[*Sommaire*]

Introduction Générale

Depuis leur création, les réseaux de communication sans fil ont connu un succès sans cesse croissant au sein des communautés scientifiques et industrielles. Grâce à ses divers avantages, cette technologie a pu s'instaurer comme acteur incontournable dans les architectures réseaux actuelles. Le média hertzien offre en effet des propriétés uniques, qui peuvent être résumées en trois points : la facilité du déploiement, l'ubiquité de l'information et le coût réduit d'installation. Au cours de son évolution, le paradigme sans fil a vu naître diverses architectures dérivées, telles que : les réseaux cellulaires, les réseaux locaux sans fils et autres. Durant cette dernière décennie, une architecture nouvelle a vu le jour : les réseaux de capteurs sans fil (RCSF).

UnRCSF est composé d'un ensemble d'unités de traitement embarqués appelés MOTTES communiquant via des liens sans fils .Le but générale d'un RCSF est la collecte d'un ensemble de paramètres de l'environnement entourant les MOTTES tel que la température afin de les acheminer vers une station de base pour les traités localement.

Les RCSF ont un vaste domaine d'application tel que l'environnement le commerce ou la médecine, et c'est ce qui nous intéresse, un RCSF dans le domaine médicale est connu sous le nom de WBAN.

WBAN est un ensemble de nœud implanté dans le corps humain pouvant effectuer des mesures, et leur transmission a la station de base vu l'importance des données récolter il est nécessaire de mettre en place un système de sécurité.

Les mécanismes de sécurité traditionnelle sont inappropriés parce que les nœuds sont limités en termes de mémoire, CPU et d'énergie

Dans ce projet nous avons développés un mécanisme de gestion de clés léger et approprié au WBAN.

Chapitre I

Réseaux de capteurs corporels sans fil

I.1 – Introduction :

Depuis quelques années, Internet suscite un engouement croissant, tant dans les domaines de recherche, de l'éducation et celui des affaires. Ainsi, le nombre de personnes qui accèdent à Internet pour leurs travaux, leurs études ou leurs loisirs augmente considérablement, de même que les services offerts sur ce réseau (messagerie électronique, e-commerce, eLearning, etc.). Cette diversité de services et d'utilisateurs est principalement due au fait qu'Internet regroupe un grand nombre de réseaux différents. De l'autre côté, le progrès réalisé dans le domaine sans fils a contribué à l'évolution de l'Internet en facilitant l'accès aux usagers. L'évolution dans le domaine des communications sans fils et l'informatique mobile gagne de plus en plus de popularité et les composants mobiles deviennent de plus en plus fréquents (PDA, laptops, handsets). Ceci a permis l'apparition d'un nouveau type de réseaux sans fils appelé réseaux de capteurs sans fil.

Dans ce chapitre, nous présenterons les réseaux de capteurs sans fil RCSF et notamment les réseaux de capteurs corporels sans fil WBANs.

I.2 – Les réseaux de capteurs sans fil :

Un Réseau de Capteurs Sans Fil (RCSF) est un ensemble de dispositifs très petits, nommés nœuds capteurs, variant de quelques dizaines d'éléments à plusieurs milliers.

Dans ces réseaux, chaque nœud est capable de surveiller son environnement et de réagir en cas de besoin en envoyant l'information collectée à un ou plusieurs points de collecte, à l'aide d'une connexion sans fil [1].

Dans le cas d'un réseau de petite échelle (corps humain par exemple), les capteurs seront dans le voisinage direct du puits (un réseau de type étoile à un saut).

Cependant, dans le cas d'un réseau à grande échelle (forêt, barrage, champs de batail…), les capteurs ne sont pas tous dans le voisinage du puits et les messages seront acheminés du nœud source vers le puits en transitant par plusieurs nœuds, selon un mode de communication multi-sauts comme le l'illustre la figure I-1.

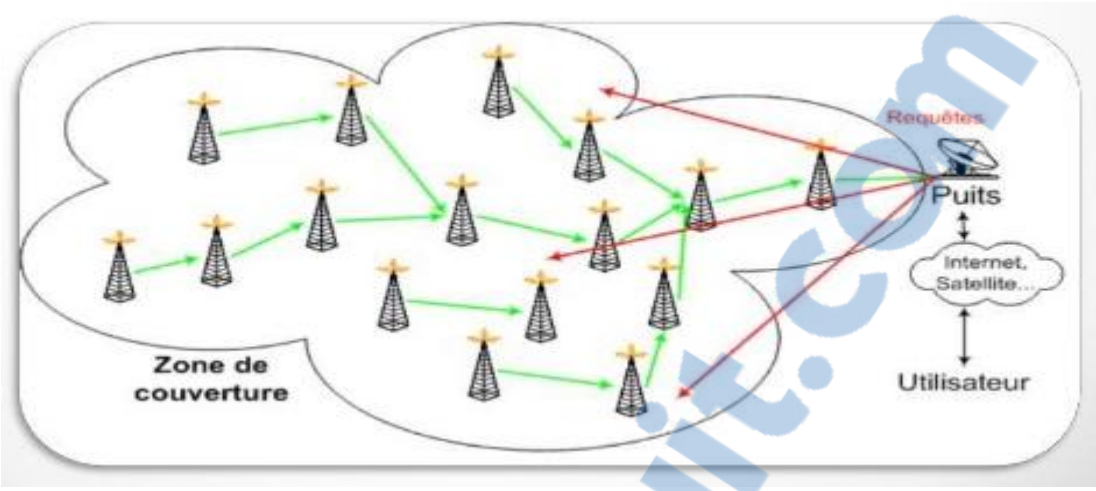


Figure I.1- réseau de capteurs sans fil [2]

I-3 Applications des réseaux de capteurs sans fil :

Le champ d'applications des réseaux de capteurs est de plus en plus élargi grâce aux évolutions techniques que connaissent les domaines de l''electronique et des télécommunications. Parmi ces évolutions, on peut citer la diminution de taille et du cout des capteurs, ainsi que l''elargissement des gammes de capteurs disponibles (mouvement, température, ...) et l'évolution des supports de communication sans fil. En effet, les applications des réseaux de capteurs peuvent être militaires, médicales, environnementales, commerciales, etc.

Applications militaires : Un réseau de capteurs déployé dans un secteur stratégique ou difficile d'accès, permet par exemple d'y surveiller tous les mouvements (allies ou ennemis), ou d'analyser le champ de bataille avant d'y envoyer du renfort ([3] [4]).

Applications médicales : Il existe déjà dans le monde médical, des gélules multi-capteurs pouvant être avalées qui permettent, sans avoir recours a la chirurgie, de transmettre des images de l'intérieur du corps humain ([5] [6]).

Applications environnementales : Des capteurs de température peuvent être disperses a partir d'avions dans le but de détecter d'éventuels problèmes environnementaux dans le domaine couvert par les capteurs dans une optique d'intervenir `a temps afin d'empêcher que d''eventuels incendie, inondation, volcan ou tsunami ne se produisent ([7] [1] [2]).

Applications commerciales : Des nœuds capteurs peuvent être utilises pour améliorer les processus de stockage et de livraison. Le réseau peut ainsi être utilise pour connaitre la position, l'état et la direction d'une marchandise. Un client attendant une marchandise peut alors avoir un avis de livraison en temps réel et connaitre la position des marchandises qu'il a commandées ([8]).

I-4 architecture d'un micro capteur :

Un *« nœud capteur »* contient quatre unités de base : l'unité de captage, l'unité de traitement, l'unité de transmission, et l'unité de contrôle d'énergie. Selon le domaine d'application, il peut aussi contenir des modules supplémentaires tels qu'un système de localisation (GPS), ou bien un système générateur d'énergie (cellule solaire). Quelques micro-capteurs, plus volumineux, sont dotés d'un système mobilisateur chargé de les déplacer en cas de nécessité [9].

- ✓ **L'unité de captage :** Le capteur est généralement composée de deux sous-unités : le récepteur (reconnaissant l'analyste) et le transducteur (convertissant le signal du récepteur en signal électrique). Le capteur fournit des signaux analogiques, basés sur le phénomène observé, au convertisseur Analogique/Numérique. Ce dernier transforme ces signaux en un signal numérique compréhensible par l'unité de traitement.
- ✓ **L'unité de traitement :** Elle comprend un processeur généralement associé à une petite unité de stockage. Elle fonctionne à l'aide d'un système d'exploitation spécialement conçu pour les micro-capteurs (TinyOS par exemple). Elle exécute les protocoles de communications qui permettent de faire collaborer le nœud avec les autres nœuds du réseau. Elle peut aussi analyser les données captées pour alléger la tâche du nœud puits.
- ✓ **L'unité de transmission :**Elle effectue toutes les émissions et réceptions des données sur un *médium « sans-fil »*. Elle peut être de type optique (comme dans les nœuds Smart Dust), ou de type radiofréquence.
    - Les communications de type optique sont robustes vis-à-vis des interférences électriques. Néanmoins, ne pouvant pas établir de liaisons à travers des obstacles, elles présentent l'inconvénient d'exiger une ligne de vue permanente entre les entités communicantes.
    - Les unités de transmission de type radiofréquence comprennent des circuits de modulation, démodulation, filtrage et multiplexage ; ceci implique une augmentation de la complexité et du coût de production du micro-capteur.

Concevoir des unités de transmission de type radiofréquence avec une faible consommation d'énergie est un défi car pour qu'un nœud ait une portée de communication suffisamment grande, il est nécessaire d'utiliser un signal assez puissant et donc une énergie consommée importante. L'alternative consistant à utiliser de longues antennes n'est pas possible à cause de la taille réduite des micro-capteurs.

- ✓ **L'unité de contrôle d'énergie :**Un micro-capteur est muni d'une ressource énergétique (généralement une batterie).

Étant donné sa petite taille, cette ressource énergétique est limitée et généralement non-remplaçable. ceci fait souvent de l'énergie la ressource la plus précieuse d'un réseau de capteurs, car elle influe directement sur la durée de vie des micro-capteurs et donc du réseau entier.
L'unité de contrôle d'énergie constitue donc une partie essentielle du système. Elle doit répartir l'énergie disponible aux autres modules, de manière optimale (par exemple en réduisant les dépenses inutiles et en mettant en veille les composants inactifs). Cette unité peut aussi gérer des systèmes de rechargement d'énergie à partir de l'environnement via des cellules photovoltaïque par exemple.

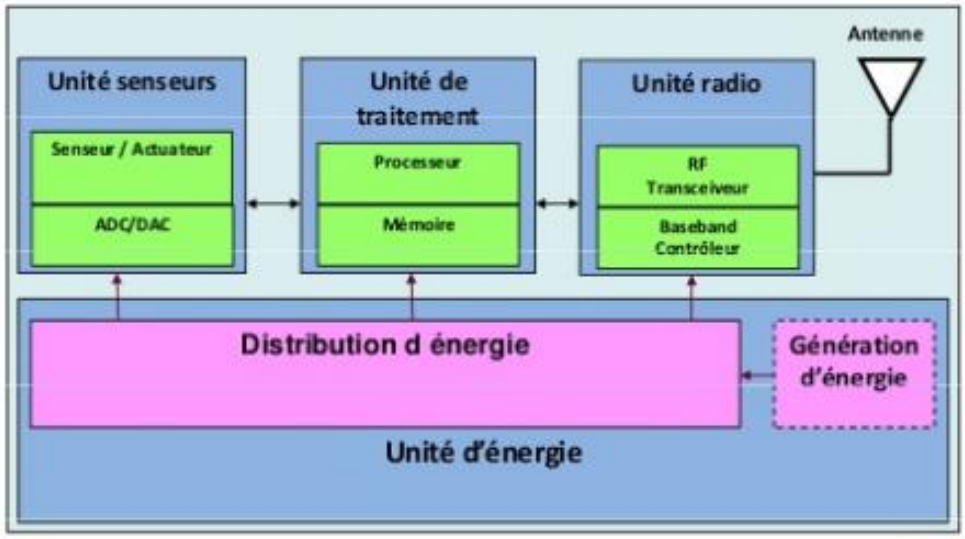


Figure I.2- Architecture d'un nœud de capteur [10].

I-5 Systèmes embarqués pour les capteurs :

Les avancées technologiques récentes ont permis de faire embarquer des systèmes d'exploitation (OS : Operating System) au sein des capteurs, mais leurs fonctionnalités restent toutefois limitées.

Les systèmes d'exploitation pour les réseaux de capteurs sans fil sont des interfaces informatiques spécifiques destinées au fonctionnement des capteurs dans les réseaux.

Le rôle du système d'exploitation pour un capteur en réseau est d'être l'interface entre les ressources matérielles et les applications distribuées. Il doit fournir une variété de services systèmes basiques comme la gestion de l'allocation des ressources sur les périphériques de matériels divers et la gestion et la planification des tâches. Le but du système d'exploitation est de faciliter la programmation des applications, mais aussi d'optimiser les utilisations des ressources.

Il existe plusieurs systèmes d'exploitation pour les réseaux de capteurs sans fils comme : TinyOS, Contiki, MANTIS OS, LiteOS, RETOS, Nano-RK [11], [12], [13], [14]. Il y a certaines caractéristiques qui font la différence entre ces systèmes d'exploitation [11], par exemple : l'architecture, le modèle de programmation, la gestion de la mémoire, le langage de programmation. Le Tableau 1 fait une comparaison entre les caractéristiques de quelques systèmes d'exploitation.

Caractéristique/OS	Architecture	Modèle de programmation	Gestion de la mémoire	Langage de programmation
TinyOS	Monolithique	Evénementielle	Mémoire statique	NesC
Contiki	Modulaire	Evénementielle et multitâche	Mémoire dynamique	C
MANTIS	Sous forme des couches	Multitâche	Mémoire dynamique	C
Nano-RK	Monolithique	Multitâche	Mémoire statique	C
LiteOS	Modulaire	Evénementielle et multitâche	Mémoire dynamique	LiteC++

Tableau I.1 Comparaison entre les caractéristiques de quelques systèmes d'exploitation[11]

Parmi les systèmes d'exploitation actuels, nous décrivons les OS les plus utilisés dans le domaine scientifique qui sont : TinyOS, Contiki et MANTIS OS.

I.5.1-TinyOS :

TinyOS est un système d'exploitation open source pour les réseaux de capteurs sans fil qui trouve sa genèse au sein du laboratoire d'informatique de l'université de Berkeley et qui a été l'un des premiers systèmes d'exploitation conçus pour les réseaux de capteurs miniatures. En effet, TinyOS est le plus répandu des OS pour les réseaux de capteurs sans-fil. Il est capable d'intégrer très

Rapidement les innovations en relation avec l'avancement des applications et des réseaux eux-mêmes tout en minimisant la taille du code source en raison des problèmes inhérents de mémoire dans les réseaux de capteurs.

La librairie de TinyOS comprend des protocoles réseau, des applications de services distribués, des pilotes (drivers en anglais) de capteurs et des outils d'acquisition des données. La contrainte énergétique due à l'autonomie des capteurs implique l'utilisation de puissance de calcul réduite. Cela entraîne le développement de logiciels contraint par la capacité de la mémoire et par la rapidité d'exécution. Les applications pour TinyOS sont écrites en langage de programmation NesC (Network Embedded System C), une extension du langage programmation C. L'utilisation du langage NesC permet l'optimisation du code et par suite réduit l'usage de la mémoire à accès aléatoire (RAM).

Un programme sous TinyOS ne doit comporter que les composants nécessaires à son exécution, ce qui réduit la taille du programme à insérer dans l'unité de traitement du capteur.

Un autre but de TinyOS est de prolonger la durée de vie du capteur. Dans cette optique, la programmation sous TinyOS est une programmation événementielle, c'est-à-dire que l'exécution des différentes instructions s'effectue en fonction des événements enregistrés par l'unité de traitement. Ce type de programmation est adapté aux capteurs car il n'y a pas de traitement que lors d'apparitions d'événements, ce qui permet au capteur de rester dans un état de veille le reste du temps afin de préserver son énergie.

Par contre, les programmes développés pour fonctionner sous le noyau TinyOS pourront être difficilement utilisables sous un autre système d'exploitation.

I.5.2 Contiki :

Contiki est également un système d'exploitation open source. C'est un système configurable modulaire pour les réseaux de capteurs. L'architecture hybride du noyau Contiki autorise deux modes de fonctionnement : soit multitâche, soit basé sur les événements. Contiki est un système d'exploitation conçu pour prendre le moins de place possible, avec une faible empreinte mémoire. Pour cela, le code est écrit en langage C.

Un système utilisant Contiki contient des processus, qui peuvent être des applications ou des services, c.à.d. un processus proposant des fonctionnalités à une ou plusieurs applications. La communication entre processus se fait par l'envoi d'événements.

Le noyau Contiki reste, nativement, un système d'exploitation basé sur les événements. Pour obtenir le mode multitâche, une bibliothèque doit être installée. Les fonctions associées à cette

bibliothèque n'accèdent pas directement à l'ensemble des ressources du capteur sans fil. Elles doivent, dans certains cas, faire appel à la partie du noyau dédié à la gestion des événements. Cette structure à deux niveaux a pour conséquence une dégradation des performances du système quand le mode multitâche est activé.

I.5.3 MANTIS OS :

MANTIS (MultimodAl NeTworks of In-situ micro Sensor) OS apparu en 2005, a été conçu par l'université du Colorado [15]. C'est un système d'exploitation léger et multitâche pour les capteurs adapté aux applications où plusieurs traitements, chacun associé à un ou plusieurs processus, sont en concurrence pour accéder aux ressources du capteur sans fil.

Il dispose d'un environnement de développement Linux et Windows. La programmation d'application sur MANTIS OS se fait en langage C. Son empreinte mémoire est faible : 500 octets en mémoire RAM et 14 kilo-octets en mémoire flash. C'est un système modulaire dont le noyau supporte également des entrées/sorties synchrones et un ensemble de primitives de concurrence.

L'économie d'énergie est réalisée par MANTIS à l'aide d'une fonction de veille appelée sleep function qui désactive le capteur lorsque toutes les taches actives sont terminées. MANTIS est un système dynamique ; les modifications applicatives peuvent être réalisées pendant le fonctionnement. MANTIS apporte une compatibilité avec le modèle événementiel TinyOS à travers TinyMOS (MOS est la contraction de MantisOS), dont son noyau est équipé.

I.6 Protocoles de communications sans fil :

Le médium utilisé par les réseaux de capteurs sans fils médicaux est l'onde radio. Parmi les grandes normes radios qui ont été utilisées pour des applications à bases de réseaux de capteurs nous citons:

I.6.1 La norme IEEE 802.15.1 / Bluetooth : Initialement, la norme Bluetooth a été proposée pour transmettre la voix et les données [2]. Elle avait pour objectif préalable de permettre des communications sur de courtes distances avec un débit de communication limitée. Ses caractéristiques ont ainsi retenu l'attention des développeurs de capteurs. Par exemple les capteurs BtNode sont conçus pour une communication de type Bluetooth. Pour autant, le protocole Bluetooth n'est pas le protocole le plus utilisé dans les réseaux de capteurs, bien qu'il puisse répondre en partie aux problèmes de préservation de l'énergie, car il est gravement handicapé par la taille limitée du réseau qu'il peut former (8 nœuds, 1 maître et 7 esclaves).

I.6.2 La norme Wibree (Ultra Low Power Bluetooth) : Elle est considérée comme une version allégée de la norme Bluetooth fonctionnant dans la bande de fréquence des 2,4 GHz. Wibree n'utilise pas de sauts de fréquences. Cette norme prend en charge une topologie en étoile avec un maître et sept esclaves [3]. Afin de réduire la consommation d'énergie de Bluetooth, Wibree utilise une puissance de transmission et un débit symbole faibles. La consommation d'énergie de Wibree est l'équivalent de 10% de celle d'une connexion par Bluetooth. Sa limite principale est la faible portée de communication: 5 à 10 m.

I.6.3 La norme IEEE 802.15.3 / UWB (Ultra Wide Band) : Cette norme utilise des signaux radio envoyés avec une intensité très faible et des impulsions très courtes [4]. Elle opère dans la bande de fréquence de 3,1GHz à 10,6 GHz. UWB est conçue pour remplacer la norme Bluetooth afin d'offrir plus de bande passante, moins d'interférences avec les autres technologies et un délai plus court. UWB est utilisée pour les transmissions à haut débit avec une consommation électrique (proche de 400 mW). Cette technologie offre des avantages par rapport à Bluetooth. Elle consomme 50 fois moins d'énergie pour transmettre un bit par rapport à Bluetooth. Selon Akyildiz et al. [5], aujourd'hui, le standard IEEE 802.15.3 est devenu le candidat le plus intéressant pour fournir la qualité de service dans les réseaux WMSNs (Wireless Multimedia Sensor Networks). L'inconvénient majeur de la technologie UWB est sa faible portée de communication (environ 10 m).

I.6.4 La norme IEEE 802.15.4 / Zigbee : Elle est conçue pour être utilisée dans les communications à très faible puissance et sur des distances réduites. Cette technologie est utilisée dans les réseaux de capteurs sans fil **[10].** Par rapport à Bluetooth, cette technologie fournit une faible latence ; une couche physique « DSSS : Direct Sequence Spread Spectrum » permet aux nœuds de basculer en mode sommeil sans perdre la synchronisation. Le protocole Zigbee est basé sur le standard déploiement de réseau dense à plus de 65000 nœuds avec une portée de l'ordre de 100 mètres pour un débit de 250 Kbits/s. Ces caractéristiques en font aujourd'hui le principal protocole utilisé dans les réseaux de capteurs.

I.6.5 La norme IEEE 802.15.6 : Cette norme de courte portée est utilisée par des objets ou dispositifs à ultra basse consommation, placés sur ou à proximité d'un corps humain. Elle permet un débit maximal de 10 Mbits/s. Cette norme combine des caractéristiques de sécurité, de fiabilité, de qualité de service, de basse consommation d'énergie et de protection contre les interférences, ce qui la rend adaptées de multiples applications de réseaux radio corporels (WBAN, Wireless Body Area Networks) [22].

La norme IEEE 802.15.6 définit une couche MAC unique et trois couches physiques différentes utilisables en fonction des applications visées. La couche NB PHY (NB pour Narrow Band) autorise des transmissions a bande étroite dans les bandes ISM (Industrial, Scientific and Medical) traditionnelles avec des débits pouvant atteindre 500 Kbits/s. La couche physique UWB PHY s'appuie sur la technologie radio ultralarge bande (UWB), pour cela elle est appelée UWB PHY. Elle permet des débits allant jusqu'à 10 Mbits/s dans des bandes de fréquences situées autour de 4 GHz et 8 GHz. Enfin, la couche HBC PHY (HBC pour Human Body Communication) s'inspire du standard de communication en champ proche et exploite les bandes 16 MHz et 27 MHz.

I.6.6 La norme IEEE 802.11x/WiFi :

Le protocole de communication WiFi est le protocole le plus utilisé pour toutes les applications sans fil. Il offre une large bande passante (de 11 à 320 Mbits/s) ce qui a permis de démocratiser l'utilisation de latechnologie sans-fil dans les réseaux classiques WLANs. Les premiers capteurs sans-fil ont eu recours à ce protocole pour permettre la communication entre nœuds. Cependant, le standard de communication WiFi n'apparait plus actuellement comme une solution viable pour les réseaux de capteurs sans fil, du fait d'un besoin énergétique trop important pour son utilisation. La durée de vie des capteurs sans fil alimentés par des piles ne dépasse que rarement quelques heures. C'est pourquoi, les applications de capteurs à base de communication sans fil WiFi sont très peu répandues.

I.6.7 Choix de la norme : Le choix d'une technologie de communication sans fil dépend des services proposés, ainsi que des besoins du concepteur du réseau. Certains paramètres comme la consommation d'énergie, le débit, la durée de vie de la pile, la portée et le nombre de nœuds supportés doivent être pris en compte. Dans le Tableau 7, nous faisons une comparaison entre les protocoles de communications cités ci-dessus [11].

Protocole	Bluetooth	UWB	ZigBee	WiFi	IEEE 802.15.6
Norme IEEE	802.15.1	802.15.3	802.15.4	802.11x	802.15.6
Nombre de nœuds maximum	8	128	65000	32	256
Durée de vie moyenne de la pile	Plusieurs jours	Plusieurs minutes	Plusieurs mois à plusieurs années	Plusieurs minutes à plusieurs heures	---
Débit théorique maximum	Bluetooth Low Energy:1Mbit/s Bluetooth 3.0 + High Speed: 3-24 Mbit/s	110-480 Mbit/s	20 Kbit/s (EU), 40 Kbit/s (US) 250 Kbit/s(Global)	11-320 Mbit/s	10 Mbit/s
Bande de fréquence	2.4 GHz	3.1-10.6 GHz	868 MHz (EU), 915 MHz (US) 2.4 GHz (Global)	2.4 GHz, 5 GHz	---
Portée théorique maximum	10 m	<10 m	10-100 m	10-100 m	5-10 m
Consommation d'Energie	100-200 mW	400 mW pour 200 Mbit/s	30 mW	750-2000 mW	Jusqu'à 50 mW

Tableau I.2 Comparaison entre les différentes technologies sans fil

Dans notre application qui est les réseaux WBAN, nous n'avons pas besoin d'un très grand nombre de capteurs dans le réseau. Par contre, la faible consommation d'énergie, la longue durée de vie de la pile, le débit et la portée sont des facteurs très importants dans le cas d'une surveillance médicale à distance.

En tenant compte de ces contraintes, la technologie ZigBee peut être envisagée pour la transmission de données médicales collectées par les capteurs déployés sur le corps humain vers le nœud de collecte c.à.d. dans les communications intra-BAN et inter-BAN. En effet, cette technologie présente une faible consommation d'énergie et une longue portée mais son inconvénient est le faible débit des données.

Par contre, la technologie IEEE 802.15.6 présente un débit élevé et une consommation d'énergie acceptable, mais son point faible est sa portée réduite.

Donc le choix de la technologie de transmission sans fil dans les réseaux WBAN dépend de l'application et du type du capteur médical utilisé. Si le capteur présente un débit élevé et l'application n'a pas besoin d'une longue portée donc c'est la technologie IEEE 802.15.6 qui est préférée. Tandis que si le capteur présente un débit faible et l'application nécessite une longue portée alors la technologie ZigBee est préférable.

I.7 Les réseaux WBAN

I.7.1 Comparaison entre les réseaux WBAN et les réseaux RCSF :

I.7.1.1 Définition :

Wireless Sensors Networks (RCSF) : un réseau de capteurs sans fil est un réseau ad-hoc avec un grand nombre de nœuds. Ces nœuds sont des capteurs capables de récolter et de transmettre des données environnementales d'une manière autonome. La position de ces nœuds n'est pas obligatoirement prédéterminée. Ils peuvent être aléatoirement dispersés dans une zone géographique, appelée « champ de captage » correspondant au terrain d'intérêt pour le phénomène capté comme le montre la figure suivante.

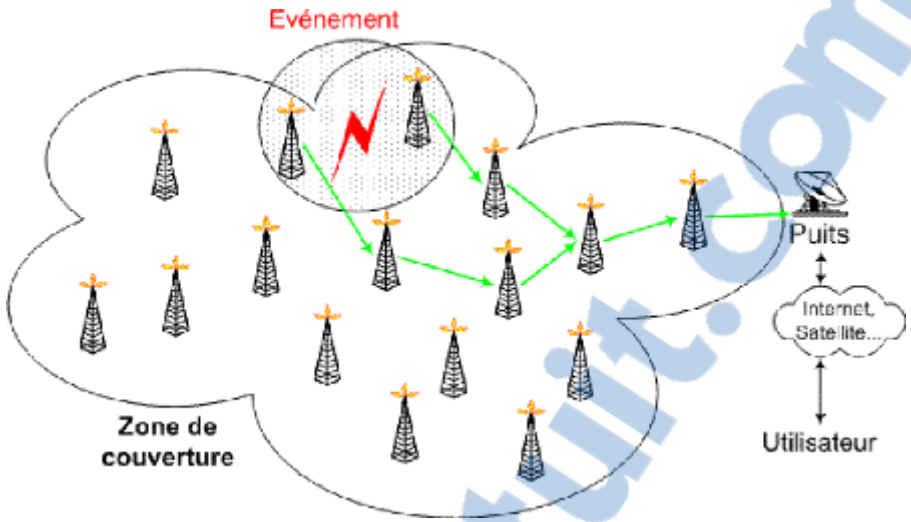


Figure I.3 Réseau RCSF [16]

Wireless Body Area Networks (WBAN) : un réseau de capteurs corporels sans fil est un réseau constitué de mini-capteurs portables ou implantés dans le corps humain. Chaque nœud capteur est généralement capable de détecter une ou plusieurs caractéristiques physiologiques à partir du corps humain ou de son environnement. Le nœud capteur stocke puis transmet les données mesurées par l'intermédiaire d'un réseau sans fil à un dispositif de traitement central connu sous le nom de serveur personnel. Les WBANs ont plus d'exigences en termes de sécurité et de miniaturisation des capteurs par rapport aux RCSFs.

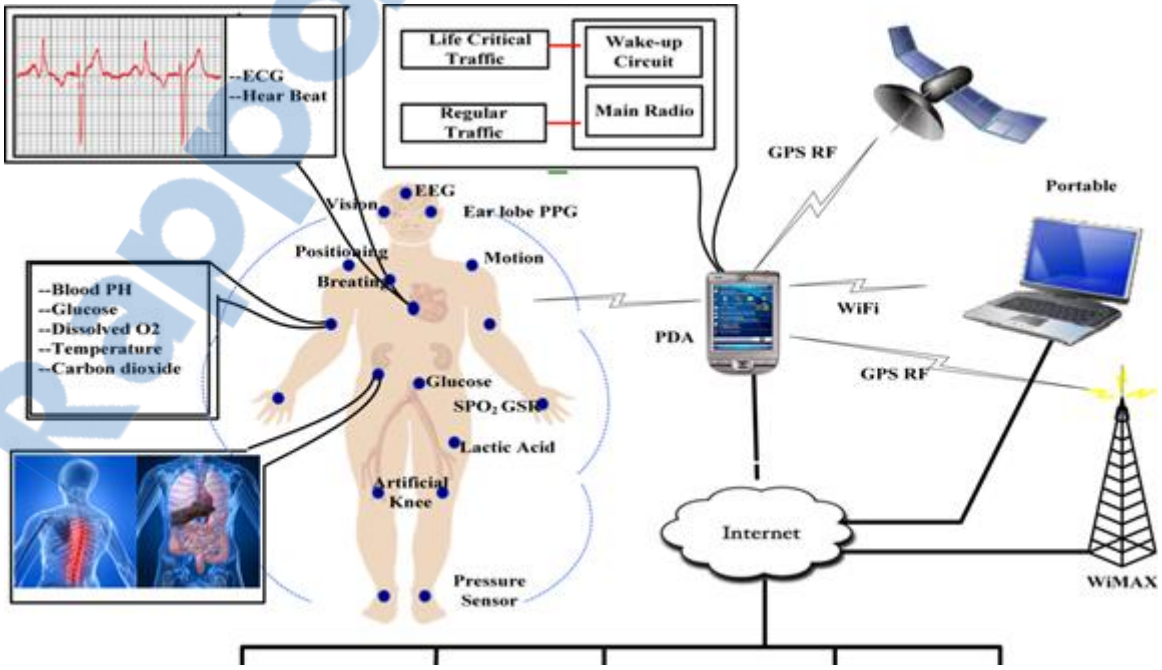


Figure I.4 Réseau WBAN [17].

I.7.1.2 Différence entre WBAN et RCSF : Nous présentons ici les différences entre WBAN et RCSF qui sont classifiées selon plusieurs facteurs. Le Tableau 3 résume ces différences.

Réseau / Facteur	WBAN	WSN
Déploiement	Sur le corps humain	Dans des endroits qui ne sont pas facilement accessibles
Densité	Pas dense	Dense
Débit	Actions périodiques	Actions à des intervalles irréguliers
Latence	Facilement accessibles, temps de latence réduit	Difficilement accessibles, temps de latence élevé
Mobilité des nœuds	Nœuds mobiles	Nœuds stationnaires

Tableau I.3 Différences entre WBAN et RCSF [18]

Déploiement et densité: Le nombre des nœuds capteurs déployés par l'utilisateur dépend de différents facteurs. Typiquement, les nœuds dans les WBAN sont placés stratégiquement sur le corps humain, ou sont cachés sous les vêtements. Les réseaux WBAN n'emploient pas de nœuds redondants pour faire face à divers types de défaillances. Par conséquence, le nombre de nœuds dans les réseaux WBAN n'est pas dense.

Par contre, dans les réseaux RCSF, les nœuds sont souvent déployés dans des endroits qui ne sont pas facilement accessibles, ce qui exige de placer un nombre plus élevé de nœuds pour établir une architecture de redondance afin de contourner les problèmes de défaillance des nœuds.

Débit de données: La plupart des réseaux RCSF sont utilisés pour la surveillance des événements, où ces événements peuvent se produire à des intervalles irréguliers. Par contre les réseaux WBAN sont utilisés pour mesurer des activités physiologiques et des actions qui peuvent se produire d'une manière plus périodique et peut donner lieu à des flux de données présentant des taux relativement stables.

Latence: Dans le cas des réseaux WBAN, le remplacement des batteries pour les capteurs est beaucoup plus facile par rapport au cas dans les réseaux RCSF dont les nœuds peuvent

être physiquement inaccessibles après le déploiement. Par conséquence, il peut être nécessaire de maximiser la durée de vie des batteries dans un réseau RCSF. Le temps de latence dans les WBAN est plus petit par rapport au temps de latence dans les RCSF à cause de nombre des sauts réduits.

Mobilité: Dans le cas des réseaux WBAN, les personnes portant des capteurs peuvent se déplacer et par conséquence les nœuds capteurs sont des nœuds mobiles contrairement aux nœuds RCSF qui sont habituellement considérés comme des nœuds stationnaires.

I.7.2– Topologies des réseaux WBAN : Dans cette section, nous décrivons les topologies les plus utilisées pour le déploiement des réseaux WBAN. Nous distinguons les topologies suivantes : point-à-point, étoile, maille et arbre. La Figure 4 représente ces quatre topologies.

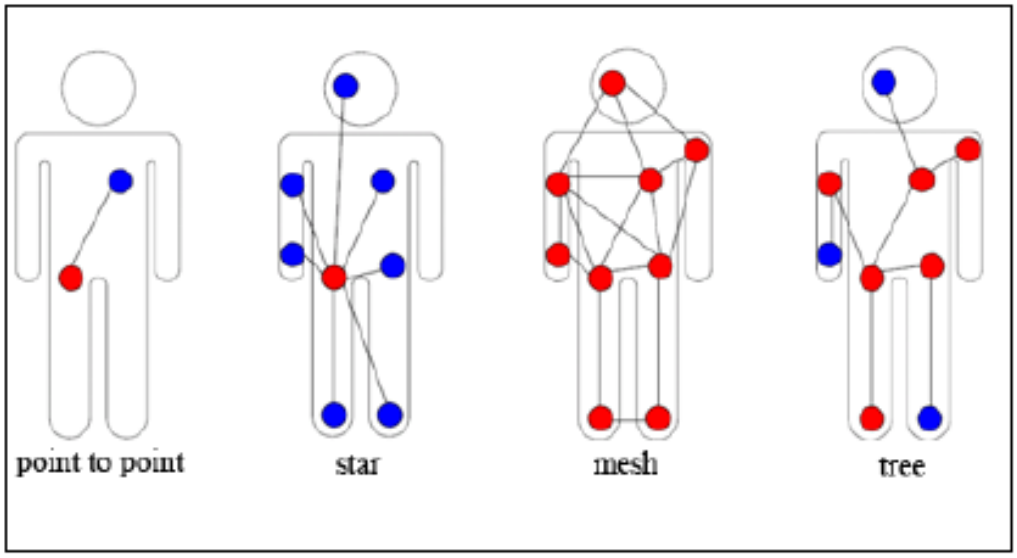


Figure I.5 Les topologies dans les réseaux WBAN [18]

I.7.2.1 Topologie Point-à-point :

C'est la topologie la plus simple dans les réseaux. Cette topologie est destinée à une seule liaison, par exemple entre un collecteur de données et un nœud capteur. Le principal avantage de cette topologie est la simplicité qui permet souvent l'utilisation d'un protocole simple, la faible latence et le débit élevé. Les inconvénients comprennent ses fonctionnalités limitées ainsi que sa faible couverture [18].

I.7.2.2 Topologie en Etoile :

Une topologie dans laquelle tous les nœuds sont connectés par l'intermédiaire d'un nœud central est une topologie en étoile (*Star* en anglais). Ces nœuds peuvent seulement envoyer ou recevoir un message à ou de l'unique nœud central. Il ne leur est pas permis de s'échanger des messages directement entre eux. Le nœud central joue le rôle d'un relais entre les différents nœuds À ce jour, cette topologie est la plus proposée et utilisé pour les réseaux WBAN.

Cette topologie présente des avantages qui peuvent être résumés par la simplicité, la faible consommation d'énergie des nœuds et la moindre latence de communication entre les nœuds et le nœud central. Par contre, son inconvénient majeures la vulnérabilité du nœud central car tout le réseau est géré par un seul nœud [18].

I.7.2.3Topologie en Maille :

Une topologie avec une connectivité complète entre les nœuds est une topologie maillée (*Mesh* en anglais). Dans ce cas (dit « communication multi-sauts »), tout nœud peut échanger avec n'importe quel autre nœud du réseau s'il est à portée de transmission. Un nœud voulant transmettre un message à un autre nœud hors de sa portée de transmission, peut utiliser un nœud intermédiaire pour envoyer son message au nœud destinataire.

L'avantage d'utiliser la topologie en maille est la possibilité de passer à l'échelle du réseau, avec redondance et tolérance aux fautes et une bonne couverture. Par contre, les inconvénients d'une telle topologie sont l'importante consommation d'énergie induite par la communication multi-sauts ainsi que la latence créée par le passage des messages à travers plusieurs nœuds avant d'arriver au nœud destinataire.

L'utilisation d'une topologie maillée est une considération primordiale dans toutes les situations dans lesquelles la fiabilité et la communication flexible sont prioritaires par rapport à l'efficacité énergétique et la durée de vie du réseau [18].

I.7.2.4 Topologie en Arbre :

Une topologie en arbre (*Tree* en anglais) contient un sommet avec une structure de branches au-dessous. Les connexions entre les nœuds sont structurées hiérarchiquement, ce qui signifie que chaque nœud peut être un fils à un nœud de niveau supérieur et un père à un nœud de niveau inférieur.

Cette topologie divise le réseau en sous-parties de sorte qu'il devient plus facile à gérer. Elle présente une bonne tolérance aux fautes, une bonne couverture, une bande passante élevée et une faible latence. Mais toutefois, les nœuds pères peuvent consommer beaucoup d'énergie.

Le Tableau 2 résume les avantages et les inconvénients de chacune des topologies décrites ci-dessus.

Topologie	Avantages	Inconvénients
Point-à-point	-Simplicité -Faible latence -Débit élevé	-Fonctionnalités limitées -Faible couverture
Etoile	-Simplicité -Faible consommation d'énergie -Faible latence -Bande passante élevée	-Vulnérabilité du nœud central
Maille	-Redondance -Tolérance aux fautes -Bonne couverture	-Consommation d'énergie importante -Latence élevée
Arbre	-Bonne tolérance aux fautes -Bonne couverture -Faible latence -Bande passante élevée	- Consommation d'énergie des nœuds pères

Tableau I.4 Lesavantages et les inconvénients des topologies dans les réseaux WBAN [18]

I.8 Conclusion :

Dans ce chapitre, nous avons présenté un état de l'art sur les réseaux de capteurs sans fils médicaux. Après une introduction générale sur les réseaux de capteurs sans fil médicaux, nous avons parlé des systèmes WBAN où nous avons fait une comparaison entre les réseaux WBAN et RCSF.

Ensuite nous avons donné une définition technique du capteur médical et nous avons présenté plusieurs types de capteurs médicaux avec leurs fonctions. Puis nous avons présenté l'architecture d'un nœud capteur, ses caractéristiques et les systèmes d'exploitation dans les capteurs.

Dans le chapitre suivant, Nous abordons dans le chapitre suivant d'une part les attaques et menaces qui peuvent compromettre le réseau WBAN et d'autre part, nous présentons en détail notre mécanisme de gestion de clés pour les réseaux WABNs.

Chapitre II
Gestion de clés dans les réseaux corporels sans fil

[Chapitre II Gestion des clés dans les réseaux corporels sans fil]

II.1 Introduction : Les réseaux de capteurs médicaux soulèvent de nouveaux défis en termes de sécurité et de protection contre les anomalies et les attaques. Le mode de communication sans fil utilisé entre ces capteurs et le nœud de collecte accentue ces vulnérabilités. La sécurité des données et la détection des attaques et d'anomalies dans les réseaux de capteurs sans fil médicaux constituent actuellement l'un des principaux challenges à relever.

Il faut cependant noter que la sécurisation du réseau est nécessaire mais pas suffisante. En effet, un attaquant peut dans certains cas modifier les données ou injecter des données erronées et générer une fausse alerte. Par conséquence, le réseau doit aussi utiliser des tests de plausibilité qui permettent de vérifier que les mesures obtenues sont cohérentes. Ces tests sont généralement réalisés par le nœud de collecte [18].

En raison des contraintes spécifiques aux réseaux de capteurs médicaux, il est difficile d'employer directement les approches de sécurité existantes pour les réseaux classique. Par conséquence, il faut développer des mécanismes de sécurité pour les réseaux de capteurs tout en empruntant des idées à partir des techniques de sécurité en vigueur.

Dans ce chapitre, et en premier lieu, nous allons brièvement présenter l'aspect sécurité dans les réseaux WBANs, les défis à relever et les problèmes de sécurité. En deuxième lieu, nous allons présenter notre protocole de gestion de clés pour les réseaux WBANs.

II.2 Les attaques et les anomalies dans les systèmes WBAN : Les différentes spécificités et contraintes des réseaux de capteurs sans fil médicaux citées précédemment exposent les réseaux de capteurs à de nombreuses menaces. Si certaines de ces menaces peuvent se retrouver dans les réseaux ad-hoc, d'autres sont spécifiques aux réseaux de capteurs sans fil et s'attaquent tout particulièrement à l'énergie limitée des capteurs [18].

II.2.1 Classifications des attaquants : Différents types de modèles d'attaquants avec différentes motivations peuvent mener une même attaque, ce qui rend la modélisation d'un attaquant essentielle dans l'étude de la sécurité des réseaux de capteurs. La modélisation d'un attaquant dépend du type de l'attaque à exécuter, de sa position par rapport au réseau et du nombre d'adversaires utilisés. Dans un réseau de capteurs, un attaquant peut être classifié selon plusieurs critères (Tableau II.1).

II.2.1.1 Selon son intention :

Attaquant passif : où l'attaquant essaye de collecter des données sur le réseau sans affecter son fonctionnement.

Attaquant actif: où l'attaquant essaye de détruire le fonctionnement du réseau d'une manière partielle ou bien totale.

II.2.1.2 Selon sa position par rapport au réseau :

Attaquant externe: où l'attaquant est considéré comme un "étranger" par rapport au réseau. Il s'agit d'un utilisateur non autorisé qui s'introduit depuis l'extérieur du périmètre de sécurité du réseau.

Attaquant interne: où l'attaquant se manifeste comme une entité légitime du réseau autorisée à accéder aux ressources fournies par le système. L'attaquant est ainsi authentifié et reconnu par l'ensemble des éléments du réseau.

II.2.1.3 Selon sa capacité :

Attaquant fort: l'attaquant est équipé de ressources supplémentaires par rapport à l'ensemble des nœuds présents dans le réseau. Par exemple, un attaquant utilise un PC portable avec un médium radio sophistiqué.

Attaquant ordinaire: l'attaquant possède les mêmes caractéristiques que les autres nœuds du réseau. De ce fait, il n'a aucun avantage par rapport aux nœuds légitimes.

Selon son intention	Selon sa position par rapport au réseau	Selon sa capacité
-Attaquant passif *-Attaquant actif*	*-Attaquant externe* *-Attaquant interne*	*-Attaquant fort* *-Attaquant ordinaire*

Tableau II.1 Classifications des attaquants [18].

II.3 Objectifs de la sécurité :

vise généralement cinq principaux objectifs :

- ✓ L'authentification : L'authentification des capteurs est nécessaire pour s'assurer que l'identité déclarée par un capteur est bien celle du capteur déclarant. En l'absence d'un mécanisme permettant d'authentifier clairement un nœud du réseau, de nombreuses attaques peuvent se mettre en place [18].

- ✓ L'intégrité des données : Les données circulant sur le réseau WBAN ne doivent pas pouvoir être altérées au cours de la communication. Il faut donc s'assurer que personne ne puisse capturer et modifier les données du réseau. Aussi, il faut vérifier que les données n'ont pas subi d'altérations dues à un disfonctionnement du matériel, qui est un risque important sur des capteurs sensibles aux altérations d'états [18].
- ✓ La confidentialité des données : Le réseau doit s'assurer que les données transmises soient confidentielles et ne puissent être lues par des dispositifs ou personnes autres que l'équipe médicale (médecins, infirmiers, etc.). Une personne extérieure au réseau ne doit pas être capable de lire les informations échangées. Les données doivent être cachées ou cryptées de telle manière que personne ne puissent y accéder [18].
- ✓ La disponibilité du réseau : Le réseau doit pouvoir être disponible à tout instant, c.à.d. que l'envoi d'information ne doit pas être interrompu, de même que la circulation de l'information ne doit pas être stoppée. Dans le cas d'un réseau de capteurs réactif, il faut qu'un capteur, qui détecte un événement, puisse transmettre à tout instant cette information vers la base du réseau de capteurs pour l'en informer
- ✓ La fraîcheur des données : Par fraîcheur des données, nous entendons savoir si les données sont récentes ou non. Cela signifie qu'il faut s'assurer que la donnée transmise corresponde à un état présent. La fraîcheur des données garantit ainsi que ces données ne reflètent pas un état passé [18].

II.4 Les contraintes des réseaux WBAN :

Un réseau de capteurs sans fil médicaux est un réseau spécial qui a un certain nombre de contraintes par rapport à un réseau informatique classique. Ces contraintes sont le résultat des limitations concernant la mémoire du capteur, sa réserve énergétique, sa capacité de traitement ainsi que l'utilisation d'une communication sans fil. Les contraintes dans un réseau de capteurs sans fil médicaux sont classées en deux catégories : contraintes matérielles et contraintes réseau. Le Tableau II.2 résume ces contraintes.

Contraintes matérielles	Contraintes réseau
Mémoire et espace de stockage limités Energie Limitée Capacité de calcul limitée Faible débit	Communication incertaine

Tableau II.2 Les contraintes de sécurité dans un RCSF corporels [18]

II.4.1Contraintes matérielles :

Ces contraintes sont liées aux capacités matérielles et physiques des capteurs, ce qui représente un handicap pour les besoins en sécurité qui nécessitent en général des ressources supplémentaires. Toutes les approches de sécurité nécessitent une certaine quantité de ressources pour la mise en œuvre, y compris la mémoire des données, l'espace pour le code, et de l'énergie pour alimenter le capteur. Toutefois, actuellement, ces ressources sont très limitées dans un minuscule capteur sans fil.

Mémoire et espace de stockage limités : un capteur est un petit dispositif avec une mémoire très réduite et un espace de stockage limité. Donc pour construire un mécanisme de sécurité efficace, il est nécessaire de limiter la taille du code de l'algorithme de sécurisation.

Energie Limitée : l'énergie est le principal obstacle aux capacités de capteurs sans fil. Lors de l'ajout d'un code de sécurité à un nœud capteur, nous nous intéressons à l'impact que la sécurité présente sur la durée de vie de la batterie. L'énergie supplémentaire consommée par les nœuds de capteurs en raison de la sécurité est liée au traitement nécessaire pour les fonctions de sécurité.

Capacité de calcul limitée : Malgré les progrès dans la fabrication de capteurs de plus en plus puissants, les capteurs actuels possèdent une capacité de calcul très réduite. Cette faible capacité de calcul ne permet pas d'utiliser des algorithmes complexes, et particulièrement des algorithmes cryptographiques gourmands en ressources CPU [18].

Faible débit : le débit actuel dans les réseaux de capteurs ne dépasse pas les quelques centaines de kilo-octets par seconde.

II.4.2 Contraintes réseaux :

La communication non fiable constitue une autre menace à la sécurité du capteur. La sécurité des réseaux de capteurs repose en grande partie sur un protocole bien défini, ce qui dépend à son tour de la communication.

Communications incertaines : les communications sans fil sont en général incertaines car des paquets peuvent être perdus ou endommagés à cause de la transmission radio. Ce manque de fiabilité dans la communication constitue un problème additionnel pour les nœuds capteurs.

II.5 Cryptographie :

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité.

Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

II.5.1La cryptographie symétrique : également dite à clé secrète (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé. On a des traces de son utilisation par les Égyptiens vers 2000 av. J.-C. Plus proche de nous, on peut citer le chiffre de Jules César, dont le ROT13 est une variante.

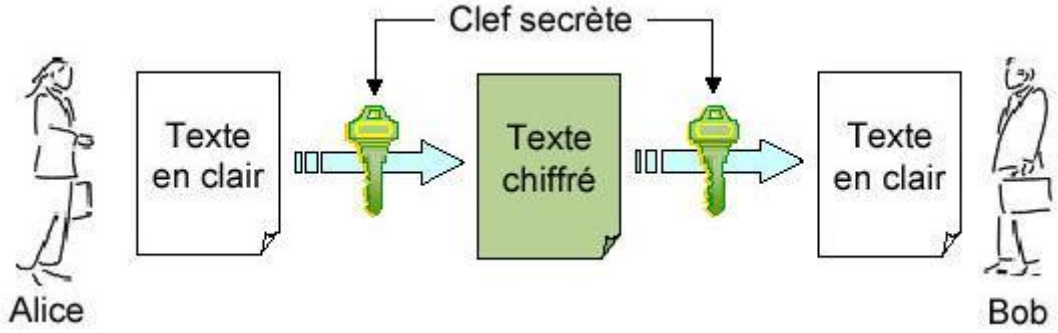


Figure II.1 cryptage/décryptage symétrique [20].

II.5.2 La cryptographie asymétrique :

Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) est apparu en 1976, avec la publication d'un ouvrage sur la cryptographie par *Whitfield Diffie* et *Martin Hellman*.

Dans un crypto système asymétrique (ou *crypto système à clés publiques*), les clés existent par paires (le terme de *bi-clés* est généralement employé) :

- Une clé publique pour le chiffrement ;
- Une clé secrète pour le déchiffrement.

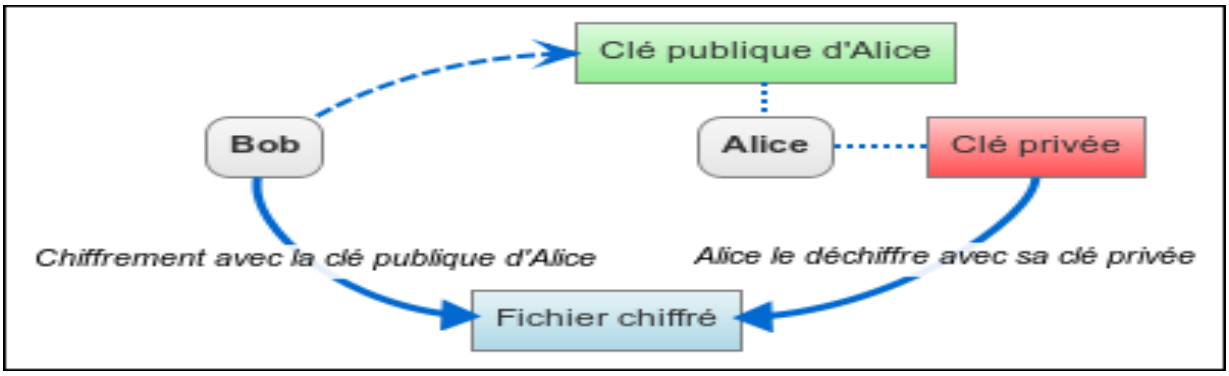


Figure II.2 principe cryptage/décryptage asymétrique [21].

II.6 fonction de hachage : Une fonction de hachage est typiquement une fonction qui, pour un ensemble de très grande taille (théoriquement infini) et de nature très diversifiée, va renvoyer des résultats aux spécifications précises en général des chaînes de caractère de taille limitée ou fixe [22].

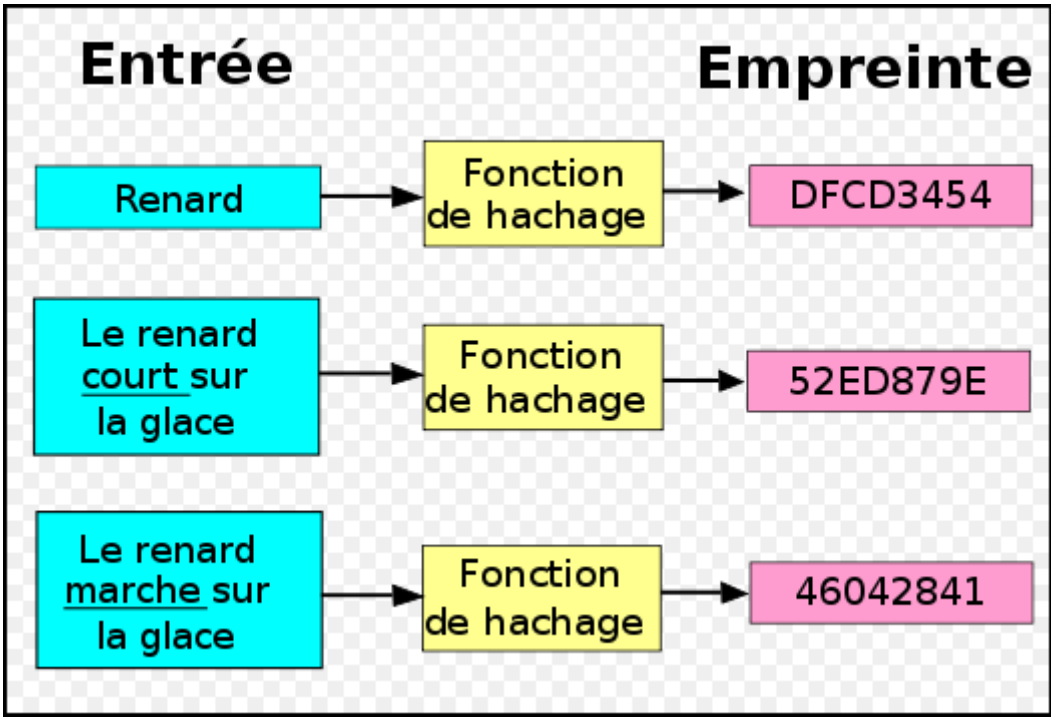


Figure II.3 Fonction de hachage [23].

- **Fonctions de hachage usuelles :**

- MD4 et MD5 (Message Digest) furent développées par Ron Rivest. MD5 produit des hachés de 128 bits en travaillant les données originales par blocs de 512 bits.
- SHA-1 (Secure Hash Algorithm 1), comme MD5, est basé sur MD4. Il fonctionne également à partir de blocs de 512 bits de données et produit par contre des condensés de 160 bits en sortie. Il nécessite donc plus de ressources que MD5.
- SHA-2 (Secure Hash Algorithm 2) a été publié récemment et est destiné à remplacer SHA-1. Les différences principales résident dans les tailles de hachés possibles : 256, 384 ou 512 bits. Il sera bientôt la nouvelle référence en termes de fonction de hachage.
- RIPEMD-160 (Ripe Message Digest) est la dernière version de l'algorithme RIPEMD. La version précédente produisait des condensés de 128 bits mais présentait des failles de sécurité importantes. La version actuelle reste pour l'instant sure; elle produit comme son nom l'indique des condensésde 160 bits. Un dernier point la concernant est sa relative gourmandise en termes de ressources et en comparaison avec SHA-1 qui est son principal concurrent.

II.7 Mécanismes de gestion de clés dans les WBANs :

La gestion de clés vise à offrir les quatre foncions principales suivantes :

- la génération
- la distribution
- le stockage
- la vérification de clés

Sous les contraintes des réseaux WBANs, la conception d'un mécanisme de gestion de clés est un grand défi.

La cryptographie à clé publique est une solution très efficace qui fournit des mécanismes plus sûrs et fiables pour l'authentification et la distribution des clés. Traditionnellement, la cryptographie asymétrique exige un espace mémoire assez grand et de haute capacité de calcul, ce qui la rend inappropriée pour les réseaux de capteurs. Cependant, des recherches récentes ont montré la faisabilité d'appliquer la solution à clé publique aux réseaux de capteurs en choisissant les bons algorithmes et les paramètres appropriés. Pour cette raison, la plupart des schémas de gestion de clés proposes pour les WBANs sont basés sur la

cryptographie symétrique [16]. Cependant le principal inconvénient de la cryptographie symétrique c'est l'échange préalable de la clé.

La solution commune est d'utiliser une méthode de pré-distribution dans laquelle les clés sont chargées dans les nœuds capteurs avant le déploiement.

II.7.1 les Objectifs de la gestion des clés :

L'établissement de clés cryptographiques entre les nœuds du réseau permet de :

- Sécuriser le routage
- Sécuriser l'agrégation
- Garantir l'intégrité des données échangées
- Assurer l'authentification

Comme a été déjà mentionné précédemment, les nœuds capteurs possèdent des ressources limitées en termes de calcul, stockage et énergie. Les réseaux de capteurs ont une structure Ad-hoc d'où l'absence d'une infrastructure. Aussi les nœuds du réseau sont sujets à compromission. Toutes ces contraintes doivent être prises en considération lors de l'établissement d'un protocole de gestion de clés.

II.7.2 choix de la Solutions :

II.7.2.1une seul clé pré-partagé par le réseau : (cryptage symétrique)

Cette solution consiste à utiliser une clé unique pré-partagée par tous les nœuds du réseau. Parmi ces avantages :

-Gestion simple des clés, car il suffit de pré-charger les nœuds, avant le déploiement, par une seule clé commun.

- Toutes les communications peuvent être chiffrées simplement en utilisant un minimum de mémoire (stockage d'une seule clé et c'est l'avantage du cryptage symétrique).

L'inconvénient de cette solution c'est que si la clé est connu par un nœud étranger tout le réseau est menacé puisque tout les nœuds partage la même clé.

II.7.2.2 deux clés partagée par paire de nœuds : (cryptage asymétrique)

Dans cette solution, chaque nœud est pré-chargé avec (N-1) clés secrètes, chacune de ces clés est connue seulement par ce nœud et un des (N-1) autres nœuds (N étant le nombre de nœuds dans le réseau). Cette solution permet une parfaite résilience car la compromission d'un nœud n'affecte pas la sécurité des autres nœuds. Par contre cette solution n'est pas appropriée aux réseaux de capteurs car: Elle exige une capacité mémoire importante pour stocker les (N-1) clés. L'ajout de nouveaux nœuds est difficile parce que les nœuds existants ne possèdent pas les clés de ces nouveaux nœuds.

II.8 – Notre protocole de gestion de clefs :

Dans cette partie, nous allons présenter notre protocole de gestion de clés dans les réseaux WBANs, qui vise à établir des clés de session entre les nœuds du réseau WBAN et la station de base.

II.8.1 – Hypothèses :

On suppose que :

- ✓ Chaque nœud capteur est créé avec un identificateur de périphérique unique (UID) qui n'est connu que par ce nœud capteur.
- ✓ Les identificateurs de tous les nœuds doivent être programmés manuellement dans la station de base.
- ✓ Chaque UID agit comme un secret initial partagé entre le nœud capteur et la station de base
- ✓ Chaque UID n'est jamais échangé en clair

II.8.2 – Phase d'établissement de clés entre un nœud capteur et la station de base :

Cette phase a pour objectif d'établir efficacement et sûrement les clés cryptographiques symétriques entre les nœuds capteurs et la station de base.

La figure suivante illustre notre approche de génération et de distribution de clés entre un nœud capteur et la station de base.

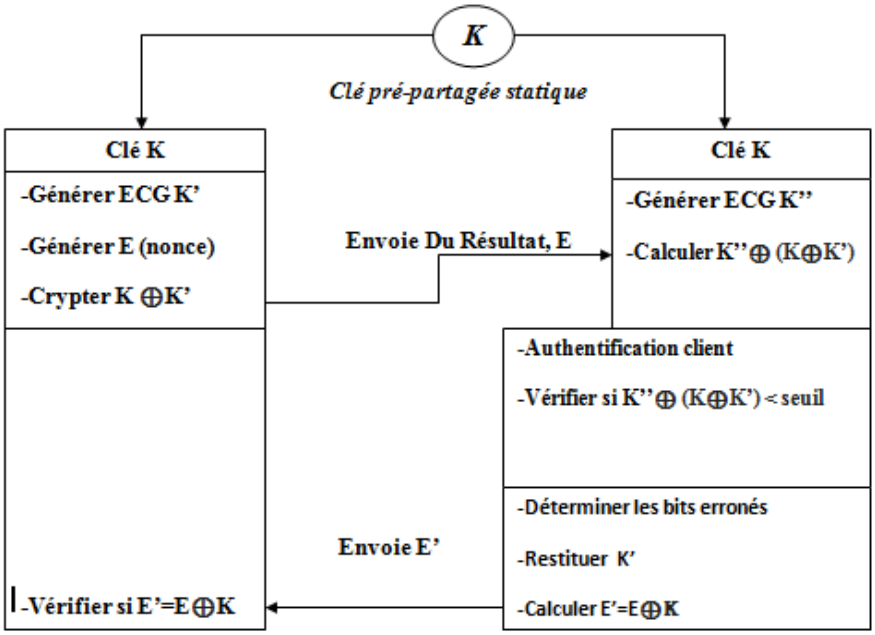


Figure II.4 Phase d'établissement de communication entre les nœuds et la station de base.

Chaque nœud qui vise à établir une clé de session symétrique avec la station de base effectue les étapes suivantes :

- Etape 1: générer ECG K' coté Capteur et K'' coté station de base.
- Étape 2: Crypter ECG K' à l'aide de la clé K envoyer le résultat etE a la station de base
- Étape 3: coté station de base générer K'' puis calculer K''⊕ (K⊕K')
- Étape 4: Authentification du client si K''⊕ (K⊕K') < seuil
- Étape 5: Déterminer les bits erronés s'ils y'on a restitué K' puis calculer E'.
- Etape 6 : coté client vérifier que si E'=E⊕K.

II.8.3 – Analyse du protocole en termes de services de sécurité :

Confidentialité: Cet aspect est assuré par l'utilisation du chiffrement symétrique pour chiffrer le trafic échangé entre la station de base et les nœuds de capteurs. Intégrité et authenticité.

II.9 – Conclusion

La sécurité des réseaux de capteurs corporels contre les éventuelles attaques et menaces est indispensable. Le développement des mécanismes de protection pour les réseaux WBANs est un défi majeur car ces systèmes sont d'une part limités en termes de ressources mémoire, CPU et énergie, d'autre part ces réseaux ont une topologie ad hoc i.e. sont sans infrastructure ce qui rend les solutions de sécurité traditionnelles inapplicables dans ce type de réseau. Dans ce chapitre, nous avons développé un protocole léger de génération et de distribution de clés cryptographiques dans les réseaux de capteurs corporels afin de protéger les informations véhiculées dans ces réseaux. Le chapitre suivant est consacré à l'évaluation et la validation de notre solution en utilisant le système d'exploitation Contiki et le simulateur Cooja.

Chapitre III
Réalisation et simulation

III.1 – Introduction :

Dans ce chapitre, nous allons tout d'abord aborder l'environnement de travail, ensuite nous allons détailler l'implémentation de notre protocole de gestion de clés, et enfin nous allons présenter les résultats de simulation.

III.2 – Environnement de travail et outils de développement :

Contiki est un système open source, léger, flexible et générique qui s'appuie sur un modèle de fonctionnement hybride. Ce système a été développé par un groupe de développeurs de l'industrie et du monde universitaire par Adam Dunkels de l'institut suédois d'informatique en 2002. Destiné à être embarqué dans des capteurs miniatures ne disposant généralement que de ressources limitées, Contiki a présenté l'idée d'utiliser la communication IP dans des réseaux de capteurs basse consommation. En plus il supporte les protocoles IPV6 et 6LOWPAN cela s'avère particulièrement utile dans la mesure où les nœuds communiquent en IPV6 et utilisent le standard 802.15.4 définie par l'IEEE. Contiki contient deux piles de communications : uIP et Rime.

uIP est une petite pile de TCP/IP qui permet a Contiki de communiquer sur internet. Rime est une pile de communication légère conçue pour des radios basse puissance. Il fournit une vaste gamme de communications primitives.

Cooja est un simulateur qui est fourni avec Contiki.

III.3 – Les étapes de développement du protocole :

III.3.1 – Installation de Contiki 3.0 :

Dans cette partie, nous allons décrire les étapes d'installation de Contiki 3.0 sous Ubuntu 16.04 lts 64 bits.

- Téléchargement de contiki 3.0 a partir du lien suivant :http://www.contiki-os.org/download.html

Ou par ligne de commande : wget https://github.com/contiki-os/contiki/archive/3.0.zip

- décompressez le fichier dans / home / user / contiki a l'aide de la commande sudo unzip contiki – 3.0.zip.
- Installation de package nécessaires pour tout les plateformes :

```
sudo apt-get install build-essential binutils-msp430 gcc-msp430 msp430-libc msp430mcu
mspdebug gcc-arm-none-eabi gdb-arm-none-eabi openjdk-8-jdk openjdk-8-jre ant libncurses5-dev
```

- Enfin pour vérifier que l'installation c'est terminée avec sucées suivre les étapes suivantes :
  1. Dans la fenêtre du terminal, accédez au dossier Exemple /Hello World : cd Example/hello-world
  2. Compilez le code de la plate-forme native (à utiliser lorsqu'aucuncapteur n'est connecté à l'ordinateur portable).Make TARGET = native
  3. Une fois la compilation terminée, exécutez le programme Hello World. ./hello-world.native
  4. Vous devriez voir ce qui suit sur le terminal:

```
Contiki 3.0 started with IPV6, RPL
 Rime started with address 1.2.3.4.5.6.7.8
 MAC nullmac RDC nullrdc NETWORK sicslowpan
 Tentative link-local IPv6 address
fe80:0000:0000:0000:0302:0304:0506:0708
```

```
Hello, world
```

III.3.2 Cooja :

COOJA est l'acronyme de Contiki OS Java Simulator.

Pour développer les programmes au sein de Contiki, le système met à disposition un simulateur réseau appelé Cooja. Le logiciel permet d'émuler des nœuds et de charger un programme compilé. Ceci est particulièrement utile pour tester les programmes avant de les mettre dans la mémoire flash des nœuds réels, puisque le logiciel simule les conditions d'exécution et de mémoire de I MSP430. Les données collectées provenant du sink via sa sortie standard peuvent être enregistrées dans des fichiers ou lus par des logiciels qui peuvent par la suite traiter et présenter les données à l'utilisateur.

Comment lancer cooja a partir du terminal ? :

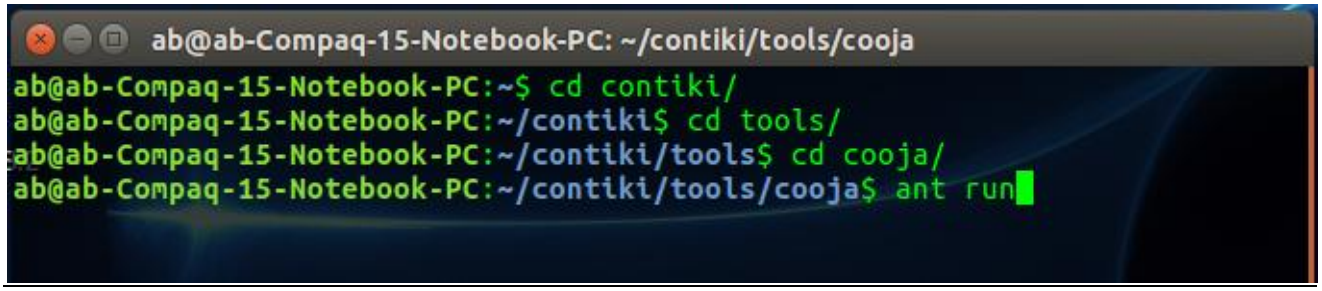


Figure III.1 lancement de cooja à partir du terminal

Apres le démarrage de cooja créer une nouvelle simulation comme cela :

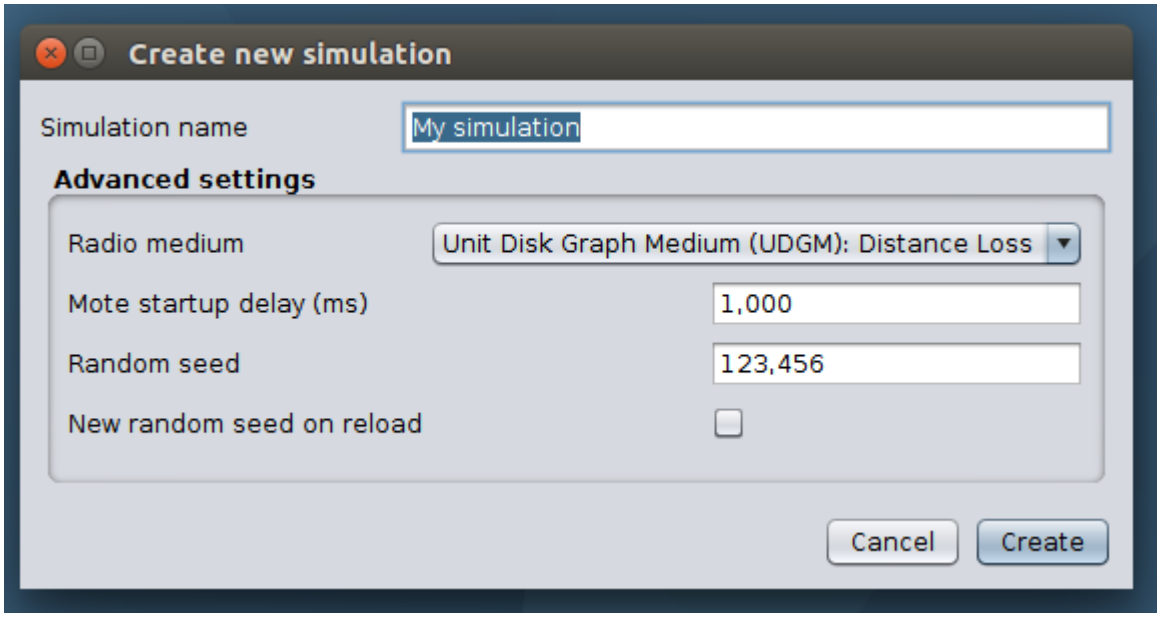


Figure III.2création d'une nouvelle simulation

Puis chargement du programme client ensuite compile est faire create

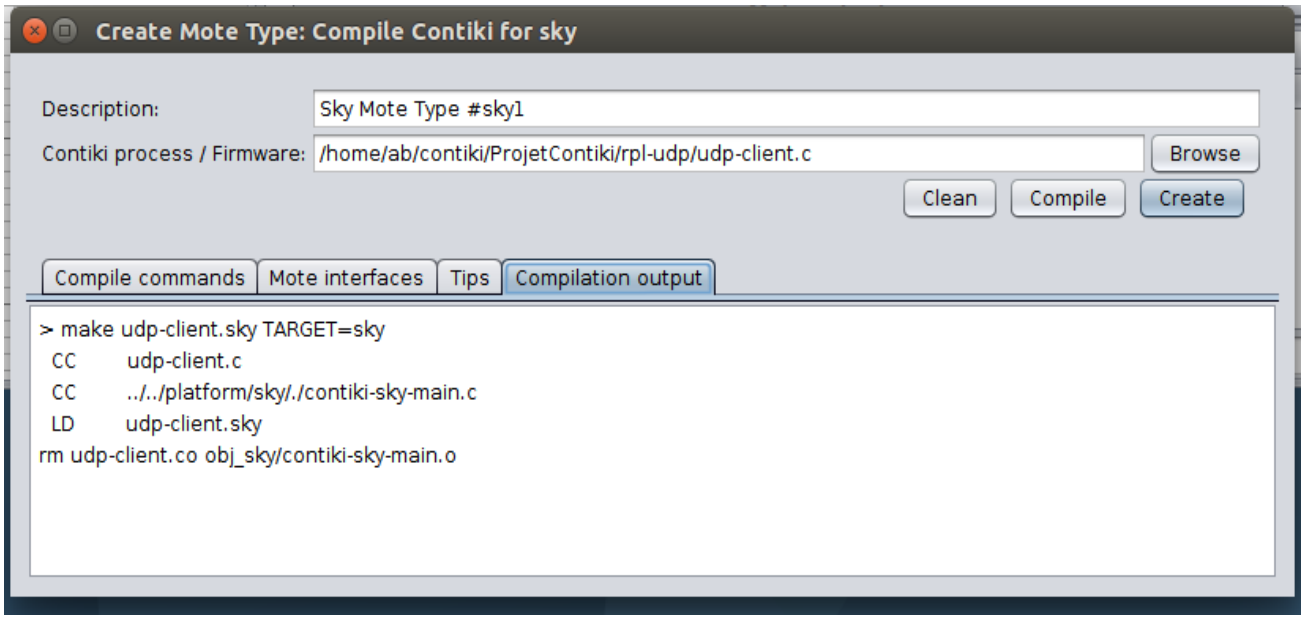


Figure III.3 chargement du programme au capteur

Enfin lancer la simulation avec start.

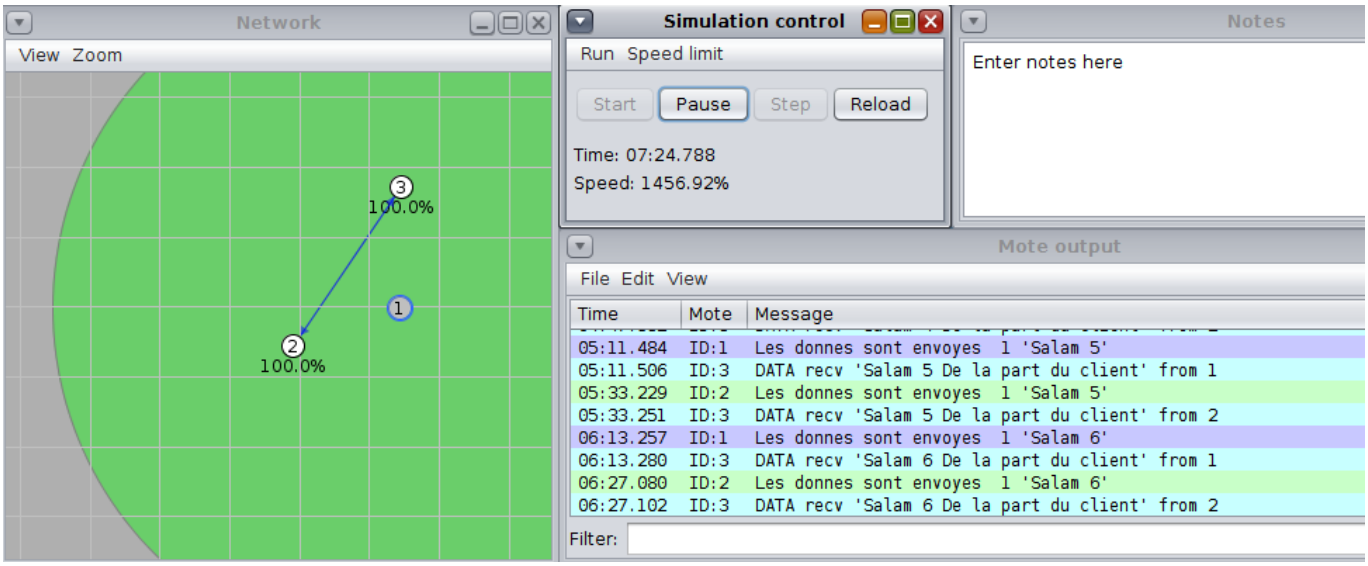


Figure III.4lancement de la simulation

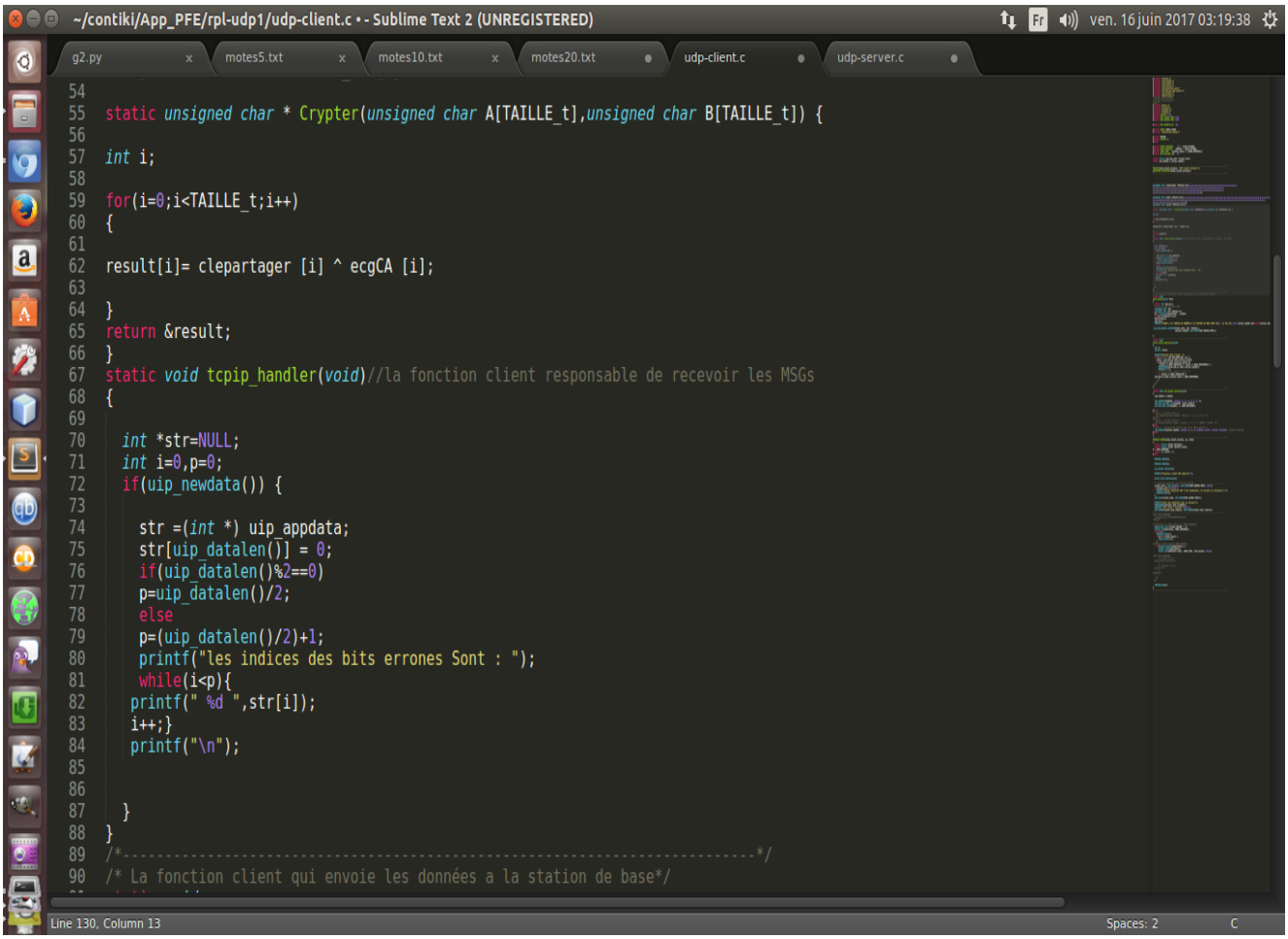
II.4-Implémentation et Evaluation de notre protocole de gestion de clés :

Cette partie décrit l'implémentation et l'évaluation de notre protocole de gestion de clés dans les réseaux de capteurs corporels sans fil.

III.4.1 –La partie du code :

Le code de notre protocole comprend deux parties, une partie concerne les capteurs clients et l'autre partie concerne la station de base.

III.4.1.1- Partie client : la parie du code qui est implémenter coté client pour pouvoir se connecter a la station de base.



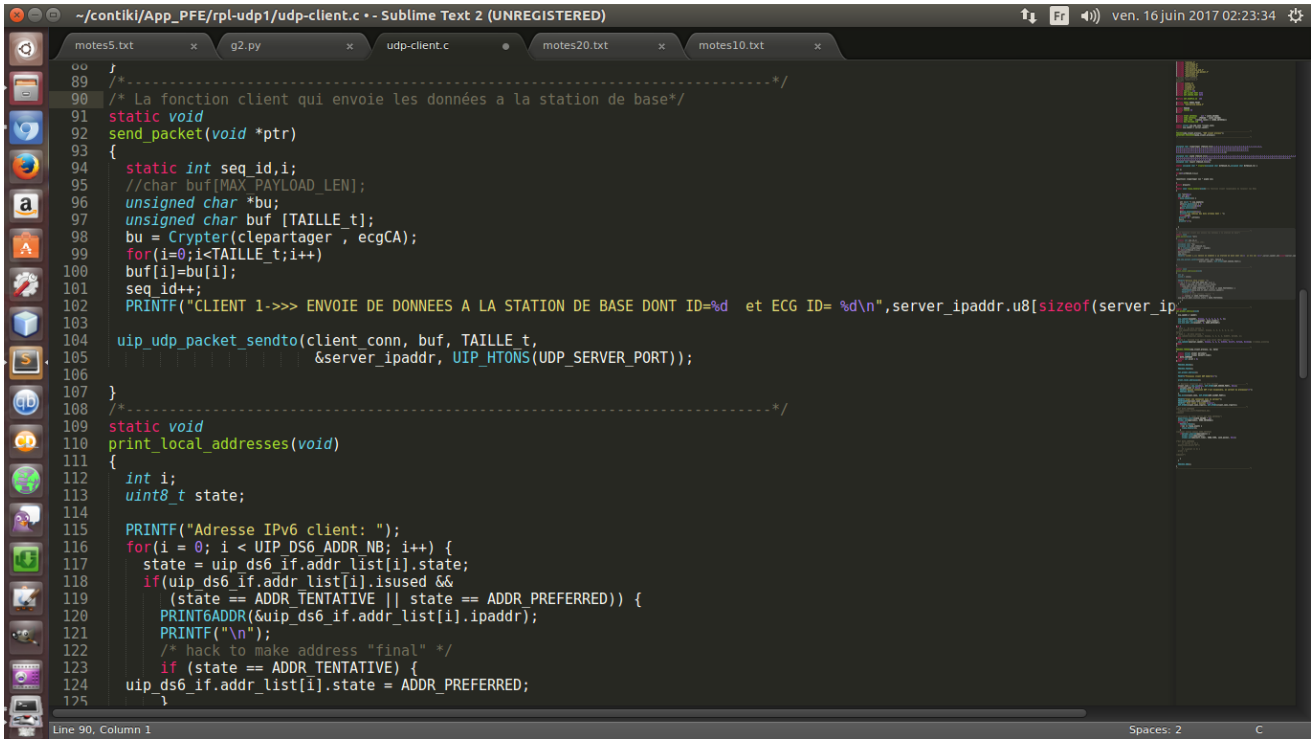
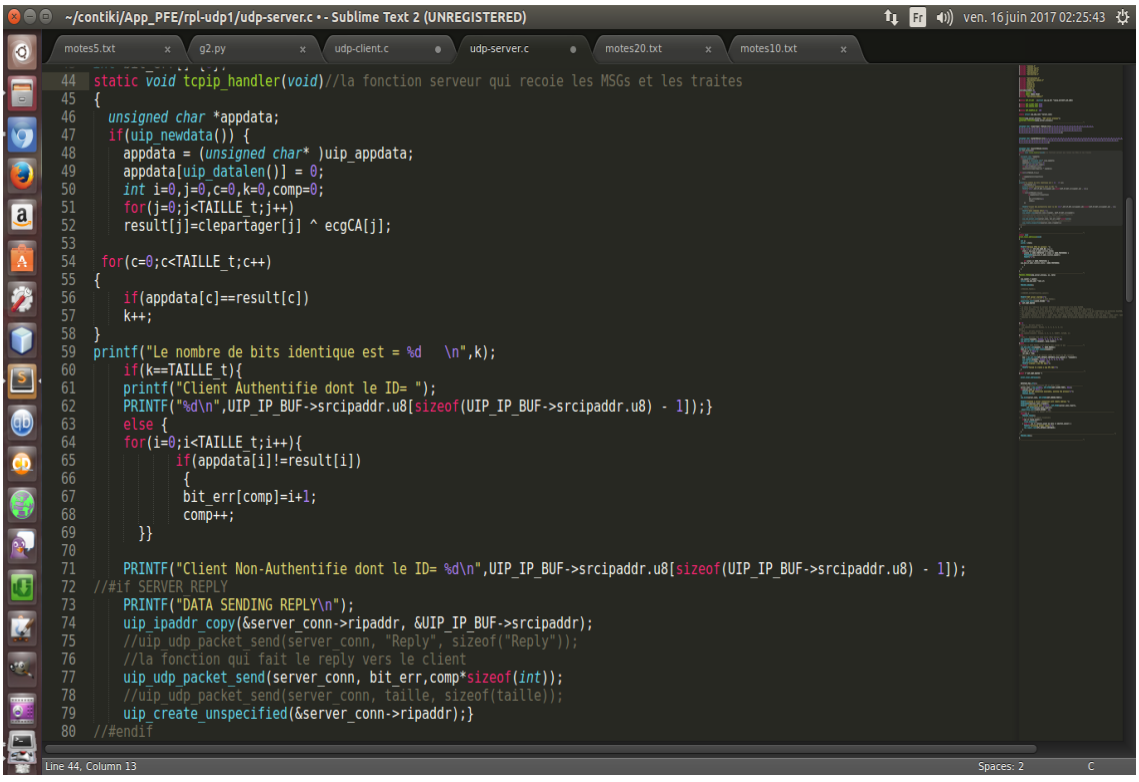


Figure III.5- Partie client

III.4.1.2- Partie station de base :



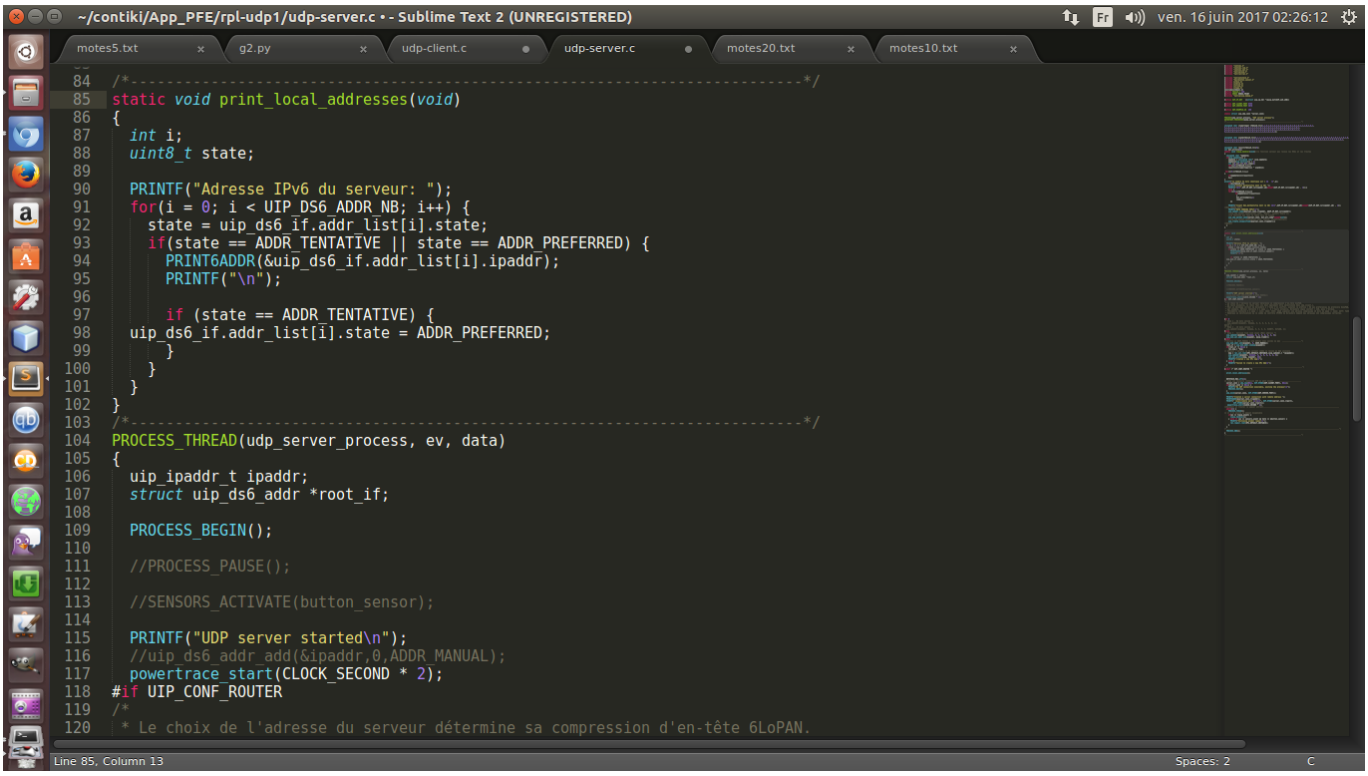


Figure III.6- Partie Station de base

III.5 –Evaluation de notre protocole de gestion de clés :

Dans cette partie nous allons évaluer les performances de notre protocole en termes d'énergie consommée. Pour ce faire, nous avons implémenté notre protocole sur six nœuds (cinq capteurs client et la station de base) puis onze nœuds ensuite vingt nœuds en relançant pour chaque scenario pour une durée d'une minute.

La figure suivante montre les différentes étapes de notre protocole(authentification et les messages échangés entre le nœud capteur) (client) et la station de base.

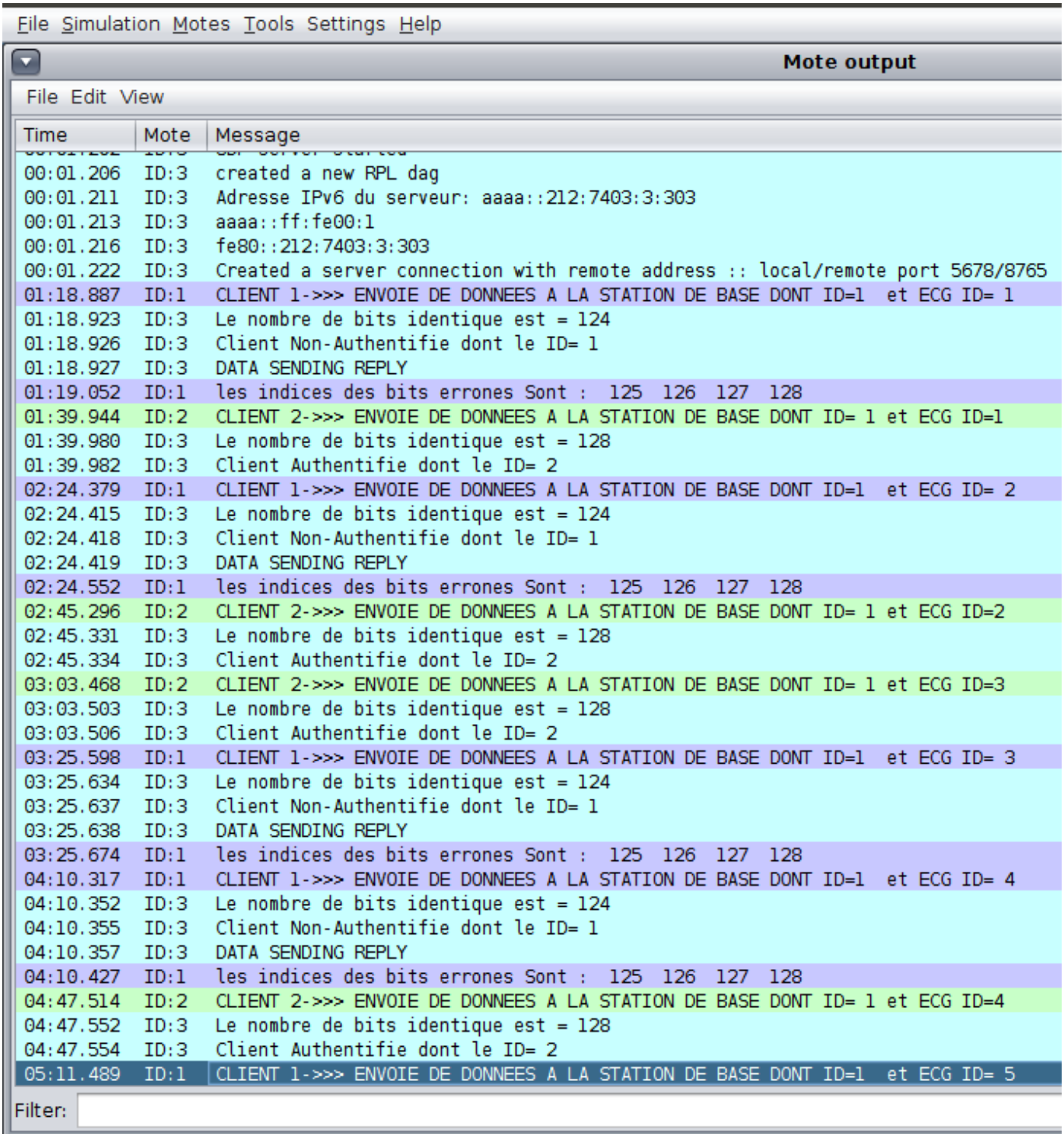


Figure III.7- Simulation du protocole sous cooja.

III.5.1- La Consommation d'énergie :

PowerTrace pour calculer l'énergie consommée par les capteurs et la station de base et nous avons utilisé également un script Python pour tracer et visualiser l'énergie consommée a partir de données récolter sous cooja et enregistrer dans un fichier texte.

***1*-sudo apt-get install python-matplotlib** *//installation de matplot*

***2*-**ajouter la ligne suivante **_start(CLOCK_SECOND * 2);** juste après le **PROCESS_BEGIN ( )**

***3*-** ajouter la ligne suivante **#include "powertrace.h"** *//pour pouvoir utiliser Powertrace*

***4*-APPS+=powertrace** *//à ajouter dans le fichier Makefile pour la compilation*

5*-lancer la simulation sous cooja puis enregistré la sortie dans un fichier texte.*

6*-exécuter le script python pour avoir les graphes.*

```
1 00:02.722       ID:1     263 P 0.18 0 6707 60248 2611 456 0 378 6707 60248 2611 456 0 378
  (radio 4.58% / 4.58% tx 3.89% / 3.89% listen 0.68% / 0.68%)
2 00:04.722       ID:1     519 P 0.18 1 8610 123861 2611 1097 0 783 1900 63613 0 641 0 405
  (radio 2.79% / 0.97% tx 1.97% / 0.00% listen 0.82% / 0.97%)
3 00:06.724       ID:1     775 P 0.18 2 15475 182494 5687 1727 0 1188 6862 58633 3076 630 0 405
  (radio 3.74% / 5.65% tx 2.87% / 4.69% listen 0.87% / 0.96%)
4 00:08.723       ID:1     1031 P 0.18 3 17158 246304 5687 2159 0 1620 1680 63810 0 432 0 432
  (radio 2.97% / 0.65% tx 2.15% / 0.00% listen 0.81% / 0.65%)
5 00:10.723       ID:1     1287 P 0.18 4 18763 310190 5687 2591 0 2052 1602 63886 0 432 0 432
  (radio 2.51% / 0.65% tx 1.72% / 0.00% listen 0.78% / 0.65%)
6 00:12.723       ID:1     1543 P 0.18 5 20717 373746 5687 3265 0 2680 1951 63556 0 674 0 628
  (radio 2.26% / 1.02% tx 1.44% / 0.00% listen 0.82% / 1.02%)
7 00:14.724       ID:1     1799 P 0.18 6 26985 432988 8680 3749 0 3085 6265 59242 2993 484 0 405
  (radio 2.70% / 5.30% tx 1.88% / 4.56% listen 0.81% / 0.73%)
8 00:16.723       ID:1     2055 P 0.18 7 28717 496764 8680 4181 0 3517 1729 63776 0 432 0 432
  (radio 2.44% / 0.65% tx 1.65% / 0.00% listen 0.79% / 0.65%)
```

Figure III.8- Le contenu du fichier texte pour tracer les courbes.

```
#!/usr/bin/python
#!/usr/bin/env python

import csv
import matplotlib.pyplot as plt

# for P lines
#0-> str,
#1 -> clock_time(),2-> P, 3->rimeaddr_node_addr.u8[0],rimeaddr_node_addr.u8[1], 4-> seqno,
#5 -> all_cpu,6-> all_lpm,7-> all_transmit,8-> all_listen,9-> all_idle_transmit,10-> all_idle_listen,
#11->cpu,12-> lpm,13-> transmit,14-> listen, 15 ->idle_transmit, 16 -> idle_listen, [RADIO STATISTICS...]


from collections import defaultdict
cpuOverTime =  defaultdict(list)

with open('listener2.txt', 'rb') as f:
    reader = csv.reader(f,delimiter=' ')
    for row in reader:
        if row[2] is 'P':
            cpuOverTime[row[3]].append(row[11])

for i in cpuOverTime:
    plt.plot(cpuOverTime[i])
plt.show()
##########
```

Figure III.9- Le script python.

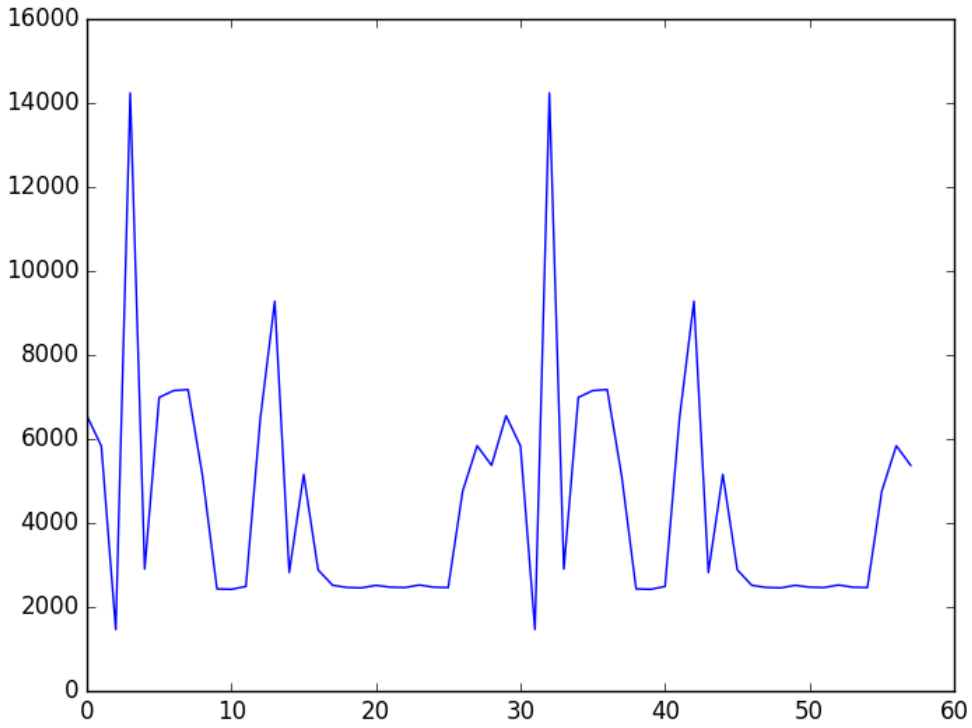


Figure III.10- Energie consommée par CPU pour la station de base avec cinqclients.

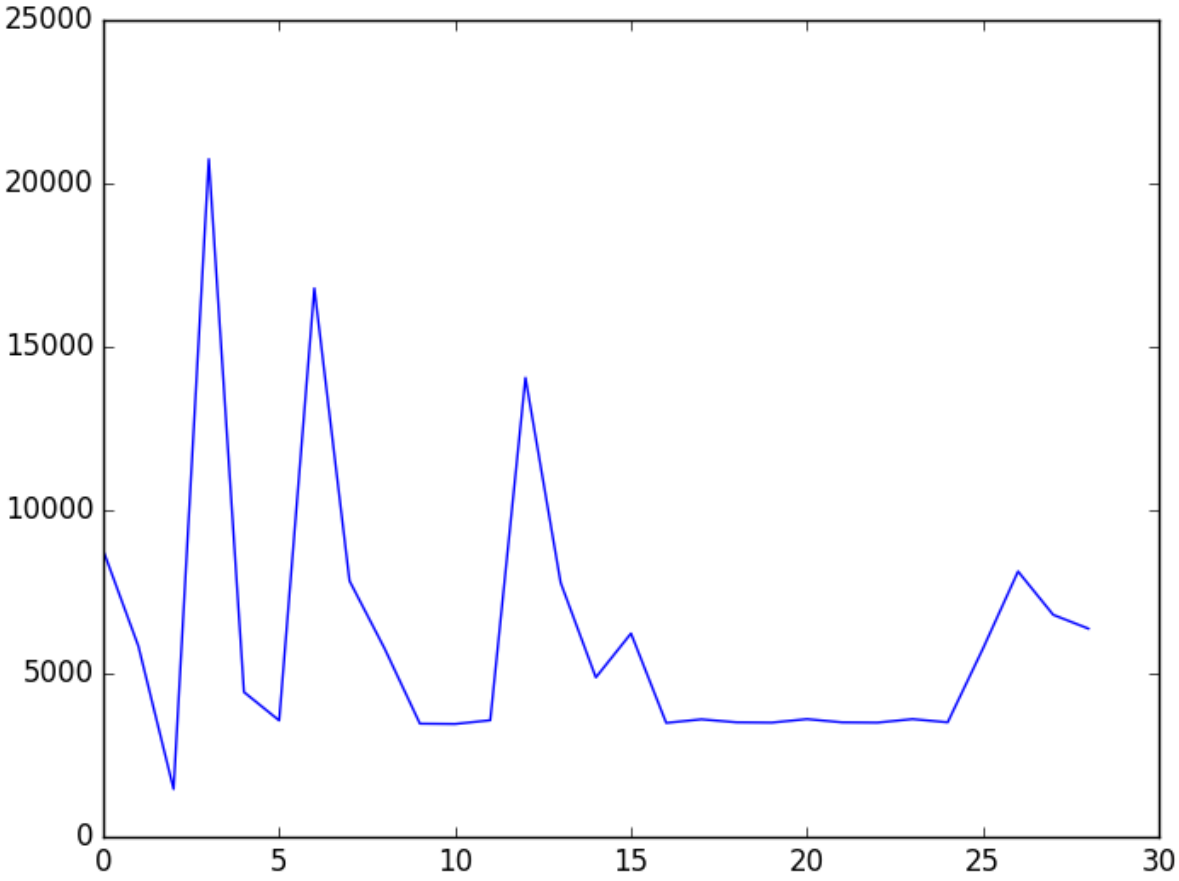


Figure III.11- Energie consommée par CPU pour la station de base avec dix clients.

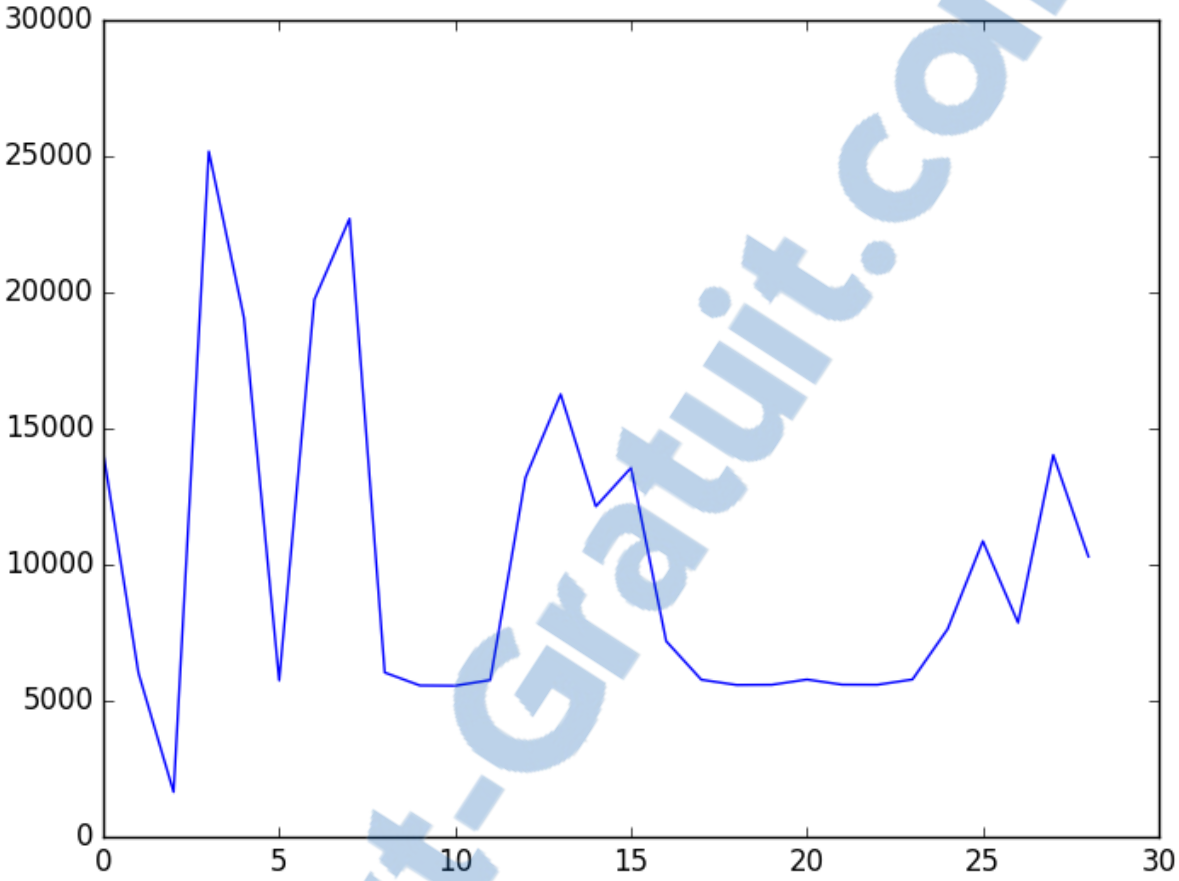


Figure III.12- Energie consommée par CPU pour la station de base avec vingt clients.

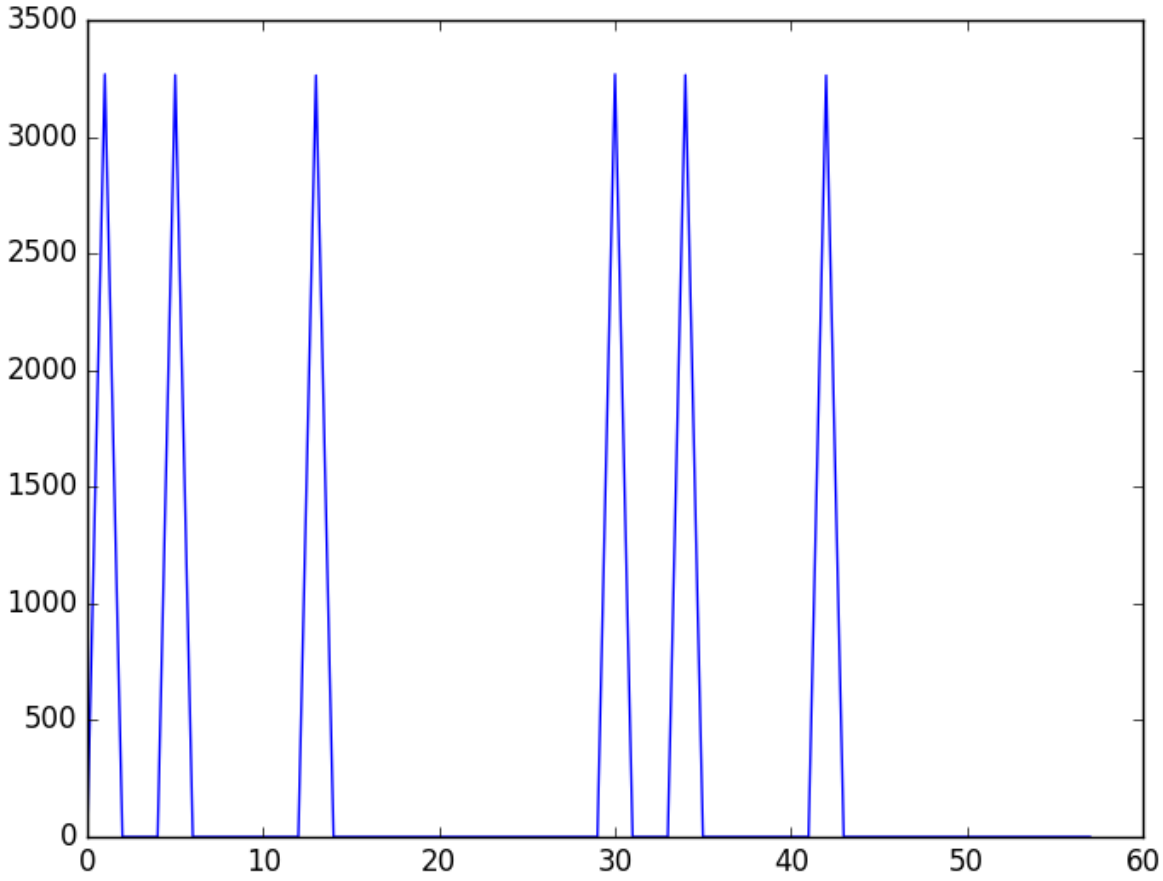


Figure III.13- Energie consommée pour la transmission pour cinq clients.

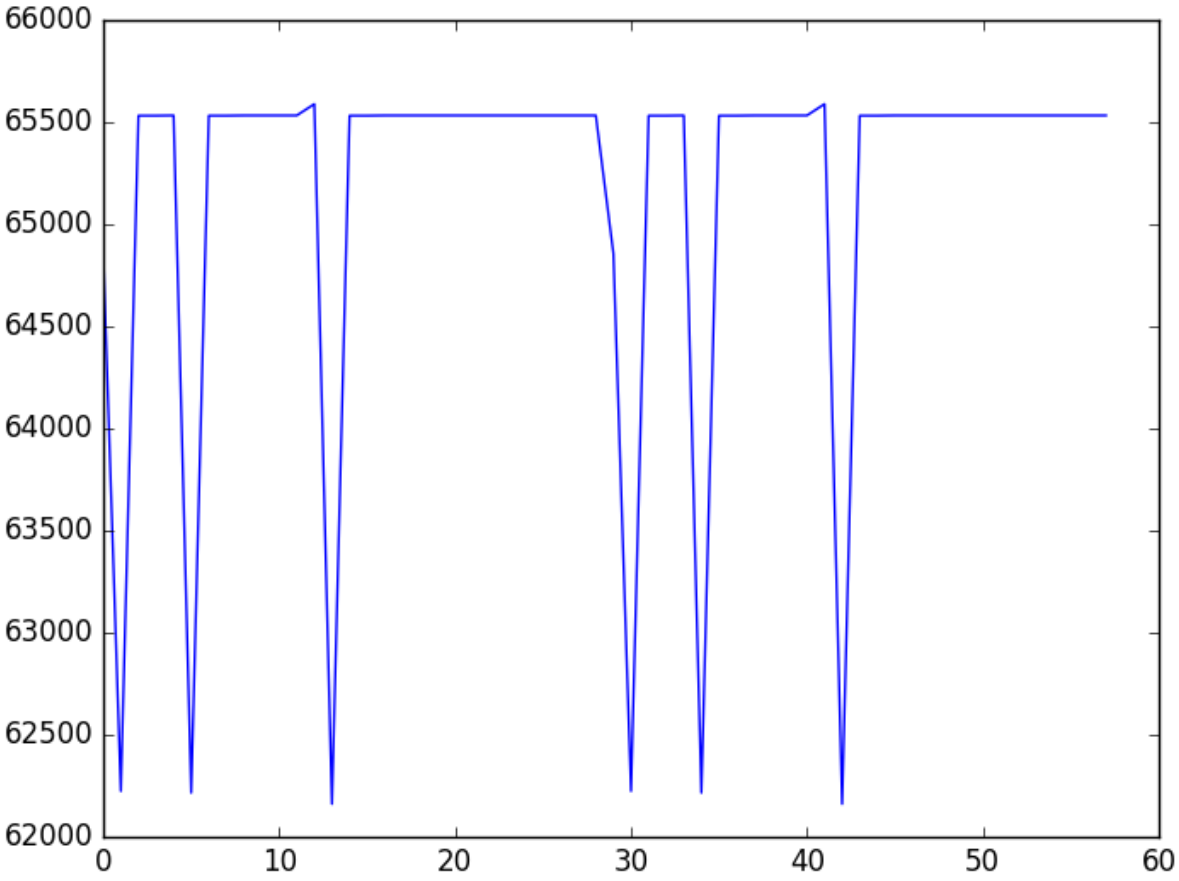


Figure III.14- Energie consommée pour la réception pour cinq clients.

III.6 – Conclusion :

Dans ce chapitre nous avons décrit l'implémentation et la simulation de notre protocole de gestion de clés dans les réseaux de capteurs corporels sans fil sous Contiki-Cooja.

L'avantage de notre protocole consiste à l'utilisation de la cryptographie symétrique pour la gestion de clés ce qui permet de minimiser la consommation d'énergie et par conséquent augmenter considérablement la durée de vie du réseau de capteurs corporels.

Conclusion générale

Dans ce mémoire, nous avons mis en avant le besoin et la nécessité de la sécurité dans les réseaux de capteurs corporels sans fil. Nous avons présenté les réseaux de capteurs sans fils médicaux. Après une introduction générale sur les réseaux de capteurs sans fil médicaux, nous avons parlé des systèmes WBAN où nous avons fait une comparaison entre les réseaux WBAN et RCSF.

Dans le deuxième chapitre, nous avons abordé la gestion de clés dans les réseaux de capteurs corporels. En effet, la gestion de clés constitue un service très important pour la sécurité de n'importe quel système de communication. Les mécanismes traditionnels de gestion de clés sont inappropriés pour les réseaux de capteurs corporels car ces derniers sont limités en termes de capacité de calcul, de stockage et d'énergie. Pour cela, nous avons développé un protocole de gestion de clés cryptographiques pour les réseaux WBANs en prenant en compte la contrainte d'énergie pour garantir une plus longue durée de vie du réseau.

Dans le troisième et dernier chapitre, nous avons mis l'accent sur l'implémentation et la simulation de notre protocole de gestion de clés dans les réseaux de capteurs corporels. L'implémentation et la simulation ont été réalisées sous Contiki Cooja.

Enfin la sécurité des données transmis dans un WbAN est une phase phare qui nécessite une recherche approfondie en ce qui concerne l'élaboration de nouveaux protocoles de sécurité.

Références bibliographiques

[1]M. Badet, W. Bonneau. " Mise en place d'une plateforme de test et d'expérimentation", Projet de Master Technologie de l'Internet 1ere année, Université Pau et des pays de l'Adour. 2006.

[3]Mohamed Hamdi, Noureddine Boudriga, and Mohammad S. Obaidat.Whomoves : An optimized broadband sensor network for military vehicletracking. Int. J. Communication Systems, 21(3) :277–300, 2008.

[4]Tibor Istv´an Nagy and J´ozsef Tick. Intelligent sensor networks in the militaryand civil sectors. In 5th International Symposium on Applied Computational Intelligence and Informatics, SACI 2009, Timisoara, Romania,May 28-29, 2009, pages 471–474. IEEE, 2009.

[5] David M. Davenport, Budhaditya Deb, and Fergus J. Ross. Wireless propagation and coexistence of medical body sensor networks for ambulatorypatient monitoring. In Sixth International Workshop on Wearable and ImplantableBody Sensor Networks, BSN 2009, Berkeley, CA, USA, 3-5 June2009, pages 41–45. IEEE Computer Society, 2009.

[6] Mehmet R. Yuce, Peng Choong Ng, and Jamil Y. Khan. Monitoring of physiological parameters from multiple patients using wireless sensor network.J. Medical Systems, 32(5) :433–441, 2008.

[7] Fran¸cois Ingelrest, Guillermo Barrenetxea, Gunnar Schaefer, Martin Vetterli,Olivier Couach, and Marc Parlange. Sensorscope : Application-specific sensor network for environmental monitoring. ACM Transactions On SensorNetworking, 6(2) :1–32, 2010.

[8] Vassileios Tsetsos, George Alyfantis, Tilemahos Hasiotis, Odysseas Sekkas,and Stathes Hadjiefthymiades. Commercial wireless sensor networks : Technicaland business issues. In 2nd International Conference on Wireless onDemand Network Systems and Service (WONS 2005), 19-21 January 2005,St. Moritz, Switzerland, pages 166–173. IEEE Computer Society, 2005.

[11]M.O. Farooq and T. Kunz, "Operating systems for wireless sensor networks: A Survey", Sensors, Volume 11, (Issue 6), pages: 5900–5930, 2011.

[12]A. Dunkels, B. Gronvall and T. Voigt, "Contiki - a light weight and flexible operating system for tiny networked sensors", IEEE 29th International Conference on Local Computer Networks, pages: 455-462, November 2004.

[13]S. Bhatti, J. Carlson, H. Dai, J. Deng, J. Rose, A. Sheth, B. Shucker, C. Gruenwald, A. Torgerson, and R. Han, "Mantis OS: An embedded multithreaded operating system for wireless micro sensor platforms", Mobile Networks and Applications Journal, Volume 10 (Issue 4), pages: 563-579, 2005

[14]P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, and D. Culler, "TinyOS: An Operating System for Sensor Networks", Book: Ambient Intelligence, Chapter 7, pages:115-148, 2005.

[15]Mark A. Hanson, Harry C. Powell Jr., Adam T. Barth, Kyle Ringgenberg, Benton H. Calhoun, James H. Aylor, John Lach, "Body Area Sensor Networks:Challenges and Opportunities", IEEE Computer, Volume 42, Issue: 1, pages: 58-65, January 2009.

GYzZi1iYzdhLTllYWUwNzkzYmZkZg.png

[18]Thèse r Ali MAKKE pour obtenir le grade de docteur de l'Université Paris Descartes Spécialité: Informatique et Réseaux Détection d'attaques dans un système WBAN de surveillance médicale à distance

[10]https://fr.slideshare.net/MilagrosRomanEngjrMA/presentationRCSF

[16] http://www.memoireonline.com/02/12/5433/tat-de-lart-sur-les-reseaux-de-capteurs-sans-fil35.png

[17]https://media.licdn.com/mpr/mpr/AAEAAQAAAAAAAAkWAAAAJDk1YTkxMGJjLWFhMzAtN

[20]http://igm.univ-mlv.fr/~dr/XPOSE2007/vma_PKI/images/clef_symetrique.jpg

[21]http://www.flatland.tuxfamily.org/images/schemas/schema_chiffrementasymetrique.png

[23]https://fr.wikipedia.org/wiki/Fonction_de_hachage#/media/File:Hash_function_fr.svg

[2]https://fr.slideshare.net/achrefbenhelel/rseau-de-capteurs-sans-fils-RCSF

[9]https://fr.wikipedia.org/wiki/R%C3%A9seau_de_capteurs_sans_fil#Architecture_d.27un_microcapteur

[Listes Des Figures]

Liste Des Figures

Liste Des Tableaux

Liste Des Abréviations

RCSF:Réseaux de capteurs sans fil

RCSF:Wireless Sensor Network

MANET:Mobile Ad hoc NETworks

GPS:Global Positioning System

UWB : Ultra Wide Band

WBAN:Wireless Body Area Networks

XOR : OU exclusif

Résumé

Les réseaux de capteurs corporels sans fil ont attiré un grand intérêt dans la dernière décennie, et ont amélioré grandement la qualité de soins médicaux. Mais le problème majeur consiste à sécuriser la communication entre les nœuds via de robuste et de nouveau protocoles tout en tenant compte de l'utilisation de la CPU et l'économie d'énergie.

Mots-clefs : WBANs, Sécurité, Gestion de clés.

Abstract

Wireless body sensor networks have attracted great interest in the last decade, and have greatly improved the quality of medical care. The more important hardware is to secure communication between the nodes via the robust protocols and again while taking into account CPU usage and energy saving.

Keywords: WBAN, Security, Key management.

ملخص

جذبت شبكات الاستشعار اللاسلكية الجسم اهتماما كبيرا في العقد الأخير، وتحسنت بشكل كبير على نوعية الرعاية الطبية. معظم المعدات الرئيسية هي تأمين الاتصالات بين العقد عبر بروتوكولات قوية وجديدة مع الأخذ بعين الاعتبار استخدام وحدة المعالجة المركزية وتوفير الطاقة.

كلمات البحث: الأمن الشبكات اللاسلكية الشخصية