République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A. Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Fin de Cycle

En vue de l'obtention du diplôme de Master Recherche en Informatique

Option : Réseaux et Systèmes Distribués

Thème

Sécurité pour la qualité de service dans les réseaux corporels sans fil

Réalisé par

M^{lle} BOUCHELAGHEM Siham

Devant le jury composé de

Président :	M. SADI Mustapha	Maître Assistant A	Université A. Mira Béjaïa
Examinateur :	M. AISSANI Sofiane	Maître Assistant A	Université A. Mira Béjaïa
Examinatrice :	M^{lle} BERMAD Nabila	Maître Assistante B	Université A. Mira Béjaïa
Encadrant :	M. OMAR Mawloud	Maître de Conférences A	Université A. Mira Béjaïa
Co-encadrante :	M^{lle} YESSAD Nawel	Doctorante LMD	Université A. Mira Béjaïa

Promotion 2015 - 2016

Remerciements

C'est avec un immense plaisir que je réserve ces quelques lignes en signe de gratitude et de reconnaissance à tous ceux qui ont contribué de près ou de loin à l'élaboration de ce travail.

Je souhaite adresser, en premier lieu, mes remerciements les plus sincères à mon encadrant Dr OMAR Mawloud pour ses conseils lucides et pertinents, sa patience et son précieux suivi tout au long de la réalisation de ce travail. Sa disponibilité, ses qualités pédagogiques et humaines, et ses compétences m'ont apporté un encadrement déterminant dans toutes les phases de ce travail. Qu'il trouve ici le témoignage de mon profond respect.

Mes remerciements vont aussi à ma co-encadrante M^{lle} YESSAD Nawel, pour sa gentillesse, sa disponibilité et l'aide précieuse qu'elle m'a apportée. Sa compréhension, son soutien et son suivi m'ont permis de mener à bien ce travail. Qu'elle trouve ici l'expression de ma sincère gratitude.

Je tiens également à remercier les membres du jury d'avoir consacré une partie de leur temps à la lecture de ce mémoire et pour l'intérêt qu'ils ont porté à ce travail.

Mes remerciements s'étendent à tous mes enseignants du département d'Informatique de l'Université Abderrahmane Mira de Béjaïa.

Je remercie enfin toutes les personnes qui ont contribué de près ou de loin à l'accomplissement de ce travail.

Dédicaces

Je tiens sincèrement à dédier ce modeste travail à la personne la plus chère à mon cœur, ma MAMAN. Elle qui a tant fait pour nous et à qui je dois tous mes succès. A mon PAPA, mon modèle de courage et de sacrifices. Tout au long de sa vie, il n'a su ménager ses efforts pour notre bien. A ma sœur adorée *Ahlem*, qui m'apporte chaque jour un soutien indéniable. A la mémoire de mon unique grand-père *Braham* parti trop tôt. A ma meilleure amie et alter ego *Tina*. A toutes les personnes que je porte fort dans mon cœur et qui sauront se reconnaître.

♡

Table des matières

Table des figures

Liste des tableaux

Liste des acronymes

AP	Application Provider
AT	Assistive Technology
CH	Cluster Head
CL-PKC	Certificateless Public Key Cryptography
DES	Data Encryption Standard
DoS	Denial of Service
DR	Detection Rate
ECC	Elliptic Curve Cryptography
FAR	False Acceptance Rate
FFT	Fast Fourier Transform
FRR	False Rejection Rate
HMAC	Hash-based Message Authentication Code
IBE	Identity-Based Encryption
IJS	Improved Jules Sudan
IPI	Inter-Pulse-Interval
KDF	Key Derivation Function
KGC	Key Generation Center
MAC	Message Authentication Code
MD5	Message Digest 5
MEMS	Micro Electro Mechanical Systems
NM	Network Manager
PDA	Personal Digital Assistant
PV	Physiological Value
RSSI	Received Signal Strength Indication
TA	Trusted Authority
WBAN	Wireless Body Area Network
WSN	Wireless Sensor Network

Introduction générale

L'essor des nouvelles technologies ainsi que les progrès récents survenus dans les communications sans fil et les systèmes micro-électro-mécaniques (MEMS - *Micro-Electro-Mechanical Systems*) ont permis la réalisation de capteurs à faible puissance, intelligents, miniaturisés et autonomes placés et/ou implantés dans le corps humain afin de surveiller certains signes vitaux tels que la température, le rythme cardiaque, la pression artérielle, la saturation en oxygène, etc. Ce nouveau domaine de recherche appelé « *réseaux corporels sans fil* » ou « *Wireless Body Area Networks* (WBANs) » [2] représente un atout majeur dans la conception d'applications ubiquitaires largement utilisées pour la surveillance médicale à temps réel, les divertissements, les besoins militaires, etc. et ce, sans entraver les activités de l'utilisateur.

Les WBANs recèlent un énorme potentiel pour révolutionner le domaine médical en fournissant une surveillance en temps réel des patients, un diagnostic précoce et une possibilité de délivrer des médicaments aux malades et d'intervenir le plus rapidement possible dans les situations d'urgence. Dans de telles applications, les capteurs peuvent recueillir des informations sur l'état de santé d'un patient, les transmettre à une unité de traitement locale (ou point de collecte) dénommée *sink*, qui se chargera ensuite de relayer les données médicales en temps réel à un hôpital ou tout autre établissement de santé. La sécurité dans les WBANs est donc très importante tant les données collectées sont sensibles et directement associées à un patient particulier [15]. Ainsi, afin de garantir une collecte et une transmission fiables de ces informations critiques, il est essentiel d'assurer l'authentification des nœuds du WBAN pour empêcher un attaquant d'usurper l'identité d'un capteur légitime et d'injecter de fausses données pouvant mettre en péril la vie du patient.

Dans ce contexte, de nombreux travaux de recherche portent sur l'utilisation de la cryptographie pour la mise en œuvre de mécanismes d'authentification dans les WBANs. En raison de diverses contraintes de ressources telles que l'énergie, l'espace mémoire, la capacité de calcul, etc., les solutions proposées pour les réseaux de capteurs sans fil (WSN - *Wireless Sensor Network*) ne sont pas adaptées aux WBANs [4]. S'éloignant des systèmes classiques de génération de clés, les chercheurs se sont servis de la nature aléatoire et variante dans le temps des signaux physiologiques pour générer des clés cryptographiques symétriques permettant de sécuriser les communications dans le réseau tout en assurant l'authentification des capteurs. D'autres travaux se sont basés sur la cryptographie à clés publiques et sur la difficulté à résoudre certains problèmes calculatoires, comme le logarithme discret, afin de gérer la distribution des clés de chiffrement utilisées pour sécuriser les communications et authentifier les nœuds capteurs.

Notre contribution consiste à proposer un système d'authentification d'équipements étrangers dans un réseau corporel sans fil. Le protocole proposé est conçu pour déterminer si un nœud capteur se trouvant à portée de communication, est déployé ou non, sur le corps d'un patient. La résolution de ce problème présentera des avantages très importants. Le réseau économisera considérablement de l'énergie en mettant de côté les outils d'authentification cryptographiques traditionnels qui sont consommateurs en ressources, tant en matière de charge de calcul qu'en charge de communication. Il fournira également une gestion plus efficace du flux de données échangées entre les capteurs si des patients se trouvent à proximité. Pour ce faire, nous nous basons sur le changement de postures du corps humain durant les activités quotidiennes pour développer un modèle de mouvements des nœuds capteurs qui sera utilisé pour déterminer la position de chaque capteur à n'importe quel instant et ainsi identifier les équipements étrangers au WBAN déployé sur le corps du patient. L'évaluation de performances du protocole proposé est réalisée par des simulations en le comparant à d'autres protocoles d'authentification existants dans la littérature.

Ce mémoire est organisé en quatre chapitres répartis en deux parties principales : une partie état de l'art et une partie contribution. La partie état de l'art présente les WBANs et leurs domaines d'application ainsi qu'une discussion critique de certains travaux de recherche concernant la sécurité dans ces réseaux. La partie contribution expose notre proposition pour l'authentification des capteurs dans les WBANs. Dans le chapitre 1, nous décrivons les WBANs, leur architecture générale et leurs spécificités par rapport aux WSNs. Nous présentons également les domaines d'application des WBANs, notamment les avantages apportés dans le domaine médical. Les principales contraintes et exigences de sécurité liées aux WBANs sont finalement discutées en particulier dans les applications de surveillance médicale à distance. Dans le chapitre 2, nous discutons certains travaux de recherche concernant les mécanismes de sécurité dans les WBANs, notamment les systèmes de gestion de clés et d'authentification. Une comparaison des différentes approches est ensuite présentée pour mettre en évidence leurs points forts et points faibles en termes de sécurité mais aussi de charges de stockage, de calcul et de communication. Dans le chapitre 3, nous présentons notre contribution pour l'authentification des nœuds capteurs dans les WBANs en détaillant les étapes du protocole et en fournissant une analyse théorique de ses propriétés de sécurité. Dans le chapitre 4, nous exposons les résultats obtenus suite à l'évaluation des performances de notre protocole et montrons l'intérêt de la solution proposée. Enfin, nous clôturons ce mémoire par une conclusion générale résumant les points essentiels de notre travail et dégageons quelques perspectives envisagées pour la solution proposée.

Chapitre 1

Réseaux corporels sans fil

1.1 Introduction

Les progrès réalisés ces dernières décennies dans le domaine des systèmes micro-électro-mécaniques et de la technologie sans fil ont permis la réalisation des réseaux corporels sans fil. Ces réseaux représentent un atout majeur dans la conception d'applications ubiquitaires largement utilisées pour la surveillance médicale à temps réel, les divertissements, les besoins militaires et ce, sans contraindre les activités de l'utilisateur. Dans ce chapitre, nous présenterons les WBANs tout en effectuant une comparaison avec les WSNs. Nous passerons ensuite en revue les différents domaines d'application des WBANs. Puis, nous décrirons l'architecture générale de ces réseaux. Enfin, nous examinerons les principales contraintes et exigences de sécurité liées aux WBANs notamment dans le domaine médical.

1.2 Définitions

Définition 1.2.1. Un réseau de capteurs sans fil est considéré comme un type particulier de réseaux ad hoc où des nœuds capteurs couvrent une zone d'intérêt afin de mesurer une grandeur physique ou surveiller un évènement et 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 [25].

Définition 1.2.2. Un réseau de capteurs corporels sans fil est un réseau constitué d'un ensemble de capteurs et actionneurs miniaturisés portables ou implantés dans le corps humain utilisés pour assurer la surveillance continue des signes physiologiques (pression artérielle, fréquence cardiaque, température, etc.) [16].

1.3 Comparaison entre les WBANs et les WSNs

Nous présentons dans ce qui suit, les principales différences entre les WBANs et les WSNs qui sont classifiées selon certains critères. La Table 1.1 [4] résume ces différences.

Critère de comparaison	WBAN	WSN
Densité	Distribution dense limitée par la taille du corps humain	Quelques uns à plusieurs milliers de nœuds
Déploiement	Sur le corps humain	Dans des endroits difficilement accessibles
Taille des capteurs	Miniaturisation nécessaire	Aucune limitation
Remplacement des capteurs	Difficile à réaliser (cas d'un capteur implanté)	Peut être réalisé
Changement de batteries	Difficile à réaliser	Peut être réalisé
Mobilité des nœuds	Nœuds mobiles	Nœuds mobiles ou stationnaires
Débit de données	Activités périodiques	Activités irrégulières
Niveau de sécurité	Niveau plus élevé pour protéger les données des patients	Niveau bas (dépend de l'application)

TABLE 1.1 – Différences entre les WBANs et les WSNs.

1.4 Domaines d'application des WBANs

Les applications des WBANs couvrent un grand nombre de domaines tels que le domaine militaire, les soins de santé, le sport, les divertissements et bien d'autres encore. La norme IEEE 802.15.6 catégorise les applications du WBAN en deux principaux domaines : médical et non médical [4].

1.4.1 Domaine médical

Les WBANs possèdent un énorme potentiel pour révolutionner l'avenir de la surveillance médicale en diagnostiquant de nombreuses maladies mortelles et en fournissant aux patients une surveillance en temps réel. Dans cette section, nous passons en revue quelques exemples d'application des WBANs dans le domaine des soins de santé [3].

- **Surveillance en temps réel des patients**

Une des applications clés des WBANs est leur utilisation dans la surveillance médicale. Des capteurs médicaux sont placés et/ou implantés dans le corps du patient afin de mesurer ses paramètres physiologiques. Ces données mesurées sont ensuite envoyées à une équipe médicale via un réseau haut débit afin qu'elle puisse surveiller l'état de santé du patient et alerter le cas échéant les services d'urgence. Il est même possible d'injecter un médicament au moyen d'un actionneur disposé près du corps.

- **Assistance aux personnes handicapées**

Beaucoup de personnes souffrent d'un handicap tel que la paralysie, la cécité, etc. et dépendent fortement de leurs familles, du gouvernement ou de toute organisation non gouvernementale. Les technologies d'assistance (AT - *Assistive Technology*) visent à pallier aux effets du handicap en permettant aux personnes concernées de devenir plus autonomes dans leur vie, participer à des activités communautaires et obtenir un emploi.

- **Surveillance de l'état de santé des animaux**

Au cours de ces dernières années, la qualité de la viande s'est nettement améliorée mais dû au manque de soins de santé délivrés aux animaux souffrant de maladies respiratoires, une variété de maladies gastro-intestinales et métaboliques sont apparues [27]. Les capteurs portables permettent de bénéficier d'un diagnostic en temps réel de l'état de santé de l'animal. La détection précoce des maladies transmissibles pourrait être utile afin d'éviter les pertes financières énormes dans l'industrie de l'agriculture animale.

- **Urgence médicale**

Un autre scénario médical est le cas d'urgence ou de catastrophe. Les patients sont équipés de petits capteurs permettant d'aider les équipes de secours et les médecins à gérer d'une façon efficace un nombre plus élevé de victimes. Par exemple, le premier secouriste qui arrive dans une zone sinistrée, placera un capteur sur chaque patient. Ce capteur peut envoyer les signes vitaux et l'emplacement de chaque patient à l'équipe médicale la plus proche.

1.4.2 Domaine non médical

Dans ce qui suit, nous présentons quelques applications non médicales des WBANs [4].

- **Domaine militaire**

Les réseaux de capteurs corporels sans fil sont utilisés pour surveiller les signes vitaux des soldats sur le champ de bataille et pour éviter les embuscades. L'utilisation des WBANs dans des environnements hostiles peut contribuer à réduire la probabilité de blessure tout en améliorant la surveillance et les soins le cas échéant.

- **Domaine sportif**

Dans le domaine du sport, les WBANs sont utilisés pour l'entrainement, la surveillance, l'auto-évaluation et l'amélioration des performances des sportifs. Les différents capteurs permettent la lecture de paramètres physiologiques tels que la fréquence cardiaque, la distance parcourue, l'oxymétrie et l'accélération.

- **Domaine des jeux et des divertissements**

Cette catégorie comprend les applications de jeux et les réseaux sociaux. Dans le domaine des jeux vidéo, par exemple, l'avatar d'un monde virtuel prend les positions réelles du joueur grâce aux capteurs de mouvement qui l'équipe.

- **Urgence non médicale**

Des capteurs placés dans une maison, par exemple, sont capables de détecter une urgence non médicale comme un incendie ou un gaz inflammable, voire toxique, présent dans la maison et doivent communiquer d'urgence ces informations à des appareils portés sur le corps pour avertir l'utilisateur de l'état d'urgence.

1.5 Architecture générale d'un système WBAN de surveillance médicale

La Figure 1.1 illustre l'architecture générale d'un système WBAN de surveillance médicale, où plusieurs types de capteurs corporels envoient leurs données mesurées à un serveur par le biais d'une connexion sans fil. Ces données sont ensuite transmises (via Internet, par exemple) à une équipe médicale pour obtenir un diagnostic en temps réel, à une base de données médicale pour être enregistrées, ou bien à un équipement correspondant qui émet une alerte d'urgence.

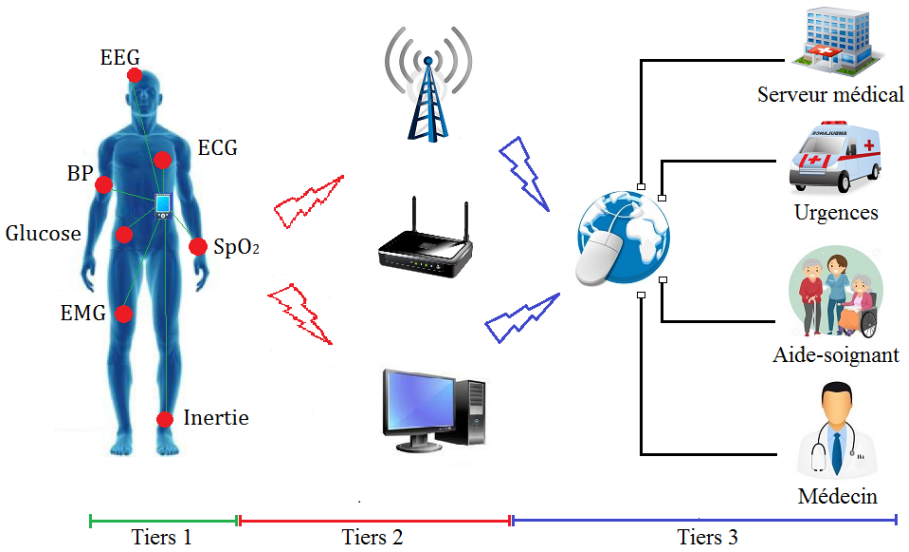

FIGURE 1.1 – Architecture générale d'un système WBAN de surveillance médicale.

L'architecture des communications dans un WBAN peut être décomposée en trois (03) tiers [4] :

- **Tiers 1 : communications intra-WBAN**

Ce tiers concerne les communications se déroulant autour du corps humain, à savoir les communications entre les différents capteurs corporels ainsi que les communications entre les capteurs corporels et le point de collecte (serveur personnel ou nœud coordinateur). Ce dernier peut être un dispositif caractérisé par une puissance de calcul et une réserve d'énergie plus importantes par rapport aux capteurs corporels.

- **Tiers 2 : communications inter-WBAN**

Ce tiers se compose des communications entre le point 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.

- **Tiers 3 : communications extra-WBAN**

Ce tiers rassemble les 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 extra-WBAN peuvent améliorer la surveillance médicale en permettant aux personnels de la santé (médecins et infirmières) d'accéder à distance aux informations médicales des patients et d'intervenir dans les cas d'urgence.

1.6 Contraintes et exigences de sécurité dans les WBANs

Dans cette section, nous décrivons les contraintes et exigences de sécurité auxquelles les WBANs doivent faire face.

1.6.1 Contraintes des WBANs

Les WBANs possèdent des caractéristiques et des contraintes critiques comparées aux réseaux de capteurs traditionnels rendant l'exécution des mesures de sécurité existantes irréalistes. 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 [23]. Ces contraintes qui rendent la conception de protocoles et de mécanismes de sécurité plus complexe, sont classées en deux catégories : matérielles et réseau [19].

1.6.1.1 Contraintes matérielles

Toutes les approches de sécurité nécessitent une certaine quantité de ressources pour leur mise en œuvre, dont une mémoire, de l'espace pour le code et de l'énergie pour alimenter le capteur [23]. Toutefois, ces ressources sont très limitées dans un minuscule capteur sans fil notamment dans ceux implantés dans le corps humain.

- **Mémoire et espace de stockage limités**

Un capteur est un petit dispositif avec une mémoire très réduite et un espace de stockage limité. De ce fait, pour construire un mécanisme de sécurité efficace, il est nécessaire de limiter la taille du code de l'algorithme [23].

- **Énergie limitée**

L'énergie est un autre facteur important à considérer lors de la conception de mécanismes de sécurité. Par exemple, dans le cas de capteurs implantés dans le corps humain, il est très important de limiter la consommation en énergie et de prolonger la durée de vie de la batterie. De ce fait, ajouter des mesures de sécurité a nécessairement un impact significatif sur la consommation en énergie ; par exemple, exécuter les fonctions de chiffrement et de déchiffrement, échanger des clés, etc. [19].

- **Capacité de calcul limitée**

Malgré les progrès réalisés 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 coûteux en ressources CPU [20].

- **Portée radio limitée et faible débit**

La majorité des capteurs possèdent une portée radio de quelques dizaines de mètres variable selon l'environnement et la fréquence radio utilisée. De plus, le débit actuel dans les réseaux corporels sans fil ne dépasse pas les quelques dizaines de mégabits par seconde [19].

1.6.1.2 Contraintes réseau

Les communications sans fil sont en général incertaines. En effet, 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 [19].

1.6.2 Exigences de sécurité

Bien que les questions de sécurité soient une priorité dans la plupart des réseaux, peu d'études ont été effectuées dans ce domaine pour les WBANs [4]. En outre, en raison de contraintes strictes liées aux ressources, notamment en termes de puissance, de mémoire, de charge de communication et de capacité de calcul ainsi qu'aux failles de sécurité inhérentes, les spécifications de sécurité proposées pour les WSNs ne sont pas applicables aux WBANs. Le déploiement pratique des WBANs et l'intégration de mécanismes de sécurité nécessitent une connaissance des exigences de sécurité que nous citons ci-après [4].

1.6.2.1 Disponibilité

La disponibilité des données relatives à l'utilisateur doit être assurée à tout moment en particulier dans les applications liées à la surveillance médicale. En effet, une attaque contre la disponibilité dans les WBANs pourrait être, par exemple, la capture et la désactivation d'un nœud de l'ECG conduisant à une fin tragique pour le patient. Par conséquent, la maintenance et la capacité de passer à un autre WBAN en cas de perte de disponibilité est essentielle.

1.6.2.2 Confidentialité des données

Dans les applications médicales, les nœuds du WBAN transmettent des informations sensibles sur l'état de santé d'un patient. Ces informations critiques peuvent être espionnées durant les communications provoquant une quantité considérable de dommages au patient si elles sont utilisées à des fins illégales. La confidentialité des données peut être assurée grâce au chiffrement des données du patient et ce, en utilisant une clé partagée sur un canal de communication sécurisé entre les nœuds du WBAN et leur point de collecte.

1.6.2.3 Authentification des données

Les applications médicales et non médicales requièrent une authentification des données. Les nœuds du WBAN et le point de collecte doivent vérifier que les données proviennent bien d'une entité de confiance et non d'un adversaire. Pour ce faire, ils doivent calculer un code d'authentification de message (MAC - *Message Authentication Code*) pour toutes les données en partageant une clé secrète. Si le code calculé est correct alors le point de collecte saura que le message reçu a bien été envoyé par un nœud légitime du réseau.

1.6.2.4 Intégrité des données

Les informations transmises dans un WBAN non sécurisé peuvent être altérées. Un intrus malintentionné est capable de modifier les données relatives à un patient avant qu'elles n'atteignent le point de collecte mettant ainsi en danger la santé du patient et peut être même sa vie. Par conséquent, le point de collecte doit être sûr que les données reçues n'ont pas été altérées et ce, en utilisant des protocoles d'authentification de données appropriés.

1.6.2.5 Fraîcheur des données

Afin d'assurer l'intégrité et la confidentialité des données, il est nécessaire d'utiliser des techniques de fraîcheur de données. Un adversaire est capable de capturer des données durant les transmissions et les rejouer ultérieurement pour créer une confusion au niveau du point de collecte. La fraîcheur des données garantit que les données ne sont pas réutilisées et que les trames sont ordonnées.

1.7 Conclusion

Les WBANs représentent une technologie prometteuse pouvant révolutionner les applications de soins de santé et de divertissements de la prochaine génération. Cependant, ces réseaux apportent un nouvel ensemble de défis notamment en termes de sécurité. Dans ce chapitre, nous avons présenté les WBANs. Nous avons ensuite décrit certains de leurs domaines d'application. Puis, nous avons présenté l'architecture générale de ces réseaux. Enfin, nous avons cité les contraintes et les principales exigences de sécurité dans les WBANs et plus particulièrement dans les applications de surveillance médicale. Le chapitre suivant sera consacré à un état de l'art sur les mécanismes de sécurité dans les WBANs.

Chapitre 2

État de l'art sur les mécanismes de sécurité dans les WBANs

2.1 Introduction

Assurer la sécurité et la confidentialité des données dans les WBANs représente un défi majeur, non encore résolu, dû aux contraintes strictes liées aux ressources des dispositifs du WBAN et au besoin de trouver un équilibre entre sécurité et praticité. Ce chapitre sera consacré à la présentation et l'étude critique de quelques solutions existantes, afin d'offrir aux WBANs une meilleure sécurité. Pour cela, nous commencerons par déterminer les critères d'analyse, suivi par une classification des solutions étudiées, puis nous présenterons et discuterons chaque solution. Enfin, nous conclurons ce chapitre par une comparaison des travaux analysés et une synthèse.

2.2 Critères d'évaluation des solutions existantes

Afin de bien évaluer les travaux de recherche étudiés, nous avons établi certains critères jugés pertinents, compte tenu des besoins et contraintes liés aux réseaux corporels sans fil. Nous nous intéresserons de ce fait au coût en termes de stockage, de calcul et de communication, à la résistance aux attaques ainsi qu'à la convivialité du système.

2.2.1 Charge de stockage

La capacité de stockage des nœuds capteurs est relativement faible, en particulier pour ceux implantés dans le corps humain. Il est donc nécessaire de limiter le nombre et la taille des paramètres cryptographiques (clés de chiffrement, algorithmes de hachage, etc.) à stocker.

2.2.2 Charge de calcul

Étant donné la miniaturisation des nœuds capteurs et le manque de puissance de calcul dont souffrent ces derniers, il est recommandé d'utiliser des algorithmes cryptographiques moins complexes. En effet, la charge de calcul influe directement sur l'énergie consommée.

2.2.3 Charge de communication

Dans un réseau de capteurs sans fil, les communications sont les opérations les plus coûteuses en termes d'énergie. Il est donc nécessaire de limiter la charge de communication entre les capteurs en limitant le nombre de messages échangés entre les nœuds.

2.2.4 Résistance aux attaques

En raison des données sensibles échangées par les capteurs, un mécanisme de sécurité développé pour les WBANs doit être résistant aux attaques et répondre aux principales exigences de sécurité.

2.2.5 Convivialité

Nous définissons un mécanisme de sécurité « convivial » comme étant un mécanisme pouvant fonctionner directement au déploiement du réseau de manière à respecter le paradigme *plug and play*[1] ; avec un minimum de procédures d'initialisation (idéalement aucune). Cette propriété est d'autant plus importante dans les WBANs, où les utilisateurs pouvant se trouver dans une situation d'urgence sont incapables d'effectuer ces procédures.

2.3 Classification des travaux étudiés

Après avoir analysé les travaux récoltés, il nous est apparu qu'une classification était nécessaire afin de répertorier les différentes approches suivies. La Table 2.1 représente notre classification des différentes solutions proposées pour le problème de sécurité dans les réseaux corporels sans fil.

Classification des travaux étudiés	
Solutions basées sur les signaux physiologiques	- Mana et al. [12] - Venkatasubramanian et al. [22] - Venkatasubramanian et al. [17] - Rajasekaran et al. [10] - Zhang et al. [11]
Solutions basées sur le clustering	- Zhao et al. [7] - Ali et al. [5]
Solutions basées sur la cryptographie à courbe elliptique	- Pan et al. [9]
Solutions basées sur une approche polynomiale	- He et al. [6]
Solutions basées sur la cryptographie à base d'identité	- Tan et al. [21]
Solutions basées sur la cryptographie à clés publiques sans certificats	- Liu et al. [8]

TABLE 2.1 – Classification des travaux étudiés.

1. Procédure qui permet une installation requérant un minimum d'intervention de la part de l'utilisateur.

Les solutions basées sur les signaux physiologiques utilisent les *signaux mesurés* par les capteurs (électrocardiogramme, variabilité de la fréquence cardiaque, etc.) pour extraire des clés de chiffrement nécessaires à la sécurité des communications inter-capteurs. Les solutions basées sur le clustering utilisent une structure de réseau organisée en *clusters* afin d'établir des clés symétriques entre les nœuds capteurs. Les solutions basées sur la cryptographie à courbe elliptique reposent sur la difficulté à résoudre un problème calculatoire connu qui est *le logarithme discret sur la courbe elliptique* afin de distribuer la clé de chiffrement utilisée pour sécuriser les échanges entre les capteurs du réseau. Les solutions basées sur une approche polynomiale utilisent un *polynôme pré-distribué* pour dériver la clé symétrique partagée entre deux capteurs. Dans les solutions basées sur la cryptographie à base d'identité, la *clé publique* utilisée pour le chiffrement des données peut être choisie librement. Une *autorité de confiance* se chargera ensuite de dériver la *clé privée* correspondante qui servira au déchiffrement des messages. Dans les solutions basées sur la cryptographie à clés publiques sans certificats, l'autorité de confiance ne connait pas la clé privée des utilisateurs. Elle génère uniquement une *clé privée partielle* selon l'identité de l'utilisateur qui sera utilisée par ce dernier pour générer sa véritable clé privée.

2.4 Étude critique des travaux

Protéger les données relatives aux patients est d'une importance capitale dans les WBANs. Plusieurs recherches ont été menées afin de réaliser un mécanisme de sécurité qui répond aux exigences de ces réseaux. Dans ce qui suit, nous étudions une partie des travaux réalisés dans ce contexte.

2.4.1 Solutions basées sur les signaux physiologiques

2.4.1.1 Trust Key Management Scheme for Wireless Body Area Network

Mana et al. [12] ont proposé un système visant à sécuriser l'échange de clés entre les nœuds capteurs et la station de base, ainsi que les communications entre les capteurs eux-mêmes. Ce système utilise des points de repères essentiels dans un battement de cœur tels que des intervalles de temps, des ondes particulières et leurs amplitudes pour extraire la séquence binaire représentant la clé. Pour communiquer avec la station de base, les nœuds les plus proches de cette dernière agissent comme une passerelle. La station de base possède une paire de clés publique/privée, où la clé publique est connue par tout les nœuds capteurs avant le déploiement, et se charge de générer les clés pour sécuriser les communications entre les capteurs et leur passerelle. Le protocole se déroule en quatre (04) phases comme décrit ci-après.

- **Phase de génération de la clé**

Un nœud A souhaitant rejoindre le réseau commence par calculer une clé $Biokey_A$ en utilisant le signal ECG (électrocardiogramme [2]). Bien que la suite binaire générée soit déjà adaptée à un système de chiffrement symétrique et par souci de confidentialité, une fonction de morphing $M(.)$ est utilisée afin d'enlever toute corrélation entre la clé générée et les données médicales d'origine.

$$K_{sessionA} = M(Biokey_A).$$

- **Phase d'échange de la clé**

Le nœud A diffuse sa requête chiffrée avec la clé publique de la station de base (SB) qui passe par la passerelle, le nœud B par exemple (voir la Figure 2.1).

$$A \rightarrow B : Id_A, E_{pub}(Biokey_A), MAC(K_{sessionA}, Id_A||Biokey_A).$$

A la réception, le nœud B rajoute ses informations et transmet le message à la station de base.

$$B \rightarrow SB : Id_A, E_{pub}(Biokey_A), MAC(K_{sessionA}, Id_A||Biokey_A), Id_B, E_{KsessionB}(N_B),$$

où : N_B est un nonce généré par le nœud B.

Une fois le message reçu, la station de base effectue les vérifications nécessaires puis envoie au nœud A les informations requises pour rejoindre le réseau.

$$SB \rightarrow A : E_{KsessionA}(Ok, cmp_A, Id_B, K_{A-B}),$$

où : cmp_A est un compteur initialisé à une valeur aléatoire ;
K_{A-B} est la clé d'authentification informant le nœud A que sa passerelle pour atteindre la station de base est le nœud B ($K_{A-B} = M(K_{sessionB}||N_B)$).

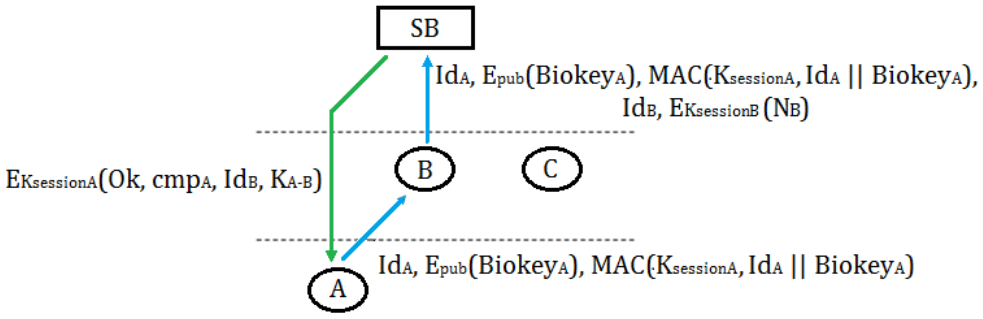

FIGURE 2.1 – Le nœud A initie l'échange de clés.

2. Enregistrement de l'activité électrique du cœur nécessaire à ses contractions.

- **Phase d'authentification de la clé**

En recevant l'identifiant Id_B et la clé K_{A-B}, le nœud A tente de s'authentifier auprès de sa passerelle B comme suit :

$$A \rightarrow B : Id_A, E_{KA-B}(N'_A);$$
$$B \rightarrow A : Id_B, E_{KA-B}(N'_A, N'_B);$$
$$A \rightarrow B : Id_A, E_{KA-B}(N'_B).$$

- **Phase de mise à jour de la clé**

Les WBANs pouvant être déployés pour plusieurs jours voire plusieurs mois, la mise à jour des clés est nécessaire afin de prévenir les attaques à long terme visant à extraire les clés de chiffrement en analysant le trafic sur le réseau. Pour cela, la station de base diffuse une requête de mise à jour à tous les nœuds capteurs qui, une fois reçue, génèrent une nouvelle clé *Biokey'*.

⁎ **Discussion et critiques**

Le système proposé est résistant aux attaques ; en effet, l'utilisation de compteurs permet d'éviter l'attaque par rejeu et garantit la fraîcheur des données. De plus, l'authentification mutuelle entre les différents nœuds du réseau est assurée en utilisant des clés de session générées à partir du signal ECG. Un attaquant ne pouvant mesurer le signal ECG du patient portant le WBAN, il ne peut donc pas connaitre directement les clés utilisées et se faire passer pour un nœud légitime. Néanmoins, la charge de communication s'avère élevée pour les nœuds les plus proches de la station de base qui servent de relais pour les autres nœuds. Le protocole nécessite également de l'espace mémoire pour sauvegarder les différentes clés ; la clé publique de la station de base, les clés de session entre chaque nœud et la station de base et les clés de communication entre les capteurs les plus éloignés de la station de base et leur passerelle respective.

2.4.1.2 EKG-based Key Agreement in Body Sensor Networks (EKA)

Préserver la vie privée d'une personne, d'une manière efficace, est très important dans des infrastructures critiques telles que les réseaux corporels sans fil. Venkatasubramanian et al. [22], ont proposé un système de gestion de clés permettant à deux capteurs de se mettre d'accord sur une clé commune générée à partir des signaux de l'électrocardiogramme. Ce protocole vise à sécuriser les communications entre les différents nœuds tout en suivant le paradigme *plug and play* ; assurer la sécurité du WBAN sans recourir à une pré-configuration (pré-déploiement) du réseau. Pour établir une communication sécurisée en utilisant le signal ECG, les deux entités communicantes doivent échantillonner le signal simultanément, à une fréquence d'échantillonnage spécifique et durant une période de temps fixe (125Hz et 5s respectivement), produisant ainsi *625 échantillons*. Ces échantillons sont

ensuite divisés en 5 parties de 125 échantillons chacune. La Transformée de Fourier Rapide (FFT - *Fast Fourier Transform*) est appliquée sur chaque partie pour obtenir un vecteur F de *320 coefficients* en concaténant les 64 premiers coefficients FFT de chaque partie. Pour générer une clé à partir du vecteur F, ce dernier est divisé en *20 blocs* de 16 coefficients chacun. Chaque bloc est quantifié afin d'obtenir un flux binaire, où la quantification d'un coefficient produit une valeur de 4 bits. Au final, nous obtenons 20 blocs quantifiés de *64 bits* chacun au niveau de chaque capteur communicant. Une fois les blocs obtenus, les deux nœuds peuvent entamer le processus de génération de la clé qui se déroule comme décrit ci-après.

- **Phase d'engagement**

Durant cette phase, les nœuds s'échangent les blocs générés. Soit B_{S1} l'ensemble des blocs générés par le nœud S_1 où $B_{S1} = \{b_1^1, b_2^1, \cdots, b_{20}^1\}$. Ces blocs étant la base pour obtenir la clé finale, ils ne peuvent donc pas être échangés en clair. C'est pourquoi, chaque bloc sera haché, en utilisant une fonction de hachage à sens unique (SHA-256), avant d'être transmis.

$S_1 \rightarrow S_2 : \langle\, ID_1, \mathrm{N}, \mathrm{hash}(b_1^1, \mathrm{N}), \cdots, \mathrm{hash}(b_{20}^1, \mathrm{N}), \mathrm{MAC}(K_R, ID_1, \mathrm{N}, \mathrm{hash}(b_1^1, \mathrm{N}), \cdots, \mathrm{hash}(b_{20}^1, \mathrm{N}))\,\rangle\,;$

$S_2 \rightarrow S_1 : \langle\, ID_2, \mathrm{N}', \mathrm{hash}(b_1^2, \mathrm{N}'), \cdots, \mathrm{hash}(b_{20}^2, \mathrm{N}'), \mathrm{MAC}(K_R', ID_2, \mathrm{N}', \mathrm{hash}(b_1^2, \mathrm{N}'), \cdots, \mathrm{hash}(b_{20}^2, \mathrm{N}'))\,\rangle,$

où : N et N′ sont des nonces ;
K_R et K_R' des clés générées aléatoirement par les nœuds S_1 et S_2 respectivement.

- **Phase de traitement**

Une fois les blocs hachés échangés, chaque nœud arrange les valeurs hachées reçues et le haché des blocs locaux en deux matrices 20×64 (U et V respectivement). Les deux nœuds calculent ensuite une matrice W où un élément W[i,j] représente la distance de Hamming entre la i^{eme} ligne de la matrice U et la j^{eme} ligne de la matrice V. La matrice W est utilisée pour identifier les indices des blocs identiques au niveau de chaque capteur qui serviront à générer la clé commune K de 128 bits. Maintenant que la clé est générée par chaque capteur, ils peuvent vérifier l'intégrité des blocs reçus précédemment en s'échangeant les messages suivants :

$S_1 \rightarrow S_2 : \langle\, \mathrm{G} = K_R \oplus K_A, \mathrm{MAC}(K_A, \mathrm{G})\,\rangle\,;$
$S_2 \rightarrow S_1 : \langle\, \mathrm{G}' = K_R' \oplus K_B, \mathrm{MAC}(K_B, \mathrm{G}')\,\rangle.$

Les clés K_A et K_B sont les clés générées lors de la phase de traitement et sont supposées identiques.

Les capteurs S_1 et S_2 commencent par vérifier le MAC reçu en utilisant leurs clés K_A et K_B respectivement. Si la vérification réussit, ils extraient les clés K'_R et K_R respectivement puis vérifient l'intégrité des blocs reçus lors de la phase d'engagement.

⁎ Discussion et critiques

Le protocole proposé nécessite peu de communications entre les capteurs pour réussir à établir une clé commune. Le caractère aléatoire des clés générées rend difficile pour un adversaire de deviner la clé utilisée. De plus, si un adversaire tente de former une clé avec un nœud arbitraire en émettant d'anciens messages, l'attaque échouera grâce aux nonces et au fait que les clés générées changent à chaque fois qu'un nœud tente d'établir une clé commune avec un autre nœud. Cependant, appliquer une fonction de hachage sur des blocs de 64 bits rend une attaque par force brute facile à réaliser. Enfin, générer la clé commune nécessite beaucoup de calcul.

2.4.1.3 Physiological Value-Based Efficient Usable Security Solutions for Body Sensor Networks (PVS)

Venkatasubramanian et al. [17] ont proposé le système PVS (Physiological Value-based Security) pour sécuriser les communications inter-capteurs dans les WBANs. Ce système consiste à distribuer la clé utilisée pour chiffrer un message donné, avec le message lui-même. En effet, la clé est cachée en utilisant une valeur physiologique (PV), qui peut être le rythme cardiaque, la température, le niveau de glucose dans le sang, etc. Tout d'abord, les deux entités communicantes doivent s'entendre sur une valeur physiologique à mesurer simultanément, ici la valeur utilisée est la Variabilité de la Fréquence Cardiaque (IPI - *Inter Pulse Interval*), les valeurs successives mesurées sont ensuite codées en binaire. Pour chiffrer les données qu'il souhaite transmettre, l'émetteur utilise une clé qu'il génère aléatoirement puis la cache grâce à la représentation binaire de la valeur PV mesurée (il effectue un XOR entre les deux). Il transmet alors la clé cachée et les données encryptées comme étant un seul message. A la réception, le nœud récepteur récupère la clé cachée, grâce à sa valeur locale de PV, puis décrypte les données reçues.

⁎ Discussion et critiques

En plus d'éliminer le besoin de distribution explicite des clés cryptographiques, le système proposé réduit considérablement la charge de communication entre les capteurs puisque les clés sont distribuées durant la transmission des données, améliorant ainsi l'efficacité du réseau en termes d'énergie. L'efficacité du WBAN en termes de stockage est également améliorée puisqu'une seule mesure de la valeur PV suffit pour sécuriser toutes les communications. Mesurer cette valeur nécessite toutefois une forte synchronisation entre les capteurs afin de réussir à retrouver la clé aléatoire nécessaire au déchiffrement des données reçues.

2.4.1.4 An Efficient and Secure Key Agreement Scheme Using Physiological Signals in Body Area Networks

Rajasekaran et al. [10] ont proposé un système ayant pour objectif d'assurer une communication sécurisée entre les capteurs du WBAN. Pour ce faire, deux nœuds voisins se mettent d'accord sur une clé symétrique partagée, en utilisant les signaux physiologiques obtenus à partir du patient. Émetteur et récepteur se mettent d'accord sur le signal physiologique à mesurer (le protocole utilise le signal ECG) et commencent à l'échantillonner, simultanément, à une même fréquence et pendant la même durée de temps. Le signal échantillonné est alors quantifié et transformé en chaine binaire. Le nœud émetteur utilise ensuite cette chaine pour générer un polynôme *spline cubique*, où la concaténation des coefficients du polynôme forme la clé secrète K, puis ajoute des *points faussés* afin de brouiller l'information et ainsi cacher la clé dans un *coffre-fort* (vault) verrouillé R qu'il transmet au récepteur ; c'est la technique du *Fuzzy Vault*. A la réception, le nœud récepteur déverrouille le coffre et récupère la clé en utilisant le signal ECG mesuré de son côté. En effet, en superposant ses éléments avec ceux de l'émetteur, il sera capable de localiser plusieurs points similaires et pourra ainsi reconstruire le polynôme et donc la clé secrète K (voir la Figure 2.2). Les messages échangés sont alors :

Émetteur $\rightarrow$ Récepteur : ID_E, ID_R, R, N, MAC(K, R||N||ID_E) ;

Récepteur $\rightarrow$ Émetteur : MAC(K, N||ID_E||ID_R).

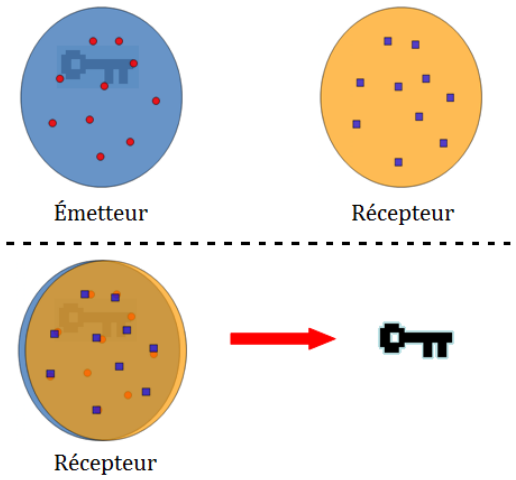

FIGURE 2.2 – Technique du Fuzzy Vault.

⁎ Discussion et critiques

Dans ce protocole, la sécurité du WBAN réside dans la taille de la clé. En utilisant l'interpolation spline cubique, la taille maximale de la clé peut atteindre $64n$ bits avec n le nombre de points utilisés ce qui nécessite un espace mémoire considérable pour stocker la clé. Bien que la technique du Fuzzy Vault nécessite de publier un ensemble de points où certains correspondent à ceux utilisés pour cacher la clé, un intrus malintentionné ne pourra mener une attaque par force brute afin de retrouver la clé secrète car il ne peut mesurer le signal ECG.

2.4.1.5 ECG-Cryptography and Authentication in Body Area Networks (ECG-IJS)

Zhang et al. [11] ont proposé d'utiliser le signal ECG et l'algorithme IJS (Improved Jules Sudan), une version améliorée de l'algorithme du *Fuzzy Vault* [24], pour sécuriser les communications entre les capteurs du WBAN. Le nœud émetteur mesure le signal ECG, extrait une fonction F à partir de ce signal et forme la clé secrète K. Il utilise ensuite la fonction F comme entrée de l'algorithme IJS pour construire un polynôme monique [3] de degré s et calcule les coefficients du polynôme. Il transmet alors au nœud récepteur les données chiffrées avec la clé secrète K, un sous-ensemble des coefficients IJS et un message MAC. Une fois le paquet reçu, le nœud récepteur utilise le signal ECG qu'il a mesuré pour extraire une fonction F' ainsi que le sous-ensemble des coefficients reçu pour retrouver la clé K et déchiffrer les données médicales. Il vérifie ensuite l'authenticité du message en recalculant le MAC et envoie un acquittement (ACK) en cas de succès, le paquet est rejeté dans le cas contraire. Le processus ainsi décrit est représenté par le schéma d'authentification de la Figure 2.3.

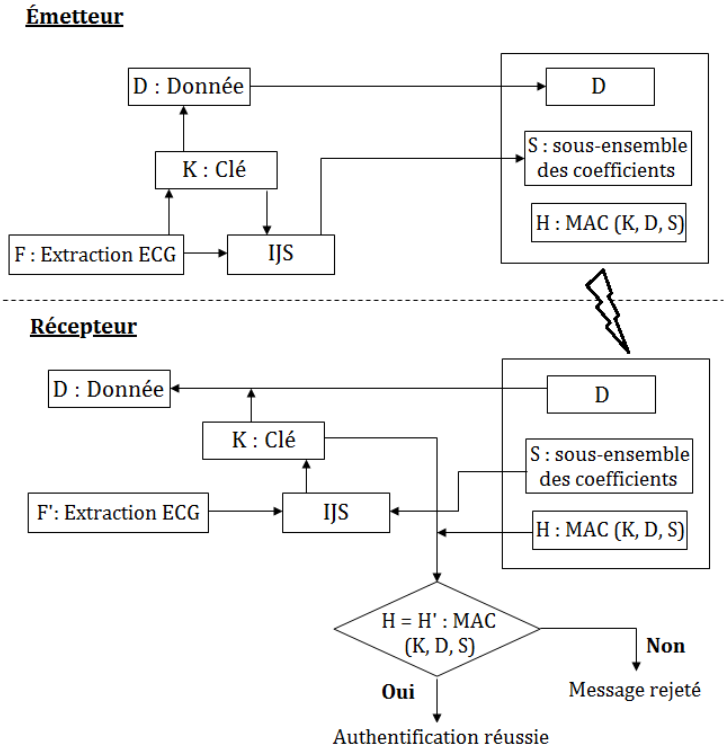

FIGURE 2.3 – Schéma d'authentification ECG-IJS [11].

⁎ Discussion et critiques

Dans le protocole ECG-IJS proposé, les capteurs n'ont besoin de stocker que les coefficients du polynôme généré, et seulement un sous-ensemble de ces coefficients doit être transmis au nœud récepteur. Ainsi, ce système réduit considérablement la charge de stockage et de communication du réseau. De plus, contrairement à la version originale du Fuzzy Vault, l'algorithme IJS n'utilise pas

3. Polynôme unitaire, c'est-à-dire dont le coefficient du terme de plus haut degré est égal à 1.

de points faussés pour cacher la clé secrète K ce qui minimise la charge de calcul. Enfin, le sous-ensemble des coefficients est public car sans une extraction similaire du signal ECG mesuré sur le même patient, un attaquant serait incapable de régénérer la clé K.

2.4.2 Solutions basées sur le clustering

2.4.2.1 An Energy Efficient Key Management Scheme for Body Sensor Networks

Zhao et al. [7] ont proposé d'utiliser une topologie hybride multi-sauts pour deux applications principales des WBANs ; la surveillance médicale et le traitement intelligent. Basé sur cette structure, les auteurs ont proposé un mécanisme de gestion de clés permettant de sécuriser les communications inter-capteurs tout en minimisant la consommation en énergie. La structure du réseau comprend trois (03) types de dispositifs : un PDA (*Personal Digital Assistant*), des nœuds portables et des nœuds implantés. Les nœuds portables sont utilisés comme cluster heads (CH) car ils sont généralement plus grands que les nœuds implantés et possèdent donc plus de ressources en termes d'énergie, de capacités de calcul et de stockage. De plus, le fait qu'ils soient placés sur le corps humain les rend facilement rechargeables. Pour exécuter un traitement intelligent, les nœuds implantés s'organisent en clusters pour échanger des données. Par exemple, sur la Figure 2.4, les nœuds 1, 2, 3 et 4 forment un cluster où le nœud 1 doit recevoir les données pour délivrer des médicaments au patient et le nœud 2 est le cluster head.

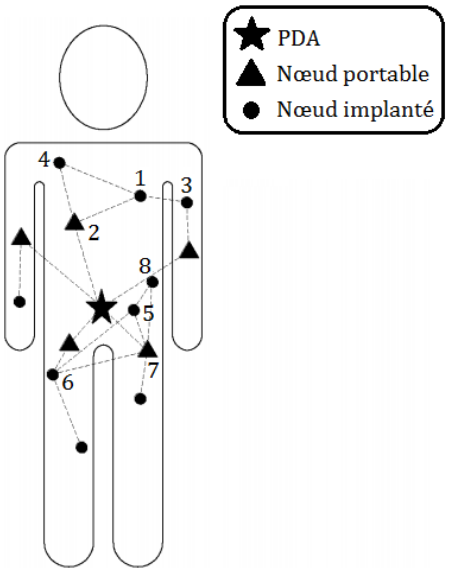

FIGURE 2.4 – Structure hybride multi-sauts du réseau [7].

Avant le déploiement, deux clés K_1, K_2 et une fonction de hachage $H(.)$ sont chargées dans chaque nœud capteur. La portée de transmission d'un nœud implanté étant configurée pour être inférieure à celle de son CH, le nœud capteur doit alors trouver un chemin multi-sauts pour atteindre le CH. Pour ce faire, le nœud commence par diffuser un message pour chercher un CH. Si un CH adjacent (à une distance d'un saut) reçoit le message, il répond avec un message contenant la clé du cluster

K_{CH} chiffrée avec K_1 et son énergie moyenne $\bar{\xi} = \xi_{CH}/nnc$, où ξ_{CH} est l'énergie du CH et nnc le nombre de nœuds dans le cluster. Le nœud implanté pouvant recevoir plusieurs réponses provenant de nœuds portables adjacents, il choisit celui qui a l'énergie maximale. Toutefois, durant une période de temps ts, si le nœud ne reçoit aucune réponse alors il n'y a aucun CH à une distance d'un saut. Le nœud rediffuse alors son message. Durant cette période, si un autre nœud a déjà obtenu la clé du cluster et qu'il reçoit le message diffusé, il répond avec un message contenant son énergie, l'énergie de son CH, le nombre de fois qu'il a été routeur, le nombre de sauts entre lui et son CH et la clé du cluster K_{CH} (voir la Figure 2.5). Le nœud implanté peut, cependant, recevoir plusieurs réponses, il choisit alors le chemin qui a l'énergie maximale et donc le CH correspondant.

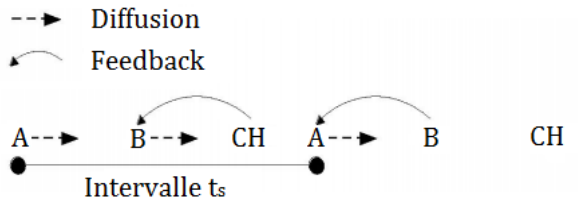

FIGURE 2.5 – Etablissement d'une communication multi-sauts.

Dans certains cas, les nœuds qui n'appartiennent pas au même cluster ont besoin de communiquer, d'où la nécessité de distribuer des clés de session. Si un nœud A souhaite communiquer avec un autre nœud B et que A et B sont à une distance d'un saut alors A génère une clé secrète K_s qu'il chiffre avec la clé K_1 puis chiffre son message avec K_s et envoie le tout au nœud B. Toutefois, si les deux nœuds sont à une plus grande distance alors le nœud B doit d'abord trouvé une route qui mène vers A. Le nœud B diffuse alors un message qui sera transféré par les nœuds intermédiaires jusqu'à atteindre le nœud A qui choisi le chemin avec une énergie maximale et un nombre de sauts minimal suivant l'équation énergétique suivante :

$$\xi' = \left(\sum_{i=1}^{h} \xi_i / nnr_i \right) \; / \; h,$$

où : h est le nombre de sauts d'un chemin de A vers B ;
nnr_i le nombre de fois qu'un nœud i a été routeur.

⁎ Discussion et critiques

Lorsqu'un nœud souhaite générer une clé, il collecte des données biométriques puis les transfèrent sous forme de chaine binaire d. Il calcule ensuite la clé $K = H(K_2, d)$. L'adversaire ne connaissant pas la clé K_2, l'authentification et l'intégrité des données sont ainsi garanties. Néanmoins, le nombre de clés à stocker s'avère considérablement élevé. En effet, ce nombre s'élève à 8 clés pour les cluster heads, ce qui correspond à un espace mémoire de 128 octets, et à 6 clés pour les nœuds implantés soit 96 octets (les clés ont une taille de 128 bits). De plus, les CHs et les nœuds qui servent de routeurs consomment beaucoup d'énergie ; plus le nombre de nœuds dans un cluster augmentera, plus les CHs consommeront d'énergie.

2.4.2.2 A Cluster-Based Key Agreement Scheme Using Keyed Hashing for Body Area Networks

Ali et al. [5] ont proposé un mécanisme d'authentification de messages qui utilise une fonction de hachage avec clé (HMAC-MD5) pour protéger les informations personnelles circulant dans le WBAN. Le modèle de réseau proposé forme un unique cluster où un nœud capteur H-sensor (High-end sensor) joue le rôle du cluster head (CH) et plusieurs nœuds L-sensors (Low-end sensors) des membres du cluster. Les nœuds capteurs commencent par mesurer et échantillonner le signal ECG en utilisant la Transformée par Ondelettes Discrètes (DWT - *Discret Wavelet Transform*), puis quantifient les blocs obtenus en flux binaire. Le H-sensor diffuse ensuite une requête $\{ID_H, data_{Req}, \text{nonce}\}$ à destination des L-sensors qui génèrent la clé partagée avec le H-sensor $K_{H,L}$ en appliquant une fonction de hachage avec clé aux blocs quantifiés comme suit :

$$K_{H,L} = \text{HMAC}((b_1^i, \text{N}), (b_2^i, \text{N}), \cdots, (b_{20}^i, \text{N}), ID_H||ID_L),$$

où : ID_H et ID_L sont les identifiants du H-sensor et L-sensor respectivement.

La clé $K_{H,L}$ servira à chiffrer les données transmises au CH.

Afin de pouvoir communiquer de manière sécurisée au sein du cluster, une clé commune est nécessaire. Après avoir généré les clés partagées entre le H-sensor et chaque L-sensor, le CH diffuse un message pour notifier les L-sensors de générer la clé du cluster CK où :

$$CK = \text{HMAC}((b_1^i, \text{N}), (b_2^i, \text{N}), \cdots, (b_{20}^i, \text{N}), ID_H).$$

Cette clé est rafraichie à la demande du CH et à des intervalles de temps fixes.

⁎ Discussion et critiques

Le système proposé utilise un réseau de capteurs composé d'un nœud puissant H-sensor et de plusieurs L-sensors qui sont de petits dispositifs à faible consommation énergétique et à faible capacité en termes de calcul. En utilisant un seul H-sensor, la charge de calcul du système est réduite. De plus, bien que le protocole réponde aux principales exigences de sécurité des WBANs, la sécurité du système présenté dépend néanmoins des propriétés cryptographiques de la fonction de hachage utilisée. En effet, la sécurité du MD5 n'est plus garantie depuis son exposition aux attaques de collisions.

2.4.3 Solutions basées sur la cryptographie à courbe elliptique

2.4.3.1 Security Mechanism for a Wireless Sensor Network Based Healthcare Monitoring System

Les données médicales d'un individu sont très personnelles, sensibles et doivent être accessibles uniquement par des entités fiables et autorisées. Cependant, les signes vitaux personnels transmis dans le WBAN peuvent être espionnés pendant les communications sans fil. Pire encore, un adversaire pourrait même modifier, injecter ou usurper les données médicales privées. Pan et al. [9], ont proposé un système de gestion de clés hybride, basé sur la cryptographie à courbe elliptique (ECC - *Elliptic Curve Cryptography*) afin de protéger les données sensibles dans ces réseaux à ressources limitées. Cette approche hybride utilise un système de chiffrement symétrique ; une version modifiée de la structure de Feistel, pour chiffrer et déchiffrer les données physiologiques, et ECC pour gérer la distribution, la mise à jour et la révocation des clés. Tout d'abord, une clé K de 128 bits est générée aléatoirement pour les *04 itérations* du chiffre de Feistel (au lieu des 16 itérations habituelles). La clé K est ensuite divisée en quatre (04) sous-clés $K_1K_2K_3K_4$ de 32 bits chacune. Le texte en clair de 64 bits est divisé en deux blocs de 32 bits puis chiffré selon la procédure illustrée par la Figure 2.6

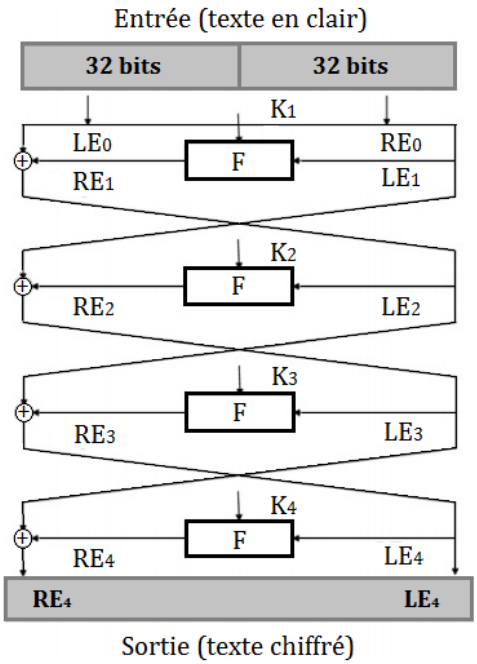

FIGURE 2.6 – Procédure de chiffrement de l'algorithme de Feistel modifié.

- **Procédure de chiffrement**

$LE_i = RE_{i-1}, \quad i = 1, 2, 3, 4.$
$RE_i = LE_{i-1} \oplus F(RE_{i-1}, K_i), \quad i = 1, 2, 3, 4.$

LE_i et RE_i sont les parties gauche et droite du texte en clair respectivement.

- **Procédure de déchiffrement**

$LD_i = RD_{i-1}, \quad i = 1, 2, 3, 4.$
$RD_i = LD_{i-1} \oplus F(RD_{i-1}, K_{4-i+1}), \quad i = 1, 2, 3, 4.$

LD_i et RD_i sont les parties gauche et droite du texte chiffré respectivement.

Afin de distribuer la clé de chiffrement, le protocole proposé utilise la cryptographie à courbe elliptique dont la sécurité repose sur le *problème du logarithme discret*. Pour commencer, le nœud capteur et la station de base se mettent d'accord, publiquement, sur une courbe elliptique *E(a,b,p)* où p est un domaine fini et *a, b* deux éléments de ce domaine, puis choisissent un point G situé sur la courbe. Ensuite, chacun de leur côté, et secrètement, le nœud capteur choisit sa clé privée r et calcule sa clé publique $R = rG$, la station de base choisit également sa clé privée d_B puis calcule sa clé publique $P_B = d_B$G. En s'échangeant les clés publiques R et P_B, les deux entités communicantes partagent un secret commun qui est le point $(x, y) = rP_B = d_BR = rd_B$G. Si un intrus a espionné leurs échanges, il connait $E(a, b, p)$, G, rG et d_BG. Pour pouvoir retrouver le secret rd_BG, il faut pouvoir calculer r connaissant G et rG. C'est ce qu'on appelle résoudre le problème du logarithme discret sur la courbe elliptique. Le nœud capteur se sert ensuite du secret commun et d'une fonction de dérivation de clé (KDF - *Key Derivation Function*) pour générer une nouvelle clé dont les s bits premiers constituent une clé K_s pour encrypter la clé de chiffrement K et les t bits restants constituent une clé K_{MAC} pour assurer l'intégrité des données.

⁎ **Discussion et critiques**

L'algorithme de Feistel utilisé dans ce protocole nécessite moins de temps pour les opérations de chiffrement/déchiffrement que DES (*Data Encryption Standard*) puisqu'il n'y a que 04 itérations au lieu de 16 à l'origine. De plus, bien que ECC utilise des clés plus courtes que celles utilisées dans d'autres systèmes de chiffrement à clé publique, elle offre néanmoins le même niveau de sécurité avec un espace de stockage de clés réduit et des opérations arithmétiques plus rapides. Toutefois, le protocole proposé est vulnérable aux attaques de rejeu.

2.4.4 Solutions basées sur une approche polynomiale

2.4.4.1 Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks

He et al. [6] ont proposé un système d'authentification basé sur les polynômes pour sécuriser les transmissions entre les nœuds capteurs et la station de base et gérer l'admission de nœuds légitimes uniquement. Lors de la phase d'initialisation, l'administrateur du WBAN génère aléatoirement un

polynôme $f(x,y) = \sum_{i,j=0}^{t} a_{ij}x^i y^j$ ayant la propriété *f(x,y) = f(y,x)*. Au moment du déploiement, chaque nœud capteur S_j est pré-chargé d'une partie du polynôme $f(sid_j, y)$ où sid_j indique l'identifiant du nœud S_j. De la même manière, la station de base est pré-chargée d'une partie du polynôme $f(pid_i, y)$ où pid_i indique l'identifiant de la station de base. Après le déploiement, la station de base diffuse son identifiant pid_i et chaque nœud capteur S_j calcule la clé individuelle $K_j = f(sid_j, pid_i)$, qu'il partage avec la station de base, en évaluant $f(sid_j, y)$ au point pid_i. Le temps est divisé en rounds. Chaque nœud capteur collecte une seule donnée par round, qu'il chiffre avec sa clé individuelle avant de la transmettre à la station de base. Au round r, chaque capteur S_j calcule le texte chiffré c_j^r= E($\{data_j^r, r\}$, K_j), $h(K_j, data_j^r)$ et transmet à la station de base le message $\{sid_j, pid_i, c_j^r\}$. A la réception, la station de base génère la clé individuelle $K_j = f(pid_i, sid_j) = f(sid_j, pid_i)$ en évaluant $f(pid_i, y)$ au point sid_j puis déchiffre le message reçu et calcule $h(K_j, data_j^r)$ pour le comparer à la valeur reçue. Si le résultat est identique alors la station de base est convaincue que le message provient bien du nœud S_j et qu'il n'a pas été modifié par un adversaire. S'il s'agit du premier message provenant du nœud S_j, la station de base sauvegarde $\langle sid_j, K_j \rangle$ pour une utilisation future.

Pour établir la clé partagée entre un nœud capteur S_j et son voisin (à une distance d'un saut), le nœud S_j diffuse un message HELLO = (sid_j, nonce) puis attend de recevoir un acquittement (ACK). A la réception du message de découverte, chaque nœud voisin S_l génère une clé partagée $K_{jl} = f(sid_l, sid_j)$ en évaluant $f(sid_l, y)$ au point sid_j, transmet le message $\{sid_l, h(K_{jl}, \text{nonce})\}$ et ajoute $\langle sid_j, K_{jl} \rangle$ à sa table de voisins. Le nœud S_j calcule alors $K_{jl} = f(sid_j, sid_l) = f(sid_l, sid_j)$ et vérifie l'intégrité du message $h(K_{jl}, \text{nonce})$ puis ajoute $\langle sid_l, K_{jl} \rangle$ à sa table de voisins.

Pour mettre à jour une clé individuelle durant un round r, chaque nœud capteur S_j effectue un XOR entre la clé du round précédent (r-1) et le haché de la donnée récoltée durant le round r où :

$$K_j^r = K_j^{r-1} \oplus h(data_j^r) = K_j^0 \bigoplus_{n=1}^{r} h(data_j^n).$$

⁎ Discussion et critiques

Le protocole proposé se base sur l'hypothèse qu'un adversaire qui espionne les communications sans fil fait face à des erreurs inévitables qui lui font ainsi manquer certaines informations transmises dans le WBAN. De ce fait, même si l'attaquant obtient la clé individuelle initiale K^0 et tente de l'utiliser pour se faire passer pour un nœud légitime à un moment ultérieur, il ne pourra y arriver car la nouvelle clé est générée à partir de toutes les données collectées précédemment. Les clés individuelles étant des valeurs hachées, elles rendent une attaque par dictionnaire difficile. De plus, l'utilisation de données récoltées par le nœud capteur pour mettre à jour la clé individuelle fournit un degré de hasard tel que l'adversaire ne peut la déduire et ainsi compromettre la sécurité du système. Bien que le système proposé soit résistant à plusieurs attaques, il nécessite tout de même un espace de

stockage élevé afin de sauvegarder les polynômes utilisés pour générer les clés, les tables de voisins les plus proches et les clés de communication.

2.4.5 Solutions basées sur la cryptographie à base d'identité

2.4.5.1 Body Sensor Network Security : An Identity-Based Cryptography Approach

Tan et al. [21] ont proposé un protocole basé sur le système de cryptographie à base d'identité (IBE - *Identity-Based Encryption*), pour offrir une sécurité et une confidentialité au WBAN tout en assurant un accès flexible aux données stockées. Le modèle de réseau proposé comporte plusieurs nœuds capteurs rattachés au corps humain, un site de stockage permettant d'archiver les données médicales collectées et une tierce partie de confiance (TA - *Trusted Authority*) qui gère l'accès à ce site (voir la Figure 2.7). Lors de la phase d'initialisation, une courbe elliptique *E(p,q,D)* est choisie avec un point G de cette courbe, un ensemble de n clés secrètes $x_1, x_2, \cdots, x_n \in D$ est ensuite choisi pour générer la clé secrète maître $X = (x_1, x_2, \cdots, x_n)$. Les n clés publiques correspondantes sont générées pour former la clé publique maître $Y = (y_1, y_2, \cdots, y_n)$ où $y_i = x_i \cdot G$, et une fonction de hachage à sens unique *h(.)* est choisie. Les paramètres $(Y, G, h(.))$ sont alors chargés dans chaque nœud capteur du WBAN et la clé secrète maître X est stockée au niveau de l'autorité de confiance (TA). Lorsqu'un nœud collecte une donnée, il génère une chaine arbitraire *str*, qui peut être l'heure à laquelle la donnée à été récoltée (par exemple $str = \{\text{Lundi}|\text{1pm}|\text{ECG}\}$), qu'il utilise pour dériver une clé publique $y_{str} = \sum_{i=1}^{n} h_i(str) \cdot y_i$, où $h_i(str)$ est le i^{eme} bit de $h(str)$, puis chiffre la donnée avec cette clé en utilisant ECC. Les données chiffrées sont ensuite transmises au site de stockage pour être archivées. Lorsqu'un médecin ou un membre du personnel soignant, souhaite accéder aux données relatives à un patient, il demande d'abord la permission à l'autorité de confiance en lui prouvant son identité grâce à la chaine *str*. L'autorité de confiance dérive ensuite la clé secrète correspondante $x_{str} = \sum_{i=1}^{n} h_i(str) \cdot x_i$, nécessaire pour décrypter les données. Le médecin récupère alors les données requises au niveau du site de stockage et procède au déchiffrement.

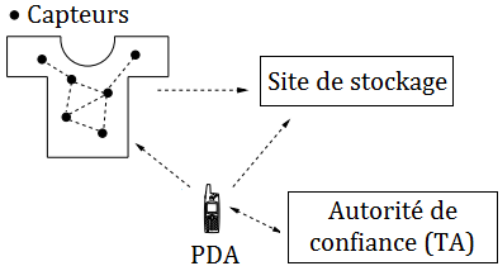

FIGURE 2.7 – Modèle du WBAN proposé par le système IBE-Lite [21].

⁕ **Discussion et critiques**

Le protocole proposé simplifie la gestion des clés puisqu'il n'est pas nécessaire de garder une trace des clés publiques y_{str} utilisées pour chiffrer les données. Il suffit que la chaine *str* soit la même pour générer la clé secrète x_{str} correspondante et déchiffrer les données. De plus, un adversaire ne peut obtenir aucune donnée utile en compromettant un nœud capteur puisque ce dernier ne sauvegarde que les paramètres publics utilisés pour la génération des clés. Enfin, bien que le site de stockage soit accessible au public, les données qui y sont stockées sont chiffrées et ne révèlent donc rien sur les données originales. Néanmoins, pour éliminer la possibilité de remonter jusqu'à la clé secrète maître X, le nombre de clés n doit être assez élevé nécessitant ainsi un espace mémoire considérable.

2.4.6 Solutions basées sur la cryptographie à clé publique sans certificats

2.4.6.1 An Efficient Certificateless Remote Anonymous Authentication Scheme for WBANs

Liu et al. [8] ont proposé un protocole d'authentification anonyme à distance basé sur la cryptographie à clés publiques sans certificats (CL-PKC - *Certificateless Public Key Cryptography*), pour permettre un accès en toute sécurité aux services du WBAN et préserver l'anonymat de l'utilisateur. Ce protocole implique trois (03) types de participants dans le WBAN ; un client demandeur de services, un gestionnaire de réseau (NM - *Network Manager*) qui gère l'ensemble du WBAN et des autorités, et un fournisseur d'application (AP - *Application Provider*) qui fournit les services demandés. Le protocole proposé se déroule en trois (03) phases :

- **Phase d'initialisation**

Le gestionnaire de réseau (NM) joue le rôle du centre de génération de clés (KGC - *Key Generation Center*) et met en place le système d'enregistrement. Étant donné un paramètre de sécurité l, le NM génère et publie les paramètres du système $\{l, G_1, G_2, q, P, e, H, h\}$ où $(G_1, +)$ et $(G_2, \cdot)$ sont des groupes cycliques d'ordre $q > 2^l$, P un générateur[4] de G_1, $e : G_1 \times G_1 \rightarrow G_2$ un couplage et $H : \{0,1\}^* \times G_1 \rightarrow G_1$, $h : \{0,1\}^* \times G_1 \rightarrow \mathbb{Z}_q^*$ des fonctions de hachage.

Le NM détermine ensuite sa paire de clés publique/privée $\langle Q_{NM}, s_{NM} \rangle$, où $Q_{NM} = s_{NM}P$.

Le fournisseur d'application possède également sa paire de clés publique/privée $\langle Q_{AP}, s_{AP} \rangle$, où $Q_{AP} = s_{AP}P$.

4. Élément de G_1 tel que tout élément du groupe peut s'exprimer sous forme d'un multiple de P.

- **Phase d'enregistrement**

Un client du WBAN ayant un identifiant C, doit s'enregistrer auprès du NM avant de pouvoir accéder au fournisseur AP pour des services médicaux. Durant cette phase d'enregistrement, le client choisit une paire de clés publique/privée partielle $\langle Q_1, s_1 \rangle$, où $Q_1 = s_1 P$ et obtient l'autre clé privée partielle $S_2 = s_{NM} Q_2$ calculée par le gestionnaire NM où $Q_2 = H(C, Q_1)$.

Le gestionnaire crée ensuite un compte de la forme $\langle C, ind_{Cv}, ind_{Cs}, droit \rangle$ pour le client C, où $ind_{Cv} = e(Q_2, Q_1)$ sert à vérifier le compte du client, $ind_{Cs} = e(Q_2, Q_{NM})$ est utilisé pour la signature et *droit* comprend des informations sur le type de services médicaux et le délai de prescription. Le NM transmet alors $\langle I, ind_{Cv}, droit \rangle$ au client et au fournisseur AP, où $I = ind_{Cv} P$.

- **Phase d'authentification anonyme à distance**

Afin d'être authentifié par le fournisseur d'application, le client du WBAN doit exécuter certaines étapes résumées par la Figure 2.8.

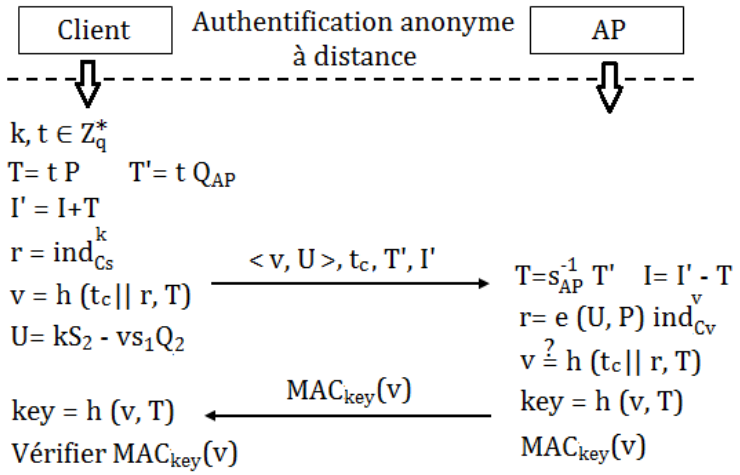

FIGURE 2.8 – Protocole d'authentification anonyme à distance [8].

- ⁎ **Discussion et critiques**

Le protocole proposé se base sur le cryptosystème CL-PKC, où le centre de génération de clés n'a pas accès à la clé privée de l'utilisateur mais lui fournit uniquement une clé privée partielle qui permettra à ce dernier de calculer sa vraie clé privée. De ce fait, le gestionnaire de réseau ne peut se faire passer pour un utilisateur légitime bien qu'il joue le rôle du KGC. De plus, l'indice du compte ind_{Cv} est calculé en utilisant une opération à sens unique $e(Q_2, Q_1)$, ainsi aucune entité, y compris le fournisseur AP, ne peut associer cet indice à l'identité réelle du client correspondant. Enfin, le protocole garantit une authentification mutuelle entre le client et le fournisseur d'application ; en effet, le calcul de la clé de session *key* est lié à celui de T qui ne peut être retrouvé que par le

fournisseur AP (en utilisant sa clé privée s_{AP}). Un attaquant peut toutefois tenter de remplacer la clé publique d'un client légitime, s'enregistrer auprès du gestionnaire de réseau sous l'identité de ce dernier et obtenir la clé privée partielle associée à cette identité.

2.5 Étude comparative

La Table 2.2 illustre une étude comparative que nous avons menée sur les différents protocoles analysés précédemment selon les critères d'évaluation discutés en section 2.2.

Protocole	Charge de stockage	Charge de calcul	Charge de communication	Résistance aux attaques	Convivialité
[12]	01× Identifiant du nœud 04× Clé de 128 bits 01× Fonction de hachage	01× Extraction des caractéristiques du signal ECG 01× Opération de hachage 03× Chiffrement 02× Déchiffrement 01× Opération MAC 01× Collecte de données	06× Round de communication	Vulnérable aux attaques : - Trou noir - Selective forwarding	Non
[22]	01× Identifiant du nœud 20× Bloc de 64 bits 04× Clé de 128 bits 20×20 Matrice des distances de Hamming 20× Bloc haché avec SHA-256	01× Extraction des caractéristiques avec FFT 01× Opération de hachage sur les 20 blocs 02× Génération de clés 04× Opération MAC 02× Opération XOR 01× Distance de Hamming de deux matrices 01× Collecte de données	04× Round de communication	Vulnérable aux attaques : - Force Brute - Jamming	Oui
[17]	01× Identifiant du nœud 01× PV de 128 bits 01× Clé pour chiffrer/déchiffrer	01× Opération MAC 01× Opération XOR 01× Calcul du CRC 01× Chiffrement 01× Déchiffrement 01× Collecte de données	02× Round de communication	Vulnérable aux attaques : - Sybil - Jamming	Oui
[10]	01× Identifiant du nœud 01× Clé de 64n bits (n est le nombre de points) 01× Vault (y compris les points faussés)	01× Extraction des caractéristiques avec FFT 01× Interpolation spline cubique 01× Vault, calcul du CRC 02× Opération MAC 01× Collecte de données	03× Round de communication	Vulnérable aux attaques : - Denial of Service - Jamming	Oui
[11]	01× Identifiant du nœud 01× Caractéristiques du signal ECG 01× Clé pour chaque coefficient IJS	01× Extraction des caractéristiques avec FFT 01× Chiffrement 01× Déchiffrement 02× Opération MAC 01× Collecte de données	02× Round de communication	Vulnérable aux attaques : - Usurpation d'identité - Sybil - Jamming	Oui

Protocole	Charge de stockage	Charge de calcul	Charge de communication	Résistance aux attaques	Convivialité
[7]	06× Clé de 128 bits 01× Fonction de hachage	06× Opération de hachage 03× Chiffrement 03× Déchiffrement 01× Collecte de données	06× Round de communication	Vulnérable aux attaques : - Selective forwarding - Jamming	Non
[5]	01× Identifiant du nœud 20× Bloc de 64 bits 02× Clé de 128 bits	01× Extraction des caractéristiques avec DWT 03× Opération HMAC 01× Chiffrement 01× Déchiffrement 01× Collecte de données	03× Round de communication	Vulnérable aux attaques : - Hash collision - Jamming	Oui
[9]	01× Identifiant du nœud 01× Clé de 128 bits 02× Clé de 160 bits 02× Clé dérivée	05× Opération XOR 01× Chiffrement 01× Déchiffrement 01× Opération HMAC 01× Collecte de données	03× Round de communication	Vulnérable aux attaques : - Rejeu - Denial of Service	Oui
[6]	01× Identifiant du nœud 01× Polynôme de degré t 01× Clé partagée avec la station de base 01× Table des nœuds voisins 01× Valeur hachée de la clé	01× Chiffrement 02× Opération de hachage 01× Opération XOR 01× Collecte de données	04× Round de communication	Vulnérable aux attaques : - Hello flood - Sybil	Non
[21]	01× Clé publique de 160 bits 01× Point de la courbe elliptique 01× Fonction de hachage	01× Génération d'une clé publique 04× Opération de hachage 02× Opération XOR 02× Chiffrement 01× Collecte de données	04× Round de communication	Vulnérable aux attaques : - Force Brute - Denial of Service	Non
[8]	01× Identifiant du nœud 01× Paire de clés publique/ privée 02× Clé publique 01× Clé privée partielle 01× Clé de session 02× Fonction de hachage	02× Opération de hachage 01× Opération MAC 01× Collecte de données	05× Round de communication	Vulnérable aux attaques : - Public Key Replacement	Non

TABLE 2.2 – Comparaison des solutions analysées.

2.6 Synthèse

Notre étude des travaux basés sur les signaux physiologiques montre que les solutions proposées présentent un réel potentiel pour éliminer le besoin de distribution explicite des clés de chiffrement, permettant aux capteurs du WBAN de se mettre d'accord sur une clé commune, à la demande, et assurant leur authentification mutuelle d'une manière à respecter le paradigme *plug and play*. Ces solutions nécessitent cependant que tous les capteurs puissent mesurer le même type de paramètre physiologique ; cette hypothèse est plutôt restrictive et fait que cette approche n'est pas adaptée à beaucoup d'applications des WBANs. De plus, l'extraction de caractéristiques à partir de signaux physiologiques demande une puissance de traitement considérable qui n'est pas en adéquation avec des réseaux à ressources limitées tels que les réseaux corporels sans fil. Ceci est d'autant plus valable pour le reste des solutions analysées qui, bien qu'elles soient résistantes à plusieurs types d'attaques, s'appuient sur des algorithmes cryptographiques complexes entrainant une charge de calcul, une charge de stockage, mais également une charge de communication élevées. En effet, les solutions basées sur le clustering nécessitent l'échange d'un grand nombre de messages afin de pouvoir établir la clé partagée entre un nœud appartenant au cluster et son CH. Elles montrent également des failles en termes de sécurité où des attaques liées au routage des paquets à travers les nœuds intermédiaires peuvent entrainer la perte de données critiques pouvant mettre en péril la vie du patient dans des systèmes WBAN de surveillance médicale par exemple. Les solutions basées sur une approche polynomiale quant à elles présentent une charge de stockage élevée puisque les nœuds capteurs doivent garder en mémoire toutes les données mesurées afin de pouvoir mettre à jour leur clé partagée avec la station de base. Enfin, les solutions basées sur la cryptographie à base d'identité nécessitent des opérations arithmétiques coûteuses où la sécurité du système repose sur la confiance accordée à une tierce partie qui doit être sans faille car elle est intrinsèquement capable de régénérer la clé privée de tout utilisateur, et par conséquent de réaliser sans autorisation des signatures ou des déchiffrements.

A l'issue de cette étude comparative, nous avons pu appréhender les enjeux majeurs qui entourent la sécurité dans les WBANs. Il nous est alors apparu qu'un protocole d'authentification qui ne serait pas basé sur la cryptographie pourrait être une réponse au problème de sécurité, mais aussi de ressources dont souffre les réseaux corporels sans fil.

2.7 Conclusion

La sécurité des données dans les WBANs et les systèmes de santé liés aux WBANs est un domaine important, et il reste encore un certain nombre de défis considérables à surmonter. La recherche dans ce domaine est encore à ses débuts, mais il suscite de plus en plus d'intérêt. Dans ce chapitre, nous avons établi un état de l'art sur les travaux de recherche concernant les mécanismes de sécurité dans les WBANs. Pour ce faire, nous avons proposé une classification des solutions selon l'approche suivie. Ensuite, nous avons brièvement décrit chaque solution étudiée suivie d'une discussion des points forts et des points faibles. Enfin, nous les avons comparées selon les différents critères retenus. Le chapitre suivant sera consacré à la description détaillée de notre solution.

Chapitre 3

A Body-Motion-based Authentication Protocol for Wireless Body Area Networks

3.1 Introduction

La mobilité joue un rôle essentiel dans la performance des protocoles développés pour les WBANs dû au mouvement du corps humain où les nœuds capteurs accompagnent ce mouvement. En effet, durant les activités quotidiennes, le corps humain présente différentes postures, comme se mettre debout, s'asseoir, marcher, courir, etc. Dans les réseaux corporels sans fil, ce changement de postures influe inévitablement sur les positions des capteurs et donc sur la distance qui les sépare du *sink*. Dans ce chapitre, nous décrirons en premier lieu le modèle de réseau et le modèle d'attaque sur lesquels repose notre contribution. Nous présenterons, par la suite, notre protocole d'authentification pour les systèmes WBAN de surveillance médicale implémentant un modèle de mouvements des nœuds capteurs en fonction de différentes postures que peut prendre le corps humain. Nous conclurons par une analyse de sécurité de la solution proposée.

3.2 Modèle de réseau et hypothèses

Dans un WBAN, plusieurs nœuds capteurs sont déployés sur le corps humain afin de surveiller différents paramètres physiologiques tels que la pression artérielle, la saturation en oxygène, le rythme cardiaque, etc. Dans ce qui suit, nous considérons un WBAN composé d'un nombre prédéfini de nœuds capteurs déployés sur le corps d'un patient et transmettant les données mesurées à un nœud stationnaire dénommé *sink* placé sur la poitrine du patient. Le *sink* est responsable de la collecte et du transfert des données provenant de tous les capteurs vers un serveur externe. Les capteurs placés sur le corps humain sont capables de mesurer continuellement différents paramètres physiologiques et de détecter tout type de stimuli (voir Figure 3.1). Les hypothèses relatives à notre modèle de réseau sont identifiées ci-après :

- Le placement des nœuds capteurs sur le corps humain est de telle manière à ne pas entraver les activités quotidiennes du patient ;
- Le *sink* possède des capacités de calcul et de stockage, ainsi qu'une réserve d'énergie plus importantes qu'un nœud capteur ordinaire ;

- La capture physique d'un nœud capteur est impossible car tous les nœuds sont sous la surveillance du patient.
- Les horloges de tous les capteurs sont synchronisées.

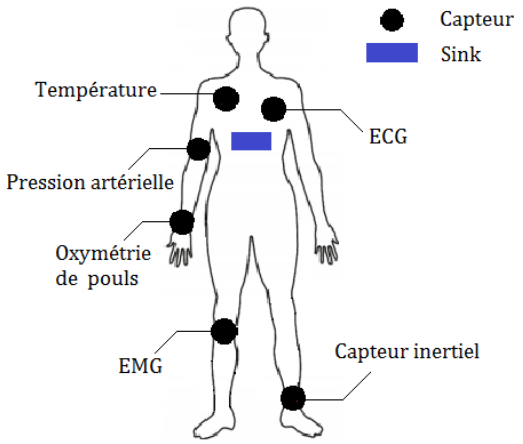

FIGURE 3.1 – Déploiement des nœuds sur le corps du patient.

3.3 Modèle d'attaque

Afin d'identifier les aspects vulnérables du WBAN, nous définissons un modèle d'attaque démontrant les points de sécurité critiques auxquels nous devrions fournir des solutions. Les capteurs du WBAN étant attachés au corps humain sont supposés être sous la surveillance du patient, il est donc impossible pour une personne malintentionnée de capturer un nœud sans être détectée. Dans les WBANs, les nœuds capteurs collectent des données physiologiques relatives au corps humain auquel ils sont attachés, puis les transmettent au *sink* chargé de stocker et d'agréger les données provenant de tous les capteurs. Il y a beaucoup de problèmes de sécurité, sans mentionner des problèmes de confidentialité, avec ce scénario. En effet, un attaquant externe peut perturber les communications en brouillant le canal de communication, usurper l'identité d'un nœud légitime ou encore prétendre être plusieurs nœuds légitimes ou inexistants (identités multiples). Dans ce cas, comment le *sink* authentifie-t-il les capteurs valides. Comment le *sink* peut-il être sûr que les données reçues proviennent d'un capteur attaché au même corps et non d'un capteur étranger. Le protocole d'authentification que nous proposons tente de résoudre ce problème, qui a récemment été formalisé sous le nom de *« one-body authentication problem »* [14].

3.4 Notre protocole d'authentification

Dans cette section, nous présentons notre protocole d'authentification pour les systèmes WBAN de surveillance médicale. Notre solution est conçue en deux phases distinctes : une phase d'apprentissage et une phase d'authentification. La première phase consiste à modéliser les postures du patient

à travers les différentes distances séparant les nœuds capteurs du *sink* en fonction du temps. La seconde phase consiste à authentifier les capteurs selon le modèle développé. Dans ce qui suit, nous présentons le détail de chaque phase. Les notations utilisées pour la description du protocole, ainsi que leurs significations sont données dans la Table 3.1.

Notation	Signification
S_j	Nœud capteur j
d_{j_i}	Distance cartésienne séparant le capteur j du *sink* à l'instant t_i
P_j	Polynôme d'interpolation de Newton correspondant au capteur j
$D_{i,k}$	Coefficients du polynôme d'interpolation de Newton
t	Début de la transmission des identifiants par les nœuds capteurs
Δt	Intervalle de temps durant lequel le *sink* collecte les distances
T	Durée de la phase d'apprentissage par posture

TABLE 3.1 – Notations.

3.4.1 Phase d'apprentissage

Dans les WBANs, la mobilité des nœuds est en corrélation avec le *sink*. De ce fait, les positions des capteurs peuvent être déterminées relativement à celui-ci. Pour déterminer les différentes positions des nœuds capteurs, nous devons tout d'abord identifier la posture du corps humain puis le mouvement correspondant. Les mouvements effectués par le corps humain lorsqu'il prend une posture donnée peuvent être déterminés à partir des traces réelles de la mobilité humaine. Afin de modéliser les mouvements des nœuds capteurs, le patient sera invité à passer par une phase d'apprentissage une fois les capteurs déployés.

Avant d'entamer la phase d'apprentissage, la posture du corps humain doit être définie. Le patient sera ensuite invité à exercer le mouvement durant lequel le *sink* analysera les différentes distances cartésiennes estimées à travers la puissance des signaux. Dans ce travail, nous nous intéressons à trois (03) postures en particulier ; lorsque le patient est debout (au repos), en position de marche, et lorsqu'il est entrain de courir. Dans ce qui suit, nous décrivons les mouvements effectués par le corps suivant les trois postures citées précédemment.

- **Position debout**

Dans cette position, le patient est debout au repos, le regard droit, les bras sur le côté, et les pieds serrés et parallèles. C'est la position anatomique de référence. En position debout, les distances entre les capteurs et le *sink* sont constantes puisque le corps humain est dans une position statique (voir Figure 3.1).

- **Position de marche**

Durant la marche, les bras et les jambes se déplacent d'avant en arrière de façon répétitive. Par conséquent, les nœuds placés sur les membres du corps se déplacent également dans les directions avant et arrière. De plus, comme le tronc du corps est peu mobile, les nœuds placés sur ce dernier montrent peu de variations dans leurs positions par rapport au *sink*. La Figure 3.2 représente le cycle de la marche humaine avec chaque étape i correspondant à un instant t_i. A chaque instant t_i, le corps est caractérisé par des distances cartésiennes spécifiques d_i entre le *sink* et les nœuds capteurs.

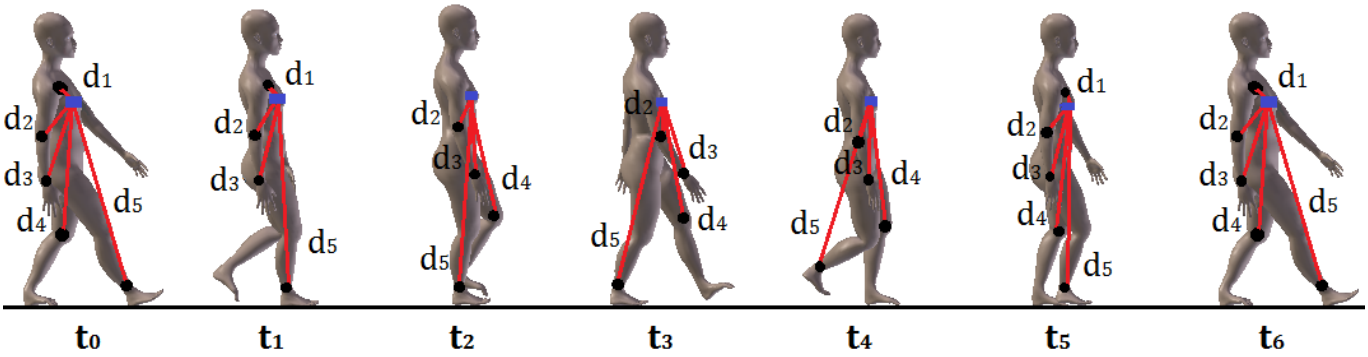

FIGURE 3.2 – Mouvements du corps humain lors de la marche.

- **Position de course**

Lorsque nous courons, il y a un mouvement répétitif de certains membres du corps tels que les bras et les jambes. Ces derniers effectuent des mouvements continus d'avant en arrière. Dans cette position, semblable à la marche, le bras gauche et la jambe droite sont synchronisés et se déplacent d'avant en arrière en même temps. De ce fait, les nœuds placés sur ces membres se déplacent dans la même trajectoire. Ces mouvements tels que décrits précédemment sont illustrés par la Figure 3.3 où chaque étape i correspond à un instant t_i. A chaque instant t_i, le corps est caractérisé par des distances cartésiennes spécifiques d_i entre le *sink* et les nœuds capteurs.

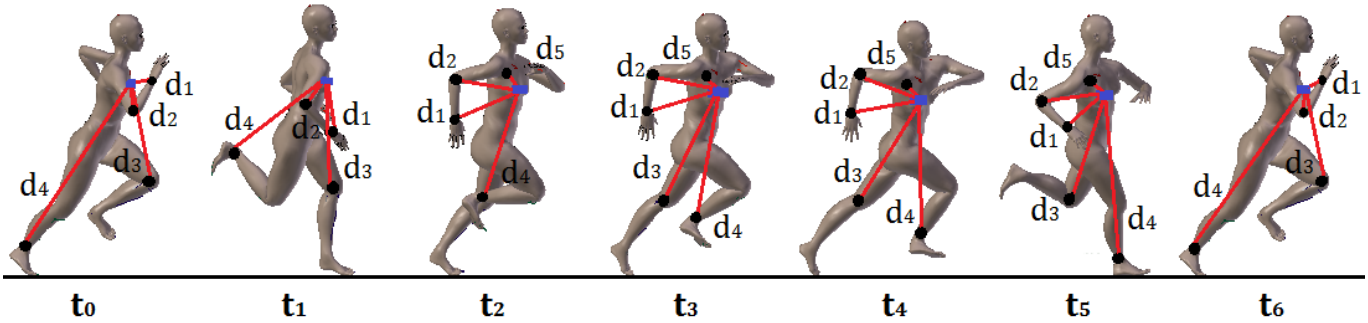

FIGURE 3.3 – Mouvements du corps humain lors de la course.

Durant la phase d'apprentissage, le *sink* initie le protocole en diffusant une requête aux nœuds capteurs $Req = \langle t, \Delta t, T \rangle$. Cette requête exige que chaque capteur S_j commence, après t millisecondes, à transmettre son identifiant, continuellement, chaque Δt millisecondes durant une période de T millisecondes. A chaque instant t_i, chaque capteur S_j envoie son identité au *sink*. Ce dernier estime, pour chaque instant t_i, la distance cartésienne d_{j_i} qui le sépare du nœud émetteur S_j à travers la puissance du signal radio reçu (en utilisant par exemple, RSSI - *Received Signal Strength Indication* [18]). Le *sink* maintient alors une table des distances cartésiennes correspondant à chaque instant t_i pour les différents capteurs déployés. Pour chaque nœud capteur, le *sink* collecte $n' = \frac{T}{\Delta t}$ distances cartésiennes.

Étant donné (n+1) points $\{(t_0, y_0), (t_1, y_1), \cdots, (t_n, y_n)\}$ tels que :

$$y_i = d_{j_i}, \quad \forall\ i = 0..n. \tag{3.1}$$

Le *sink* construit un polynôme P_j de degré n pour chaque capteur S_j tel que :

$$P_j(t_i) = d_{j_i}, \quad \forall\ i = 0..n. \tag{3.2}$$

Ce polynôme est calculé à l'aide de la formule d'*interpolation de Newton* où :

$$P_j(t) = D_{0,0} + (t - t_0)D_{0,1} + (t - t_0)(t - t_1)D_{0,2} + \cdots + (t - t_0)...(t - t_{n-1})D_{0,n}, \tag{3.3}$$

où les coefficients $D_{i,k}$ sont appelés *différences divisées* et sont calculés grâce à une formule de récurrence comme suit :

$$D_{i,i} = y_i, \quad \forall\ i = 0..n. \tag{3.4}$$

$$D_{i,k} = \frac{D_{i+1,k} - D_{i,k-1}}{t_k - t_i}, \quad \forall\ i = 0..n, \quad \forall\ k = 1..n, \quad k > i. \tag{3.5}$$

L'interpolation polynomiale a pour avantage une grande simplicité et une facilité de calcul. Les trois (03) méthodes d'interpolation classiques (*Lagrange*, *Neville-Aitken* et *Newton*) sont équivalentes ; elles calculent le même polynôme, mais diffèrent en coût opératoire. La méthode la moins onéreuse est celle de *Newton*. En effet, comme le montre la définition des différences divisées, des points supplémentaires peuvent être ajoutés pour créer un nouveau polynôme d'interpolation, sans pour autant recalculer les coefficients [28].

3.4.2 Phase d'authentification

Notre protocole d'authentification a pour objectif de vérifier l'identité d'un nœud capteur souhaitant communiquer avec le *sink*. A la réception des données mesurées par un capteur S_j, le *sink* calcule la distance d'_j qui le sépare de ce capteur suivant la puissance de son signal d'émission. Une fois cette distance obtenue, le *sink* estime l'instant t' en résolvant l'équation $P_j(t') = d'_j$, où P_j est le

polynôme d'interpolation correspondant au capteur S_j. Le *sink* peut conclure que le capteur S_j se trouvant à la distance d'_j est déployé sur le corps du patient seulement si $t' \approx \frac{t_i}{\Delta t} \ mod \ n'$, où t_i est l'instant correspondant à la réception des données. De cette manière, il est impossible pour un nœud illégitime se trouvant à proximité d'usurper l'identité d'un nœud valide dans le réseau.

3.5 Analyse de sécurité

Dans cette section, nous passons à l'analyse des propriétés de sécurité de la solution proposée afin de montrer qu'elle est résistante aux types d'attaques décrits en section 3.3.

3.5.1 Attaque d'usurpation d'identité

L'attaque d'usurpation d'identité, également appelée *attaque par spoofing*, est une attaque dans laquelle un adversaire assume avec succès l'identité de l'une des parties légitimes dans un système ou dans un protocole de communication. Contrairement aux approches traditionnelles, notre protocole n'utilise aucun paramètre cryptographique dans le processus d'authentification. De ce fait, le succès de cette attaque nécessite uniquement de générer une *puissance de signal* spécifique à un *instant* bien précis. En effet, supposons qu'un attaquant A se fasse passer pour un nœud valide B et transmette un message au *sink* sous l'identité légitime de ce dernier. Lors de la réception du message, le *sink* calcule la distance d'_j le séparant du nœud émetteur grâce à la puissance de son signal d'émission, estime l'instant t' correspondant, et le compare à l'instant de réception t_i. Le processus d'authentification échouera alors et le *sink* déduira qu'il s'agit d'un nœud étranger au corps du patient.

3.5.2 Attaque Sybil

Il s'agit d'une version avancée de l'attaque d'usurpation d'identité où un nœud malveillant peut prétendre être *plusieurs* nœuds légitimes ou inexistants dans le réseau. En d'autres termes, l'attaquant peut revendiquer différentes identités dans le but de prendre l'avantage sur les nœuds légitimes. Supposons qu'un nœud malveillant souhaite usurper l'identité de plusieurs nœuds valides pour envoyer de fausses informations au *sink*. A un instant donné, l'attaquant doit générer plusieurs signaux avec différentes puissances pour espérer tromper le *sink*. Or, en recevant ces signaux ce dernier va calculer la position du nœud émetteur qui à un instant t ne peut avoir qu'une seule position. Les messages reçus seront alors rejetés et l'attaquant est détecté.

3.5.3 Attaque de l'homme du milieu et rejeu

Dans l'attaque de l'homme du milieu (*man-in-the-middle attack*), un intrus malveillant s'interpose entre deux entités communicantes, se faisant passer pour l'une et l'autre à leur insu, et obtient l'accès aux informations que les deux parties s'échangent. Dans le WBAN, tous les nœuds capteurs sont à portée du *sink*. Le processus d'authentification s'effectue donc directement entre le nœud capteur et

le *sink* sans avoir recours à des nœuds intermédiaires. Même si un attaquant essaie de s'interposer entre les deux parties, il n'aura aucun moyen de se faire passer pour l'une ou l'autre. En effet, il est difficile de mener une attaque de l'homme du milieu dans ce cas, car les deux nœuds reçoivent les messages transmis par l'attaquant. De plus, rejouer d'anciens messages dans une nouvelle session est également impossible pour un attaquant dû à la mobilité des nœuds, et de ce fait à la puissance du signal qui diffère d'un instant à un autre.

3.5.4 Attaque de déni de service

Une attaque de déni de service (DoS - *Denial of Service*) a pour but de perturber le fonctionnement normal du réseau. Bien que notre protocole ne puisse pas empêcher cette attaque de se produire, il assure tout de même l'authentification des nœuds capteurs lorsqu'une telle attaque survient ou qu'elle est combinée avec une autre attaque. Supposons que l'attaquant inonde le *sink* avec des messages inutiles dans le but de revendiquer l'identité d'un nœud valide. Le processus d'authentification échouera alors étant donné que l'attaquant est incapable de transmettre des signaux avec une puissance spécifique.

3.6 Conclusion

L'authentification est un problème difficile à résoudre dans les WBANs dû à l'utilisation de nœuds capteurs limités en termes de puissance de traitement et de ressources. Tout protocole de sécurité conçu pour une utilisation dans les WBANs devrait être robuste contre les attaques et devrait avoir un faible impact sur la durée de vie du réseau. Dans ce chapitre, nous avons présenté notre contribution dans la sécurité des réseaux corporels sans fil. Tout d'abord, nous avons décrit le modèle de réseau et le modèle d'attaque sur lesquels nous nous sommes basés pour concevoir notre protocole. Puis, nous avons présenté notre protocole d'authentification basé sur les mouvements du corps humain durant certaines activités quotidiennes telles que la marche et la course. Enfin, nous avons conclu par une analyse de sécurité de la solution proposée. Le chapitre suivant sera consacré à l'évaluation de performances de notre protocole d'authentification.

Chapitre 4

Évaluation de performances

4.1 Introduction

Ce chapitre est consacré à l'évaluation des performances de notre protocole d'authentification. Nous présenterons en premier lieu l'environnement et les paramètres de simulation considérés pour l'évaluation des performances de notre solution. Nous décrirons par la suite les critères et métriques de simulation utilisés. Les résultats obtenus à l'issue de ces simulations seront finalement interprétés et comparés avec tous les protocoles étudiés dans le chapitre de l'état de l'art.

4.2 Environnement de simulation

Dans cette section, nous présentons au préalable les paramètres de simulation, puis nous décrivons les critères et métriques de simulation utilisés.

4.2.1 Paramètres de simulation

Notre protocole d'authentification à été simulé sous l'environnement *Java*. Les simulations ont été réalisées avec 6 capteurs et un nœud *sink* déployés sur le corps d'un patient. Chaque capteur possède une portée radio d'environ $1m$ et une énergie initiale $E_0 = 0.5$ *Joules*. Afin de mesurer l'énergie consommée par un nœud capteur lors d'une transmission, nous nous sommes basés sur le modèle radio de consommation d'énergie proposé par Heinzelman et al. [26], où l'énergie consommée par un capteur lors de l'émission d'un message de k bits vers un nœud situé à une distance de d mètres est $E_{Tx} = (E_{elec} \times k + E_{amp} \times k \times d^2)$. Les paramètres fixés pour la réalisation des simulations sont définis dans la Table 4.1.

Paramètre	**Valeur**
Nombre de nœuds	6
Zone de simulation	10 m × 10 m
Temps de simulation	150 s
Durée de la phase d'apprentissage par posture (T)	10 s
Portée radio d'un capteur	1 m
Débit de données	1 Mbit/s
Énergie initiale d'un capteur (E_0)	0.5 J
Énergie consommée par le circuit électronique (E_{elec})	16.7 nJ/bit
Énergie d'amplification (E_{amp})	1.97 nJ/bit/m^2

TABLE 4.1 – Paramètres de simulation.

Les simulations ont débuté par la phase d'apprentissage où le *sink* récupère, à chaque intervalle de temps $\Delta t = 1s$, les distances cartésiennes qui le sépare de chaque nœud capteur et ce, pendant une durée $T = 10s$ pour chacune des postures (debout, marche et course). Les positions initiales des capteurs lors du déploiement sont illustrées sur la Figure 4.1.

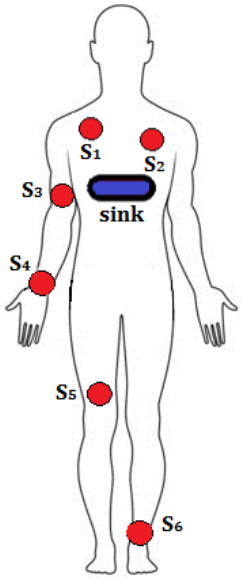

FIGURE 4.1 – Positions des capteurs lors du déploiement.

Les capteurs du WBAN sont capables de mesurer, continuellement, différents paramètres physiologiques. A cet effet, la taille des données générées par chaque capteur varie selon sa fonction. La Table 4.2 illustre la taille des données mesurées par chaque capteur.

Capteur	**Fonction**	**Taille des données (octets)**
S_1	Température	1
S_2	ECG	128
S_3	Pression artérielle	4
S_4	Oxymétrie de pouls	2
S_5	EMG	64
S_6	Inertie	192

TABLE 4.2 – Taille des données mesurées selon la fonction du capteur.

Un modèle de mobilité approprié est une condition essentielle pour l'évaluation de performances des protocoles développés pour les réseaux sans fil avec mobilité des nœuds. Dans les WBANs, les nœuds capteurs présentent une forte mobilité. La topologie du WBAN peut complètement changer en raison d'un changement de posture et des mouvements qui l'accompagne. Pour l'évaluation des performances de notre protocole d'authentification, nous nous sommes basés sur le modèle de mobilité MoBAN (*Mobility Model for BANs*) [13] permettant de simuler les protocoles intra- et extra-WBAN, et que nous avons implémenté sous l'environnement *Java*. Ce modèle de mobilité prend en compte le mouvement global du WBAN, en introduisant différentes postures du corps humain, et met en œuvre la mobilité individuelle des nœuds déployés dans le réseau.

4.2.2 Critères et métriques de simulation

Dans cette section, nous présentons les critères et métriques de simulation que nous avons utilisés pour l'évaluation de performances de notre protocole d'authentification.

4.2.2.1 Critères de simulation

Les critères de simulation utilisés pour l'évaluation de performance de notre protocole sont la fiabilité du canal de transmission et la fréquence de transmission.

- **Fiabilité du canal de transmission**

Les réseaux corporels sans fil diffèrent des réseaux typiques de capteurs sans fil dans de nombreux aspects parmi lesquels les caractéristiques du canal de transmission et les liaisons qui sont en général de faible qualité. Les capteurs du WBAN étant déployés sur le corps humain, il existe donc une forte mobilité des nœuds et un changement fréquent de la topologie du réseau. De ce fait, la qualité du canal de transmission et la connexion entre les nœuds dépendent fortement de leurs positions relatives. Dans un canal de transmission non fiable, les messages peuvent être perdus à tout moment sans notification. Ce paramètre est d'autant plus important dans les WBANs où les données échangées sont très critiques.

- **Fréquence de transmission**

Dans des systèmes WBAN de surveillance médicale à distance, les nœuds capteurs récoltent des données liées à l'état de santé du patient en temps réel. Dans de telles applications, la fréquence de transmission se trouve être un paramètre important à prendre en compte, où la transmission d'une quantité considérable de données par unité de temps peut indiquer une situation d'urgence pouvant alerter les équipes médicales de l'état critique du patient.

4.2.2.2 Métriques de simulation

Afin d'évaluer les performances de notre protocole, nous utilisons les métriques de simulation suivantes : la charge de transmission, la charge de calcul et l'énergie consommée. Contrairement aux autres protocoles d'authentification qui nécessitent le stockage d'au moins une clé de 128 bits, la charge de stockage au niveau des capteurs du WBAN est, dans notre cas, quasiment nulle c'est pour cette raison qu'elle n'a pas été retenue parmi les métriques de performance à évaluer. L'usage des métriques citées précédemment est motivé par les points décrits ci-après.

- **Charge de transmission**

Dans les réseaux de capteurs sans fil, les communications sont les opérations les plus coûteuses en termes d'énergie. En plus de la quantité de données échangées, ce paramètre est d'autant plus important dans les WBANs en raison de la mobilité des nœuds capteurs où la topologie du réseau change avec le mouvement du corps humain. En effet, plus la distance entre les nœuds lors d'une transmission augmente, plus l'énergie consommée augmentera également comme le montre l'équation du modèle de consommation d'énergie décrit en section 4.2.1.

- **Charge de calcul**

Malgré les progrès réalisés dans la fabrication de capteurs de plus en plus puissants, les capteurs sans fil actuels possèdent une puissance de calcul très réduite. En plus d'avoir une répercussion directe sur l'énergie, une charge de calcul élevée est fortement préjudiciable pour le temps de réponse du réseau notamment dans les systèmes WBAN de surveillance médicale à contraintes temporelles.

- **Énergie consommée**

L'étude de la consommation en énergie de la solution proposée est indispensable pour apprécier l'effet produit sur la batterie des capteurs et de ce fait sur la durée de vie du réseau. Dans les WBANs, il est indispensable de trouver un compromis entre la capacité énergétique des capteurs et l'énergie consommée par les opérations de traitement et de communication afin d'éviter le remplacement fréquent des nœuds capteurs notamment ceux implantés dans le corps humain qui sont difficilement accessibles.

4.3 Résultats et discussion

Dans cette section, nous nous sommes intéressés à comparer les performances des protocoles étudiés dans le chapitre de l'état de l'art avec celles de notre protocole. Pour plus de précision, les résultats obtenus ont été calculés à partir d'une moyenne effectuée sur plusieurs simulations. Dans ce qui suit, nous présentons sous forme de graphiques puis interprétons les résultats obtenus.

4.3.1 Impact de la fiabilité du canal de transmission

Dans ce qui suit, nous discutons l'impact de la fiabilité du canal de transmission sur les trois métriques de simulation utilisées. Il est à noter que la charge de calcul est représentée par le temps de réponse du réseau.

La Figure 4.2 illustre la variation de la charge de transmission en fonction de la fiabilité du canal de transmission.

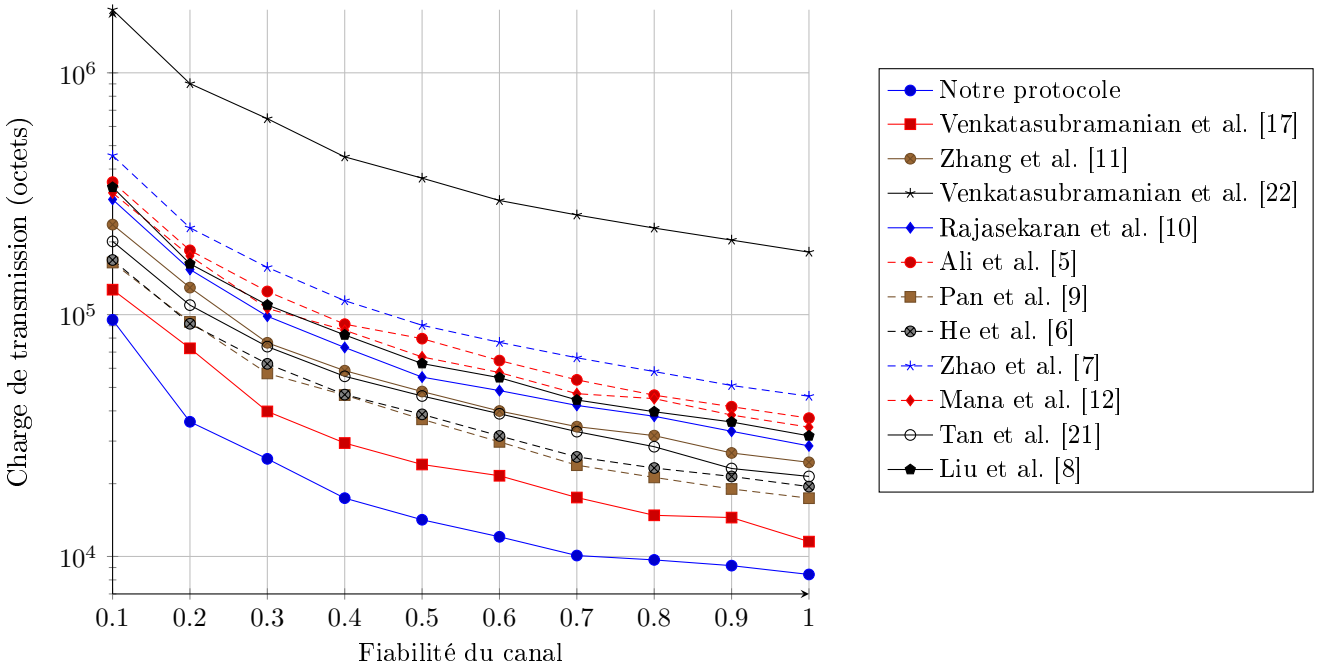

FIGURE 4.2 – Charge de transmission en fonction de la fiabilité du canal de transmission.

La Figure 4.3 illustre l'évolution du temps de réponse en fonction de la fiabilité du canal de transmission.

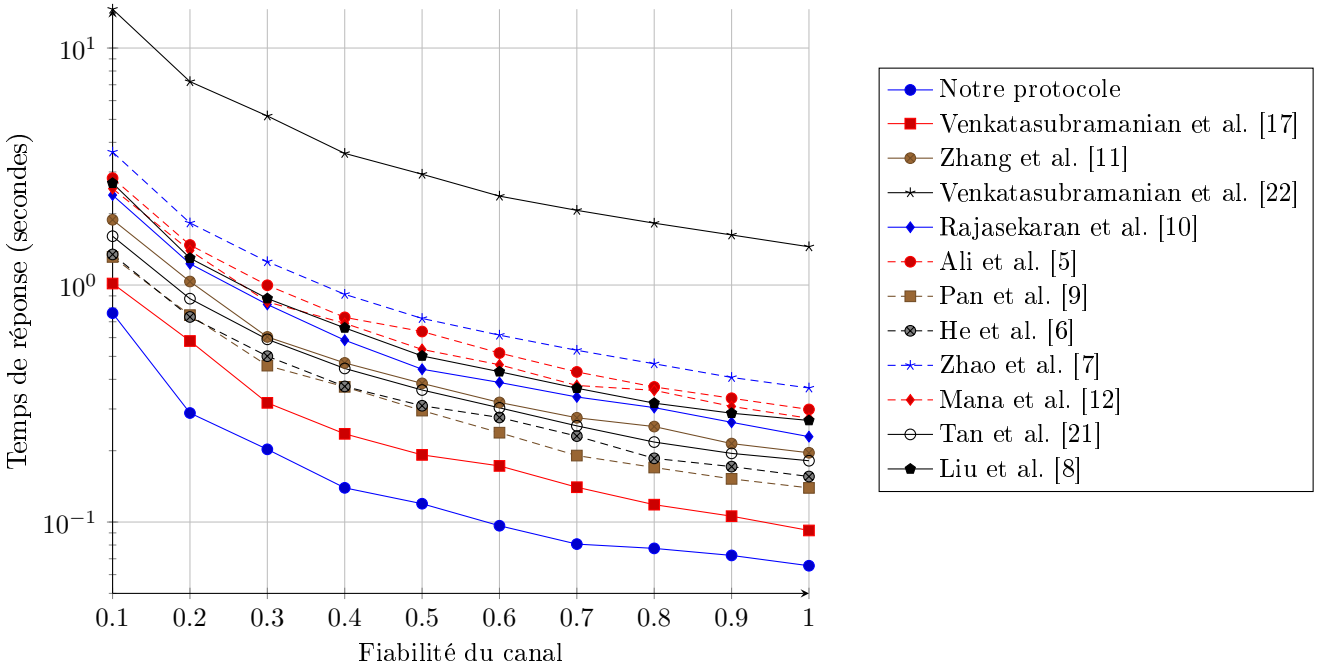

FIGURE 4.3 – Temps de réponse en fonction de la fiabilité du canal de transmission.

La Figure 4.4 illustre l'évolution de la consommation en énergie en fonction de la fiabilité du canal de transmission.

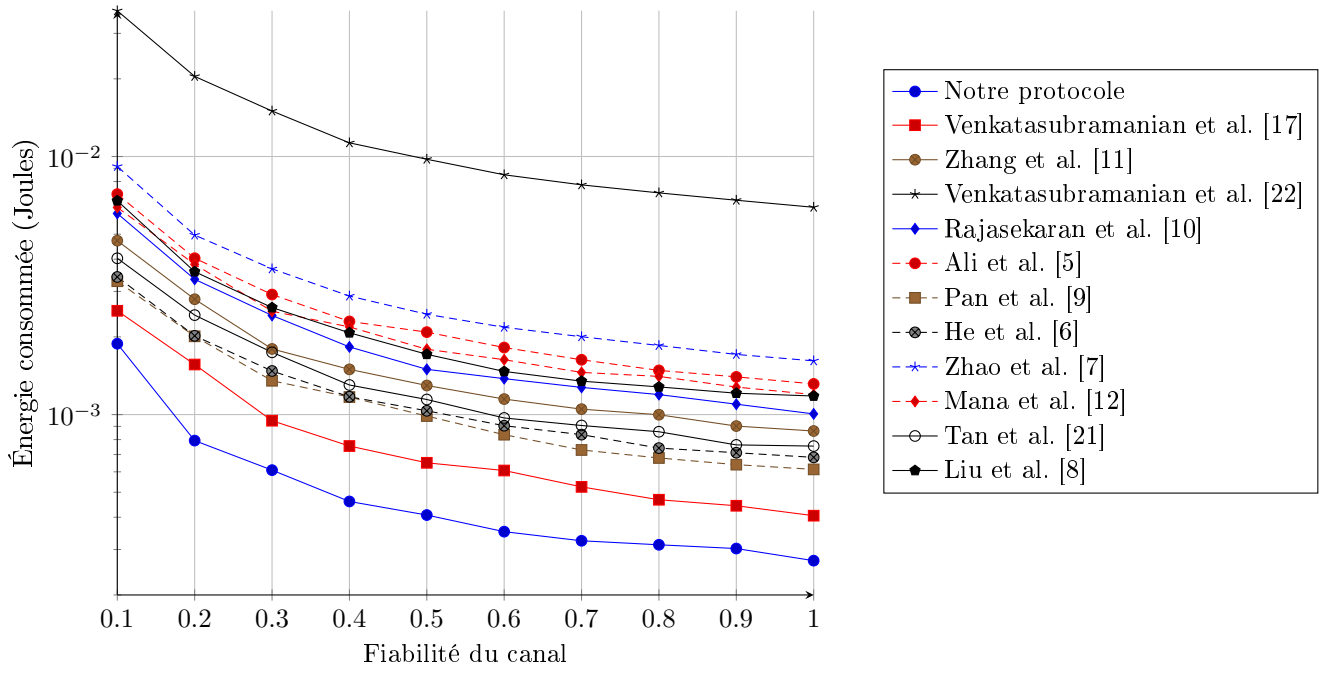

FIGURE 4.4 – Énergie consommée en fonction de la fiabilité du canal de transmission.

L'analyse des trois graphiques précédents montre une relation inverse entre la fiabilité du canal de transmission et les trois métriques mesurées. En effet, lorsque la fiabilité du canal de transmission augmente, la charge de transmission, le temps de réponse et l'énergie consommée diminuent. Ceci est compréhensible dans la mesure où dans un canal de transmission non fiable, des erreurs de transmission peuvent survenir et des messages peuvent être perdus à tout moment. Les capteurs du WBAN doivent alors retransmettre leurs données entrainant ainsi une charge de transmission élevée, un temps de réponse considérable, et de ce fait une forte consommation en énergie.

Concernant la charge de transmission, nous constatons que notre protocole donne de meilleurs résultats comparé aux autres solutions, avec une réduction considérable de la charge de transmission dès une fiabilité de 0.2. Ce résultat est dû au fait que contrairement aux autres protocoles qui, en plus des données mesurées, requièrent l'échange de plusieurs paramètres cryptographiques (clés de chiffrement, identifiants, MAC, etc.) pour assurer l'authentification des capteurs, notre protocole n'utilise que les données médicales récoltées par ces derniers. En effet, pour le protocole proposé par Venkatasubramanian et al. [22], par exemple, la charge de transmission reste très importante. Ce résultat est crédible dans la mesure où la taille des 20 blocs générés à partir du signal de l'électrocardiogramme, hachés avec SHA-256 et échangés entre les capteurs (640 *octets*) introduit une forte charge de transmission dans le réseau. Pour le protocole proposé par Ali et al. [5], par contre, la charge de transmission est moins élevée car les 20 blocs issus de l'électrocardiogramme (chaque bloc est de 8 *octets*) sont transmis directement sans être hachés.

Concernant le temps de réponse du réseau, la Figure 4.3 montre que notre protocole présente également de meilleurs résultats par rapport aux autres solutions avec un temps de réponse de base de 65ms (lorsque le canal est fiable). En effet, dans notre protocole, les données recueillies par les

capteurs sont transmises directement vers le *sink* sans passer par des nœuds intermédiaires. En revanche, pour le protocole proposé par Zhao et al. [7], par exemple, les paquets envoyés transitent par plusieurs chemins avant d'atteindre leur destination, occasionnant ainsi un temps de réponse plus élevé qui continue de croître avec le nombre de réémissions.

De ces résultats, il en découle que la consommation en énergie est faible pour notre protocole en comparaison avec les autres solutions (voir Figure 4.4) ce qui permet de gérer efficacement la capacité énergétique des capteurs et de prolonger la durée de vie du réseau. En résumé, malgré les caractéristiques inhérentes au canal de transmission et aux liaisons qui sont en général de faible qualité dans les WBANs, notre protocole d'authentification montre des résultats très satisfaisants en termes de charge de transmission, de temps de réponse et d'énergie consommée, ce qui lui permet d'être adapté aux applications mobiles de soins et de santé.

4.3.2 Impact de la fréquence de transmission

Dans ce qui suit, nous discutons l'impact de la fréquence de transmission sur les trois métriques de performance précédemment citées.

La Figure 4.5 illustre la variation de la charge de transmission en fonction de la fréquence de transmission.

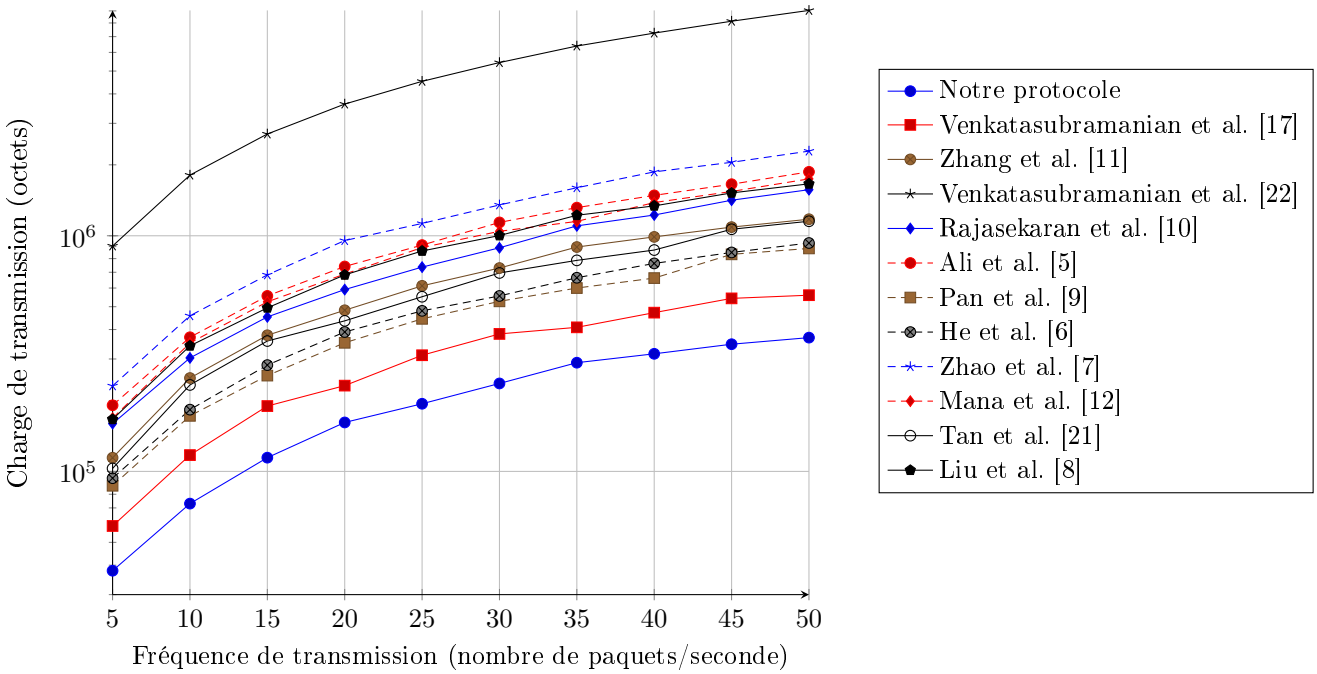

FIGURE 4.5 – Charge de transmission en fonction de la fréquence de transmission.

La Figure 4.6 illustre la variation du temps de réponse en fonction de la fréquence de transmission.

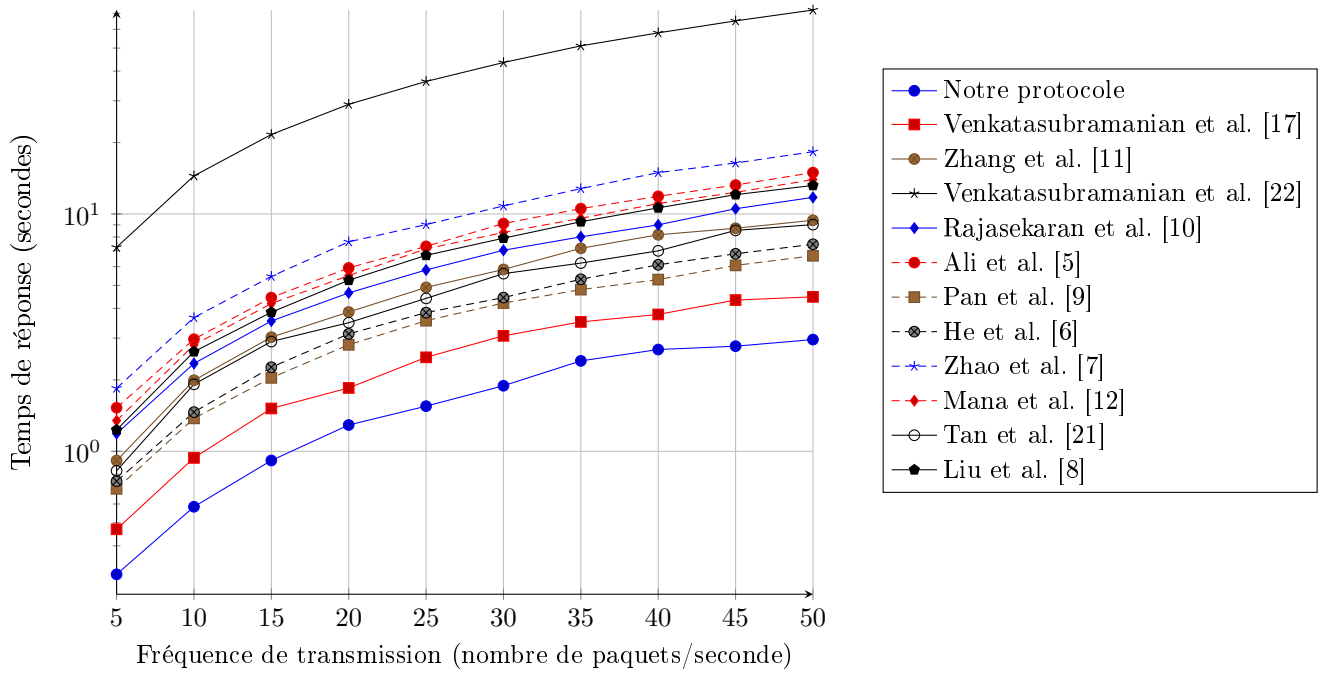

FIGURE 4.6 – Temps de réponse en fonction de la fréquence de transmission.

La Figure 4.7 illustre l'évolution de la consommation en énergie en fonction de la fréquence de transmission.

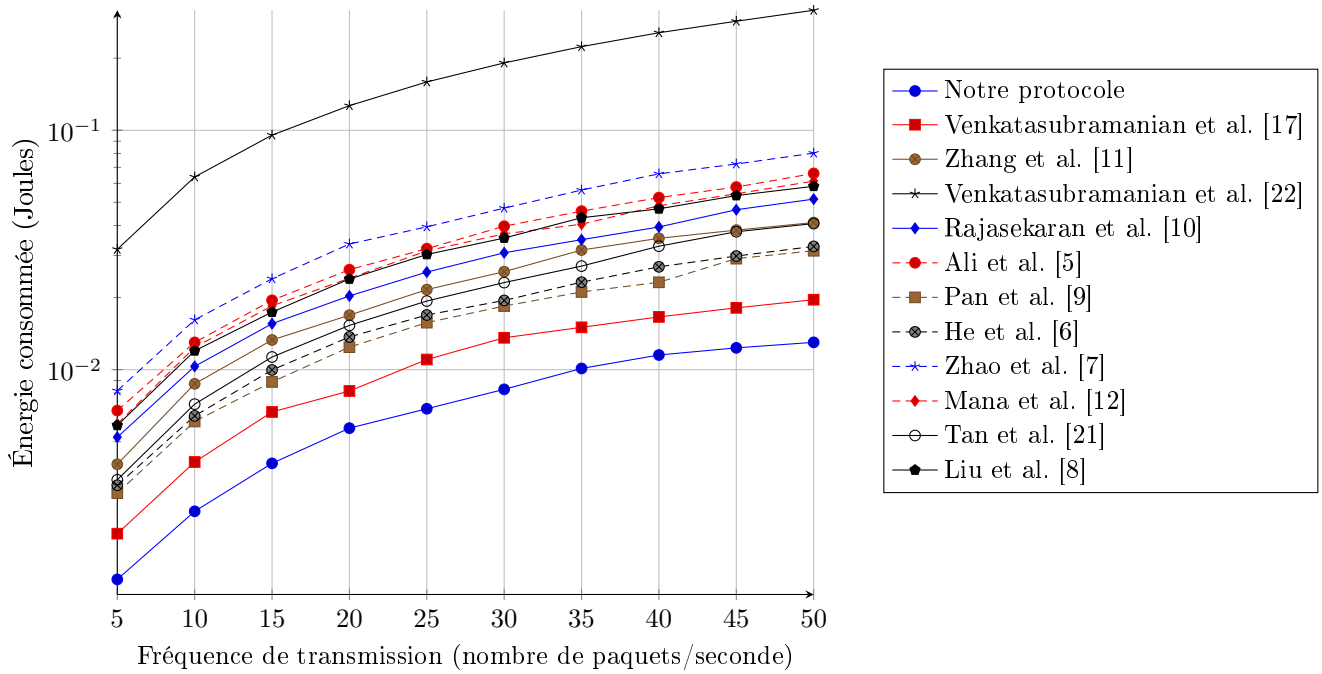

FIGURE 4.7 – Énergie consommée en fonction de la fréquence de transmission.

En étudiant les graphiques précédents, nous constatons que l'augmentation de la fréquence de transmission entraine l'accroissement des trois métriques mesurées. Ce résultat s'avère crédible étant donné la quantité de données à transmettre par unité de temps et la forte densité du trafic qui parcourt le réseau.

Concernant la charge de transmission, notre protocole montre de meilleurs résultats comparés aux autres protocoles en raison de la taille des données transmises qui se résument aux valeurs physiologiques recueillies par les capteurs. Le protocole proposé par Venkatasubramanian et al. [22] montre une augmentation considérable de la charge de transmission due à la quantité de données échangées entre les capteurs (640 *octets*) nécessaire à l'établissement d'une clé commune. Pour le protocole proposé par Venkatasubramanian et al. [17], par contre, la charge de transmission est moindre car la clé de chiffrement est directement émise avec les messages de données captées par les nœuds du réseau.

Concernant le temps de réponse, les résultats relatifs à notre protocole sont très satisfaisants et meilleurs que ceux présentés par les autres solutions avec une hausse tolérable étant donné le nombre de paquets échangés qui devient de plus en plus élevé. Nous remarquons une légère différence entre le protocole proposé par Rajasekaran et al. [10] et celui de Zhang et al. [11]. En effet, les deux solutions se basent sur la technique du Fuzzy Vault pour l'échange de la clé secrète partagée mais diffèrent dans le calcul du Vault. Pour le premier protocole, la clé secrète est dissimulée dans le Vault grâce à des points faussés (*chaff points*) qui seront émis avec ce dernier. En revanche, le second protocole utilise une nouvelle technique du Fuzzy Vault où les points faussés sont inutiles entrainant ainsi un temps de réponse moins important. Pour le protocole proposé par Mana et al. [12], le temps de réponse est élevé en raison du nombre de paquets transitant par plusieurs nœuds intermédiaires avant d'atteindre leur destinataire.

Enfin, la Figure 4.7 montre des résultats acceptables pour notre solution concernant l'énergie consommée comparés à ceux présentés par le restant des protocoles dont les valeurs élevées ont un impact préjudiciable sur la durée de vie du réseau. De cette discussion, il en résulte que notre protocole est adapté aux applications de surveillance médicale à distance prenant en compte les situations d'urgence à fréquence de transmission élevée.

4.3.3 Performances de sécurité

Dans cette section, nous évaluons les performances de notre protocole d'authentification dans la détection d'équipements étrangers se trouvant à portée de communication des capteurs du WBAN. Pour ce faire, nous estimons le taux de détection (DR - *Detection Rate*), le taux de faux rejets (FRR - *False Rejection Rate*) et le taux de fausses acceptations (FAR - *False Acceptance Rate*) en fonction du nombre de périodes Δt choisi lors de la phase d'apprentissage et utilisé pour construire le polynôme d'interpolation nécessaire à l'authentification des capteurs.

- **Taux de détection**

C'est le rapport entre le nombre d'attaques détectées et le nombre total d'attaques existantes. Le taux de détection exprimé en pourcentage est défini comme suit :

$$DR = \frac{Nombre\ d'attaques\ détectées}{Nombre\ total} \times 100$$

- **Taux de faux rejets**

C'est la probabilité que le système rejette à tort un capteur légitime du WBAN. Le taux de faux rejets exprimé en pourcentage est défini comme suit :

$$FRR = \frac{Nombre\ de\ noeuds\ légitimes\ non\ authentifiés}{Nombre\ total} \times 100$$

- **Taux de fausses acceptations**

C'est la probabilité que le système authentifie à tort un équipement non-autorisé. Le taux de fausses acceptations exprimé en pourcentage est défini comme suit :

$$FAR = \frac{Nombre\ d'équipements\ étrangers\ authentifiés}{Nombre\ total} \times 100$$

La Figure 4.8 illustre les résultats obtenus lors de simulations de notre protocole en présence d'équipements étrangers.

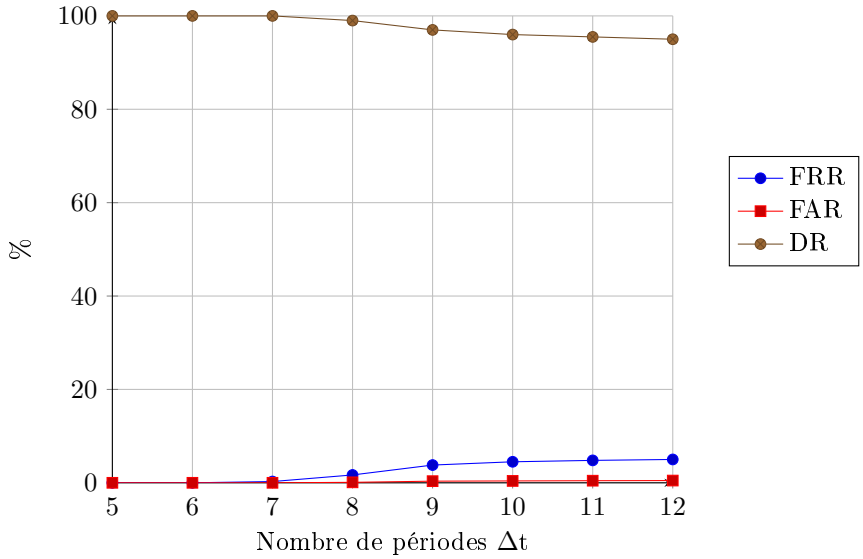

FIGURE 4.8 – DR, FRR et FAR en fonction du nombre de périodes Δt.

Nous remarquons que quelque soit le nombre de périodes Δt, le taux de détection reste très élevé avec un pourcentage toujours supérieur à 97%. Ces résultats viennent ainsi confirmer l'efficacité de notre approche dans l'identification d'équipements étrangers au WBAN. D'autre part, nous notons que le taux de faux rejets est relativement bas et sa croissance en fonction du nombre de périodes Δt reste très faible. Ce résultat est plutôt compréhensible dans la mesure où lorsque le nombre de périodes Δt augmente, c'est l'intervalle de temps qui devient de plus en plus petit. Les distances entre un capteur et le *sink*, à des périodes consécutives, deviennent alors très rapprochées et une légère différence peut faire échouer le processus d'authentification. Cette légère hausse du FRR est toutefois acceptable du moment que le taux de fausses acceptations reste quasi nul permettant ainsi de garantir la détection d'éventuels attaquants.

4.4 Conclusion

Dans ce chapitre, nous avons évalué les performances de notre protocole proposé en le comparant avec d'autres protocoles d'authentification existants dans la littérature. Pour ce faire, nous avons varié deux paramètres à savoir la fréquence de transmission et la fiabilité du canal de transmission afin d'étudier leur impact sur la charge de transmission, la charge de calcul et l'énergie consommée par les capteurs du WBAN. Les résultats obtenus montrent que notre protocole est adapté aux applications pratiques dans des environnements de soins de santé mobiles fournissant un compromis entre la sécurité et l'efficacité. En effet, en plus de garantir un niveau de sécurité élevé en détectant les équipements étrangers au WBAN déployé sur le corps d'un patient, notre protocole présente une haute performance en termes de consommation en énergie, de charges de stockage, de calcul et de communication, ce qui lui permet d'être idéal pour des réseaux à ressources limitées tels que les réseaux corporels sans fil.

Conclusion générale et perspectives

Un système de santé promettant une collecte continue et fiable et une analyse objective des aspects physiologiques et comportementaux d'un patient, tout en fournissant ces informations aux médecins, a été l'objectif des *réseaux corporels sans fil* (WBANs). Ces réseaux sont apparus comme une technologie ayant le potentiel pour révolutionner la prestation des soins de santé dans les ambulances, les salles d'urgence, les salles d'opération, les cliniques et même dans nos maisons. Toutefois, les WBANs sont encore au stade précoce de leur développement, et plusieurs défis de recherche doivent être surmontés afin qu'ils puissent être largement acceptés. L'authentification est l'un des principaux défis à relever tant les données collectées sont sensibles et directement associées à un patient particulier. Un intrus malintentionné peut tenter d'usurper l'identité d'un nœud légitime afin d'injecter des données pouvant mettre en danger la santé du patient. De plus, la conception d'un mécanisme de sécurité pour les WBANs doit faire face à certaines contraintes en raison de l'utilisation de nœuds capteurs limités en termes de puissance de calcul, de réserve d'énergie, d'espace de stockage, etc.

Ce document a débuté par une étude générale sur les réseaux corporels sans fil. Nous avons présenté en premier lieu les caractéristiques, l'architecture des communications et les domaines d'application de ces réseaux. Nous avons ensuite effectué une comparaison entre les WBANs et les WSNs en termes de déploiement, de densité du réseau, de mobilité, de niveau de sécurité, etc. Enfin, nous avons clôturé cette étude en décrivant les principales contraintes et exigences de sécurité dans la conception des WBANs. Par la suite, nous avons présenté une étude critique, selon plusieurs critères, de certains travaux de recherche menés dans l'axe de l'authentification dans les réseaux corporels sans fil. Nous avons ainsi constaté que dans la plupart de ces travaux, les principales exigences de sécurité sont assurées au détriment des ressources du réseau. La deuxième partie de ce mémoire concerne notre contribution dans la sécurité des WBANs. Nous avons proposé un protocole d'authentification des nœuds capteurs pour les systèmes WBAN de surveillance médicale. Notre protocole se base sur les mouvements effectués par le corps humain lorsqu'il prend certaines postures (debout, marche et course) et vise à déterminer si un capteur se trouvant à portée de communication, est déployé ou non sur le corps d'un patient. Notre solution s'inscrit comme une réponse à un problème qui a récemment été formalisé sous le nom de *« one-body authentication problem »* [14]. Nous avons ensuite évalué les performances de notre protocole d'authentification en le comparant avec d'autres protocoles existants dans la littérature, et dont les résultats ont démontré l'adaptabilité de notre protocole pour des applications pratiques dans des environnements de soins de santé mobiles fournissant un compromis entre la sécurité et l'efficacité. En effet, en plus de garantir un niveau de sécurité élevé permettant de détecter plus de 97% des équipements étrangers au WBAN, notre protocole d'authentification

montre une haute performance en termes de consommation en énergie, de charges de stockage, de calcul et de communication. Enfin, notre travail a fait l'objet d'un article qui a été soumis à la conférence *IEEE International Smart Cities Conference (ISC2), session : Health and Well-being* [1].

Pour conclure ce document, nous présentons des perspectives qui feront l'objet de nos futures recherches, à commencer par étendre notre protocole pour résoudre la version forte du *one-body authentication problem* qui consiste à authentifier les capteurs du WBAN d'une part, et identifier le patient auquel ils sont rattachés d'autre part. Nous envisageons également de mettre en œuvre notre protocole d'authentification sur une plateforme expérimentale.

Bibliographie

[1] Bouchelaghem S., Yessad N., Ouada F. S. & Omar M., A Lightweight Cryptographic-less Authentication Protocol for WBANs, Submitted to *IEEE International Smart Cities Conference*, Trento, Italy, 2016.

[2] Macwan S., Gondaliya N. & Raja N., Survey on Wireless Body Area Networks, In *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 5, pp. 107-110, 2016.

[3] Nadeem A., Hussain M. A., Owais O., Salam A., Iqbal S. & Ahsan K., Application Specific Study, Analysis and Classification of Body Area Wireless Sensor Network Applications, In *Computer Networks*, Vol. 83, pp. 363-380, 2015.

[4] Movassaghi S., Abolhasan M., Lipman J., Smith D. & Jamalipour A., Wireless Body Area Networks : a survey, In *IEEE Communications Surveys and Tutorials*, Vol. 16, pp. 1658-1686, 2014.

[5] Ali A., Irum S., Kausar F. & Khan F. A., A Cluster-Based Key Agreement Scheme Using Keyed Hashing for Body Area Networks, In *Springer Science+Business Media Multimedia Tools and Applications*, Vol. 66, pp. 201-214, 2013.

[6] He D., Chen C., Chan S., Bu J. & Zhang P., Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks, In *IEEE Journal of Biomedical and Health Informatics*, Vol. 17, pp. 664-674, 2013.

[7] Zhao H., Qin J. & Hu J., An Energy Efficient Key Management Scheme for Body Sensor Networks, In *IEEE Transactions on Parallel and Distributed Systems*, Vol. 24, pp. 2202-2210, 2013.

[8] Liu J., Zhang Z., Kwak K. S. & Sun R., An Efficient Certificateless Remote Anonymous Authentication Scheme for Wireless Body Area Networks, In *Proceedings of IEEE International Conference on Communications*, Ottawa, Canada, pp. 3404-3408, 2012.

[9] Pan J., Li S. & Xu Z., Security Mechanism for a Wireless-Sensor-Network-Based Healthcare Monitoring System, In *IEEE IET Communications*, Vol. 6, pp. 3274-3280, 2012.

[10] Rajasekaran R. T., Manjula V., Kishore V., Sridhar T. M. & Jayakumar C., An Efficient and Secure Key Agreement Scheme Using Physiological Signals in Body Area Networks, In *Proceedings of the ACM International Conference on Advances in Computing, Communications and Informatics*, Chennai, India, pp. 1143-1147, 2012.

[11] Zhang Z., Wang H., Vasilakos A. V. & Fang H., ECG-Cryptography and Authentication in Body Area Networks, In *IEEE Transactions on Information Technology in Biomedecine*, Vol. 16, pp. 1070-1078, 2012.

[12] Mana M., Feham M. & Bensaber B. A., Trust Key Management Scheme for Wireless Body Area Networks, In *International Journal of Network Security*, Vol. 12, pp. 75-83, 2011.

[13] Nabi M., Geilen M. & Basten T., MoBAN : A Configurable Mobility Model for Wireless Body Area Networks, In *Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques*, Barcelona, Spain, pp. 168-177, 2011.

[14] Cornelius C. & Kotz D., On Usable Authentication for Wireless Body Area Networks, In *Proceedings of the first USENIX Workshop on Health Security and Privacy (HealthSec)*, Washington, USA, 2010.

[15] Li M., Lou W. & Ren K., Data Security and Privacy in Wireless Body Area Networks, In *IEEE Wireless Communications*, Vol. 17, pp. 51-58, 2010.

[16] Patel M. & Wang J., Applications, Challenges and Prospective In Emerging Body Area Networking Technologies, In *IEEE Wireless Communications*, Vol. 17, pp. 80-88, 2010.

[17] Venkatasubramanian K. K. & Gupta S. K. S., Physiological Value Based Efficient Usable Security Solutions for Body Sensor Networks, In *ACM Transactions on Sensor Networks*, Vol. 6, pp. 31-65, 2010.

[18] Xu J., Liu W., Lang F., Zhang Y. & Wang C., Distance Measurement Model Based on RSSI in WSN, In *Journal of Wireless Sensor Networks*, Vol. 2, pp. 606-611, 2010.

[19] Znaidi W., Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil, *Thèse de Doctorat en Informatique*, INSA de Lyon, 2010.

[20] Neves P., Stachyra M. & Rodrigues J., Application of Wireless Sensor Networks to Healthcare Promotion, In *Journal of Communications Software and Systems*, Vol. 4, pp. 181-190, 2008.

[21] Tan C. C., Wang H., Zhong S. & Li Q., Body Sensor Network Security : An Identity-Based Cryptography Approach, In *Proceedings of the first ACM Conference on Wireless Network Security*, Virginia, USA, pp. 148-153, 2008.

[22] Venkatasubramanian K. K., Banerjee A. & Gupta S. K. S., EKG-based Key Agreement in Body Sensor Networks, In *Proceedings of IEEE INFOCOM Workshops*, Arizona, USA, pp. 1-6, 2008.

[23] Walters J. P., Liang Z., Shi W. & Chaudhary V., Wireless Sensor Network Security : a survey, In *Security in Distributed, Grid, and Pervasive Computing*, Vol. 1, pp. 367-404, 2007.

[24] Dodis Y., Reyzin L. & Smith A., Fuzzy Extractors : How to Generate Strong Keys from Biometrics and Other Noisy Data, In *Advances in Cryptology - Lecture Notes in Computer Science Series*, Cachin C. & Camenisch J., Springer, Berlin Heidelberg, Vol. 3027, pp. 523-540, 2004.

[25] Akyildiz I. F., Sankarasubramaniam W. S. & Cayirci E., Wireless Sensor Network : a survey, In *Computer Networks*, Vol. 38, pp. 393-422, 2002.

[26] Heinzelman W. R., Chandrakasan A. & Balakrishnan H., Energy Efficient Communication Protocol for Wireless Microsensor Networks, In *Proceedings of IEEE 33rd Annual Hawaii International Conference on System Sciences*, Maui, Hawaii, pp. 8020-8029, 2000.

[27] Sowell B., Branine M., Bowman J., Hubbert M., Sherwood H. & Quimby W., Feeding and Watering Behaviour of Healthy and Morbid Steers in a Commercial Feedlot, In *Journal of Animal Science*, Vol. 77, pp. 1105-1112, 1999.

[28] Liem C. B., Shih T. M. & Lü T., The Splitting Extrapolation Method : a New Technique in Numerical Solution of Multidimensional Problems, In *Series on Applied Mathematics*, World Scientific, London, Vol. 7, 1995.

Résumé

Les réseaux corporels sans fil (WBANs - *Wireless Body Area Networks*) sont apparus comme une nouvelle technologie dans le domaine de la santé. Ces réseaux permettent à des données liées aux signes vitaux et aux mouvements d'un patient d'être recueillies par de petits capteurs portables et/ou implantés dans le corps, puis communiquées à une équipe médicale en utilisant des techniques de communication sans fil adaptées. Les WBANs ont su montrer un grand potentiel pour améliorer la qualité des soins de santé et ont donc trouvé un large éventail d'applications notamment dans la surveillance médicale à distance et les systèmes d'intervention médicale d'urgence. La sécurité des données récoltées par les WBANs est considérée comme un sujet de préoccupation majeure non encore résolu, avec des défis résultant des contraintes liées aux ressources limitées des dispositifs du WBAN. L'objectif de ce mémoire est de répondre au problème d'authentification des nœuds capteurs dans les WBANs. Pour atteindre cet objectif, nous avons proposé un protocole d'authentification basé sur les mouvements du corps humain. Les activités quotidiennes telles que la marche ou la course sont caractérisées par un modèle de mouvements permettant d'identifier les nœuds capteurs rattachés au patient. L'analyse de sécurité a permis de démontrer la robustesse de notre protocole contre certaines attaques connues. De plus, les résultats des simulations de notre protocole et une comparaison avec d'autres solutions existantes dans la littérature ont mis en évidence les avantages de notre protocole en termes de charges de stockage, de calcul, de communication et de consommation en énergie.

Mots clés : *WBAN, Sécurité, Authentification, Mouvement du corps, Soins de santé.*

Abstract

The Wireless Body Area Networks (WBANs) have emerged as a new technology in the health field. These networks allow the data related to vital signs and movements of a patient to be collected by small wearable and/or implantable sensors and communicated to medical staff using suitable wireless communication techniques. The WBANs have shown great potential in improving healthcare quality, and thus have found a wide range of applications from remote health monitoring to emergency medical response systems. The security of data collected from a WBAN is a major unsolved concern, with challenges coming from stringent resource constraints of WBAN devices. The objective of this paper is to respond to the problem of sensor nodes authentication in WBANs. To achieve this goal, we proposed a body-motion-based authentication protocol. The routine activities, as walking or running, are characterized through a movement model to identify sensor nodes attached to the patient. Through the security analysis, we demonstrate the robustness of our protocol against some well known attacks. Moreover, the simulation results of our protocol and a comparison with the existing solutions in the literature highlight the advantages of our protocol in terms of energy consumption, storage, computational and communication overheads.

Keywords : *WBAN, Security, Authentication, Body-motion, Healthcare.*