RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Dr YAHIA FARES DE MEDEA

Faculté des sciences et de la technologie

Département du génie électrique et de l'informatique

Mémoire de fin d'études pour l'obtention du diplôme de Master en Génie électrique

Option : Systèmes de Télécommunications

THEME

SIMULATION DU SYSTÈME BLUETOOTH À BASE DU CIRCUIT INTÉGRÉ LMX3162

Proposé et dirigé par :

*Mr. **Batel Noureddine***

Présenté par:

SOUIHEL Ayoub

BENDJEBBES Amine

Promotion : 2012/2013

Remeciement

Nous tenons à remercier le tout puissant qui nous a donné le courage et la patience qui a éclairé notre chemin pour achever ce travail.

Nous remercions très vivement notre encadreur de thèse Dr. Batel Noureddine , pour nous avoir suivi et soutenu dans ce parcours, pour nous avoir conseillé et encouragé et pour nous avoir fait partager son expérience et ses connaissances.

Nous remercions chaleureusement les membres du jury de leur lecteur de ce mémoire et sa correction .

Enfin, nous remercions nos collègues, Benrouissi Mustapha

et Otman Bakir pour leur soutien et leurs encouragements.

ملخص

تقنية البلوتوث هي تكنولوجيا لارسال البينات عن طريق الموجات الراديوية ، في نطاق التردد 2.4 الى 2.4835 غيغاهرتز موجه للشبكات المنزلية الصغيرة القصيرة المدى.

هذا النظام اللاسلكي قصير المدى يسمح بتبادل لكل من الصوت و البيانات بتكلفة منخفضة.

والمنتج من طرف LMX في عملنا هذا ، نحاول دراسة ومحاكاة نظام بالاعتماد على دارة متكاملة بالخصوص 3162 .National Semiconductor

الكلمات المفتاحية: الطبقة المادية، النطاق الترددي الصناعي العلمي والطبي، التضمين، الاستخلاص.

Abstract

Bluetooth is a transmission technology supported by radio waves in the frequency band 2.4 to 2.4835 GHz for a home Wireless networking of varied devices near their receiver.
The short-range radio system allows both voice and data exchange at low cost.
In our work, we try to study and simulate a Bluetooth system based on an integrated circuit in particular National Semiconductor LMX3162.
Keywords: physical layer, ISM, system architecture, modulation, demodulation.

Résumé

Le Bluetooth est une technologie de transmission supportée par des ondes radio dans la bande de fréquence 2,4 à 2,4835 GHz permettant une mise en réseau domestique sans fils d’appareils divers et variés en proximité de leur récepteur.
Ce système radio à courte distance permet à la fois les échanges de voix et données à faible coût.
Dans notre travail, nous essayerons d’étudier et simuler un système Bluetooth à base d’un circuit intégré qui porte le nom LMX3162 de National Semiconductor.
Mots clés : couche physique, ISM, architecture de système, modulation, démodulation.

Sommaire

Introduction générale ……..1

Chapitre I : architecture générale de Bluetooth

I.1 Introduction……..…… ..…2

I.2 Contexte de normalisation :……..……...…….…….....2

I.3 Architecture générale du système ……..…….…….…….…..3

I.3.1 Concept de piconet :…….……...3

I.3.2 Concept de scatternet…….……..……3

I.3.3 Identification :……..……..……..…4

I.3.4 Modèle architectural :…… ……....…….5

I.4 canal physique:……..……..…….…….....7

I.4.1 définition :……...…….……....7

I.4.2 Gammes de fréquences :……...…..…….…….... 8

I.4.3 Tranches de temps (Time slots) :……..…….……..... 8

I.4.4 Modulation :……...…….....……...……..... 9

I.4.5 Caractéristiques radio :……....……... ……...…..……. ….10

I.5.1 Liens physiques :……..…..…….……..……..…..…10

I.6. Format général des paquets :……..……...……...…….....12

I.7 Mécanismes de correction d'erreurs :……..……...……..…….… .13

I.7.1 Mécanismes FEC :...……...……...…….……. 13

I.7.2 Mécanisme ARQ :……..……..……14

I.8 Mécanismes de sécurité :……..…...…….….. 14

I.8.1 Sécurité :……..…….…… 14

I.8.2 Gestion des clés……..14

I.8.2.1 Clé unité :……..... 14

I.8.2.2 Clé d'initialisation et clé maitre :…….. …. 15

I.8.3 L'authentification :…….……..16

I. 8.4 Chiffrement :……...……...……..... 17

Chapitre II : présentation et étude du circuit intégré LMX3162

Introduction : ……..…….……...…19

II.1.1 Émetteur :……..…….……..……..……..…….....19

II.1.2 Synthétiseur de fréquence :…….....20

II.1.3 Transmetteur :…….……20

II.2.1 Récepteur :…….…….……25

II.2.2 Démodulation……...:…….…….26

Chapitre III : simulation et les résultats

III.1 Présentation du simulateur :…….……...……..... 31

III.1.1 L'environnement de conception du SystemVue 2006 :……..……..…31

Fenêtre de système :…….31

Barre de menu :…….……32

Barre d'outils :……..32

barrette des blocs :…….……..32

Horloge système : ……33

III.2 Simulation du circuit intégré LMX3162 :……...……...…….…….……34

III.3 Resultatas de Simulation : …….…….……...…….…….…….40

Conclusion générale ……...…..….42

Abréviation :

ACL	Asynchronous Connection Less
ACO	Authenticated Ciphering Offset
AFH	Adaptive Frequency Hopping
AM_ADDR	Active Member Address
ARQ	Automatic Repeat reQuest
BD_ADDR	Bluetooth Device Address
BER	Bit Error Rate
CAC	Channel Access Code
CRC	Cyclic Redundancy Check
DAC	Device Access Code
DH	Data High
DIAC	Dedicated Inquiry Access Code
DM	Data Medium
DV	Data Voice
EDR	Enhanced Data Rate
ESCO	Extended SCO
FEC	Forward Error Correction
FHS	Frequency Hopping Synchronization
FHSS	Frequency Hopping Spread Spectrum
GFSK	Gaussian Frequency Shift Keying
GIAC	General Inquiry Access Code
GPS	Global Positioning System

HCI	Host Controller Interface
HEC	Header Error Code
HV	High-quality Voice
IAC	Inquiry Access Code
L2CAP	Logical Link Controller and Adaptation Protocol
LAP	Low Address Part
LC	Link Controller
LLC	Logical Link Control
LM	Link Manager
LMP	Link Manager Protocol
NAP	Non significant Address Part
OBEX	Object Exchange
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PIN	Personal Identification Number
PM_ADDR	Parked Member Address
POS	Personal Operating Space
PPP	Point to Point Protocol
RSSI	Received Signal Strength Indicator
SCO	Synchronous Connection Oriented
SDP	Service Discovery Protocol
SIG	Special Interest Group
TDD	Time Division Duplex
UAP	Upper Address Part

WAP	Wireless Application Protocol
WLAN	Wireless Local Access Network
WPAN	Wireless Personal Access Network

Liste des figures

Figure I.1 :Topologies de réseaux Bluetooth 4

Figure I.2:Structure de l'adresse BD-ADDR compatible IEEE 5

Figure I.3 : Modèle architectural Bluetooth 7

Figure I.4: Le saut de fréquence 9

Figure I.5: transmission sur un lien SCO 11

Figure I.1: format général des paquets 13

Figure I.7 : Génération de la clé unité 15

Figure I.8 : Génération de la clé d'initialisation 16

Figure I.9 : Authentification d'une station esclave par le maître 17

Figure I.10 : Chiffrement et déchiffrement des données 18

Figure II-1: application typique d'un émetteur-récepteur 20

Figure II-2: L'architecture de l'émetteur du LMX3162. 21

Figure II-3 densité spectrale de puissance du signal transmis GFSK 22

Figure II-4 : La synchronisation exigée pour transmettre en mode de boucle ouverte 23

Figure II-5: La sensibilité en boucle fermée 24

Figure II-6 : La synchronisation exigée pour transmettre des données en boucle bloquée 25

Figure II-7: architecture de récepteur de LMX3162 25

Figure II.8 : circuit démodulateur 26

Figure II.9 démodulateur en quadrature 26

Figure II.10 circuit déphaseur du démodulateur 27

Figure II.11 diagramme de Bode 29

Figure II.12 : courbe caractéristique le démodulateur en quadrature 30

Liste des figures

Figure III.1 : fenêtre de system 31

Figure III.2 : Horloge système 33

Figure III.3 : schéma synoptique d'un émetteur –récepteur Bluetooth 34

Figure III.4 : simulation de Bluetooth par SystemVue 36

Figure III.5 : émetteur Bluetooth 37

Figure III.6 : convertisseur RF en IF 38

Figure III.7 : densité spectrale de puissance de signal de sortie de convertisseur RF en FI 38

Figure III.8 la réponse fréquentiel au niveau du filtre SAW 39

Figure III.9 : chaine de réception 39

Figure III.10 : donnés reçue 39

Figure III.11 superposition des données émies et reçues 40

Figure III.12 : Chronogrammes des données transmises et le saut de fréquence 40

Figure III.13 : les deux saut de fréquence 41

Liste des tableaux :

Tableau I.1-Récapilutatif des versions de Bluetooth SIG 3

Tableau I.2-recapulatif les bandes passantes et les canaux dans certain payes 8

Tableau I.3-différent classe de puissance 10

Tableau I.4-Les différents types de paquet de la bande de base 12

Tableau III.1-caractéristique Bluetooth a simulés 35

Introduction générale



Introduction générale :

Le Bluetooth équipe maintenant un grand nombre de matériels (téléphones, tablettes, claviers, autoradios..), Grâce à cette technologies sans fil, de nouvelles perspectives se sont ouvertes dans le domaine de communication.

La technologie Bluetooth est développée par la société Ericsson, pour véhiculer des données sur de courtes distances, étant donné la puissance d'émission très faible des stations.

Bluetooth utilise une transmission point-à-multipoint où une station maître commande jusqu'à sept esclaves. Le maître est la première station ayant été configurée. L'ensemble du réseau est constitué par le maître et ses esclaves et porte le nom de piconet. Si une huitième station est activée, elle devient la station maître d'un second piconet et ainsi de suite. Les stations maîtres peuvent communiquer de manière à assurer la connectivité entre des stations de piconets distincts.

Bluetooth utilise la bande de fréquence de 2,4 GHz qui présente l'avantage de ne pas nécessiter de licence mais en contrepartie, est une source de bruit importante (micro-ondes,...). Bluetooth utilise le saut de fréquence (FHSS) pour assurer une meilleure robustesse face à ces sources de bruit. La spécification précise jusqu'à 1600 sauts de fréquence par seconde en fonctionnement normal. Une transmission sur une fréquence donnée dure donc au maximum 625 µs. La gestion du saut de fréquence est assurée par la station maître du piconet. Le débit maximum peut atteindre 1 Mbit/s.

A partir de ces avantages et l'utilisation large de cette technologie, nous avons choisi ce projet s'articulant autour de ce sujet.

Le but de l'étude est de faire une recherche bibliographique offrant une description globale de cette technique dans le chapitre, Concernant la norme, l'architecture , les spécifications physiques ,les protocoles…etc.

Le chapitre II est basé sur l'étude de circuit intégré (LMX3162), utilisé pratiquement dans ce domaine.

Le chapitre III est basé sur la simulation de la couche physique et l'interprétation des résultats obtenus.

Une conclusion générale résume l'etude faites ainsi que l'évaluation des performances du circuit intégré par le biais de la simulation.

Chapitre I

architecture générale de Bluetooth



I.1 Introduction

Bluetooth est une technologie par radio à courte portée, conçue en 1994 aux communications mobiles d'Ericsson comme remplaçant de câble pour les dispositifs mobiles. Il devait typiquement être employé pour relier des téléphones portables aux PCs pour synchroniser et aux données d'échange, ou aux accessoires, tels qu'un dispositif mains libres sans fil. Bluetooth a été conçu avec un point fort sur la puissance faible et le coût bas. Ericsson ainsi que Nokia, IBM, Intel, et Toshiba, ont constitué un groupe d'intérêt (SIG),

En 1998, la technologie a été normaliser. en 1999 les spécifications de Bluetooth aboutessent à la version 1.0.

I.2 Contexte de normalisation :

La spécification du système radio Bluetooth est la résultante des efforts conjugués d'un groupe d'industriels réunis autour d'Ericsson en 1998 dans le SIG (Special Interest Group) Bluetooth. Il a initialement été conçu comme un système de remplacement des câbles de connexion utilisés entre les appareils portatifs tels que les téléphones portables, les PDA (Personal Digital Assistant) et les ordinateurs portables. En particulier, il avait pour but de s'affranchir des problèmes d'interconnexion et de configuration liés à l'utilisation d'interfaces filaires.

L'étude des WPAN™ au sein de l'IEEE (Institute of Electrical and Electronics Engineers) a commencé en 1997. Cette activité, démarrée dans le groupe 802.11 WLAN (Wireless Local Access Network) sous l'appellation wearable computing, a donné naissance en 1998 au groupe 802.15. Celui-ci est subdivisé en plusieurs sous-groupes dont le premier, appelé TG1 (ou 802.15.1 a), pour mission de reprendre la spécification initialement produite par des industriels au sein du SIG Bluetooth, afin d'en faire un standard IEEE. La correspondance entre les documents du SIG Bluetooth et des normes IEEE est donnée dans le tableau 1.1.

Par ailleurs, en mars 2006, le SIG Bluetooth s'est engagé vers l'implémentation de l'UWB (Ultra Wide Band), pour contrer la menace représentée par l'USB 2.0 sans fil (ou WUSB) et ses débits de 60 Mbit/s. À l'origine de cette annonce, un accord est signé entre le SIG Bluetooth et la WiMedia Alliance, l'association à l'origine d'une des deux normes UWB du marché, basée sur l'OFDM (Orthogonal Frequency Division Multiplexing). Les produits

Bluetooth nouvelle version offriront des débits théoriques de 100 Mbit/s, soit un bond majeur comparé à la version 2.0 fixée à 3 Mbit/s théorique. [2]

N° de version SIG	Approbation	Norme IEEE correspondante	Approbation par IEEE	Nouveautés
1.0B	Juillet 1999	Non repris par IEEE		Version de base
1.1	Avril 2002	802.15.1-2002	Avril 2002	Mesures RSSI (Received Signal Strength Indicator)
1.2	Novembre 2003	802.15.1-2005	Juin 2005	AFH (Adaptive Frequency Hopping), pour réduire les interférences avec Wi-Fi, ESCO (extended SCO), amélioration de la qualité radio par la retransmission des paquets corrompus.
2.0	Novembre 2004			EDR (Enhanced Data Rate), transmission 3 à 10 fois plus rapide et réduction de la consommation Nouveaux types de paquets

Tableau I.1 -Récapitulatif des versions de Bluetooth SIG

I.3 Architecture générale du système :

I.3.1 Concept de piconet :

Dans la suite, le terme station est utilisé pour désigner tout appareil (PDA, appareil photo numérique, etc.) susceptible de contenir un module de transmission Bluetooth.

Bluetooth a inauguré le concept de piconet : réseau éphémère se utilisé au gré des besoins. La gestion du piconet est centralisée et confiée à une station appelée maître.

Par extension, toutes les stations non maître incluses dans un piconet sont appelées esclaves. Un maître ne peut communiquer qu'avec un des esclaves de son piconet et un esclave ne communique qu'avec son maître. Cette limitation peut en partie être levée grâce à l'interconnexion de plusieurs piconets par une station principale , ou station relais.

L'ensemble constitué d'au moins deux piconets interconnectés est appelé scatternet, "figure I.1"

I.3.2 Concept de scatternet :

Par exemple, si le maître d'un premier réseau devient actif, en tant qu'esclave, dans un deuxième réseau, tous ses esclaves du premier réseau sont, pendant ce temps, bloqués, et le débit diminue. Un esclave et un maître ne peuvent communiquer qu'après avoir négocié une « période *sniff* ». Si l'esclave est alors en communication dans un autre piconet, le maître termine la connexion. Il Faut donc que ces périodes soient différentes et qu'elles ne se recouvrent pas, quand une station appartient à plusieurs piconets.

Les stations décident de leur rôle dans les piconets en fonction des informations qu'elles disposent en local. Il faut des algorithmes efficaces pour que ces choix soient judicieux, et qu'elles puissent changer de rôle, si cela est nécessaire.

Il existe plusieurs algorithmes pour la formation des scatternet, BlueTrees, Bluenet, Bluestars, BlueMesh, TSF, etc. C'est un sujet de recherche important. Bluetooth et la norme SIG ne proposent pas d'algorithme spécifique.

Un réseau Bluetooth est prévu pour avoir au maximum 10 piconets interconnectés, soit 72 stations actives. Tout matériel Bluetooth n'a pas la possibilité technique d'appartenir à plusieurs piconets, c'est précisé dans les caractéristiques techniques du matériel.

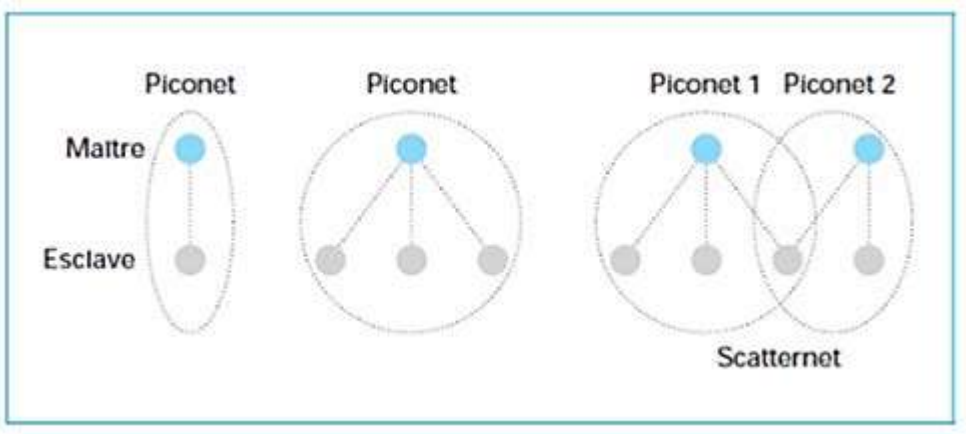


Figure1.1-Topologies de réseaux Bluetooth

I.3.3 Identification :

Chaque équipement Bluetooth possède un identifiant unique appelée BD_ADDR (Bluetooth Device Address). Il est codé sur 48 bits et reprend la même structure que pour Ethernet (spécification IEEE 802-2001). Il est constitué de trois parties, " figure1.2" :

— LAP (Low Address Part) sur 24 bits, correspond au numéro de série du module Bluetooth affecté par le constructeur ;

— NAP (Non significant Address Part) sur 16 bits ;

— UAP (Upper Address Part) est formée des 8 bits de poids forts.

Les deux parties NAP et UAP forment donc un ensemble de 24 bits (3 octets) qui constituent l'identifiant du constructeur du module Bluetooth (figure 1.2). Seules les parties LAP et UAP de l'adresse BD_ADDR sont utilisées dans les algorithmes (principalement l'algorithme de saut de fréquences). C'est cette particularité qui explique le nom NAP (partie non signifiante de l'adresse) attribué aux 16 bits du milieu. **[2]**

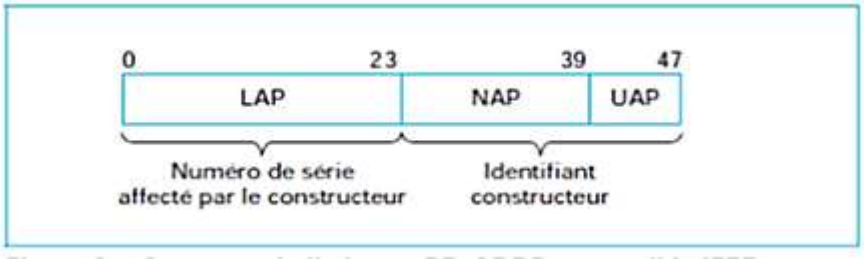


Figure 1.2-Structure de l'adresse BD-ADDR compatible IEEE

I.3.4 Modèle architectural :

Bluetooth propose un modèle architectural qui comprend un empilement de protocoles au sens du modèle OSI, mais qui suggère également une architecture physique, certaines fonctions étant placées dans un module spécifique Bluetooth et d'autres étant placées dans l'équipement (par exemple un ordinateur).

Le modèle place également dans l'architecture les fonctions de gestion interne ,"figure1.3".

Au sens purement protocolaire, l'architecture en couches est la suivante :

— la couche radio spécifie comment sont transmis et reçus les signaux, c'est-à-dire les fonctions de modulation et démodulation ;

— le protocole de contrôle de liaison (LC : Link Controller) comprend les échanges nécessaires pour l'établissement d'un piconet, son maintien ; il gère principalement le multiplexage des différentes transmissions sur une liaison radio unique ;

— le protocole de gestion du lien (LMP : Link Manager Protocol)

permet l'établissement et le contrôle du lien (authentification, chiffrement, polling, gestion du mode économie de batterie) ;

— L2CAP (Logical Link Control and Adaptation Protocol) fournit des services orientés connexion ou non, aux protocoles de niveaux supérieurs. Le multiplexage au niveau LC est géré par une entité interne appelée Baseband Resource Manager. Les autres fonctions de gestion sont prises en charge par l'entité Device Manager. Typiquement les couches basses (radio, LC, LMP) et les gestionnaires (Baseband Resource Manager et Device Manager) sont dans un même module physique appelé Bluetooth Controller. L'interface de commande de ce module est spécifiée précisément et constitue le HCI (Host Controller Interface).

Plusieurs protocoles standard peuvent être utilisés avec Bluetooth :

— SDP (Service Discovery Protocol) offre aux applications clientes les moyens de découvrir l'existence des services fournis par les applications serveurs, ainsi que les propriétés (attributs) de ces services ; il utilise les services de L2CAP ;

— TCS (Telephony Control protocol Specification) est un protocole de signalisation téléphonique au-dessus de L2CAP qui permet d'échanger des commandes (envoi d'un appel, décroché, raccroché, etc.) ;

— RFCOMM, permet l'émulation du port série au-dessus du protocole L2CAP ;

— LLC (Logical Link Control) permet de disposer d'une couche liaison de données IEEE802.2 au-dessus de L2CAP et donc d'être conforme aux standards 802 ;

— la couche Audio gère le codage/décodage numérique de la voix, qui est transportée directement par le LC.

La figure 1.3 donne un exemple d'implémentation d'une architecture Bluetooth. Les fonctions liées aux couches basses sont intégrées dans une carte Bluetooth spécifique. Il s'agit de la partie émission/réception radio (Radio Transceiver), du contrôle de lien en bande de base (Link Controller/Baseband) et de la gestion de lien (Link Manager). Les fonctions des couches plus hautes sont supposées être purement logicielles et intégrées par exemple dans le PC.

Il s'agit de la liaison de données et de services spécifiques. Dans le présent document, le terme « module Bluetooth » est utilisé pour désigner l'entité matérielle hébergeant les fonctions des couches basses (Radio Transceiver, LinkController/Baseband et LM). **[6]**

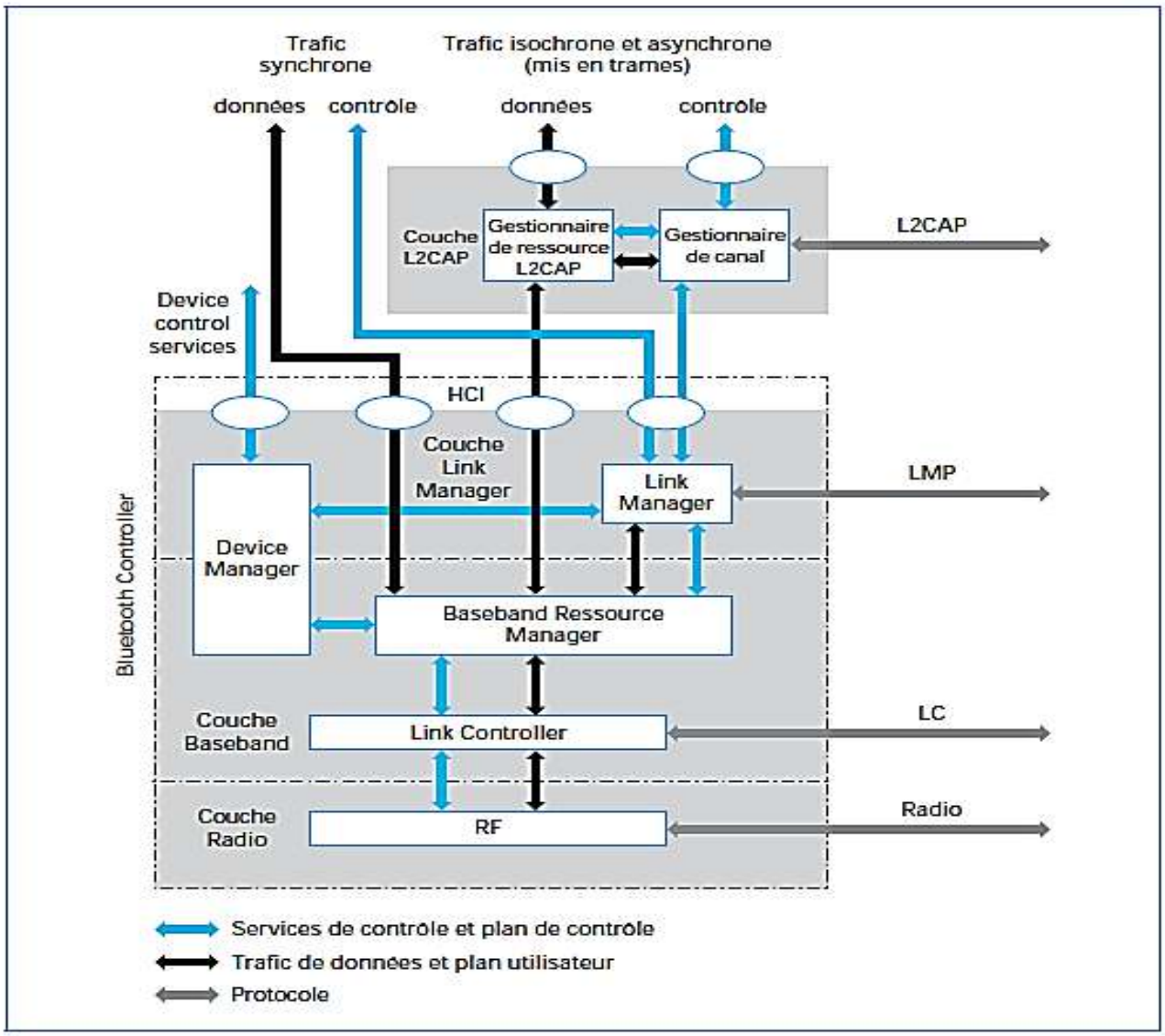


Figure1.3-Modèle architectural Bluetooth

I.4 canal physique :

I.4.1 définition :

Le canal est représenté par saut de fréquence pseudo-aléatoire d'ordre de 79 ou 23 canaux RF. Cet ordre est unique pour le piconet et est déterminé par l'adresse de dispositif de Bluetooth du maître. la phase dans l'ordre de saut est déterminée par l'horloge de Bluetooth du maître. Le canal est divisé en tranches de temps où chaque slot correspond à une fréquence.Le taux nominal de saut est 1600 saut/s. [5]

I.4.2 Gammes de fréquences :

Bluetooth fonctionne dans la bande de 2.4 GHZ ISM. Bien que globalement disponible, l'endroit exact et la largeur de la bande peuvent différer par pays. Aux USA et l'Europe, une bande de largeur de 83.5 MHZ est disponible ; dans cette bande, 79 canaux de RF ont espacé 1 MHZ de distance sont définis. Au Japon, Espagne, et en France, une plus petite bande est disponible ; dans cette bande, 23 canaux de RF ont espacé 1 MHZ de distant sont définis. **[2]**

Country	Frequency Range	RF Channels	
Europe* & USA	2400 - 2483.5 MHz	f = 2402 + k MHz	k= 0,...,78
Japan	2471 - 2497 MHz	f = 2473 + k MHz	k= 0,...,22
Spain	2445 - 2475 MHz	f = 2449 + k MHz	k= 0,...,22
France	2446.5 - 2483.5 MHz	f = 2454 + k MHz	k= 0,...,22

Tableau I.2-recapulatif des bandes passantes et canaux dans certains pays

I.4.3 Tranches de temps (Time slots) :

Le canal est divisé en tranches de temps chaque 625 µs de longueur. Les tranches de temps sont numérotées selon l'horloge de Bluetooth du maître de piconet. La numérotation s'étend de (0 à 227-1) et est cyclique avec une longueur de cycle de 227.

Dans les tranches de temps, le maître et l'esclave peuvent transmettre des paquets.

Un arrangement TDD est employé où le maître et l'esclave transmettent alternativement. Le maître commencera sa transmission dans les tranches paires de temps seulement, l'esclave commence sa transmission dans des tranches de temps impaires seulement. Le début de paquet sera aligné avec le début de slot. Les paquets transmis par le maître ou l'esclave peuvent se prolonger jusqu'à cinq tranches de temps. Le saut de fréquence demeure fixe pour la durée du paquet : **[1]**

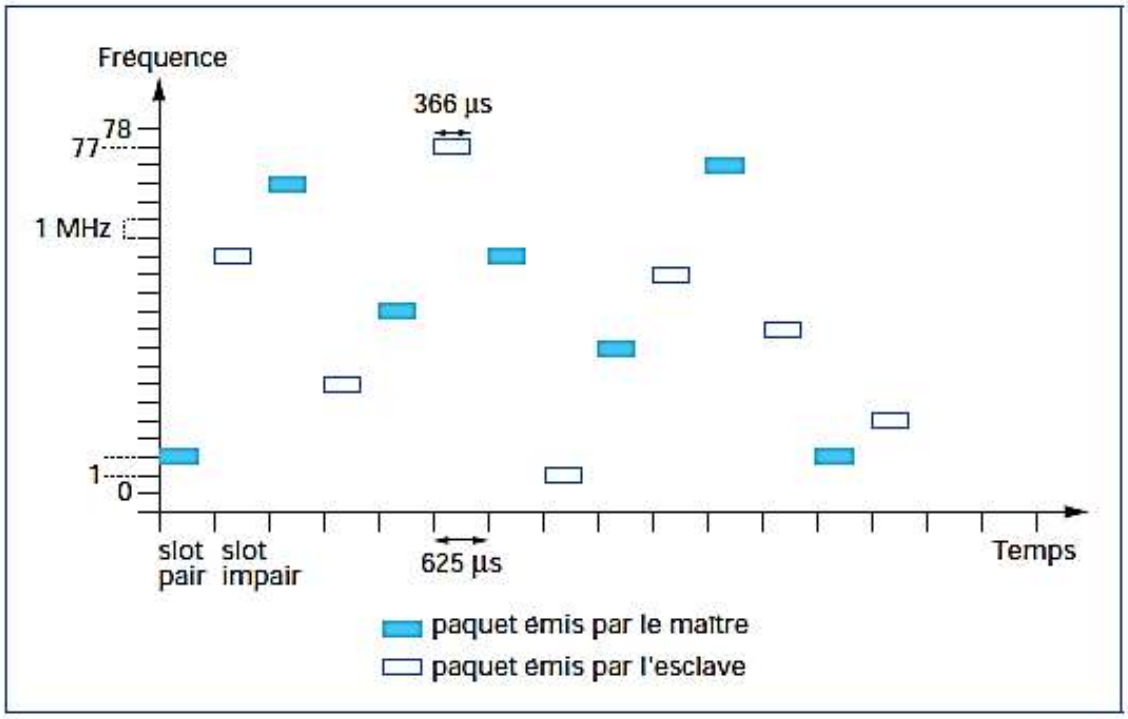


Figure I.4- Le saut de fréquence

I.4.4 Modulation :

La modulation utilisée est GFSK (Gaussian Frequency Shift Keying) avec un débit de 1 Mbit/s sur la voie radio. C'est une modulation de fréquences de type FSK à deux états, dont le signal modulant est filtré par un filtre gaussien. Les données sont transmises sur une fréquence centrale Fc . La modulation FSK fait correspondre à un élément binaire de valeur 1, une déviation de fréquence positive (transmission sur la fréquence Fc + Δf), et à un élément binaire de valeur 0, une déviation négative (transmission sur la fréquence Fc – Δf). L'indice de modulation (2*Δf /D où D est le débit) est compris entre 0,28 et 0,35. ce qui correspond à 140 kHz ≤Δf≤ 175 kHz.

Bluetooth EDR (Enhanced Data Rate) défini dans la version 2.0 du SIG augmente le débit par un facteur de 2 à 3 grâce à des modulations plus évoluées. Avec la DQPSK (Differential Quadrature PSK), on dispose de 2 bits par symbole et on multiplie le débit par 2. Avec une modulation 8-DPSK, on dispose de 3 bits par symbole et on multiplie donc le débit par 3. Pour que l'augmentation de débit soit réelle au niveau applicatif, le taux d'erreur doit rester modéré et donc le rapport signal/bruit du signal doit être plus important si la modulation a plus de points dans la constellation. **[2]**

I.4.5 Caractéristiques radio :

- puissance et sensibilité :

Trois classes de puissance ont été définies : classe 1 à 100 mW (20 dBm), classe 2 à 2,5 mW (4 dBm) et classe 3 à 1 mW (0 dBm).

Les classes de puissance correspondent aux puissances maximales des équipements. Il est possible d'implémenter un algorithme de contrôle de façon à réduire la puissance réellement utilisée .

À l'intérieur, la puissance d'émission dans la bande de fréquences de 2,4 GHz reste limitée à 100 mW, tandis qu'à l'extérieur, l'usage de 100 mW est autorisé entre 2,4 et 2,454 GHz et réduit à 10 mW entre 2,454 et 2,483. afin d'éviter les risques de brouillage avec les appareils de communication militaires [1]. Le contrôle de la puissance est obligatoire pour les équipements de classe 1 et optionnel pour les autres classes. L'intérêt de contrôler la puissance d'émission est double : réduire l'interférence sur les autres utilisateurs du réseau et réduire la consommation d'énergie. Le niveau de sensibilité du récepteur est défini pour un taux d'erreur de bit (BER : Bit Error Rate) de 0,1 %. La norme impose une sensibilité au moins égale à – 70 dBm. Dans un milieu avec des obstacles, la portée maximale pour cette sensibilité sous une puissance de 100 mW est d'environ 100 m.

Classe	Puissance maximale	Puissance minimale	Puissance nominale	Contrôle de puissance	Portée
Classe 1	100 mW (20 dBm)	1 mW (0 dBm)	N/A	Obligatoire entre 4 et 20 dBm	100 m
Classe 2	2,5 mW (4 dBm)	0,25 mW (– 6 dBm)	1 mW (20 dBm)	Optionnel	10 m
Classe 3	1 mW (0 dBm)	N/A	N/A	Optionnel	1 m

Tableau I.3-différentes classe de puissance

I.5.1 Liens physiques :

Il y a plusieurs genres de paquets qui sont liés aux différents types de lien.

Selon l'application, nous identifions globalement trois genres de paquets.

- Paquets de commande : ils sont employés entre le serveur et les esclaves pour porter une information relative la radio (méthode du saut de fréquence, horloge) au lien (établissement, sécurité) ou à la connexion (demandes de connexion).

- le lien SCO est un lien point-à-point entre le maître et un esclave. Il consiste à réserver régulièrement un slot pour le service considéré et il est donc adapté aux services comme la transmission de la voix. Il peut y avoir jusqu'à trois liens SCO par piconet, "figure 1.5". Le maître réserve à des instants périodiques (tous les 2,4 ou 6 slots), deux slots (un dans chaque sens) qui sont consacrés aux flux SCO. **[6]**

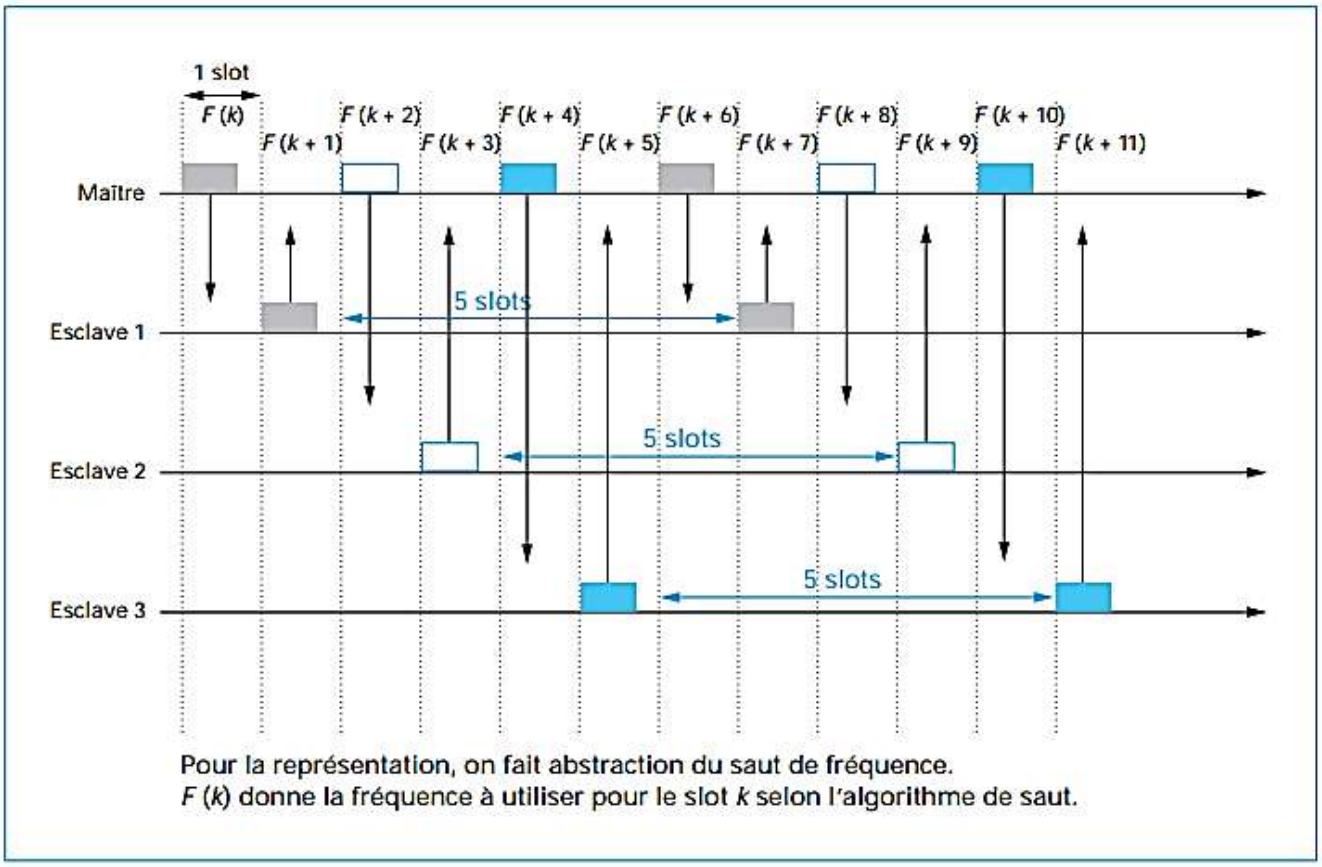


Figure 1.5- transmission sur un lien SCO

- Le lien ACL est un lien point-à-multipoint entre le maître et l'ensemble des esclaves. Il n'en existe qu'un par piconet. Les liens directs entre esclaves ne sont pas possibles, mais peuvent éventuellement être simulés au niveau application. Le lien ACL utilise les slots non réservés par les liens SCO. Le maître attribue les slots afin de satisfaire au mieux les besoins des différents esclaves. Un esclave est habilité à émettre sur le canal s'il a reçu, dans le slot précédent, une trame du maître contenant son adresse comme adresse destination. Pour éviter des tailles d'en-tête importantes, on utilise une adresse courte codée sur 3 bits appelée AM_ADDR qui est allouée lors de la constitution du piconet. Le lien ACL est utilisé pour le transfert de données en tout genre. Les débits sur le lien sont rendus variables par l'utilisation de paquets plus ou moins longs. Ceux-ci peuvent occuper jusqu'à 5 slots. Le service ACL

permet de disposer d'une fonction de contrôle de flux. Si son tampon de réception est plein, une station peut demander l'arrêt des émissions en affectant le bit FLOW.

Le tableau 1.4 rassemble tous les types de paquets définis dans Bluetooth, en précisant leur utilisation et leurs caractéristiques.

Types	Lien	Nom	Signification	Slot	FEC (sur données)	CRC (sur données)	Caractéristiques
Contrôle		ID	Identify	1/2	sans objet	sans objet	Utilisé pour l'*inquiry* et le *paging* Code d'accès uniquement
		NULL	Null	1	sans objet	sans objet	Code d'accès du canal et un en-tête, sans acquittement, pour envoyer de l'information sur le lien
		POLL	Poll	1	sans objet	sans objet	Idem NULL, mais avec acquittement, envoyé par le maître à ses esclaves pour tester les liens
		FHS	FrequencyHopping Synchronisation	1	2/3	oui	Adresse du maître (donc séquence de sauts) et horloge du maître, pour la synchronisation du piconet, avec FEC et CRC
Voix	SCO	HV	High Quality Voice	1	oui	non	Voix avec correction d'erreur 1/3 ou 2/3 FEC sans CRC
Données/voix	SCO	DV	Data Voice	1	2/3 pour données	oui pour données	Voix, données avec correction 2/3 FEC et CRC
Données	ACL	DM	Data Medium	1, 3, 5	2/3	oui	Données avec CRC et correction 2/3 FEC
		DH	Data High	1, 3, 5	non	oui	Idem DM, sans correction d'erreur
		AUX	Auxiliaire	1	non	non	Idem DH, sans CRC

Tableau 1.4-Les différents types de paquet de la bande de base

I.6. Format général des paquets

Un paquet est composé de trois parties : un code d'accès, un en-tête et le corps "figure 1.6". Le code d'accès est utilisé comme identifiant de piconet et permet la synchronisation du récepteur sur l'émetteur. L'en-tête de paquet qualifie le paquet. Il contient des informations telles que le type de paquet et l'adresse du destinataire . Le corps contient les données à transmettre. Dans certaines situations particulières, des paquets ne contiennent que le code d'accès ou bien le code d'accès et l'en-tête mais sans données. **[2]**

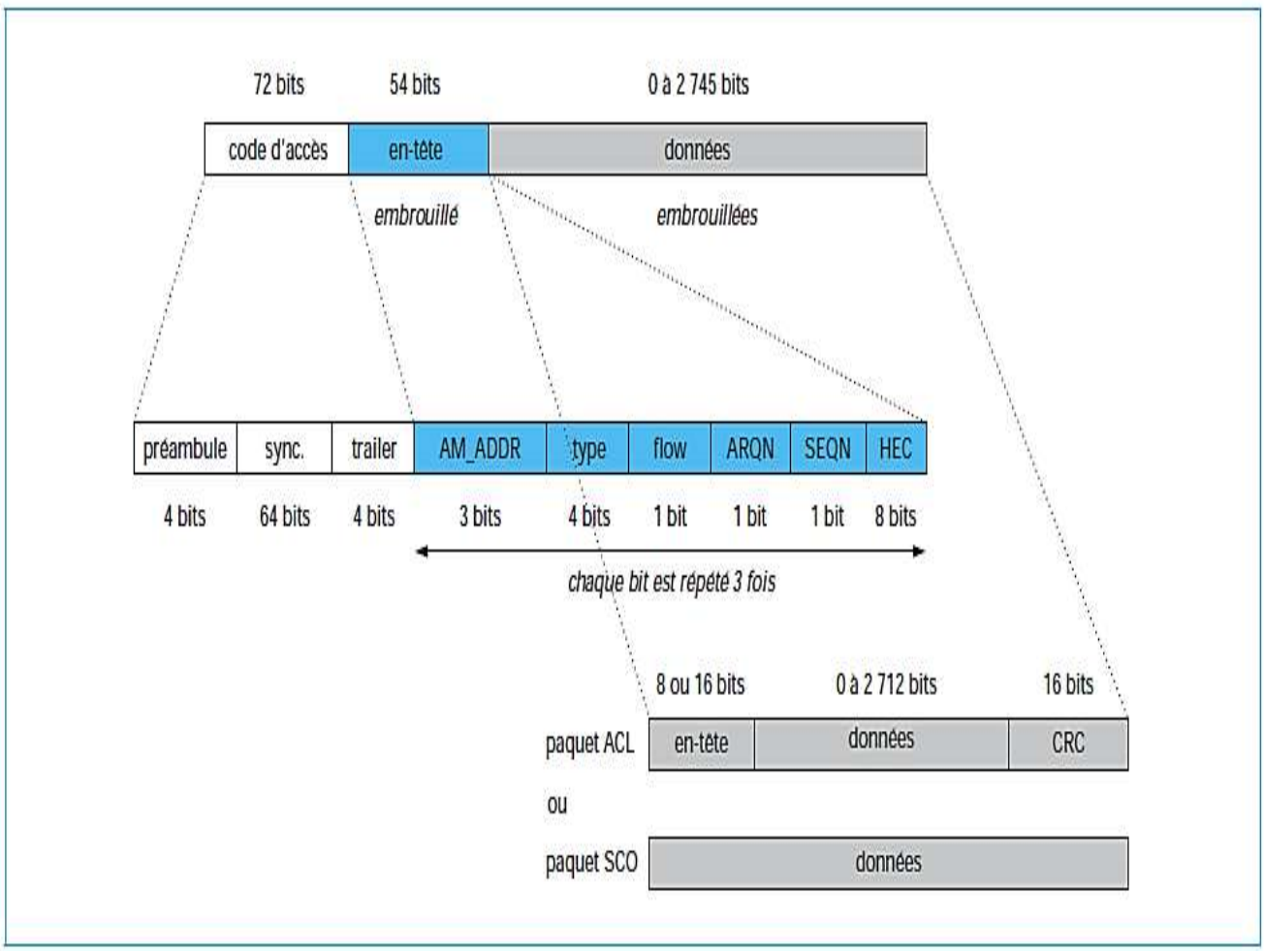


Figure I.6 –format général des paquets

I.7 Mécanismes de correction d'erreurs

Comme la plupart des interfaces radio, Bluetooth permet de combiner la correction d'erreurs par redondance (FEC : Forward Error Correction) et la correction par un mécanisme protocolaire par répétition (ARQ : Automatic Repeat reQuest). [5]

I.7.1 Mécanismes FEC

Deux types de FEC sont possibles :

— code à répétition de taux 1/3 où chaque bit est répété 3 fois (ce codage est peu efficace mais présente l'avantage d'être extrêmement simple).

— code de Hamming de taux 2/3 ; on utilise un code de Hamming court (15, 10). Ce code peut corriger toutes les erreurs simples et détecter toutes les erreurs doubles.

I.7.2 Mécanisme ARQ

Dans le mécanisme ARQ, les paquets sont retransmis jusqu'à ce qu'un acquittement soit reçu, ou que le quantum de temps soit dépassé. Les paquets sont numérotés sur un bit grâce au champ SEQN. En cas de répétition d'un même paquet, le champ SEQN n'est pas modifié. En cas d'émission d'un nouveau paquet, la valeur de SEQN est modifiée. Dans le sens de transmission opposé, le champ ARQN indique un acquittement positif ou négatif. Un paquet de retour perdu est considéré comme un acquittement négatif.

I.8 Mécanismes de sécurité

I.8.1 Sécurité

Du fait de l'utilisation des technologies radio et de la portée maximale théorique des appareils (100 m), les informations circulant dans les réseaux Bluetooth sont susceptibles d'être interceptées, la sécurité est donc un point important.

Différentes politiques de sécurités sont mises en place dans Bluetooth. Il existe 3 niveaux de sécurité.

- Niveau 1 : pas de gestion de la sécurité.
- Niveau 2 : gestion de la sécurité au niveau service.
- Niveau 3 : gestion de la sécurité au niveau établissement de la liaison.

Le niveau 2 de sécurité fait intervenir un processus d'identification lors de l'accès aux services. Le niveau 3 est plus strict, il fait intervenir le processus d'authentification pendant l'établissement d'une connexion. Ceci complique un peu le schéma de connexion vu précédemment. A la suite d'une authentification réussie, des clefs sont créées de part et d'autre.

1.8.2 Gestion des clés

I.8.2.1 Clé unité

Chaque entité a sa propre clé unité, qu'elle génère une seule fois : la première fois qu'elle est allumée. Cette clé est stockée en mémoire. Elle peut être régénérée ultérieurement si, par exemple,

la station change de propriétaire.La clé unité est calculée avec l'algorithme E21, qui prend en entrée l'adresse BD_ADDR de l'entité et un nombre aléatoire.

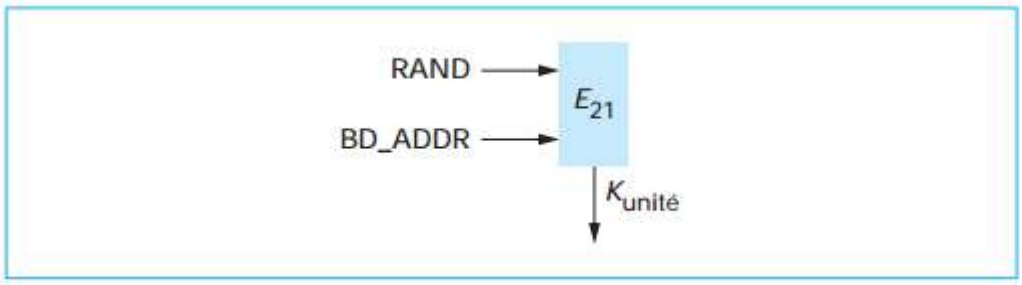


Figure I.7 –Génération de la clé unité

I.8.2.2 Clé d'initialisation et clé maitre

La clé d'initialisation est générée la première fois que deux stations veulent communiquer "figure 1.8". Cette clé est commune à deux stations. Elle impose qu'un même code PIN (Personal Identification Number) soit entré dans les deux stations, par exemple directement par l'utilisateur.

La station A génère un nombre aléatoire qu'elle transmet en clair à B. Les deux stations A et B génèrent la clé d'initialisation Kinit avec l'algorithme E 22, qui prend comme paramètres d'entrée, ce nombre aléatoire, le code PIN et la longueur du code PIN.

La procédure de génération de la clé d'initialisation s'appelle la phase de couplage ou pairing. Cette phase dite de couplage n'est pas nécessaire à chaque nouvelle connexion. Elle intervient seulement lors d'une première connexion entre deux entités, si la sécurité est au niveau de la connexion. Par la suite, elle peut être relancée, lorsqu'une des deux stations ne dispose plus en mémoire d'une clé de liaison pour la station distante. La clé maître est générée de la même façon qu'une clé d'initialisation. Elle sert lorsqu'une station maître veut faire du point-à-multipoint. Le nombre aléatoire est transmis à tous les esclaves et il est nécessaire qu'ils aient tous le même code PIN.

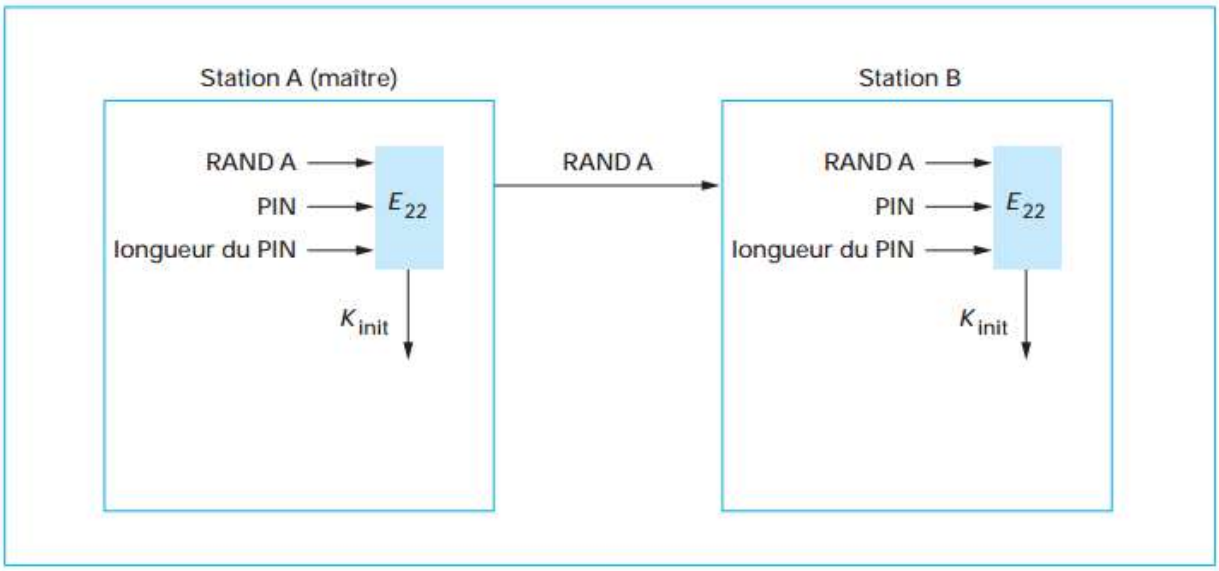


Figure I.8 – Génération de la clé d'initialisation

I.8.3 L'authentification

L'authentification est le processus de vérification de l'entité Bluetooth distante. Lorsque par exemple l'équipement A souhaite authentifier B, le mécanisme suivant est utilisé, "figure 1.9" :
-tout d'abord A envoie à B un nombre aléatoire en clair (RAND A) ;
-ensuite A et B calculent grâce à la fonction d'authentification E1 un résultat XRES pour A (eXpected Result) et SRES pour B (Signed Result). La fonction E1 prend en paramètres le nombre aléatoire RAND A, transmis par A à B, la BD-ADDR de B (connue de A puisqu'une liaison est établie avec B) ainsi que la clé de liaison (link key) ;

— une fois le calcul effectué de part et d'autre, B envoie son résultat SRES à A ;
— A peut alors vérifier si B possède ou non la clé de liaison en comparant les valeurs de SRES avec XRES. Si les deux valeurs sont égales, cela signifie que B possède la clé de liaison et l'authentification a réussi, sinon c'est un échec, B ne dispose pas de la clé de liaison et les stations ne peuvent pas s'authentifier. En plus du résultat servant à authentifier B, la fonction E1 produit un nombre appelé ACO (Authenticated Ciphering Offset). Ce nombre peut, par exemple, servir de base pour les calculs de chiffrement/déchiffrement qui ont généralement lieu après une authentification. C'est l'application qui indique qui devra être authentifié.

Par conséquent, le vérifieur n'est pas toujours le maître. Il peut y avoir également des authentifications mutuelles. Un délai est introduit si l'authentification échoue avant qu'on ne puisse la retenter. Il double après chaque échec de la même adresse jusqu'à ce que le maximum, fixé par l'application, soit atteint.

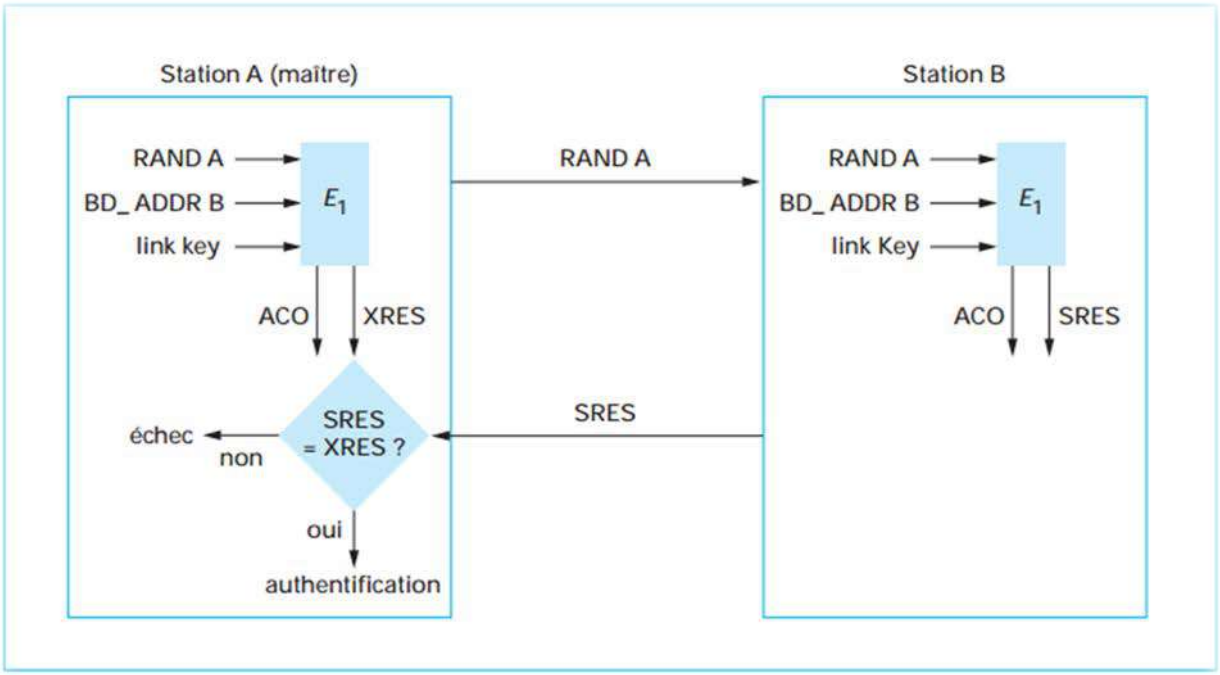


Figure I.9- – Authentification d'une station esclave par le maître

Le but n'est plus de vérifier que cette clef produite chez A est la même que chez B, mais simplement de s'en servir pour pouvoir déchiffrer les données envoyées. Les paramètres employés ici sont : un nombre aléatoire RAND créé par A, le No de série de A (BD_ADDR), l'horloge de A (clock) ainsi qu'une clef (Kc). La clef Kc elle est créée du coté de A et du coté de B grâce aux valeurs suivantes : le chiffre RAND, le chiffre précédemment calculé lors d'une authentification, l'ACO et la clef de lien. [2]

I. 8.4 Chiffrement

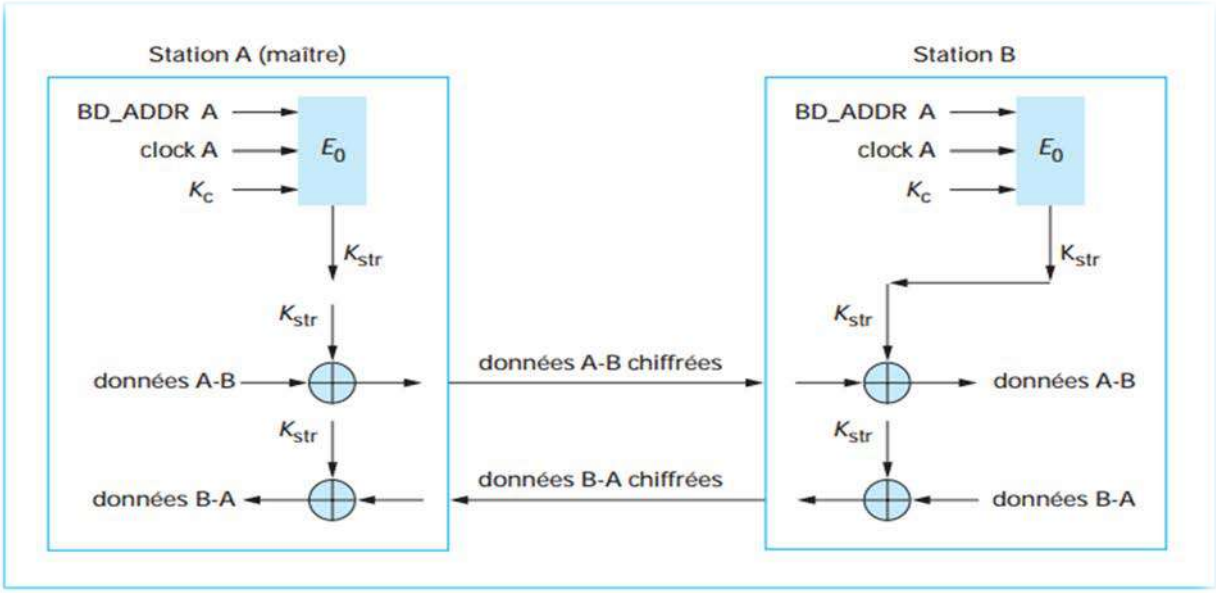
La procédure de chiffrement s'effectue suivant trois phases :

- négociation du mode de chiffrement, pas de chiffrement, chiffrement des paquets point-à-point, chiffrement des paquets point-à-point et point-à-multipoint ;
- négociation de la taille de la clé ;
- chiffrement.

La clé de chiffrement (Kc) est obtenue avec l'algorithme E3 à partir de la clé de liaison, d'un nombre aléatoire généré par la station maître et transmis en clair, et du nombre ACO calculé lors de l'authentification "figure1.10 ". Le nombre de bits de la clé de chiffrement entre 8 et

128 bits doit être négocié entre les deux stations. C'est l'application qui détermine un minimum acceptable pour éviter de baisser le niveau de sécurité.

Le mécanisme de chiffrement/déchiffrement est basé sur l'algorithme E0 qui produit une clé de chiffrement/déchiffrement (Kstr) à partir de la clé Kc, de l'adresse du maître et de son horloge, "figure 1.10". La valeur de l'horloge étant différente à chaque slot, la clé Kstr produite change à chaque paquet transmis. Il suffit alors de faire un XOR (ou exclusif) entre les données du paquet en clair et la clé Kstr pour avoir les données chiffrées. Le processus de déchiffrement est identique on réapplique la clé Kstr aux données chiffrées pour avoir les données en clair.



FigureI.10- – Chiffrement et déchiffrement des données

Chapitre II

présentation et l'étude du circuit intégré LMX3162



Introduction :

Notre étude est sur la simulation de la technique Bluetooth, basé sur l'emploi d'un circuit intégré spécifique. Ce circuit est dédié à la firme National Semiconductor.

Le LMX3162 Single Chip Transceiver radio est un émetteur-récepteur radio, intégré monolithique, optimisé pour une utilisation dans les systèmes sans fil ISM 2,45 GHz.

II.1.1- Émetteur

Le LMX3162 intègre un émetteur, récepteur sur une seule puce de silicium. la PLL et un doubleur de fréquence pour produire la transposition en fréquence dans la bande souhaitée. Le récepteur et l'émetteur partagent la même PLL. La "figure II-1" montre une implémentation typique d'une radio 2,4 GHz d'émetteur-récepteur en utilisant le LMX3162. En plus de la PLL et doubleur de fréquence ,un mélangeur à faible bruit 2,5 GHz , un amplificateur à fréquence intermédiaire (IF), un amplificateur limiteur, un discriminateur de fréquence, un indicateur de signal reçu (RSSI), et l'amplificateur d'émission, sont également intégrés. Notez que les VCO et des filtres de rejet image n'ont pas besoin d'être à l'extérieur. Le schéma de modulation mis en œuvre dans le LMX3162, est le déplacement de fréquence gaussienne (GFSK).

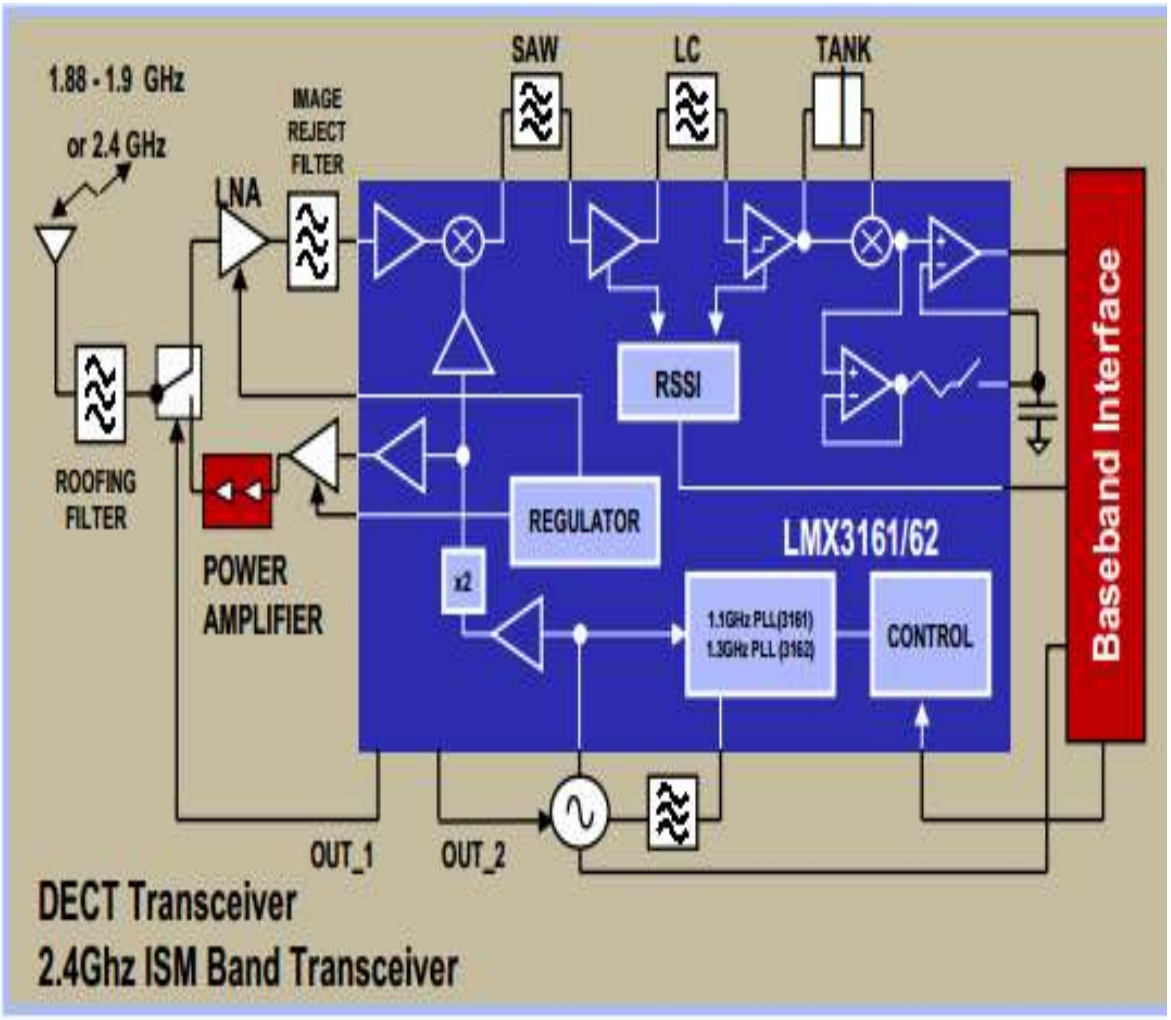


Figure II-1: application typique d'un émetteur-récepteur 2,4 GHz en utilisant LMX3162

II.1.2 Synthétiseur de fréquence

Pour générer la fréquence porteuse souhaitée, le LMX3162 prend la sortie d'une boucle PLL fonctionnant à 1,3 G Hz et la passe à travers un doubl eur de fréquence. cette architecture permet de réduire les perturbations de l'amplificateur de puissance de l'oscillateur controllé par tension à la PLL. Comme le montre la Figure II-1, la PLL est partagée entre l'émetteur et le récepteur. Le partage de la PLL est seulement possible dans les systèmes semi-duplex. En général, la PLL est la principale source de dissipation de puissance dans le LMX3162.

II.1.3 Transmetteur

Pour transmettre des données, le LMX3162 utilise un schéma de modulation directe de l'oscillateur commandé en tension comme le montre la "figure II-2". En général, moduler directement le VCO utilise une énergie plus faible que les autres architectures d'émetteurs

radio. Lors de la transmission d'un signal, un s ignal en bande de base filtré passe-bas Gaussien est appliqué à la broche de réglage de l'oscillateur VCO. L'amplitude et le débit calculée des données du signal de bande de base produit une déviation de fréquence positive ou négative à partir de la fréquence porteuse nominale de la PLL.

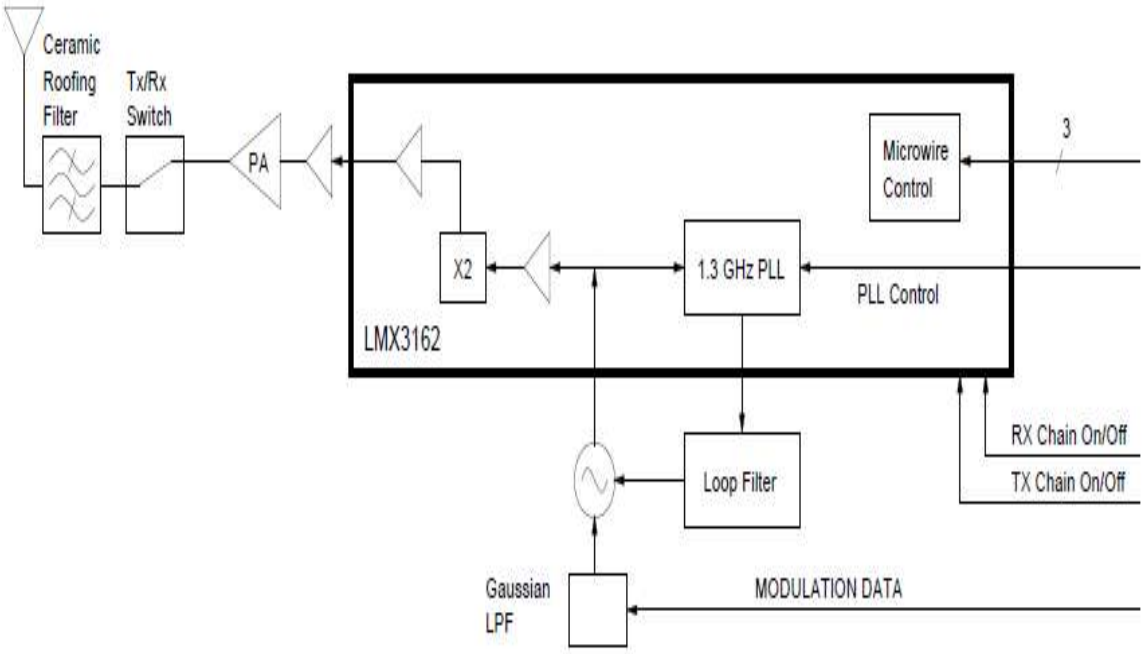


Figure II-2: L'architecture de l'émetteur du LMX3162. [4]

Comme la LMX3162 est destinée à fonctionner avec un débit R = 1 Mbps, afin de réaliser une déviation de fréquence spécifique à partir du support, seule l'amplitude du signal doit être ajustée. La densité spectrale de puissance idéale du signal transmis est représenté sur la figure II-3.

Les données d'entrée sont supposé être une séquence de bruit stationnaire, le débit du signal de données est fixé à R = 1 Mbps, l'indice de modulation est de BT = 0.5 , et la bande passante de boucle de la PLL est floop = 10 kHz. Une fois le signal d'émission est émis par LMX3162 via le doubleur de fréquence, le signal d'émission aura besoin d'être amplifié car la broche TX fournit un niveau de puissance de sortie de -7,5 dBm seulement [3]. Lorsque on a la modulation du VCO, la PLL peut être soit ouverte ou fermée. Il ya des avantages et des inconvénients des deux techniques. En modulation en boucle ouverte, la PLL doit d'abord être verrouillée sur la fréquence porteuse souhaitée avant la transmission. Cela va prendre une

période de temps déterminée. Le temps exact nécessaire pour l a PLL pour ce verrouiller dépend de la mise en place exacte de la radio. Au cours de la transmission de données, la boucle est déverrouillée et le VCO est directement modulé par le signal en bande de base. Cependant, puisque la PLL dérivera quand il est ouvert, un nombre limité de bits peut être transmis avec succès selon la façon dont la dérive change rapidement la sensibilité du récepteur. Pour assurer que cette dérive est suffisamment lente, de telle sorte qu'un nombre important de bits peut être envoyé, la dérive de fréquence de l'oscillateur VCO doit être négligeable par rapport à la porteuse fréquence. Afin de réaliser une dérive basse fréquence, un grand condensateur dans le filtre de boucle peut être nécessaire. Malheureusement, en ajoutant simplement la capacité, le temps de verrouillage va augmenter . En outre, même si la dérive est faible, le nombre de bits est encore limitée.

Si la conversion abaisseuse de fréquence déplace le contenu du signal à l'extérieur de l'IF, tous les bits ne seront pas décodés correctement .Au lieu de cela, tous les bits apparaissent comme un 1 ou un 0 en fonction de l'endroit où le contenu du signal se situe par rapport à l'IF.

"Figure II-4" affiche la synchronisation qui doit être utilisée quand des données sont transmises utilisant le mode de boucle ouverte.

Dans le mode de boucle fermée, la PLL implique que plus d'alimentation électrique sera utilisée pendant la transmission.

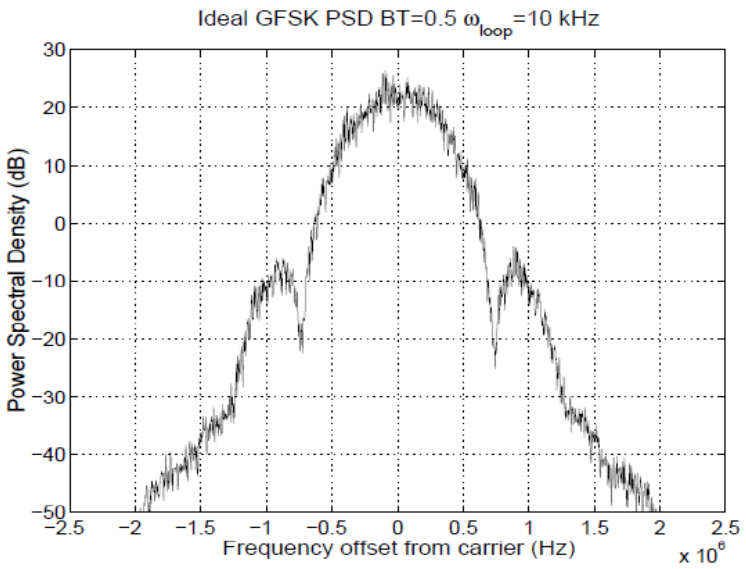


Figure II-3: densité spectrale de puissance du signal transmis GFSK

Le débit du signal de données est supposée être 1 Mbps, l'indice de modulation est de BT = 0.5 , et la bande passante de boucle de la PLL est floop = 10 kHz. La fréquence porteuse est généralement centré dans la gamme 2,40 GHz à 2,49 GHz. Un écart positif correspond à la transmission d'un 1 et un écart négatif correspond à la transmission d'un 0.

En outre, de longues séquences de uns ou de zéros auront une incidence sur la capacité du récepteur à décoder les données dans un mode nuisible. Supposons que l'utilisateur transmet une séquence des uns . Cette séquence de uns provoque une déviation de fréquence positive + Δ f de la porteuse. Initialement, la densité spectrale de puissance présentera une raie $fc + \Delta f$.

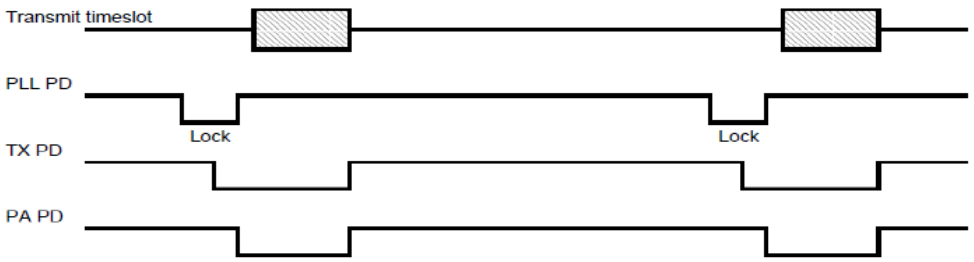


Figure II-4: La synchronisation requis pour transmettre des données en utilisant le mode en boucle ouverte est représentée. [3]

Notez que lorsque PLL PD est faible, la PLL est en marche et quand TX PD et PA PD sont faibles, l'amplificateur d'émission est activé. Notez qu'une période de temps déterminée doit être dépensée avant le verrouillage de la PLL. Egalement, la chaîne de transmission est activée avant que la boucle PLL est coupée. [3]

Cependant, parce que la PLL est a conçue pour ajuster le VCO interne tel que la PLL produira la fréquence désirée *fc* . l'écart de fréquence disparaîtra dans 1/*f*loop ou *f*loop est la bande passante de boucle. En conséquence, en raison de la technique de démodulation utilisée, récupérer les données correctement deviendra impossible.

La figure II-5 montre l'effet de l'envoi de longues séquences de uns ou de zéros, à l'entrée de modulation de l'oscillateur commandé en tension , sur la densité spectrale du signal d'émission. Si le problème de l'écart est pris en compte, alors l'avantage du mode en boucle fermée, est que des séquences plus longues de données peuvent être envoye. Notez que

pendant le temps où les données ne sont pas envoyées, la modulation directe entrée du VCO sera soumise à une longue séquence de zéros. Si la PLL est laissée au moment où aucune donnée n'est envoyée, la boucle à verrouillage de phase va tenter de se verrouiller sur une fréquence qui est -Δf ' kHz' de la fréquence souhaitée.Dans ce cas, pour éviter les problèmes de démodulation au niveau du récepteur, une séquence d'apprentissage devra être envoyée avant les données, pour s'assurer que la fréquence porteuse est produite correctement.

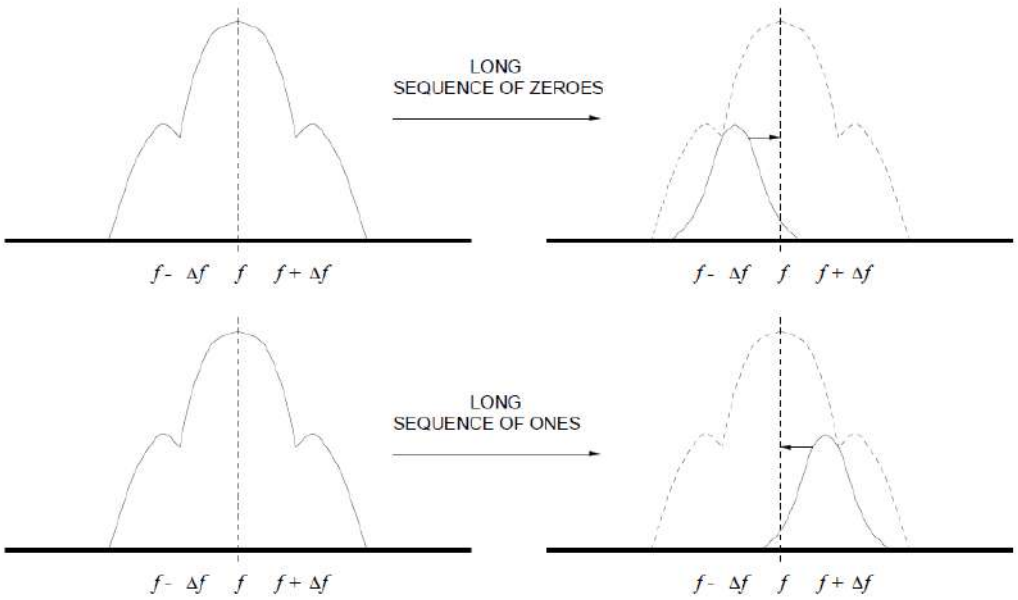


Figure II-5 La sensibilité en boucle fermée

La sensibilité en boucle fermée pour de longues séquences de 1 ou de 0 est exposée par la densité spectrale de puissance à la sortie de l'émetteur. Supposons que l'fréquence porteuse nominale est fc = 2,40 GHz et la déviation de fréquence typique est Δf .Lorsque l'une d'une longue séquence de 1 ou de 0 est appliqué à l'oscillateur commandé en tension, la réponse en fréquence de la PLL tend vers *fc* +Δ*f* ou *fc* -Δfc en fonction de la valeur de la séquence comme indiqué. Finalement, l'écart va disparaître en raison du comportement naturel de la PLL. Fermé Alternativement, on peut éteindre la PLL avant les données envoyées. Puis, lorsque les données doivent être envoyés, la PLL serait refermée. Après le temps de blocage, les données sont ensuite envoyées. Après que toutes les données ont été transmises, la PLL sera éteint à nouveau. Dans ce scénario, une séquence d'apprentissage peut ne pas être nécessaire. La synchronisation exigée pour la transmission de boucle fermé est affichée sur le schéma II-6.

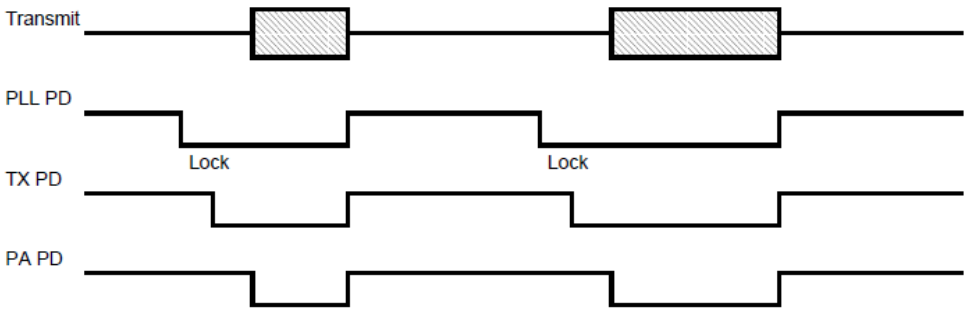


Figure II-6 : La synchronisation exigée pour transmettre des données en mode de boucle bloquée

II.2.1 Récepteur

La chaîne de réception de la LMX3162 utilise une architecture hétérodyne comme le montre la figure II-7

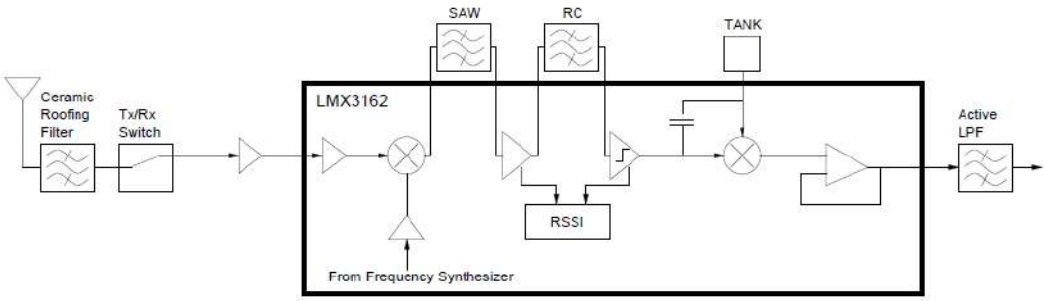


Figure II-7: architecture de récepteur de LMX3162

Le signal reçu est d'abord mélangée vers le bas à la fréquence intermédiaire (IF) avec un signal oscillant de 2,4 GHz. La fréquence IF est 110,6 MHz. Ensuite, le signal reçu passe à travers un filtre d'onde de surface acoustique (SAW) pour un re jet du bruit et des fins de filtrage. En outre, le filtrage est effectué en utilisant un filtre passe-bas RC. Le signal en bande de base reçu est produit par la démodulation du signal à l'aide du circuit tank. la Démodulation du s ignal centré autour de 110,6 MHz utilise un produit en technique de seuillage. Tout signal reçu qui a un é cart de fréquence positif (+Δf) de 110,6 MHz sera décodé comme un 1, et un signal avec une déviation négative (-Δf) sera décodé comme un 0 par le démodulateur.

II.2.2 Démodulation

Ce démodulateur est un circuit déphaseur dont la phase varie linéairement en fonction de la fréquence mais ne modifie pas l'amplitude de signal.

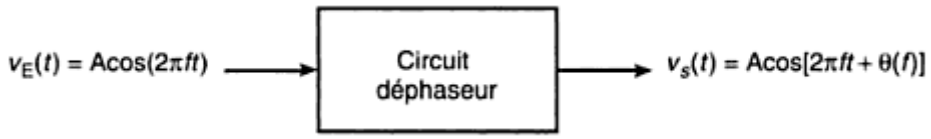


Figure II.8 circuit démodulateur

On choisi un circuit déphaseur θ(f) donné par l'équation suivante :

$$\theta(f) = \frac{\pi}{2} - \gamma \times (f - f_p)$$

Ou γ est la coefficient du démodulation

A la fréquence de la porteuse, le déphasage apporté par le circuit déphaseur est égale π/2, d'où le nom de démodulateur en quadrature.

Ensuite , il suffit d'utiliser un détecteur de phase pour obtenir un signal démodulé à la sortie de dispositif . L'ensemble est organisé selon le schéma suivant de la figure **II.9** :

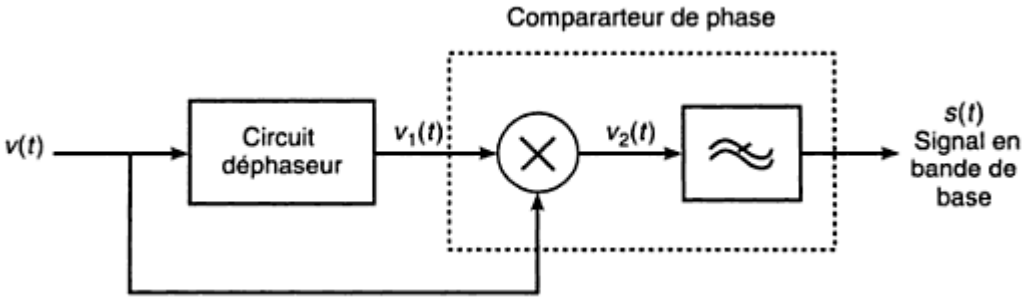


Figure II.9 démodulateur en quadrature

Le comparateur de phase est réalisé à l'aide d'un multiplieur et d'un filtre passe- bas .

Pour expliquer le fonctionnement d'un démodulateur en quadrature, nous pouvons écrire l'équation suivante :

Le signal d'entrée correspond au signal modulé en fréquence :

$$v(t) = A\cos\left[2\pi f_p t + \phi(t)\right]$$

A la sortie de circuit déphaseur , nous avons :

$$v_1(t) = A\cos\left[2\pi f_p t + \phi(t) + \theta(t)\right]$$

Le multiplieur founit la tension

$$v_2(t) = Kv_1(t)\, v(t)$$

Alors :

$$v_2(t) = \frac{KA^2}{2}\left[\cos\left(\theta(t)\right) + \cos\left(4\pi f_p t + 2\phi(t) + \theta(t)\right)\right]$$

On obtient un terme basse fréquence cos[θ(t)] et un terme haute fréquence centré sur 2fp .

Le filtre passe – bas élimine le terme haute fréquence et il reste pour le signal de sortie :

$$s(t) = \frac{KA^2}{2}\cos\left(\theta(t)\right) = \frac{KA^2}{2}\cos\left[\frac{\pi}{2} - \gamma \times \left(f(t) - f_p\right)\right] = \frac{KA^2}{2}\sin\left[\gamma \times \left(f(t) - f_p\right)\right]$$

Comme f(t)=fp+k f m(t) , nous avons :

$$s(t) = \frac{KA^2}{2}\sin\left[\gamma k_f m(t)\right].$$

Nous pouvons faire un développement limité d'ordre 1 de sinθ, alors :

$$\boxed{s(t) \approx \frac{KA^2}{2}\gamma\, k_f m(t)}$$

Nous retrouvons bien le signal modulant m{t) à la sortie de démodulateur.

Pour éliminer les fluctuations d'amplitude du signal modulé, on rajoute un circuit limiteur à l'entrée du démodulateur.

En pratique,le déphaseur est réalisé à l'aide du circuit de la figure II.10 :

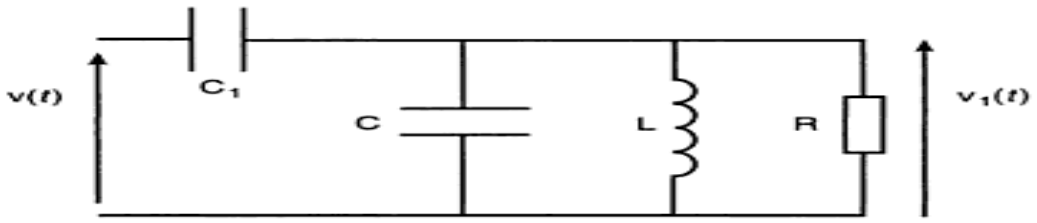


Figure II.10 circuit déphaseur du démodulateur

Calculons la fonction de transfert en régime harmonique :

$$\underline{T}(j\omega) = \frac{\underline{V}_1}{\underline{V}} .$$

D'après le diviseur de tension nous pouvons écrire :

$$\underline{T}(j\omega) = \frac{\underline{Z}_{eq}}{\underline{Z}_{eq} + \frac{1}{j\omega C_1}} = \frac{j\omega C_1}{j\omega C_1 + \underline{Y}_{eq}}$$

Avec :

$$\underline{Y}_{eq} = j\omega C + \frac{1}{j\omega L} + \frac{1}{R}$$

Soit :

$$\underline{T}(j\omega) = \left(\frac{C_1}{C_1 + C}\right) \frac{(j\omega)^2 L(C + C_1)}{1 + j\omega \frac{L}{R} + (j\omega)^2 L(C + C_1)}$$

Nous obtenons la fonction de transfert d'un filtre passe haut que nous exprimons sous la forme suivante :

$$\underline{T}(j\omega) = \alpha \frac{\left(j \frac{\omega}{\omega_0}\right)^2}{1 + j \frac{\omega}{\omega_0} \times \frac{1}{Q} + \left(j \frac{\omega}{\omega_0}\right)^2}$$

Avec :

$$\alpha = \frac{C_1}{C_1 + C} \quad , \quad \omega_0 = \frac{1}{\sqrt{L(C + C_1)}} \quad \text{et} \quad Q = R\sqrt{\frac{C + C_1}{L}} .$$

A la pulsation propre ω_0 .on obtient :

$$\boxed{\underline{T}(j\omega_0) = j\alpha Q}$$

En pratique ,le coefficient de qualité de filtre est très supérieur de un, et on obtient un phénomène de résonance très important .

La figure II.11 représente le diagramme de Bode pour un coefficient de qualité égal à 10, un coefficient de ½,pour la variable réduite x=f/f0 sur l'axe des abscisses .

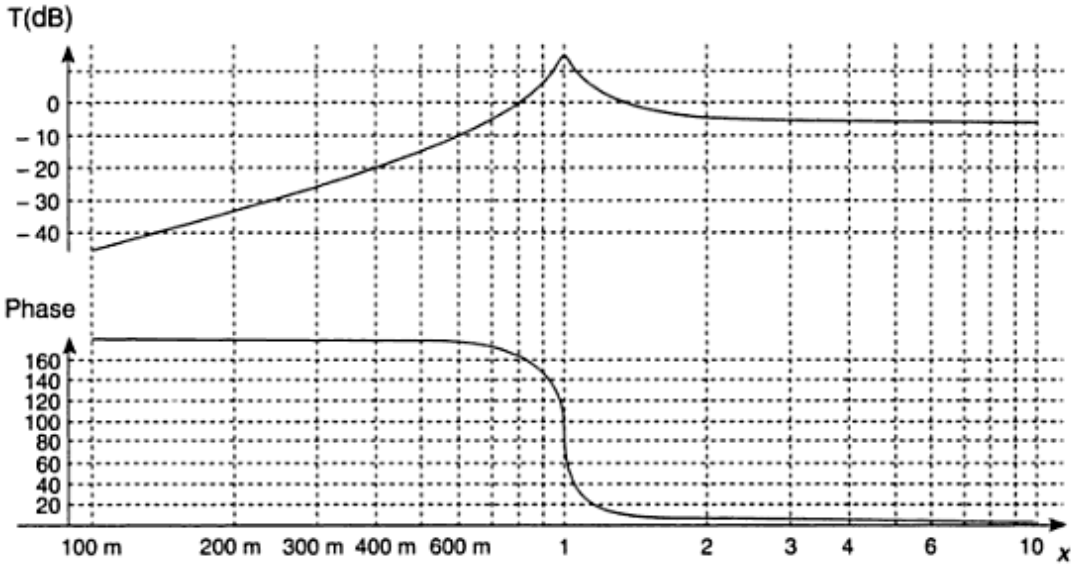


Figure II.11 diagramme de Bode

Le circuit est réglé pour que la fréquence f0 soit égale à la fréquence de la porteuse.

Pour cette fréquence, le déphasage es égal à π/2.

Pour que le filtre passe –haut fonctionne en circuit déphaseur , il faut que les variations autour de la fréquence f0, soit inférieures à la bande passante à -3dB, B=f0 /Q ,du filtre passe haut .

Nous pouvons exprimer le déphasage du circuit de la façon suivante :

$$\phi(f) = \frac{\pi}{2} + \tan^{-1}\left[\frac{1-\left(\frac{f}{f_0}\right)^2}{\frac{f}{Q \times f_0}}\right]$$

A l'aide d'un développement limité au premier ordre , nous pouvons écrire :

Pour le numérateur :

$$1-\left(1+\frac{\Delta f}{f_0}\right)^2 \approx 1-\left(1+\frac{2\Delta f}{f_0}\right) = \frac{-2\Delta f}{f_0}$$

Pour le dénominateur :

$$\frac{1}{Q}\left(1+\frac{\Delta f}{f_0}\right)\sim\frac{1}{Q}$$

Donc :

$$\phi(\Delta f)\sim\frac{\pi}{2}-\tan^{-1}\left(\frac{2Q\Delta f}{f_0}\right)$$

On suppose que $\tan^{-1}(2Q\Delta f/f0) <1$ rad , ce qui nous permet de faire à nouveau un développement limité de $\tan^{-1}(x)=x$, on obtient l'equation d'une droite pour le déphasage autour de f0 :

$$\phi(\Delta f)\sim\frac{\pi}{2}-\frac{2Q}{f_0}\Delta f.$$

A la sortie du démodulateur, on a donc :

$$s(f)\sim\frac{KA^2}{2}\frac{2\alpha Q^2}{f_0}(f-f_0)=a(f-f_0)$$

Tel que a, est le coefficient de sensibilité du démodulateur ,qui est la pente de caractéristique de s(f),et elle s'exprime en en V/Hz. Figure II.12

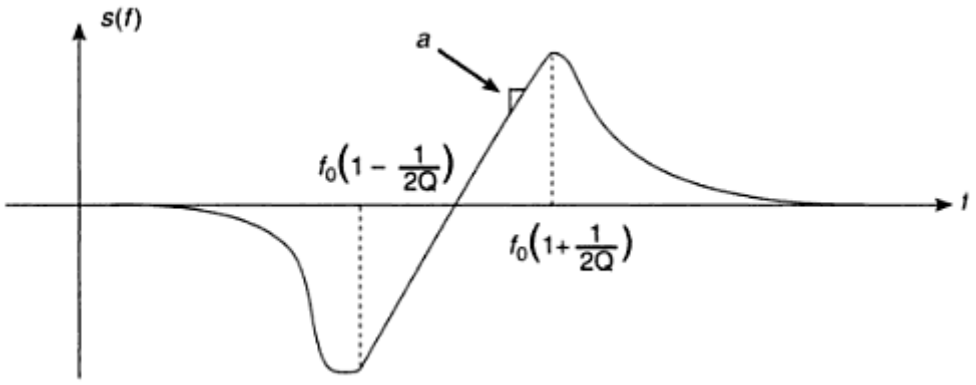


Figure II.12 : courbe caractéristique le démodulateur en quadrature

Chapitre III

Simulation du circuit intégré LMX3162





III.1 Présentation du simulateur :

SystemVue est un environnement de conception en bande de base et de communication RF, développé par Agilent Technologies. SystemVue dispose de vastes possibilité professionnelles qui prennent en charge le traitement numérique du signal DSP, conception RF analogique, et la conception de normes telles que IEEE 802.11g, Bluetooth et UWB. SystemVue peut également être utilisé pour simuler les représentations de diagrammes typiques des principes fondamentaux des systèmes de communication. L'affichage de signal temporel et spectral peut illustrer à la fois la performance idéale et dégradée de bruit additif et non-linéarités du système étudié.

III.1.1 L'environnement de conception du SystemVue 2006

L'environnement de conception par défaut, comprend plusieurs éléments de développement.

1. Fenêtre de système :

La fenêtre de système, représentée sur le schéma 3.1, se compose d'une barre de menu, une barre d'outils, des barres de défilement horizontales et verticales, une région de conception, une zone de message, et un réservoir symbolique.

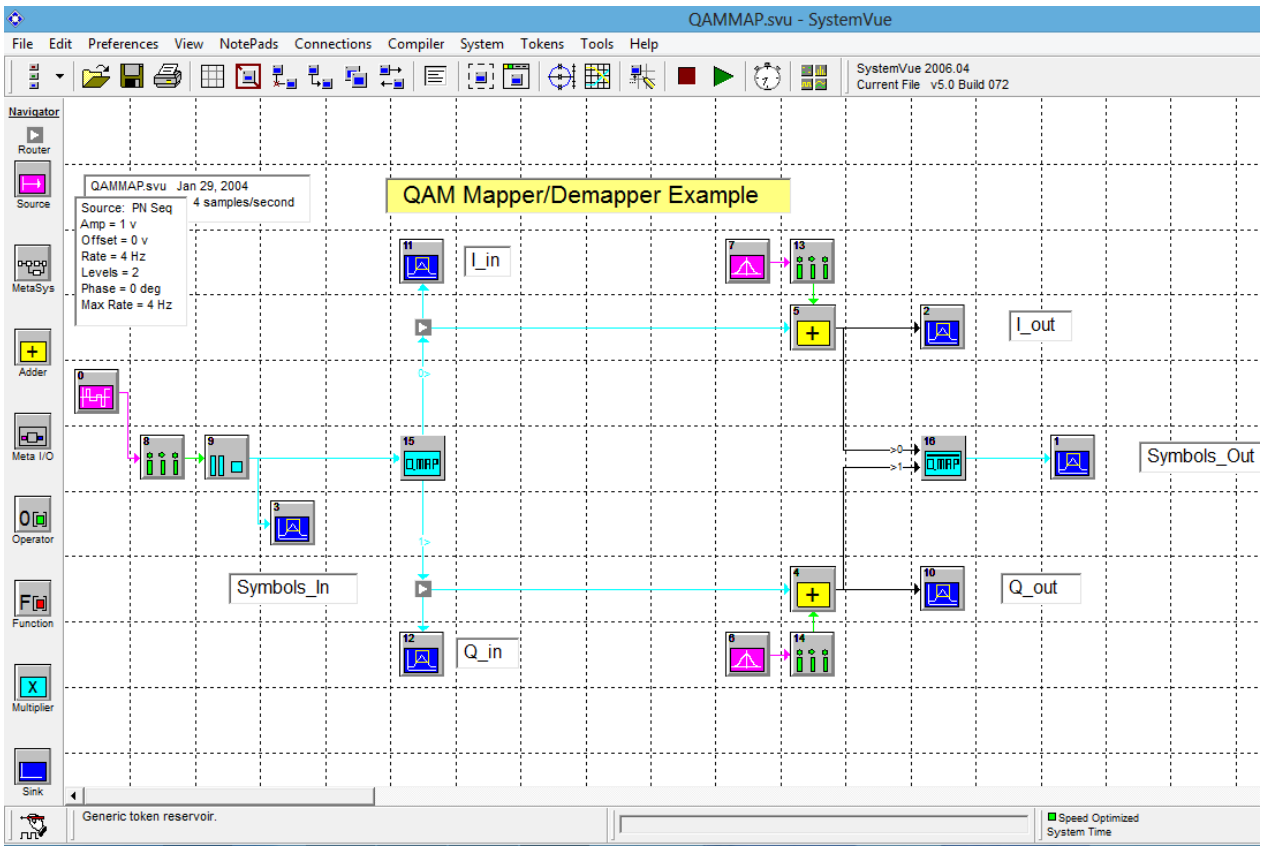


Figure III.1 : fenêtre de conception de system

2. Barre de menu :

La barre de menu affiche les fonctions et les commandes utilisés dans SystemVue : File, Edit, View, Preferences, NotePads, Connections, Compiler, System, Tokens, Tools, and Help.

3. Barre d'outils :

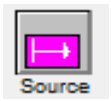
La barre d'outils se compose des boutons auxquels s'attachent certaines fonctions :

- Agissement sur des blocs ou groupes de bloc situés dans la fenêtre de système,
- Commencement et arrêt d'une simulation.
- accès à la fenêtre d'analyse et à d'autres fonctions de service.

4. barrette des blocs :

Les blocs sont des modules utilisés dans les simulations de SystemVue. La barrette sur l'aile gauche de la fenêtre ,affiche les blocs génériques représentant ceux disponibles par défaut .

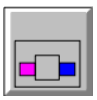
 **Bouton de bibliothèques :** permet d' alterner entre les réservoirs de bibliothèques standards et optionnelles de SystemVue.

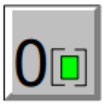


Bloc de sources : Ce bloc contient des sources des signaux à sorties seulement, et représente une bibliothèque de différentes source, (y compris à partir des fichiers externes) employées pour servir d' entrées de système.



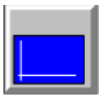
Bloc MetaSystem : Ce bloc permet d'ajouter la hiérarchie à une conception. il est employé pour importer un MetaSystem prédéfini dedans, vers le système actuel sous la conception.

 **Bloc I/O de MetaSystem:** Ce bloc définit les noeuds d'entrée et de sortie dans un MetaSystem.

 **Bloc d'opérateurs :** Ce bloc représente une bibliothèque d'opérateurs qui utilisent les données d'entrée comme arguments à l'exécution à l'aide d'opérateurs spécifique.



Bloc de fonctions: Ce bloc représente une bibliothèque des fonctions qui utilisent les données d'entrée comme arguments de divers fonction.



Bloc d'instruments : Ce bloc représente une bibliothèque pour rassembler, afficher, analyser, et faire sortir les données d'un système. Ces blocs ont des entrées seulement.

5. Horloge système :

Le boutton d'horloge situé dans la barre d'outils, donne l'accés à l'horloge du système de simulation repésentée dans la figure III.2.

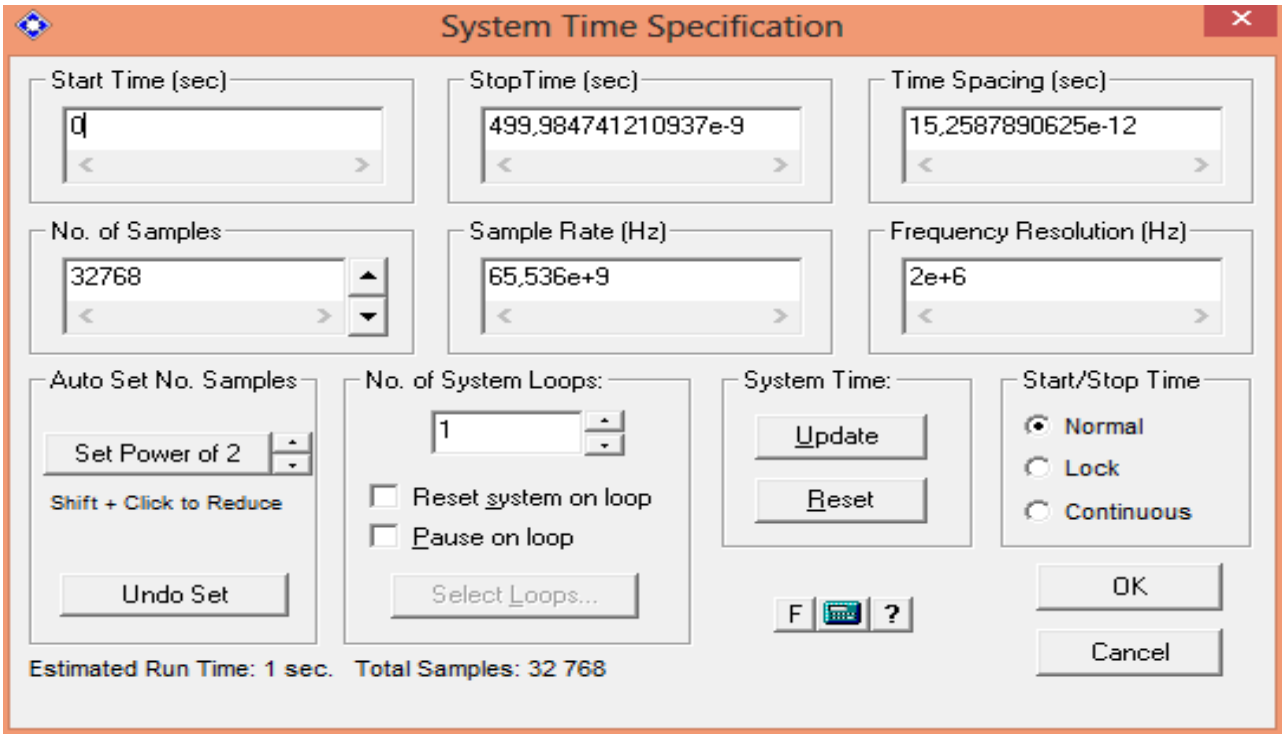


Figure III.2 : Horloge système

L'horloge permet les réglages de base pour l'analyse des flux de données (Temps arrêt / démarrage, fréquence d'échantillonnage et l'espacement temporel, nombres d'échantillons, avec configuration automatique de nombre des boucles du système , et résolution fréquentielle).

III.2 Simulation du circuit intégré LMX3162 :

Il s'agit de simuler une puce (circuit intégré) qui peut être utilisée dans la bande ISM comme radio Bluethoot.La puce inclut la modulation par GFSK, le Spectre étalé par saut de fréquence (FHSS)**,** la conversion RF en IF, et la Démodulation en Quadrature.

Le circuit intégré se compose aussi d'une PLL (boucle à verrouillage de phase), d'un émetteur et d'un circuit récepteur. Tout le filtrage est effectué en externe de la puce. Des éléments optionnels assurent un bon fonctionnement de la puce tel que l'amplificateur à faible bruit LNA dans le récepteur, et l' amplificateur de puissance en option. Dans la simulation on remplace la PLL par un simple VCO. Un schéma de principe de l'émetteur et du récepteur simulés est présentés dans la figure III.3:

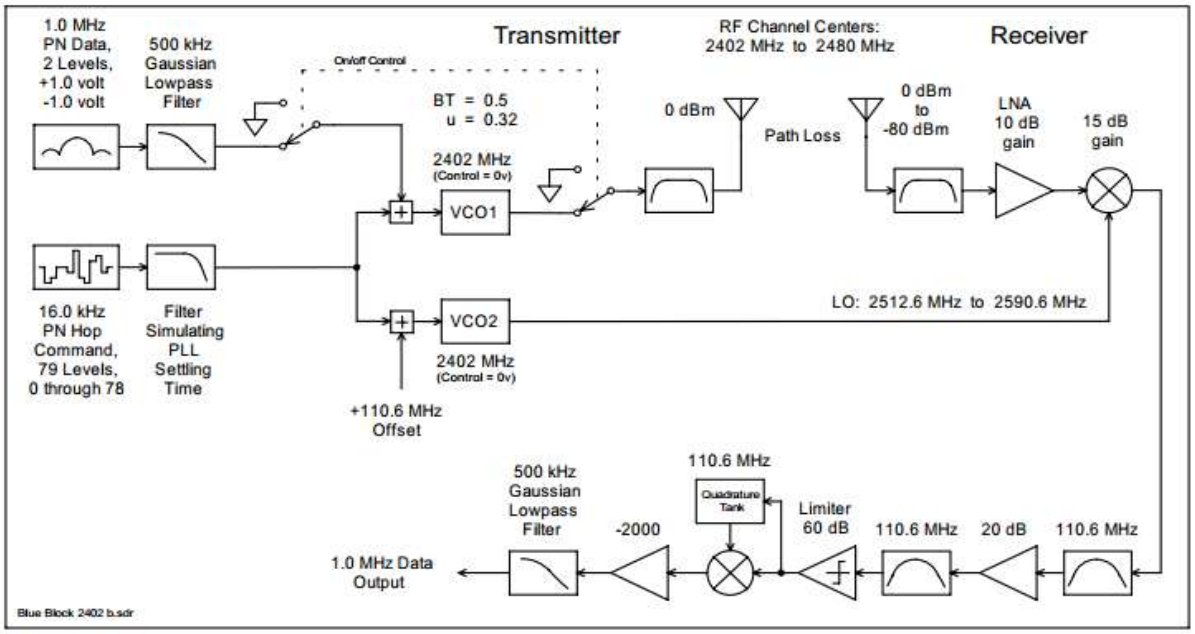


Figure III.3 :schéma synoptique d'un émetteur –récepteur Bluetooth

Les modules qui composent le système, sont :

1- une source de donnés polaires : générateur des données pseudo aléatoires , au débit de 1MHz.
2- un filtre gaussien : un filtre passe-bas gaussien avec la fréquence de coupure à 500 KHZ est nécessaire avant le modulateur.
3- oscillateur à tension contrôlé (VCO) : deux blocs de VCO (FM) pour remplacer la PLL de la puce sont utilisés.
4- des filtres passe bande.
5- des amplificateurs.
6- des mélangeurs de fréquence.

7- un démodulateur en quadrature de phase.
8- un générateur de saut de fréquence .

Nous utiliserons deux astuces pour accélérer la simulation :

- le saut de fréquence (hop) de Bluetooth est de 1,6 kHz. la simulation utilisera un saut de 16,0 kHz , ce qui est 10 fois plus rapide. Il ya moins de données par saut.

- Comme une vraie PLL n'est pas incluse dans la simulation, les sauts de fréquence sont envoyé à travers un filtre passe-bas de Tchebychev pour simuler la stabilisation de PLL pendant l'établissement de lien de communication . Au lieu des 180 micro secondes de temps de prise habituelle, la simulation utilise 18 micro seconde , des qui correspond à la 10 fois le taux de saut .

Le remplacement de la PLL est à cause de la nécessité d'une entrée qui arrive d'un microcontrôleur de la couche en bande de base ,Le remplacement n'influe pas sur les résultat de simulation.

Le **tableau III.1** résume les caractéristiques de simulation :

Type de la modulation	GFSK
GFSK BT	0.5
Le débit (bits/seconde)	1MHz
Taux de modulation	0.32
Nombre des canaux	79
La bande de canal	1MHZ
La bande ISM	2400.0 à 2483.5 M Hz
La bande de transmission	2401.0 à 2481.0 M Hz
Largeur de bande	80MHz
bande de garde à l'extrémité inférieur	2MHz
bande de garde à l'extrémité extérieur	3.5MHz
La fréquence intermédiaire	110.6MHz
Le saut de fréquence	16000 saut/seconde
temps de stabilisation de la PLL	18 µs
TDD	------
Format duplex :	62.5 µs

Tableau III.1 : caractéristiques Bluetooth à simuler

Le système Bluetooth à simuler par SystemVue est indiqué dans la figure III.4 :

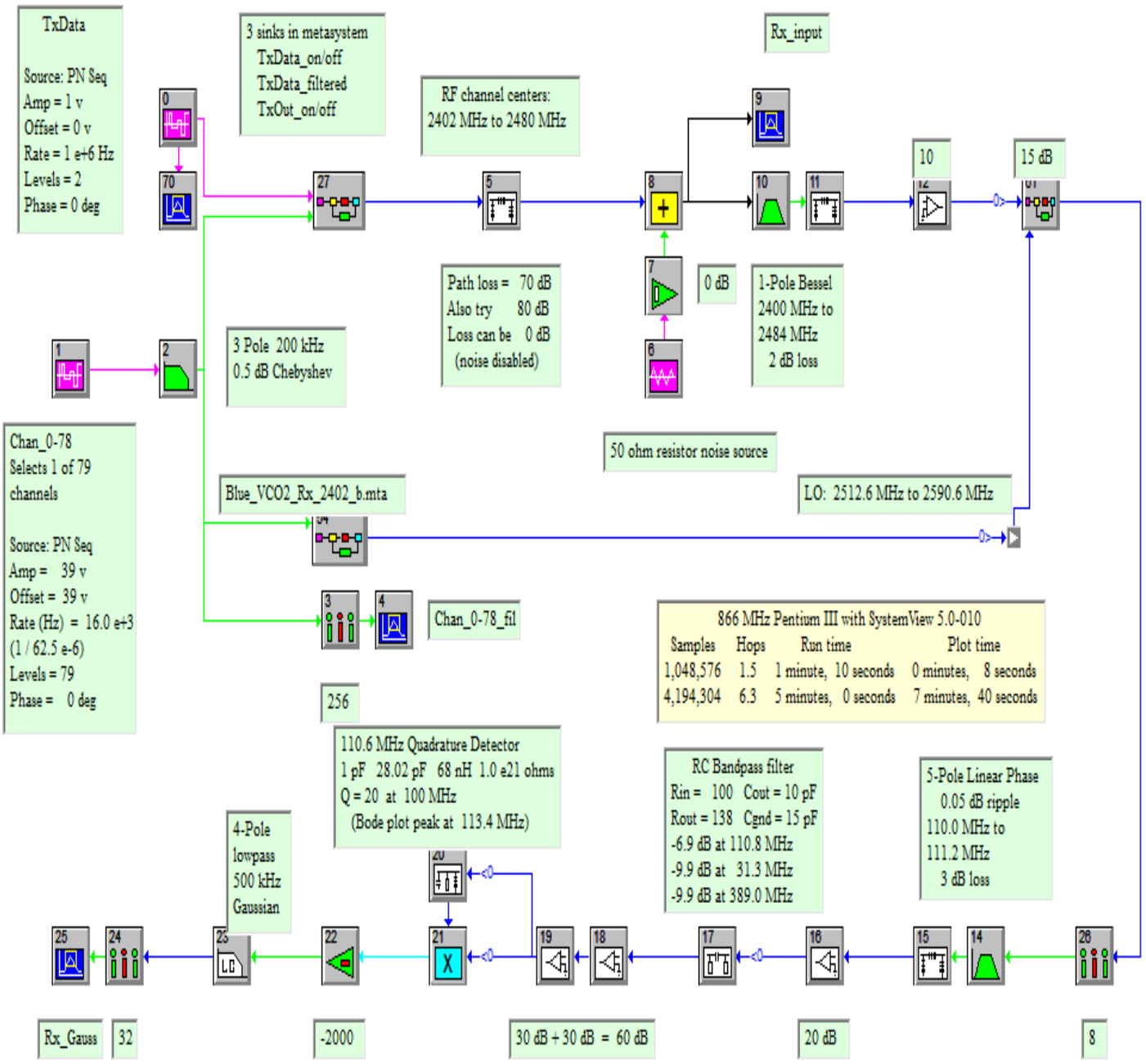


Figure III.4 :simulation de Bluetooth dans SystemVue

- le premier bloc $n^0 1$ représente une source de données polaires au débit binaire de 1MHz.
- Le générateur de saut de fréquence à 79 canaux ,ou la sortie traverse un filtre passe-bas de Tchebychev (pour remplacer la PLL).
- Le premier Meta system contient tous les bloc de l'émetteur, comme le filtre gaussien ,les VCO (modulateur FM), les amplificateurs, et les interrupteur marche/arrêt du transmetteur .
  La figure ci-dessous III.5, montre les composants de Meta system

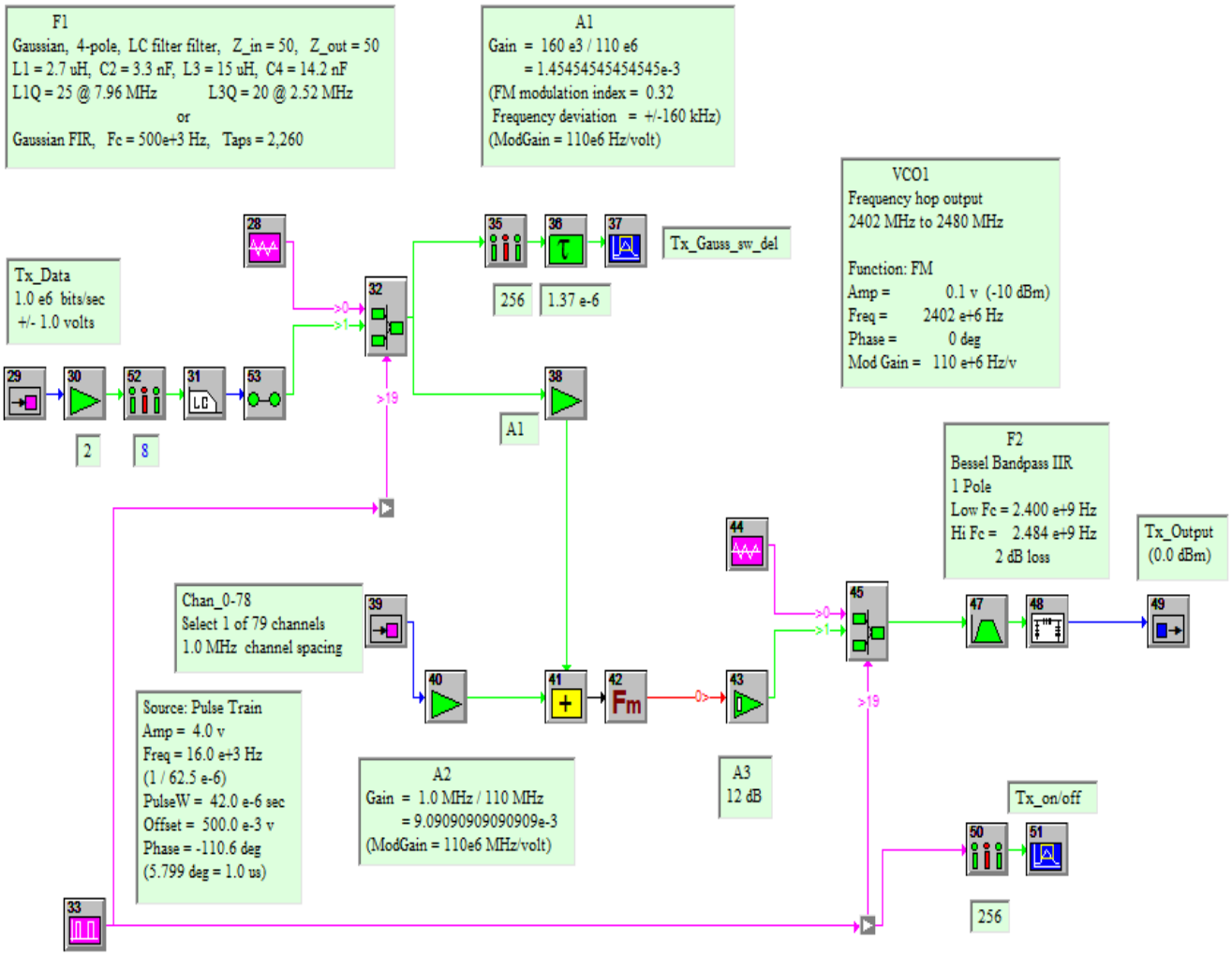
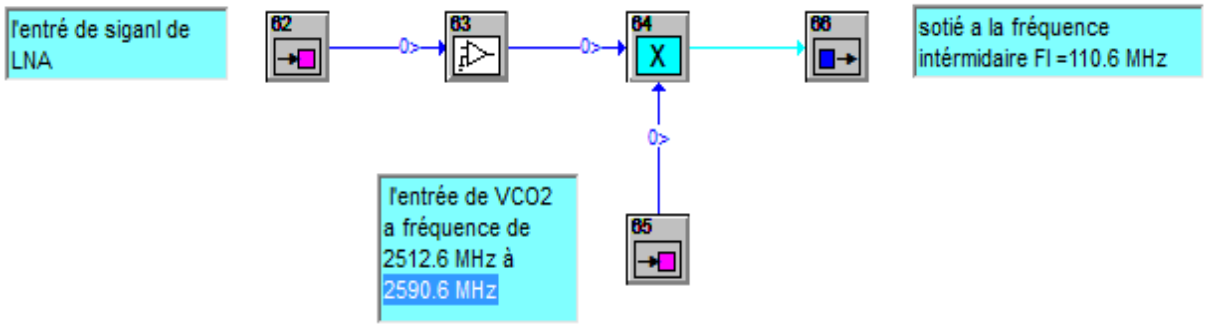


Figure III.5 émetteur bluetooth

- On a simulé les pertes de transmission due au trajet par un atténuateur à 70dB, A l'entrée de récepteur ,on ajoute une source de bruit thermique d'une résistance de 50 ohm et température de 300°K

Le convertisseur des fréquences RF à IF est illustré dans le Meta system de la figure III.6:



FigureIII.6 convertisseur RF en IF

Le mélangeur génère une distorsion de fréquence , les fréquences principales (la somme et la différence) , et les harmoniques . La figure III.7 représente la densité spectrale de puissance du signal de sortie .

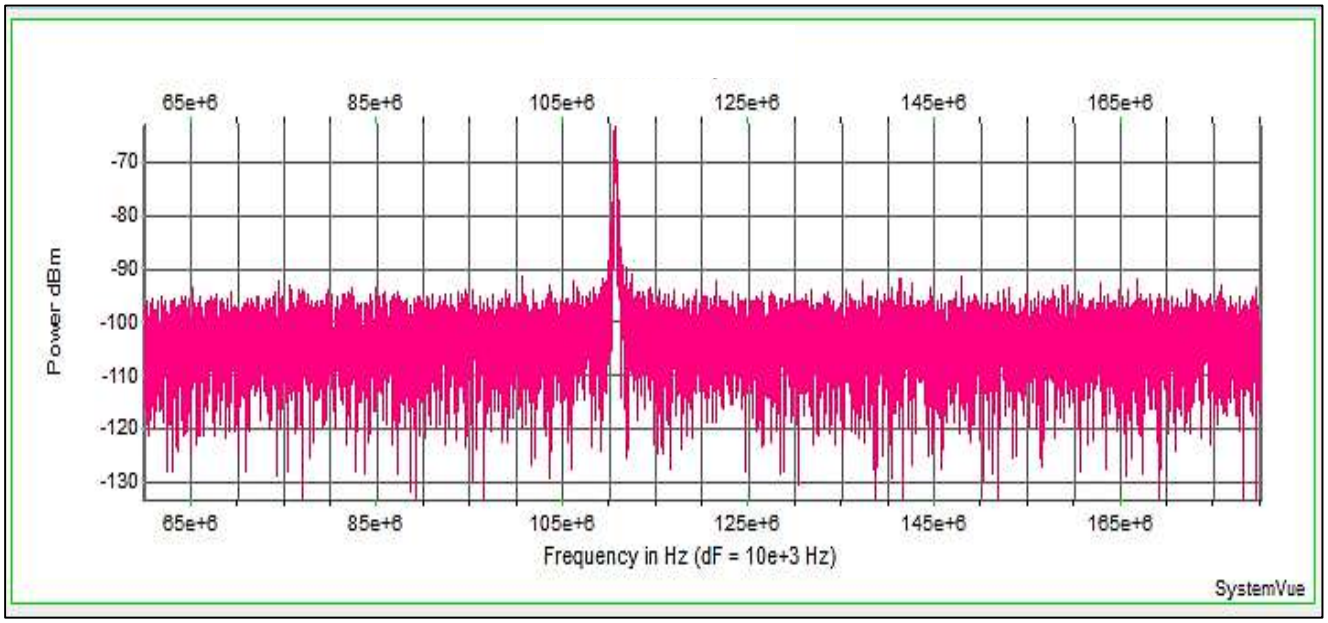


Figure III.7 : densité spectrale de puissance du signal de sortie de convertisseur ,RF en FI

Une raie à 110.6 MHz et un ensemble d'harmoniques sont générés .c'est pour ça , qu'on filtre ce signal par un filtre à phase linéaire spécifique SAW à une fréquence de 110,6 MHz. La figure III.8 montre la réponse fréquentielle au niveau de ce filtre .

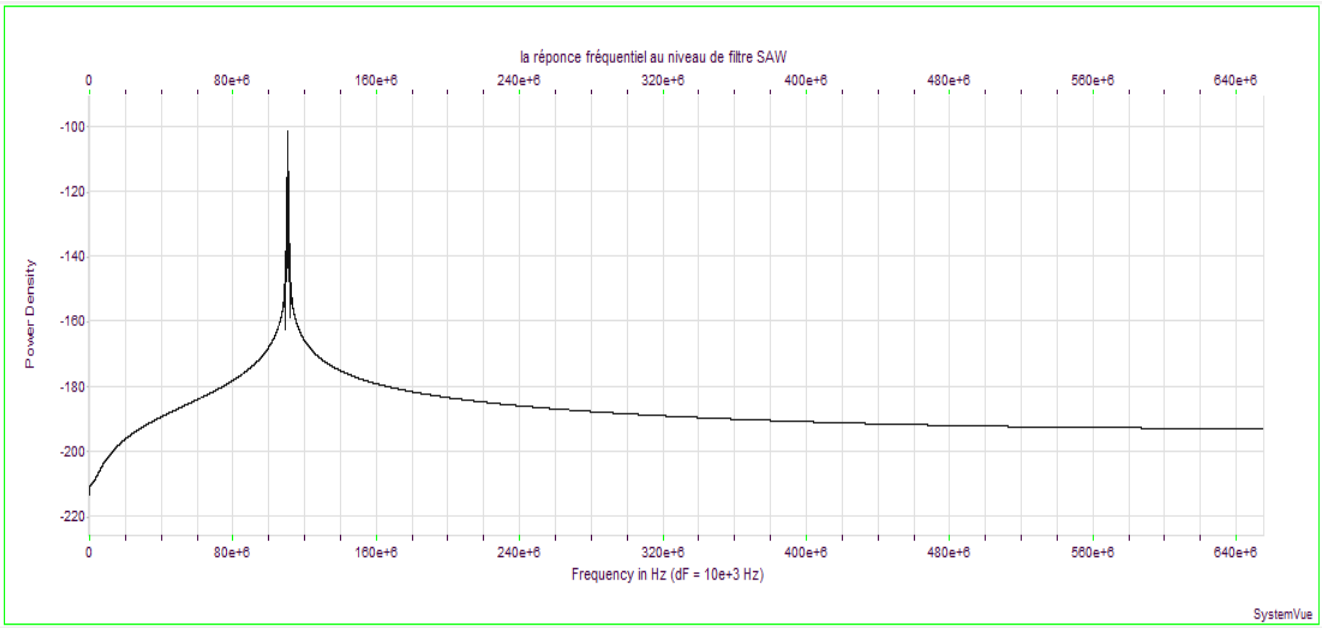


Figure III.8 la réponse fréquentielle au niveau du filtre SAW

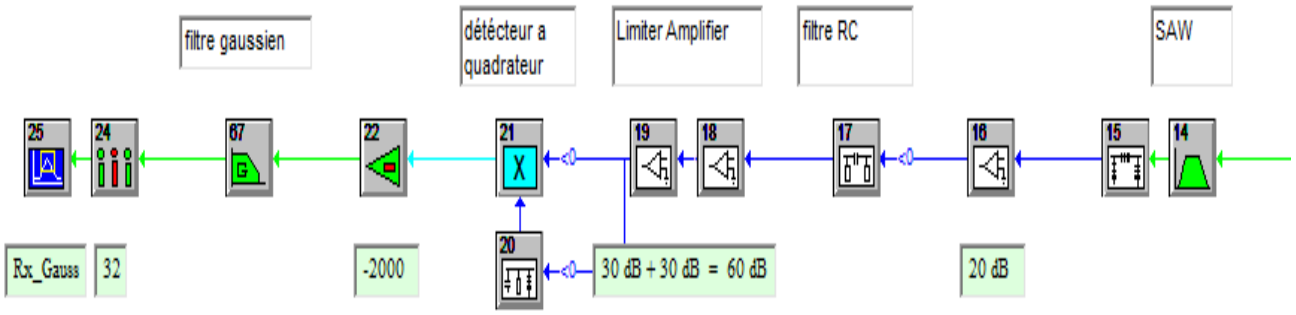


Figure III.9 : chaine de réception

Le détecteur à quadrature est l'élément le plus important de la partie récepteur, après le filtrage gaussien on obtient le signal de la figure III.10 :

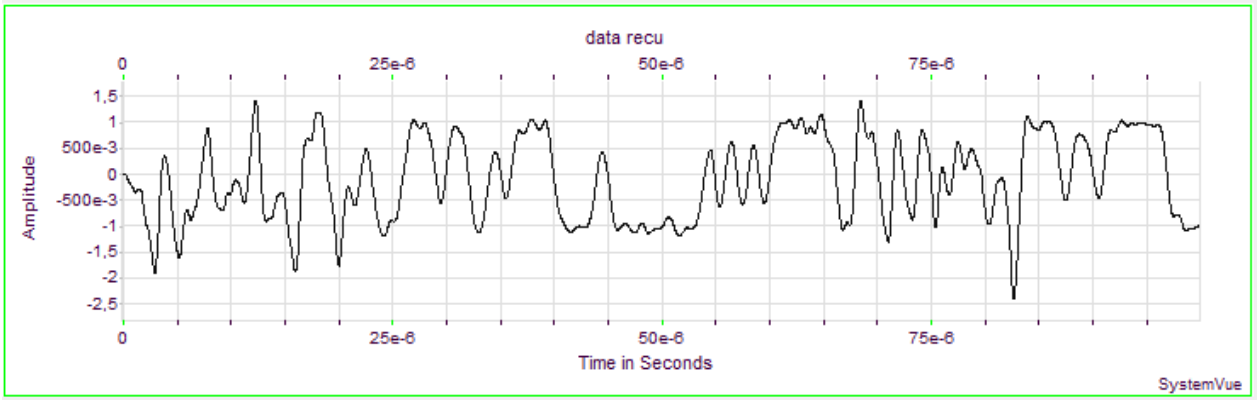


Figure **III.10** : donnés reçues

A l'aide d'un comparateur analogique, on peut reconstituer la forme plaire des données reçues.

III-3 Resultats De Simulation :

Le tracé de la figure III.11 montre la superposition entre les données émises et les données reçues.

On voit que les données sont bien superposées, En absence de données à transmettre ,on observe le bruit de canal, "Figure III.11"

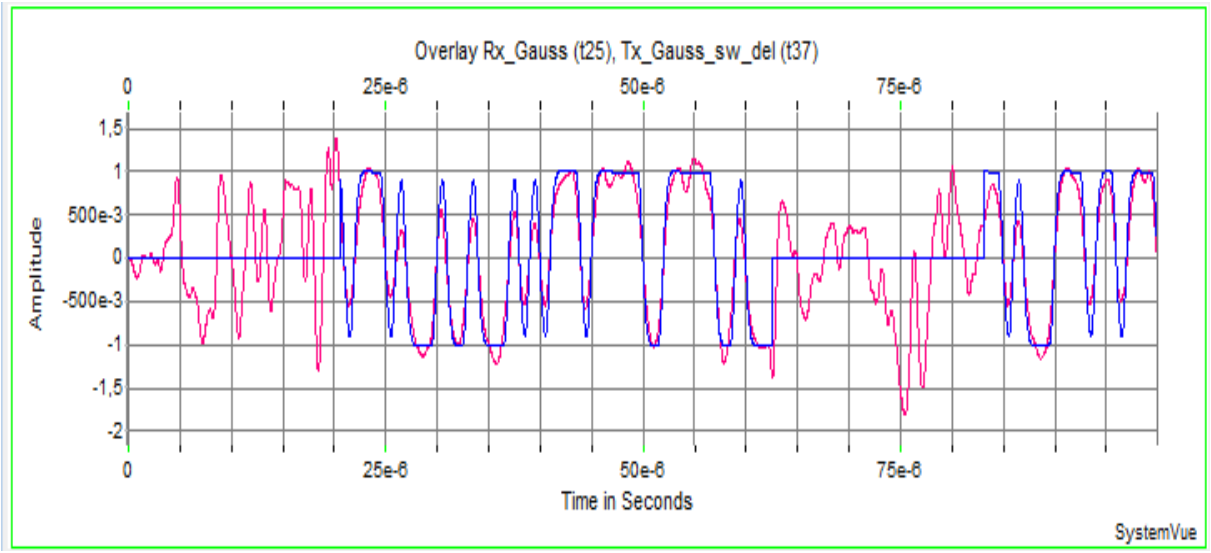


Figure III.11 superposition des données émies (blue) et reçues (rouge)

. Le tracé de la figure III.12 montre les Chronogrammes des données transmises et le saut de fréquence. On remarque que la transmission à t=18 µs, est réservée au temps de stabilisation de la PLL.

(noter que la PLL est remplacé par un générateur de saut de fréquence lié à un filtre) .

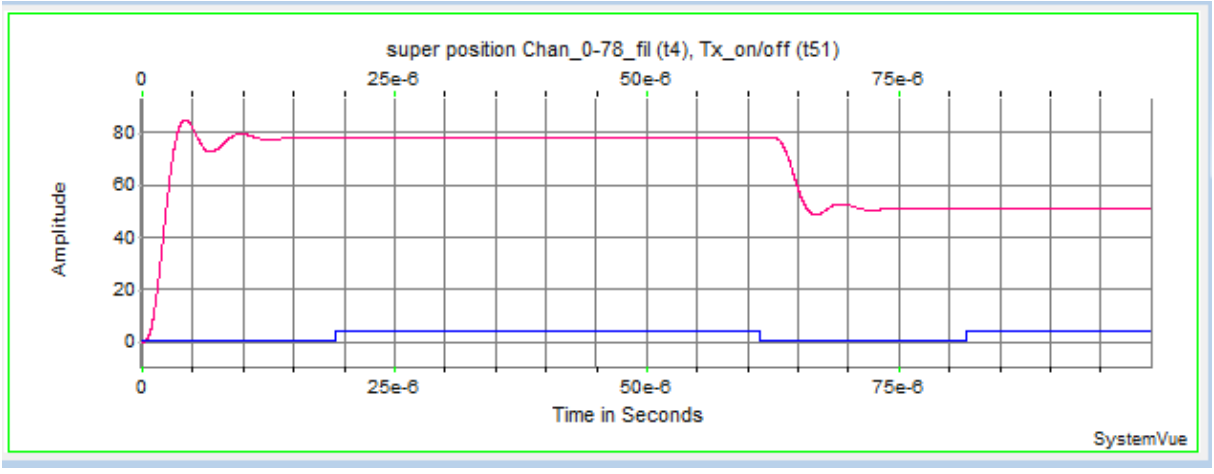


Figure III.12 : Chronogrammes des données transmises et le saut de fréquence

Dans cette partie de transmission , on a deux sauts de fréquence , l'un à 78MHz et l'autre à 51MHz . La PSD montre ces deux sauts dans la figure III.13, Les deux raies correspondent aux deux sauts ,et pour mesurer les sauts d'après la PSD , on a besoin d'un simple calcul :

Pour la première raie,elle correspond à f=2.453 MHz (la raie à gauche) ,suit

F_1=(2.453-2.402) e^{+9}= 51MHz , correspond à le premier saut.

Pour la deuxième raie on a f=2.480 MHz.

F_2= (2.480-2.402) e^{+9}= 78MHz , correspond à la deuxième saut.

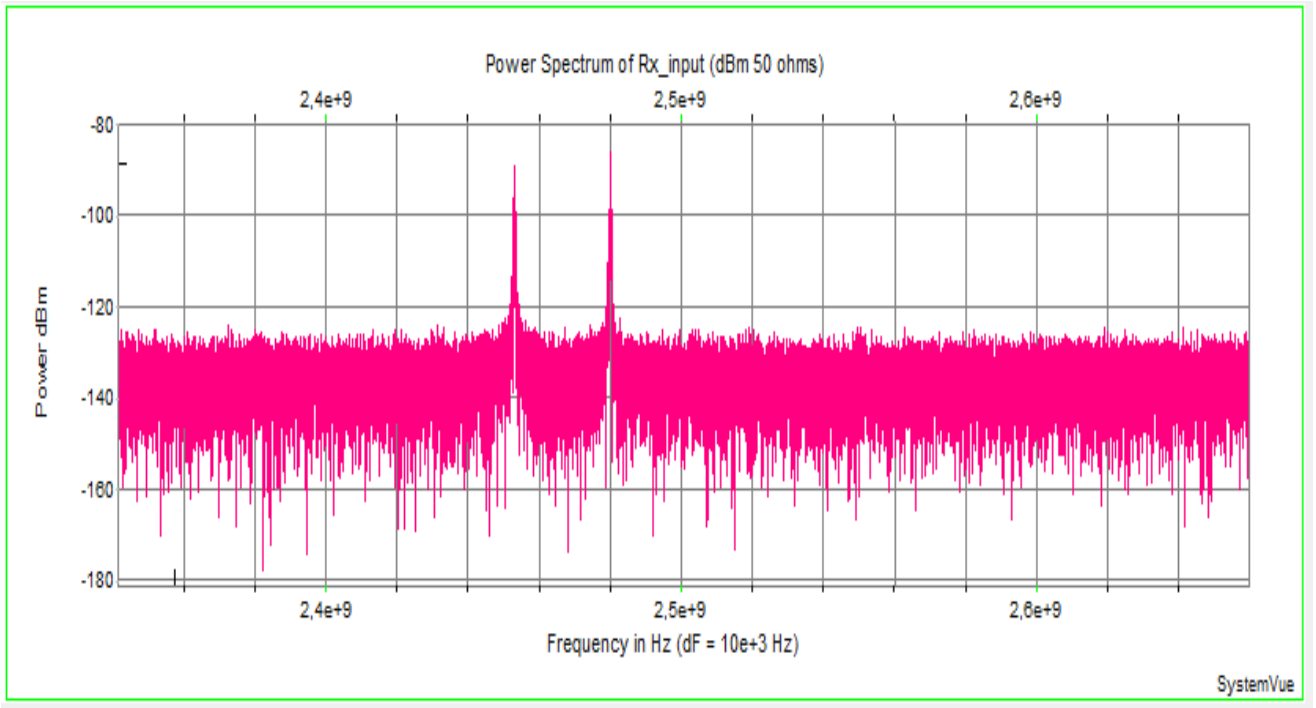


Figure III.13 : les deux sauts de fréquence

Conclusion générale



Conclusion générale :

Après une étude théorique couvrant l'aspect technique , et les mécanismes de sécurité du système Bluetooth ,nous sommes penché sur l'examination de son support physique , en terme de dispositif d'émission-réception .

Notre intérêt se focalise surtout sur la partie HF du support matériel , dont le circuit intégré LMX3162 de national semiconductors , joue un rôle primordial comme interface avec les signaux en bande de base , ce circuit RF conçu pour travailler dans la bande ISM à 2.45GHZ, est composé essentiellement d'une PLL dans l'étage d'émission ,et d'un mélangeur, amplificateur FI , et un discriminateur de fréquence partiellement conçu ; dans l'étage de réception .

A l'émetteur, nous avans étudié la modulation GFSK ou les donnes d'entrée traites avec un filtre gaussien, module le VCO interne de la PLL du circuit intégre , la saut de fréquence résultant a été obtener par simulation entre les deux valeurs 51MHZ et 71MHZ .

La réception a été simulée au niveau de son mélangeur ou la PSD de sa sortie a été tracée, celle-ci se voit démunir de ses fréquence parasites , une fois filtré par un filtre FI de type SAW .

La chaine de réception est simulée dans sa entier, ou les parties du LMX3162 correspondante ont été complétés par les filtres extérieures, SAW, RC, RC en quadrature, en plus du filtre gaussien de sortie.

Les données reçues se superposent à celles émises, avec succès ,malgré certaine distorsion constatés.

Nous souhaites que ce travail suit complété par la suite , en lui rajoutant la partie traitant la bande de base afin que l'émission-réception du système Bluetooth dans son ensemble suit étudié complètement et ne reste aucun mystère.

Bibliographie

[1] H. Labiod, H. Afifi, C. De Santis **«** WI-FI TM, BLUETOOTH TM, ZIGBEE TM AND WIMAX TM » édition springer,2010

[2] Xavier LAGRANGE, Laurence ROUILLÉ « Technologie Bluetooth » technique de l'ingénieur.

[3] National Semiconductor « Using the LMX3162 for 2.4-GHz ISM Band »,2008

[4] datasheet « LMX3162 » National Semiconductor.2008

[5] Sami Merilä « Designing a modular, open and expandable Bluetooth-platform » Lappeenranta University of Technology

[6] Ericsson « bluetooth_technical_introduction » document.

Annexe 01 : Boucle d'asservissement de phase

La boucle d'asservissement de phase est constituée de trois éléments (figure 1). La fonction du dispositif est d'asservir la phase instantanée ψs d'un signal ys délivré par un oscillateur sur la phase

instantanée ψe d'un signal d'entrée ye.ye et ys sont supposés être des signaux sinusoïdaux ou carrés, de phase instantanée respectivement ψe et ψs et on peut définir les pulsations instantanées ωe et ω s des deux signaux :

ώe= dψe /dt et ωs= dψs/dt

On décompose, de manière formelle, ψe et ψs de la manière suivante :

$$\psi_e = \omega_0 t + \varphi_e(t) \qquad \psi_s = \omega_0 t + \varphi_s(t)$$

et on suppose que les variations de ϕe(t) et ϕs(t) sont lentes vis-à-vis de cos ω0t: les signaux ye et ys sont supposés à support fréquentiel étroit autour de ω 0(avec d'éventuels harmoniques dans

le cas de signaux carrés).

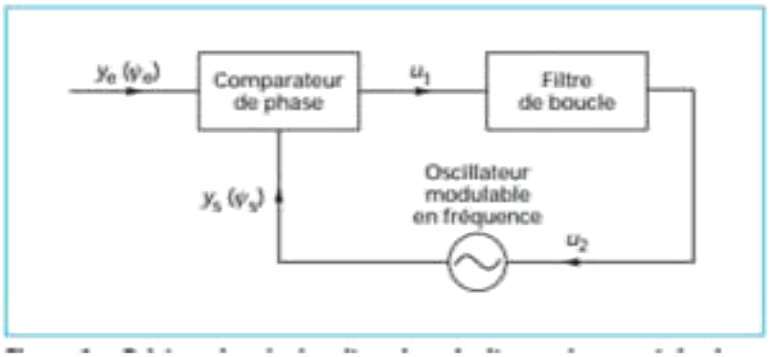


Figure01 : La boucle d'asservissement de phase

Équations

• Le comparateur de phase délivre une tension fonction de la

différence de phase instantanée des signaux ye et ys

$$u_1(t) = K_1\, g(\psi_e - \psi_s) = K_1\, g(\varphi_e - \varphi_s) = K_1\, g(\varphi)$$

avec K1 sensibilité du comparateur de phase de caractéristique g(.)

• Le filtre de boucle, analogue aux filtres correcteurs des asservissements classiques est caractérisé par une réponse impulsionnelle f(t). Le signal de sortie u2est le produit de convolution de f(t) et du signal d'entrée u1

$$u_2(t) = f(t) * u_1(t)$$

La pulsation ωs du signal ys délivré par l'oscillateur commandé est une fonction, supposée linéaire, de la tension de commande u2. Quand la tension u2 est nulle, la pulsation ωs est égale à ω0 , pulsation centrale de la boucle :

$$\omega_s = \omega_0 + K_2 u_2 \Rightarrow \frac{d\varphi_s}{dt} = K_2 u_2$$

Remarques

• Le signal effectif d'entrée de la boucle est le signal ye mais au niveau fonctionnel, l'information en entrée est la phase ϕe.

• L'information de sortie est la phase ϕs portée par ys.

• Le système est un asservissement :

—le signal d'entrée est ϕe;

—le signal de sortie est ϕs;

—ϕs tend à recopier ϕe.

La différence : ϕ= ϕe– ϕs, est l'erreur de l'asservissement.

• En fonctionnement normal, l'erreur ϕ reste limitée (la boucle est dite « accrochée ») :

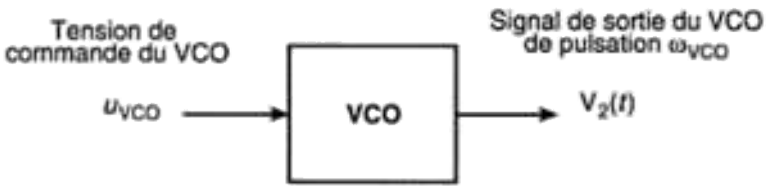
—si ϕ est constant ou nul : les signaux ye et ys sont parfaitement synchrones (ωe= ωs) ;

—si ϕ est variable mais limité : les fréquences instantanées des signaux ye et ys sont en moyenne identiques (ωs suit en moyenne ωe) ;

—si |ϕ | augmente indéfiniment avec le temps, la boucle n'est pas accrochée ou a décroché : la pulsation ωs n'est pas égale, en moyenne, à ωe . Le système est alors inutilisable.

Annexe 02 : oscillateur commandé en tension

Le VCO délivre un signal dépend d'une tension de commande .



Dans une plage de tension, qui dépend de la technologie utilisé, la loi de variation de la pulsation ώvco en fonction de la tension de commande Uvco correspond en générale à une fonction affine.

On à représenter ci-dessus la caractéristique du transfert du VCO avec une plage de fonctionnement compris entre 0 et VDD pour la tension de commande Uvco.

La pulsation du VCO peut évoluer entre la valeur minimale et maximale : $[\omega_{vco}^{min}, \omega_{vco}^{max}]$.

On appelle ω_A la pulsation centrale de la VCO telle que $\omega_A = \frac{\omega_{vco}^{min} + \omega_{vco}^{max}}{2}$.

Cette pulsation correspond à la tension de commande noté U_A qui dans notre exemple à égale de $V_{DD}/2$.

La pente de caractéristique K_0s'exprime en rad.S^{-1}.V^{-1} et s'appelle coefficient e sensibilité du VCO.

En pratique le VCO va fonctionner autour de point de fonctionnement définie par la pulsation centrale ω_A.

L'équation de la caractéristique est donné par $\omega_{VCO} = \omega_A + K_0 (u_{VCO} - U_A)$.

On s'intéresse aux la variation de la pulsation autour du point de fonctionnement , on pose $u = u_{VCO} - U_A$ et $\omega_2 = \omega_{VCO} - \omega_A$ alors nous pouvons écrire la relation suivante entre u et ω_2

$\omega_2(t) = K_0 u(t)$.

en pratique il existe diffèrent type de VCO qui dépendent du domaine de fréquence utilisé.

Annexe 03 : synthétiseur de fréquence à PLL

Un synthétiseur de fréquence à PLL va générer un signal dont la fréquence est programmable à laide d'un système numérique et utilisé un oscillateur de référence basse fréquence de grande stabilité et de grande précision.

Il va être réalisé avec les dispositifs suivants :

-un oscillateur de référence à quartz de fréquence f_{REF} .

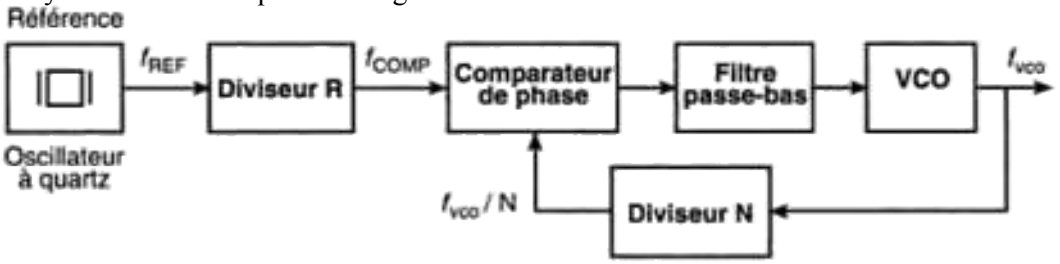
- un diviseur de fréquence par R.

-un comparateur de phase associé a un filtre passe –bas (filtre de boucle).

-un VCO délivrant un signal à la fréquence f_{VCO} .

-un diviseur de fréquence par N.

Le synthétiseur de fréquence est agencé selon le schéma ci-dessus :



La fréquence d'entré de la comparateur de phase f_{com} est liée par la fréquence de référence par l'équation suivante : $f_{com}= f_{ref} /R$.

Lorsque la PLL se verrouillé les fréquence f_{com} et f_{VCO} /N sont identique ,on en déduit

$$f_{VCO} = \frac{N}{R} f_{REF}$$

La fréquence f_{VCO} est obtenu avec une précision et une stabilité égales à celle de l'oscillateur de référence f_{REF} car :

$$\frac{\Delta f_{VCO}}{f_{VCO}} = \frac{\Delta f_{REF}}{f_{REF}}.$$

Les diviseurs de fréquence sont réalisés à l'aide de compteur.

En technologie CMOS les fréquence de fonctionnement sont limitées à 20-30 MHZ.

En règle général le diviseur de fréquence Rest fixé allor que le diviseur de fréquence N est programmable .

Lorsque le diviseur de fréquence N est incrémenté d'une unité, deviseur N+1, allor la fréquence f_{VCO} augmente d'une quantité égale au pas de synthétiseur de fréquence

$$\frac{f_{REF}}{R} = f_{COMP}.$$