Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira-Bejaïa
Faculté de Sciences Exactes
Département Informatique

Spécialité : administration et sécurité des réseaux

En vu d'obtention du diplôme master professionnel en informatique

Thème :

La surveillance des patients via des réseaux mobiles

Encadré par :
Mlle BATAT Nadia
Président de jury :
Mme ALOUI Soraya
Jury :
Mr IKHLEF A-el moumen
Mlle HOUHA Amel

Réalisé par :
HADDAD A.raouf
KORICHI Amer

Année universitaire : 2016 - 2017

Remerciments

Nous tenons à remercier tous d'abord DIEU, le tous puissant de nous avoir accordé la volonté, force, santé, détermination et courage afin d'accomplir ce modeste travail.

Ces quelques lignes ne pourront jamais exprimer la reconnaissance que nous éprouvons envers tous ceux qui, de prés ou de loin, ont contribué par leurs conseils et leurs encouragements à l'aboutissement de ce travail.

Nous remercions notre maitre de mémoire, Mlle BATTAT Nadia, de nous avoir accompagnés dans la réalisation de ce modeste travail. Elle a toujours su être de bons conseils pour la création de l'application, la rédaction du mémoire et sa présentation.

Également, nous remercions tous nos professeurs qui ont souvent cru en nous et qui nous ont guidés et encouragés à persévérer dans nos travaux de recherches toujours au bon moment.

Nous remercions chaleureusement les membres de jury qui nous ont honorés de leurs présences et d'avoir accepter d'évaluer ce mémoire à sa juste valeur.

Nous ne saurions oublier de remercier toutes les personnes ayant contribué de près ou de loin à l'aboutissement de ce travail.

Pour fi nos derniers mots de remerciements vont tout naturellement à nos familles pour leurs soutiens, à nos amis.

Dédicaces

Merci (mon dieu) de m'avoir donné la capacité d'écrire et de réfléchir.

Nous dédions ce modeste travail à :

A nos très chers parents,

A nos sœurs et nos frères

A tous nos chères amis et leurs familles.

A tous ceux qui me connaissent.

Amer & ***Raouf***

Table des matières

Table des figures

Liste des tableaux

Introduction générale

Récemment, les avancements dans les réseaux de capteurs sans fi ont permis de supporter un large gamme d'applications, y compris médical et systèmes des soins médicaux. Un réseau sans fi sur le corps humain (WBAN) est un réseau de capteurs particulier conçu pour opérer d'une manière autonome pour relier les capteurs médicaux et les appareils localisé à l'intérieur et à l'extérieur du corps humain et sont utilisés pour la surveillance des patients à long terme diriger dans un hôpital ou de façon distante. Un WBAN est constitué de capteurs biomédicaux utilisés pour surveiller les données physiologiques, tel que température, tension, électrocardiogramme (ECG), taux du cœur, etc.

Les systèmes WBAN de surveillance médicale à distance sont vulnérables à différents types d'attaques et d'anomalies. Parmi ces attaques et anomalies, il y en a ceux qui visent la disponibilité et l'intégrité du système et donc qui peuvent avoir d'une façon indirecte une infl très dangereuse sur la qualité de soin et sur la vie des patients et d'autres qui visent la confidentialité du système et donc peuvent avoir une infl ence sur la confidentialité des données médicales.

Les réseaux de capteurs médicaux sans fi soulèvent de nouveaux défis technologiques en termes de sécurité et de protection contre les anomalies et les attaques. Le mode de communication sans fi utilisé entre ces capteurs et l'unité de traitement accentue ces vulnérabilités.

Dans notre travail nous nous sommes intéressé à type particulier d'attaque qui est l'attaque de l'homme au milieu dans les réseaux de capteurs sans fi

Chapitre 1

La surveillance des patients

Introduction

Au cours des dernières décennies et grâce à l'avancée des systèmes embarqués et des technologies sans fi les Réseaux de Capteurs Sans Fil (RCSF), ou " Wireless Sensor Network (WSN) ", sont de plus en plus utilisés dans de nombreux domaines. Parmi ces domaines, nous nous intéressons aux RCSF pour les applications médicales.
Dans ce chapitre nous allons donner un aperçu sur les Réseaux de Capteurs Sans Fil (RCSF) ainsi quelque systèmes WBAN et leurs caractéristiques.

Les réseaux sans fils

Les réseaux sans fi sont divisés en trois grandes familles [10] :

LAN :

Local Area Network ou réseau local. Ce type de réseau s'étend de 1 mètre à 2 kilomètres et peut compter de 2 à 200 abonnés. Le débit courant est de 1 à 100 Mbits/s.

MAN :

Métropolitain Area Network ou réseau métropolitain. Ce type de réseau s'étend de 1 mètre à 100 kilomètres et peut compter de 2 à 1000 abonnés. Le débit courant est de 1 à 100 Mbits/s.

WAN :

Wide Area Network ou réseau grande distance. Ce type de réseau s'étend sur plus de 1000 kilomètres et peut compter plusieurs milliers d'abonnés. Le débit, étant donné la distance à parcourir, est plus faible, de 50 bits/s à 2 Mbits/s. Les deux premiers types de réseaux utilisent des connexions multipoints tandis que le WAN utilise des connexions point à point. Par exemple, le réseau Transpac, réseau français est constitué de liaisons point à point entre des nœuds situés dans les grandes villes françaises.

Les réseaux de capteurs sans fil

Un réseau de capteurs est constitué de milliers de nœuds appelés nœuds capteurs ou tout simplement capteurs, permettant de capter et collecter des informations, d'analyser les traitements et de transmettre les informations recueillies dans différents environnements. Ces nœuds peuvent avoir des positions particulières ou bien être déployés aléatoirement pour surveiller l'environnement. Les communications dans un réseau de capteurs se font souvent d'une manière multi-saut.

L'écoulement des données se termine vers des nœuds spéciaux appelés nœuds-puits ou stations de base (" sink "). Ces nœuds-puits sont des bases de contrôle qui possèdent plus de ressources matérielles et permettent de collecter et stocker les informations issues des capteurs.

En d'autres termes le fonctionnement d'un réseau de capteurs se déroule de la manière suivante : les nœuds sont déployés dans une zone appelée zone d'intérêt pour la surveiller. Lorsqu'un nœud détecte un évènement, il le traite localement et l'achemine vers la station de base via une communication multi-saut. Ce processus est illustré dans la Figure 1.1.[1]

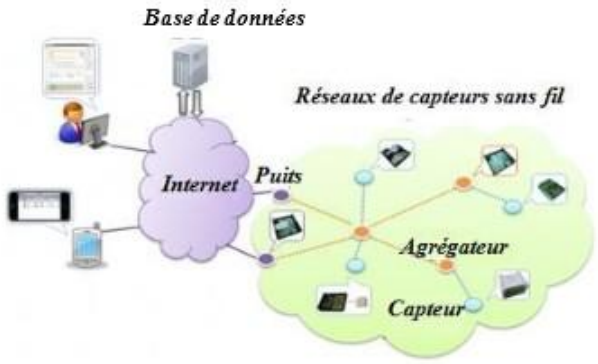

Figure 1.1 – Exemple d'un réseau de capteurs[1]

Caractéristiques des RCSF

Les caractéristiques les plus remarquables des RCSF, sont les suivantes :

- Absence d'infrastructure, ce sont des réseaux Ad-hoc ;
- Facteur d'échelle - Le nombre de nœuds déployés pour une application peut atteindre des milliers ;
- Interférences si deux nœuds proches émettent simultanément ;
- Topologie dynamique, due à la défaillance de nœud ou à l'ajout de nouveaux nœuds au réseau déjà déployé ou à la mobilité de nœud(s). Les capteurs peuvent également être attachés à des objets mobiles qui se déplacent d'une façon libre et arbitraire rendant ainsi la topologie du réseau fréquemment changeante.
- Sécurité physique limitée - les réseaux de capteurs sans fi sont plus touchés par le paramètre de sécurité que les réseaux fi classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.
- Bande passante assez faible ;
- Contrainte de ressources : énergie, de stockage et de calcul - la caractéristique la plus critique dans les réseaux de capteurs est la modestie de ses ressources énergétiques, car chaque nœud est autonome et alimenté par une batterie.[1]

Domaines d'application :

- applications militaires.
- Surveillance de l'environnement.
- La surveillance des écosystèmes.
- Contrôle du climat local des grands bâtiments.
- La prévention des catastrophes et les secours.[1]

Les réseaux de capteurs médicaux sans fil

Wireless Body Area Networks (WBAN)

Un réseau de capteurs corporels sans fi 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 fi - 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 WSNs.[2]

Avantages

- La surveillance à distance
- La surveillance en temps réel
- Les soins à long termes
- La liberté du mouvement pour le patient
- La surveillance permanente de l'état physiologique
- La surveillance permanente des organes vitaux du patient[2]

Comparaison entre les réseaux WBAN et les réseaux WSN

Wireless Sensors Networks (WSN) :

Un réseau de capteurs sans fi 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.[2] Différence entre WBAN et WSN Nous présentons ici les différences entre WBAN et WSN qui sont classifiées selon plusieurs facteurs. Le Tableau 1 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

Table 1.1 – Différences entre WBAN et WSN[2]

Architecture des réseaux WBAN

La Figure 1.2 l'architecture d'un WBAN

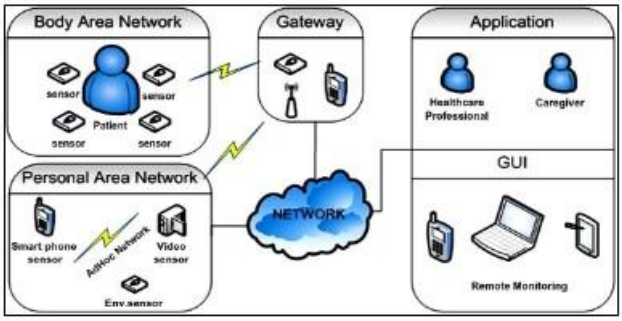

Figure 1.2 – Architecture d'un WBAN[2]

Topologies des réseaux WBAN

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.

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.

Topologie 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 32 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 topolo-

gie maillée est une considération primordiale dans toutes les situations dans lesquelles la fi é et la communication fl sont prioritaires par rapport à l'effi é énergétique et la durée de vie du réseau.

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 fi 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.[2]

Le Tableau 1.2 résume les avantages et les inconvénients de chacune des topologies décrites ci-dessus.

Topologie	**Avantages**	**Inconvénients**
Point-à-point	-Simplicité -Faible latence -Débit élev	-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

Table 1.2 – Les avantages et les inconvénients des topologies dans les réseaux WBAN[2]

Les signaux vitaux

Parmi les signaux vitaux les plus fréquemment collectes on peut souligner :

- La pression artérielle, avec une fréquence d'echantillonnage de plusieurs fois par

jour. Normalement elle est représentée par un intervalle de valeurs avec des valeurs différentes selon qui s'il s'agit de la pression systolique ou de la pression diastolique.

- Le pouls est représenté par une valeur entre 0 et 220.
- La fréquence respiratoire.
- La température est une valeur en degrés Celsius (ou Fahrenheit). Cependant, la valeur de la température peut changer selon l'endroit ou la partie du corps utilisée pour prendre l'´echantillon. Notons que la température moyenne a des petites variations selon l'endroit de mesure et l'âge du patient. Une prise de température a besoin d'un calibrage pour déterminer les valeurs normales.
- Le pouls, la fréquence respiratoire, et la température peuvent être pris avec des fréquences d'´echantillonnage variables en fonction des besoins (mesures toutes les deux, quatre, ou six heures.[2]

1.4.1.5.1 Les nœuds capteurs :

Définition d'un capteur médical

Un capteur est un dispositif ayant pour tâche de transformer une mesure physique observée en une mesure généralement électrique qui sera à son tour traduite en une donnée binaire exploitable et compréhensible pour un système d'information. Un capteur médical se constitue d'un capteur équipé d'un circuit électronique spécifique capable de mesurer un ou plusieurs paramètres physiologiques. Donc : capteur + circuit électronique spécifique = capteur médical.[2]

Les types des capteurs médicaux

Dans ce qui suit , nous décrivons plusieurs types de capteurs médicaux utilisés dans la médecine et qui sont disponibles dans le commerce .Des exemples de ces capteurs médicaux avec leurs exigences en termes de débit (montrant l'impact sur leur consommation d'énergie) sont présentés dans la Figure 1.3.

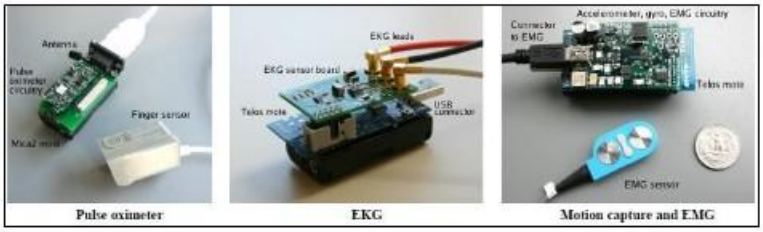

Figure 1.3 – :Exemples de capteurs médicaux[2]

Dans le tableau 1.3 nous allons trouver les différents types capteurs ainsi leurs fonctionnalités.

Nom du Capteur médical	Fonction
Accéléromètre et Gyroscope	surveillent la posture du corps et ses mouvements physiques.
Capteur de Glycémie	mesure la concentration de glucose dans le sang.
Capteur de tension artérielle	mesure la pression systolique et diastolique du sang humain.
Détecteur de gaz CO2	mesure le niveau de dioxyde de carbone pour surveiller la concentration d'oxygène lors de la respiration humaine.
Capteur ECG	mesure les signaux électriques produits par le cœur et permet d'évaluer l'activité cardiaque.
Capteur EEG	mesure l'activité électrique du cerveau.
Capteur EMG	mesure les signaux électriques produits par les muscles.
Capteur Oxymétrie de pouls (SpO2)	mesure la saturation en oxygène de l'hémoglobine.
Capteur de température	mesure la température du corps humain et/ou de l'environnement entourant le patient.
Capteur d'humidité	mesure l'humidité de l'environnement entourant le patient.

Table 1.3 – tableau récapitulatif sur les capteurs ainsi leurs fonctions.[2]

Architecture de communication dans les systèmes WBAN

les communications dans un système BAN se décomposent en trois composantes Communications ”Intra-BAN”, Communications ”Inter-BAN” et Communications ” Au-delà de BAN”.

Communications "Intra-BAN" :

Concerne les communications qui se déroulent autour du corps humain. Ce type de communications se compose des communications entre les différents capteurs corporels ainsi des communications entre les capteurs corporels et le nœud de collecte. Ce dernier peut être un dispositif caractérisé par une puissance de calcul et une réserve d'énergie plus importante par rapport aux capteurs corporels.[2]

Communications "Inter-BAN" :

Ce type se compose des communications entre le nœud de collecte et un ou plusieurs points d'accès. Les points d'accès peuvent être déployés dans le cadre de l'infrastructure, ou être placés stratégiquement dans un environnement dynamique pour gérer les situations d'urgence.[2]

Communications " Au-delà de BAN" :

Ce type se compose des communications entre le point d'accès et l'équipe médicale localisée par exemple dans un hôpital et cela via le réseau Internet ou un réseau cellulaire. Les communications " Au delà de BAN " peuvent améliorer l'application de la surveillance médicale en permettant aux personnels de la santé (médecins et infi ères) d'accéder à distance aux informations médicales des patients et d'intervenir dans les cas d'urgences.[2]

Les différentes technologies de communication sans fil

Le médium utilisé par les réseaux de capteurs sans fi 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 :

La norme IEEE 802.15.1 / Bluetooth :

Initialement, la norme Bluetooth a été proposée pour transmettre la voix et les données. 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).[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. 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 10La 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'off 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. , 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).[2]

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 fi . 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 IEEE 802.15.4 qui définit sa couche PHY et MAC et qui permet de prolonger théoriquement la

durée de vie d'un nœud sur plusieurs années. L'autre point fort de ce protocole est qu'il propose le 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.[2]

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 fi é, 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) . 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.[2]

La norme IEEE 802.11x/WiFi :

Le protocole de communication WiFi est le protocole le plus utilisé pour toutes les applications sans fi Il offre une large bande passante (de 11 à 320 Mbits/s) ce qui a permis de démocratiser l'utilisation de la technologie 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 fi du fait d'un besoin énergétique trop important pour son utilisation. La durée de vie des capteurs sans fi alimentés par des piles ne dépasse que rarement quelques heures. C'est

pourquoi, les applications de capteurs à base de communication sans fi WiFi sont très peu répandues.[2]

Dans le Tableau 1.4 nous faisons une comparaison entre les protocoles de communications cités ci-dessus.

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	Plusieursminutes	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

Table 1.4 – Comparaison entre les différentes technologies sans fi

Les applications des WBAN dans le domaine de surveillance médicale

Il existe plusieurs applications médicales pour la surveillance de la santé des patients en général et des personnes âgées en particulier. Lorsque ces applications sont explorées, nous observons que les catégories principales cibles sont[2] :

- La surveillance des activités de la vie quotidienne
- La détection de chute et du mouvement
- La localisation
- Le suivi de prise des médicaments
- La surveillance de l'état de santé

- La bio-surveillance
- La prédiction des maladies

Les projets de recherches des systèmes WBAN

Codeblue :

Le projet de CodeBlue de l'Université de Harvard considère un environnement d'hôpital où des noeuds multiples de routeur peuvent être déployés sur le mur. Tous les noeuds emploient la même radio de ZigBee. Les patients/travailleurs sociaux peuvent éditer/souscrivent au réseau maillé par la multi fusion ; il n'y a aucun serveur ou base de données centralisée ou distribuée pour la commande et le stockage. La fonctionnalité de localisation est équipée par MoteTrack d'exactitude de 1 m, basée sur la même radio. En raison de la mobilité et des transmissions de multialimentation, le système éprouve la perte considérable de paquet et est limité à la largeur de bande globale de 40 kb/s par récepteur.
CodeBlue fournit des protocoles pour la découverte de dispositif et édite/souscris le cheminement de multialimentation, comme une interface simple de question qui est travaillée pour la surveillance médicale.[3]

AID-N :

Basés sur l'architecture de CodeBlue, la santé et le réseau avancé d'aide de désastre (AID-N) sont développés à l'Université John Hopkins [2] pour des incidents d'accident de masse où des étiquettes électroniques de sélection peuvent être déployées sur des victimes.
Des possibilités sans fi additionnelles (par exemple : Wifi, et réseaux cellulaires) sont présentées pour faciliter communications entre les serveurs personnels et le serveur central où des données sont stockées. En outre, un portail Internet est fourni aux types multiples d'utilisateurs, y compris le personnel urgence de département, les commandants d'incident, et les spécialistes médicaux. Un module de système de localisation mondial est utilisé pour la localisation extérieure, alors qu'un système de MoteTrack est conçu pour dépister à l'intérieur. Cependant, les patients ont des contraintes de mobilité dues au manque de routeurs dans le réseau, et un nombre très limité de noeuds de sonde peut

être mis sur chaque patient en raison de la largeur de bande limitée.[4]

Care net :

CareNet est un environnement sans fi intégrant de sonde pour les soins de santé à distance qui utilisent un réseau sans fi à deux niveaux et une plate-forme de logiciel extensible. CareNet fournit tous les deux fortement - fi et collecte de données, transmission et accès patients intimité avertie.[5]

Architecture du système :

CareNet est construit sur une infrastructure hétérogène de gestion de réseau qui implique la collecte de données, la transmission, et les phases patientes d'accès, suivant les indications du schéma[5]

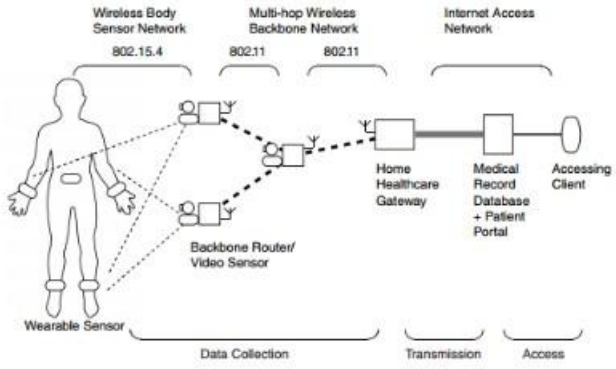

Figure 1.4 – architecture du système [5].

Comme illustré dans la fi 1.4, un réseau sans fi à deux niveaux est employé pour fournir des données sentant, des fonctions de collection, de transmission et de traitement. À la rangée inférieure, un réseau de sonde de corps se composant des sondes portables légères fournit des données sentant et des fonctions de transmission. Ces sondes peuvent communiquer avec les sondes de base-station (qui sont attachée au réseau sans fi d'épine dorsale) directement en utilisant la norme sans fi d'IEEE 802.15.4. Nous employons des grains de Telos comme dispositifs câblés. Pour la détection de mouvement et la détection de chute, ces grains sont équipés des accéléromètres et des gyroscopes. À cette rangée,

les dispositifs de sonde sont légers, portables et mobiles, qu'également les moyens ils ont le bas calcul, la puissance de communication et l'un peu de la mémoire. Ainsi dans notre conception, des tâches nécessaires seulement informatiques et de communication sont mises en application à ces dispositifs.[5]

ASNET :

ASNET permet le cheminement et la surveillance des patients et des médecins à l'intérieur et/ou en dehors de l'hôpital. D'une manière primordiale, dans le cas d'une urgence, des médecins et/ou les infi ères seront contactés automatiquement par leurs aides numériques personnels ou téléphones mobiles tenus dans la main. En étant entré en contact, le médecin/infirmière fournira à leur tour une question médicale au patient mobile spécifique ASNET. L'ASNET mis en application se compose de trois couches hiérarchiques suivant les indications du schéma 1. Les noeuds de sonde de l'ASNET agissent en tant que la première couche, et sont responsables de la mesure, du rassemblement et de la communication, par l'intermédiaire d'une interface de câble ou sans fi des lectures à un microcontrôleur qui compose la deuxième couche. En conséquence, les microcontrôleurs de différents patients communiquent avec troisième se composer de dispositifs de couche ordinateur central ou PDAs tenu dans la main/cahiers porté par des médecins/infirmières. Dans le cas d'une urgence, le microcontrôleur patient envoie directement un message de SMS aux téléphones mobiles des médecins et/ou des infi ières.[6]

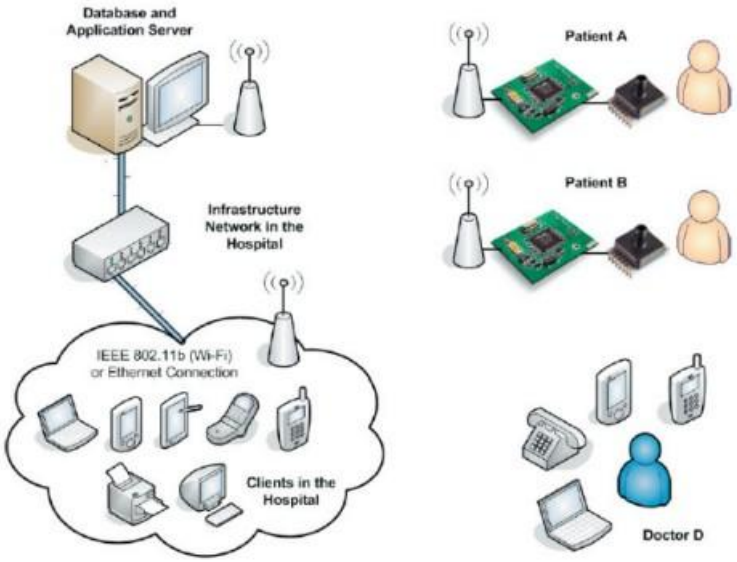

Figure 1.5 – trois couches de mettre en application de ASNET.[6]

MITHril :

MIThril est une plate-forme de la recherche portable développée par les chercheurs aux Moyens de MIT Labo. Ils utilisent des sondes portables pour diriger l'état physiologique d'un utilisateur et l'entourage de l'environnement pour découvrir de nouvelles techniques pour l'interaction humain-ordinateur. Le système MIThril est centré au sujet du "MIThril Contexte en temps réel moteur" qui goûte des sondes portées sur le corps, extraits traits pertinents des données crues, puis utilise ces données pour modeler le contexte de l'utilisateur.[4]

Les chercheurs utilisent des sondes sur commande et disponibles en magasin dans leur réseau. Les sondes communiquent via des interfaces a installées et tout situent dans un gilet. Le MIThril inclut ECG, température de la peau, sondes de la réponse (GSR) de la peau galvanique, appareils-photo minuscules et microphones.

De plus, les équipiers ont démontré et analysé l'étape de la démarche qui utilise 3-axe accéléromètres, compas gyroscopiques de taux et sondes de la pression.[6]

Figure 1.6 – GroupMedia - système MiThril caractériser un Zaurus PDA, SAK 2, accéléromètre [sur chapeau] et IR étiquettent le lecteur emballé dans un facile-portez l'étui de revolver.[6]

WHMS :

Système de l'Écoute de la santé (WHMS), a été une révolution remarquable en émergeant du Réseau de capteur sans fi (WSN) dans l'exécution de l'écoute et l'enregistrement de soins médicaux. Donc, les systèmes basé sur les réseaux de capteurs sans fi portable sont projetés de fournir mieux la gestion de la santé personnelle, condition de l'écoute de la santé omniprésente, meilleur traitement de la qualité et se soucie, permettre une effective intégration de circuit, dimensions du signal vitales fi opération basse coûte et usage du pouvoir optimum.[7]

Le système portable de surveillance de la santé (WHMS) est développé à l'université de L'Alabama et cibles un à plus grande échelle le système de télémédecine pour l'état de santé ambulatoire surveillance. À la différence de CodeBlue et d'AID-N, WHMS a un réseau de tenir le premier rôle-topologie pour chaque patient, qui est relié par l'intermédiaire de wifi ou d'un réseau cellulaire à un fournisseur de soins de santé. Le serveur personnel, mis en application sur un aide numérique personnel (PDA), téléphone portable, ou PC, coordonne la collecte de données de nœuds de capteurs utilisant un multiple temporel accès au mécanisme (TDMA), fournit une interface aux utilisateurs, et transfère des données à un serveur central à distance. Les médecins peuvent accéder à des données par l'intermédiaire de l'Internet, et des alertes peuvent être créées par un agent fonctionnant sur le serveur. Cependant, la puissance d'énergie et le coût se sont associés au long terme, les données téléchargeant peuvent gêner la réalisation de système.[4]

WiMOCA :

Le noeud sans fi de sonde pour un système de capture de mouvement avec des accéléromètres (WiMoCA) projette à plusieurs universités italiennes est concerné par la conception et l'exécution d'un système réparti d'identification de geste. Le système a une topologie d'étoile avec tous les noeuds de détection envoyant des données à un noeud de non-détection de coordonnateur utilisant a TDMA-comme l'approche, et le coordonnateur transmet par relais alternativement les données à une unité de traitement externe utilisant Bluetooth. Les modules de détection, chacun ont composé d'un accéléromètre à trois axes, peuvent être mis sur les parties multiples du corps pour la détection de mouvement. Les modules par radio de tous les noeuds fonctionnent dans la bande permis-exempte européenne de 868 mégahertz, avec le débit jusqu'à 100 de kb/s. Une interface utilisateur graphique Java basée sur le côté d'unité de traitement interprète le train de données de données pour l'identification de maintien.[4]

MIMOSA :

La plate-forme de microsystèmes pour des services et des applications mobiles (MIMOSA) est un projet de recherche faisant participer 15 associés de huit pays européens différents pour créer l'intelligence ambiante. L'approche de la MIMOSA est semblable à WHMS tandis qu'elle utilise exclusivement un téléphone portable, car le dispositif utilisateur-porté d'interface. Wibree, plus tard renommé Bluetooth, technologie de basse énergie, et étiquettes d'identification de radiofréquence sont employées pour relier des noeuds locaux de sonde. NanoIP et protocoles simples d'interface de sonde sont intégrés dans la MIMOSA pour fournir une interface de programmation API pour la connectivité locale et pour faciliter des lectures de sonde.[4]

Système	Sondes	communication Intra BAN	communication Inter BAN	communication Au-delà de BAN	l'application Visez
CodeBlue	oxymètre d'impulsion, EKG, motion	Installé	Mesh et ZigBee	--	Soin médical
AID-N	Pulse, Blood, Temperature, ECG	Installé	Mesh et ZigBee	Internet/WiFi/ Réseaux cellulaires	Incident de la Victime de masse
SMART	ECG,sonde SpO2	Installé	802.11b	--	Santé qui dirige la pièce en
CareNet	Tri-axial accelerometer / Gyroscope	--	ZigBee	Multihop 802.11 internet	Soins médicaux éloignés
ASNET	Blood pressure, Temperature	Topologie de l'étoile	GPRS/GSM	--	Ecoute de la santé éloignée
MITHril	ECG,EKG	Installé	WiFi	--	Soins médicaux
WHMS	ECG,EMG, EEG ,SpO2 ,	Topologie de l'étoile	WLAN /Bluetooth /GPRS	Internet	Telemedicine
WiMOCA	Tri-axial accelerometer	Topologie de l'étoile & La table du temps a basé MAC protocole	Bluetooth	Internet/WiFi/ Bluetooth/ Réseaux cellulaires	Faites des gestes la découverte / Sports
MIMOSA	Toute sonde / Sonde RFID	Wibree/Blue tooth/RFID	Réseaux cellulaires	Internet	Intelligence ambiante

Table 1.5 – exemple de Systèmes d'après différentes communications [8]

La technologie est entrain d'avancer donc les systèmes WBAN on aussi évoluer, dans ce qui se suit nous allons citer quelques nouveaux projets de recherches qui sont plus récents :

Bluetooth énergie basse (BLE) :

Comme partie du Bluetooth 4.0 standard, une alternative à Bluetooth classique connu comme Bluetooth L'Énergie basse (BLE) a été introduite. BLE a été développé initialement par Nokia dans 2006. C'était conçu pour fournir un pouvoir extrêmement bas au mode repos, un appareil peu compliquée et hautement fi pour le transfert de données. BLE est capable de connecter la miniature sans fi appareils du bas-pouvoir aux terminaux mobile qui le font un candidat approprié pour les applications de la surveillance médical (BAN). BLE est matériel-optimisé de la version Bluetooth à cause de ses différences principales tel que la format des paquet de données, émetteur-récepteur de la radio et band de base pour le traitement du signal numérique comparé à Bluetooth classique. BLE est capable de fournir un taux jusqu'à 1 Mbps de données. Depuis que BLE utilise

moins de nombres de canaux pour l'appareillement BLE, il consomme considérablement moins de temps (peu de millisecondes) pour la découverte de l'appareil et la synchronisation comparé à des secondes pour Bluetooth. C'est considérablement précieux pour les ressources-limités et l'état latent-critiques des appareils tels que ceux utilisés dans les applications de la surveillance médical. . BLE emploie une pile de protocole simplifié et principalement intéressé à court terme, réseau de topologie étoile avec des algorithmes d'acheminement peu compliqués.[9]

ANT :

ANT est une technologie sans fi de bas-pouvoir conçue et a développé pour une gamme générale d'applications du réseau de capteur sans fi ANT est spécifiquement appropriée pour un taux de données bas, la pile a propulsé des nœuds de capteur et couvre une gamme de topologies du réseau de point-à- point simple à réseaux de la maille complexes. ANT est candidate pour la connectivité sans fi dans les applications de la pile a propulsé tel que la surveillance médical où la consommation du pouvoir ultra-basse est exigée. ANT opère dans la bande de fréquence 2.4 GHz, supporte un taux des données de 1Mb/s et emploie l'arrangement TDMA pour adresser les questions de l'intervention. ANT+ facilite la communication sans fi des appareils de compagnies différentes en fournissant des paramètres du réseau prédéfinis et la charge utile des données structure y compris le profi de l'appareil. Les profi d'appareil ANT+ existants consistent en moniteurs du taux du cœur, vitesse pas -basée et moniteurs de la distance, vitesse du vélo et pouvoir. Plusieurs profi de l'appareil prochains incluent des balances du poids, vitesse du multi-sport et distance, et capteur de l'environnement.[9]

RuBee :

RuBee est considéré comme une alternative à Identification de la Radio-fréquence (RFID). C'est un protocole sans fi actif bidirectionnel qui emploie une grande onde signaux aimantés (pas signaux RF) pour transmettre et recevoir des paquets de 128 bits de données dans un réseau local. RuBee est basé sur l'IEEE1902.1 standard et conçu spécifiquement pour fournir la haute sécurité dans les environnements sévères. Semblable

à l'IEEE 802 standard, RuBee permet au réseau de gérer les appareils en employant le point à point émetteurs-récepteurs rayonnant actifs. Ce protocole opère à la fi de la fréquence basse, 131 kHz. Semblab à WiFi, Bluetooth et ZigBee, le RuBee est protocole basé sur les paquets sur-demande mais avec un taux de données inférieures. De plus, la fréquence du fonctionnement basse de RuBee fournit un avantage considérable quant au pouvoir de consommation. Il peut fournir une vie de la pile de jusqu'à quinze années utilisant une cellule du bouton du lithium et c'est aussi capable de fournir une distance de la couverture jusqu'à 50 pieds d'après. Cependant, La fréquence du fonctionnement basse de RuBee exige une plus grande dimension de l'antenne qui rend cette technologie une possible candidat peu approprié pour les applications de BAN où la dimension d'antenne joue un rôle important. Par contraste avec RFID, RuBee n'a pas de réflexions du signal et ne peut pas être bloqué par les matières tel que acier et liquide. Par conséquent, c'est surtout une technologie robuste dans la visibilité de l'environnement sévère et les applications de la sécurité.[9]

Sensium :

Sensium est principalement une plate-forme sans fi à pouvoir ultra-bas conçue pour fournir et personnalisé les services de la santé pour les applications de la gestion de la maladie chroniques. Sensium est capable de fournir une surveillance du pouvoir ultra-basse des signaux vitaux tel que les niveaux du PH, glucose du sang et signaux ECG. Le but principal de Sensium sera de s'enfoncé dans un plâtre numérique devant être prescrit par les médecins. Sensium opère dans la bande de la fréquence de 900 MHz et supporte un taux des données de 160 ko / s. Sensium est considéré comme un des principal technologies sans fi du pouvoir ultra-bas pour les applications du sur-corps de donnée à taux basses. Sensium utilise une structure de communication de maître / esclave dans laquelle un noeud esclave du sur-corps transmet les signaux vitaux multiples à un serveur personnel tel que téléphone intelligent, PDA ou un ordinateur individuel de temps chronométrer. Depuis que le sensium utilise une topologie de l'étoile, le réseau est dirigé centralement. La consommation d'énergie des nœuds est aussi dirigée centralement ; les nœuds sont programmés pour garder leurs radios dans le mode sommeil jusqu'à ce que des slots du

temps soient données à eux par le serveur central.[9]

Zarlink :

Zarlink est spécifiquement RF à pouvoir ultra-bas émetteur-récepteur conçu pour les applications médical de l'implantable. Zarlink utilise la découverte de l'erreur de la Redondance Cyclique (CRC) avec le plan Reed-Solomon de la correction de l'erreur qui fournir un lien de la communication très fi Il opère dans les MICS (402.405 MHz) et bandes ISM (433.434 MHz). Zarlink supporte des taux de données jusqu'à 800 ko / s. Zarlink est capable d'opérer dans un implant et un poste bas. Selon le type de système sélectionné, différentes exigences sont nécessaires surtout en termes de consommation du pouvoir. Par conséquent, Zarlink a spécifié deux modes d'opération importantes : mode implantable de l'Appareil Médicale (IMD) et mode de base. Quand Zarlink est configuré comme une mode IMD, la radio est endormie la plupart du temps qui consomme seulement μW de pouvoir a comparé à mW de pouvoir dans d'autres modes. Cependant, la communication entre deux nœuds ne peuvent pas se produire si la radio de l'un et l'autre nœud est dans le mode sommeil. Par conséquent, un mécanisme est exigé pour réveiller la radio du récepteur pour assurer la transmission de l'émetteur et que le récepteur écoutez les opérations coïncident. Cela peut être fait par l'un ou l'autre utiliser un pouvoir ultra-bas 2.4 GHz envoient par radio ou directement en utilisant le processeur IMD. Zarlink est considéré comme un des principaux technologies sans fi du pouvoir ultra-bas pour les applications de l'implantable médicales de données de taux bas (TRX = 5 MA, mode du bas-pouvoir = 1 MA et pouvoir ultra-bas circuit du réveille = 250 nA).[9]

Insteon :

Insteon est spécifiquement une technologie du réseau de maille conçue pour applications de maison et de l'électronique personnelles. Insteon fait l'usage des deux signale Fréquence de la Radio (RF) et l'infrastructure du câblage électrique (PLC) existait à la maison pour transmettre des données d'un appareil à un autre. Insteon est capable d'utiliser des RF-seuls appareils, pouvoir-ligne-seuls appareils ou peut supporter simultanément les deux types de systèmes de la communication. Par conséquent, il est considéré comme

une technologie de l'automatisation de maison la plus fi Les appareils Insteon sont appelés des pairs parce que tous les appareils Insteon sont capables de transmettre, recevez et relais d'autres messages complètement indépendant d'un contrôleur. La gamme de communication Insteon peut être étendue au moyen d'une approche du multi-petit saut. Dans cette méthode, un réseau Insteon utilise deux ou plus petits sauts pour délivrer l'information d'une source à une destination. Insteon a aussi limité le nombre maximal de petits sauts a tenu compte de chaque message à quatre. De plus, dans les applications PLC, Insteon opère à 131.65 kHz et utilise la technique de modulation Binaire phase-changement Accordage (BPSK) ; dans les applications RF il opère dans la bande ISM (902.924 MHz) et utilise le plan de la modulation accordage de fréquence-changement (FSK). Insteon utilise le plan de la Répétition Automatique de la demande (ARQ) pour accomplir une fi transmission des données sur les canaux de la communication peu fi ou bruyants. Insteon supporte un taux des données instantané de 13.165 ko / s. Il supporte aussi plusieurs méthodes du chiff t telles que roulant-code, gestion-clef et public-clef.[9]

protocole	Sécurité	L'outil utilisé	Critères évalués	Description
Bluetooth (BLE)	Clef Pré-partagé facultative, Chiffrage 128 bit	GFSK	Capteur ECG, EEG,IMU, tension,spO2	8
ANT	Chiffrement de Données AES-128, lien Certification	GFSK	Capteur ECG, EEG,IMU, tension,spO2	65,000 + 1
RuBee	AES facultatif Chiffrage, clef privée, clef publique	ASK, BPSK, BMC	Capteur ECG, EEG,IMU, tension,spO2	Illimité
Sensium	clef publique	BFSK	Capteur ECG, EEG,IMU, tension,spO2	8 + 1
Zarlink		2FSK/4FSK	Capteur ECG, EEG,IMU, tension,spO2	
Insteon	Code de roulement, clef publique	RF: FSK Ligne électrique : BPSK	Capteur ECG, EEG,IMU, tension,spO2	Illimité

Table 1.6 – comparaison entre les systèmes.

1.4.2 1.4.1.10 Les défis et les contraintes des réseaux WBAN

Les défis des réseaux WBAN :

Les applications médicales d'un système de réseaux de capteurs sans fi imposent des exigences strictes en matière de fi é du système, de qualité de service, de consommation d'énergie, de vie privée et de sécurité des données. Donc, les réseaux de capteurs médicaux WBAN présentent plusieurs défis à relever. Parmi ces défis nous citons :[2]

Le défi d'énergie

Le principal facteur limitant la durée de vie d'un réseau de capteurs est l'énergie. Donc l'optimisation de l'énergie est un défi qui est rencontré dans presque tous les domaines d'application des réseaux de capteurs sans fi parmi lesquelles les applications médicales. Les capteurs actuels ont des périodes de veille durant leur inactivité pour préserver leur batterie. Les sources de consommation d'énergie dans un nœud capteur proviennent principalement de l'unité de captage, de l'unité de traitement des données et de l'unité de communications (transmission et réception sans fi [2].

Les communications sont les actions qui coûtent le plus cher en termes d'énergie et les calculs le sont mais avec une moindre importance. Il est donc fortement nécessaire de limiter le nombre de communications entre capteurs et si possible la quantité de calculs [2].

Tolérance aux pannes

Dans les réseaux de capteurs sans fi un ou plusieurs capteurs peuvent ne pas fonctionner correctement, car les capteurs sont des entités sensibles aux altérations d'états comme des phénomènes climatiques (humidité, chaleur, etc.) ou du fait d'une batterie faible. Dans ces cas, le réseau doit être capable de détecter ce type d'erreur et d'y remédier, afin de transmettre l'information et permettre au réseau d'être toujours opérationnel [2].

La sécurité

Les applications médicales imposent des exigences strictes en termes de fi é du système de bout en bout et de livraison des données. La communication des données médicales entre les capteurs d'un système WBAN est soumise à des exigences de sécurité telles que la disponibilité du réseau, la confidentialité, l'authenticité, l'intégrité et la fraîcheur des données[2].

Les contraintes des réseaux WBAN

Un réseau de capteurs sans fi 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 fi Les contraintes dans un réseau de capteurs sans fi médicaux sont classées en deux catégories : contraintes matérielles et contraintes réseau, Le Tableau 1.7 résume ces contraintes[2].

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

Table 1.7 – Les contraintes de sécurité dans un RCSF corporels[2]

1.5 Conclusion

Dans ce nous avons présenté les réseaux de capteurs sans fi (RCSF) et leurs utilisation pour les applications de surveillance médical, de plus nous avons exposé les réseaux corporel de capteurs sans fi (avantages, architecture, topologie…) et nous avons citer quelque systèmes de surveillance médical ainsi quelque nouvelles technologies émergeantes.

Chapitre 2

Le système proposè

Introduction

Les réseaux de capteurs sans fi *RCSF*) comme tous les autres types de réseaux sont ciblés par plusieurs types d'attaques comme l'eff t(Sinkhole),l' attaque du trou de ver(wormhole attack), Jamming, Trifouillage(Tampering) ,Inondation (Flooding) et l'attaque de l'homme au milieu (*ManintheMiddleAttack*), dans notre travaille nous nous intéressons à ce dernier type d'attaque.

Les solutions existantes

l'attaque de l'homme au milieu

L'attaque de l'homme au milieu est une forme d'écoute clandestine active dans laquel l'attaquant fait des rapports indépendants avec les victimes et relaie des messages entre eux, en les faisant croire qu'ils parlent directement à chacun entre eux sur un rapport privé. L'attaquant pourra en mesure à arrêter tous les messages échangeant entre les deux victimes et injecte des nouveaux [11].

L'attaque d'Empoisonnement ARP

- Dans l'Empoisonnement ARP, l'attaquant envoie des faux messages ARP sur le réseau en disant à la victime son adresse MAC au lieu de l'adresse MAC d'appareil que la victime veut relier avec.
- Dans cet exemple (Figure 2.1), l'attaquant répondra les ARP demandent avec son adresse MAC, donc la victime le mettra comme associé avec l'adresse IP 192.168.56.8.
- L'empoisonnement ARP est possible dû aux caractéristiques d'ARP qui est décentralisé et non légalisé. Une fois que l'adresse MAC de l'attaquant est connectée à l'adresse IP de victime, l'attaquant commencera à recevoir toutes données qui sont projetées à 192.168.56.8.
- Notez que l'empoisonnement ARP peut être exécuté seulement sur les LAN qui utilisent l'ARP.

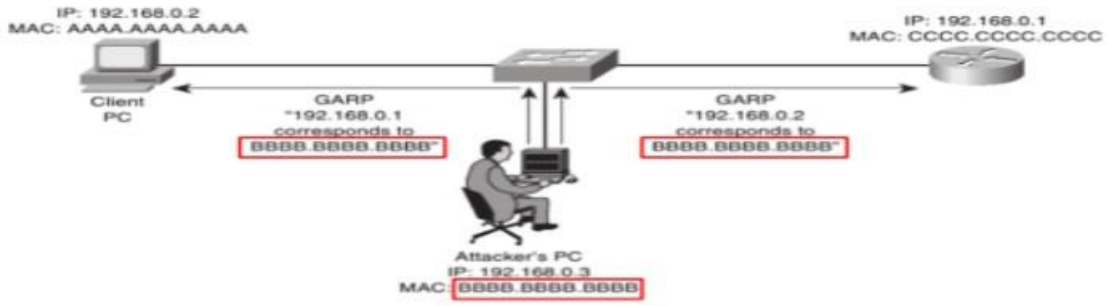

Figure 2.1 – l'attaque le l'empoisonnement ARP. [12]

Empoisonnement ARP :

Une des formes plus faciles et plus efficaces de MITM moderne attaque, empoisonnement de cachette ARP permet à un attaquant sur le même subnet comme ses victimes d'espionner toute la circulation du réseau entre les victimes. [12]

Protocole ARP :

Le Protocole de la Résolution de l'Adresse (ARP) est utilisé pour trouver l'adresse MAC d'un autre appareil dans le Réseau de Région Local (LAN) pour communiquer avec cet appareil. Pour le faire, ARP dresse une carte d'adresse de la couche du réseau (IP) pour lier l'adresse de la couche (MAC) qui est reconnue dans le LAN.
Quand un hôte veut communiquer à un autre appareil, il envoie une émission de l'Ethernet demandant l'adresse MAC d'un nœud avec une adresse IP particulière. Quand un hôte B voit une demande pour son adresse IP, il enverra une réponse avec son MAC adresse. Hôte A cachera alors le résultat pendant une courte période, utilisant cette adresse MAC pour de futurs paquets à l'adresse IP. [12]

Attaque de l'échantillon

L'attaque de l'échantillon est lancée contre une banque fi e, dû à la sensibilité de la matière. La sécurité et les contres mesures sont basés sur les situations communes utilisées par des institutions fi ères réelles. Dans cette attaque l'attaquant est assumé pour être un employé avec l'administration privilégie à un fournisseur de service Internet, cela donne à l'attaquant l'accès à beaucoup de circulation. [13]

L'attaque de Sybil

Un nœud malveillant peut prétendre avoir de multiples identités en utilisant les identités des nœuds ciblés par l'attaque. L'attaque Sybil est le nom porté par ce genre de menaces. Les nœuds ciblés par l'attaque sont connus sous le nom de Sybil nodes. Cette attaque est localisée entre la couche liaison et la couche réseau. Elle vise à dégrader l'intégrité des données, le niveau de sécurité et l'utilisation des ressources (Figure 2.2).[14]

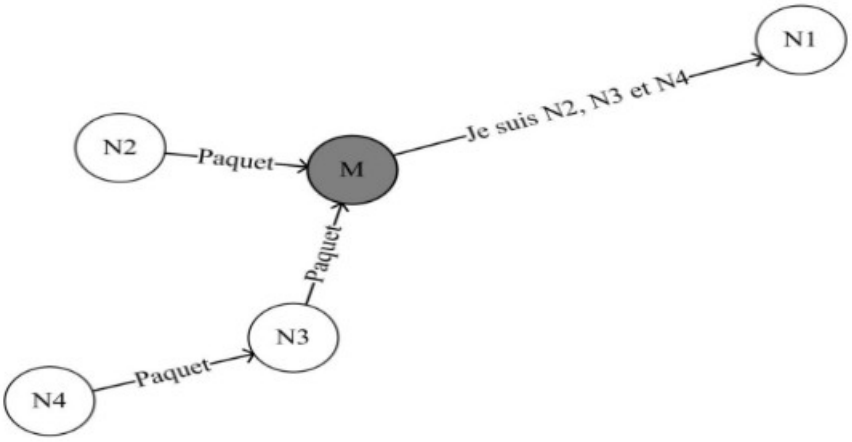

Figure 2.2 – L'attaque Sybil.

Un nœud malveillant M prend une place dans le réseau et reçoit les paquets de plusieurs nœuds, ici N2, N3 et N4. Il prétend être ces derniers auprès de N1 après avoir usurpé leur identité. Si N1 ne possède pas le moyen de vérifier l'identité des expéditeurs, M jouera le rôle des autres nœuds et l'attaque sera réussie. [14]

L'attaque de sybil à connus de nombreuse évolutions par conséquent des nouveaux genres d'attaques sont apparus :

- Agrégation des données
- Voter
- Allocation de la ressource juste
- Découverte de la mauvaise conduite

Les solutions proposées contre L'attaque de l'homme au milieu

La solution proposée contre l'attaque d'Empoisonnement ARP

Combattre efficacement contre empoisonnement ARP n'est pas une tâche facile parce que le protocole ARP ne fournit pas de possibilités d'établir l'authenticité de la source de rentrée paquets.

En dépit de tout, il y a quelques façons de protéger vos machines contre spoofers / empoisonneurs en utilisant :

- ARP statique
- Outils de la surveillance (tel que les Arpwatch, les Ettercap ou les cartes d'identité du Reniflement)[12]

La solution proposée contre l'attaque de l'échantillon

L'attaque de l'échantillon montre que l'utilisateur devrait signer quelque chose qui vérifie l'intention des utilisateurs pour priver l'attaquant des informations du laissez-passer. L'accord devrait aussi être manié dans la même demande comme l'action qui est signée, cela force l'attaquant à créer une attaque plus complexe qui augmente le risque de découverte.[13]

La solution proposée contre l'attaque sybil

Les chercheurs ont récemment proposé une technique prometteuse pour la distribution de clef dans des réseaux de sonde : predistribution aléatoire de clef .Ces techniques permettent à des nœuds d'établir des liens sûrs à d'autres nœuds. Dans la predistribution aléatoire de clef, nous assignons un ensemble aléatoire de clefs ou information clef-connexe à chaque nœud de sonde, de sorte que dans la phase principale d'installation, chaque nœud peut découvrir ou calculer les clefs communes qu'il partage avec ses voisins ; le terrain communal des clefs seront employées comme clef de session secrète partagée pour s'assurer la sécurité de nœud-à-nœud. [3 Sybil.pdf]
Nos idées principales sont :

- Associer l'identité du nœud avec les clefs assigné au nœud.
- Validation clé, c.-à-d., le réseau est capable de vérifier une partie ou toutes les clefs qu'une identité prétend avoir. [14]

Synthèse

Chacune des défenses contre l'attaque de l'homme au milieu que nous avons examinée a des différentes traditions. La plupart des défenses ne sont pas capables de défendre contre chaque type d'attaque de l'homme au milieu.
En plus, chaque défense a des coûts différent de et compte sur des prétentions différent. L'attaque de l'Empoisonnement ARP est très diffi e contrer alors on ne peut que à
se protéger de cette attaque. La solution proposer contre l'attaque de l'échantillon ne fait que compliquer la tache de l'attaquant en ajoutant une signature lors de l'envoi des informations. L'attaque de sybil a plusieurs solutions mais la pluparts d'entre elles ont s'intéressé à l'authentification et la manière de distribution des clefs.

Proposition

Hachage des données

Une fonction de hachage est une méthode permettant de caractériser une information, une donnée. En faisant subir une suite de traitements reproductibles 'a une entrée, elle génère une empreinte servant 'a identifier la donnée initiale. De telles fonctions 5 datent de la fi des années 1980 (algorithme MD2) mais l'idée est plus ancienne, et a germé dès l'apparition des codes correcteurs d'erreurs (théorie de l'information). [15]

2.4.1.1 fonctions de hachage

Nous avons choisis l'algorithme de hachage MD5 à cause de la capacité de stockage limité des capteurs.

MD5 :

Conçu par Ronald Rivest (le R dan s RSA), c'est le dernier d'une série (MD2, MD4). Cet algorithme produit un condensé de 128 bits. Il était il y a encore quelques temps l'algorithme de hachage le plus largement répandu. La cryptanalyse et l'attaque par force brute (2004) l'ont affaibli. Ses spécifi sont disponibles sur Internet dans le RFC

1321.

Vue d'ensemble

Le déroulement général d e l'algorithme est illustré à la fi 2.3.

1. Complétion : ajout de padding si nécessaire afin que le message ait une longueur de 448 mod 512. Cet ajout a toujours lieu.
2. Ajout de la longueur : on ajoute la longueur réelle du message (sur 64 bits) après les 448 bits. En conséquence, la taille totale du bloc atteint 512 bits. S i la longueur nécessite plus de 64 bits, on ne note que les 64 bits d e poids faible.
3. Initialisation : initialiser 4 buffers de 32 bits chacun (A,B,C,D), qui constitue l'IV.
4. Calcul itératif : traiter le message par blocs de 512 bits. Il y a 4 rondes de 16 opérations qui sont réalisées en fonction du bloc (512), du contenu des buff et de fonctions primitives.
5. Le résultat fi est obtenu en concaténant les résultats des additions des registres A,B,C,D avec la valeur de CVq (voir 2.3). [15]

Algorithme :

- $CV_0 = IV$
- $CV_{q+1} = \bar{+}32 V_q, RFI(Yq, RFH(Yq, RFG(Yq, RFF(Yq, CVq))))]$
- $MD = CV_L$

où :

IV : valeur initiale des registres ABCD

Yq : le $q^{eme`}$ bloc de 512 bits du message

L : le nombre de blocs de 512 bits dans le message

CV_q : variable chainée obtenue par la manipulation du q^{eme} bloc

RF_x : fonction primitive dépendante de la ronde en cours

MD : résultat fi

$\bar{+}32$: addition modulo 2^{32}.

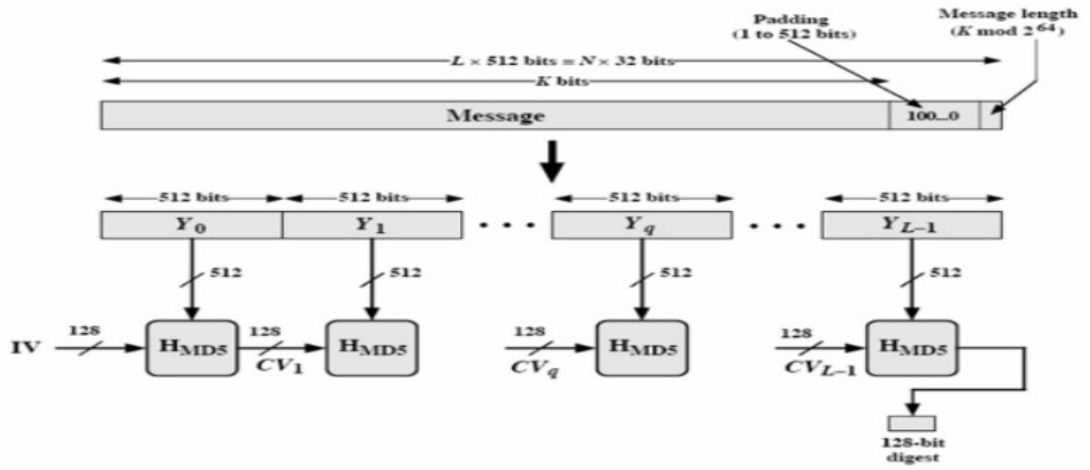

Figure 2.3 – vue d'ensemble de MD5. [15]

2.5.2 La stéganographie

La stéganographie (du grec steganos, couvert et graphein, écriture) est l'art de cacher un message secret au sein d'un autre message porteur (texte, image, son, vidéo...) de caractère anodin, de sorte que l'existence même du secret en soit dissimulée. Alors qu'avec la cryptographie, la sécurité repose sur le fait que le message chiff é soit incompréhensible pour les personnes non autorisées, avec la stéganographie, la sécurité repose sur le fait que la présence même d'un message secret ne sera sans doute pas soup çonnée et détectée.[16] Nous avons choisis la méthode LSB à cause de la capacité de stockage limité des capteurs.

2.4.2.1La Méthode LSB (Least Significant Beat), ou méthode de bit de poids faible :

Cette méthode consiste à modifi le bit de poids faible des pixels codant l'image. Une image est un tableau constitué d'un ensemble de pixels. Pour chaque pixel, on code la couleur avec trois octets : un pour le rouge, un pour le vert, un pour le bleu. Chaque octet indique l'intensité de la couleur correspondante, sur un niveau allant de 0 à 255. 255 correspond à la couleur native. Passer d'un niveau N à un niveau N - n, où n est suffisamment petit ne modifi que de peu la couleur, et c'est précisément sur cela que repose la méthode LSB. [17]

Cacher du texte dans une image :

Un texte codé en ASCII s'étend sur des valeurs allant de 0 à 127. On peut rajoute une valeur 128 pour signaler la fi du texte. Chaque caractère est donc codé par un octet. Voyons comment codé l'octet 01011101. On ne peut pas se permettre de négliger les bits de poids faible. On va donc couper cet octet en deux : 0101 et 1101. On va cacher par exemple le premier morceau dans la partie rouge de l'image et le deuxième morceau dans la partie bleue. Il va nous falloir réaliser deux programmes, l'un dissimulant notre texte, l'autre nous permettent de le restituer. Ce sont les rôles des programmes *cacher*$_t$*exteettrouver*$_t$*exte*. *cacher*$_t$*exte* prend en argument d'entrée l'image et le texte. [16] **Méthode proposé pour lutter contre l'attaque de l'homme au milieu :**

Vue générale :

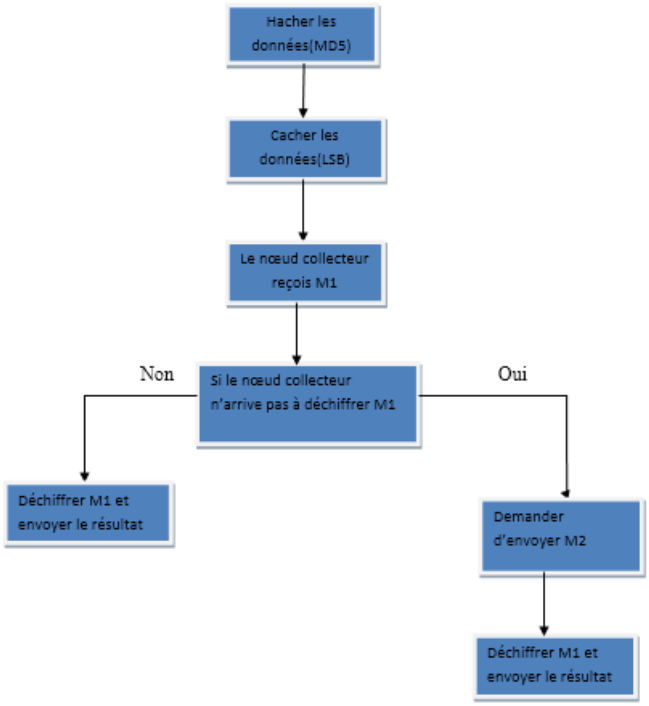

Figure 2.4 – algorithme contre l'attaque de l'homme au milieu.

La fi 2.4 représente les étapes de notre algorithme pour diminuer les probabilités pour qu'une attaque de l'homme au milieu réussis. Nous proposons d'abord de haché les

données collectées par les capteurs poser sur le corps du patient.
Ensuite nous allons faire appel à la steganographie afin de cacher les informations hachées. Dans le cas ou le réseau fonctionne normalement, le capteur envoi le message(M1) qui contient les données hachées et cachées pour empêcher qui que se soit de modifi les donnés car dans ce cas même si quelqu'un intercepte le message il sera incapable de le modifi
En cas de souci, c.à.d. le nœud collecteur n'arrive pas déchiffrer le contenu du message(M1) ou il a été remplacé par un autre. le capteur envoi deux messages le message (M1) et le message(M2) qui contient les algorithmes utilisés pour le hachage et ceux utilisés pour la steganographie.

Discussion

L'attaque de l'homme au milieu est très diffi à contrer, et surtout s'il s'agit d'un réseau de capteur sans fi alors les chercheurs ont proposé déférentes méthodes. L'avantage de notre proposition est qu'elle ne se base pas sur un système de distribution de clefs comme la pluparts des autres solutions qui est justement leur problème, de plus notre proposition assure l'intégrité des données. Mais d'un autre coté notre proposition nécessite un espace de stockage important donc nous sommes limités par la contrainte de stockage dans les réseaux de capteur sans fi

Conclusion

Dans ce chapitre nous avons présenté des travaux proposés contre l'attaque de l'homme au milieu. Ainsi notre solution détaillée.

Chapitre 3

Simulation de système proposé

Introduction

Apres avoir détaillé notre proposition de le chapitre précédant nous allons maintenant présenter notre simulation de la solution contre l'attaque de l'homme au milieu déjà proposé.

L'approche proposée

Dans notre simulation, les capteurs sont posés sur le corps humain et collectent les différentes mesures (ces mesures sont générées aléatoirement). En suite les valeurs seront hachés et envoyer à la station de base en passant par un réseau mobile. Si un intrus essaye de posséder à une attaque de l'homme au milieu alors, il va intercepter des données hachées impossible à modifi r car les fonctions de hachages sont irréversibles. Le message arrive à la station de base haché et pour le vérifier on le message en clair et no applique la fonction de hachage et le compare avec le haché reçu pour savoir si le message a été modifi

Outils utilisés

Afin de réaliser notre simulation, nous avons utilisé les outils suivants :

Netbeans

Cet IDE (environnement de développement intégré) a été créé a l'initiative de Sun Microsystems. Il présente toutes les caractéristiques indispensable à un environnement de qualité, que ce soit pour développer en Java, Ruby,*C/C* + + ou même PHP.
Netbeans est sous licence OpenSource, il permet de développer et déployer rapidement et gratuitement des applications graphiques Swing, des Applets, des JSP/Servlets, des architectures J2EE, dans un environnement fortement personnalisable.
L'IDE Netbeans repose sur un noyau robuste, la plateforme Netbeans, qui vous pouvez également utiliser pour développer vos propres applications Java, et un systéme de plugins performant, qui permet d'avoir un IDE modulable.
A coté de la version complète de l'IDE NetBeans, il existe différentes déclinaisons qui se concentrent sur une plateforme ou un langage précis (Java ME, Java : SE + ME + EE, Ruby, C/C++, PHP).
NetBeans contient, en plus du support pour CVS et SubVersion, un support pour Clear-Case, mais aussi pour Mercurial.

Il permet également de déployer des applications Web, non seulement vers Tomcat et Glassfish qui sont livrés avec le " Pack Web ", mais aussi vers JBoss, WebSphere 6.1 Weblogic 9.
NetBeans détient un support de développement d'applications Web avec des améliorations pour l'édition des JSP, la gestion serveur et le support des dernières versions de Tomcat.
Enfin cet IDE possède un débogueur de grande qualité ainsi qu'une interface graphique améliorée [17 (29)]

Java

C'est un langage de programmation orienté objet, développé par Sun Microsystème. Il permet de créer des logiciels compatibles avec de nombreux systèmes d'exploitation (Windows, Linux, Macintosh, Solaris).Java donne aussi la possibilité de développer des programme pour téléphone portable et assistants personnels. Enfin, ce langage peut-être utiliser sur internet pour des petites applications intégrées à la page web ou encore comme

langage serveur.[17 29]

Présentation des interfaces

Dans ce qui se suit nous allons présenter quelques interfaces de notre simulation.

Interface du simulateur

dans cette interface les capteur sont distribués, et le grand cercle noire est la station de base.

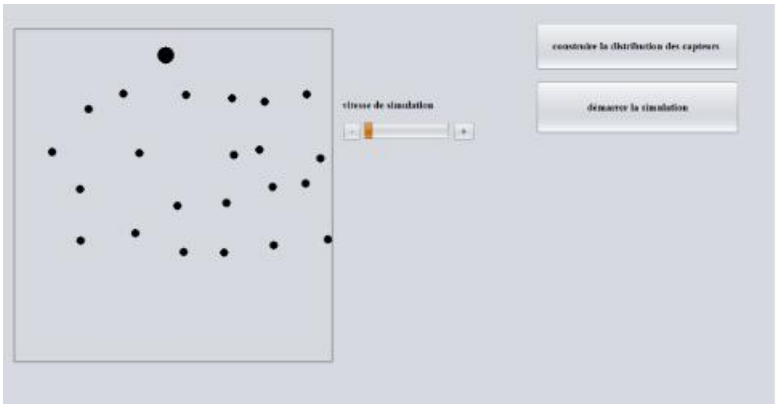

Figure 3.1 – interface du simulateur..

Interface de la collecte des mesures

Dans cette interface les capteurs commence la collecte des mesures.

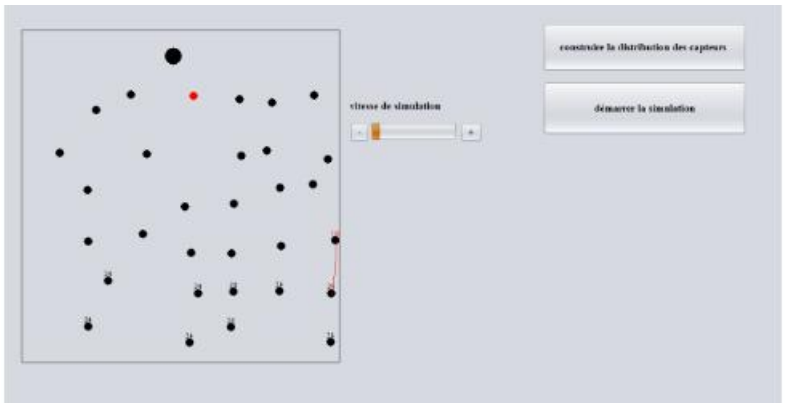

Figure 3.2 – interface de la collecte des mesures.

Interface de l'envoie des informations

Dans cette interface les mesures collectées sont envoyées à la station de base, les information envoyées sont hachés

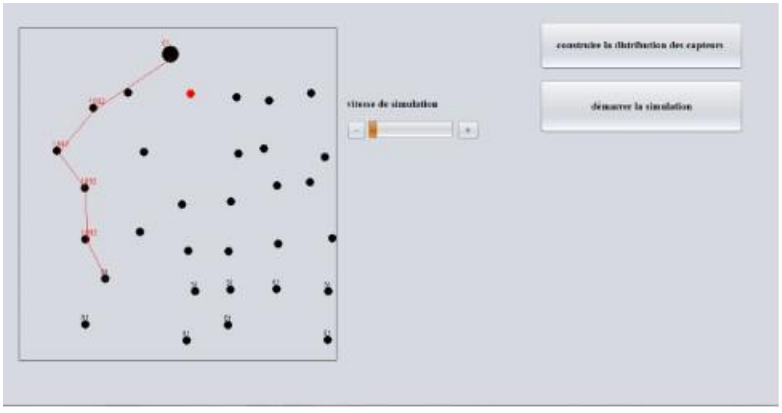

Figure 3.3 – interface de l'envoie des mesures.

Interface de l'attaque de l'homme au milieu

Dans cette interface l'intrus intercepte le message haché et le transmit à la station de base.

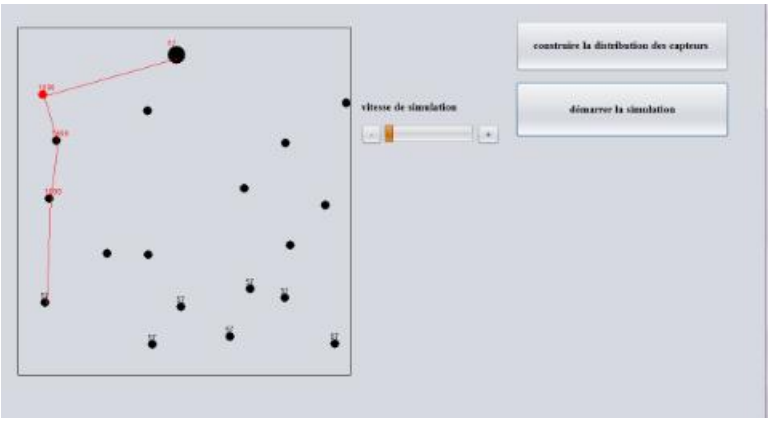

Figure 3.4 – : interface de l'attaque de l'homme au milieu.

Conclusion

De ce dernier chapitre nous avons présenté les différents outils de développement de notre simulation. En suite nous avons présenté et expliquer le fonctionnement de notre simulateur.

Conclusion et perspectives

Les réseaux de capteurs sans fi s'ouvrent à une multitude de domaines d'applications. Chaque application à ses propres contraintes et exigences. Ce mémoire à pour objectif d'apporter une solution liées à la lute contre l'attaque de l'homme au milieu dans un système WBAN (Wireless Body Area Networks) de surveillance médicale à distance.

Dans ce mémoire nous avons commencé par une présentation des réseaux de capteurs sans fi médicaux. Ainsi nous avons fait une comparaison entre les réseaux WBAN et les réseaux WSN en termes de déploiement, nombre de capteurs, débit des données, mobilité, etc. Nous avons présenté les sous-systèmes constituant un système WBAN de surveillance médicale à distance et l'architecture des communications dans ce système.

En suite nous avons présenté notre proposition contre l'attaque de l'homme au milieu avec quelque exemple de solution existante et nous avons détaillé les méthodes utilisées dans notre proposition.

Enfin nous avons présenté la simulation de notre proposition en commençant par une approche qui explique le fonctionnement de la simulation et nous avons définis les outils que nous avons utilisés dans notre projet.

Pour terminer nous espérons que notre simulation soit pris en consécration et comparer à d'autre proposition à fi de l'améliorer et de trouver une solution définitive pour l'attaque de l'homme au milieu. Nous espérons que les travaux de recherche continue dans l'élaboration sur l'attaque de l'homme au milieu. Dans ce mémoire nous avons proposé

d'utiliser des méthodes spécifiques pour la simulation, nous proposons d'essayer d'autres méthodes pour la simulation à fi de trouer le moyen le plus efficace comme utiliser d'autres méthodes pour le hachage ou pour la stéganographie. En plus il est intéressant de travailler sur d'autres types d'attaques et d'essayer de trouver des solutions pour ces attaque et nous espérons que notre mémoire apportera de l'aide a tout ceux qui vont continuer la recherche.

Resumé

Les soins médicaux changent, correction, les soins médicaux ont le besoin du changement. Le vieillissement de la population, l'augmentation dans les maladies chronique et de cœur et juste l'augmentation dans la dimension de la population accableront les courants soins médicaux dans les hôpitaux-centré. Plusieurs projets de recherche existants ont comme objectif d'assurer la surveillance des patients, par un meilleur suivi en utilisant les nouvelles technologies. En particulier les réseaux de capteurs sans fi s. Ce dernier soulève beaucoup de défis en termes de sécurité et de la protection contre les attaques.

L'objectif de ce mémoire est de traiter un type particulier d'attaque et de proposer une solution pour défendre contre l'attaque de l'homme au milieu.