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

Authentification biométrique dans les réseaux mobiles de soins et de santé

Mémoire soutenu le 30/06/2016 par :

M^lle CHERIFI **Feriel**

M^lle ZEBBOUDJ **Sofia**

Devant le jury composé de :

Président :	*M. AMAD* **Mourad**	**M.C.A, U.A.M Béjaïa**
Examinateur :	*M. NAFI* **Mohamed**	**M.A.A, U.A.M Béjaïa**
Examinateur :	*M. EL-SAKAANE* **Nadim**	**Doctorant, U.A.M Béjaïa**
Encadrant :	*M. OMAR* **Mawloud**	**M.C.A, U.A.M Béjaïa**
Co-Encadrant :	*M. MOHAMMEDI* **Mohamed**	**Doctorant, U.A.M Béjaïa**

Promotion 2015/2016

Remerciements

*Nos remerciements vont en premier lieu à notre encadrant **M. OMAR Mawloud** pour son orientation, sa disponibilité et surtout pour la préciosité de ses conseils sans lesquels nous n'aurions pu mener ce travail à bon port.*

*Nos remerciements vont également à notre co-encadrant **M. MOHAMMEDI Mohamed** pour sa patience et son soutien qui nous ont été d'une grande aide pendant l'élaboration de ce travail.*

*Nous tenons à remercier également les enseignants du département de Génie Electrique ainsi que tous les membres de l'entreprise **Bejaia Equipement Medical**, pour nous avoir fourni les outils nécessaires à nos recherches.*

Nous remercions chacun des membres du jury pour l'intérêt porté à notre travail en acceptant de l'examiner et de l'enrichir de leurs propositions.

*Nos remerciements s'étendent à tous nos enseignants et les membres du département d'Informatique de l'université **ABDERRAHMANE MIRA**.*

Ainsi qu'à tous ceux et celles qui ont contribué de près ou de loin à l'accomplissement de ce travail.

Dédicaces

A nos très chers parents, pour les sacrifices déployés à notre égard, pour leur soutien et tout les efforts consentis pour notre éducation et notre formation. Qu'ils trouvent dans ce modeste travail le témoignage de notre reconnaissance, notre profonde affection et notre attachement indéfectible.

A nos frères et sœurs et tous nos amis qui nous ont soutenues tout au long de ce travail.

A chaque main tendue et pour toute attention témoignée.

Table des matières

Liste des tableaux

Table des figures

Liste des acronymes et des abréviations

ACK	**ACK**nowledgment
ADN	**A**cide **D**ésoxyribo **N**ucléique
BAN	**B**ody **A**rea **N**etwork
BLE	**B**luetooth **L**ow **E**nergy
CRC	**C**yclic **R**edundancy **C**heck
ECC	**E**lliptic **C**urve **C**ryptography
ECDH	**E**lliptic **C**urve **D**iffie **H**ellman
ECG	**E**lectrocardiogramme
ECG-AS	**E**lectrocardigram-based **A**uthentication **S**cheme
EEG	**E**lectroencéphalogramme
EMG	**E**lectromyogramme
EM	**E**xpectation **M**aximisation
FAR	**F**alse **A**cceptance **R**ate
FFT	**F**ast **Fourier T**ransform
FRR	**F**alse **R**ejection **R**ate
GMM	**G**aussian **M**ixture **M**odel
IPI	**I**nter**P**ulse **I**nterval
MAC	**M**essage **A**uthentication **C**ode
MBASN	**M**edical **B**ody **A**rea **S**ensor **N**etwork
PPG	**P**hotoplethysmogramme

Introduction générale

De nos jours, la médecine a connu de très remarquables progrès qui ont non seulement permis de garantir une meilleure qualité de vie aux patients, mais aussi contribué à améliorer considérablement les chances de guérison. Cependant, il existe encore un bon nombre de maladies et d'épidémies dont les causes demeurent peu connues, même si elles sont assez fréquentes. Le besoin d'une surveillance continue des patients s'avère indispensable afin de mieux suivre l'évolution des maladies pour espérer les inhiber, voire empêcher qu'elles se déclarent. L'avancée technologique rapide qu'a connu les appareils mobiles et les services Web durant cette dernière décennie a permis leur intégration dans différents aspects de notre vie quotidienne. Cela a permis d'explorer de nouvelles possibilités dans le secteur médical et d'assurer une surveillance et un système de diagnostique en temps réel. Dans un futur très proche, les capteurs sans fil seront complètement intégrés dans les vêtements, les appareils, les véhicules, etc. Cela représentera un grand pas pour les systèmes mobiles de soins et de santé [1].

Le *Medical Body Area Sensor Network* (MBASN) est un réseau mobile promettant une meilleure qualité de soin. Il est composé de capteurs assurant la collecte et l'envoi des données médicales du patient aux centres de soins pour une consultation à distance. Mais, leur déploiement est actuellement ralentit par plusieurs obstacles. En particulier, la confidentialité des données médicales doit obligatoirement être garantie pour protéger ces données ainsi que l'état de santé du patient contre les attaques malicieuses qui mettent sa vie en péril [3].

Les interférences entre des capteurs de différents MBASNs est un autre problème qui doit être pris en considération. Ces interférences peuvent mener à des erreurs médicales graves car des capteurs d'un autre MBASN pourraient très bien communiquer des données médicales d'un autre patient et actionner une procédure de traitement inappropriée engendrant ainsi, des interactions médicamen-

teuses dangereuses. Plusieurs recherches ont été menées pour solutionner le problème de sécurité et des interférences ; l'authentification biométrique est une solution commune à ces problèmes [15]. En effet, les signaux physiologiques du patient, originellement mesurés par les capteurs du MBASN à des fins médicales, peuvent leur servir d'identifiants grâce auxquels on peut savoir si deux capteurs appartiennent au même MBASN ou pas. De plus, puisque les signaux, tels que l'électrocardiogramme, varient avec le temps, il serait idéal de les utiliser pour générer des clés de session aléatoires et assurer parallèlement l'identité du capteur et la confidentialité des données médicales, c'est le cas des protocoles PSKA [31] et OPFKA [13]. Néanmoins, l'application de la biométrie pour l'authentification entre capteurs peut parfois entrainer de faux rejets même au sein du même MBASN. Pire encore, les caractéristiques biométriques, si elles sont utilisées directement comme clé partagée comme dans le cas du protocole de Singh et al. [29], ne pourront pas assurer les opérations de chiffrement et déchiffrement car elles ne seront pas totalement identiques. Cela est causé par les différents bruits accompagnant l'échantillonnage des signaux physiologiques.

Dans cette optique est né le besoin de trouver une solution pour que les données médicales ne soient pas utilisées à mauvais escient ou involontairement contre le bien être du patient. Il s'agit dans ce mémoire d'apporter une solution biométrique au problème d'authentification intra-MBASN. Nous tenterons d'utiliser les caractéristiques des signaux physiologiques d'une manière plus appropriée, tout en minimisant les taux de faux rejets (FRR, *False Rejection Rate*) et de fausses acceptations (FAR, *False Acceptation Rate*) lors de l'authentification des capteurs du MBASN. Le protocole que nous proposons, nommé *Electrocardiogram-based Authentication Scheme* (ECG-AS), utilise l'électrocardiogramme (ECG) comme générateur de caractéristiques biométriques pour l'authentification intra-MBASN ainsi que la génération d'une clé symétrique pour protéger les caractéristiques biométriques. Nous prenons en considération les limites matérielles des MBASNs, en particulier celles des capteurs, pour offrir une solution plus rapide et efficace que les protocoles étudiés [5] [13] [14] [16] [29] [31] [32] [35].

Le premier chapitre de ce mémoire, « **Medical Body Area Sensor Networks : vers la médecine du futur** », portera sur quelques généralités concernant les MBASNs et la biométrie dans la sécurité des données médicales. Un état de l'art sur des protocoles d'authentification fera l'objet du deuxième chapitre, nommé « **Taxonomie des protocoles d'authentification biométrique dans les MBASNs** », où nous discuterons des points faibles et points forts de chaque protocole présenté selon différents critères. Dans le troisième chapitre, « **Secure and Efficient ECG-based Authentication Scheme for MBASNs** » , nous présenterons en détail, les différentes phases par lesquelles notre protocole, ECG-AS, passe pour assurer la gestion de clés et l'authentification. Pour prouver l'efficacité de notre protocole, nous présenterons dans le quatrième chapitre, « **Expérimentation, simulation et évaluation des performances** », une expérimentation faite sur des signaux ECG, des simulations et une comparaison avec d'autres protocoles. Une conclusion suivie de perspectives clôtureront notre

mémoire.

Chapitre 1

Medical Body Area Sensor Networks : vers la médecine du futur

1.1 Introduction

Les réseaux de capteurs corporels (BAN, *Body Area Network*), sont un type de réseaux promettant de nouvelles applications dans plusieurs domaines. Les *Medical Body Area Sensor Networks* (MBASN) peuvent être utilisés dans le domaine médical afin de faciliter l'échange de données entre les patients et les professionnels de la santé. Ils peuvent notamment être utilisés dans la télémédecine afin de résoudre les problèmes de surcharge que connait les systèmes de soins classiques et d'automatiser les traitements des patients [15]. Cependant, il existe plusieurs problèmes à résoudre avant de déployer une telle technologie. Puisqu'il s'agit de la santé des patients, il est important d'assurer la fiabilité des capteurs et surtout d'assurer entre autres, la confidentialité, l'authentification et l'intégrité des données médicales du patient [35]. D'autre part, l'utilisation de la biométrie est devenue très répandue dans les applications des MBASNs, car elle permet de régler certains de leurs problèmes, notamment celui de la sécurité des données médicale [15].

Nous aborderons ce chapitre par définir le fonctionnement des MBASNs à travers leurs architectures. Nous citerons ensuite quelques domaines d'application des MBASNs ainsi que les obstacles qui ralentissent leur déploiement. Enfin nous présenterons brièvement la biométrie et son rôle dans la

sécurité des données médicales du patient dans les MBASNs.

1.2 Medical Body Area Sensor Network

Le terme *Medical Body Areas Sensor Network* (MBASN) dérive du terme *Body Area Network* (BAN) qui désigne un ensemble de capteurs sans fil pouvant être implantés ou placés directement ou à proximité du corps. Ces capteurs ont la capacité de mesurer les caractéristiques du corps humain et de ses environnements extérieurs pour une assistance médicale à distance. Cette nouvelle technologie s'inscrit dans la cadre du développement des « Ville intelligentes », ou « Smart cities » [7], pour améliorer la qualité des services urbain et réduire ses coûts. Une bonne intégration des capteurs utilisés pour la médecine dans les systèmes mobiles de soins et de santé permettra donc d'améliorer les systèmes classiques de santé [5].Le domaine d'application des BANs ne s'arrête pas à la télémédecine, mais s'étend à d'autres applications comme illustré sur la figure 1.1.

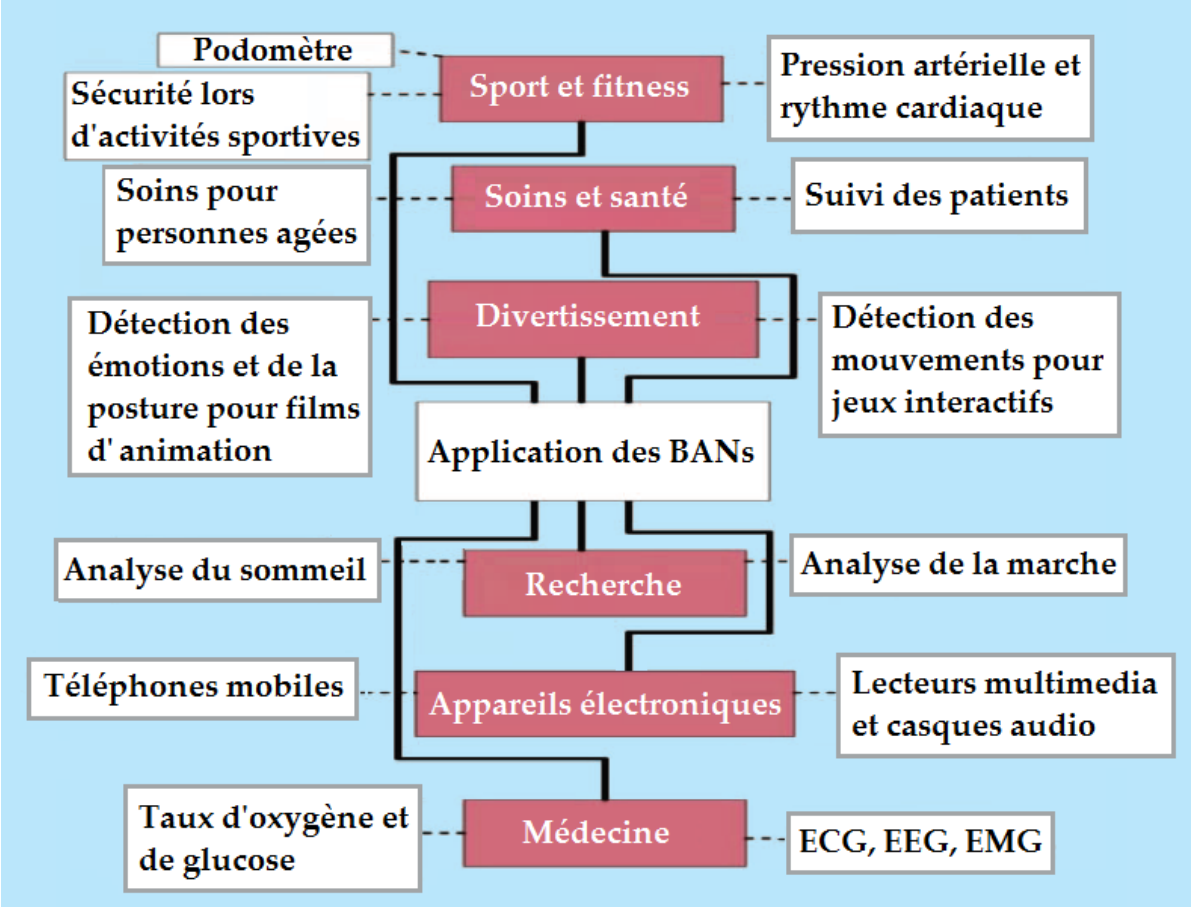

FIGURE 1.1 – Application des BANs [15]

.

1.2.1 Architecture des MBASNs

Les MBASNs, comme les BANs, ont une architecture constituée de trois tiers. Chaque tier possède une fonction et emplacement uniques [15].

1.2.1.1 Capteurs

Les capteurs sans fil peuvent avoir différentes formes et différentes tailles. Il existe différents types de capteurs pouvant mesurer des signaux différents [15] :

- les capteurs physiologiques sont utilisés pour mesurer la pression artérielle, le taux de glucose dans le sang, la température et les signaux Electrocardiogramme (ECG), Electroencéphalogramme (EEG) et Electromyogramme (EMG).
- Les capteurs, dits biocinétiques, sont utilisés pour mesurer l'accélération et la vitesse angulaire résultant des mouvements du corps.
- Les capteurs d'environnement sont utilisés pour mesurer les facteurs environnementaux tels que la température, l'humidité, la lumière et la pression acoustique.

Les données mesurées par les capteurs sont envoyé aux centres de soins où elles sont interprétées par des médecins afin d'obtenir l'état de santé du patient. La connexion entre les capteurs et les dispositifs de traitements est assurée en utilisant des technologies sans fil telle que ANT, Bluetooth classique, BLE (*Bluetooth Low Energy*), Sensium, Zarlink ZL70101 et Zigbee [21]. Le type du spectre, la topologie du réseau de capteurs et la portée varient selon le choix de la technologie utilisée [15].

1.2.1.2 Data Hub

Les données collectées par les capteurs peuvent être sauvegardées dans le Data Hub. Ce dernier est un dispositif permettant aux données des capteurs d'être stockées avant d'être envoyée directement ou ultérieurement au service de télémédecine d'un hôpital ou d'un centre médical. Il se présente généralement sous la forme d'un téléphone mobile ou d'un agenda électronique et agit comme intermédiaire pour la communication entre les trois tiers en utilisant Internet ou autre [15].

1.2.1.3 Système de soins

Le système de soin est l'entité qui reçoit toutes les informations sur l'état de santé du patient. Cette structure est généralement un hôpital, une clinique ou un centre de télémédecine où les médecins

évaluent les données médicales reçues afin de détecter et de traiter les maladies du patient à distance. Ce système doit protéger toutes les données personnelles et privées du patient et doit être capable de gérer plusieurs patients [15].

Le traitement des données médicales peut se faire de manière automatique grâce à des systèmes de rétroaction biologique, ou biofeedbacks : si une anomalie est détectée dans le corps du patient, les systèmes de biofeedback peuvent déclencher une procédure de traitement. Par exemple, si le taux de glucose dans le sang est faible ou élevé, un capteur implanté détecte le niveau de glucose et déclenche une pompe à insuline sans file pour réguler le taux de glucose. Un capteur qui détecte un arrêt cardiaque peut déclencher un défibrillateur cardiaque implantable sans fil pour alerter une ambulance, et peut envoyer un appel d'urgence à l'hôpital ou le médecin lorsque une chute est détectée. Les systèmes de biofeedback peuvent aussi être utiliser pour aider l'utilisateur dans ses mouvements. Dans ce cas, un signal physiologique tel que le mouvement d'un muscle facial peut être utilisé pour remplacer la fonction d'un membre blessé ou paralysé [15].

1.2.2 Enjeux des MBASNs

Les principaux enjeux auxquels fait face la conception des MBASNs sont [21] :

- La plage de communication sans fil doit être choisie de façon à ce que les appareils sans fil du MBASN peuvent être utilisés à l'échelle mondiale. Il existe différentes bandes de fréquences qui peuvent être utilisées pour des application des MABSNs comme MedRadio (401 $\backsim$ 406 MHz) pour les implants. Le problème d'interférences entre les communications de capteurs issus de différents MBASNs doit aussi être réglé [5].
- Le design de l'antenne d'un capteur est soumis à des restrictions sur sa taille, son matériau et sa forme. Seuls des matériaux non-corrosifs et biocompatibles comme le platinium et le titanium peuvent être utilisés pour les implants. Ces matériaux offrent, néanmoins, des performances inférieures à celle du cuivre.
- L'étude des caractéristiques de propagation du canal de transmission est impératif pour la conception de nouveaux capteurs sans fil [15]. L'expérimentation sur les capteurs implantés et portables est néanmoins difficile en raison de l'implication de sujets humains et de centres de soins ; tous deux régis par des lois gouvernementales.
- La consommation d'énergie dans les MBASNs est un enjeu majeur puisque les batteries des capteurs doivent durer plusieurs années, soit une durée d'au moins trois ans pour les capteurs assurant la stimulation cérébrale profonde. La consommation d'énergie doit essentiellement être prise en compte lors de la conception de nouveaux protocoles de la couche physique et de l'étude de nouveaux matériaux pour des équipements plus puissants et moins coûteux.

- La qualité de service et la fiabilité des MBASNs doivent être équivalentes ou meilleures à celles des technologies sans fil actuellement existantes dans les centres de santé. En effet, les applications étant souvent critiques et la surveillance à temps réel, les retards, la perte de données, l'imprécision de la localisation et d'autres erreurs peuvent avoir des conséquences graves sur la vie des patients et doivent absolument être gérées.
- La sécurité et la vie privée des patients sont un aspect majeur à prendre en considération dans les MBASNs. Les mécanismes de sécurité classiques ne sont pas adaptés en raison du manque d'interfaces utilisateurs, de leur inexpérience, de la limitation des capteurs en terme d'espace mémoire, d'énergie et de puissance de traitement, etc. Le renforcement des mesures sécuritaires est aujourd'hui un domaine de recherche à explorer encore plus [15].

1.3 Sécurité dans les MBASNs

Les MBASNs font face à de nombreux défis notamment celui de la protection contre la dégradation et l'accès illicite aux informations privées des patients. Ce problème peut être résolu grâce à la notion d'authentification qui désigne l'action d'identifier une entité puis de valider son identité selon une empreinte unique générée selon les quatre éléments ou facteur d'authentification existants [26] :

Facteur mémoriel : dont l'empreinte générée est une information que l'utilisateur a mémorisé. Exemple : mot de passe ;

Facteur matériel : dont l'empreinte est une information contenue dans un objet qu'il utilise. Exemple : certificat numérique sur une carte à puce ;

Facteur corporel : dont l'empreinte est une caractéristique corporelle. Exemple : empreinte digitale ;

Facteur réactionnel : dont l'empreinte est un geste que l'utilisateur peut reproduire. Exemple : une signature.

1.3.1 Biométrie comme moyen d'authentification

La biométrie est une technique plus souvent connue comme l'identification d'un individu en se servant de ses caractéristiques physiques [22]. Il existe plusieurs appondus biométriques, les plus connus sont [9] :

- **Biologiques :** Odeur, sang, salive, urine, Acide Désoxyribo Nucléique (ADN), etc.
- **Comportementales :** Voix, dynamique de la signature, démarche, etc.

- **Morphologiques :** Traits du visage, empreintes palmaires et digitales, iris, etc.
- **Physiologiques :** ECG, EMG, voix, etc.

En général, un identificateur biométrique, pour qu'il soit utilisé, doit répondre à certains critères [30]. Il doit être :

- **Universel :** il doit exister chez la plupart des individus, si ce n'est toute la population ;
- **Unique :** ou suffisamment différent chez deux individus quelconques ;
- **Permanent :** suffisamment invariant chez un individu pendant un intervalle de temps raisonnable ;
- **Mesurable :** et doit être facilement numérisé ;
- **Performant :** il doit assurer un bon rendement compte tenu des ressources limitées des systèmes ;
- **Acceptable :** par le public pour être utilisé comme identifiant ;
- **Robuste :** et difficile à reproduire pour éviter les actes de fraudes.

L'idée de combiner la biométrie à la cryptographie dans les MBASNs semble tout à fait être une bonne approche pour assurer la sécurité des données médicales [15] puisqu'il serait intéressant d'utiliser les ressources déjà existantes dans le corps humain comme moyen d'authentification. De plus, les identificateurs biométriques peuvent aussi servir à générer des clés de chiffrement symétriques utilisables par les capteurs dans un MBASN [5]. Pour cela, les identifiants doivent varier avec le temps afin d'assurer la fraicheur des clés de chiffrement et doivent être assez ressemblants lorsqu'ils sont mesurés simultanément par des capteurs du même corps ; c'est le cas des signaux physiologiques [22].

1.4 Conclusion

L'utilisation des MBASNs a beaucoup aidé les systèmes de soins et de santé dans leurs développement. Nous avons vu dans ce chapitre l'utilité d'un tel réseau à travers son architecture et son fonctionnement. Il s'avère être l'un des principaux fondements de l'énorme évolution que connaît la télémédecine aujourd'hui. Comme toute technologie, les MBASNs font faces à plusieurs défis et problèmes que les chercheurs concourent à résoudre. La sécurité des MBASNs est l'un des domaines de recherche où la biométrie est devenue très populaire dans l'élaboration de protocoles de sécurité. Le chapitre suivant portera sur un état de l'art des protocoles d'authentification et de partage de clé.

Chapitre 2

Taxonomie des protocoles d'authentification biométrique dans les MBASNs

2.1 Introduction

Les défis auxquels sont confrontés les *Medical Body Area Sensor Networks* (MBASNs) sont multiples et les solutions proposées n'en sont pas moins nombreuses [15] [21]. Le problème de sécurité est considéré comme un défis très important puisque les données qui transitent dans les MBASNs sont, non seulement privées, mais peuvent aussi être utilisées à mauvais escient mettant la vie des patients en péril. De ce fait, le développement de nouveaux protocoles d'authentification s'avère indispensable. Ces protocoles doivent tenir compte des bénéfices sur le plan des performances ainsi qu'à la contrainte des ressources énergétiques et matérielles limitées dans les systèmes mobiles de soins et de santé.

Ce chapitre sera consacré à la présentation et à la critique de quelques protocoles établis pour assurer l'authentification biométrique entre les capteurs sans fil. Pour cela, nous définirons les critères sur lesquels nous nous baserons pour critiquer les protocoles étudiés ainsi qu'une classification montrant les principales différences et similarités entre eux. Enfin, nous terminerons par une synthèse résumant les points forts et les points faibles des protocoles étudiés.

2.2 Critères de l'étude critique des protocoles étudiés

L'établissement de critères s'impose pour une bonne étude critique des protocoles proposés pour l'authentification biométrique. Cela nous permettra de cibler les défis auxquels nous ferons face lors de l'élaboration de notre contribution.

Notre travail s'inscrit dans le cadre de la proposition d'une technique d'authentification biométrique entre les capteurs du réseau MBASN. Les auteurs des protocoles présentés dans ce chapitre tentent tous de trouver une solution optimale au problème posé et la critique de ces protocoles se fera selon les critères suivants.

2.2.1 Sécurité et résistance aux attaques

Les MBASNs doivent être sécurisés contre tout type d'attaque portant atteinte à la vie privée du porteur et surtout au bon déroulement des processus de traitement du patient à distance. Les protocoles doivent être en mesure de contrer les attaques telles que l'usurpation d'identité, le vol de clés symétriques, l'attaque par force brute pour retrouver la clé secrète si elle a lieu et bien d'autres.

2.2.2 Exactitude des caractéristiques biométriques

Lorsque deux capteurs mesurent un même signal physiologique à un même instant, les deux ensembles des caractéristiques extraites ne sont pas tout le temps identiques. Les algorithmes proposés doivent être en mesure de contrer ce problème et réduire au maximum les taux de faux rejets (FRR,*False Rejection Rate*) et de fausses acceptations (FAR, *False Acceptance Rate*).

2.2.3 Consommation d'énergie

Les batteries des capteurs utilisés dans les MBASNs ont une durée de vie très limitée, il faut donc minimiser la consommation d'énergie.

2.2.4 Complexité de calcul et mémoire de stockage

Les capteurs disposent d'une capacité de calcul et de stockage très limitée. Un algorithme très coûteux en calculs ou en mémoire provoquera une lenteur au niveau de son exécution. Cela peut mener à des conséquences graves lors de cas d'urgences.

2.3 Etude critique de quelques protocoles d'authentification

Dans les protocoles étudiés, le problème de l'authentification biométrique entre les capteurs est abordé de deux manières différentes. D'une part, les protocoles assurent l'authentification biométrique sans générer une clé de chiffrement symétrique et, d'autre part, les capteurs s'échangent une clé symétrique, qu'elle soit générée ou non à partir de caractéristiques biométriques, tout en s'authentifiant entre eux.

2.3.1 Authentification sans partage de clés

Les protocoles suivants utilisent les caractéristiques biométriques pour l'authentification et ne prennent pas en considération la génération et l'échange de clés entre les capteurs du MBASN. Les caractéristiques biométriques sont représentées et utilisées de différentes manières afin de les comparer et de déterminer si les capteurs appartiennent au même MBASN ou pas.

- ***Un modèle d'authentification biométrique stochastique utilisant Uniformed GMM dans les réseaux corporels sans fil***

Wang et al. [32], ont proposé une approche basée sur un modèle de mélanges gaussiens (GMM, *Gaussian Mixture Model*) [25] pour générer une signature assurant ainsi l'authentification et l'intégrité des données. L'IPI (*Interpulse Interval*) [22] est utilisé ici comme générateur de caractéristiques biométriques pour la fabrication de cette signature via l'algorithme uniforme EM (*Expectation Maximisation*) [25] incluant une fonction de hachage pour assurer l'intégrité des caractéristiques biométriques et de l'information D concernant le patient à envoyer, comme le taux de glucose par exemple. Ainsi, l'ensemble de paramètres λ de la variable aléatoire IPI sont optimisés pour obtenir l'ensemble de paramètres $\tilde{\lambda}$ vérifiant le maximum de vraisemblance $J(\tilde{\lambda})$. $\tilde{\lambda}$ et $J(\tilde{\lambda})$ constituent la signature attachée à l'information D qui servira à authentifier le capteur émetteur au près du capteur récepteur.

Après réception de l'information D, le capteur récepteur suit le même algorithme uniforme EM et utilise l'information D reçue et ses propres caractéristiques IPI' pour obtenir sa propre estimation du maximum de vraisemblance $J'(\tilde{\lambda})$. Si IPI et IPI' présentent une forte ressemblance alors $J(\tilde{\lambda})$ et $J'(\tilde{\lambda})$ seront très proches. Le récepteur décidera de l'authenticité de l'information reçue si la différence entre $J(\tilde{\lambda})$ et $J'(\tilde{\lambda})$ ne dépasse pas une valeur maximale T.

Discussion et critiques

La solution proposée dans cet article assure l'authentification entre deux capteurs du même MBASN grâce à la biométrie ainsi que l'intégrité des données envoyées en utilisant une fonction de hachage. Wang et al. considèrent le fait que les signaux biométriques mesurés sur un même corps peuvent ne pas être totalement identiques, le taux de faux rejet est ainsi moins élevé. Cependant, l'utilisation des données biométriques pour générer uniquement une signature peut engendrer des coûts supplémentaires lorsque cette procédure est combinée à une autre procédure de partage de clés de chiffrement.

- ***Authentification des entités basée sur le signal physiologique dans les systèmes mobiles de soins***

Bao et al. [5], ont proposé un protocole d'authentification où la distance de Hamming est utilisée pour comparer entre les caractéristiques biométriques et déduire si les capteurs sont du même MBASN ou pas. La procédure d'authentification implique deux entités : un prouveur et un vérifieur et se déroule en deux sessions : la première session sert à authentifier un capteur et la deuxième session sert à authentifier l'autre capteur. Dans une architecture Client-Serveur, le capteur serveur entame le processus d'authentification comme illustré dans la figure 2.1.

Lors de la première session, le serveur envoie les caractéristiques biométriques I_0 chiffrées et un nombre R_s généré aléatoirement selon le protocole proposé en [4]. Le capteur client déchiffre les caractéristiques reçues à l'aide de la même procédure [4] et les compares aux siennes. Si la distance de Hamming d entre I_0 et I_1 est supérieure à une valeur maximale T, alors le processus d'authentification est abandonné, sinon le serveur est authentifié. Durant la deuxième session, le serveur devient vérifieur, le client devient prouveur et la même procédure est suivie pour authentifier le client durant la deuxième session en utilisant les mêmes caractéristiques.

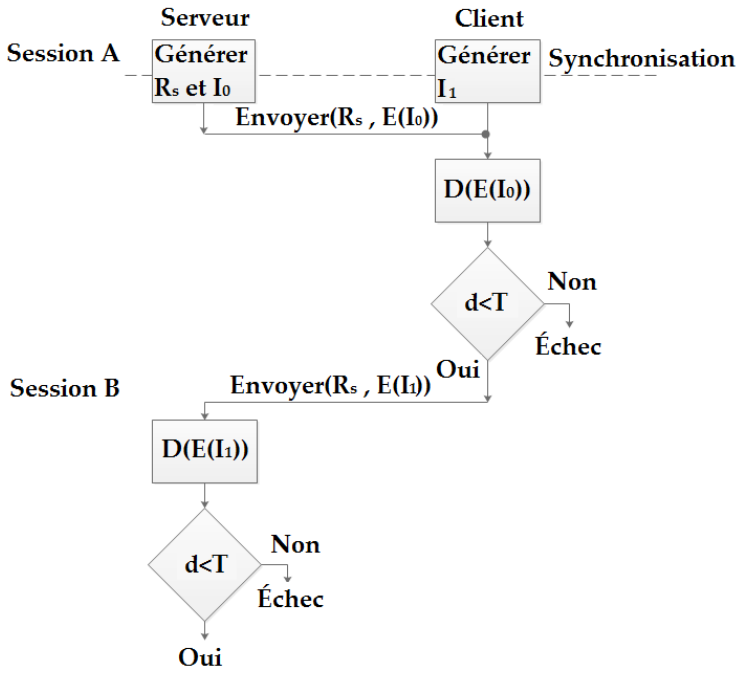

FIGURE 2.1 – Processus d'authentification [5].

Discussion et critiques

La sécurité de ce protocole dépend de celle de l'algorithme qu'il utilise pour crypter la communication entre les deux capteurs. L'utilisation d'un algorithme indépendant, peut néanmoins augmenter la complexité de la procédure en engendrant des coûts de calculs et une consommation d'énergie supplémentaires. De plus, un intrus se faisant passer pour un client, peut recevoir le message $(R_s, E(I_0))$ du serveur et le lui renvoyer directement pour s'authentifier. Ainsi, le serveur calculera la distance de Hamming entre I_0 et lui même et obtiendra $d = 0$; l'intrus est alors incrusté.

2.3.2 Authentification avec partage de clés

Les caractéristiques biométriques sont utilisées par les protocoles étudiés dans cette section pour le partage de clés de manière authentifiée. Certains de ces protocoles permettent aux capteurs du même MBASN de générer une clé secrète à partir des caractéristiques biométriques, tandis que d'autres, utilisent ces caractéristiques pour faciliter l'échange de clés. L'authentification est assurée par l'utilisation des caractéristiques biométriques propres au corps humain ; deux capteurs ne pourront générer la même clé que s'ils appartiennent au même MBASN.

2.3.2.1 Génération non biométrique des clés

Dans les protocoles présentés ci-dessous, les caractéristiques biométriques ne sont pas utilisées pour la génération d'une clé secrète, mais plutôt pour faciliter le partage de cette clé entre deux ou plusieurs capteurs appartenant au même MBASN.

- ***PSKA : Modèle de partage de clés utile et sûr pour les réseaux corporels***

Venkatasubramanian et al. [31], ont proposé un protocole basé sur les signaux physiologiques permettant à deux capteurs d'un même MBASN d'échanger une clé de chiffrement symétrique tout en s'authentifiant. Le principe de la solution proposée par Venkatasubramanian et al., PSKA, se résume comme suit : les deux capteurs (s et r) mesurent le signal physiologique à un même instant et en extraient chacun un vecteur de caractéristiques de taille n de la forme $F_i = f_i^1, f_i^2, ..., f_i^n$ où $i \in \{s, r\}$.

Le capteur émetteur (s) construit un polynôme $p(x)$ à partir de coefficients générés aléatoirement et qui, après concaténation, forment la clé symétrique. Ce polynôme est utilisé avec le vecteur F_s de l'émetteur pour former l'ensemble $P = \{(f_s^i, p(f_s^i)) : i = 1, .., n\}$ auquel sont ajoutés des points aléatoires appelés « *chaff points* » pour enfin obtenir le « *fuzzy vault* », littéralement « coffre-fort flou ». Avant d'être envoyé au capteur récepteur (r), le « *fuzzy vault* » est brouillé en permutant les positions des points le formant pour garantir que les point aléatoires et les points véritables de l'ensemble P soient indiscernables. À la réception du « *fuzzy vault* », le capteur récepteur le débrouiller en utilisant sa version locale des caractéristiques F_r. Il élimine ainsi les points aléatoires pour retrouver le polynôme $p(x)$ à l'aide de l'interpolation de Langrange et reconstruit la clé symétrique K.

La figure 2.2 illustre le processus de PSKA où R représente le « *fuzzy vault* » brouillé, émis par le capteur émetteur, et Q, l'ensemble utilisé par le capteur récepteur pour retrouver le polynôme p du départ. L'ensemble $Q = \{(b, c) : (b, c) \in R, b \in F_r\}$ est obtenu en projetant les caractéristiques du capteur récepteur F_r sur le « *fuzzy vault* » R.

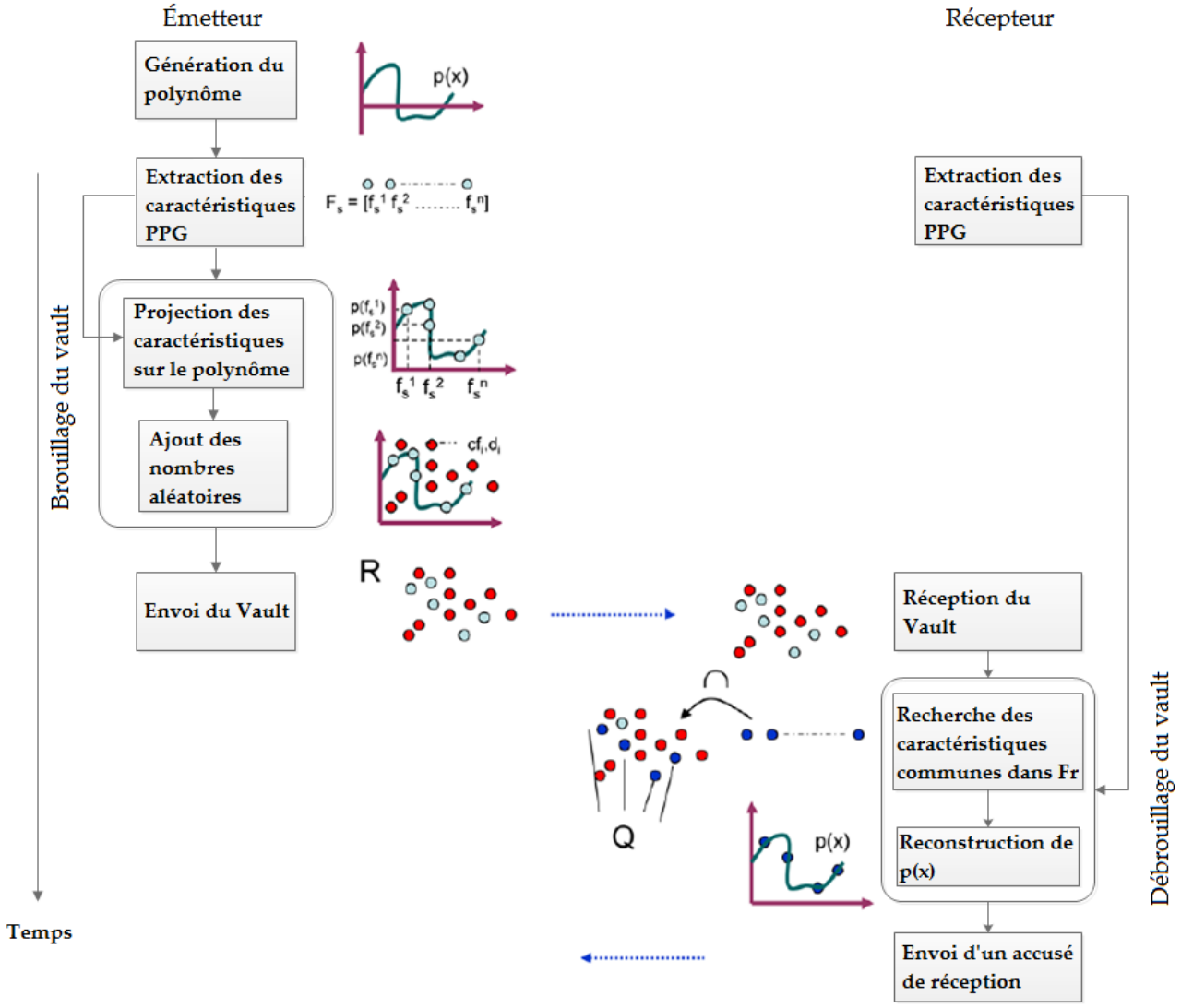

FIGURE 2.2 – Protocole PSKA [31].

Discussion et critiques

PSKA permet d'assurer l'authentification des capteurs en assurant que seuls les capteurs du même MBASN peuvent se mettre d'accord sur une clé partagée, mais aussi, d'assurer la confidentialité et l'intégrité des données échangées en utilisant une clé symétrique générée d'une manière aléatoire pour éviter l'attaque par force brute. L'utilisation du « *fuzzy vault* » assure que, même si deux capteurs peuvent ne pas obtenir exactement les mêmes caractéristiques, ils peuvent encore échanger une clé symétrique de manière sécurisée. Cela assure un taux FRR moins élevé.

La sécurité de PSKA dépend fortement de la taille du « *fuzzy vault* ». En effet, plus la taille du « *fuzzy vault* » est grande, plus un attaquant aura du mal à retrouver l'information cachée dans le

«*fuzzy vault* ». Cela augmente, cependant, la probabilité que les points aléatoires ajoutés par l'émetteur coïncident avec les caractéristiques du récepteur causant, de ce fait, un faux rejet [13]. En plus, la consommation d'énergie et la complexité en matière de stockage et de calcul deviennent élevées lors de la reconstruction du polynôme, sans compter les ressources déjà nécessaires au processus de génération aléatoire de la clé symétrique.

- ***Utilisation des signaux physiologiques pour l'authentification dans un protocole de partage de clés de groupe***

Singh et al. [29], ont proposé un protocole basé sur le processus d'échange de clés de Diffie-Hellman [11] pour générer une clé de groupe dans un MBASN. Les caractéristiques biométriques sont utilisées pour authentifier les n capteurs du même MBASN lors de l'échange de la clé de groupe.

Les capteurs sont liés entre eux en anneau. Chaque capteur S_i choisit un T_i aléatoire qu'il doit diffuser aux autres capteurs. Les signaux physiologiques sont alors mesurés par tous les capteurs aux différents instants T_i. À partir de cette étape, chaque message émis ou diffusé par un capteur S_i est chiffré en utilisant la fonction *XOR* avec le signal physiologique V_i. Le protocole de Diffie-Hellman [11] est alors appliqué : Chaque capteur S_i calcule $t_i = g^{r_i}$, où $r_i, g \in \mathbb{Z}/p\mathbb{Z}$, et l'envoie aux deux capteurs qui lui sont adjacents, puis il utilise t_{i-1} et t_{i+1} pour calculer $Z_{i-1,i} = {t_{i-1}}^{r_i}$ et $Z_{i,i+1} = {t_{i+1}}^{r_i}$. Il calcule ensuite $X_i = Z_{i,i+1} - Z_{i-1,i}$ et le diffuse aux autres capteurs. La clé de groupe Z est calculée comme suit :

$$Z = nZ_{i-1,i} + (n-1)X_i + (n-2)X_{i+1} + ... + X_{i-2}. \tag{2.1}$$

Enfin, chaque S_i diffuse (S_i, V_i) chiffré avec la clé Z pour confirmer la réussite du processus.

Discussion et critiques

L'utilisation de caractéristiques biométriques permet de générer une clé de groupe avec le protocole de Diffie-Hellman tout en assurant l'authentification au sein du MBASN. Un attaquant ou un capteur issu d'un autre MBASN ne pourra pas se faire passer pour un capteur légitime du réseau pour obtenir la clé secrète s'il n'a pas les mêmes caractéristiques biométriques. Cependant, ces caractéristiques sont issues de signaux pas tout à fait identiques entre eux ; l'ensemble des V_i obtenus n'est pas toujours le même pour tous les capteurs, les X_i diffusés en utilisant ces caractéristiques sont, de ce fait, différents. De plus, le coût de communication est élevé, compte tenu des nombreuses diffusions et échanges de messages nécessaires à la génération de clé.

2.3.2.2 Génération biométrique des clés

Les caractéristiques biométriques extraites à partir d'un signal physiologique sont utilisées par les protocoles suivants pour générer une clé secrète et faciliter son échange entre les capteurs du même MBASN.

• ***OPFKA : Protocole de partage de clés sûr et efficace basé sur des caractéristiques physiologiques ordonnées dans les réseaux corporels sans fil***

Hu et al. [13], ont proposé un protocole, OPFKA, qui permet la génération et l'échange d'une clé symétrique entre deux capteurs d'un même MBASN. Pour ce faire, chacun des deux capteurs impliqués dans ce processus extrait un ensemble de caractéristiques biométriques à partir du signal physiologique mesuré après synchronisation. Les deux ensembles générés sont ordonnés en suivant une certaine politique pour obtenir un ordre que seuls ces capteurs connaissent. La figure 2.3 illustre le déroulement de OPFKA [13], où ID_i représente l'identifiant du capteur i.

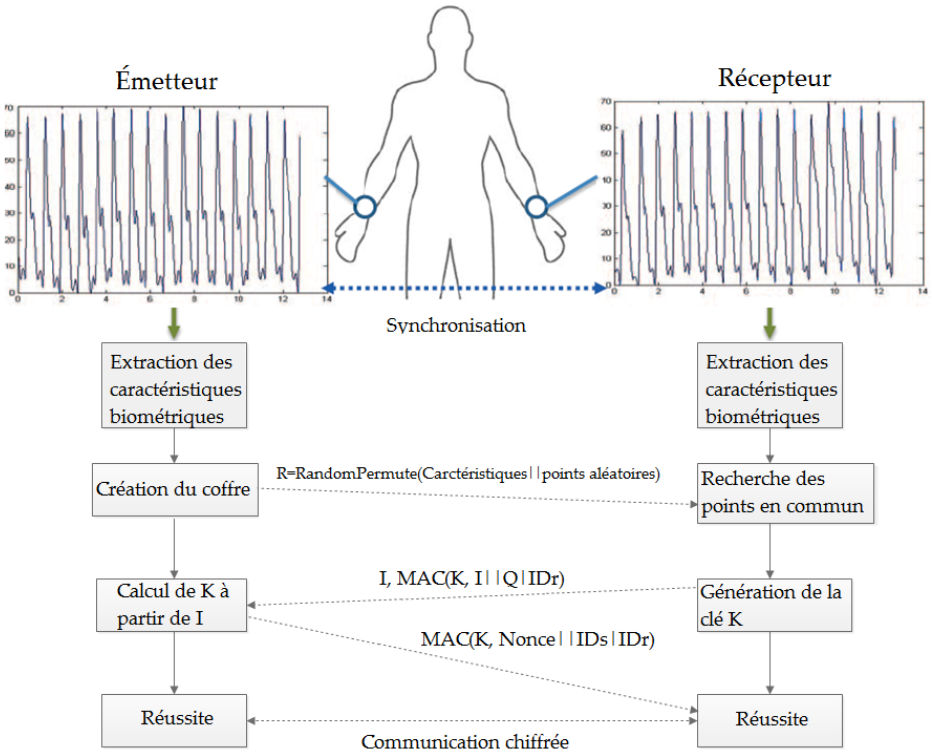

FIGURE 2.3 – Protocole OPFKA [13].

Le capteur C_1 utilise un bruit simple pour cacher son vecteur de caractéristiques biométriques dans un « Coffre » ; les postions des points aléatoires générés à partir du bruit et celles des caractéristiques

biométriques sont permutées à l'aide d'une fonction de permutation aléatoire, *RandomPermute*, avant que le coffre ne soit envoyé au capteur récepteur. C_2 le capteur récepteur, utilise sa propre version du vecteur pour identifier les caractéristiques biométriques communes Q avec C_1 dans le coffre reçu. Ainsi, C_2 génère une clé K en fonction des caractéristiques biométriques retenues. Il construit ensuite un ensemble ordonné d'indices I et l'envoie au capteur C_1 pour qu'il extraie du coffre les mêmes caractéristiques biométriques qu'a utilisé le capteur C_2 pour générer la clé symétrique K. Un code d'authentification de message (MAC, *Message Authentication Code*) est envoyé à C_2 pour confirmer la réussite de ce processus.

Discussion et critiques

L'utilisation des caractéristiques biométriques permet d'authentifier les deux capteurs et l'utilisation du coffre permet la génération d'une même clé symétrique K, même si les deux vecteurs de caractéristiques ne sont pas totalement identiques. Cependant, l'envoi non chiffré du coffre et de l'ensemble d'indices I permet à tout attaquant de déduire la clé K. En utilisant cette clé, un attaquant pourra usurper l'identité des deux capteurs et contourner le système d'authentification.

- ***Cryptographie et authentification basées sur l'ECG dans les réseaux corporels***

Zhang et al. [35], ont proposé le protocole ECG-IJS (*Electrocardiogram Improved Jules Sudan*) pour permettre à deux capteurs appartenant au même MBASN de partager une clé générée à partir de signaux ECG, tout en utilisant ces mêmes signaux pour s'authentifier entre eux. Zhang et al. supposent que les capteurs, émetteur et récepteur, ont tous les deux la capacité de mesurer les signaux ECG du corps humain et utilisent la même méthode d'extraction de caractéristiques biométriques.

Les deux capteurs, émetteur et récepteur, mesurent simultanément le signal ECG pour en extraire les caractéristiques biométriques $F = \{f_i\}$ et $F' = \{f_i'\}$. L'émetteur utilise alors F pour générer la clé secrète K et pour construire un unique polynôme unitaire p de degré s, où x est l'indéterminé. p est obtenu ainsi :

$$p(x) = \prod_{f_i \in F} (x - f_i). \tag{2.2}$$

Les coefficients obtenus entre les degrés $s-1$ et $s-t$ sont envoyés alors au récepteur, où t représente le degré de tolérance, sachant que les caractéristiques extraites ne sont pas identiques entre les capteurs.

Le capteur récepteur construit un polynôme p_{haut} de degré s à partir des coefficients reçus d'où

il déduit l'ensemble $F'' = \{(f_i', y_i) : p_{haut}(f_i') = y_i\}$. Il utilise ensuite l'algorithme Reed-Solomon [6] sur l'ensemble F'' pour construire le polynôme p_{bas} de degré $s - t - 1$. Le polynôme p peut être reconstruit ainsi :

$$p(x) = p_{haut}(x) - p_{bas}(x). \tag{2.3}$$

Enfin, la clé est obtenue en calculant les racines du polynôme p. Le processus ECG-IJS est illustré dans la figure 2.4.

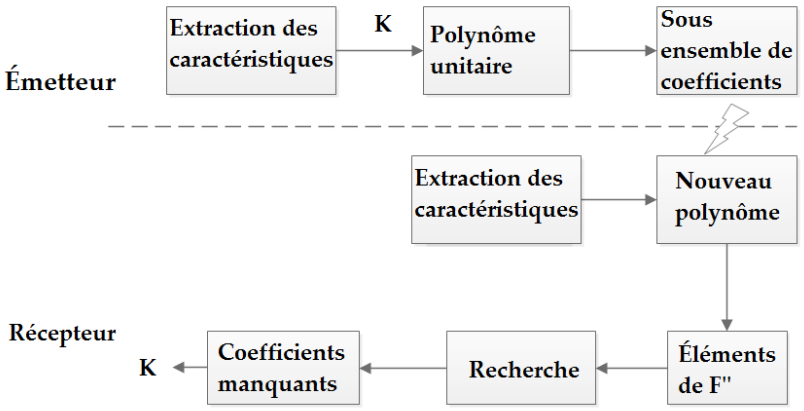

FIGURE 2.4 – Protocole ECG-IJS [35].

Discussion et critique

ECG-IJS permet la génération d'une clé symétrique aléatoirement tout en assurant sa confidentialité et l'authentification des capteurs. Le protocole tolère le fait que les caractéristiques biométriques ne soient pas totalement identiques et n'a pas recours à des points aléatoires pour cacher la clé, d'où une utilisation plus modérée de la mémoire. Cependant, il a été prouvé par Sidelnikov et Shestakov [28] qu'une attaque polynomiale peut facilement reconnaitre les codes Reed-Solomon, ce qui remet en cause la sécurité du protocole ECG-IJS.

- ***Modèle de parage de clés efficace et sûr utilisant les signaux physiologiques dans les BANs***

Kishore et al. [16], ont proposé un protocole utilisant le concept du «*fuzzy vault*» pour la génération et l'échange d'une clé secrète entre deux capteurs. Les deux capteurs concernés mesurent un même signal physiologique au même instant. Le vecteur S de caractéristiques extraites à partir du signal physiologique et des codes CRCs (*Cyclic Redundancy Check*) [23] obtenus à partir d'un ensemble de points générés aléatoirement, sont utilisés pour former l'ensemble $R = \{(s,x) : s \in S, x \in [0,1]\}$.

L'ensemble R est utilisé pour générer une spline cubique [17] ; une spline cubique est une courbe définie par morceaux en utilisant un ensemble de polynômes cubiques. Les coefficients des polynômes sont concaténés pour former la clé secrète. Le même ensemble R est caché en utilisant la technique du « *fuzzy vault* » où des points générés aléatoirement, appelés « *chaff points* », y sont ajoutés avant d'être envoyé au capteur récepteur. Ceci est illustré dans la figure 2.5.

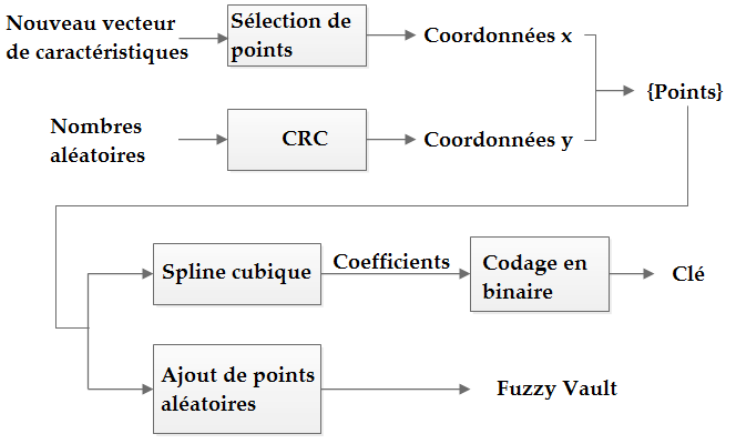

FIGURE 2.5 – Processus de génération du « *fuzzy vault* » [16].

Le capteur récepteur utilise alors sa version locale du signal physiologique mesuré pour trouver les caractéristiques biométriques cachées dans le « *fuzzy vault* » reçu et reconstruire les polynômes cubiques de la *spline*, après détection d'erreurs, pour enfin trouver la clé symétrique. Le processus de débrouillage du « *fuzzy vault* » est illustré dans la figure 2.6.

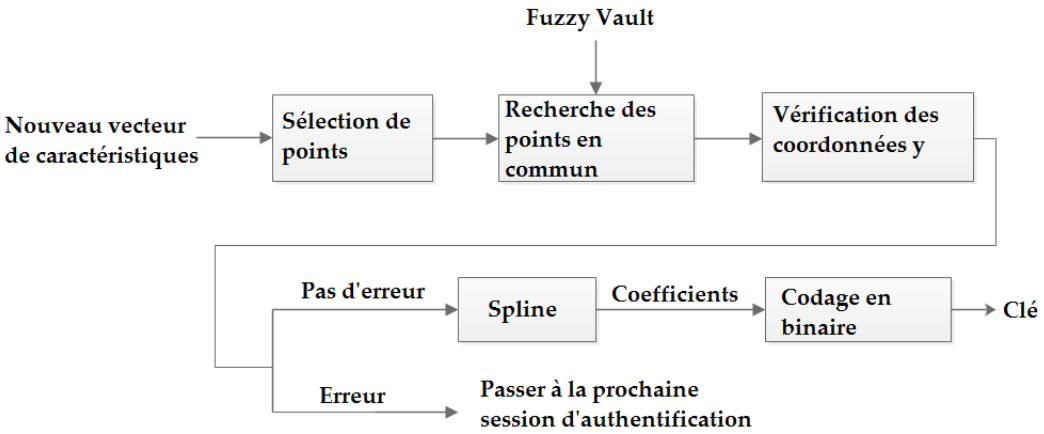

FIGURE 2.6 – Processus de débrouillage du « *fuzzy vault* » [16].

Discussion et critiques

Ce protocole assure l'authentification et l'échange de clé symétrique à l'aide de caractéristiques biométriques, tout en prenant en considération les problèmes relatifs à la collecte des caractéristiques physiologiques sur un même corps. L'utilisation du « *fuzzy vault* » assurant cela permet d'avoir des taux FRR et FAR moins élevés.

Le recours à la méthode des *splines* [17] pour l'interpolation permet d'obtenir les résultats voulus tout en réduisant la complexité de calcul liée à l'interpolation polynômiale [17]. Le problème de la taille du « *fuzzy vault* » reste néanmoins non résolu.

• ***PFKA : Partage de clés basé sur les caractéristiques physiologiques dans les réseaux corporels sans fil***

Jammali et al. [14], ont proposé le protocole PFKA pour la génération et l'échange d'une clé symétrique, à l'aide des caractéristiques physiologiques extraites à partir du signal ECG, entre deux capteurs issu d'un même MBASN. Le protocole PFKA fonctionne comme suit : les capteurs concernés mesurent le signal ECG au même moment et en extraient les vecteurs de caractéristiques F_s et F_r. Le capteur émetteur génère ensuite un vecteur F' de nombres aléatoires qu'il divise en deux parties F'_{droit} et F'_{gauche} ; il en fait de même pour le vecteur F_s et obtient F_{s_droit} et F_{s_gauche}. La fonction XOR est alors appliquée entre F'_{gauche} et F_{s_droit} et entre F'_{droit} et F_{s_gauche} pour former le nouveau vecteur $F_{modifie}$ qui devra être codé avec un codage Reed-Solomon [6] avant d'être envoyé au capteur récepteur. Le processus de modification du vecteur de caractéristiques F_s est décrit dans la figure 2.7.

Le capteur récepteur recevra en tout : les identifiants des deux capteurs, un nonce, le vecteur $F_{modifie\_code}$ et le code d'authentification de message $MAC(F' \oplus N_0)$. Le récepteur décode le vecteur $F_{modifie\_code}$ et obtient le vecteur $F_{modifie}$. Il suit ensuite le processus inverse pour retrouver le vecteur F' en utilisant F_r. À la fin du processus, chaque capteur aura en sa possession la clé K, calculée en appliquant une fonction de hachage sur le résultat de la concaténation entre le vecteur de caractéristiques F_i, où $i \in \{s,r\}$, et le vecteur F'.

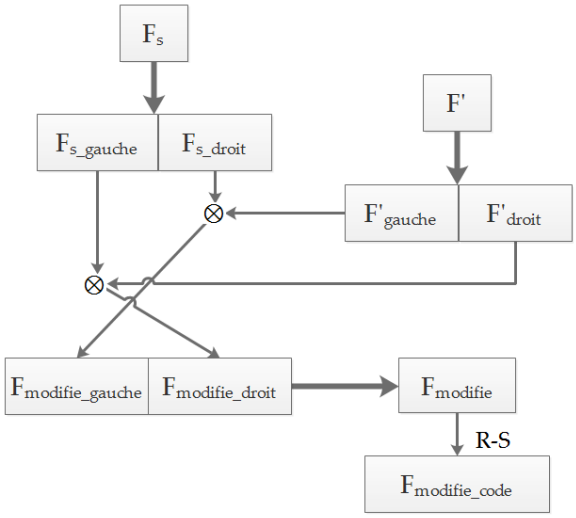

FIGURE 2.7 – Processus de modification du vecteur F_s du protocole PFKA [14].

Discussion et critiques

Le protocole PFKA permet de partager une clé entre deux capteurs de manière authentifiée. En effet, un intrus, n'ayant pas les caractéristiques physiologiques du patient, ne pourra pas retrouver le vecteur de nombres aléatoires F', et encore moins, obtenir la clé partagée. Néanmoins, le signal ECG mesuré n'est pas le même pour les deux capteurs légitimes ; bien que praticable pour l'authentification, les deux vecteurs de caractéristiques F_s et F_r issues de ce signal ne sont pas identiques, et par conséquent, la clé K calculée par les deux capteurs n'est pas exactement la même.

2.4 Synthèse

Plusieurs protocoles ont été proposés pour sécuriser les MBASNs tout en exploitant les caractéristiques biométriques changeantes du corps humain. Les protocoles étudiés permettent d'assurer l'authentification des capteurs et certains d'entre eux permettent, en plus, de générer des clés symétriques. Ces clés symétriques seront utilisées pour chiffrer et authentifier les messages échangés entre les capteurs du même MBASN. La figure 2.8 montre la classification des différents protocoles d'authentification biométrique étudiés.

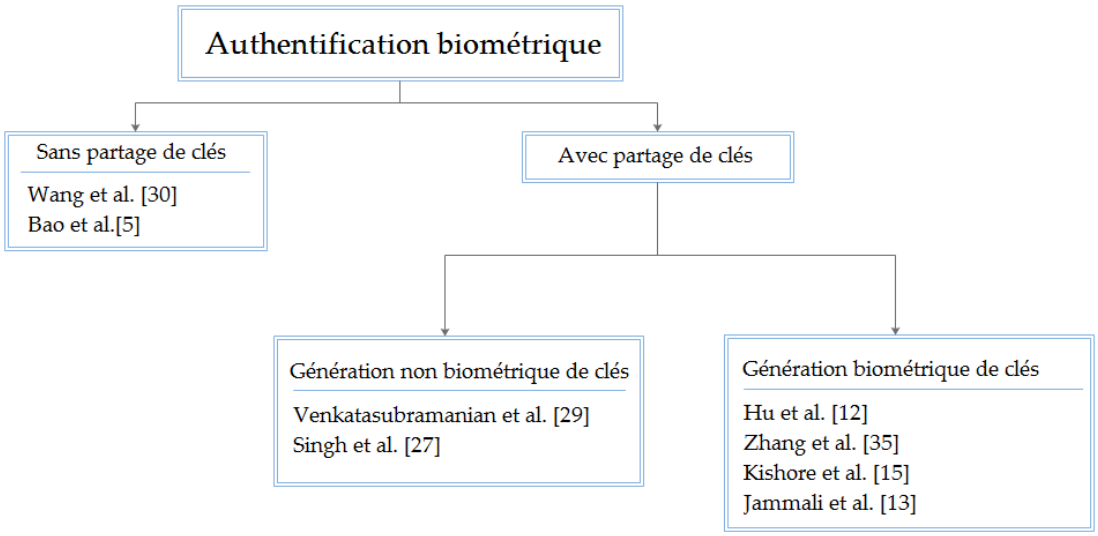

FIGURE 2.8 – Classification des protocoles étudiés pour l'authentification biométrique.

Nous avons remarqué que certains protocoles étudiés sont plus performants que d'autres, mais requièrent plus de ressources. Afin de mieux comprendre la diversité des protocoles étudiés dans ce chapitre et traitant le problème d'authentification biométrique dans les systèmes mobiles de soins et de santé, nous proposons une comparaison à base des critères de critique cités précédemment. Le tableau 4.1 résume cette comparaison entre les travaux étudiés dans ce chapitre ; le signe (✓) signifie que le protocole assure la fonction ou résout le problème de manière optimisée, contrairement au signe (X). Nous y avons ajouté notre protocole d'authentification et de partage d'une clé, dénommé ECG-AS, qui sera présenté dans le chapitre suivant.

		Sécurité et résistance aux attaques	**Exactitude des caractéristiques biométriques**	**Optimisation de la consommation d'énérgie**	**Complexité de calcul et mémoire de stockage**
Sans partage de clés	Wang et al. [32]	✓	✓	X	✓
	Bao et al. [5]	✓	X	✓	✓
Avec partage de clés	Venkatasubramanian et al. [31]	✓	✓	X	X
	Singh et al. [29]	✓	X	X	✓
	Hu et al. [13]	X	✓	✓	✓
	Zhang et al. [35]	X	✓	X	X
	Kishore et al. [16]	✓	✓	X	✓
	Jammali et al. [14]	X	X	X	X
	ECG-AS	✓	✓	✓	✓

TABLE 2.1 – Comparaison des protocoles d'authentification biométrique étudiés.

Dans certaines solutions [13] [14] [16] [35] , les signaux physiologiques, originellement utilisés pour des consultations à distance, servent à la génération et à l'échange de clés symétriques, ce qui semble être une bonne approche dans la mesure où aucun algorithme supplémentaire de génération de

nombres aléatoires ou de chiffrement n'est utilisé, réduisant ainsi la complexité en termes de stockage et surtout de calcul.

Nous avons vu à travers ces solutions que l'utilisation directe des caractéristiques physiologiques peut poser quelques problèmes lors de l'authentification et même lors de la génération de la clé symétrique. Un capteur peut être rejeté à tort parce que la différence entre ses caractéristiques et celles des autres capteurs est trop grande et la clé symétrique calculée par un capteur peut ne pas être la même que celle qui a été calculée par l'autre capteur. Les protocoles [13] [31] [32] [35] essayent quand même de contrer ce problème en utilisant des techniques comme le « *fuzzy vault* », l'algorithme EM (*Expectation Maximisation*) et IJS (*Improved Jules Sudan*).

2.5 Conclusion

Bien que l'authentification biométrique résout les problèmes d'accès aux informations privées et d'interférence entre les capteurs de plusieurs MBASNs, il est difficile de garantir l'exactitude des caractéristiques biométriques utilisées à cet effet et de trouver un accord entre performance et économie des ressources des capteurs.

Après l'étude de quelques solutions proposées, nous avons pu identifier deux catégories de protocoles : des protocoles permettant l'authentification biométrique entre les capteurs d'un même MBASN ainsi que des protocoles permettant, en plus de l'authentification biométrique, l'échange d'une clé symétrique entre deux ou plusieurs capteurs du MBASN. Ainsi, nous avons pu soulever précisément les problèmes auxquels nous devons faire face pour obtenir une solution qui répond aux critères cités précédemment et qui présentera de meilleurs résultats.

Le chapitre qui suit fera l'objet de notre contribution qui est basée l'utilisation de la biométrie pour l'authentification des capteurs dans les systèmes mobiles de soins et de santé.

Chapitre 3

ECG-AS : Electrocardiogram-based Authentication Scheme

3.1 Introduction

Dans les *Medical Body Area Sensor Network* (MBASNs), les capteurs communiquent entre eux en utilisant une transmission sans fil afin de ne pas restreindre les mouvements du patient. Cependant, la mobilité des capteurs dans les MBASNs fait qu'ils sont plus vulnérables aux attaques que les réseaux filaires. En effet, des intrus peuvent facilement s'incruster dans un réseau pour écouter le trafic et injecter ou répliquer d'anciens messages. Les capteurs doivent être en mesure de s'échanger des informations sécurisées. Les mécanismes de sécurité basés sur la biométrie permettent, en général, de cacher ou de générer des clés destinées à être partagée entre les capteurs du même MBASN.

Ce chapitre sera consacré à la présentation de notre protocole d'authentification, baptisé *Electrocardiogram-based Authentication Scheme* (ECG-AS), basé sur la technique biocryptographique permettant d'assurer l'authentification des capteurs entre eux au sein du même MBASN grâce aux données physiologiques du patient pour ainsi, sécuriser la transmission et éviter les problèmes d'interférences entre plusieurs capteurs appartenant à des MBASNs différents. Nous définirons aussi un modèle d'attaque sur lequel nous nous baserons pour démontrer le niveau de sécurité de notre protocole.

3.2 Motivation

Dans la télémédecine, l'accès en temps réel aux données du patient est un enjeu majeur pour les professionnels de soins et de santé, car cela leur permet de diagnostiquer des anomalies sur le corps du patient et de les traiter au plus vite. L'intégrité des données mesurées sur le corps du patient doit absolument être assurée, autrement, les diagnostiques seront faussés et les traitements inappropriés. Aussi, la divulgation des données médicales sur le patient peut être la cause de stigmatisations sociales et de discrimination négative lorsqu'elles concernent des troubles d'ordre psychiatrique par exemple, ou encore, elles peuvent avoir une valeur économique et être vendues aux médias. La confidentialité des données médicales doit, dans ce cas, impérativement être prise en compte, non seulement pour protéger la santé du malade, mais aussi pour protéger sa vie privée [3].

Dans les MBASNs, plusieurs capteurs peuvent être à portée sans pour autant appartenir au même corps. Les interférences entre les différents capteurs constitue une autre menace pour les MBASNs. En effet, ces interférences peuvent influencer les diagnostiques à distance, soit en masquant une anomalie qui doit être traitée, soit en administrant un traitement causant des interactions médicamenteuses dangereuses [15]. En résume, les systèmes mobiles de soins et de santé peuvent être en proie à plusieurs menaces, et les attaques peuvent être tant bien intentionnelles qu'accidentelles.

Le but de notre travail est de protéger la communication entre les capteurs du MBASN en garantissant l'authentification lors du partage d'une clé de chiffrement symétrique. La biométrie combinée à la cryptographie semble être une bonne approche pour l'authentification et la génération de clés aléatoires dans les MBASNs [15]. En effet, les capteurs d'un même MBASN peuvent s'authentifier entre eux en utilisant un attribut unique du corps qui les porte. Outre ces capteurs, une autre entité ne pourra ni deviner les caractéristiques biométriques, ni en reproduire d'autres pour s'authentifier auprès de ces capteurs. De plus, les signaux physiologiques tels que l'électrocardiogramme (ECG) et le photoplethysmogramme (PPG) ne sont pas stables et varient avec le temps, ce qui garantit la fraicheur des clés générées à partir de ces signaux [22]. Cependant, l'insuffisance des ressources énergétiques, de calculs et de stockage chez les capteurs rend la tâche ardue lors de l'établissement d'un protocole d'authentification équilibrant entre efficacité et coût minimal.

3.3 Notions préliminaires sur la cryptographie par courbes elliptiques

Une courbe elliptique E est définie sur un corps fini F_p, où p est le cardinal du corps, par l'équation suivante [2] :

$$y^2 \bmod p = x^3 + ax + b \bmod p, \tag{3.1}$$

où a et b sont des nombres entiers répondant à la condition suivante :

$$4a^3 + 27b^2 \bmod p \neq 0. \tag{3.2}$$

Les constantes a et b ainsi qu'un point générateur G appartenant à la courbe, constituent en grande partie les paramètres du domaine de la cryptographie par les courbes elliptiques (ECC, *Elliptic Curve Cryptography*) [2].

3.3.1 Multiplications et additions dans les les courbes elliptiques

L'addition de deux points d'une courbe se fait à travers l'opération dite du « *point addition* » [2] :

Soit $L(x_l, y_l)$ le résultat de l'addition de deux points distincts $K(x_k, y_k)$ et $J(x_j, y_j)$ de la courbe elliptique E, et soit (D), la droite passant par les point K et J. Le point L est la réflexion de l'intersection entre la droite (D) et la courbe E. Ceci est illustré sur la figure 3.1(a).

Analytiquement, les coordonnées de L sont obtenues ainsi [2] :

$$x_l = s^2 - x_j - x_k, \tag{3.3}$$

$$y_l = -y_j + s(x_j - x_l), \tag{3.4}$$

où s est la pente de la droite (D) obtenue comme suit :

$$s = \frac{y_j - y_k}{x_j - x_k}. \tag{3.5}$$

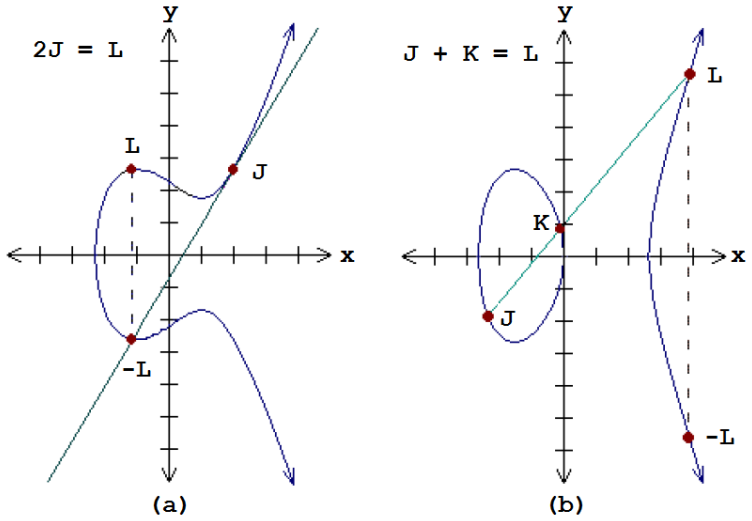

FIGURE 3.1 – Opérations du « *point addition* » (a) et du « *point doubling* » (b) [2].

Lorsque $K = J$, l'opération du « *point doubling* », illustrée sur la figure 3.1(b), est alors utilisée. La seule différence entre les deux opérations réside dans le calcul de s. Dans le « *point doubling* », s est la tangente à la courbe E au point K, elle est calculée comme suit [2] :

$$s = \frac{3x_j^2 + a}{2y_j}. \tag{3.6}$$

La multiplication d'un point de la courbe par un nombre requiert l'utilisation combinée des deux opérations « *point doubling* » et « *point addition* ».

3.4 Identificateur biométrique utilisé

Selon Poon et al. [22], le rythme cardiaque peut être un excellent générateur de caractéristiques biométriques pour la sécurisation des MBASNs. En effet, les signaux issus du rythme cardiaque sont de nature chaotique, pouvant ainsi générer des caractéristiques biométriques aléatoires.

L'ECG, ou la mesure du signal électrique du cœur, présente une entropie élevée et est difficile à falsifier ou à reproduire [33] ; idéale pour l'authentification, la génération et la mise à jour de clés aléatoires, contrairement aux identificateurs biométriques morphologiques moins robustes tels que l'iris, le visage et l'empreinte palmaire [22]. En effet, l'intervalle de temps entre deux battements du cœur successifs, à un instant donné, est le même pour tous les capteurs mesurant le même signal ECG, mais est différent pour chaque individu. L'IPI (*Interpulse Interval*) peut, dans ce cas, être utilisé pour

différencier entre les capteurs appartenant au même MBASN et ceux appartenant à un autre réseau [33]. De plus, la mesure du signal ECG peut se faire à partir de plusieurs endroits du corps humain et à basse fréquence, ce qui permet un prélèvement à moindre coût, sans compter qu'il est plus universel puisqu'il concerne tout être vivant, quelle que soit sa morphologie.

En conséquence, nous utiliserons dans notre protocole, des caractéristiques physiologiques extraites à partir de l'ECG pour la génération et la mise à jour de clés symétriques aléatoires, ainsi que pour l'authentification entre les capteurs du même MBASN.

3.5 Modèle du système

Dans les MBASNs, les capteurs sans fil ont la capacité de mesurer des paramètres de santé (ECG, PPG, EEG, ect.) sur le corps du patient qui les porte. Ces données peuvent être envoyées, soit directement, soit par l'intermédiaire d'un nœud head chargé de les envoyer au data hub, qui les transmettra ensuite au centre de traitement centralisé ou au serveur d'information de l'hôpital où les professionnels de soins et de santé pourront établir un diagnostique.

Notre protocole vise à sécuriser la communication entre les capteurs de façon à ce qu'aucun capteur ne puisse échanger de message relatif au patient avec un intrus. La figure 3.2 illustre le modèle de système pris en compte dans notre travail et les différents intrus pouvant l'affecter.

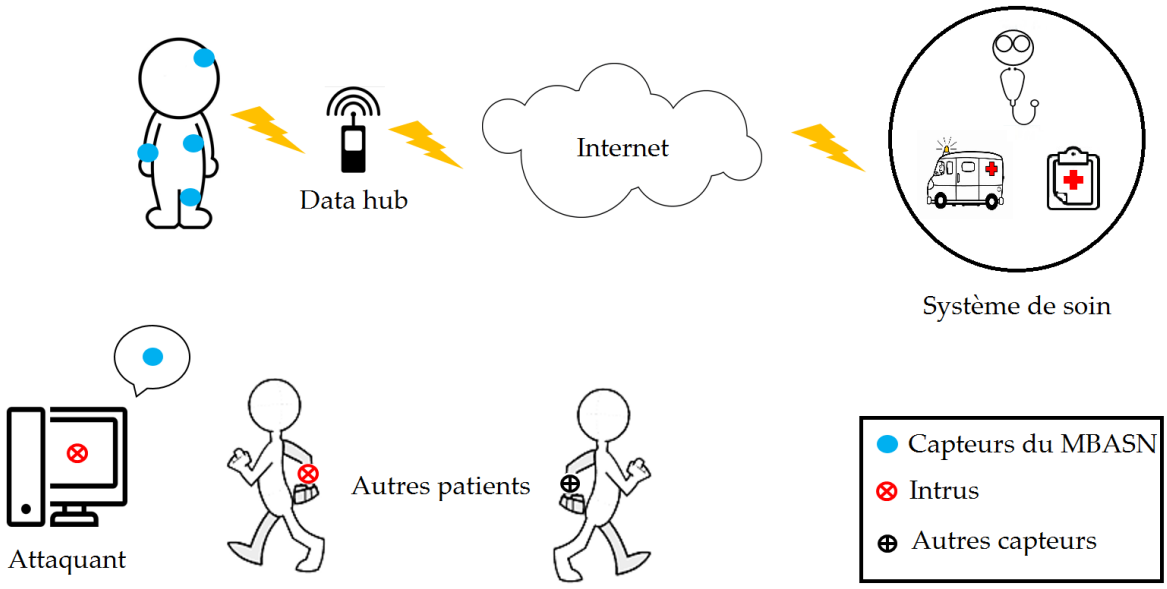

FIGURE 3.2 – Modèle du réseau.

Nous supposons, dans notre système, que les capteurs peuvent être placés sur le corps du patient ou, éventuellement, implantés dans le corps et que tous ces capteurs sont à portée. La durée de vie des capteurs peut varier selon son rôle dans l'application ; les capteurs implantés durent au moins 3 ans [21]. Seuls les capteurs ajoutés par le médecin ou le chirurgien sont légitimes et en contact direct avec le patient ; ils sont donc les seuls à pouvoir mesurer les signaux physiologiques du patient. Un intrus peut se présenter sous la forme d'un attaquant à portée des capteurs légitimes et voulant avoir accès aux informations du patient échangés dans le MBASN. Il peut aussi être un capteur porté par un autre patient mais qui est à portée des autres capteurs légitimes du MBASN.

3.6 Notre protocole

Le protocole que nous proposons permet à deux capteurs de s'échanger une clé de chiffrement symétrique avec laquelle ils pourront s'authentifier et sécuriser la communication entre eux. Ce partage de la clé se fait grâce au protocole de Diffie-Hellman basé sur les courbes elliptiques (ECDH, *Elliptic Curve Diffie-Hellman*) [2]. Ce protocole, n'assurant pas l'authentification entre les entités échangeant une clé, nous proposons d'ajouter une phase d'authentification afin de s'assurer que seuls les capteurs appartenant au même réseau MBASN peuvent s'envoyer les données sensibles du patient. L'authentification entre les capteurs se fait en utilisant une technique biométrique basée sur la mesure du signal ECG.

Ainsi, le processus de partage d'une clé symétrique et d'authentification de notre protocole passe par quatre (04) phases essentielles :

1. L'initialisation où les deux capteurs se mettent d'accord sur les différents paramètres à prendre en compte lors de l'exécution du processus d'échange de la clé et d'authentification de notre protocole.
2. L'extraction des caractéristiques biométriques à partir du signal ECG.
3. La génération et le partage d'une clé symétrique servant à chiffrer les données biométriques échangées lors de l'authentification.
4. L'authentification où les données biométriques des capteurs sont comparées.

Pour la convenance de la description, la terminologie et les notations utilisées dans notre protocole sont récapitulées dans le tableau 3.1.

Notation	**Description**
ID_i	Identifiant d'un capteur i
T_i	Délai tiré par un capteur i
F_p	Corps fini de cardinal p
E	Courbe elliptique
$G(x_g, y_g)$	Point générateur issu d'une courbe elliptique
$\langle d_i, K_i \rangle$	Clé privée/publique d'un capteur i
I_i	Vecteur de caractéristiques biométriques généré par un capteur i
I_i^d	Partie droite du vecteur de caractéristiques biométriques d'un capteur i
I_i^g	Partie gauche du vecteur de caractéristiques biométriques d'un capteur i
$H(A,B)$	Distance de Hamming entre les séquences binaires A et B
KP_{ab}	Clé partagée entre les capteurs A et B
$\langle +, \cdot \rangle$	Addition et multiplication des points sur une courbe elliptique

TABLE 3.1 – Notations utilisées dans notre protocole.

3.6.1 Phase d'initialisation

Cette première phase est primordiale pour le déroulement correct du processus de ECG-AS. Elle permet entre autre, de s'entendre sur une courbe elliptique et de générer les clés privées de chaque capteur.

Initialement, les capteurs se mettent publiquement d'accord sur un courbe elliptique $E(a,b,p)$ définie sur F_p. Les capteurs du MBASN se mettent aussi d'accord sur un point générateur $G(x_g, y_g)$, qui est utilisé pour le calcul de la clé symétrique [2].

Une fois la courbe définie et le point générateur choisi, le protocole Diffie-Hellman basé sur les courbes elliptiques [2] stipule que chaque capteur i choisisse aléatoirement un nombre d_i dans $\mathbb{N}^*$ comme clé privée. Il en dérive ensuite sa clé publique $K_i = \langle Q_i, G \rangle$ où $Q_i = d_i \cdot G$.

Le calcul de la clé privée d_i requiert généralement un algorithme de génération de nombres aléatoires. Cela engendre une consommation supplémentaires en terme de temps et de calcul, surtout si la mise à jour de cette clé se fait fréquemment. Nous proposons donc d'utiliser des caractéristiques biométriques extraites à partir d'un signal ECG comme clé privée. Les caractéristiques ayant déjà servi à l'authentification peuvent aussi être réutilisées ultérieurement comme clé privée. En effet, si l'authentification réussit, les caractéristiques biométriques formeront la nouvelle clé privée d_i'. Sinon, le capteur mesure le signal ECG à un temps aléatoire et en extraie la nouvelle clé.

3.6.2 Phase d'extraction des caractéristiques biométriques

Dans le cadre de notre travail, nous proposons une nouvelle méthode d'extraction de caractéristiques en utilisant la fonction d'intégration. Le processus d'extraction fonctionne comme illustré dans la figure 3.3.

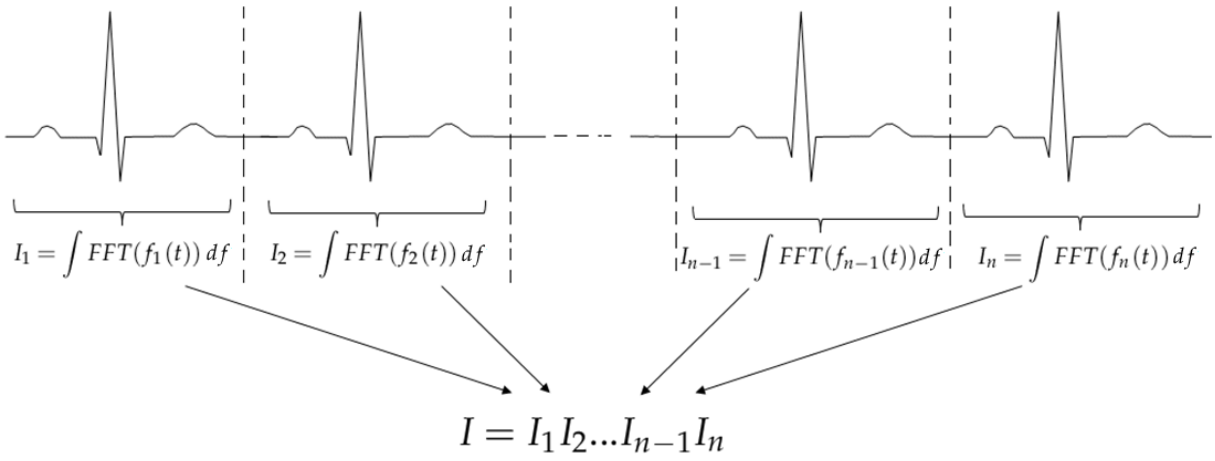

FIGURE 3.3 – Processus d'extraction des caractéristiques biométriques.

Le signal ECG mesuré est découpé en plusieurs segments égaux et chaque segment est soumis tout d'abord à une transformé de Fourier rapide (FFT, *Fast Fourier Transform*) puis à un calcul d'intégrales. La concaténation des résultats du calcul d'intégrales forment le vecteur de caractéristiques biométriques I. L'intérêt de calculer l'intégrale est de prendre en compte tous les points de la courbe formant le signal pour exploiter au maximum l'aspect chaotique du rythme cardiaque, contrairement à la méthode *Enhanced Fast Fourier Transform* (*Enhanced FFT*) [31] qui ne prend en compte qu'un nombre de points très limité.

Afin que les capteurs puissent s'authentifier à l'aide de caractéristiques biométriques basées sur le signal ECG, il est nécessaire pour les deux capteurs de se synchroniser afin de mesurer le signal ECG au même moment. L'étape de synchronisation est illustrée dans la figure 3.4.

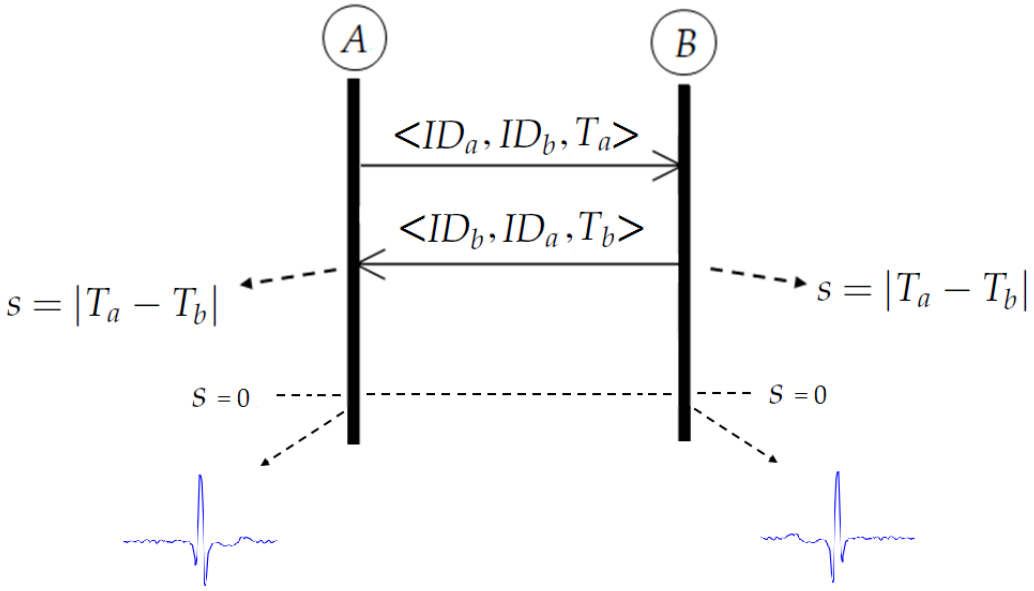

FIGURE 3.4 – Processus de synchronisation de ECG-AS.

Les différents traitements et échanges entre le capteur A et B sont décrits comme suit :

1. Le capteur A voulant communiquer avec le capteur B, envoie un message à B composé des identifiants de A et B, notés respectivement ID_a et ID_b, et d'un temps T_a.
2. B renvoie le même message avec un temps T_b différent de celui de A.
3. Chacun des capteurs calcule, la différence entre T_a et T_b. Soit s cette différence :

$$s = |T_a - T_b|. \tag{3.7}$$

4. Les capteurs attendent alors un temps s et commencent à mesurer le signal ECG pour en extraire les caractéristiques biométriques I_a et I_b de A et de B, respectivement.

3.6.3 Phase de partage de la clé

Dans cette phase, les capteurs A et B calculent une clé partagée KP_{ab} selon le protocole ECDH [2]. Les capteurs étant tous à portée, cette phase se déroule directement entre A et B sans passer par un nœud intermédiaire. Le processus de partage de la clé symétrique est décrit comme suit :

1. Les capteurs A et B s'échangent respectivement Q_a et Q_b ;
2. A calcule le point $L_a = (x_a, y_a) = d_a \cdot Q_b$;

3. Au même moment, B calcule le point $L_b = (x_b, y_b) = d_b \cdot Q_a$.

Puisque :

$$d_a \cdot Q_b = d_a \cdot d_b \cdot G = d_b \cdot d_a \cdot G = d_b \cdot Q_a, \tag{3.8}$$

alors $L_a = L_b$, d'où la clé secrète $KP_{ab} = L_a = L_b$.

3.6.4 Phase d'authentification biométrique

Cette dernière phase détermine si la clé symétrique calculée pourra être utilisée pour sécuriser la communication ou pas. La figure 3.5 illustre la phase d'authentification de notre protocole.

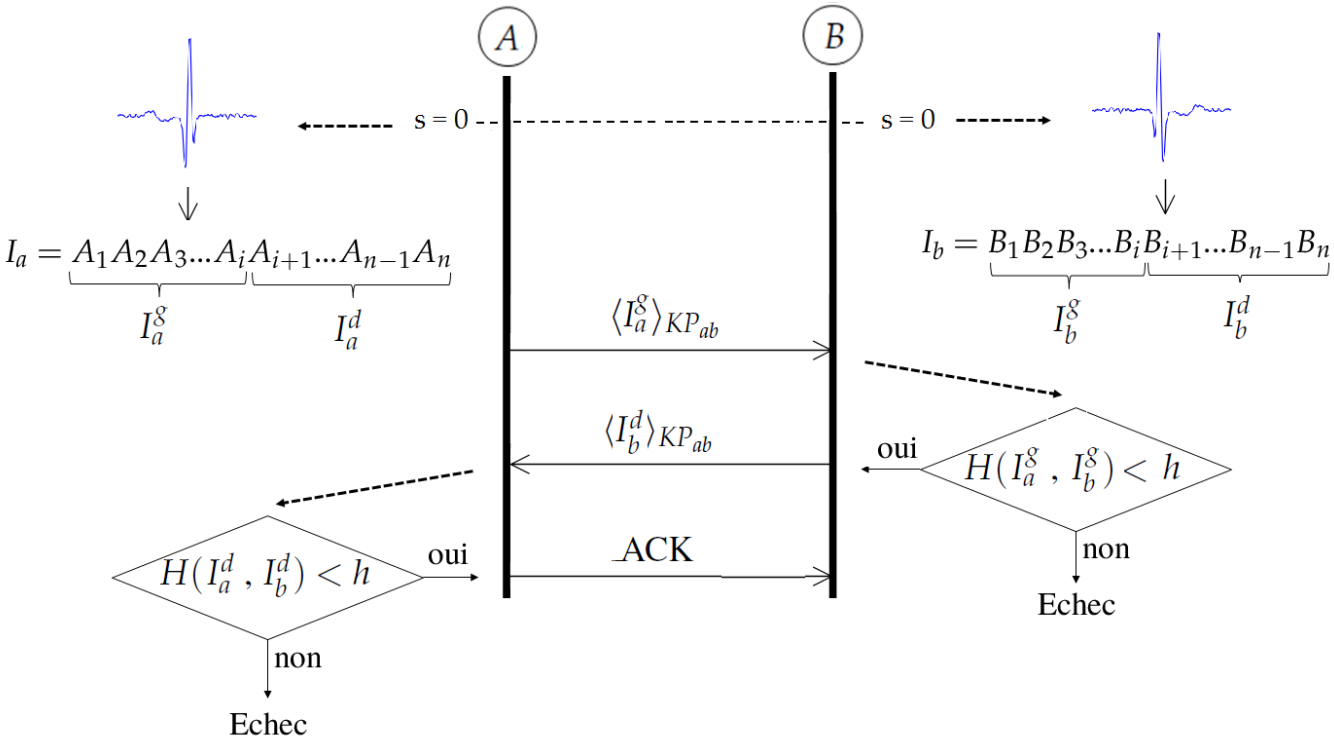

FIGURE 3.5 – Processus d'authentification biométrique de ECG-AS.

1. Les capteurs A et B divisent chacun leurs vecteurs de caractéristiques en deux parties égales, une partie gauche, I_i^g, et une partie droite, I_i^d , où $i \in \{a, b\}$.
2. A, voulant s'authentifier auprès de B, lui envoie $\langle I_a^g \rangle_{KP_{ab}}$, sa partie gauche chiffrée avec la clé symétrique KP_{ab}.

3. B déchiffre $\langle I_a^g \rangle_{KP_{ab}}$ en utilisant Kp_{ab} et calcule la distance de Hamming (H) entre sa partie gauche I_b^g et I_a^g. Si $H(I_a^g\ ,\ I_b^g) > h$, où h est la distance maximale tolérée, B conclut que A n'a pas la même version des caractéristiques que lui et rejette donc, sa demande d'authentification. Sinon, il acquitte cette demande en envoyant à son tour sa partie droite des caractéristiques biométriques I_b^d chiffrées avec KP_{ab} à A.
4. A vérifie, après déchiffrement, si la partie droite I_b^d de B est assez ressemblante à celle qu'il a. Si $H(I_a^d\ ,\ I_b^d) < h$, il envoie un acquittement à B pour confirmer la réussite de l'authentification. Dans le cas contraire, la clé K_{ab} est supprimée par les deux capteurs et l'authentification échoue.

3.7 Analyse de sécurité de notre protocole

Dans cette section, nous présenterons différentes attaques que peut subir un MBASN en général afin de mieux démontrer les différents objectifs de sécurité que notre protocole permet d'assurer.

3.7.1 Modèle d'attaque

Ci-dessous, les principales attaques que l'on peut mener sur une communication dans les MBASNs :

- **Attaque d'usurpation d'identité (*Impersonation attack*) [8] :** est une attaque consistant à se faire passer pour un capteur légitime dans le but de mener des actions que seuls les capteurs appartenant au MBASN sont autorisés à réaliser.
- **Attaque de l'homme au milieu (*Man in the middle attack*) [27] :** où l'attaquant a pour but de s'insérer entre deux entités qui communiquent, A et B, en se faisant passer pour A auprès de B et pour B auprès de A. Ainsi, toute communication vers A ou vers B passera par l'homme du milieu, qui pourra intercepter tous les messages de A et de B, récupérer des informations sensibles et pire encore, modifier les messages de l'un avant de les renvoyer vers l'autre.
- **Attaque du vol de session (*Session hijacking attack*) [8] :** un intrus attend que deux capteurs, A et B, entament une session de communication pour prendre ensuite la place de l'un d'entre eux. Si l'intrus veut pouvoir dialoguer avec A, il doit mettre hors-jeu B. Pour cela, il peut lancer une attaque par déni de service contre B par exemple.
- **Attaque Sybille (*Sybil attack*) [20] :** l'objectif de cette attaque est d'usurper l'identité de plusieurs capteurs afin de prendre l'avantage sur la plupart des capteurs légitimes du MBASN.
- **Attaque par rejeu (*Replay attack*) [20] :** consiste à réutiliser les messages échangés entre les capteurs sous leur forme cryptée. Même si un intrus ne peut pas déduire la clé de chiffrement

afin de lire les données cryptées, il peut réutiliser le message chiffré pour s'authentifier plus tard auprès des capteurs.

- **Attaque par force brute (*Brute force attack*) [18] :** est une technique utilisée en cryptanalyse pour trouver un mot de passe ou une clé de chiffrement. Il s'agit de tester, une à une, toutes les combinaisons possibles.
- **Attaque par déni de service (*Denial of service attack*) [27] :** cette attaque vise à empêcher les capteurs de réaliser une action quelconque. Cela peut se présenter sous différentes formes, entre autre, encombrer la communication entre les capteurs en utilisant toute la bande passante du réseau, ou encore, submerger un capteur par des acquittements (ACK, *ACKnowledgment*).

3.7.2 Scénarios d'attaque

Dans cette section nous analyserons le niveau de sécurité de notre protocole en démontrant comment il protège les données du patient selon les différents cas d'attaques cités précédemment.

- **Attaque d'usurpation d'identité (*Impersonation attack*) :** l'authentification biométrique est une solution pour contrer ce type d'attaque. Si un intrus I veut s'authentifier en tant que « nouveau capteur » ou en tant que capteur légitime déjà existant dans le réseau MBASN (s'il arrive à affaiblir son signal pour qu'il n'atteigne qu'une partie du réseau où le capteur dont l'identité a été usurpée ne puisse repérer l'intrusion), il doit obtenir les caractéristiques biométriques à partir du signal ECG. Or, I ne pourra pas le mesurer et le signal ECG est difficile à falsifier à cause de la nature chaotique du rythme cardiaque [22]. Supposons qu'un intrus I réussisse à échanger une clé avec un capteur A du MBASN. A la phase d'authentification, A doit attendre la partie gauche des caractéristiques de I avant de lui envoyer sa partie droite ; chose que l'intrus ne possède pas ; au bout d'un certain temps A abandonne le processus et l'authentification échoue.
- **Attaque de l'homme au milieu (*Man in the middle attack*) :** les capteurs du MBASN étant tous à portée, le processus d'authentification se fera directement entre les capteurs concernés sans passer par un quelconque nœud intermédiaire. Un intrus voulant se placer entre deux capteurs A et B n'aura pas non plus l'occasion de se faire passer pour A auprès de B et pour B auprès de A au même moment sous peine d'être repéré par les deux capteurs. L'attaque de l'homme au milieu est donc impossible à mettre en œuvre lors du partage de la clé symétrique.
- **Attaque du vol de session (*Session hijacking attack*) :** une fois les capteurs A et B authentifiés, tous les messages émanant de ces capteurs sont chiffrés avec la clé de session KP_{ab}. Un intrus, s'il attend que A s'authentifie avant de lui voler sa session, devra soit obtenir la clé secrète de A pour calculer la clé de session, soit obtenir directement Kp_{ab}. Il devra ensuite dissimuler son intrusion auprès de A avant d'usurper son identité et voler ses messages. Or, la clé KP_{ab} n'est

connue que de A et B et le calcul de d_a connaissant G et $d_a \times G$ revient à résoudre le problème du logarithme discret [2]. L'intrus ne pourra donc ni déchiffrer les messages échangés, ni se faire passer pour A s'il ne possède pas la clé KP_{ab}.

- **Attaque Sybille (*Sybil attack*) :** supposons qu'un intrus veuille se faire passer pour deux capteurs distincts auprès de A et B. Pour ce faire, il devra d'abord échanger une clé KP_{ia} avec A et une autre clé KP_{ib} avec B. Il peut ensuite tenter d'obtenir les caractéristiques biométriques de B pour pouvoir s'authentifier auprès de A et ceux de A pour s'authentifier auprès de B. Mais ni A ni B n'enverra de caractéristiques biométriques à l'intrus avant de n'en recevoir et de vérifier s'ils sont valides à travers la fonction de Hamming. L'authentification ne pourra donc pas avoir lieu. Ceci étant aussi valable pour un intrus pouvant usurper plus de deux identités, l'attaque Sybille ne peut être menée à bien.
- **Attaque par rejeu (*Replay attack*) :** un intrus ne pourra pas réutiliser les messages d'une session lors d'une autre session future puisque la clé de chiffrement est mise à jour périodiquement et les caractéristiques biométriques changent constamment avec le signal d'où elles ont été extraites. Supposons qu'un intrus arrive à intercepter le message $\langle I_a^g \rangle_{Kp_{ab}}$ ainsi que K_a, la clé publique de A. Supposons aussi que B n'ait pas encore mis à jour sa clé privée. Il utilisera K_a comme clé publique lors de l'échange de la clé avec B et réutilisera $\langle I_a^g \rangle_{Kp_{ab}}$ à la phase d'authentification pour s'authentifier. Lorsque B vérifiera les caractéristiques biométriques I_a^g après les avoir déchiffrées, il obtiendra une distance de Hamming supérieure à valeur maximale tolérée puisque les caractéristiques biométriques I_a^g, n'ayant pas été extraites d'un signal ECG mesuré à l'instant s de la session en cours, sont très différentes de celles de B.
- **Attaque par force brute (*Brute force attack*) :** l'attaque par force brute est contournée par notre protocole grâce à la randomisation et au renouvellement constant des clés de chiffrement et des caractéristiques biométriques utilisées pour l'authentification. En effet, la nature chaotique du rythme cardiaque ne permet pas retrouver facilement et rapidement les caractéristiques pouvant être extraites du signal ECG, ni même d'en déduire les prochaines ; les attaques par dictionnaire sont dans ce cas inefficaces. De plus, la limite temporelle n'octroie pas à un intrus le temps nécessaire pour tester toutes les possibilités de clés ou de caractéristiques biométriques ; pour une séquence binaire de 64 bits, un intrus aura 1.8×10^{19} possibilités de clés ou de caractéristiques biométriques à tester.
- **Attaque par déni de service (*Denial of service attack*) :** l'attaque par déni de service n'est pas prise en compte par ECG-AS dans le sens où le protocole ne peut pas empêcher cette attaque de survenir. Il assure cependant l'authentification et la confidentialité des données lorsque cette attaque se produit ou est combinée à une autre attaque. Un intrus qui, à l'aide d'un terminal, submerge le capteur A de requêtes inutiles dans le but de mener une attaque d'usurpation d'identité ou de vol de session, ne pourra ni s'authentifier, ni obtenir une quelconque information confidentielle sur le patient.

3.8 Conclusion

Ce chapitre a été consacré à la présentation de notre contribution pour la sécurité dans les MBASNs. ECG-AS est un protocole permettant à deux capteurs d'un même MBASN de se mettre d'accord sur une clé secrète qu'ils s'échangent de manière authentifiée afin de sécuriser la communication entre eux. Dans ECG-AS, le protocole Diffie-Hellman basé sur les courbes elliptiques est utilisé pour générer une clé symétrique qui assure non seulement le chiffrement mais aussi l'authentification biométrique des capteurs dans un MBASN. Nous avons aussi dédié une partie de ce chapitre à l'analyse de la sécurité de notre protocole en présentant différentes attaques qu'un MBASN peut subir et comment notre protocole protège ce type de système.

Le chapitre suivant fera l'objet d'une analyse des performances ainsi que d'une évaluation des coûts de notre protocole ECG-AS.

Chapitre 4

Expérimentation, simulation et évaluation des performances

4.1 Introduction

Après avoir décrit les différentes phases et étapes de ECG-AS dans le chapitre précédent, une évaluation des performances s'impose afin de démontrer par une expérimentation et à travers des simulations la performance de notre protocole.

Ce chapitre sera consacré à l'analyse des performances de ECG-AS. Pour cela, nous effectuerons des simulations. L'efficacité de notre méthode d'extraction des caractéristiques biométriques sera aussi démontrée à travers des experimentations menées sur un ensemble d'échantillons d'éléctrocardiogrammes (ECGs), suivies d'une comparaison avec la méthode *Enhanced Fast Fourier Transform* (FFT) [31]. Enfin, une deuxième étude comparative sera menée en terme de temps d'exécution et de taux de communication entre notre protocole ECG-AS et les protocoles de gestion de clé étudiés au deuxième chapitre.

4.2 Expérimentation de notre méthode d'extraction

Dans le cadre de cette analyse, nous avons utilisé des données ECGs recueillies auprès de 11 patients différents en utilisant des moniteurs Holter [1] fournis par l'entreprise Bejaia Equipement Médicale (BEM). Les données ECGs ont été essentiellement recueillies à des fins médicales avec une fréquence d'échantillonnage de 200Hz. Nous avons utilisé environ des données ECG mesurées pendant une durée de 2s pour chaque échantillon avec une taille de fenêtre de 30 points et un seuil de 22.

Nous avons effectué une analyse dans le domaine fréquentiel, plutôt que dans le domaine temporel. L'intérêt est que le traitement du signal ECG dans le domaine fréquentiel présente de nombreux avantages [31] :

1. Les caractéristiques extraites à partir de deux signaux physiologiques, à un moment donné, se ressemblent plus que lorsqu'ils sont représentés dans le domaine temporel, indépendamment du lieu où ils sont été mesurés sur le même corps ;
2. L'échantillon du signal physiologique nécessaire pour l'échange de clé est beaucoup plus petit ;
3. Le niveau de synchronisation exigé pour mesurer les signaux physiologiques au niveau des capteurs n'est pas très haut.

De plus, l'utilisation de la transformée de Fourier rapide (FFT, *Fast Fourier Transform*) ne requiert que $\mathcal{O}(n \log n)$ flops, contrairement aux $\mathcal{O}(n^2)$ flops nécessaires pour une transformée de Fourier Discrète [12].

Les taux de faux rejets (FRR, *False Rejection Rate*) et de fausses acceptations (FRR, *False Acceptation Rate*) sont utilisés afin d'évaluer les performances de notre méthode d'extraction de caractéristiques biométriques. La figure 4.1 montre la variation des taux FRR et FAR en fonction du nombre de bits de poids fort (MSB, *Most Significant Bit*) pris de chaque résultat du calcul d'intégrales. FRR = 0,16 et FAR = 0,17 sont les meilleurs taux et sont obtenus lorsque l'on considère MSB = 10 bits. Dans ce cas, seul 60 ms des données ECG sont utilisées pour obtenir un vecteur de caractéristiques de 128 bits.

1. Les moniteurs Holter sont de petits appareils d'enregistrement de l'ECG. Ils permettent la lecture du pouls et du rythme cardiaque au cours d'une période minimale de 24 heures pour diagnostiquer les anomalies du rythme cardiaque, plus spécifiquement pour trouver l'origine des palpitations ou des étourdissements [10].

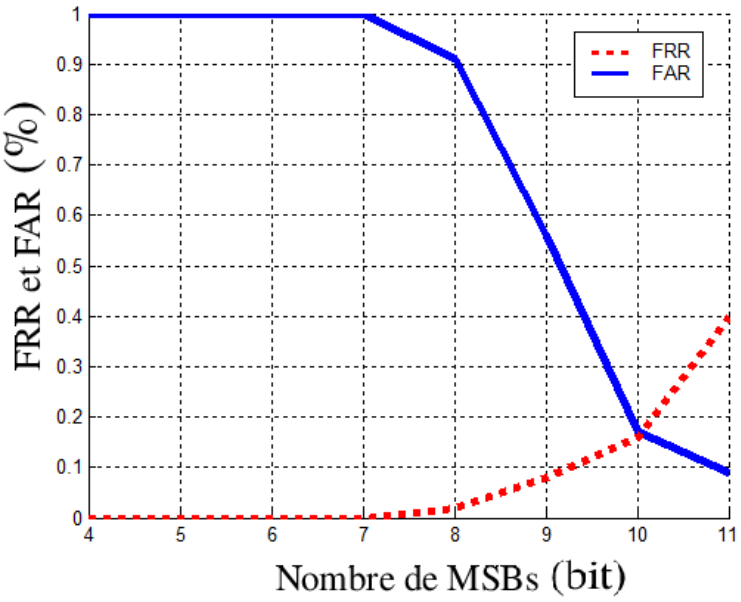

FIGURE 4.1 – FRR et FAR de notre méthode d'extraction.

4.2.1 Discussion

Alors que dans notre méthode d'éxtraction le signal ECG est soumis à un calcul d'intégrales, la méthode d'extraction Enhanced FFT de Venkatasubramanian et al. [31], utilise un algorithme de détection de pics pour obtenir les caractéristiques biométriques. En effet, la méthode Enfanced FFT ne prend en considération qu'un nombre limité de points à partir du signal ECG mesuré. Ceci entraine une perte d'information sur la nature chaotique du rythme cardiaque [24] en plus d'une latence et d'une sauvegarde d'information inutile que notre méthode ne cause pas. Il est à noter aussi qu'aucun algorithme d'interpolation n'est utilisé dans notre protocole, contrairement à la méthode Enhanced FFT qui est complétée par l'interpolation de Langrange et le « *Fuzzy vault* » afin d'obtenir les résultats utilisés lors de cette comparaison. Les meilleurs taux FRR et FAR de la méthode Enhanced FFT sont obtenus lorsque l'ordre du polynôme utilisé est 14 [31]. Nous avons comparé nos résultats avec ceux de la méthode Enhanced FFT obtenus par Venkatasubramanian et al. [31] en se basant sur les métriques citées dans le tableau 4.1.

Métriques	Enhanced FFT	Notre méthode
Taille de la population	180	100
Taille des caractéristiques (bit)	$\backsim$ 1105	128
Durée du signal (s)	$\backsim$ 4	$\backsim 60 \times 10^{-3}$
FAR (%)	0.18	0.17
FRR (%)	0.23	0.16

TABLE 4.1 – Comparaison entre la méthode Enhanced FFT et notre métode

Les résultat obtenus démontrent l'efficacité de notre méthode. En effet, elle engendre des taux FRR et FAR inférieurs à ceux de la méthode Enhanced FFT [31] et garantit une meilleure utilisation de la mémoire ainsi qu'un temps de mesure beaucoup plus inférieur ; les cas d'urgence ne seront donc pas affectés. Ainsi, les caractéristiques biométriques obtenues à travers notre méthode d'extraction peuvent très bien servir pour l'authentification et la génération de clé aléatoire. Les taux FAR et FRR ne doivent, cependant, pas être négligés lors du partage d'une clé entre deux capteurs tant que la distance de Hamming entre les deux vecteurs de caractéristiques n'est pas nulle. Autrement, la clé symétrique ne sera pas la même pour les deux capteurs ; le chiffrement et le déchiffrement seront erronés ; c'est le cas du protocole présenté par Singh et al. [29]. Dans ce protocole, il s'agit de chiffrer, à l'aide d'une opération XOR, les messages échangés par une clé directement extraite à partir des signaux physiologiques. Or, si le vecteur I_a est différent du vecteur I_b, le message chiffré $\{M\}_{I_a}$ ne pourra pas être déchiffré à l'aide de la clé I_b car $I_a \oplus M \oplus I_b \neq M$. Notre protocole utilise donc mieux les caractéristiques biométriques pour l'échange de clé.

4.3 Simulation

Cette partie sera consacrée à la simulation de ECG-AS, ainsi que des protocole de Venkatasubramanian et al. [31], Hu et al. [13], Zhang et al. [35], Kishore et al. [16] et Jammali et al. [14] qui utilisent les caractéristiques biométriques à travers différentes méthodes pour l'échange de clé.

4.3.1 Paramètres de la simulation

Les simulations ont été réalisées en utilisant le langage de programmation Java. Pour l'évaluation des performances de chaque protocole, nous avons simulé les capteurs déployés sur le corps du patient pour surveiller son état de santé. L'authentification est faite à partir des caractéristiques biométriques

extraites des signaux ECG mesurés par les capteurs sur le corps humain. Les paramètres de performance sont : le temps de traitement, qui représente le temps d'exécution nécessaire à un capteur à chaque exécution du protocole et le coût de communication, qui est le nombre total d'octets envoyés à partir d'un capteur à chaque exécution du protocole. Nous avons évalué ces paramètres en fonction de la taille de la clé de chiffrement : 128, 160, 192 et 224 bits. Les résultats de la prochaine section sont la moyenne de 20 itérations simulées et sont obtenus en utilisant un processeur de 2.4GHz et une mémoire RAM de 4Go.

4.3.2 Résultats obtenus

Les coûts de communication de ECG-AS et des protocoles de Venkatasubramanian et al. [31], Hu et al. [13], Zhang et al. [35], Kishore et al. [16] et Jammali et al. [14] sont illustrés sur la figure 4.2. Comme nous pouvons le voir, le nombre d'octets échangés par le capteur émetteur augmente pour tous les protocoles lorsque la taille de la clé augmente. Ceci est expliqué par l'augmentation de la taille des caractéristiques échangés pour l'établissement de la clé symétrique ou l'authentification. En effet, les protocoles basés sur la technique du *fuzzy vault* [31] [16] et du « Coffre » [13] se basent sur l'ajout de points aléatoires, ou « *chaff points* », pour cacher les caractéristiques biométriques envoyées ce qui, en partie, augmente la taille de messages envoyés. Les codes d'authentification de messages (MAC, *Message Authentication Code*) participent aussi à l'augmentation du coût de communication des protocoles concurrents. Nous remarquons que ECG-AS est plus performant puisque ni les *chaff points* ni les MACs ne sont nécessaires à l'authentification des messages du capteur émetteur.

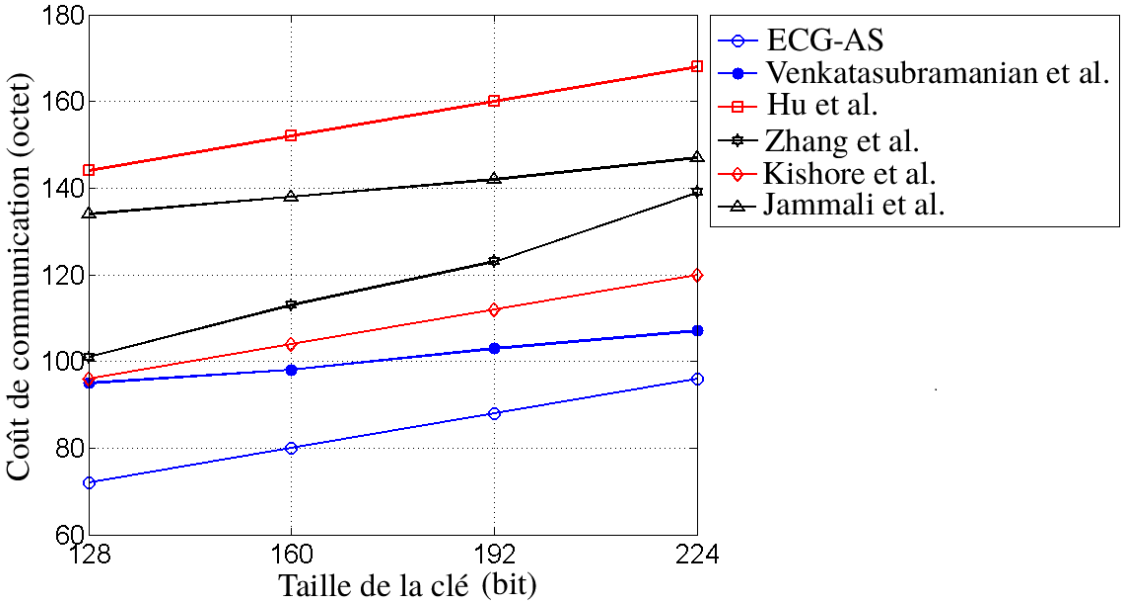

FIGURE 4.2 – Coût de communication chez l'émetteur.

La figure 4.3 illustre les résultats obtenus en terme de temps d'exécution pour ECG-AS et les protocoles concurrents. Le temps d'exécution augmente en augmentant la clé de chiffrement pour tous les protocoles. Les performances de notre protocole sont néanmoins plus élevées que les autres. Ceci est expliqué par le calcul des codes MACs. En effet, dans ECG-AS, il n'est pas nécessaire d'envoyer de tels codes avec les caractéristiques biométriques pour la phase d'authentification puisque la clé symétrique obtenue à partir du protocole de Diffie-Hellman sur courbes elliptiques (ECDH, *Elliptic Curve Diffie-Hellman*) sert à authentifier ces caractéristiques.

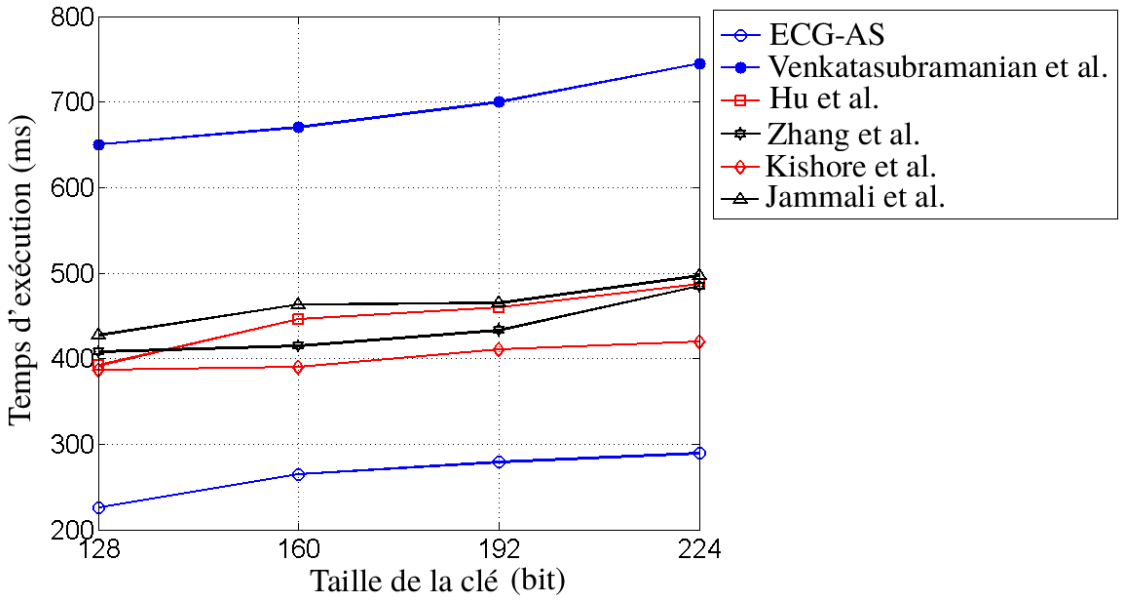

FIGURE 4.3 – Temps d'exécution chez l'émetteur.

4.4 Conclusion

Ce chapitre clôture notre travail avec une étude expérimentale sur le signal ECG ainsi que des simulations faites sur notre protocole ECG-AS et les protocoles de gestion de clés étudiés au deuxième chapitre. Les résultats de l'expérimentation ont démontré que notre méthode d'extraction de caractéristiques biométriques, basée sur le calcul d'intégrales, offre des taux FRR et FAR meilleurs que ceux de la méthode Enhanced FFT [31]. Nous en avons conclu que la durée d'extraction du signal ECG est aussi inférieure pour notre méthode, ce qui rendra le processus d'authentification plus rapide. Nous avons également évalué les performances de ECG-AS en terme de temps d'exécution et de coût de communication. Les simulations des protocoles ont démontré que ECG-AS assure un temps d'exécution et un coût de communication plus bas que tous les protocoles concurrents.

Conclusion générale et perspectives

Les *Medical Body Area Networks* (MBASNs) sont une grande évolution technologique dans le domaine de la médecine. Un MBASN est constitué de capteurs capables de mesurer les signaux physiologiques du patient pour la télémedecine. Toutefois, le déploiement d'une telle technologie est ralenti par de nombreux obstacles, notamment celui de la sécurité du patient. Ces capteurs peuvent aussi dialoguer avec un centre de soin, par exemple, pour pouvoir apporter un diagnostique et des traitements médicamenteux à distance ou alerter automatiquement les services urgences en cas d'événement grave.

L'objectif de ce travail était de proposer une solution biométrique pour l'authentification dans les systèmes mobiles de soins et de santé. Nous avons proposé à cet effet, un protocole, nommé *ECG-Authentication Scheme* (ECG-AS), qui permet à deux capteurs de pouvoir s'échanger une clé secrète tout en s'authentifiant entre eux.

Dans ce travail, nous avons mené une étude critique des recherches menées sur l'échange de clé et l'authentification biométrique intra-MBASN. Nous en avons dégagé les points faibles et points forts des différents protocoles étudiés afin de mieux établir notre solution. Nous avons ensuite détaillé les différentes phases de notre protocole ECG-AS où nous avons proposé une nouvelle méthode d'extraction des caractéristiques biométriques. Nous avons enfin, évalué notre méthode d'extraction et notre protocole à base d'une analyse de sécurité, d'expérimentations, de simulations et de comparaisons avec les différents protocoles étudiés. Nos résultats sont encourageants. En effet, nous avons démontré à travers une analyse de sécurité, la robustesse de ECG-AS contre différents types d'attaques telle que l'attaque d'usurpation d'identié. Des expérimentations sur le signal ECG ont ensuite montré que notre méthode d'extraction est caractérisée par des taux de faux rejets (FRR, *False Rejection Rate*) et de fausses acceptations (FAR, *False Acceptation Rate*) plus bas que ceux de Enhanced FFT [31] tout en

garantissant une durée de mesure du signal ECG plus courte. Enfin, la simulation de ECG-AS et des protocoles étudiés a prouvé que le temps d'exécution et le coût de communication de ECG-AS sont plus bas que les protocoles concurrents.

Une première partie de ce travail a fait l'objet d'un article de recherche accepté par une conférence internationale [34]. En guise de perspectives, notre futur travail concernera la modélisation analytique de notre protocole ECG-AS et à sa mise en œvre pratique. Nous aspirons à ce que ECG-AS soit continuellement amélioré à travers de meilleures méthodes d'extraction de caractéristiques de différents signaux physiologiques et d'étendre notre travail pour le soumettre à une revue internationale.

Bibliographie

[1] D. Acharya et V. Kumar : Security of MBAN based Health Records in Mobile Broadband Environment. *In proc. 8th Internatinal Conference on Mobile Information Systems*, pages 539–545, Ontario, 2011.

[2] M-S. Anoop : Elliptic Curve Cryptography – an implementation tutorial. Rapport technique, Tata Elxsi Ltd, 2007.

[3] A. Appari et M-E. Johnson : Information security and privacy in hhealthcare : Current state of research. *International Journal of Internet and Enterprise Management*, 06(04):pages 279–314, 2010.

[4] S-D. Bao, Y-T. Zhang et L-F. Shen : A new symmetric cryptosystem of body area sensor networks for telemedicine. *In proc. 6th Asian-Pacific Conference on Medical and Biological Engineering, Springer*, Tsukuba, 2005.

[5] S-D. Bao, Y-T. Zhang et L-F. Shen : Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. *In proc. 27th Annual International Conference of the Engineering in Medicine and Biology Society, IEEE*, pages 2455–2458, Shanghai, 2005.

[6] R-E. Blahut : *Theory and Practice of Error Control Codes*. Ed. Addison Wesley Longman Publishing Co., Massachusetts, 1983.

[7] S. Blanc : Les Intelligences de la Smart City. `http://www.lagazettedescommunes.com/dossiers/smart-city-les-cles-de-la-ville-intelligente/`, 2016. [Consulté le : 01-Juillet-2016].

[8] A. Bouadjemi : *Conception et Réalisation d'un AGL pour la Sécurisation d'Intranet Sécurisé selon un CdC Prédéfini*. Thèse de magister en Informatique, Université d'Oran, 2009.

[9] S. Chantaf : *Biométrie par Signaux Physiologiques*. Thèse de doctorat en Sciences, Université Paris-Est, 2011.

[10] Fondation des Maladies du Cœur et de l'AVC : Enregistrement ECG par la Méthode Holter. `http://www.fmcoeur.com/site/c.ntJXJ8MMIqE/b.3562269/k.5EAB/Maladies_du_coeur__Enregistrement_ECG_par_la_m233thode_Holter.htm`, 2012. [Consulté le : 10-Juin-2016].

[11] W. Diffie et M. Hellman : New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):pages 644–654, 1976.

[12] S. Haynal et H. Haynal : Generating and Searching Families of FFT Algorithms. *Journal on Satisfiability, Boolean Modeling and Computation*, 7:pages 145–187, 2011.

[13] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao et D. Chen : OPFKA : Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. *In proc. 32nd IEEE International Conference on Computer Communications, IEEE*, pages 2275–2282, Turin, 2013.

[14] N. Jammali et L-C. Fourati : PFKA : A physiological feature based key agreement for wireless body area network. *In proc. IEEE International Conference on Wireless Networks and Mobile Communications, IEEE*, pages 1–8, Marrakech, 2015.

[15] B. Johny et A. Anpalagan : Body area sensor networks : Requirements, operations and challenges. *IEEE Potentials*, 33(2):pages 21–25, 2014.

[16] V. Kishore, V. Manjula, R-T. Rajasekaran, T-M. Sridhar et C. Jayakumar : An efficient and secure key agreement scheme using physiological signals in body area network. *In proc. International Conference on Advances in Computing, Communications and Informatics, ACM*, pages 1143–1147, India, 2012.

[17] G-D. Knott : *Interpolating Cubic Splines*. Série : Progress in Computer Science and Applied Logic (num. 18). Ed. Birkhäuser Basel, Boston, 2000.

[18] F. Legendre : *Exploitation de la Logique Propositionnelle pour la Pésolution des Problèmes Cryptographiques*. Thèse de doctorat en Informatique, Université de Grenoble & Faculté des Sciences de Tunis, 2012.

[19] D. Marohn : Biometrics in healthcare. *Biometric Technology Today*, 14(9):pages 09–11, 2006.

[20] D. Martins : *Sécurité dans les Réseaux de Capteurs sans Fil : Stéganographie et Réseaux de Confiance*. Thèse de doctorat en Informatique, Université de Franche-Comté, 2010.

[21] M. Patel et J. Wang : Applications, challenges and prospective in emerging body area networking technologies. *IEEE Wireless Communications*, 17(1):pages 80–88, 2010.

[22] C-C-Y. Poon, S-D. Bao et Y-T. Zhang : A novel biometrics method to secure wireless body are sensor networks for telemedecine and m-health. *IEEE Communication Magazine*, 44(4):pages 73–81, 2006.

[23] G. Pujolle : *Les Réseaux 7e édition*. Ed. Eyrolles, Paris, 2011.

[24] I. Radojicic, D. Mandic et D. Vulic : On the Presence of Deterministic Chaos in HRV Signals. *In proc. Computers in Cardiology*, page 465–468, Rotterdam, 2001.

[25] R. Redner et H. Walker : Mixture densities, maximum likelihood and the EM algorithm. *SIAM Rev.*, 26(2):pages 195–239, 1984.

[26] D. Seguy et P. Gamache : *Sécurité PHP5 et MySQL 3e édition*. Ed. Eyrolles, Paris, 2011.

[27] L. Sfaxi : *Construction de Systèmes Répartis Sécurisés à base de Composants*. Thèse de magister en Informatique, Université de Reims Champagne-Ardenne, 2014.

[28] V-M. Sidelnikov et S-O. Shestakov : On Insecurity of Cryptosystems based on Generalized Reed-Solomon Codes. *Discrete Mathematics and Applications*, 02(4):pages 439–444, 1992.

[29] K. Singh et V. Muthukkumarasamy : Using physiological signals for authentication in a group key agreement protocol. *In proc. 30th IEEE Conference on Computer Communications Workshops, IEEE*, pages 720–725, Shanghai, 2011.

[30] U. Uludag, S. Pankanti, S. Prabhakar et A-K. Jain : Biometric cryptosystems : Issues and challenges. *Proceedings of the IEEE*, 92(6):pages 948–960, 2004.

[31] K-K. Venkatasubramanian, A. Banerjee et S-K-S. Gupta : PSKA : Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine*, 14(1):pages 60–68, 2010.

[32] W. Wang, K. Hua, M. Hempel, D. Peng, H. Sharif et H. Chen : A stochastic biometric authentication scheme using uniformed GMM in wireless body area sensor networks. *In proc. 21th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications, IEEE*, pages 1620–1624, Instanbul, 2010.

[33] L. Yao, B. Liu, K. Yao, G. Wu et J. Wang : An ECG-based signal key establishment protocol in body area networks. *In proc. 7th International Conference on Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing*, pages 233–238, Xian, Shaanxi, 2010.

[34] S. Zebboudj, F. Cherifi, M. Mohammedi et M. Omar : Secure and Efficient ECG-based Authentication Scheme for MBASNs. *Accepted in the 2nd IEEE International Smart Cities Conference, Session : Health and Well-being*, September 2016. Italy.

[35] Z. Zhang, H. Wang, A-V. Vasilakos et H. Fang : ECG-cryptography and authentication in body area networks. *IEEE Transactions on Information Technology in Biomedicine*, 16(6):pages 1070–1078, 2012.

Annexe

Article accepté à la conférence : 2^{nd} IEEE International Smart Cities Conference, Session : Health and Well-being, September, Italy. URL : http ://events.unitn.it/en/isc2-2016

Résumé

Dans les *Medical Body Area Sensor Networks* (MBASNs), les capteurs sont déployés sur ou dans le corps du patient et sont capables de communiquer en utilisant des interfaces sans fil. Ce mode de communication rend le réseau plus vulnérable aux attaques. Un intrus peut s'incruster dans le réseau et espionner, injecter ou réutiliser les données médicales. Les capteurs doivent donc être capables d'échanger des informations médicales du patient en toute sécurité. Les mécanismes de sécurité basés sur les caractéristiques biométriques permettent de générer des clés pour être partagées entre les capteurs et les authentifier. Dans ce travail, nous avons proposé un système d'authentification basé sur l'électrocardiogramme (ECG) pour les MBASNs ainsi qu'une nouvelle méthode d'extraction de caractéristiques biométriques. Cette méthode extrait, avec une grande précision, les caractéristiques basées sur l'ECG et rend l'authentification entre les capteurs plus performante. Grâce à l'analyse de la sécurité, nous avons démontré la robustesse de notre système contre les attaques ainsi que la fiabilité de notre solution en terme de coût de communication et de temps de traitement à travers des simulations.

Mots clés : MBASN, ECG, Authentication, ECDH, Télémédecine.

Abstract

In Medical Body Area Sensor Networks (MBASNs), the body medical sensors are deployed on or in the patient's body and communicate using wireless interfaces. This mode of communication makes the network more vulnerable to attacks. An intruder can encrust in the network and eavesdrops, injects or replays medical data. The sensors must be able to exchange secure medical information of the patient. The security mechanisms based on biometric features allow to hide and generate keys to be shared among the sensors. In this work, we propose an electrocardiogram-based authentication scheme for MBASNs, in which we develop a new mechanism of feature extraction. This mechanism extracts with a high precision the electrocardiogram-based features and achieves better the efficiency of authentication among the sensors. Through the security analysis, we demonstrate the robustness of our scheme against the attacks. Moreover, we demonstrate through simulations the reliability of our solution in terms of communication overhead and processing time with comparison to concurrent schemes.

Keywords : MBASN, ECG, Authentication, ECDH, Telemedicine.