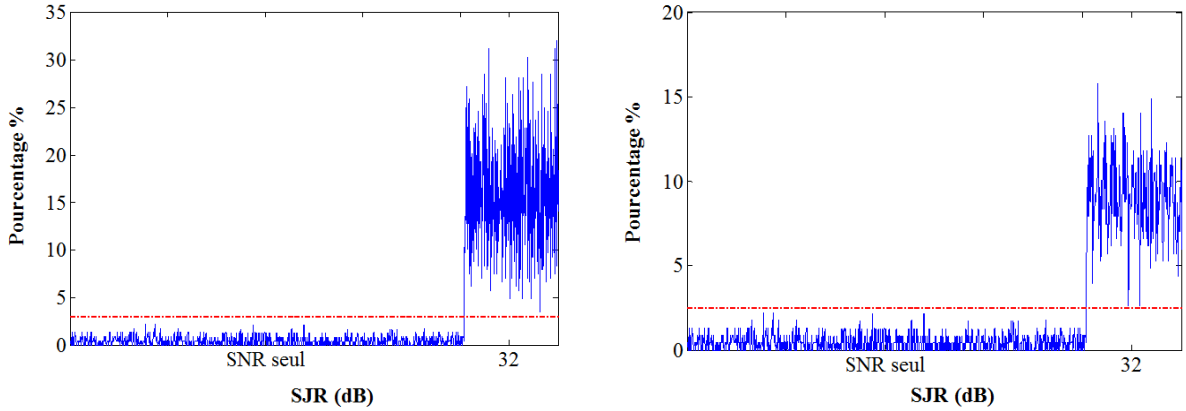
Les résultats présentés traitent les échantillons représentant la totalité de la base de données. En dépit de la présence de la perturbation, il subsiste cependant des échantillons qui respectent le modèle de normalité. À *SNR* constant, on constate que les échantillons ne sont pas tous affectés de la même manière.

Comme précédemment, nous considérons maintenant un traitement sur 57 symboles consécutifs. Ainsi que le montre la figure 4.8, une ligne horizontale délimite les deux fonctionnements et représente la limite sélectionnée pour la détection, sur cette période de 57 bits.

Nous calculons les pourcentages des données contenues dans 57 symboles successifs supérieures au seuil de détection. Nous constatons que pour la base d'apprentissage C'1, moins de 2.5 % des valeurs sont supérieures à ce seuil.

Ainsi nous concluons pour la perturbation $G_1(t)$, qu'à partir de 3 % d'échantillons sur les 57 symboles supérieurs au seuil, nous sommes perturbés. Pour ce qui est de la perturbation $G_2(t)$, nous estimons être perturbés à partir de 2.5 %.

La figure 4.8 illustre ces résultats, nous y présentons les données de la base C'1 ainsi que celles de C'2 et C'3, pour un *SJR* de 32 dB.



(a) (b)

Figure 4.8. Pourcentage de détection de *TT*(*t*) sur une durée de 57 symboles en fonction du *SJR* pour a : la perturbation $G_1(t)$ et b : la perturbation $G_2(t)$.

La limite de cette méthode est qu'elle n'est efficace que jusqu'à un *SJR* de 32 dB. Pour des *SJR* plus élevés, il s'avère difficile de déceler les perturbations.

- **Conclusion**

Dans les conditions de simulation favorables sélectionnées, notre système de détection par descripteur *TT*(*t*) fonctionne également efficacement. Expérimentalement, il révèle quelques limitations auxquelles nous remédions en augmentant le nombre de bursts d'analyse.

Les deux descripteurs présentés précédemment procurent des résultats proches pour des valeurs de *SJR* comparables, ils sont fondés sur la même information physique.

III. Mise en œuvre de la détection et de la reconnaissance d'attaques EM dans l'espace des fréquences

Reprenant la seconde méthode de détection décrite lors du chapitre 3, cette partie étudie les signaux de communication dans l'espace des fréquences. La méthode repose sur la mesure de la densité spectrale de puissance (dsp) **S** du signal des brouilleurs qui peut être modélisée par une fonction de densité probabiliste (pdf). Sur cette base nous essayons de détecter différentes catégories de situation, en les identifiant aux modèles établis.

III.1. Méthodologie

Cette deuxième approche exploite également un mode supervisé requérant une phase d'apprentissage pour la mise en place des modèles.

Pour cette modélisation, nous considérons le seul contexte fondé sur les acquisitions obtenues depuis le banc de mesure décrit au chapitre 2. Comme pour la méthode précédente, nous définissons l'environnement dit « normal » en fixant le *SNR* à 30 dB. Nous utilisons la densité spectrale de puissance des signaux récupérés via l'analyseur de spectre en exploitant les équations présentées chapitre 3.

L'apprentissage est mené dans plusieurs environnements exploitant différents brouilleurs disponibles. Le modèle prend ainsi en considération la communication avec différents niveaux de *SNR* en présence de différents signaux de brouillage potentiels.

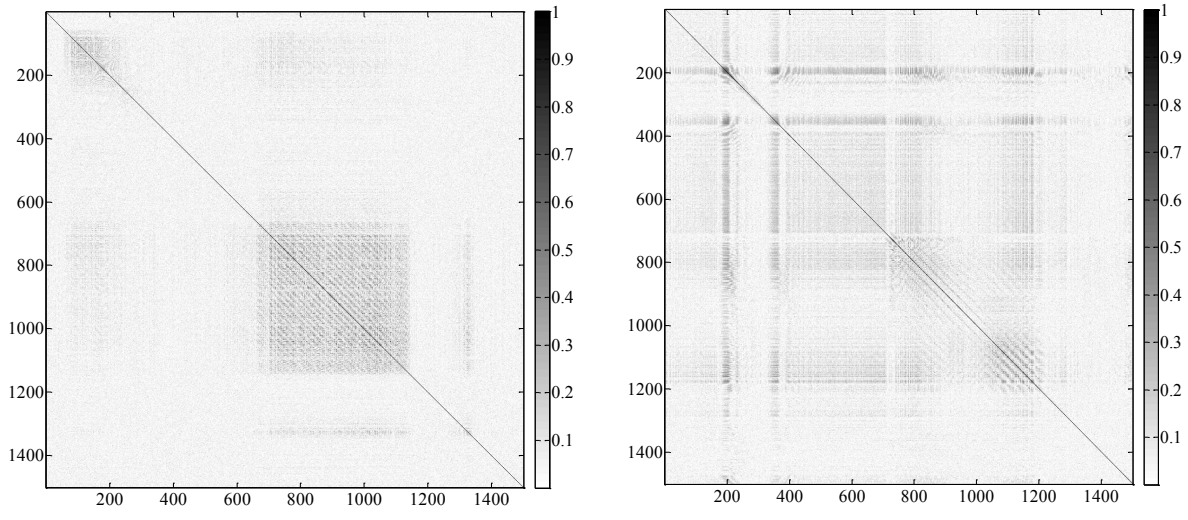
L'étude consiste à modéliser la dsp de chaque fréquence du spectre en fonction de sa pdf, suivant un modèle multi-gaussien.

Nous procéderons par la suite à la construction des bases de test qui serviront à évaluer nos modèles.

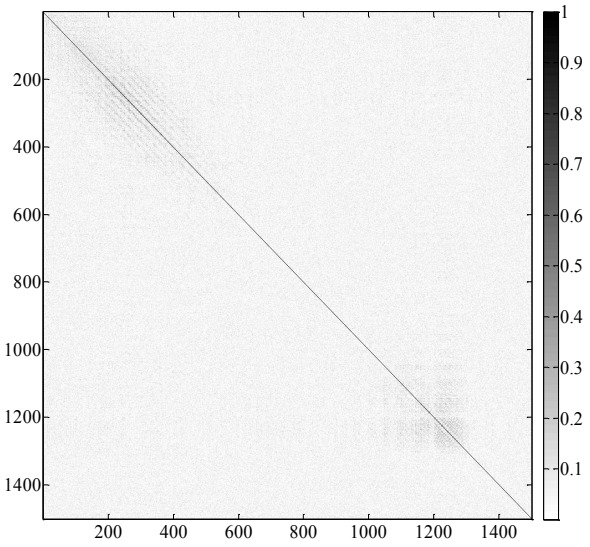
III.2. Conformité de modèles et matrices de covariance

En fonction de l'étude présentée au chapitre 3, notre modélisation repose sur la nécessité d'avoir une bonne décorrélation entre les différentes composantes spectrales pour chacun des brouilleurs. De ce fait, nous présentons dans un premier temps les matrices de covariance obtenues pour chacun des trois brouilleurs utilisés. Ceci nous permet d'étudier la liaison entre les différentes variables fréquentielles.

Dans notre cas nous proposons les matrices sous forme de cartes de covariances normalisées où les coefficients sont représentés par des nuances de gris selon la valeur des coefficients. La figure 4.9 décrit la valeur absolue de la covariance normalisée, ou le noir représente la valeur maximum.



(a) (b)



(c)

Figure 4.9. Matrice de covariances des densités spectrales de puissance pour, a : brouilleur 1, b : brouilleur 2, c : brouilleur 3.

Les matrices sont symétriques et la diagonale toujours remplie de un, car elle représente la corrélation de la variable avec elle-même. Les dimensions des figures sont égales au nombre de fréquences de chaque spectre (1501), et visualisent rapidement s'il existe des liaisons. On constate une bonne décorrélation entre les dsp des différentes fréquences et cela pour les trois différents brouilleurs. Il apparait également quelques corrélations qui peuvent être négligées sans impacter sur la qualité du modèle.

Maintenant que nous avons vérifié la décorrélation entre les dsp des fréquences, nous passons à la création des différentes bases de données.

III.3. Construction des bases de données d'apprentissage

La base de données est constituée des observations de spectre de fréquence pour les différents brouilleurs et dans différentes configurations de *SNR*.

Initialement, nous considérons un premier contexte en présence du signal de communication et en appliquant un *SNR* variable obtenu à l'aide d'un générateur de *BBAG* externe. Un second contexte ajoute un brouillage à puissance fixe, tout en faisant varier la puissance utilisée pour la communication. Les trois brouilleurs disponibles sont exploités.

La base de données utilisée pour l'apprentissage contient 21900 observations enregistrées avec une fréquence d'échantillonnage de 100 ms. Cette base de données peut être subdivisée en quatre parties, s1 contient 5700 observations du spectre de la communication seule, s2 contient 5400 observations du spectre de la communication avec le brouilleur 1, s3 contient 5400 observations du spectre de la communication avec le brouilleur 2 et s4 contient 5400 observations du spectre de la communication

avec le brouilleur 3. Chacune de ces observations couvre les *Nf* = 1501 points de fréquence du spectre allant de 850 MHz à 1 GHz. Cela signifie que chaque fréquence du spectre de chacun des trois brouilleurs fait l'objet de 5400 observations.
Pour cette première partie, nous faisons varier la puissance de la communication entre -24 dBm et -40 dBm, par pas de 2 dB, en prenant 300 enregistrements pour chaque valeur de puissance.
Pour les parties deux, trois et quatre de la base de données nous ajoutons l'effet du brouillage issu respectivement des brouilleurs 1, 2 et 3.

Nous enregistrons, par pas de 2 dB sur le signal de communication, 300 observations pour chaque valeur de *SJR* comprise entre 4 dB et 20 dB pour le brouilleur 1, 6 dB et 22 dB pour le brouilleur 2, 16 dB et 32 dB pour le brouilleur 3. Ces valeurs de *SJR* différentes par brouilleur résultent des écarts de puissance de sortie entre les différents brouilleurs disponibles que nous avions observés dés la figure 2.22.

Nous utilisons cette première base pour estimer les différents paramètres du modèle statistique. Nous estimons les paramètres (la moyenne μ_{fn} et la variance σ_{fn}) du modèle multi-gaussien (cf. figure 3.15) pour chaque situation (brouillée ou non brouillée), pour chacune des fréquences du spectre étudié et pour des modèles utilisant un mélange de une à quatre gaussiennes. Afin de réaliser cet apprentissage nous utilisons les équations de l'algorithme « Expectation Maximisation » présenté en annexe 3.

III.4. Construction de la base de données de test

De la même manière que nous avons procédé pour les bases d'apprentissage, nous construisons les bases de test.
Une première base K1 contient des enregistrements obtenus dans le même environnement qu'en base d'apprentissage. 200 enregistrements sont acquis à chaque fois pour une communication sans brouilleur, avec une puissance variant entre -24 dBm et -40 dBm.
200 enregistrements sont également acquis successivement pour chaque configuration en présence des trois brouilleurs et d'une communication avec un *SJR* variant entre 4 dB et 32 dB. La dernière partie de la base de données contient, pour chacun des trois brouilleurs, 200 enregistrements de leurs spectres émis.
Une deuxième base K2 est construite en renouvelant les opérations effectuées pour la base K1 mais en faisant varier les puissances des brouilleurs. Elles sont atténuées ou amplifiées afin de simuler des atténuations plus au moins importantes des signaux de brouillage lors de leur propagation avant

d'atteindre l'antenne du récepteur. Nous considérons par rapport à la base K1 une atténuation de 10 dB ou une amplification de 10 dB, soit une dynamique de puissance de brouillage de 20 dB.

III.5. Résultats de détection

Nous avons testé la capacité de notre modèle à reconnaître les attaques EM en utilisant les règles de Bayes et les équations présentées dans le chapitre 3. Nous utilisons les bases de données K1 et K2, en appliquant l'équation (III.19) pour estimer la situation (brouillage ou non brouillage) et tenter de reconnaître le brouilleur utilisé.

Nous avons sélectionné le modèle multi gaussien avec G = 3 comme étant le meilleur modèle en termes de résultats de détection et de complexité du modèle. Ce choix est précisé en annexe 3.

Les résultats sont présentés dans les tableaux suivants. Le premier tableau présente les résultats de détection sur une base contenant la communication seule, en fonction du modèle de la communication. Pour le second tableau, les lignes représentent respectivement le $k^{ième}$ brouilleur utilisé (k = 1, 2, 3), tandis que les colonnes indiquent le taux d'identification pour chacun des brouilleurs.

Tableau 4.10 Résultats de reconnaissance de la communication seule à la fréquence apprise avec un modèle multi gaussien G = 3.

Communication seule	**Reconnue**	**Non reconnue**
Reconnaissance	100%	0%
Test OK, le *BBAG* n'est jamais reconnu en tant que brouilleur		

Tableau 4.11 Résultats de reconnaissance de la base de données K1 avec un modèle multi gaussien G = 3.

	***k*=1**	***k*=2**	***k*=3**
k=1	**100%**	0%	0%
k=2	0%	**100%**	0%
k=3	0%	0%	**100%**

Le tableau 4.10 puis le tableau 4.11 montrent d'excellents résultats obtenus par la fonction de reconnaissance lorsque nous utilisons la base de données K1 composée des spectres des trois brouilleurs et des communications. Ce succès est réalisé pour tous les modèles statistiques en intégrant l'effet du TDMA, la présence de bruit seule en absence de communication n'est jamais assimilée à un brouilleur.

Les résultats obtenus à partir de la base de données K2 sont présentés dans le tableau 4.12 et le tableau 4.13.

Tableau 4.12 Résultats de reconnaissance de la base de données K2 avec amplification.

	k=1	**k=2**	**k=3**	**Communication**
k=1	**98 %**	2%	0%	0%
k=2	0%	**100%**	0%	0%
k=3	0%	**100%**	0%	0%
Communication	0%	0%	0%	**100%**

Tableau 4.13 Résultats de reconnaissance de la base de données K2 avec atténuation.

	k=1	**k=2**	**k=2**	**Communication**
k=1	**100%**	0%	0%	0
k=2	0%	0%	0%	**100%**
k=3	0%	0%	0%	**100%**
Communication	0%	0%	0%	**100%**

Dans le cas où la puissance du brouilleur est amplifiée, nous parvenons à détecter la présence des attaques à 100%. Pour ce qui est de la reconnaissance des perturbateurs, nous parvenons à identifier le brouilleur 1 et le brouilleur 2, mais le brouilleur 3 est confondu avec le brouilleur 2.
Nous pouvons expliquer cette non reconnaissance par le fait qu'en amplifiant la puissance du brouilleur 3, nous obtenons une puissance résultante de l'ordre de celle du brouilleur 2 prise pour l'apprentissage. Ceci représente une limitation de notre méthode. Néanmoins, nous décelons systématiquement la présence des perturbations.

Dans le cas où la puissance du brouilleur est atténuée, nous détectons la présence du brouilleur 1 à 100%. Cependant, dans cette situation, nous n'identifions que le brouilleur 1 et la communication. Les brouilleurs 2 et 3 sont confondus avec la communication. Ceci peut s'expliquer par le fait que les puissances des signaux deviennent, après atténuation, en partie noyées dans le bruit, notamment pour le brouilleur 3.

III.5.1. Conclusion

Les modèles statistiques fournissent d'excellents résultats en termes de reconnaissance s'ils sont estimés sur une bande de fréquence suffisamment large, supérieure ici à la bande allouée au GSM-R et avec des puissances de brouilleurs similaires entre brouilleurs et à la puissance du signal de communication. Avec des puissances très différentes, la méthode que nous proposons pour améliorer

la détection, et éviter les fausses alarmes, consiste à effectuer un apprentissage plus large, prenant en compte plus précisément les variations des puissances des brouilleurs.

Ce travail a été effectué dans des conditions de laboratoire contrôlées, c'est à dire en absence de réflexions multiples, du bruit de l'environnement EM complexe du milieu ferroviaire. La section suivante projette d'utiliser ces traitements en environnement réel. Dans ces conditions, les enregistrements composant les bases de données tenteront de prendre en compte cette complexité de l'environnement EM ferroviaire.

IV. Mesures in situ

Cette section regroupe les différents traitements de détection qui ont été élaborés, confrontés cette fois à des environnements réels. Nous décrirons les campagnes de mesure réalisées pendant ce travail de thèse, la configuration utilisée pour caractériser l'environnement ainsi que les bases de données élaborées.

Si les hypothèses et notamment de *BBAG* étaient pleinement satisfaisantes dans le cas de la simulation et dans le cas des essais sur le banc de mesure reliant les équipements par câbles, cette fois, sur le site de mesure réel, l'hypothèse d'un bruit blanc additif gaussien n'est plus totalement valide. Des travaux antérieurs ont été menés afin de caractériser l'environnement EM ferroviaire [4.1], [4.2] et [4.3] et montrent que de nombreux bruits transitoires peuvent en particulier s'avérer présents. Nous proposons toutefois d'exploiter nos modèles existants avec, de ce fait, les précautions qui s'imposent. Les résultats attendus ne seront pas nécessairement idéaux dans cette phase. Une perspective de travail future concerne la prise en compte de cet environnement EM réel issu des travaux antérieurs, riche en perturbations transitoires non intentionnelles à proximité d'une voie ferroviaire.

IV.1. Description de la campagne de mesure

Nous avons fait le choix de réaliser nos mesures le long d'une ligne TGV où le GSM-R n'est pas encore exploité afin de pouvoir procéder aux différents tests, sans risquer d'influer négativement sur le trafic ferroviaire.

Nous nous sommes positionnés le long des voies comme le montre la figure 4.10, sur la ligne reliant Paris à Londres et Bruxelles. A cet endroit circulent des trains TGV, Thalys et Eurostar, souvent à pleine vitesse. La campagne de mesures permettant l'acquisition des données s'est déroulée sur une durée approximative de trois heures. Durant ce laps de temps, de nombreux trains ont circulé sur la

ligne toute proche. Par conséquent, entre le début et la fin de la création de nos différentes bases de données l'environnement EM a évolué notablement.

Le programme d'essai consiste à émettre des trames *GMSK* dans un environnement ferroviaire aux passages des trains et à injecter un signal de brouillage supplémentaire. Cette situation reprend le scénario détaillé figure 2.15 à la section IV.2. du chapitre 2, où le perturbateur serait disposé à proximité d'une BTS.

Figure 4.10. Campagne de mesure le long d'une ligne à grande vitesse.

Dans le cadre ce ces mesures, nous travaillons avec une antenne cornet double ridge à l'émission et une antenne GSM-R à la réception. Le dispositif de brouillage possède sa propre antenne. La figure 4.11 suivante représente les deux antennes utilisées.

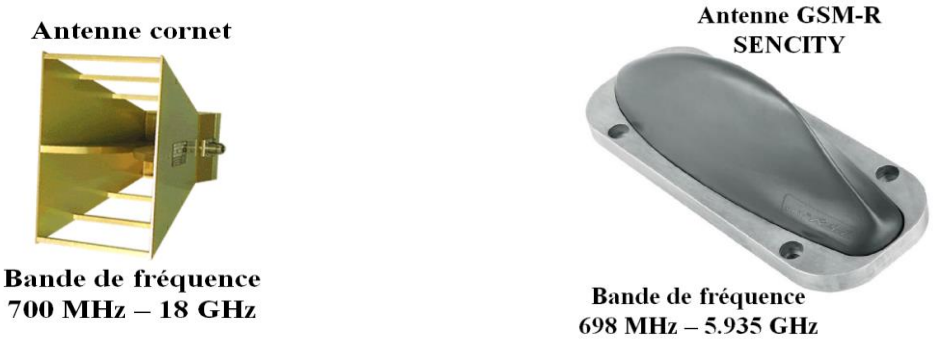


Figure 4.11. Antenne cornet double ridge utilisée à l'émission et antenne GSM-R utilisée à la réception.

Nous fixons une distance de six mètres entre l'émission et la réception et nous disposons le brouilleur à proximité de l'antenne d'émission pour représenter une situation de brouillage à proximité immédiate de la BTS.

IV.1.1. Configuration d'essai dans l'espace des signaux en quadrature

Dans cette partie, nous considérons le même principe que celui retenu en laboratoire, où la trame de communication est transmise par un générateur GMSK Rohde et Schwarz via l'antenne cornet. À la réception, nous utilisons le démodulateur FSIQ 7 déjà présenté qui récupère et démodule le signal issu de l'antenne GSM-R, figure 4.12.

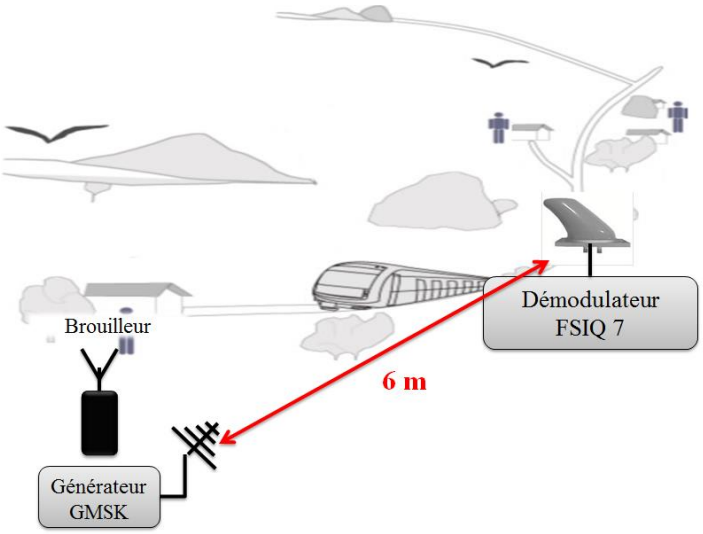


Figure 4.12. Mesures dans l'espace des signaux en quadrature.

Nous utilisons une puissance de 4 dBm transmise par le générateur GMSK à l'antenne. Alliée à une faible puissance du brouilleur, ceci ne perturbe pas fortement l'environnement ferroviaire pour ces essais.

Sur le dispositif de brouillage, nous insérons un atténuateur variable entre le brouilleur et son antenne afin de simuler des pertes d'espace plus ou moins importantes. Le *SJR* résultant varie au niveau de l'antenne GSM-R entre 23 dB et 3 dB.

Comme pour les mesures réalisées en laboratoire, nous procédons à l'enregistrement en parallèle des bases de données contenant les valeurs d'EVM_{rms} et de rayon $TT(t)$.

Pour l'apprentissage, nous utilisons Ap = 150 bursts contenant les mesures de communication seules, cela nous donne Ap valeurs d'EVM_{rms} et (Ap*T_e*N_b) 88 800 échantillons de rayon $TT(t)$.

Les résultats présentés par la suite sont établis sur une base contenant les données de 1200 bursts utilisés pour les tests.

Nous avons Nbr = 870 bursts perturbés donnant Nbr valeurs d'EVM_{rms} et 515 040 échantillons de rayon $TT(t)$. Nous avons également Ncm = 330 bursts correspondant à une communication seule, donnant Ncm valeurs d'EVM_{rms} et 195 360 échantillons de rayon $TT(t)$.

IV.1.2. Configuration d'essai dans l'espace des fréquences

Dans cette seconde partie, nous travaillons dans l'espace des fréquences. Le signal de communication utilisé est également un signal GMSK continu, sans utilisation du protocole GSM.
Nous utilisons le générateur de signaux GMSK avec une antenne cornet à proximité d'un brouilleur. A la réception nous utilisons l'antenne GSM-R reliée à un analyseur de spectre de chez Agilent (MXA 100) permettant de récupérer les spectres des signaux à analyser. La figure 4.13 illustre cette configuration.

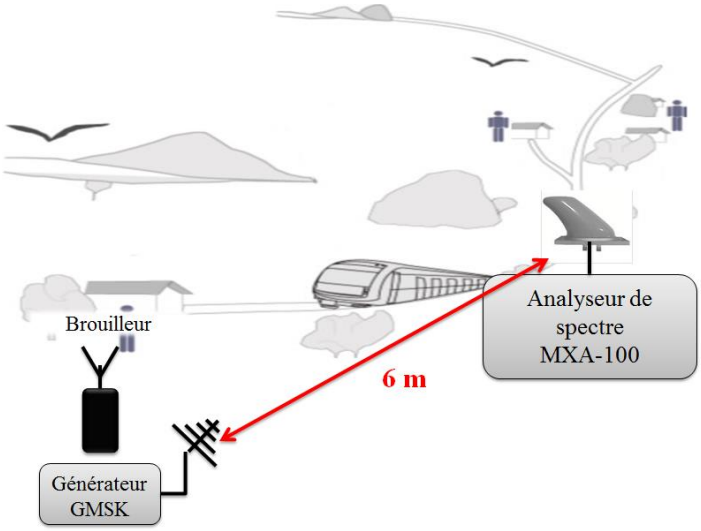


Figure 4.13. Mesures dans l'espace des fréquences.

Nous conservons la même configuration que pour les mesures en quadrature, à savoir 6 m entre l'émission et l'analyseur de spectre, avec une puissance de communication toujours maintenue à 4 dBm.
Nous réalisons les enregistrements avec une largeur de bande de 100 MHz couvrant les fréquences de 875 MHz à 975 MHz, où chaque spectre contient $Nf1$ = 1001 points de fréquence. Deux bases de données sont utilisées, l'une pour l'apprentissage et l'autre pour le test.

Pour la première base de données, qui nous sert pour l'apprentissage, nous considérons deux environnements distincts. Le premier contient 400 spectres représentant l'environnement normal en présence de communication, mais avec ou sans passage de trains. Un second environnement contient les spectres du brouilleur reçus à différents niveaux de puissance, en présence de la communication.

Dans ce cas nous avons effectué l'enregistrement de 600 spectres pour le brouilleur considéré en faisant varier l'atténuateur inséré entre le brouilleur et son antenne, par pas de 10 dB.

Pour ce qui concerne les bases utilisées pour le test nous considérons également les deux environnements suivants, l'enregistrement de 200 spectres représentant la communication seule et 400 spectres supplémentaires représentant l'environnement en présence de la communication et du brouillage variable, dans les mêmes conditions que précédemment décrites.

IV.2. Résultats des tests de détection

Dans la section suivante, nous présentons les résultats de détection obtenus dans l'espace des signaux en quadrature puis, dans l'espace des fréquences.

IV.2.1. Résultats de mesure dans l'espace des signaux en quadrature

En utilisant les bases de données présentées dans la section précédente nous passons à la réalisation des tests de détection pour les deux descripteurs.

IV.2.1.1. Détection basée sur l'*EVM*

En fonction de l'équation III.8 du chapitre 3, nous procédons à la phase de détection des perturbations et à l'analyse du fonctionnement du modèle de détection testé au laboratoire. La figure 4.14 fournit un aperçu de la représentation de l'EVM_{rms} dans notre environnement réel. Le brouilleur est à plusieurs reprises éteint puis, mis en fonctionnement, sa puissance est également modifiée afin de multiplier les conditions d'essai.

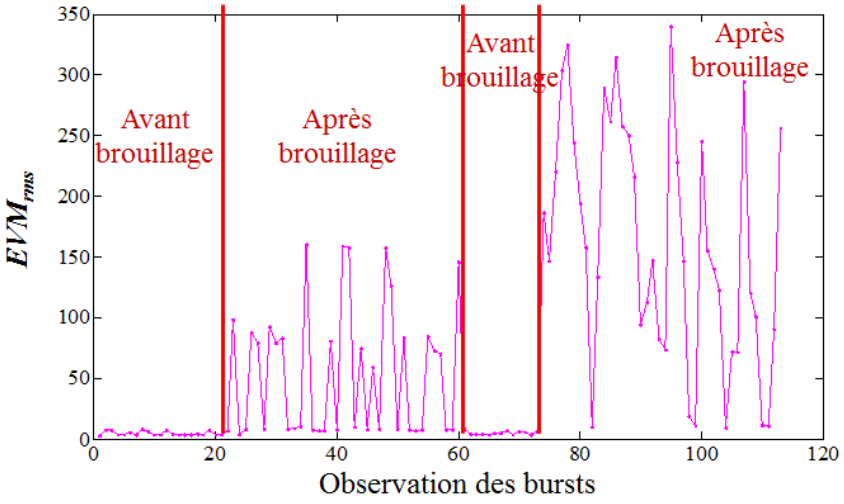


Figure 4.14. Observation en fonction du temps de l'EVM_{rms} des bursts de communication avec et sans brouillage.

➢ **Traitement sur un burst**

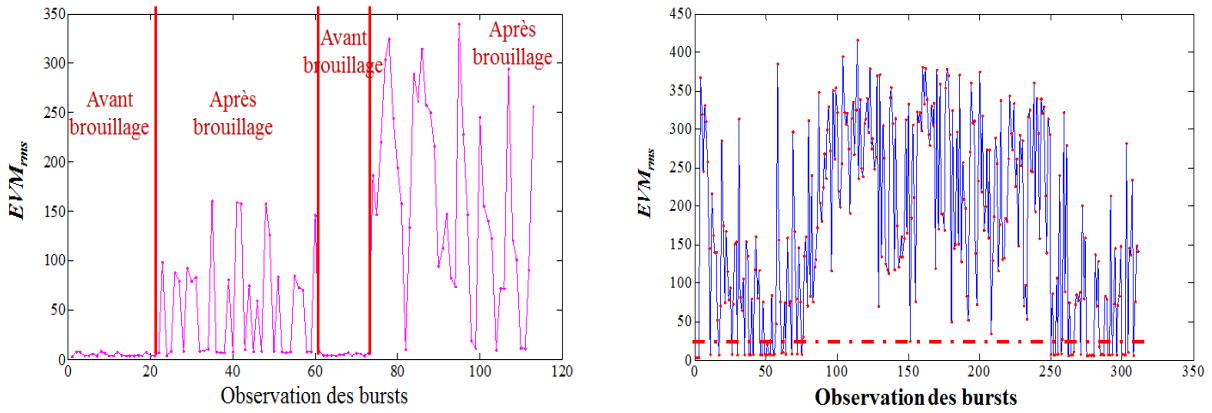
Chacune des bases est évaluée et le pourcentage de bonne détection et de non-détection est présenté tableau 4.14. Nous travaillons dans un premier temps sur un burst unique comme précédemment.

Tableau 4.14 Taux de détection des perturbations par EVM_{rms} sur 1 burst

Mode	Détection	Absence de détection
Perturbé	85.73 %	14.27 %
Mode	Détection	Fausses alarmes
Non perturbé	97.56 %	2.45 %

Nous obtenons un taux de détection qui pourrait être acceptable. Cependant le taux de fausse alarme reste significatif, ce qui dégrade les performances de notre système de détection. Afin d'expliquer ce résultat, la figure 4.15 montre certaines des observations réalisées durant la période d'observation pour les bursts dans deux situations distinctes avec et sans présence de brouillage.

La ligne horizontale qui apparait sur les deux figures représente le seuil calculé délimitant le fonctionnement normal.



(a) (b)

Figure 4.15. Observation de l'EVM_{rms} des bursts de communication, a : sans brouillage, b : avec brouillage.

Que ce soit dans l'environnement normal ou bien brouillé, les valeurs d'EVM_{rms} ne respectent pas systématiquement le modèle choisi. En l'absence de brouillage, certaines valeurs d'EVM_{rms} excèdent le seuil tandis qu'en présence de brouillages, certaines valeurs d'EVM_{rms} sont inférieures au seuil.

En environnement réel, ces fausses alarmes peuvent être imputables aux modifications de l'environnement EM enregistré lors de la campagne de mesure. En particulier, en absence de brouillage, on peut ponctuellement obtenir des valeurs très élevées d'EVM_{rms} qui peuvent être certainement imputables aux perturbations transitoires produites au passage du train.

➢ **Traitement multi burst**

Afin d'éviter ces fausses alarmes nous réalisons notre traitement sur une durée plus longue que celle d'un burst unique. Nous le portons à 8 bursts successifs. Cette durée représente pour le GSM-R la durée d'une trame. Les résultats sont présentés figure 4.16.

Pour étendre la période d'observation, nous considérons le pourcentage d'EVM_{rms} supérieur au seuil de détection sur une durée correspondant à 8 bursts.

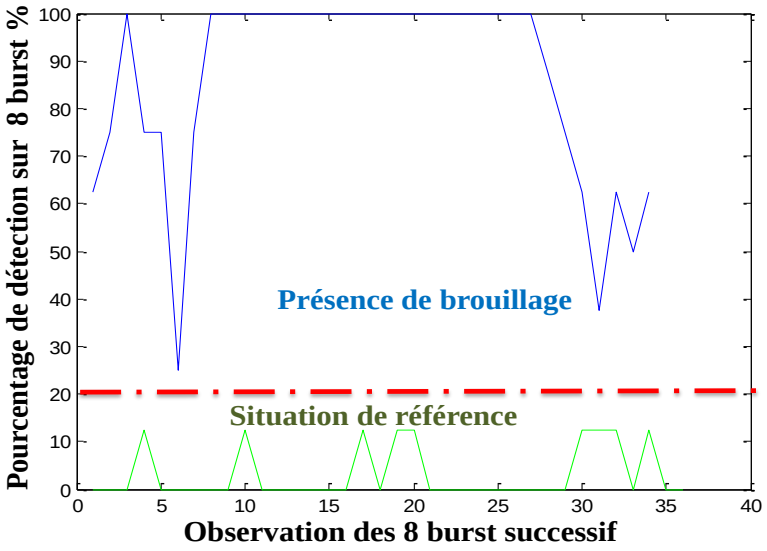


Figure 4.16. Taux de détection d'EVM_{rms} sur une fenêtre de 8 bursts successifs en présence et en absence de perturbation.

Pour l'environnement de référence, moins de 15% des valeurs excédent le seuil calculé. Pour l'environnement perturbé, plus de 25 % des valeurs sont supérieures au seuil de détection.

Ces nouvelles valeurs de 15 % et de 25 % représentent les limites exploitées dans cette configuration à 8 bursts permettant de distinguer la situation normale de celle perturbée et d'éviter les fausses alarmes. Ces seuils nous donnent les résultats regroupés tableau 4.15.

On fixe donc la règle de détection sur 8 bursts à 20 % des valeurs qui dépassent le seuil.

Tableau 4.15 Taux de détection par EVM_{rms} sur 8 bursts

Mode	Détection	Absence de détection
Perturbé	100 %	0 %
Mode	Détection	Fausses alarmes
Non perturbé	100 %	0 %

Ainsi, en augmentant la durée d'observation, nous obtenons une détection parfaite.

IV.2.1.2. Détection basée sur le rayon *TT*(*t*)

De la même façon, nous procédons aux tests de détection en exploitant la technique du rayon. Nous évaluons les bases de données afin de déceler la présence des perturbations et d'en déduire les performances de notre modèle de détection. Cette fois, nous n'avons pas évalué la méthode de détection par échantillons vu les faibles performances obtenues sur les données en environnement contrôlé de laboratoire.

- **Traitement sur un burst**

Chacune des bases est évaluée et le pourcentage de bonne détection et de non-détection de brouillage est présenté tableau 4.16. Nous imposons un minimum de deux échantillons non successifs supérieur au seuil présent dans un burst pour considérer que nous sommes en situation perturbée.

Tableau 4.16 Taux de détection des perturbations sur un burst avec le descripteur *TT*(*t*)

Mode	Détection	Absence de détection
Perturbé	97.56 %	2.44 %
Mode	Détection	Fausses alarmes
Non perturbé	76.20 %	23.80 %

Par rapport à la méthode utilisant l'EVM_{rms}, on note une capacité de détection accrue mais un pourcentage de fausses alarmes beaucoup plus important. On passe ainsi pour le taux de fausses alarmes de 2.45 % avec l'EVM_{rms} à 23.8 % pour *TT*(*t*).

- **Traitement sur un ensemble de symboles**

Nous présentons les résultats de détection effectués au niveau d'échantillons de 5 bursts. En effet, si l'on considère un symbole unique, l'environnement réel est fortement bruité et induit trop de fausses alarmes. Une taille d'échantillons de 5 bursts déterminée empiriquement correspond à un compromis satisfaisant obtenu expérimentalement.

La figure 4.17 fournit la représentation des pourcentages de *TT*(*t*) inclus dans une période de 5 bursts, supérieurs au seuil calculé.

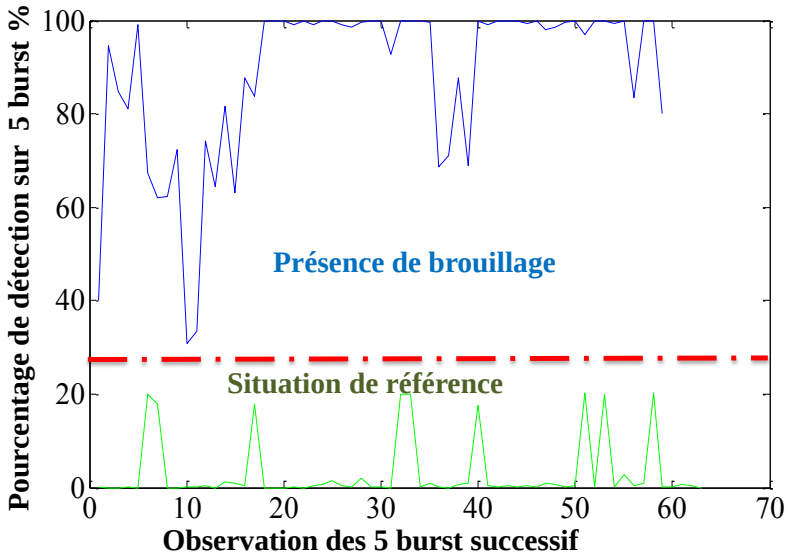


Figure 4.17. Taux de détection de *TT*(*t*) sur une fenêtre de 5 bursts successifs en présence et en absence de perturbation.

Pour la base de référence, le pourcentage des valeurs de rayons supérieures au seuil est inférieur à 15 %. Pour la base brouillée, le pourcentage des valeurs de rayon est quant à lui supérieur à 30 %. Dans ces conditions, en fixant une limite de 25 %, nous pouvons distinguer les deux situations.
Si nous avons plus de 25 % des valeurs contenues dans cette fenêtre de 5 bursts, alors nous sommes dans une situation de brouillage. Dans le cas contraire, nous sommes en situation normale. À partir de ce raisonnement nous obtenons les résultats présentés tableau 4.17.

Tableau 4.17 Taux de détection sur 5 bursts avec le descripteur *TT*(*t*)

Mode	Détection	Absence de détection
Perturbé	100 %	0 %
Mode	Détection	Fausses alarmes
Non perturbé	100 %	0 %

Nous obtenons une détection parfaite comme dans le cas précédent exploitant l'EVM_{rms}.

L'étude présentée dans cet environnement ferroviaire réel confirme les résultats obtenus en laboratoire. Le descripteur *TT*(*t*) fournit une détection parfaite dès l'exploitation de 5 bursts successifs. Le descripteur EVM_{rms} délivre une détection parfaite dès l'exploitation de 8 bursts successifs. L'EVM_{rms} constitue toutefois un critère de qualité largement employé en télécommunication, souvent implémenté sur les récepteurs.
Notre recommandation est d'utiliser ce paramètre EVM_{rms} et de l'étendre à la détection de brouillage.

IV.2.2. Résultats de mesure dans l'espace des fréquences

De la même manière qu'en laboratoire, nous testons la capacité de notre modèle à identifier les situations d'attaques EM par cette méthode dans l'espace des fréquences.

Nous utilisons cette fois les bases de données enregistrées sur site pour identifier la situation dans laquelle on se trouve de type brouillage ou non brouillage.

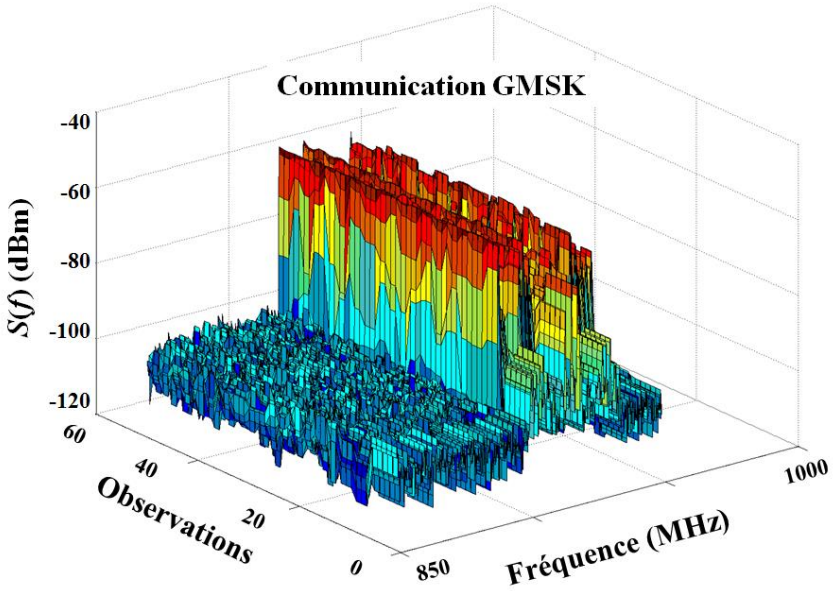
Afin d'être en accord avec les tests effectués en laboratoire nous considérons un modèle multi gaussien avec $G = 3$.

Nous présentons les résultats de détection dans le tableau 4.18.

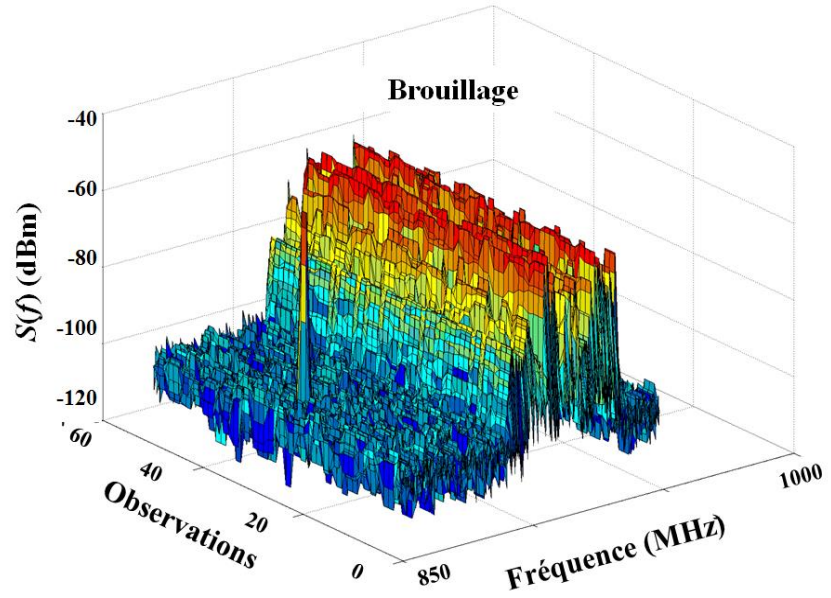
Tableau 4.18 Taux de détection en utilisant un modèle multi gaussien avec G = 3.

Mode	Détection	Absence de détection
Perturbé	100 %	0 %
Mode	Détection	Fausses alarmes
Non perturbé	20 %	80 %

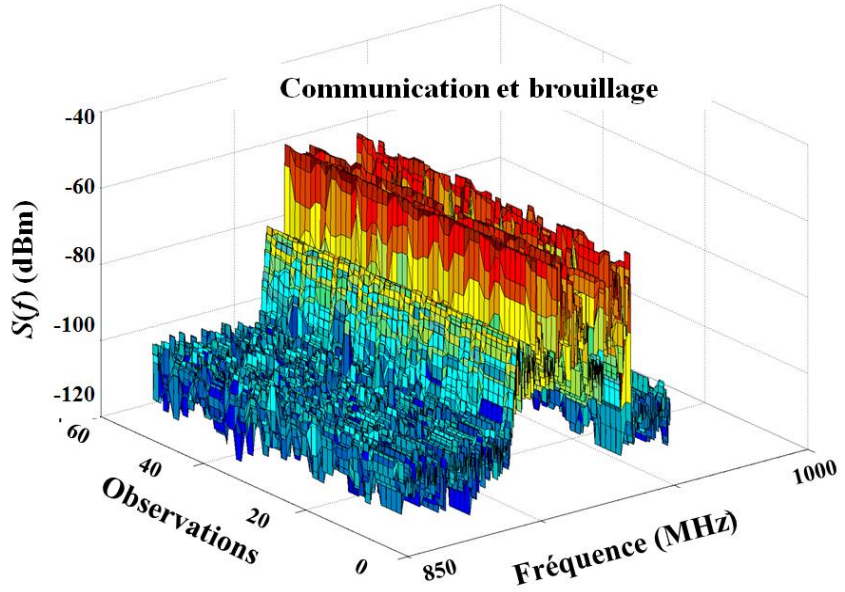
Nous obtenons sur ce tableau un taux de détection parfait dans le cas où nous avons un brouillage. En absence de brouillage, nous obtenons toutefois de nombreuses fausses alarmes. Ceci est probablement imputable à la variation rapide de l'environnement EM de mesure et au caractère non parfaitement gaussien du bruit affectant le canal de propagation. Cela peut être du au fait que le brouilleur ne couvre que les fréquences du downlink et à la forte occupation de cette bande par les communications *GSM*. il est donc difficile de distinguer les spectres du brouilleurs de celui lié aux communication, comme le montre la figure 4.18.



(a)



(b)



(c)

Figure 4.18. Représentations spectrales de l'environnement de mesure avec, a : la communication *GMSK*, b : le brouillage, c : la communication et le brouillage.

Une durée d'apprentissage plus longue ainsi, qu'un nombre de gaussiennes plus élevé pour représenter le modèle, permettrait probablement de pallier une partie du problème, au prix d'un temps de calcul plus élevé.

Nous terminons ce chapitre par le tableau 4.19 et le tableau 4.20 qui récapitulent l'ensemble des résultats. Le premier traite des deux descripteurs quadratiques, le second porte sur les résultats obtenus dans l'espace des fréquences.

Tableau 4.19 Résumé des taux de tests de détection dans l'espace des signaux quadratiques.

❖ **Simulation**				
• **Fausses alarmes**				
FAR	EVM_{rms}		$TT(t)$	
	Pas de fausse alarme		1.5 %	
• **Traitement sur un échantillon**				
Sur 1 échantillon	EVM_{rms}		$TT(t)$	
			Détection	Non détection
$G_1(t)$	Impossible		86.75 %	13.25 %
$G_2(t)$			82.56 %	17.44 %
• **Traitement sur un burst**				
Sur 1 burst	EVM_{rms}		$TT(t)$	
	Détection	Non détection	Détection	Non détection
$G_1(t)$	99.64 %	0.36 %	98.84 %	1.16 %
$G_2(t)$	99.70 %	0.30 %	99.30 %	0.70 %
• **Traitement multi symboles**				
Sur 1 burst	EVM_{rms}		$TT(t)$	
$G_2(t)$ et $G_2(t)$	Pas besoin		57 symboles	
❖ **Mesures au laboratoire**				
• **Fausses alarmes**				
FAR	EVM_{rms}		$TT(t)$	
	Pas de fausse alarme		51 %	
• **Traitement sur un échantillon**				
Sur 1 echantillon	EVM_{rms}		$TT(t)$	
			Détection	Non détection
$G_1(t)$	Impossible		44.58 %	55.42 %
$G_2(t)$			47.30 %	52.70 %
• **Traitement sur un burst**				
Sur 1 burst	EVM_{rms}		$TT(t)$	
	Détection	Non détection	Détection	Non détection
$G_1(t)$	73.33 %	26.67 %	86.28 %	13.72 %
$G_2(t)$	88.95 %	11.05 %	95.30 %	4.70 %
• **Traitement multi symboles**				
Sur 1 burst	EVM_{rms}		$TT(t)$	
$G_1(t)$ et $G_2(t)$	5 bursts		57 symboles	
❖ **Mesures sur site ferroviaire**				
• **Fausses alarmes**				
FAR	EVM_{rms}		$TT(t)$	
	2.45 %		23.80 %	
• **Traitement sur un burst**				
Sur 1 burst	EVM_{rms}		$TT(t)$	
	Détection	Non détection	Détection	Non détection
Perturbé	85.73 %	14.27 %	97.56 %	2.44 %

• **Traitement multi bursts**		
Sur 1 burst	EVM_{rms}	$TT(t)$
Perturbé	8 bursts	5 bursts

Tableau 4.20 Résumé des taux de test de détection en espace des fréquences.

❖ **Mesures au laboratoire**			
	Contexte d'apprentissage	Contexte amplifié	Contexte atténué
Détection	100 %	100 %	50 %
Identification	100 %	50 %	33.33 %
❖ **Mesures sur site ferroviaire**			
	Contexte d'apprentissage		
FAR	80 %		
Détection	100 %		

V. Conclusion

Dans ce quatrième chapitre nous avons procédé à la mise en œuvre des différentes méthodes de détection supervisées présentées lors du chapitre 3.

Nous avons différencié deux études, l'une considérant l'espace des signaux quadratiques, l'autre celui des fréquences.

Dans l'espace des signaux quadratiques, nous avons présenté notre méthodologie de travail, les différentes données nécessaires à notre étude ont été décrites ainsi que les étapes du travail.

Une première étape d'évaluation des paramètres s'est avérée nécessaire avant d'entamer la mise en œuvre des systèmes de détection. Une fois cette évaluation terminée nous avons pu fixer les paramètres de départ qui ont permis de créer les différentes bases de données nécessaires.

Deux bases de données ont été enregistrées pour chacun des deux descripteurs EVM_{rms} et $TT(t)$. Une première base d'apprentissage nous a permis de fixer les paramètres du modèle de référence. Une seconde base nous a servi pour le test.

L'étape suivante a consisté à utiliser les modèles appris pour réaliser la détection.

Nous avons commencé par le premier descripteur EVM_{rms} et nous avons procédé à la détection sur les données de simulation puis, sur les mesures en laboratoire. Le modèle choisi a donné de bons résultats que nous avons par la suite améliorés pour finalement obtenir un taux de succès de 100 % en effectuant un traitement plus long, sur une durée équivalente à 5 bursts.

Nous avons procédé de la même manière avec le second descripteur $TT(t)$. Les tests de détection se sont avérés initialement acceptables et nous avons à nouveau amélioré les performances du modèle en effectuant un traitement plus long, sur une durée de 57 symboles, pour obtenir un taux de succès de 100 %.

Dans l'espace des fréquences, nous avons de la même manière décrit la méthodologie de travail, fixé les paramètres des environnements et procédé à l'enregistrement des bases de données. Nous avons clôturé cette partie par les différents résultats de détection réalisés sur différents environnements. Notre modèle s'avère efficace et donne dans ces conditions idéales tant en simulation qu'en laboratoire des taux d'identification de 100 %.

Une fois les parties simulation et mesures en laboratoire menées à bien, nous sommes passés à l'évaluation des techniques réalisées sur site ferroviaire. Dans cette section, nous avons présenté une des campagnes de mesures réalisée en décrivant notamment l'environnement de mesure ainsi que le matériel utilisé pour l'acquisition.

À nouveau, dans cette partie, nous avons procédé à la création des bases de données qui nous ont permis de modéliser l'environnement et de déterminer la capacité de notre modèle à détecter la présence d'un brouilleur ainsi que son taux de fausses alarmes.

Deux études ont été menées en parallèle ici également, dans l'espace des signaux en quadrature et dans l'espace des fréquences.

Pour les signaux en quadrature les deux descripteurs ont été évalués successivement. Dans la continuité des mesures précédentes, une durée de traitement plus longue a permis d'obtenir des résultats idéaux.

Pour l'EVM_{rms}, une durée de 8 bursts permet d'atteindre une capacité de détection de 100 %. Pour le descripteur rayon $TT(t)$ nous obtenons une détection parfaite dès 5 bursts successifs.

Enfin la dernière partie porte sur l'évaluation de la technique dans le domaine spectral.

Les résultats de détection que nous avons obtenus sont idéaux en termes de détection mais présentent l'inconvénient de nombreuses fausses alarmes. Il serait nécessaire de les améliorer en utilisant des bases de données d'environnement normal plus riches, ainsi qu'en améliorant notre modèle multi gaussien.

VI. Références du chapitre 4

[4.1] S. Braun, F. Krug et P. Russer, A novel automatic digital quasi-peal detector for a time domain mesurment system, *EMC Europe*, Eindhoven, The Netherlands, 2004.

[4.2] A. Wisten et P. Makikaltio, Methods of measuring electromagnetic emission from train, *EMC Europe*, Hindhoven, The Netherlands, 2004.

[4.3] M. N. Ben Slimen, Recherche de procédures de caractérisation de l'environnement electromagnetique ferroviaire adaptées au contexte des systèmes de communication embarqués : Lille, Doctorat de l'Université des sciences et technologie de Lille 1, 2009.

Conclusion

Le travail de recherche mené dans cette thèse constitue l'un des premiers traitant de la détection des attaques électromagnétiques contre le système ferroviaire. Il est financé dans le cadre du projet de recherche européen SECRET du septième programme cadre de recherche et de développement.

Lors de ces travaux, nous nous sommes concentrés sur l'étude de la résistance de systèmes de radiocommunication déployés pour l'exploitation des chemins de fer vis-à-vis d'agressions électromagnétiques intentionnelles. Du bon acheminement des radiocommunications entre sol et trains dépend en effet significativement la disponibilité du système de transport. Ainsi, en absence de nouveaux messages reçus depuis le sol apportant de nouvelles consignes de marche, les trains en mouvement sont obligés d'effectuer rapidement un arrêt d'urgence. L'arrêt d'urgence d'un train entraine des perturbations se répercutant ensuite rapidement sur l'exploitation de la ligne entière, voire au-delà.

Il existe donc un intérêt à définir et à développer des méthodes de détection rapides et efficaces des perturbations qui permettent de mettre en œuvre rapidement des contre-mesures efficaces contre ces brouillages, à différents niveaux de l'architecture d'un système de radiocommunication, de la couche physique aux couches les plus élevées du protocole.

GSM-R constitue une technique de radio sol-trains actuellement en cours de déploiement et de généralisation sur l'ensemble des réseaux ferrés européens. Il s'avère donc nécessaire d'assurer le bon fonctionnement de cette radio GSM-R en toutes circonstances. Ceci constitue le point d'entrée principal de ce travail. Nous avons considéré différentes sources de brouillage intentionnelles en mesure de perturber, voire d'interrompre une communication GSM-R exploitée dans les bandes de fréquence européennes allouées.

Dans le premier chapitre, nous avons présenté successivement nos objectifs puis, positionné ce travail dans son contexte. L'objectif essentiel consiste ainsi à détecter rapidement et efficacement la présence

de signaux de brouillage superposés à ceux de communication utiles, voire à identifier ces brouilleurs à partir de phases d'apprentissage antérieurs. En ce qui concerne le contexte de ce travail, nous avons rappelé ce que sont les infrastructures critiques ainsi que leurs rôles dans l'activité économique des états. Parmi ces infrastructures critiques, celle de transport ferroviaire possède des caractéristiques particulières, en lien notamment avec son déploiement géographique considérable, son rôle majeur pour la mobilité des citoyens et des biens, et sa nécessaire interopérabilité inter états. Nous avons ensuite rappelé les composantes de cette interopérabilité ferroviaire.

Le deuxième chapitre a analysé différents systèmes et différentes configurations pouvant perturber les communications GSM-R. Nous avons entamé ce chapitre en rappelant quelques sources d'interférences d'origines naturelles et industrielles en mesure de perturber les radiocommunications. Le cas plus particulier des brouilleurs électromagnétiques intentionnels a été mentionné et leur classification rappelée. Nous en avons identifié de trois catégories, selon leur largeur de bande de brouillage : ultra large bande, à sinusoïde amortie et à bande étroite.
Les éléments pertinents pour l'étude d'une architecture de communication GSM-R ont ensuite été rappelés et nous avons considéré différentes dispositions de brouillage, le brouilleur étant disposé soit le long de l'infrastructure ferroviaire, soit à bord du train. Les puissances de brouillage susceptibles d'être reçues par les récepteurs des BTS et du train en ont été déduites. Nous avons également effectué une évaluation de la portée du brouilleur, qui peut être conséquente et induire, ainsi que mentionné précédemment, des conséquences sur l'exploitation ferroviaire.
Ce chapitre s'est poursuivi par une analyse de l'impact d'un brouillage sur une communication GSM-R effectuée à l'aide d'un banc de mesures. Nous avons montré que, lorsque les puissances de communication et de brouillage sont du même ordre de grandeur, alors la communication peut être interrompue et devenir effectivement impossible.
Dans une dernière étape de ce chapitre, nous avons modélisé la chaîne d'émission réception GSM-R qui nous servira tout au long de la suite de l'étude et nous avons retenu deux méthodes possibles permettant de détecter voire d'identifier la présence de brouilleurs que nous emploierons par la suite. L'une exploite les déformations particulières de la constellation des signaux $I(t)$ et $Q(t)$ prélevés dans le récepteur en présence de signaux de brouillage. L'autre considère l'analyse spectrale des signaux reçus par l'antenne menée à partir d'un dispositif d'acquisition distinct.

Le troisième chapitre s'est attaché à décrire et à développer les outils nécessaires à mettre en œuvre les deux méthodes de détection retenues. Nous avons commencé par introduire l'architecture du système de détection avant d'exposer plus en détails ces méthodes de détection et de reconnaissance. Le travail de description et de construction des outils s'est poursuivi en développant la partie détection dans

l'espace des signaux en quadrature. Nous avons extrait les signaux issus de la chaîne de communication GSM-R afin de mettre en avant la représentation en quadrature par les signaux *I* et *Q*. L'étape suivante nous a permis de traiter les deux descripteurs sélectionnés afin de mettre en œuvre le système de détection. Il s'agit des déformations du rayon *TT(t)* de la constellation *I* et *Q* puis, des variations de l'*EVM* en présence de signaux de brouillage. Nous avons validé la pertinence de ces descripteurs en présentant les histogrammes des situations normales et perturbées. Le processus de détection a été introduit par la suite en fonction de ces raisonnements.

Dans une seconde partie du chapitre nous avons développé la méthode de détection fondée sur l'analyse des signaux dans l'espace des fréquences. Nous avons présenté le modèle statistique de détection et d'identification élaboré en utilisant les représentations spectrales des signaux de communication GSM-R en présence ou non de brouillage. Dans ce but, une modélisation statistique de la densité spectrale de puissance associée aux fréquences en utilisant un classifieur bayésien a été menée. Ce descripteur nous a permis de mettre en place la détection par classification. Nous faisons non seulement la comparaison par rapport au fonctionnement normal, mais aussi par rapport aux états appris qui représentent les différentes situations de brouillage.

Ce troisième chapitre s'est conclu en proposant, dans un tableau récapitulatif, une comparaison des avantages et des inconvénients de chacune des méthodes utilisées appliquées à nos signaux.

Lors du quatrième chapitre, nous avons procédé à la mise en œuvre des différentes méthodes de détections supervisées décrites lors du chapitre 3. Dans l'espace des signaux quadratiques, nous avons présenté notre méthodologie de travail, les différentes données nécessaires à l'étude et les étapes du travail. Une première étape d'évaluation des paramètres a été nécessaire avant d'entamer la mise en œuvre des systèmes de détection. Une fois cette évaluation terminée nous avons pu fixer les paramètres de départ permettant de créer les bases de données. Deux bases de données ont été enregistrées pour chacun des deux descripteurs EVM_{rms} et $TT(t)$. Une première base d'apprentissage a permis de fixer les paramètres du modèle de référence. Une seconde base a servi pour le test. L'étape suivante a consisté à utiliser les modèles appris pour réaliser la détection. Nous avons commencé par le premier descripteur EVM_{rms} et nous avons procédé à la détection sur des données de simulation puis, sur les mesures en laboratoire. Le modèle choisi a donné de bons résultats, améliorés par la suite, pour finalement obtenir un taux de succès de 100 % moyennant un temps de traitement étendu à une durée équivalente à 5 bursts consécutifs.

Le second descripteur a fait l'objet d'un travail similaire. Les tests de détection se sont avérés initialement acceptables pour obtenir au final un taux de succès de 100 % moyennant également un temps de traitement plus long, étendu cette fois à une durée équivalent à 57 symboles consécutifs.

La seconde partie s'est concentrée sur l'analyse dans l'espace des fréquences. Le modèle de détection s'avère efficace et procure, dans ces conditions idéales tant en simulation que sur banc de mesures en laboratoire, des taux d'identification de 100 %.

À l'issue des travaux effectués en simulation et en laboratoire, et bien que les hypothèses théoriques de ce travail ne soient plus toutes respectées, nous avons tenté de mettre en œuvre ces différents outils dans un environnement réel, sur site ferroviaire. Nous avons présenté l'une des campagnes de mesures réalisées en décrivant notamment le site de mesure ainsi que le matériel utilisé pour l'acquisition. À nouveau, dans cette partie, nous avons procédé à la création des bases de données qui ont permis de modéliser l'environnement et de déterminer la capacité de nos modèles à détecter la présence d'un brouilleur ainsi que le taux de fausses alarmes.
Pour les signaux en quadrature, les deux descripteurs ont été évalués successivement. Dans la continuité des mesures précédentes, une durée de traitement plus longue a permis d'obtenir des résultats idéaux. Pour les signaux mesurés dans l'espace de fréquences, dans cette étape de faisabilité, le modèle de détection s'avère efficace et donne dans des résultats acceptables. En revanche, il entraine un taux de fausses alarmes excessif qu'il est nécessaire d'améliorer en utilisant des bases de données plus riches.

En termes de perspectives, ainsi que nous le soulignions au début de cette conclusion, ce travail de recherche constitue l'un des premiers à traiter de la détection des attaques électromagnétiques contre le système ferroviaire. Au-delà de cette étude initiale, beaucoup reste ainsi à faire. Les deux méthodes de détection que nous avons mises en place ont été évaluées in situ mais toutefois sur un site spécifique, le long d'une ligne à grande vitesse qui n'est pas représentatif de l'ensemble des sites ferroviaires susceptibles d'être surveillés. La prise en compte globale de l'ensemble des environnements EM normaux nécessitera des travaux complémentaires. Une étape importante et nécessaire à réaliser maintenant serait de multiplier ces évaluations dans autant de sites ferroviaires que pertinents et notamment à bord de trains. L'environnement d'apprentissage deviendrait ainsi beaucoup plus riche et, peut être en mesure de traiter une bonne partie de la complexité de l'environnement EM ferroviaire globale.
Si l'on considère l'environnement particulier à bord des trains. Nous aurons besoin dans un premier temps d'utiliser les enregistrements réalisés à bord des trains pour constituer des bases d'apprentissage et mettre ainsi en place le système de référence. Il nous faudra également acquérir des enregistrements de brouillage à l'intérieur des trains, ce qui implique de prendre de nombreuses précautions afin de ne pas perturber la circulation effective du train abritant ces mesures. Nous pourrons dès lors implémenter

le système de détection. L'antenne GSM-R existante embarquée pourra servir à l'acquisition des données.
La méthode traitant l'espace quadratique devra être adaptée à cette exploitation en mobilité et de ce fait, nous devrons enrichir les bases d'apprentissage. Il faudra en outre optimiser les descripteurs utilisés afin de prendre en compte les caractéristiques transitoires des bruits présents dans ces différents environnements électromagnétiques ferroviaires. La détection quant à elle devra prendre en compte un suivi temporel de l'évolution des paramètres. Un autre aspect à considérer porte sur la méthode de détection utilisée. En faisant varier l'environnement, nous devrons mettre en place un système de détection statistique en fonction des différentes gaussiennes représentant le nouveau modèle. À nouveau, le traitement multi gaussien avec une détection bayésienne doit pouvoir s'appliquer. En ce qui concerne l'implémentation matérielle, celle-ci reste assez facile à mettre en œuvre. Comme pour les indicateurs de qualité de type RxQual, le paramètre EVM_{rms} peut être extrait directement du récepteur et surveillé. Le second descripteur peut quant à lui, se greffer directement au niveau du récepteur et récupérer les données utilisées. Dans ce second cas, le système de détection consistera en un bloc de test à implanter sur le récepteur.
Pour la méthode opérant dans l'espace des fréquences, un traitement permettant d'obtenir les spectres de puissance des signaux reçus durant le trajet sera nécessaire afin de les traiter en temps réel. Ces spectres représenteront l'entrée du système de détection.

Une autre méthode de détection est également envisagée et a fait l'objet d'investigations préliminaires. Inspirée de la thèse de Stephen Dudoyer « Méthode de Détection et de Reconnaissance de Bruits Electromagnétiques permettant la Prédiction de leurs Effets sur les Transmissions GSM-R » récemment effectuée au laboratoire, elle donnerait lieu à une adaptation des méthodes de classification utilisées. Le principe de ce travail consiste à exploiter la représentation temps fréquence afin d'en déduire de nouveaux descripteurs adaptés. Une méthode de classification supervisée par *SVM* (Support vector machine) pourrait également être utilisée pour détecter les situations de brouillage.

Quelle que soit la méthode sélectionnée au final, les résultats de détection génèreront ensuite une alarme ou lanceront automatiquement les contre-mesures adaptées en cas de détection de brouillage. Pour que le système soit utile à l'exploitant, le taux de fausses alarmes devra être très bas.

Annexe 1

Cette annexe présente les étapes de calcul permettant d'établir les formulations théoriques des signaux en quadrature modulés en GMSK

I. Chaîne de communication GMSK

La modulation Gaussian Minimum Shift Keying (GMSK) est dérivée de la modulation MSK, qui est une modulation à phase continue, où la porteuse ne contient pas de discontinuités de phase.
Pour adapter le spectre de puissance relativement large de la MSK aux communications sans fil, il est nécessaire d'utiliser une pré-modulation utilisant un filtre passe-bas.
Une pré-modulation gaussienne est adoptée pour la modulation GMSK.

La séquence de données (train d'impulsions) pour ce type de modulation est transmise à travers un filtre gaussien, puis modulée en MSK. On utilise un filtre gaussien dont la largeur ($L*T_b$) est déterminée par la largeur de bande en temps, avec un produit de modulation $BT_b = 0.3$ pour le standard GSM, où T_b correspond à la durée d'un bit.

Nous décrivons ci-dessous les étapes nécessaires à la transmission d'une séquence binaire. Ces éléments ont été publiés dans [1], cité à la fin des annexes.

Nous commençons par décrire le filtre gaussien utilisé :

$$h(t) = \frac{1}{\sqrt{2\pi}\sigma T_b} \exp\left(\frac{-t^2}{2\sigma^2 T_b{}^2} \right) \quad (1)$$

où la variance $\sigma = \frac{\sqrt{\ln(2)}}{2\pi B T_b}$ dépend de B, la bande passante du filtre à 3 dB.

Sa réponse impulsionnelle est décrite comme suit :

$$g(t) = h(t) * rect\left(\frac{t}{T_b} \right) \quad (2)$$

avec la fonction rectangle décrite par :

$$rect\left(\frac{t}{T_b} \right) = \begin{cases} \frac{1}{T_b} & \text{pour} |t| < \frac{T_b}{2} \\ 0 & \text{ailleurs} \end{cases}$$

ce qui donne la réponse impulsionnelle suivante :

$$g(t) = \frac{t}{2T_b}\left[Q\left(2\pi BT_b \frac{t - T_b/2}{T_b\sqrt{\ln(2)}} \right) - Q\left(2\pi BT_b \frac{t + T_b/2}{T_b\sqrt{\ln(2)}} \right) \right] \tag{3}$$

avec la fonction Q décrite par :

$$Q(t) = \int_t^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{k^2}{2} \right) dk$$

Pour la modulation GMSK, g(t) est décrit par la relation suivante :

$$g(t) = \begin{cases} \dfrac{t}{2T_b}\left[Q\left(2\pi BT_b \dfrac{t - T_b/2}{T_b\sqrt{\ln(2)}} \right) - Q\left(2\pi BT_b \dfrac{t + T_b/2}{T_b\sqrt{\ln(2)}} \right) \right] & -(L-1)T_b/2 \le t \le (L+1)T_b/2 \\ 0 & \text{ailleurs} \end{cases} \tag{4}$$

où L (L = 3 dans notre cas) est le paramètre fixé qui correspond au produit BT_b = 0.3.

En règle générale, le signal de communication pour une modulation à phase continue s'écrit selon les équations suivantes [1]:

$$y(t) = \sqrt{\frac{2E_b}{T_b}} \cos(2\pi f_c t + \phi(t, \alpha)) \tag{5}$$

avec E est l'énergie associée au bit d'une durée T_b, et f_c la fréquence de la poretuse, où la phase instantanée est décrite par :

$$\phi(t, \alpha) = 2\pi \sum_{i<N} \alpha_i h q(t - iT_b) \tag{6}$$

$\alpha_{i<N}$ (α_1, α_2, α_3, α_4, α_5 ……..) est la séquence binaire à transmettre, possédant la même probabilité d'avoir un +1 que d'avoir un -1. $h = 2\Delta f T_b$ est l'index de modulation (Δf est la dérivation de la fréquence de la porteuse) et q(t) est la réponse de phase normalisée donnée par :

$$q(t) = \int_{-\infty}^{t} g(\tau) d\tau \tag{7}$$

En remplaçant dans l'équation 5 et en appliquant un filtre gaussien la modulation GMSK donne :

$$y(t)=\sqrt{\frac{2E_b}{T_b}}\cos\left(2\pi f_c t+\frac{\pi}{2T_b}\sum_i \alpha_i \int\left[Q\left(\frac{2\pi BT_b}{\sqrt{\ln(2)}}\left(\frac{\tau}{T_b}-(i+1)\right)\right)-Q\left(\frac{2\pi BT_b}{\sqrt{\ln(2)}}\left(\frac{\tau}{T_b}-(i-1)\right)\right)\right]d\tau\right) \tag{8}$$

qui peut se simplifier par :

$$y(t)=\sqrt{\frac{2E_b}{T_b}}\left[\cos\phi(t,\alpha)\cos 2\pi f_c t-\sin\phi(t,\alpha)\sin 2\pi f_c t\right] \tag{9}$$

où la phase instantanée est donnée par :

$$\phi(t,\alpha)=\frac{\pi}{2T_b}\sum_i \alpha_i \int\left\{Q\left(\frac{2\pi BT_b}{\sqrt{\ln(2)}}\left(\frac{\tau}{T_b}-(i+1)\right)\right)-Q\left(\frac{2\pi BT_b}{\sqrt{\ln(2)}}\left(\frac{\tau}{T_b}-(i-1)\right)\right)\right\}d\tau \tag{10}$$

à ce niveau le signal est transmis à travers le canal *BBAG*. Nous obtenons l'expression :

$$s(t)=y(t)+N_g(t) \tag{11}$$

où $N_g(t)$ représente l'effet apporté par le canal *BBAG*.
Par la suite le signal $s(t)$ reçu par l'antenne de réception est démodulé afin d'extraire les signaux $I(t)$ et $Q(t)$ nécessaires à l'étude. Pour cela, nous utilisons les signaux $I_m(t)$ et $Q_m(t)$ à la réception données par les équations :

$$I_m(t)=\left(\cos(2\pi f_c t+\theta_0(t))s(t)\right) \tag{12}$$

$$Q_m(t)=\left(\sin(2\pi f_c t+\theta_0(t))s(t)\right) \tag{13}$$

Nous avons introduit $\theta_0(t)$ l'offset ajouté à la porteuse par la synchronisation de phase, nous considérons également l'effet du canal de communication $N_g(t)$ en ajoutant une fréquence de dérivation $\theta_d(t)$, ce qui nous permet de réécrire le signal comme suit :

$$s(t)=\left[\cos(2\pi f_c t+\theta_d(t))i(t)+\sin(2\pi f_c t+\theta_d(t))q(t)\right] \tag{14}$$

On peut calculer les signaux en quadrature en fonction de cette nouvelle formule ce qui nous donne :

$$I_m(t) = \frac{i(t)}{2}\left[\cos(4\pi f_c t + \theta_0(t) + \theta_d(t)) + \cos(\theta_0(t) - \theta_d(t))\right] - \frac{q(t)}{2}\left[\sin(4\pi f_c t + \theta_0(t) + \theta_d(t)) + \sin(\theta_0(t) - \theta_d(t))\right] \quad (15)$$

$$Q_m(t) = \frac{i(t)}{2}\left[\sin(4\pi f_c t + \theta_0(t) + \theta_d(t)) + \sin(\theta_0(t) - \theta_d(t))\right] - \frac{q(t)}{2}\left[\cos(4\pi f_c t + \theta_0(t) + \theta_d(t)) + \cos(\theta_0(t) - \theta_d(t))\right] \quad (16)$$

Ces signaux sont transmis à travers le filtre gaussien de la chaîne de réception. Ce filtre similaire à celui utilisé à l'émission, a pour but de supprimer l'effet de la composante ($2*f_c$).

$$I(t) = g(t) * I_m(t) \quad (17)$$

$$Q(t) = g(t) * Q_m(t) \quad (18)$$

Après calculs et simplifications les composantes I(t) et Q(t) sont données par :

$$I(t) = \frac{i(t)}{2}\left[\cos(\theta_0(t) - \theta_d(t))\right] - \frac{q(t)}{2}\left[\sin(\theta_0(t) - \theta_d(t))\right] \quad (19)$$

$$Q(t) = \frac{i(t)}{2}\left[\sin(\theta_0(t) - \theta_d(t))\right] - \frac{q(t)}{2}\left[\cos(\theta_0(t) - \theta_d(t))\right] \quad (20)$$

Maintenant nous considérons le signal de communication dans le cas de présence de perturbations.

- ***G_1(t)***

Le signal de communication devient :

$$s_T(t) = \left[\cos(2\pi f_c t + \theta_d(t))i(t) + \sin(2\pi f_c t + \theta_d(t))q(t)\right] + G_1(t) \quad (21)$$

le signal $G_1(t)$ est donné par l'équation :

$$G_1(t) = A_1 \cos(2\pi f_c t) \quad (22)$$

ce qui donne les deux signaux en quadrature :

$$I_m1(t) = \left(\cos(2\pi f_c t + \theta_0(t))s_T(t)\right) \quad (23)$$

$$Q_m1(t) = \left(\sin(2\pi f_c t + \theta_0(t))s_T(t)\right) \quad (24)$$

qui deviennent :

$$I_m1(t) = I_m(t) + G_1(t)\cos(2\pi f_c t + \theta_0(t)) \quad (25)$$

$$Q_m1(t) = Q_m(t) + G_1(t)\sin(2\pi f_c t + \theta_0(t)) \quad (26)$$

les signaux à la réception deviennent maintenant :

$$I1(t) = g(t) * I_m1(t) \quad (1)$$

$$Q1(t) = g(t) * Q_m1(t) \quad (2)$$

après simplification et filtrage, nous obtenons :

$$I1(t) = I(t) + \frac{A_1}{2}\cos(\theta_0(t)) \quad (3)$$

$$Q1(t) = Q(t) + \frac{A_1}{2}\sin(\theta_0(t)) \quad (4)$$

- ***$G_2(t)$***

Le signal de communication devient :

$$s_T(t) = \left[\cos(2\pi f_c t + \theta_d(t))i(t) + \sin(2\pi f_c t + \theta_d(t))q(t)\right] + G_2(t) \quad (27)$$

le signal $G_2(t)$ est donné par l'équation :

$$G_2(t) = A_2\cos(2\pi f_c t + k\cos(2\pi\Delta f t)) \quad (28)$$

ce qui donne les deux signaux en quadrature :

$$I_m2(t) = \left(\cos(2\pi f_c t + \theta_0(t))s_T(t)\right) \quad (29)$$

$$Q_m2(t) = \left(\sin(2\pi f_c t + \theta_0(t))s_T(t)\right) \quad (30)$$

qui deviennent maintenant :

$$I_m 2(t) = I_m(t) + G_2(t)\cos(2\pi f_c t + \theta_0(t)) \tag{31}$$

$$Q_m 2(t) = Q_m(t) + G_2(t)\sin(2\pi f_c t + \theta_0(t)) \tag{32}$$

les signaux à la réception s'écrivent ainsi :

$$I2(t) = g(t) * I_m 2(t) \tag{33}$$

$$Q2(t) = g(t) * Q_m 2(t) \tag{34}$$

après simplification et filtrage nous obtenons :

$$I2(t) = I(t) + \frac{A_2}{2}\cos(\theta_0(t) + k\cos(2\pi\Delta f t)) \tag{35}$$

$$Q2(t) = Q(t) + \frac{A_2}{2}\sin(\theta_0(t) + k\cos(2\pi\Delta f t)) \tag{36}$$

Annexe 2

Cette annexe a pour objectif d'indiquer les étapes de calcul du descripteur EVM_{rms} et les relations qui le lient au *SNR*.

I. Relation entre *EVM* et *SNR*

Nous considérons les deux signaux y_n et s_n représentant respectivement le vecteur défini par les composantes $I_y(nT_e)$ et $Q_y(nT_e)$ pour le signal avant canal et le vecteur défini par les composantes $I_s(nT_e)$ et $Q_s(nT_e)$ pour le signal estimé après canal.

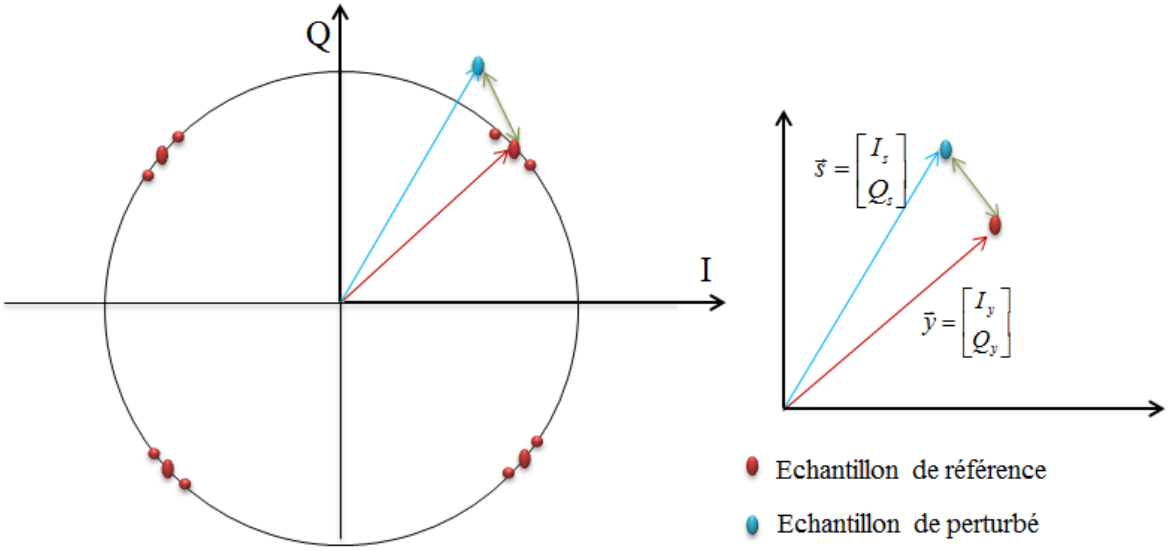


Figure 1. Constellation quadratique et représentation de l'*EVM*

Comme décrit dans le chapitre 3, l'*EVM* est calculé en utilisant l'équation suivante :

$$EVM = |s_i - y_i| \Rightarrow \begin{cases} \|y_i\| = \sqrt{I_y{}^2 + Q_y{}^2} \\ \|s_i\| = \sqrt{I_s{}^2 + Q_s{}^2} \end{cases} \quad (1)$$

Pour quantifier l'*EVM*, nous utilisons la valeur moyenne du vecteur d'erreur (EVM_{rms}) calculée sur la séquence de 156 bits correspondant à la longueur d'un burst. Comme indiqué dans l'équation 2, l'EVM_{rms} représente le module du vecteur d'erreur moyenne à l'échelle du burst.

$$EVM_{rms} = \sqrt{\frac{\sum_n |s_i - y_i|^2}{\sum_n |y_i|^2}} \quad (2)$$

plus en détails :

$$EVM_{rms}{}^2 = \frac{\sum_N (X_I{}^2 + Y_Q{}^2)}{\sum_N y_i{}^2} \quad \text{avec} \quad \begin{cases} X_I = I_y - I_s \\ Y_Q = Q_y - Q_s \end{cases} \quad (3)$$

où Σy_i, la somme des échantillons i du burst est donnée par la relation :

$$y_i^{\,2} = (\sqrt{I_y^{\,2} + Q_y^{\,2}})^2 = 1 \tag{4}$$

Dans le cas où nous ne considérons que l'effet du canal *BBAG* nous obtenons :

$$EVM_{rms}^{\,2} = \frac{\sum_N (I_s - I_y)^2}{N} + \frac{\sum_N (Q_s - Q_y)^2}{N} \tag{5}$$

$$EVM_{rms}^{\,2} = \sigma_I^{\,2} + \sigma_Q^{\,2} = \sigma_b^{\,2} \tag{6}$$

L'$EVM_{rms}^{\,2}$ décrit l'écart type produit par les déformations liées au *BBAG* comme on peut l'observer figure 2. On note en bleu la constellation des signaux en quadrature avant passage dans le canal de transmission et, en vert, l'estimation de cette constellation après l'effet du canal *BBAG* avec un *SNR* de 20 dB.

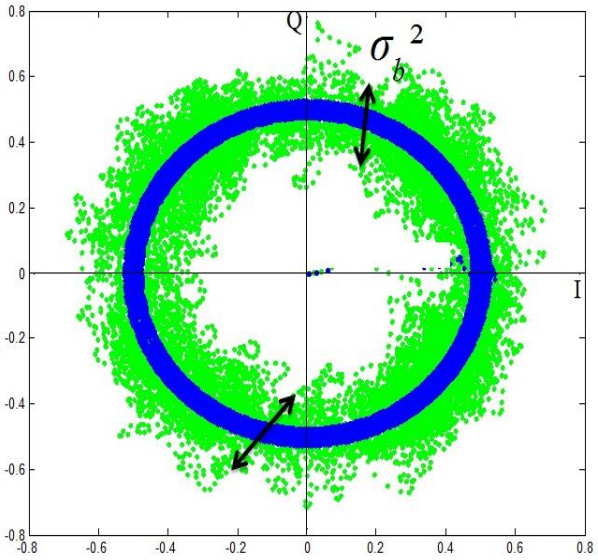


Figure 2. Constellation quadratique du signal (bleu) de référence avant canal et du signal (vert) après canal *BBAG*.

Nous établissons maintenant le lien entre l'$EVM_{rms}^{\,2}$ et le *SNR*.

L'$EVM_{rms}^{\,2}$ peut également être noté sous la forme suivante :

$$EVM_{rms}^{\,2} = \frac{\frac{1}{N}\sum_N |s(n) - y(n)|^2}{P} \tag{7}$$

N est le nombre de symboles contenus dans un burst, *P* représente la puissance moyenne des symboles transmis lors d'une communication idéale (burst).

$$P = \frac{1}{N}\sum_{N}\left|y(n)\right|^2 \tag{8}$$

Dans le cas où le bruit du canal est gaussien on peut écrire :

$$EVM_{rms}{}^2 = \frac{\frac{1}{N}\sum_{N}\left|N_g(n)\right|^2}{P} \tag{9}$$

sachant que la puissance du bruit est égale à :

$$N_0 = \frac{1}{N}\sum_{n<N}\left|N_g(n)\right|^2 \tag{10}$$

L'expression de l'$EVM_{rms}{}^2$ peut être simplifiée sous la forme :

$$EVM_{rms}{}^2 = \frac{N_0}{P} \tag{11}$$

ce qui donne :

$$EVM_{rms} \approx \sqrt{\frac{1}{SNR}} \tag{12}$$

II. Principe de détection par rayon *TT*(t)

Nous présentons figure 3 l'organigramme décrivant le système de détection qui utilise le descripteur *TT*(t).

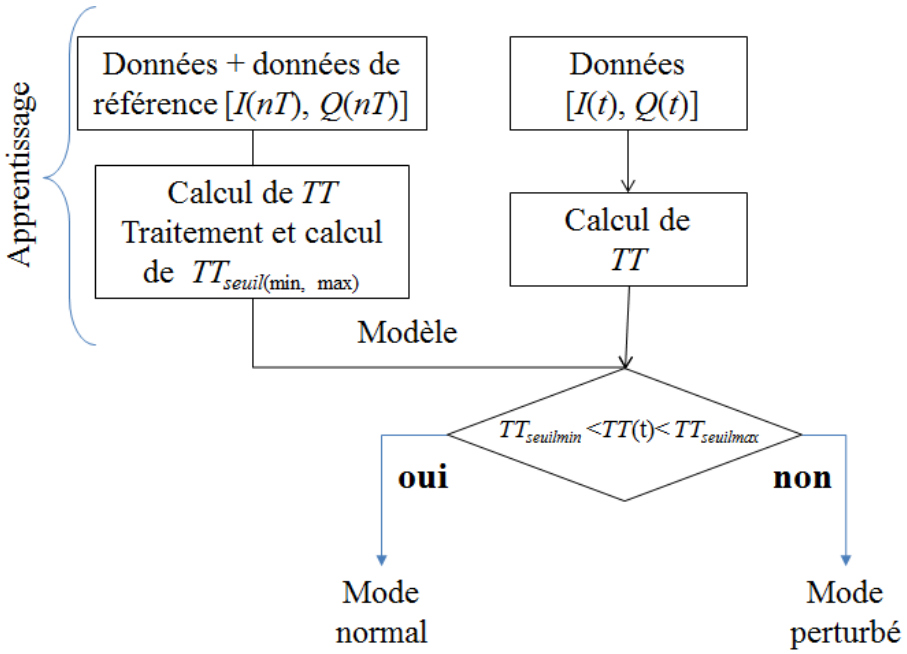


Figure 3. Organigramme de détection pour TT(t).

III. Principe de détection par *EVM*

Nous présentons figure 4 l'organigramme décrivant le système de détection qui utilise le descripteur EVM_{rms} dans les simulations Matlab™.

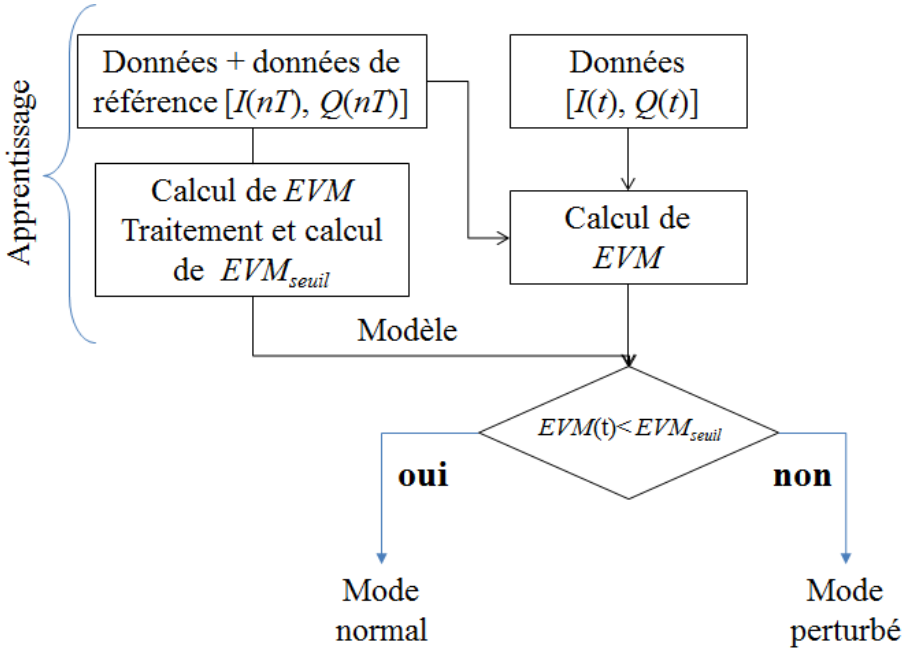


Figure 4. Organigramme de détection pour l'*EVM* en simulation.

L'organigramme qui décrit le processus de mesure est présenté figure 5 :

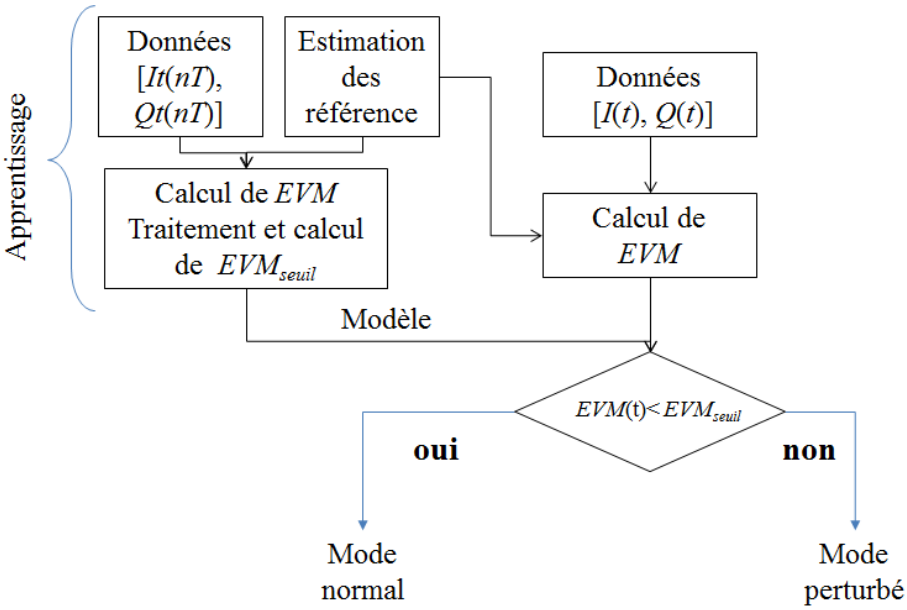


Figure 5. Organigramme de détection pour l'*EVM* avec le banc de mesure.

Annexe 3

Cette annexe possède pour objectif de décrire l'algorithme « Expectation Maximisation » utilisé pour la mise en place des modèles statistiques.

I. Description de l'algorithme Expectation Maximisation

Dans cette partie nous rappelons la méthode du Modèle de Mélange Gaussien (MMG) que nous utilisons durant ce travail.

Cette méthode repose sur une bonne estimation des paramètres en utilisant l'algorithme « Expectation Maximization » (E.M). Celle-ci repose sur une optimisation itérative des paramètres du modèle à savoir le calcul de la moyenne, de la matrice de covariance, et de la probabilité a posteriori des composantes du mélange, où chaque groupe de données possède sa propre distribution.

- **Algorithme du modèle MMG**

Pour un modèle EM, si les événements sont issus d'une composition de *N* phénomènes, la densité de probabilité prend la forme d'une composition de lois Normales, approximée par une somme pondérée par le facteur α de densités Normales où la probabilité du mélange est donnée par l'équation :

$$p(X) = \sum_{n=1}^{N} \alpha_n \mathcal{N}(X\ ; \mu_n, \sigma_n) \tag{1}$$

Avec :

$$\mathcal{N}(x; \mu, \sigma) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{1}{2}\left(\frac{x-\mu}{\sigma} \right)^2 \right) \tag{2}$$

La mise en œuvre du modèle réside dans l'estimation des paramètres d'espérance et de variance $C_i\{\ \mu_i, \sigma_i\}$ tout en maximisant la vraisemblance. Ces paramètres sont estimés à partir d'une séquence d'apprentissage en utilisant un algorithme itératif. Pour une séquence de *N* phénomènes $X = \{x_1, \ldots, x_N\}$, la probabilité du mélange suppose l'indépendance entre les vecteurs. Ceci peut être écrit sous la forme :

$$p(X / C_i) = \prod_{n=1}^{N} p\ (x_n / C_n) \tag{3}$$

Le principe de l'algorithme EM repose sur l'utilisation d'un modèle initial (C_n) pour estimer un nouveau modèle. Le nouveau modèle devient alors le modèle initial pour l'itération suivante, le processus est répété jusqu'à ce qu'un seuil de convergence prédéfini soit atteint.

Pour assurer le bon fonctionnement du modèle, nous devons respecter les équations suivantes :

$$\sum_{n=1}^{N} \alpha_n = 1 \tag{4}$$

$$\alpha_n = \frac{1}{N} \sum_{n=1}^{N} p(n/x_n, C_n) \tag{5}$$

On souhaite trouver une estimation qui minimise la probabilité d'erreur, ce qui a pour effet de maximiser la log-vraisemblance de $p(X/C_n)$.

$$\log \Gamma(X / C_k) = \log \prod_{n=1}^{N} \mathcal{N}(x_n / C_n) \tag{6}$$

Comme tous les algorithmes itératifs, EM nécessite l'initialisation des paramètres du modèle de mélange des gaussiennes. Les matrices de covariance sont initialisées par des matrices identités et les K vecteurs moyennes sont initialisés par les centres de différentes gaussiennes du mélange estimés par l'algorithme de K-moyennes.

L'algorithme EM nous fournit alors les paramètres en suivant les étapes de calcul suivante:

- Etape E

$$p(n/x_n, C_n) = \frac{\alpha_n \mathcal{N}(n/x_n, C_n)}{\sum_{n=1}^{G} \alpha_n \mathcal{N}(n/x_n, C_n)} \tag{7}$$

où $p(n/x_n,C_n)$ est la probabilité d'appartenir à une gaussienne n sachant x_n, on fixe un nombre G de gaussiennes pour l'estimation du mélange.

- Etape M

Pour cette méthode, on calcule la moyenne μ_i, et la variance σ_i exprimées par :

$$\mu_n = \frac{\sum_{n=1}^{N} p(n/x_n, C_n) x_n}{\sum_{n=1}^{N} p(n/x_n, C_n)} \tag{8}$$

$$\sigma_n^2 = \frac{\sum_{n=1}^{N} p(n/x_n, C_n) x_n^2}{\sum_{n=1}^{N} p(n/x_n, C_n)} - \mu_n^{\,2} \tag{9}$$

Nous utilisons cette méthode et l'appliquons à nos brouilleurs.

Cela nous nous permet d'avoir les paramètres nécessaires à la réalisation des tests de reconnaissance.

Afin d'évaluer le modèle, nous utilisons le test du χ^2 déjà employé dans [2] pour en démontrer la qualité. Pour les traitements statistiques, le test du chi-carré est utilisé afin de tester si un échantillon de données appartenant à une population suit une loi de probabilité spécifique définie a priori, selon l'équation suivante :

$$\chi^2 = M \sum_{i=1}^{I} \frac{(h_i(x) - p_i(x))^2}{p_i(x)} \tag{10}$$

Où $h_i(x)$ représente la distribution observée en fonction de l'histogramme de la variable x décomposée en I intervalles, $p_i(x)$ est la distribution estimée pour l'intervalle i. L'équation (10) démontre que plus χ^2 est petit, plus la distribution $p_i(x)$ est représentative de la distribution de la variable x.

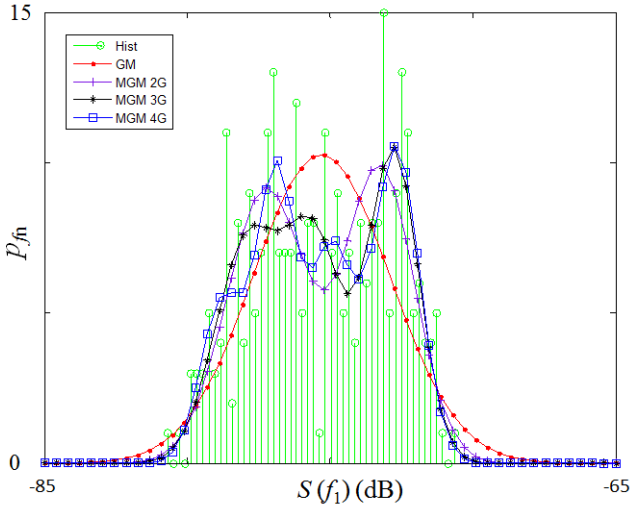


Figure 1. Histogramme et pdf de la fréquence f1 = 924.8 MHz pour un modèle multi-gaussien G = 1, 2, 3, 4.

Nous appliquons le test du χ^2 pour un des dispositifs de brouillage utilisés. La figure 1 montre les observations faites pour une fréquence f_1 ainsi que les modèles proposés à cette fréquence. Sur ces observations nous appliquons le test du chi 2 comme le montre la figure 2.

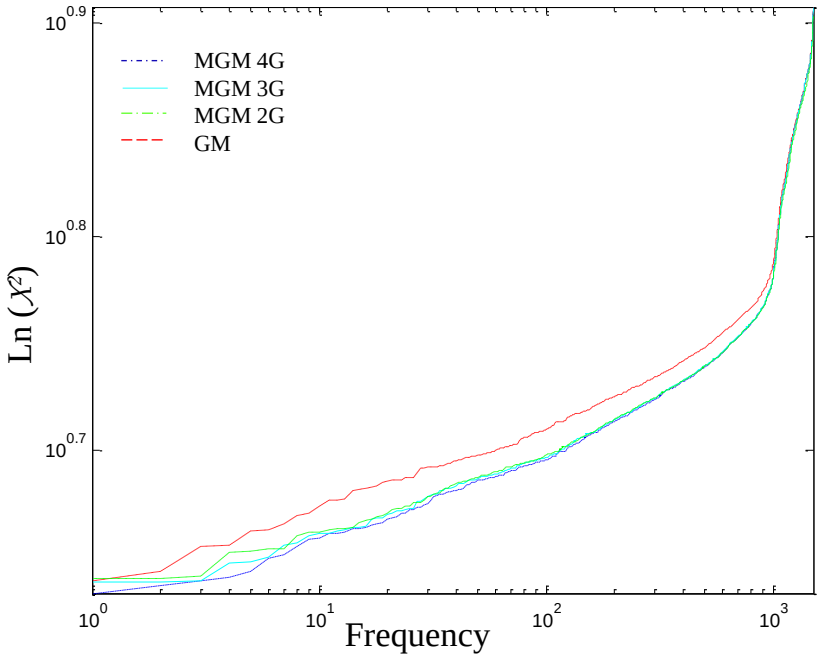


Figure 2. Représentation logarithmique du χ^2 pour le mélange multi gaussien avec G = 1, 2, 3, 4.

Les résultats du χ^2 sont triés par ordre croissant. Bien que tous les modèles aient été rejetés pour un test réalisé avec un niveau de confiance de 5 %, on remarque que les erreurs sont plus importantes pour le modèle gaussien que le modèle multi gaussien.

En conclusion nous obtenons que le meilleur modèle décrit par le test s'avère être ici le modèle *GMM* avec $G = 3$ gaussiennes.

Références Annexes

[1] M. K. Simon, Bandwidth-Efficient Digital Modulation With Application to Deep-Space Communication, Wiley, 2003.

[2] B. Rivet, L. Girin et C. Jutten, Log-Rayleigh Distribution: A simple and efficient Statistical Representation of Log-Spectral Coefficients, *IEEE trans. on audio, speech, and language processing*, vol. 15, no 13, pp. 796-802, 2007.

Bibliographie

Communication de l'auteur en relation avec les travaux de thèse :

Revues

- **S**. **Mili,** D. Sodoyer, V. Deniau, M. Heddebaut, Modeling and analysis of railway GMSK reception vulnerability to electromagnetic interference. International Journal of Advances in Computer Science and Technology, 2(7), July 2013, 115-118.
- **S**. **Mili,** D. Sodoyer, V. Deniau, M. Heddebaut, Detection of electromagnetic jamming signals interfering with a railway track-to-train radio communication. Journal of telecommunications (***Accepté***).
- **S. Mili**, V. Deniau, D. Sodoyer, M. Heddebaut, S. Ambellouis, Detection methods of Electromagnetic jamming to protect the railway communication. IEEE Communication magazine (***Soumis***).

Conférences

- **S. Mili**, V. Deniau, D. Sodoyer, M. Heddebaut, Modélisation d'une chaîne de communication GSM-R pour la détection d'attaques électromagnétiques. Journée des doctorants 2012, Villeneuve d'Ascq, 13 - 14 juin 2012.
- **S. Mili**, V. Deniau, D. Sodoyer, M. Heddebaut, Modeling of a GSM-R communication chain submitted to transient IEMIs. EuroEm 2012. Toulouse, 28 juillet - 1 août 2012.
- **S**. **Mili,** D. Sodoyer, V. Deniau, M. Heddebaut, Modeling and analysis of railway GMSK reception vulnerability to electromagnetic interference. Colloque International TELECOM'2013 & 8ème JFMMA 2013. Marakech, 13 - 15 mars 2013
- **S. Mili**, V. Deniau, D. Sodoyer, M. Heddebaut, Caractérisation et modélisation de l'environnement EM ferroviaire pour la reconnaissance de conditions EM critiques. Doctoriales Lille Nord de France 2013.Lille, 2 - 7 juin 2013.
- **S**.**Mili,** D. Sodoyer, V. Deniau, M. Heddebaut, H. Philippe, F. Canavero, Recognition process of jamming signals superimposed on GSM-R radiocommunications. Electromagnetic

Compatibility (EMC EUROPE), 2013 International Symposium on , vol., no., pp.45,50, 2-6 Sept. 2013.

- M. Heddebaut, **S. Mili**, D. Sodoyer, E. Jacob, M.Aguado, C. P. Zamalloa, and V. Deniau. Towards a resilient railway communication network against electromagnetic attacks. Transport Research Arena 2014, Paris, 14-17 avril 2014.
- **S. Mili**, V. Deniau, D. Sodoyer, M. Heddebaut, Détecter la présence d'un brouilleur en étudiant les représentations en quadrature des signaux de communication. 17ème Colloque International et Exposition sur la Compatibilité ElectroMagnétique (CEM 2014), Clermont-Ferrand, 1-3 juillet 2014.
- **S. Mili**, V. Deniau, D. Sodoyer, M. Heddebaut. Detection of railway signalling jamming signals using the EVM method. AmerEm 2014. Albuquerque 27 juillet – 1 août 2014.

Résumé :

Ces dernières années, les nombreux travaux dont l'objectif général est de conduire à l'interopérabilité ferroviaire ont permis l'émergence d'un système paneuropéen de contrôle-commande ferroviaire. Ce système exploite des radiocommunications sol-trains fonctionnant selon le protocole GSM-R (Global System for Mobile communications – Railways), actuellement en cours de déploiement à grande échelle. La bonne marche de l'exploitation ferroviaire dépend, pour une part, du bon acheminement des données entre sol et trains. Il s'avère donc nécessaire d'assurer un fonctionnement efficace de cette radio sol-trains en dépit de perturbations électromagnétiques intentionnelles ou non intentionnelles qui pourraient le perturber. Ce travail de thèse s'intéresse à cette seconde catégorie de perturbations. Nous développons des méthodes de détection de brouilleurs électromagnétiques superposant leurs signaux à la communication sol-trains. Cette détection permettra de mettre en œuvre rapidement des contre-mesures efficaces contre ces brouillages, à différents niveaux de l'architecture radio, de la couche physique, aux couches les plus élevées du protocole.

Nous mettons en œuvre un système de détection supervisé permettant de détecter la présence de signaux de brouillage intentionnels voire, pour certaines méthodes mises en œuvre, de les reconnaître. Fondé sur l'analyse des signaux échangés, nous développons et évaluons deux méthodes distinctes. L'une exploite les signaux en quadrature mis en évidence par le récepteur dans le canal de communication employé. L'autre méthode considère la densité spectrale de puissance des signaux recueillis dans une bande de fréquence plus large, centrée dans la gamme allouée aux communications GSM-R, et s'étendant de part et d'autre de celle-ci. Ces méthodes sont successivement évaluées par simulation, sur des données issues d'un banc de mesure puis, sur un site ferroviaire réel.

Abstract:

In recent years, numerous studies whose ultimate goal is to drive the railway interoperability have allowed the emergence of a pan-European train control system. This system uses ground-to-train radio operating on the GSM-R (Global System for Mobile communications - Railways) protocol, currently being deployed on a large scale along railway lines. The smooth running of railway operations depends, in part, of the proper routing of radio communications between trains and ground. Therefore, it is necessary to ensure the effective operation of this ground to train link in presence of intentional or unintentional electromagnetic interference that could disrupt communication. This thesis focuses on this second category of disturbances. We develop methods for detecting electromagnetic interference superimposing their signals to GSM-R signals. Then, this detection will promptly set off effective countermeasures against such interference at different levels of the radio architecture, the physical layer, the higher protocol layers. We implement a supervised detection system to detect the presence of jamming signals and, for potentially to recognize them. Based on the analysis of signals exchanged, we develop and evaluate two methods. One considers the quadrature signals recovered by the receiver in the used communication channel. The second method exploits the power spectral density of the signals collected in a wider frequency band, centered in the range allocated to the GSM-R communications and extending on either side thereof. These methods are successively evaluated by simulation, on data obtained using a test bench, and on a real railway site.